Czech University of Life Sciences Prague

Faculty of Economics and Management

Department of Information Engineering

Master's Thesis

Concept of Cloud Computing & Challenges for Security Issues

Md Kamrujjaman Shimon

CZECH UNIVERSITY OF LIFE SCIENCES PRAGUE

Faculty of Economics and Management

DIPLOMA THESIS ASSIGNMENT

Md Kamrujjaman Shimon

Systems Engineering and Informatics
Informatics

Thesis title

Concept of Cloud Computing & Challenges for Security Issues

Objectives of thesis

The main objective of this thesis is to highlight the concept of cloud computing, the various cloud models, challenges for security issues and the associated benefits of cloud computing in the ICT.

However, the partial objectives are as follows:
– To evaluate the numerous factors that contributed many business companies to adopt cloud computing
– To characterize the current state of cloud services in the business world
– To analyze services of cloud computing providers for individual users and companies
– To provide a comprehensive review of the existing security and privacy issues in cloud environments
– To identify the challenges related to cloud securities and countermeasures to resolve those problems

Methodology

Research methodology refers to the process or the way of managing and solving research problems systematically. To achieve the goals of research we can use different methods, techniques and procedures. In this research paper, the explanatory approach is used for addressing the research questions and objectives. The data collected for primary research is scientific sources like digital or printed literature published by established authors. The secondary data was collected by descriptive analysis.

This thesis begins with introducing the topic area and research questions. It is also equally important a literature review to complete this research paper. The literature review is conducted based upon various scientific articles, books, journals, but also internet blogs to compensate for the shortage of scientific research. Scientific papers include several books, online sources, journals and blogs etc. published in the area of cloud computing. These resources will help to form the basis for the literature review together with the scientific papers.

The proposed extent of the thesis

60 – 80 pages

Keywords

security, cloud computing, cloud servise, cloud models, ICT

Recommended information sources

Clogger. (2014) 'Types of Cloud Computing', Cloud Drive Consulting, [Internet]. Available from: http://clouddriveconsulting.restoreup.com/2014/01/types-of-cloud-computing.html [accessed 25 August 2021].

HILL Richard, Guide to cloud computing: principles and practice. London: Springer. 2013. 278 s. ISBN 978-1-4471-4602-5

Puthal, Deepak, et al. "Cloud computing features, issues, and challenges: a big picture." 2015 International Conference on Computational Intelligence and Networks. IEEE, 2015.

Sasubilli, Manoj Kumar, and R. Venkateswarlu. "Cloud Computing Security Challenges, Threats and Vulnerabilities." 2021 6th International Conference on Inventive Computation Technologies (ICICT). IEEE, 2021.

Velte, Anthony T., Toby J. Velte, and Robert Elsenpeter. "Cloud Computing: A Practical Approach." ISSN 2278 (2019): 0181.

Expected date of thesis defence

2021/22 SS – FEM

The Diploma Thesis Supervisor

doc. Ing. Jan Tyrychtr, Ph.D.

Supervising department

Department of Information Engineering

Electronic approval: 23. 11. 2021

Ing. Martin Pelikán, Ph.D.

Head of department

Electronic approval: 25. 11. 2021

Ing. Martin Pelikán, Ph.D.

Dean

Prague on 11. 06. 2023

Declaration

I declare that I have worked on my diploma thesis titled **"Concept of Cloud Computing and Challenges for Security Issues"** by myself and I have used only the sources mentioned at the end of the thesis. As the author of the master's thesis, I declare that the thesis does not break copyrights of any their person.

In Prague on 30/11/2023 _____

Md Kamrujjaman Shimon

Acknowledgement

I would like to express my appreciation and gratitude to my supervisor doc. Ing. Jan Tyrychtr, Ph.D. for his guidance and encouragement throughout the whole thesis writing process. He gave me most of the key information on my thesis. I am always please with his patience because he always clarifies all of my concerns.

Next, I would like to thank the organizations who made time available for my interviews. The names of the interviewees will not be disclosed because of confidentiality.

Additionally, I would like to express my deepest gratefulness to my parents, and my sisters for their consistent support, advice, and patience during the course and work on this thesis.

Special thanks to God for blessing, guidance, and pushing me to work on this thesis hard and for every action toward my accomplishments.

Concept of Cloud Computing & Challenges for Security Issues

Abstract

Technology that is fast evolving and looks promising is cloud computing. The global computing infrastructure is rapidly increasing and moving to a cloud-based design. Cloud computing enables an organization's IT infrastucture to be greater flexible, more cost-effective, faster data transfer than with traditional IT. Thus, it is essential to determine if cloud computing can provide value for emerging small and medium enterprises (SMEs) or existing ICT business firms.

Cloud computing provided such solutions that can be huge benefits for SMEs in the context of IT. This study examines the potential benefits of cloud computing and the security challenges for cloud adoption while companies are migrating to a Cloud-based systems. It also provides an overview of cloud computing as well as the security challenges for organizations that arise relating to cloud computing and cloud infrastructure.

The thesis was discussed both theoretical and practical aspects of Cloud computing. The theoretical part includes the theoretical background of cloud computing, its features, cloud models, services, advantages, and disadvantages of Cloud with relevant works of literature as well as the current research concerns and implications. The practical part focuses on research of using cloud computing in business organization specially for SMEs. This part discusses how cloud security risks and threats are affecting the current and protential cloud users' decisions for adopting to their buisness. The possibilities of cloud computing are explored along with the challenges and threats in order to implement for small and medium enterprises.

This study will highlight various aspects of cloud computing in order to draw a meaningful conclusion and to make recommendations on the potential usage of cloud computing in ICT-intensive business. Furthermore, we will explore existing security threats and point out the limitations of current solutions, as well as provide insights on future security possibilities.

Keywords: Cloud computing, cloud services, cloud models, SMEs, cloud benefits, risks, security, and ICT

Koncepce cloud computingu a výzvy pro bezpečnostní problémy

Abstrakt

Technologie, která se rychle vyvíjí a vypadá slibně, je cloud computing. Globální výpočetní infrastruktura se rychle rozrůstá a přechází na cloudový design. Cloud computing umožňuje IT infrastruktuře organizace být flexibilnější, nákladově efektivnější a rychlejší přenos dat než u tradičních IT. Proto je nezbytné určit, zda cloud computing může poskytnout hodnotu pro vznikající malé a střední podniky (MSP) nebo stávající obchodní firmy v oblasti ICT.

Cloud computing poskytl taková řešení, která mohou být pro malé a střední podniky v kontextu IT obrovským přínosem. Tato studie zkoumá potenciální výhody cloud computingu a bezpečnostní výzvy pro přijetí cloudu, zatímco společnosti migrují na cloudové systémy. Poskytuje také přehled cloud computingu a také bezpečnostních výzev pro organizace, které vznikají v souvislosti s cloud computingem a cloudovou infrastrukturou.

V práci byly diskutovány teoretické i praktické aspekty Cloud computingu. Teoretická část zahrnuje teoretická východiska cloud computingu, jeho vlastnosti, cloudové modely, služby, výhody a nevýhody Cloudu s relevantními literárními díly a také aktuální výzkumné problémy a implikace. Praktická část je zaměřena na výzkum využití cloud computingu v obchodních organizacích speciálně pro malé a střední podniky. Tato část pojednává o tom, jak rizika a hrozby zabezpečení cloudu ovlivňují rozhodnutí současných a potenciálních uživatelů cloudu o přijetí do svého podnikání. Možnosti cloud computingu jsou zkoumány spolu s výzvami a hrozbami za účelem implementace pro malé a střední podniky.

Tato studie upozorní na různé aspekty cloud computingu, aby bylo možné vyvodit smysluplný závěr a poskytnout doporučení ohledně potenciálního využití cloud computingu v podnikání náročném na ICT. Dále prozkoumáme stávající bezpečnostní hrozby a poukážeme na omezení současných řešení a poskytneme pohled na budoucí možnosti zabezpečení.

Klíčová slova: Cloud computing, cloudové služby, modely cloudu, MSP, výhody cloudu, rizika, bezpečnost a ICT

Table of content

1. Introduction 15

2. Objectives and Methodology 17

2.1 Objectives 17

2.2 Research Questions 17

2.3 Methodology 18

2.3.1 Research Approach and Design 18

2.3.2 Data Collection Methods 20

2.3.3 Interview 20

2.3.4 Survey 21

2.3.5 Questionnaires 21

2.3.6 Data Sources 21

2.3.7 Collecting Data from Real World 22

2.4 Data Analysis Technique 22

3. Literature Review 23

3.1 Key Concept of Cloud Computing 23

3.1.1 What is Cloud Computing 23

3.1.2 Features of Cloud Computing 24

3.2 Types of Cloud Computing Services 24

3.2.1 Infrastructure as a Service 24

3.2.2 Platform as a Service 25

3.2.3 Software as a Service 25

3.3 Deployment Models of Cloud Computing 26

3.3.1 Public Cloud 26

3.3.2 Private Cloud 26

3.3.3 Hybrid Cloud 26
3.3.4 Community Cloud 27
3.3.5 Virtualization of a Cloud 27
3.4 Background of Computing Evolution 28
3.4.1 Overview of Cloud Computing 29
3.4.2 Historical View of Cloud Computing 30
3.4.3 Cloud Computing Compared with other Technologies 31
3.4.4 Benefits of Cloud Computing 33
3.4.5 Drawbacks of Cloud Computing 33
3.4.6 Problem Identification 34
3.4.7 Cloud Computing Adoption 35
3.5 Small and Medium Enterprises (SMEs) 35
3.5.1 Definition of SMEs 35
3.5.2 SMEs and Cloud Computing in Bangladesh 37
3.6 Cloud Computing Challenges and its Security Issues 37
3.6.1 Cloud Computing Challenges 37
3.6.2 Issues with Cloud Computing 38
3.7 Security Related Issues in Cloud Computing 39
3.7.1 Security 39
3.7.2 Privacy 41
3.7.3 Confidentiality 41
3.7.4 Load Balancing 42
3.7.5 Data Breaches 42
3.7.6 Reliability 42
3.7.7 Data Integrity 43
3.8 Others Security Threats 44

3.9 Cloud Computing Related Technologies 46

4. Practical Part 50

4.1 Introduction 50

4.2 Data Analysis 50

4.2.1 Cloud Computing Service Provider in BD 51

4.2.2 About CSP1 51

4.2.3 About CSP2 51

4.2.4 About CSP3 51

4.4.5 SMEs in Bangladesh 52

4.3 Data from Interviews Presented 52

4.3.1 Benefits of Cloud Computing 53

4.3.2 Security Issues 54

4.3.3 Security Challenges 56

4.4 Data from Survey Presented 57

4.4.1 Cloud Computing Adoption and factors influencing it 58

4.4.1.1 Current Cloud adoption percentage 58

4.4.1.2 Perceived critical benefits of cloud adoption by organizations 58

4.4.1.3 Challenges faced by organizations in cloud service implementation & management 59

4.4.1.4 Importance of security in cloud adoption decision-making 61

4.4.1.5 Relationship between knowledge of cloud computing & cloud adoption 61

4.4.1.6 Relationship between security importance and cloud adoption 63

4.4.2 Factors Influencing the Selection of Cloud Vendors & Security Considerations 65

4.4.2.1 Relationship between type of data stored in cloud and security accreditation expected by the cloud service provider 65

4.4.2.2 Data type stored in the cloud and expected security accreditation 65

4.4.2.3 Security factors influencing cloud vendor selection 66

4.4.3 Confidence/Trust in CSPs and Concerns with Cloud Service Providers 67

4.4.3.1 Concerns of cloud security in CSPs 67

4.4.3.2 Confidence in CSPs to secure cloud and security measures offered/ implemented and overall ability to handle different aspects of cloud security 68

4.4.3.3 Cloud security vs on-premises solutions security……70

4.4.4 Knowledge & Awareness of Cloud Security..... 71

4.4.4.1 Knowledge area analysis..... 71

4.4.4.2 Impact of knowledge and awareness of cloud security on the occurrence of security breaches 73

4.4.5 Implementation of Cloud Security Defensive Measures 74

4.4.5.1 Frequency of audits and occurrences of cloud security breaches or incidents ... 74

4.4.5.2 Effectiveness of Security measures in preventing breaches..... 75

4.4.5.3 Relation between Data confidentiality and security measures implemented 77

4.4.6 Challenges for SMEs when implemeting cloud security sollutions..... 78

4.4.7 Future Trends and Expectation in Cloud Computing Security..... 80

5. Results and Discussion..... 81

6. Recommendation..... 83

7. Conclusion..... 85

8. References..... 86

9. Appendix..... 95

List of Figures

Figure 1: Model of cloud computing and characteristics.....23
Figure 2: Cloud Computing Types.....27
Figure 3: Milestones of Computing History.....28
Figure 4: Cloud Adoption.....58
Figure 5: Perceived critical benefits of cloud computing by organizations.....59
Figure 6: Challenges faced by organization in cloud service implementation and management.....60
Figure 7: Importance of security in cloud adoption decision-making.....61
Figure 8: Knowledge of Cloud Computing Line FIT Plot..... adoption).....63
Figure 9: Security Importance Line Fit Plot.....64
Figure 10: Relationship between different data types and their relevant security accreditations.....66
Figure 11: Security factors when choosing vendor.....67
Figure 12: Concerns regarding security implemented by the CSPs.....68
Figure 13: Confidence in security measures.....70
Figure 14: Cloud security vs on-premises solutions security.....71
Figure 15: Knowledge and awareness related to cloud & cloud security.....73
Figure 16: Security measures applied and occurrence of security breaches or incidents...76
Figure 17: Data confidentiality and the security measures implemented.....78
Figure 18: Challenges for SMEs when implementing cloud security solutions.....79
Figure 19: The primary drivers for cloud adoption.....79
Figure 20: Future Trends and Expectations in cloud computing security.....80

List of Tables

Table 1: Europa (2022).....36
Table 2: Definitions of Bangladeshi SMEs.....37
Table 3: Regression Analysis 1..... 62
Table 4: T-Test Result (Relationship between knowledge of cloud computing and cloud adoption).....62
Table 5: Regression Analysis 2.....64
Table 6: T-Test Result (Relationship between security importance and cloud adoption).....64
Table 7: Knowledge level of cloud computing.....72
Table 8: Occurrence of Cloud Security Breaches or Incidents.....74
Table 9: Security Measure for Cloud Implementation.....77

List of abbreviations

API	Application Programming Interface
AWS	Amazon Web Service
CIA	Confidentiality, Integrity and Authentication
CSA	Cloud Security Alliance
CSP	Cloud Service Provider
EULAs	Licensing Agreements
EC2	Elastic Compute Cloud
ERP	Enterprise Resource Planning
IaaS	Infrastructure as a Service
ISO	International Organization for Standardization
ICT	Information and Communication Technology
ISP	Internet Service Provider
IT	Information Technology
ITC	Information and Technology Community
NIST	National Institute of Standards and Technologies
PaaS	Platform as a Service
QoS	Quality of Service
SaaS	Software as a Service
SLA	Service Level Agreement
SMEs	Small and Medium Enterprises
SP	Service Provider
VM	Virtual machine
XAAS	Everything as a Service
XML	Extensible Markup Language

1. Introduction

One of the most important aspects of economic and business development is that the growth of technologies specially in the field of information and communication technology (ICT) in the last fifty years or more. Hence, it is not exception for Cloud computing as well. It is a new technology which are gaining popularity in the business and IT industry. Large companies like Google, Microsoft, Amazon, IBM, and other leading cloud computing service providers are working to advance it and offering services to a large number of clients. A new paradigm in cloud computing that enables users to store data or develop applications dynamically and access them from any location at any time by connecting to an application via internet (Vaquero et al., 2008).

It also can be used to provide a platform for creating applications, infrastructure to store and work on company data, and applications to perform user regular tasks, depending on the user's needs. When a customer chooses to use cloud services, data stored in local repositories that is transferred to a remote data center (Mollah et al., 2012). This data can be accessed or managed from remote locations with the use of cloud service providers' services. This means that data must be sent via a channel (the internet) to a remote server in order to store or process it in the cloud (Iankoulova & Maya, 2012). This data processing and storage must be done with extreme caution to avoid data breaches. If appropriate security measures are not applied for data transferred and operated on the cloud, it can be more vulnerable in regards to security when stored or operated in local repositories (Yu et al., 2010).

We are aware that cloud computing is an emerging technology, and many businesses particularly small and medium enterprises or SMEs are currently embracing it. Like other businesses, SMEs have begun utilizing cloud computing in Bangladesh, however the majority of SMEs are still not completely aware of its benefits. Different studies (such as Oliveira & Martins, 2010 & Adam & Musah, 2014) indicate that cloud computing can play important role for business organizations, particularly small and medium-sized enterprises. It ensures that SMEs can take advantage of utilizing this latest technology to increase their productivity and business activities by adopting cloud computing. Thus, it is crucial for us to discuss the overall opportunities of Cloud computing and security issues for SMEs in Bangladesh.

According to the discussion above, it is very important to have a clear idea regarding Cloud computing before deploying cloud computing in business enterprises; security issues and challenges relating to cloud adoption and accessibility must be addressed (Dillon et al., 2010). It will be essential to identify security challenges for the future implementation of cloud computing as well as improving and updating solutions may overcome these challenges.

2. Objectives and Methodology

2.1 Objectives

The main objective of this thesis is to highlight the concept of cloud computing, the various cloud models, challenges for security issues and the associated benefits of cloud computing in the ICT. This research paper will identify the possible security challenges for cloud computing and some of the possible solutions for these challenges. It will explore the existing research issues and implications in cloud computing such as security, reliability, privacy, and so on.

However, the partial objectives are as follows:

- To evaluate the numerous factors that contributed many business companies to adopt cloud computing
- To characterize the current state of cloud services in the business world
- To analyze services of cloud computing providers for individual users and companies
- To provide a comprehensive review of the existing security and privacy issues in cloud environments
- To identify the challenges related to cloud securities and countermeasures to resolve those problems

2.2 Research Questions

To accomplish the research objectives stated above, the necessary knowledge will need to be acquired and combined. The following research questions will guide this research:

RQ: What exactly the cloud computing is & what impact can arise adopting it on Information Technology?

SQ1: What are the key points to build a successful cloud in the context of SMEs?

SQ2: What are the benefits and usages of cloud in our life and work?

SQ3: What are possible issues that occur with cloud computing?

SQ4: What are the security concerns of cloud computing?

SQ5: What are the possible security measures to address the security concerns?

2.3 Methodology

Research methodology refers to the process or the way of managing and solving research problems systematically. To achieve the goals of this research, we can use different methods, techniques and procedures. In this research paper, the explanatory approach is used for addressing the research questions and objectives. The data collected for primary research is scientific sources like digital or printed literature published by established authors. The secondary data was collected by descriptive analysis.
This thesis begins with introducing the topic area and research questions. It is also equally important a literature review to complete this research paper. The literature review is conducted based upon various scientific articles, books, journals, but also internet blogs to compensate for the shortage of scientific research in the area of cloud computing. These resources will help me in creating the framework for the literature review in this research.

This thesis is written based on scientific papers through the examination of published materials and studies. This also analyzes the existing issues along with available countermeasures in order to assess the overall concept of cloud computing and the challenges for security issues. Online resources and technical whitepapers will be referenced to a certain degree in order to present and analyze the latest trends in cloud computing in the context of ICT.
There is an online survey using questionnaires and interview conducted as empirical approaches in this study by selecting the target group of exsisting and prospective cloud users for getting real-world views on cloud computing security. The analysis has been carried out using Microsoft Excel to develop general explanations based upon the information gathered from the literature review and the outcome from the practical part. It helps the researcher to identify the key findings to formulate the recommendations and conclusion.

2.3.1 Research Approach and Design

Research approach is the process used to carry out and evaluate a research development. Two important approaches of research qualitative and quantitative are used to complete this thesis. The researcher used a qualitative approach first for exploratory purposes before

switching to a quantitative approach to provide more detailed and comprehensive examination of the study problem. Qualitative data gave the researcher in-depth knowledge of cloud service providers and cloud services in the context of IT, while quantitative data gave a broad generalized trend about SMEs in Bangladesh and the usage of cloud services. As cloud adoption continues to grow in many organizations, it becomes crucial to understand the factors that influencing cloud adoption associated with security considerations. In this paper, we will analyze cloud computing and its adoption trends, key factors for businesses, security concerns, knowledge and awareness of cloud security. Moreover, we will employ a wide range of data analysis and statistical techniques, both qualitative and quantitative to derive meaningful insights from the collected data.

A quantitative methodology is used for this study as it intended to quantify data from the survey in order to provide an analysis regarding cloud adoption and the associated security considerations based on the selected sample. Additionally, beacuse the generalizability of the findings, the data can be analyzed in order to create possible measures using numbers and statistics to determine whether or not the hypotheses should be rejected (Ghauri & Grønhaug, 2005; Bryman & Cramer, 2004).
Security is the main concern of cloud computing, so will explore the significance of security considerations in organizations' decision-making processes and examine the relationship between knowledge of cloud computing and cloud adoption. By conducting regression analyses, we quantify the impact of knowledge on cloud adoption and highlight the positive correlation between the two variables. Additionally, we assess the importance of security in the selection of cloud vendors, analysing the factors that organizations prioritize, such as data protection regulations, certifications, disaster recovery capabilities, and transparency in security procedures.

Other suitable methods will be used for this study. Microsoft Excel will be used for data analysis. Charts, graphs, and table were produced by exporting responses to an Excel file. In order to perform a regression analysis for my thesis, I must first create an independent variable. Afterwards, I may determine how changes in the dependent variable are connected to the independent variable's value.

$Yi = \beta 0 + \beta 1 Xi + \in i$

Where, Yi = dependent variable.

$\beta 0$ = intercept.

Xi =independent variable

$\in i$ = disturbance term

Linear regression usually takes data from an existing data set of measurements of the values of two variables, X and Y, to create a model that can predict the value of the dependent variable, Y, for given values of X.

2.3.2 Data Collection Methods

The most crucial aspect of the research is data collection for drawing conclusion. This study explores the potential benefits and security challenges of implementing cloud computing for SMEs in Bangladesh. Interviews with cloud service providers and experts highlighted potential benefits, weaknesses, and effects, while online survey from cloud users collected insightful feedback, views, their individual security concerns and previously encountered security risks. The author conducted structured qualitative interviews and online surveys with cloud service providers, cloud users, IT professionals and managers from SMEs throughout the empirical phase. For in-depth knowledge from their first-hand experience, it was decided to conduct at least three interviews with practitioners dealing with cloud security risks. This gave them the ability to express and share their expertise on a more personal level. This approach also helps in determining the benefits and effects of cloud computing on SMEs that have not yet adopted, but are considering to embrace it for therir business. The usage of cloud services by SMEs is generally recognized to increase productivity and efficiency in addition to reducing administrative costs.

2.3.3 Interview

Interview is a strategy for gathering information from individuals through discussion. Besides, it is a technique for gathering information and expertise from participants. Data obtained from respondents is used as the investigation's major source of information. It is quite impressive for a researcher because it does not require many technological concerns initially and only need a skill to organize a discussion. According to (Gray, 2004), using interviews is beneficial for the following reasons.

- Needed for highly personalized data
- Potential need for investigation
- Reasonable response rate
- Respondents' language issues

2.3.4 Survey

Surveys are considered the most effective technique for gathering the original data from a population that is too large for observation directly (Suzanne, 1998). By asking questions of a sample from the responds, surveys often help the researcher in understanding and interpreting the findings (John, 2008).

2.3.5 Questionnaires

The approach of collecting data through questionnaires is extremely effective and flexible. It needs to be done very precisely to fulfill the criteria of a specific thing in research, otherwise it might overlook the important aspects that need to be taken into consideration before using. A questionnaire is a very cost-effective way to collect data from large groups of people with little effort and expense (Walliman, 2001). The quickest and least costly method of gathering data is a questionnaire, which has advantages and disadvantages (Bot et al., 2013). According to (Kveton et al., 2007), a web-based questionnaire is the most practical method for quickly and reasonably gathering data.

2.3.6 Data sources

The purpose of this section to verify the gathered information with experts who have practical expertise with cloud computing. Data was collected using two different approaches. Firstly, interviewees were given open-ended questions during an interview. This was done intentionally as we wanted to see if they would identify the same issues that we have addressed in this thesis without influencing their responses. The service providers were targeted for these interviews.

The second technique of data collection was conducting a survey using specific questions to direct the respondents. There were four categories of questions: technical, security-related, challenges and data categorization. The target group for the survey were companies who recently implemented cloud computing services or in the process of implementing it. Thus, they would be familiar with the issues they had to deal with as a way to make the implementation work.

2.3.7 Collecting Data from Real World

The interview is a procedure for getting detailed information to the interviewer's questions from the participant. Here the interviewer asks a question and anticipates receiving a response in return. To get the necessary information, the interviewer might also modify the questions based on the answers. On the other hand, the surveys often begin with a set of predetermined questions that are directed to a particular group of people. Surveys have been chosen over other empirical study techniques because they are typically simple and fast to complete. The surveys are used to provide a quantitative or numerical analysis of trends, opinions, or attitudes (John, 2008).

2.4 Data Analysis Technique

The qualitative and quantitative research approach are being used for this thesis. A qualitative study provides information about people's experiences, behaviors, and attitudes. In contrast, a quantitative study may undoubtedly produce statistical evidence using techniques like survey research or quantitative questionnaires (Dawson, 2002). It would be more reliant on interviews, questionnaires or numerical information from particular analyses.

There are a number of common steps that can be identified for this research. The thesis begins with a review of the relevant literature in the field of cloud computing. It covers every details of the thesis topic. The interviews come next that provide a basic information for the initial analysis. Then the survey is enhanced with brief questions, multiple-choice questions, and some questions with a likert scale to collect data on various necessary criteria. The primary data was obtained through a survey utilizing this questionnaire. Various websites, journals, scientific articles, books, and other publications are used as secondary data sources for this study. From this point, the data for the entire thesis may be analyzed. Finally, we can discuss our findings and address the main research question. The conclusion is based on both the main research topic and the supporting questions.

3. Literature Review

3.1 Key Concept of Cloud Computing

3.1.1 What is Cloud Computing

There is no widely accepted definition of cloud computing till now. There are numerous definitions can be found for cloud computing. Simply, cloud computing is the delivery of various services over the Internet. These resources include tools and applications such as data storage, servers, databases, networking, and software. The National Institute of Standards and Technology (NIST) defines cloud computing as follows (Mell & Grance, 2011).

"Cloud computing is a model which enables suitable, on-demand network access to a shared pool of resources configurable computing resources (e.g.,services, networks, data centers, applications and storage) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

A definition of cloud computing must acknowledge the underlying traits that identify cloud computing services. The National Institute of Standards and Technology (NIST) identified five basic characteristics of cloud computing which include: on-demand self-service, broad network access, resource pooling, rapid elasticity or extension, and measured service.

Cloud computing architecture consists of three layers: (i) Software as a service (SaaS); (ii) Platform as a service (PaaS) and (iii) Infrastructure as a service (IaaS).

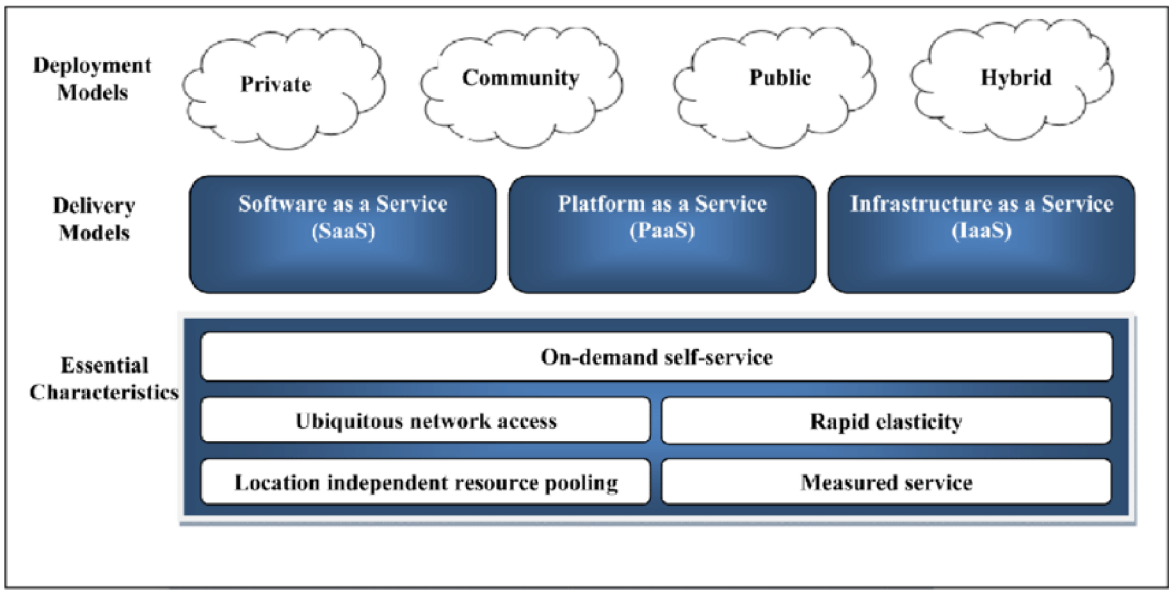

Figure 1: Model of cloud computing and characteristics (Mell & Grance, 2011)

3.1.2 Features of Cloud Computing

Cloud computing brings a number of new features and benefits compared to traditional concepts of computing. These features are described as follows.

- Scalability and On-Demand Services - Users of cloud can access resources and services in the cloud whenever they needed. The resources are scalable means multiple data centers are able to provide the resources.
- Quality of Service (QoS) - Cloud computing can ensure to their customer that they have access to bandwidth, memory, and hardware/processor performance while using cloud computing.
- User-friendly Interface - Web services and web browsers are two examples of well-known interfaces that may access cloud interfaces from any location.
- Autonomous System - Cloud computing are independent and openly controlled for users. It means software and data stored in the cloud can be automatically modified and merged into a systém depending on user's needs.
- Cost/pricing of Cloud - It does not require any kind of investment. Customers of cloud can pay or choose to pay for services and capacity as needed.

3.2 Types of Cloud Computing Services

Cloud computing has different types of services. It could possibly be broken down into three major service delivery segments. This section will go through these three different categories of technical skills that are offered as services (Narasimhan, 2009).

3.2.1 Infrastructure as a Service

IaaS stands for infrastructure as a service. The most fundamental service model and the one with the most control over the infrastructure resources is IaaS. It provides virtual machines with low-level services like storage, a perimeter firewall, load balancing, or IP addresses provided. It is logical that enterprises who must manage their entire virtual infrastructure and only pay for the resources they use (OpEx cost model) will select an IaaS service (Subashini, 2010). One such example is Amazon Web Services, where infrastructure is offered on a pay-per-use self-service basis. Customers may obtain servers, storage, and network configuration, put all of that up, and operate it without worrying about co-location, renting, or datacenters (Amazon, 2022).

3.2.2 Platform as a Service

The second level is PaaS, which is beneficial for developers who must build their own applications, install them, and maintain them while the service provider handles all the underlying infrastructure-related tasks like managing networks, servers, storage, etc. (Subashini, 2010). It offers the customer a computing platform and a solution stack as a service with tools and libraries (Mell & Grance, 2011). Examples of this approach are based on Application Programming Interfaces (APIs) and Software Development Kits (SDKs), which make it simple to create environments and applications.

Developers may take use of these services, which allow them to manage their own hardware and software, as well as a solution stack, online. This service covers the whole lifecycle of an application or service's deployment, including design, implementation, testing, deployment, database integrity, and so on. This service has three distinguishing features (Pahl & Xiong, 2013):

- Testing and maintenance of apps may be provided by these services
- Scalability, or multi-user architecture.
- Collaborative tools are essential for a successful project. Google's App Engine is an example of this kind of service.

3.2.3 Software as a Service

SaaS is the highest-level cloud computing model. SaaS is a software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted in the cloud (Mell & Grance, 2011) customers receive a full software package that is available when it is needed for a monthly or yearly charge. There is, however, a limit to how much customization the vendor will allow. Gmail is one of the most popular instances of an application of this type, and it is based on a multi-tenant architecture. In this architecture, all customers utilize the same version of the program with the same settings. Applications are frequently scaled horizontally in order to provide scalability, (Cloud Academy, 2016).

These are Internet-based apps. Typically, these programs may be operated via a web browser. Using a web browser, the user may access various data and features without having to worry about the specifics of the hardware or program being used. Dedicated to present users, such as Google Docs, is one example (Satyanarayana, 2012).

3.3 Deployment Models of Cloud Computing:

According to NIST, there are primarily four types of cloud models: public cloud, private cloud, hybrid cloud, and community cloud.

3.3.1 Public Clouds

A public cloud includes the classic idea of cloud computing, allowing users to use computer resources from any location in the globe. It is possible to use the clouds in a so-called pay-per-use fashion, which means that only the resources that are really used will be covered by transaction costs (Armbrust et al., 2009; Johnston, 2009). The resources are distributed widely, and users can access them from many places throughout the world (Rauline, 2011). Public cloud examples that are often used include Microsoft Azure Service Platform, Google App Engine, and Amazon Elastic Cloud Compute.

3.3.2 Private Clouds

A private cloud is identical to a public cloud, except it is exclusively run and created for a single business (Finn, 2012). It is often controlled by the IT department and works inside the corporate boundaries of the company. It is clear that a private cloud is more secure than the typical public clouds. It provides better cloud security and customizability by resolving the issues of control over data and applications (Mike, 2012).

3.3.3 Hybrid Clouds

A hybrid cloud combines two or more similar or different cloud models to provide customers the advantages of each. The clouds inside the hybrid are still separate, but they are connected in such a way that a user may benefit from both cloud deployment models' advantages (Ghanam, 2012). Typically, when an organization uses a hybrid cloud, just a small portion of the cloud resources are maintained internally and the majority are handled by a cloud service provider (Mike, 2012).

An overview of all three cloud computing types is illustrated by the graph below:

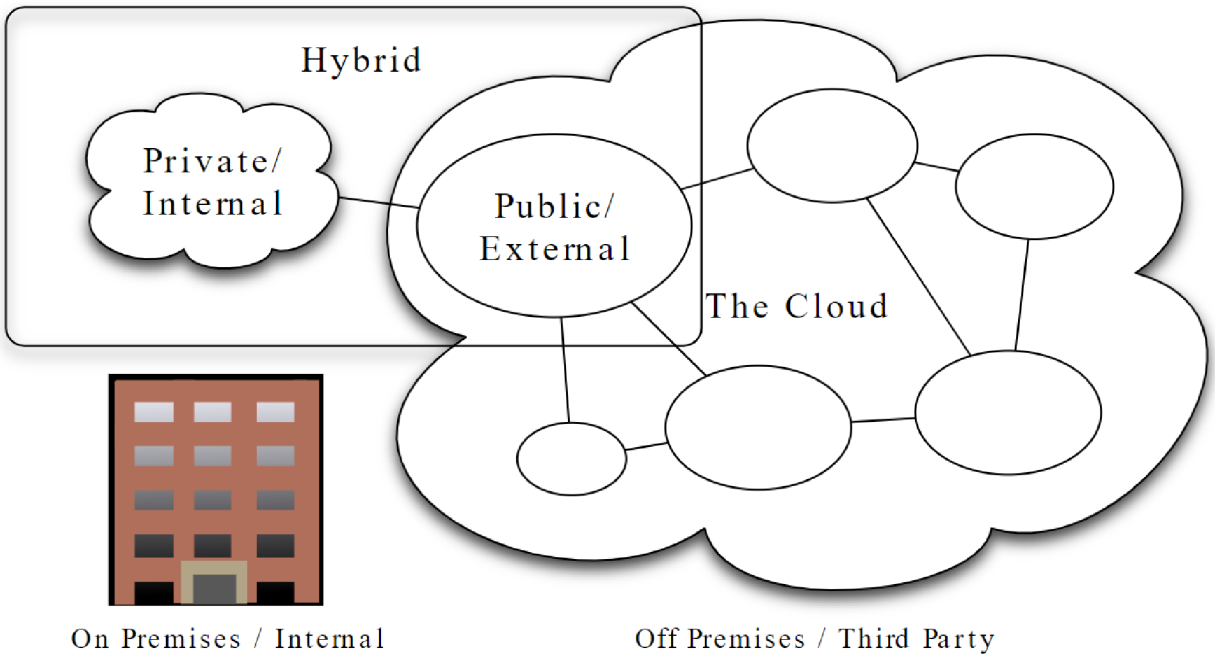

Figure 2: Cloud Computing Types (Johnston, 2009)

3.3.4 Community Cloud

This type of cloud infrastructure supports a specific group with similar needs and requirements used by a number of organizations. Community cloud offers the advantages of both public and private clouds, including multi-tenancy, pay-as-you-go charging, and an increased degree of security, privacy, and policy compliance controls. On-premises or off-premises hosting options are available for the community cloud, which can be maintained internally or by a third party (Rouse, 2012).

3.3.5 Virtualization of a Cloud

Virtualization is an important feature in cloud computing services and facilities. It allows to build the integration of several independent systems into a single hardware platform by creating a virtualized computing resources such as network, server, CPUs, storage, and so on (Singh et al., 2016). It helps the IT team to create, manage, and deploy the cloud and increases the cloud's agility, scalability, and operability (Cafaro & Aloisio, 2010).

3.4 Background of Computing Evolution

The concept of a computer or information utility is becoming immensely popular day by day. John McCarthy, a well-known computer scientist, predicted in 1961 that computer time-sharing technology would lead to a future in which computing power and even specific programs might be marketed via the utility business model (McCarthy, 1961). This plan, however, was never fulfilled since information and communication technologies could not support it at the time. Recent advancements in information and communication technology have resulted in a more distributed computer environment, while simultaneously revitalizing the utility of centralized storage.

Cloud computing is an example of utility computing, in which computing is considered as a public utility. Cloud computing has progressed through Grid and Utility Computing, Application Service Providers, Software as a Service, and now Cloud (Stark, 2012). Today, cloud computing refers to a set of services offered through the Internet and tailored specifically to the size, industry, or present needs of a firm. Solutions can range from a single SaaS application for several users to a team of technology specialists who supplement an internal IT team or a fully outsourced, virtual IT department that can take full responsibility for day-to-day management. Cloud computing provides businesses with a far more flexible and configurable strategy than traditional on-premise computers. Cloud computing provides enterprises with a much more flexible and configurable paradigm than traditional on-site computing.

The graph below, adapted from Bohm et al, depicts computing history milestones.

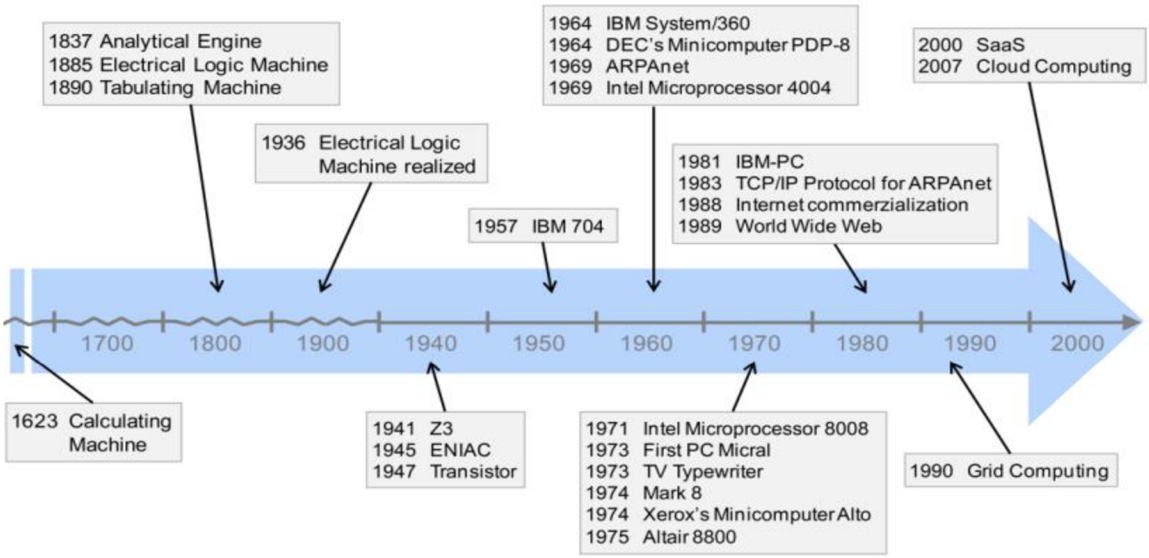

Figure 3: Milestones of computing history (own exhibit) Source: Bohm et al

3.4.1 Overview of Cloud Computing

Cloud computing refers to a system in which data is stored in a networked cloud that is fully hidden from end users and underlies all of the previously mentioned technologies (Sadiku et al., 2014). A cloud computing definition has yet to be established. Various definitions offered by credible entities will be used to try to come up with a solution to this problem. Whatis.com defines cloud computing as "anything that incorporates the provision of hosted services through the Internet." There are three distinct advantages to using a cloud service over traditional hosting. Any length of time needed by the customer can be purchased, and the service is handled entirely by the provider (the customer need only have access to a computer with Internet connectivity in order to use this service)." It is defined as "a paradigm in which information is permanently stored on servers over the internet and cached briefly on clients" by the IEEE.

According to one of the world's most recognized technical institutions, "cloud computing" is defined as: "Cloud Computing refers to both a service that is offered via the Internet and the gear and software in the datacenters that enable such services," As a result, cloud computing is a computing paradigm that relies on the consumption of resources, such as computing power and software, that can be accessible through the internet and used at the user's leisure. All of these services are governed by service level agreements, regardless of whether they are free, public, or subject to regulation. Service level agreements control these services. Generalist solutions are frequently the focus since they are intended to benefit the greatest number of people.

Internet and new technologies are already a part of daily life for many people, whether they're doing it for work or just for fun. Any piece of information can be found at any moment, wherever in the world. That was unthinkable just a few short years ago. In the modern era, there are numerous ways to gain access to both public and private information, such as high-speed internet and mobile devices that provide Internet access virtually anywhere. Most of us are now checking our email on the internet, creating collaborative papers using web browsers and uploading holiday photos to virtual albums. They are using the Internet to run apps and store data, rather than their own computers. Users require nothing more than a simple web page to begin using services that are hosted on a remote server and allow them to share sensitive information or access the processing power of a large number of servers that they will never be able to see in real life (Antonopoulos &

Gillam, 2010). More and more people are making use of the so-called "cloud computing services." It's because of this assumption that the Internet is like a cloud that the user can't see what's inside.

A simple function call (such as requesting the current temperature in a particular city around the world for inclusion in a web page), as well as more complex ones (such as the use of a virtual machine with its own operating system, applications, and storage space for running applications), can be provided for free or on a demand basis (pay for consumption) (like the usage of a virtual machine with its own operating system, applications and storage space for running applications). Users and businesses can avoid installing software on their computers or increase their computing capacity by using a cloud computer connected to the internet, or create their own private cloud and administer it completely, or combine both options when demand is strong (Hayes, 2008).

3.4.2 Historical View of Cloud Computing

"Computation may eventually be structured as a public utility," John McCarthy predicted in the 1960s. There's nothing concrete about this. As if it were an electricity provider, the customer requests the exact amount they want and only pays for what they really use. This creates the appearance of an endless supply. While we're at it, let's take a look back in time. Large mainframe computers were used in the early 1960s and 1970s to deliver services to employees who could access them through dumb terminals. All of the information and calculations were done by these computers. The mainframe received commands from a dumb terminal and returned the information to that terminal, which was connected to the Internet. However, the cost of these mainframes was prohibitive. Servers based on ordinary computers were discovered in the 1980s, and they proved to be cheaper than mainframes. Users were able to feel more in control because of this. Consequently, these mainframes were increasingly being replaced by computers for the end-users, as personal computers became more affordable. It was in the 1990s, when the Internet was beginning to take hold throughout the world that the trend of many computers accessing a single server returned (Armbrust et al., 2010).

A lot of power was needed on the web servers at that time to handle the traffic. Since then, the Internet has grown in both the number of services it provides and the amount of storage it requires from its users. Computer programmers' logic is increasingly being moved to

Internet servers because of the internet increasing speed and accessibility (mobile dispositive). A single infrastructure may now be used by a large number of people, boosting its efficiency while simultaneously lowering its costs, because big-processing businesses can handle it (Mollah et al., 2012).

A brief history of the cloud Distributed computing and grid computing have evolved into Cloud Computing (CC). CC has evolved over time, and many firms are now considering using it as a means of communication. In the 1960s, J.C.R. Licklider and many other researchers dreamed of better interconnecting systems, which led to the creation of ARPANET (Advance Research Projects Agency Network). ARPANET's role in connecting a group of computers led to the development of the Internet, where bridging the gap between systems became easy.

The Internet has facilitated a wide range of activities, including human interaction (via social media and instant messaging, for example) and corporate needs (online shopping, financial services, etc.). Further progress in this area of the Internet led to the development of ASP, grid and utility computing, and cloud computing. Conventional interconnection of systems was replaced by a shared resource pool accessed via the internet. CC introduced a new paradigm.

Data centers used less than 10% of their capacity at the end of the dot-com bubble in the late 1990s because they wanted to save the rest for spikes. One of the earliest concepts in cloud computing, on-demand computing, was employed by Amazon to address this issue. For the first time in 1999, Salesforce.com offered software as a service (SaaS) to businesses via their website. It was in 2002 that Amazon released AWS, a set of services that included storage and compute power. Online retailer Amazon introduced EC2 in 2006, which allowed small businesses and individuals to run their own cloud-based computer applications. Eucalyptus was the first open-source AWS API-compliant solution for building private clouds after it was launched in 2008. Apps was launched in 2009 as part of the company's browser-based corporate software suite, Google Apps.

3.4.3 Cloud Computing Compared with Other Technologies

With a better grasp of what cloud computing is, we might notice some similarities with other technologies. This part explains what cloud computing is and how it differs from similar-looking technology. Because most of these technologies are older than cloud

computing and are more familiar to the audience; consequently, they must be distinguished from cloud computing.

Autonomic computing systems are the first to be combined with cloud computing. This type of computing differs in its operation. The purpose of autonomic computing is to develop systems that operate autonomously (White, 2004). This means they must be capable of self-management. They must configure and repair failures themselves. It is related to cloud computing because it includes large computer systems with high-level human guidance.

Cloud computing is frequently mistaken with grid computing, despite the fact that the concepts are different. Cloud computing is often confused with grid computing although the concept is different. In grid computing, a network of computers share processing power to solve a single problem, whereas cloud computing uses a series of smaller applications that run independently on a system. Grid computing focuses on large-scale computing, while cloud computing delivers services for both small and large-scale computing. Grid computing often gives high performance constantly, however cloud computing (the primary advantage) provides performance just when needed (Buyya & Murshed, 2002).

Another comparison is made with mainframes; the differences are obvious, but there are also similarities. A mainframe can be compared to a cloud. Despite the fact that it is obvious that a mainframe provides access to employees in large organizations and the mainframe is entirely centralized. That is where cloud computing differs, as does its performance. Mainframes provide constant high performance and cloud computing just when needed (Armbrust et al, 2009).

Peer-to-peer systems have also been compared. This is because there is a complete cloud of users who are both "clients" and "servers" (Stoica et al., 2002). This is another distinction. Clients in cloud computing do not function as service providers.

The final comparison that is discussed is with service-oriented computing. Of course, cloud computing is a service. However, service-oriented computing focuses on techniques that run in the cloud. As previously stated, cloud computing focuses on providing computing services rather than the techniques.

3.4.4 Benefits of Cloud Computing

Some of the most common advantages of cloud computing are as follows (John & James, 2009):

- Lower Costs: As cloud technology is implemented incrementally (step by step), enterprises save money overall.
- More Storage: When compared to private computer systems, huge amounts of storage are available.
- Flexibility: When compared to traditional computer approaches, cloud computing allows an entire organizational segment or portion of it to be outsourced.
- Greater mobility: Having access to information whenever and wherever it is required in contrast to traditional systems (which store data on personal computers and allow access to it only when close to it.
- IT emphasis shift: Organizations can shift their attention to innovation (i.e., creating new product strategies) rather than worrying about maintenance difficulties like software updates or computing issues.

The Information and Technology Community (ITC) is very interested in the benefits of cloud computing. According to an ITC survey conducted in 2008 and 2009, many firms and individuals are coming to realize that CC is more beneficial than traditional computer methods (Ramgovind et al., 2010).

There is widespread acceptance of the benefits of cloud computing for small, medium, and large businesses. As the cloud has developed over the past few years, greater interest has been shown from various kinds of businesses and individual users. The usage of cloud computing increased to 77% from 63%, according to Right Scale (Weins, 2016), which focuses on infrastructure as a service. Nearly two-thirds of the world's population will have access to the Internet by 2023, according to a different Cisco research (Cisco, 2020). By 2023, there will be 5.3 billion Internet users worldwide, which is an increase from 2018's 3.9 billion users (or 51% of the world's population).

3.4.5 Drawbacks of Cloud Computing

Despite all its advantages, cloud computing has a number of security concerns. One of the key issues is the necessity to make organizational information available to everyone in the globe. Organizations are essentially turning up their data to outside service providers when

they switch to distributed computing, who then store and process it in the cloud (Horrigan, 2008).

- There are security and privacy issues while utilizing services from other vendors.
- As it is an internet-based service, it faces the risk of downtime i.e. internet breakdown or connection problems
- It is vulnerable and prone to cyber attacks.
- Vendor lock-in – It occurs when a customer of cloud wants to move to a different vendor services but they are unable to do it without paying a considerable costs.

3.4.6 Problem Identification

If a corporation or a consumer is dealing with a large amount of data or a complicated activity, they will require a lot of processing power to get it done. If personal computers are not able to do the work within a certain amount of time, then it could be pointless to buy the required hardware. Scilab, for example, may be unproductive for a user who just needs to use the application once or twice, such as in university labs. For these reasons, we think it's a good idea to let people use some programs without installing them on their own computers, as well as provide them the option of getting greater processing power. In other words, we must provide the means for students to resolve issues with the university's cloud. If you wish to run Scilab on a cloud service like Eucalyptus, you don't need to know about the underlying infrastructure, because you're dealing with apps and not infrastructure; as we'll see later. Using Scilab on the cloud necessitates a user-friendly interface, which necessitates the user to know their instructions and how to utilize them.

A user-friendly interface for accessing and running applications housed in the eucalyptus private cloud is the purpose of this thesis. To achieve this, Eucalyptus need a programming language that it can communicate with. EC2 and Eucalyptus share a number of commonalities. Typica, a Java API that can interface with Amazon EC2 and Eucalyptus, requires a little searching because these web services are interoperable with all languages (xml/soap) because they employ standards. Developers may help make this API a reality by utilising this open source and deployable API instead of reinventing communication in Java from the ground up. A Java graphic library will be used to communicate the

interface's deployment. Swing is a Java-based graphics library that simplifies the creation of user interfaces for various Java applications and platforms. NetBeans' IDE features a "Project Matisse" GUI builder, which makes it easy to design and deploy GUIs. A private cloud is a new concept to me. I'll learn about its inner workings and how to interface with it, as well as the solutions it can bring. The fact that Amazon EC2 and Eucalyptus share the same API version 9 is very exciting to me because I'm working with an open-source solution that mimics the capabilities of a well-used commercial solution like Amazon EC2.

3.4.7 Cloud Computing Adoption

Cloud computing is not just about the technological advancements of data centers, it also involves how IT is supplied and utilized (Creeger, 2009). Before adopting and utilizing cloud computing, businesses need to consider the advantages, disadvantages, and other impacts on their operations and use practices (Khajeh Hosseini et al.,). In businesses, the development of organizational and cultural processes matters just as much as the technology itself when it comes to cloud computing adoption (Fellowes, 2008). It may take 10 to 15 years before the typical organization makes this change to cloud computing, according to some predictions (Sullivan, 2009).

According to the predictions, adoption of cloud computing will not happen immediately and it may take 10 to 15 years before the typical business organization makes the change (Sullivan, 2009). Therefore, we are presently at the beginning of a transition phase during which numerous decisions need to be taken with regard to the adoption of cloud computing in the organization.

3.5 Small & Medium Enterprises (SMEs)

3.5.1 Definition of SMEs

The term "SME" refers to small and medium enterprises. Small and medium enterprises (SMEs) are an essential component of the overall business sector for any country. SMEs are essential to the industrialization and economic development of Bangladesh. It has been defined quite differently throughout time in Bangladesh. The evidence provided in this section is based on the employment cutoff values for various business size groups (National Industrial Policy, 2010).

Size Group	No. of Workers
Micro	10 – 24
Small	25 – 99
Medium	100 – 249
Large	250 or more

SMEs are organizations that employ less than 250 people. Additionally, they must have a balance sheet total of no more than EUR 43 million or an annual turnover of up to EUR 50 million (The EU definition). SME definition

Company category	Employees	**Turnover**	**Balance sheet total**
Medium-sized	< 250	≤ € 50 m	≤ € 43 m
Small	< 50	≤ € 10 m	≤ € 10 m
Micro	< 10	≤ € 2 m	≤ € 2 m

Table 1: Europa, 2022 (Source)

According to the SME Foundation (2015) and National Industry Policy Bangladesh (2010) the definitions of Bangladeshi SMEs of different types are below. In the context of Bangladesh, the growth of SMEs is a dynamic tool for reducing poverty and accelerating domestic development. But unlike so many other nations, Bangladesh has no particular or distinctive definition of SMEs. According to (Hashim & Abdullah, 2000), SMEs are defined to a variety of standards and principles that are utilized for determining the size of the company or business.

SI	Type of Industry		The amount of investment (Replacement cost and value of fixed assets, excluding land and factory buildings)	Number of employed workers
1.	**Cottage Industry**		Below 5 lakh	number of workers not exceed 10
2.	**Micro Industry**		5 lakh to 50 lakh	10 to 24
3.	**Small Industry**	Manufacturing	50 lakh to 10 crore	25 to 99
		Service	5 lakh to 1 crore	10 to 25
4.	**Medium Industry**	Manufacturing	10 crore to 30 crore	100 to 250
		Service	1 crore to 15 crore	50 to 100
5.	**Large Industry**	Manufacturing	More than 30 crore	More than 250
		Service	More than 15 crore	More than 100

Table 2: Definitions of Bangladeshi SMEs (Adapted from: National Industry Policy (2010)

3.5.2 SMEs and Cloud Computing in Bangladesh

Small and medium-sized businesses (SMEs) represent the foundation of the national economies of all nations, and Bangladesh is no exception. Bangladesh is one of the most ambitious developing countries in the world in which Small and medium-sized businesses (SMEs) are key to the economic growth and success of Bangladesh (SME Foundation, 2015). However, the country is not benefiting as much as expected from the SME sector due to the lack of technology, and several SMEs are failing in the commercial market. Many Small and Medium-Sized Enterprises (SMEs) are moving to the virtual clouds, because cloud is becoming increasingly popular among SMEs and provide a platform that is flexible and cost-effective benefits (Shimba, 2010; Widyastuti and Irwansyah, 2018). The advantages of cloud computing would encourage SMEs to quickly adopt it. However, poor of infrastructure makes it difficult to meet the businessmen's expectations and discourages them from utilizing new technology (Widyastuti & Irwansyah, 2018).

3.6 Cloud Computing Challenges and its Security Issues

3.6.1 Cloud Computing Challenges

Despite the obvious benefits of using cloud services, cloud computing presents unique difficulties for IT workers:

- **Cloud security** -- Frequently regarded as cloud computing's biggest obstacle. Organizations that depend on the cloud computing faces some security issues such as data breaches, API and interface hacking, password stolen, and authentication

problems. Furthermore, there is a lack of transparency regarding the handling of sensitive data by the cloud service providers where it is stored and how it is utilized.

- **Cost management** -- Pay-as-you-go cloud subscription plans and variable workloads can make it challenging to define and forecast ultimate expenses.
- **Lack of resources and expertise** -- Organizations are finding it difficult to keep up with the rising demand for tools and workers with the necessary skill sets and expertise due to the fast advancement of cloud-supporting technology.
- **IT governance --** The lack of control over the provisioning, de-provisioning, and management of infrastructure activities in the cloud can make IT governance challenging. It may be difficult to manage risks, IT compliance, and data quality effectively as a result.
- **Compliance with industry laws --** It can be challenging to maintain compliance with industry requirements through a third party when moving data from on-premises local storage to cloud storage.
- **Management of multiple clouds --** Multi-cloud installations may fragment attempts to solve broader cloud computing issues.
- **Performance --** largely out of the hands of the company using a cloud service provider. If firms do not have backup plans in place, outages may reduce productivity and interfere with company operations.
- **Building a private cloud --** IT departments may find this to be a difficult challenge.
- **Cloud migration --** Applications and other data are frequently complicated to move to a cloud infrastructure, which leads to problems. The duration and cost of migration efforts usually exceed expectations.
- **Vendor lock-in --** Changing cloud providers can frequently result in serious problems. Technical compatibility issues, legal restrictions, and high expenses are all examples of this.

3.6.2 Issues with Cloud Computing

New technologies come with risks and unexpected threats. Something that cloud computing does not differ from. Business organizations that rely heavily on IT will essentially outsource their processes. Some of them may be related to their primary business. With inadequate security, these firms will be exposed to significant risk, as their

important data may be exposed to the outside world. Other challenges involve legal and privacy concerns (Khajeh-Hosseini et al., 2010).

Security Issues

There are several security issues with cloud computing (Bikram, 2009], which gives researchers or investigators a vast scope to explore. A technology always has two faces and cloud computing is no exception. one that promotes prosperity, while other addresses problems and rises to its challenges. Similar to traditional computing, cloud computing has a variety of security concerns (Lakshmisri, 2019). The purpose of this section of the study is to analyze the various challenges that cloud computing faces.

3.7 Security-related issues in Cloud Computing

The issue of security is a very important point to consider while analyzing the drawbacks of Cloud computing. As a result, any organization interested in implementing this technology must ensure that they are willing to hand over sensitive data to a third-party provider of cloud services. Making such information available could put the organization at risk. As a result, the choice of cloud service providers must be of the highest caliber.

Security is especially important for the successful operation/use of a cloud computing architecture because the associated problems are huge and frequently vary over time (Khorshed et al., 2012). In fact, cloud-based services are vulnerable to the majority of computer network threats (Ahmed & Hossain, 2014). In this sense, the user's personal data security (King & Raja, 2012) and data location (Teneyuca, 2011) are major concerns. The key security challenges in cloud computing are mostly around data integrity and data confidentiality. In addition to the technical aspects of security, the provider's strategic policies are critical to ensuring the security of the users' data (Joint & Baker, 2011).

However, there are still numerous concerns with cloud computing today, with contemporary researchers or practitioners pointing out that data security and privacy risks have become the top concern for people transferring or migrating to cloud computing.

3.7.1 Security

Recent advancements in the field of could computing have significantly changed the way we compute as well as the concept of computing resources. The resources in a cloud-based

computing infrastructure are typically located on someone else's premise or network and are accessed remotely by cloud users (Ogigau-Neamtiu, 2012; Singh & jangwal, 2012).

Companies are still concerned about security while employing cloud computing. Users are particularly concerned about the vulnerability to attacks that occurs when information and critical IT resources are located outside the firewall. Where is the data more secure, on a local hard disk or on high-security cloud servers? In the cloud, however, data will be distributed over the network via individual computers regardless of where the data repository is ultimately stored. Hackers may infiltrate virtually any server, and figures show that one-third of breaches are caused by stolen or lost laptops and other devices, as well as employees accidentally exposing data on the Internet, with insider stealing representing around 16 percent (Elinor, 2009).

Security has always been important to safe computing practices. As a result, security has always been a concern with cloud computing practices. Cloud computing is mainly classified into four types: private cloud, community cloud, public cloud, and hybrid cloud (Ogigau-Neamtiu, 2012; Singh et al., 2012).

Various security threats connected to the usage of cloud computing services in businesses will be discussed in this section. Confidentiality, integrity, and availability are the most common aspects of security. In addition, three additional factors—compliance, policy, and risk—must be taken into consideration due to the nature of cloud computing (Hobson, 2009).

The cloud's exact position can be anywhere (Velte, 2009). As a user, we cannot always predict where our information will be at any given moment. This implies that they could be offering their services in nations with different legal restrictions. This can lead to different security requirements for a certain nation and endanger the cloud-based firm.

There are different organizations in the cloud; they work all along in that same cloud. It is not hard to imagine that when fifty different organizations access the cloud it could happen that data gets mixed up.

This brings several security issues. For an example not knowing where your data physically is stored, what would happen in the case of a natural disaster? The provider should provide a back-up for when such disasters happen. This is something that needs to be discussed with a provider.

What cannot be checked with cloud computing is to see who has access from the provider side. The provider determines which employees have access, however they do not manage access control. Anyone with the login data could access the cloud of an organization and access all their data.

3.7.2 Privacy Issues

Some security difficulties are partially accompanied by privacy concerns. This makes sense because they are tied to one another. Because the way security is handled affects privacy in some way, it is not useful to fully redefine these problems. In the cloud, personal data and even crucial data of enterprises circulate. Because it is out of the viewing range of the organization it is risky as they cannot see who is using the cloud. It is risky since it is out of sight of the company, as they cannot see who is utilizing the cloud. They must convince the supplier that access is managed and only accessible to authorized individuals.

Unlike the traditional computing model, cloud computing makes use of virtual computing technology, which allows users' personal data to be dispersed across various virtual data centers rather than remaining in the same hard drive physical location, even across national borders. At this time, data privacy protection will be contested by different legal systems. Users, on the other side, may reveal sensitive information when using cloud computing services. Attackers can analyze the important task based on the computing task given by the users (Jianchun & Weiping, 2010).

Another aspect to consider is how the cloud is managed. It is essential to remember that not everyone in the cloud has the same access permissions and can see all information. Top management need different information than a regular employee. Aside from that, they require other information provision; it would be dangerous for any employee to have access to the organization's important information, as this might easily be leaked to the outside world.

3.7.3 Confidentiality

The concept of confidentiality states that sensitive or protected data is only accessible by the authorized persons who have the necessary the rights and privileges granted by the data owner (Albeshri et al., 2012). As there are more parties connected to the cloud model, including other users who are accessing the same cloud, so there is a greater chance of data confidentially being compromised. In addition, the control of data has been given to the

cloud provider, but there is hardware segregation between users in the cloud. As a result, there is a higher possibility of a confidentiality breach as the data is no longer under the control of the data owner and are now available to third parties (Zissisand & Lekkas, 2012).

3.7.4 Load Balancing

Load balancing is the key to success for cloud architectures. It is capable of distributing the working processes evenly between 2 or more computers, so that resources can be used efficiently and therefore increases performance and availability (MacVittie, 2009). A so-called load balancer is automatically able to deal with different amount of work capacity by adapting its distribution decisions according to the moments a request is made. A load balancing solution is often used in internet services, where the idea of load balancing is run by an application (MacVittie, 2009).

3.7.5 Data Breaches

The concept of data breach is occurred when an unauthorized or malicious person gains access to a company network and steals or uses confidential or sensitive information (Ardagna et al., 2015). Cloud service providers, government agencies, and customers are all greatly impacted by data breaches (Srinivasan, 2014). Data breaches may lead to permanent data loss which is the major security concern that is affecting both data and computation integrity in the cloud computing envirnment. If any individual entering a cloud environment with malicious intent might make the entire cloud environment a high value target because data from several individuals and businesses is stored there (Piers, 2011). A breach may arise as a result of an insider attack (Xiaoqi, 2012) or unintentional transmission errors (such breaches have occurred in amazon and Google CCs).

3.7.6 Reliability

Cloud computing continues to provide 24-hour availability. There were a few incidents where cloud computing services went down for a few hours. Expect more cloud computing providers, more services, established standards, and best practices in the present and future. Cloud servers have the same issues as your own local servers. Cloud servers likewise undergo downtimes and slowdowns; the difference is that customers are more reliant on cloud service providers (CSPs) in the cloud computing taxonomy. If you choose a specific provider, you may be locked in, posing a possible company security risk.

It describes the history of the cloud, its evolution, definition, service models, deployment patterns, and some current challenges. There is no doubt that cloud computing will be a future development trend. Cloud computing provides us with nearly endless computing capabilities, strong scalability, on-demand service, and so on, as well as security, reliability, and privacy difficulties, legal issues, and so on. We acknowledge the cloud computing era, and it is necessary to solve and prevent existing challenges and implications for maximal necessity.

3.7.7 Data integrity

This relates to maintaining and assuring the correctness, consistency, and validity of data across its entire lifecycle (Wang, 2012). Data integrity requires that data be safeguarded against all forms of human errors, data transmission problems, viruses, disk breakdowns, and natural disasters. The primary obligation of a cloud vendor is to ensure data integrity (Saranya & Abburu, 2012).

In this study, the authors listed their findings, including the problem that was discussed and the approach taken to solve it. However, they indicate that cloud computing faces several security issues from the user's viewpoint. According to them, this is the sole drawback of clod computing that is significant enough to discuss. They also mention the following issues as being crucial to addressed:

Users authentication: To prevent malicious users from gaining access to the powerful computing systems in CC, user authentication procedures must be improved (CSA).

Data leakage or loss: If an unauthorized individual accesses a shared resource pool and deletes or changes data, there is a danger that data can be lost. Data loss or leakage: Data might be at danger if someone who shouldn't have access to a shared resource pool deletes or edits data. If there is no backup of the data, the risk may grow further (CSA).

Customers trust: Strong authentication procedures must be used to make sure that the customers' data is protected from unwanted access (CSA).

Malicious users handling: Malicious users include attackers who utilize cloud services with the intention of doing harm or an insider who has earned the trust of the firm but tries to access private data that is kept in the cloud (CSA).

Hijacking of sessions: These types of attacks can occur when a trustworthy user is vulnerable to phishing schemes or poorly secured application interfaces that may be used

by attackers. Attackers that carry out these types of attacks to take control of authorize users' sessions (CSA).

Using cloud computing and related services incorrectly: Cloud computing service companies allow users to trial their services for free for a short time. Some users take advantage of this trial time to improperly utilize the resources they have received from the cloud service provider (CSA).

3.8 Other Security Threats

Virtualization

The virtualization software might potentially be exploited. Its primary function is to change any relationship between the operating system and the hardware. Therefore, the cloud service providers need to manage and protect the extra layer appropriately. Another risk associated with virtualization is that causing the whole system to be vulnerable. Therefore, we must upgrade our plan in order to use virtualization. Therefore, wo must upgrade your plan in order to use virtualization.

Storage

A security concern with cloud computing is storing data on a public cloud. Because of centralized storage facilities, hackers can access your data. Therefore, when sensitive data is involved, it is advisable to use a private cloud to avoid these types of threat.

Data Ownership

Data ownership is another crucial that has emerged from cloud computing. When a user keeps their data on a cloud service, the privacy of the data could be lost along with the ownership. Additionally, the users of cloud are also at risk of losing control over their data and their right to disclose it by giving ownership of their data to cloud service providers (Attrapadung et al., 2012). The original data owner has the right of disclosure in addition to its legal ownership (Krutz and Vines, 2010), although the owner's rights may still be violated. Some cloud providers are still considered the right of disclosure as data custodians, while others do not.

Data Location

One of the most common compliance problems that business organizations encounter when adopting cloud computing is data location. A company or business organization usually controls its computational environment; which affects where data is kept and what

security measures used to protect their data with an in-house computer system (Buyya et al., 2013). Nevertheless, with cloud computing, an organization's data is redundantly kept in several physical places without providing the company with specific location information (Tang ET AL., 2012). Because of this, it can be difficult to figure out whether sufficient security measures have been implemented s have been implemented to secure the data. Additionally, it is impossible for the customers to know if service providers have complied with legal or regulatory obligations. (Svantesson and Clarke, 2010).

Multitenancy

The biggest risk in cloud computing is having shared access to another user's data. Because there is always the possibility that other users will get access to your sensitive information. Your data may potentially be accessed by hackers due to another user's mistakes.

Data Handling by a Third

Since it is well known that data is handle and maintain by a third party in the cloud; the largest issue is how the third party secures the data and what guarantees are provided. No third party can ensure 100% individual data security. As a result, data security cannot be properly ensured.

Cyber Attack

Cyberattacks are the main security issue with cloud computing. The data is targeted by a variety of attacks, including infrastructure flaws, malware, ransomware, and simple setup errors (Tadapaneni, 2017). There are several difficulties that we can observe; modern malware is quite versatile and concurrently can attacks from several distinct routes. In order to control it, one needs to look a somewhat different perspective when considering cloud security.

Insider Attack: Consider the possibility that there would be no data privacy if the cloud provider where you kept your data allowed people to simply access it.

Lack of Standardization

The standards used by various Cloud providers are not necessarily the same. It indicates that there is no proper standards used in various processes such as access control, authentication, or encryption.

Integrity of Data

There is a possibility that data will be changed or modified by an unauthorized user. Essentially, the cloud service provider must ensure that data cannot be changed by an

unauthorized user (Selviandro, 2015). When data is moved from one cloud to another cloud, the second principle of integrity applies. In order to prevent data from being changed by an unauthorized user at that point, the Cloud Service Provider must take certain precautions.

Transparency Issues

The specific information of how their data will be secured are not provided to a given business when they purchase a cloud service from a provider as a public, private, or hybrid cloud solution. It is challenging for enterprises to determine if the stored and processed data is entirely safe because of this lack of service transparency (Winkler, 2011). Users are not even quite certain if their data is protected.

Insecure APIs

The range of APIs that a certain customer's cloud service provider is employing is not actually known to the client when a cloud is being rented to them.

3.9 Cloud Computing Related Technologies

In this section, a number of cloud computing-related technologies will be discussed.

Web applications

While cloud computing is predicated on offering services, what precisely is a service and how does it work? We've discussed this previously. Most of the time, two programs written in different languages and running on different operating systems cannot communicate, but there are a number of protocols and standards in place that allow data to be exchanged between programs regardless of the language or operating system in which they are written. For example, when we don't know how a program operating on the Internet is implemented, this is quite helpful. OASIS (Organization for the Advancement of Structured Information Standards) and W3C (World Wide Web Consortium) have made this feasible (World Wide Web Consortium). Text is the medium of exchange in this conversation. As a result, it is less effective than methods such as CORBA or RMI (Remotely triggered technique of execution) (Zhu, 2010).

There are a variety of ways to communicate with each other:

XML (Extensible Markup Language)

Based on the use of labels, it is a metalanguage. It's well-structured and enables for communication across various applications or systems. The word "extensible" refers to the ease with which additional labels may be defined.

SOAP (Simple Object Access Protocol)

It's a protocol that specifies how XML messages may be exchanged between two separate processes.

WSDL (Web Services Description Language)

WSDL is the public interface in the world web service industry based on XML. It describes all the services that exist in one location and the way to interact with them.

UDDI (Universal Description, Discovery and Integration)

It's a list of all the web services available on the Internet, but it's no longer widely used. It's an XML document.

WS-Security (Web Service Security)

It's a SOAP extension for web service security.

Cloud Computing Security

Security in the cloud is governed by these rules, which concentrate on the protection of personal data as well as network and computer systems. A user's data must be completely separate from another user's data, and it must be transported safely inside the cloud (Malik, Wani, & Rashid, 2018).

Use of identities

It is essential that the physical infrastructure be entirely secure, and that only authorized individuals have access to data.

Users must constantly have access to their data; this cannot happen at any one time to a single user (Alsaeed & Saleh, 2015).

All cloud-based services must be safe and secure. Encryption is required for any data that may be considered sensitive.

Google Apps

It's a web-based office suite that anybody may access through a web server. Included are the following:

• **Gmail** IMAP and POP3 are the most popular email protocols in use across the globe. There are now 193.3 million active users of the stable version, which was published in 2007 (Khmelevsky & Voytenko, 2010).

• **Google Calendar** compatible with other calendars. You may use Google Docs to create and modify documents together with other users in real time and to share them with others.

• **Google Groups**, discussion groups may take use of this service

• **Google Talk**, a service about instant messaging and video chat.

• **Google Sites**, a service that makes it simple to create and modify web pages and intranets.

Amazon S3 (Simple Storage System)

It's an online storage solution provided by a web service. Standard interfaces like REST or SOAP are used to provide compatibility across a wide range of platforms. Bit Torrent can also be used to download data, but the default protocol is HTTP. Fecundity and security against invasions are ensured by the system, and the integrity of the data is checked routinely. Usage is tracked in Gigabytes/month, therefore the trend is ever-changing and dependent on the amount of data a certain customer stores (Han, 2015).

Microsoft Online Services

A variant of Microsoft's cloud-based software and services includes both cloud-based services and on-premises apps that run on a client computer. An advantage of this is that

the user can operate a programme online while still retaining their data on their own machine. Communications are the focus of the services offered. They have two options:

- Messages sent with Microsoft Exchange Online are delivered via the Exchange Server messaging platform.
- SharePoint Online: It's a place on the internet where people can work together. Working in a group is easier when everyone has access to the same resources.
- A videoconference and instant messaging (IM) service for office workers is provided by Office Communications Online.
- A network security solution from Microsoft, Forefront protects servers, desktops, and mobile devices. Including anti-virus, anti-malware, anti-spam, and other security measures.

4. Practical Part

The main goal of this section is to discuss the practical aspect of this research. This practical part includes key information on our chosen data, data collection, analyzed of that data as well as the strategies for ensuring the findings is valid.

4.1 Introduction

For the empirical investigation, two different types of sources are used. Firstly, service providers were asked open-ended questions to encourage them to express their own views on the requirements for using the cloud.

However, the survey is given to the main attention for the implementation process itself. This is because we assumed they would not bring up any relevant issue as we were unable to ask the service providers for this information. As an alternative, a number of enterprises that were known to have recently implemented cloud computing services and other users of cloud were contacted. Some people were open to sharing their expertise and some people were open to sharing their knowledge.

The limitation of the practical part is the lack of enough sources. Though surveys is indicating that a large number of businesses are considering employing cloud computing services, it is challenging to compile a list of those participants and contact specific individuals who were involved in these projects.

4.2 Data Analysis

This part of this study focused on examining cloud computing benefits, challenges, and risks with regard to ICT in the context of SMEs in Bangladesh. The three cloud service providers were selected for this research which provided these types of cloud computing services. These service models, including SaaS, PaaS, and IaaS, are illustrated in the theoretical framework. They were given the assurance of their anonymity because security is a sensitive issue for the chosen organizations in order to encourage interviewees to be more open with their answers. The first two companies are telecommunications companies with a wide range of products and services and most recently introduced cloud services SaaS, PaaS and IaaS. In the following, the researcher will refer to them as Cloud Service Provider CSP1 and CSP2 respectively. The third company, cloud & technology consulting provider, is relatively new into the ICT industry which provides SaaS, PaaS, and IaaS and it will be denoted to CSP3.

4.2.1 Cloud Computing Service Provider in Bangladesh

4.2.2 About CSP1

CSP1 is a leading company in terms of offering a variety of communications services, such as phone calls, messages, pictures, internet access and video calls. Customers from public and private sectors use the products and services offered by the organization. Customers of CSP1 have access to a variety of devices, including smartphones, tabs, laptops, and desktop computers etc. Customers of this company are both private and corporate client including the government people, multinational corporations, small and medium-sized enterprises, and individual clients. These clients are employed in a variety of business sectors, including finance, manufacturing, transportation, hospitality, ICT, education, healthcare, service sector, and so on.

4.2.3 About CSP2

CSP2 is one of the largest companies in ICT sector and offers a comprehensive variety of telecommunications products and services. Their key business operations are carried out different services regarding IT. To be more explicit, they presently include cloud computing into their projects. They use it for their clients when implementing solutions. They believe that cloud computing should adhere to both their own and their customers' security requirements. Also, they must perceive benefits for both themselves and their clients in adopting it. They employ cloud computing and mostly they use Software as a Service & Platform as a Service. CSP2 has noted the high cost of IT software and hardware as a challenge for small and medium sized enterprises (SMEs). As a result, SMEs, like their larger corporate counterparts would benefit from higher efficiency and the optimization of company processes, but they are facing challenges by limited resources and IT experience. SMEs will be able to reduce expenses with the help of CSP2 cloud service which will offer affordable and simple solutions for their needs by increasing production and efficiency. Businesses organization would benefit a lot from CSP2 Cloud services including the flexibility that comes with allowing employees to access files and data from any location, even whether they're working remotely or after regular business hours.

4.2.4 About CSP3

CSP3 is a technological business company offers cloud services and cloud-based applications. It provides consultation and expertise for internet technologies such as

implementing of domain name registries and registrar infrastructure services. This company, furthermore, offers a powerful scalable cloud platform that enables customers to detach apps from physical resources. It is eliminating the need to equip a device with every application, and minimizing conventional end user licensing agreements (EULAs), ongoing maintenance of software, operation updates, and others support. Users of the CSP3 cloud platform have access to a variety of essential business applications as well as the ability to safely store and manage multimedia data. The key part of the company is unique value proposition having storage and software reside on CSP3 servers rather than on the premises of the user organization, and using a pay-per-use approach to eliminate the expenses of purchasing, installation, deployment, and maintenance costs. With a flexible platform that scales services effectively and reduces initial capital expenditure, CSP3 is well positioned to benefit from the paradigm change.

4.2.5 SMEs in Bangladesh

This study's primary goal is to describe the security advantages and difficulties of migrating business data to the cloud in the context of SMEs in Bangladesh. It also provides recommendations on the best methods for transferring business data to the cloud. To achieve these goals, a mixed method research strategy was used. The purpose of this approach is to provide a understanding of the research issue as well as a generalization of Bangladesh's service providers' and users' perspectives on the trend in cloud adoption and security threats. The researcher used a qualitative approach first for exploratory purposes before switching to a quantitative approach to provide a more detailed and comprehensive examination of the research problem. Qualitative data gave the researcher in-depth knowledge of cloud service providers and cloud services with regard to information security, while quantitative data presented a wide generalized trend about SMEs and the use of cloud services.

4.3 Data from Interviews Presented

This study aims to emphasize the benefits, security issues, and threats from the perspectives of cloud service providers and customers of migrating data to the cloud. Interviews were conducted with IT managers, Information security officer, Security analysts and cloud service users. The following aspects were covered during the interview:

- Benefits of cloud computing

- Security challenges of cloud computing
- Data ownership & segregation
- Security concerns of cloud service providers
- Security concerns of cloud users

4.3.1 Benefits of Cloud Computing

The main goal of this study was to examine the potential benefits that cloud computing offers to SMEs and identify the security issues, risks, and challenges that come with it. The theoretical framework has examined the key elements of the cloud computing model including broad network access, rapid elasticity, measured service, on-demand self- service that provide a huge range of options for the customers. The researcher was interested in discovering how these factors can infulence organizations' cloud adoption decisions for SMEs, because the growth of cloud service adoption for many organizations over the last few years. It became obvious in the course of the interview that Bangladeshi cloud service providers were aware of the demands of SMEs in the local market and they believed that SMEs can be benefited a lot by implementing cloud computing services. The three service providers (CSP1, CSP2, and CSP3) agreed that SMEs would benefit by adopting cloud computing in a variety of ways.

One of the benefits that is mostly highlighted is cost savings. Users can go on a pay-per-use basis; SMEs can take this advantage over their competitor as they are struggling to maintain their IT infrastructure and they are becoming more and more dependent on IT services nowadays. Another challenge for SMEs development and growth is lack of financing options. Thus, SMEs will benefit greatly from economic perspective as they do not have to pay the upfront cost of purchasing IT infrastructure.

IT officer of CSP2 highlighted these SMEs' operating costs are crucial for their businesses expansion and every opportunity must be capitalize to reduce the costs and improve the quality of the services they offered. By using cloud computing, organizations may save up-front infrastructure expenditures and concentrate on their core competencies.

The CSP3 security analyst further stated that when costs are managed effectively, positive outcomes spread throughout the business. As a result, this can help in achieving economies of scale, which positively affects products and services. Because, pay-per-use, cloud

computing allows businesses or companies taking advantages over their competitors, regardless of their size or financial status.

Improved accessibility is a further advantage mentioned by the service providers. Since cloud services are delivered through the internet, customers can access them from any location as long as they have internet connectivity.

Because of their greater mobility, employees now have access to information from anywhere. "Clients get benefit from increased availability and independence of specialized hardware, software, and maintenance to cloud computing" said CSP1 IT manger. The redundancy provided by cloud service providers is far better than what individual SME's can provide. As a result, in terms of the accessibility of hardware and software, data is significantly secure in the cloud.

Scalability is another key benefit of any cloud computing services. If more resources are needed, they can be used because there are endless computing resources accessible. It's not an issue if, for instance, a company determines that it requires additional resources to meet their demands. The finest part of this is that resources that might not be needed do not have to be purchased in advance; instead, they are paid for based on how often they are used. When a resource is used more frequently, it is paid for at that time; if it is not used frequently or less, it is no longer need to pay.

4.3.2 Security Issues

The following issues were intended to cover through interviews in regard to the theoretical framework and the literature review on cloud computing security. 1) Cloud-based information security concerns; 2) Data ownership & segregation; 3) Responsibilities for Cloud Service Provider Security; and 4) Responsibilities for Cloud Users Security. The author has enquired about expert opinions on the study's topic in the interview sections.

A *major drawback of cloud for CSP1 IT manager states that is the fact that "no official cloud-security industry standard has been acknowledged," and that typically an SLA must be agreed without the possibility of changing individual aspects. "Privacy, risks, and regulatory compliance" are introduced as a result. CSP2 IT officer stated that "cloud security is much more concerned with virtualization and network security". In our perspective, private cloud is more secured. Then there is no concerned if you use private clouds.*

There is a considerable risk of losing sensitive data due to the lack of data backup and data redundancy in the conventional IT environment. If the network goes down, there is possibility of hardware failure that may lead to data loss somehow. In contrast, several servers located in various locations are used to deliver cloud services. Users can continue working without being aware of any downtime for any unusual incident occured. If a server where client data is kept can go offline for any reason. However, "there are several data centers can provide cloud services. If any data center experiences technical issues, cloud services could be still provided services without the user knowing or any changes to their service. As a result, users of the cloud get assurances that user data will not be lost and even downtime will not be detected by cloud users.

CSP3 security analyst claim, "Data in the cloud is typically in a shared environment stored by different customer regarding data segregation. Although effective, encryption is not an ideal solution. He primarily focuses on the necessity of data classification to enhance data handling decision-making." Therefore, we made a similar statement that some data would never be stored in a (public) cloud, no matter how much assurance we can obtain from the service providers.

There is a widespread perception that the service provider retains control over who has access to data while data is stored in the cloud. Service providers believed that once the proper security measures are put in place by users, they had the technical expertise to maintain it secure to prevent any catastrophic data loss and unwanted access.

"...as long as the proper security measures put into practice, data will be protected from data breach and unauthorized access." IT Manager CSP1

The majority of SMEs managers who were interviewed admitted that they lacked internal IT personnel. However, cloud providers have the technical expertise for implementing security measures that can protect cloud services. They have staff members that are specifically assigned to do security-related duties including software upgrades and backups. As a result, users of these services will be benefited who choose to acquire this software.

"We have more technical expertise compared to what in-house IT might offer. This will include security updates, offering cloud-based software and up-to-date packages to address any vulnerabilities; this offers users a security advantage over other package-

based products that demand a license before an upgrade can be completed. Security analyst SPC3,"

4.3.3 Security Challenges

Despite the advantages highlighted above, there are still certain drawbacks with cloud computing like other technology. According to the theoretical framework, users and service providers share responsibilities for maintaining data security in the cloud. The lack of direct control over system, application, hence data security is the key problem. It indicated one of the main issues businesses face while migrating to the cloud is security. As large amount of data are being transferred to the cloud by many companies, so cloud computing has become a prime target for malicious attackers over the time.

Secure data transfer

Users of the cloud have mostly accessed services over the internet. The important issue is building trust in remote execution when a user application runs on a remote host a data center; customers must make sure that his application is performed properly in regrd to maintaining integrity and confidentiality. Since the internet is an open resource that is accessible to everyone:

It is advised for cloud customers to make sure that their data is constantly traveling via a secure route. This might be accomplished by employing industry standard protocols, such as Internet Protocol Security (IPsec), which were created particularly for securing Internet traffic, to encrypt data and authenticate authorized users.

Secure software interfaces

Application Program Interfaces (APIs) are mostly utilized to communicate with cloud services on the network of the service provider. Since data is transferred through the internet which is a public domain, this might be attacked if the proper security measures are not implemented.

Users are advised to be familiar with the software interfaces, or APIs, that are used to communicate with cloud services by the Cloud Security Alliance (CSA, 2010).

Secure stored data

Data should be secured in the cloud while at rest transferring. As the cloud is a shared resource, both internal and external risks could occur. *Cloud service providers take precautions to secure their own operations and protect the customers from the risk that*

may occur. Users are encouraged to have their own encryption method to protect their data since the cloud environments are shared in order to avoid unwanted access. Customers are encouraged to have their own encryption technique for their data to avoid unauthorized access as the cloud environments are shared medium.

User access control

The traditional approach of application-centric access control is ineffective in the cloud environment due to its shared nature. It is essential for users to find out who has access to their data and where it is maintained. Users can select their own access control models with user-centric restrictions on access to protect their privacy.

4.4 Data from Survey Presented

The report begins by examining the current cloud adoption landscape and the factors that influence organizations' decisions to adopt cloud computing. We analyze survey responses from 100 respondents to determine the percentage of organizations that have embraced cloud services and explore the perceived benefits of cloud adoption. Utilizing data visualization techniques such as pie charts and bar charts, we highlight the importance organizations place on cost-saving strategies, business continuity planning, scalability, and remote access capabilities.

Next, we turn our attention to the challenges faced by organizations during the implementation and management of cloud services. By analyzing responses related to data privacy, security, regulatory compliance, and vendor lock-in, we gain valuable insights into the obstacles organizations encounter during their cloud adoption journey. These findings underscore the need for robust data mobility solutions, seamless integration with existing systems, and comprehensive security measures to ensure successful cloud implementation.

4.4.1 Cloud Computing Adoption and factors influencing it

4.4.1.1 Current cloud adoption percentage

Based on the responses from 100 respondents, the Figure 4 illustrates the current technology adoption trends. The survey results indicate that most organizations have adopted cloud computing, with 89 respondents (89%) utilizing cloud services within their company. On the other hand, 11 respondents (11%) reported not using cloud computing.

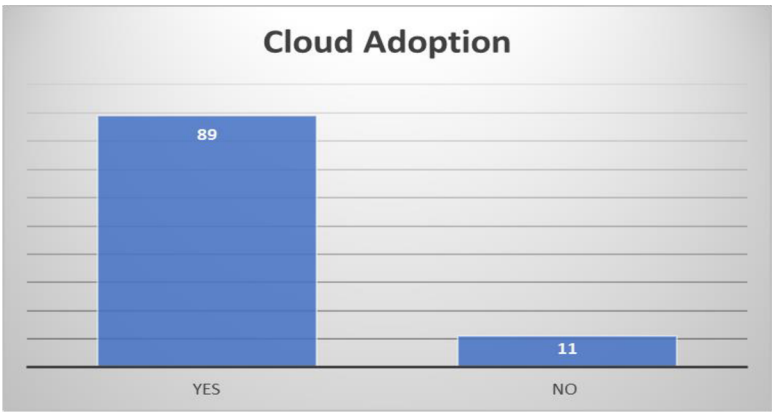

Figure 4: Cloud Adoption

4.4.1.2 Perceived critical benefits of cloud adoption by organizations

The pie chart in figure 5 illustrates the critical benefits perceived by organizations during the adoption of cloud computing. It shows that 35% of organizations prioritize cost-saving pay-as-you-go pricing strategies. Simplified business continuity planning and disaster recovery are crucial to 22% of organizations. Improved IT infrastructure scalability and flexibility are valued by 27% of organizations. Lastly, 16% of organizations emphasize the importance of improved remote access and collaboration capabilities. This analysis highlights the varying degrees of importance of these specific benefits, providing valuable insights into organizations' priorities during the cloud adoption process.

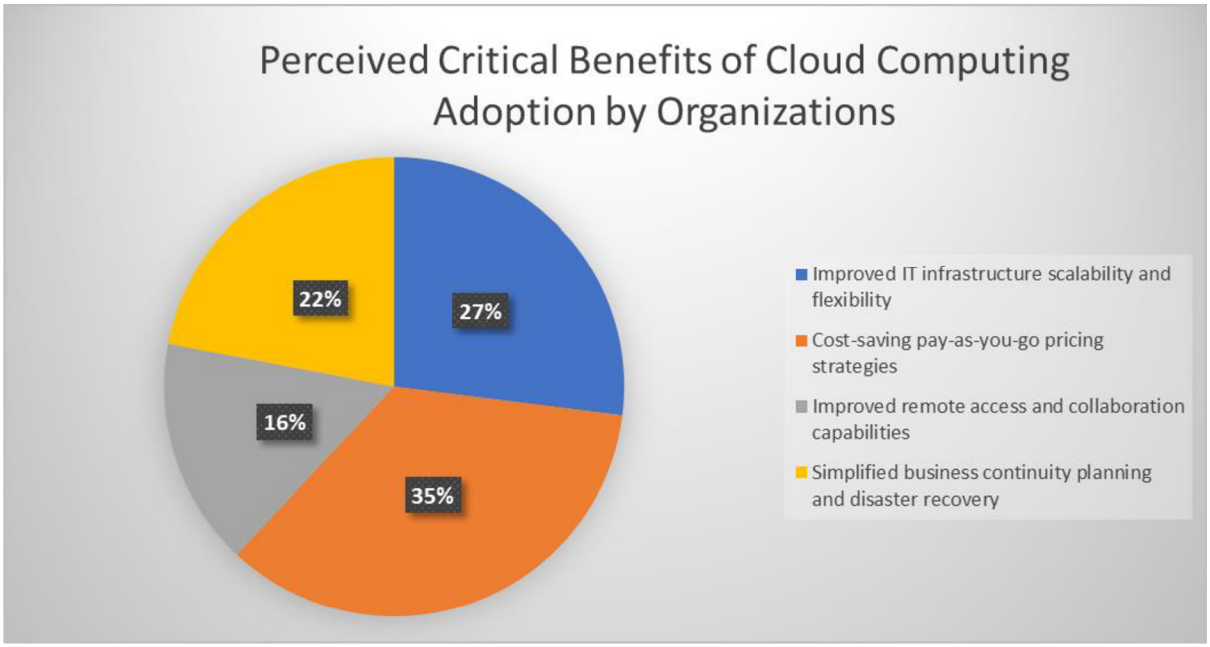

Figure 5: Perceived critical benefits of cloud computing by organizations

4.4.1.3 Challenges faced by organizations in cloud service implementation and management

The bar chart in figure 6 illustrates the challenges faced by organizations when setting up and managing cloud services. The responses reveal several critical areas of concern, including data privacy and security, integration with existing systems, regulatory compliance, and data mobility/vendor lock-in. Notably, data mobility and vendor lock-in emerge as the most significant challenge, identified by 30 respondents, accounting for 30% of the total respondents. Integration with existing systems closely follows, with 29 respondents representing 29% of the total. Data privacy, security, and regulatory compliance also feature prominently in the responses, with 26 respondents (26%) and 15 respondents (15%) respectively highlighting these concerns. These findings provide valuable insights into the obstacles organizations face during cloud adoption and underscore the importance of addressing these challenges to ensure the successful implementation and management of cloud services.

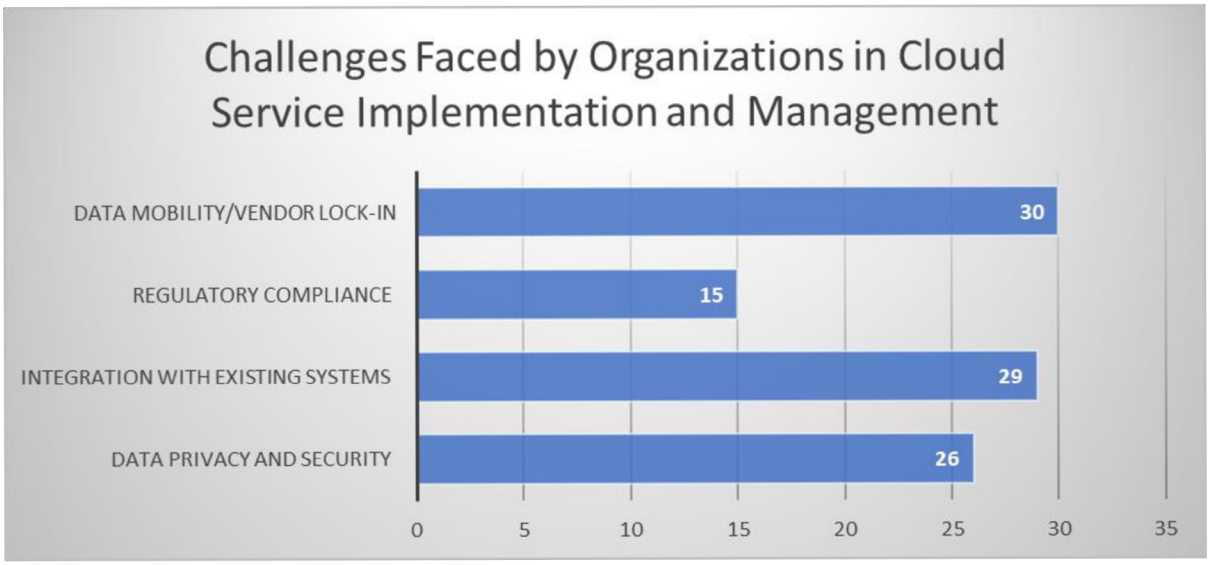

Figure 6: Challenges faced by organization in cloud service implementation & management

4.4.1.4 Importance of security in cloud adoption decision-making

The bar chart in figure 7 visualizes the responses to the question regarding the importance of security in the decision to use cloud computing. The majority of respondents perceived security as either extremely important (40 respondents) or important (30 respondents). A smaller portion considered security somewhat important (20 respondents), while a minority deemed it not important (10 respondents). The average score provides an overall perspective, with the highest average score of 25 indicating a significant emphasis on security. These findings highlight the significance placed on security considerations in organizations' decision-making processes when adopting cloud computing technologies.

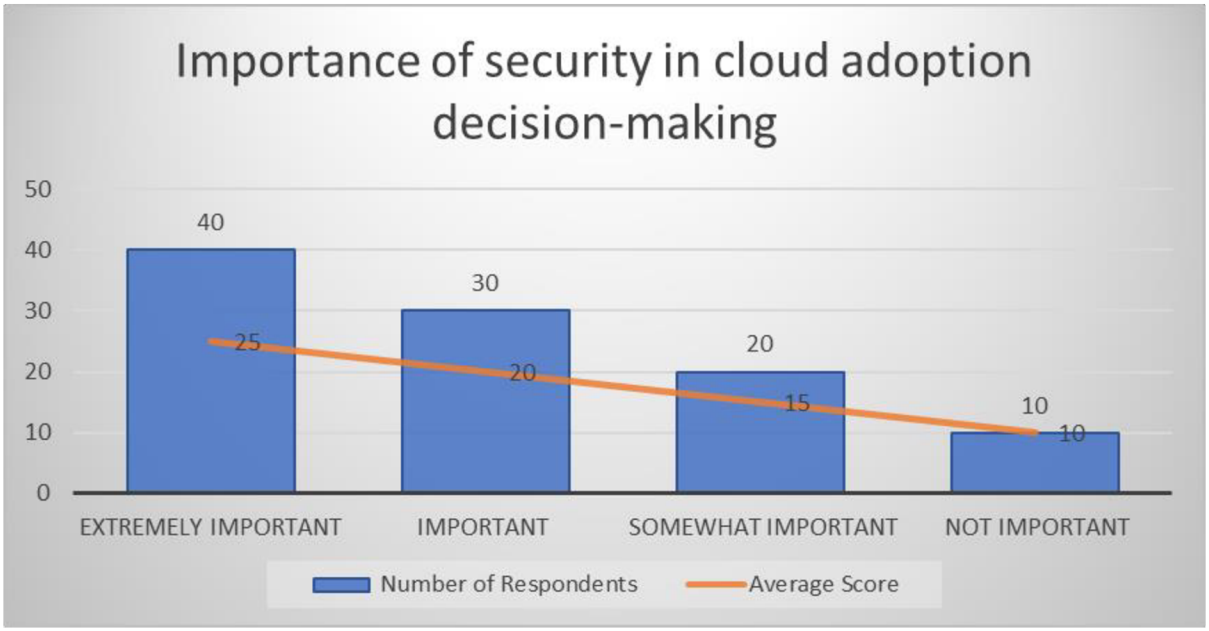

Figure 7: Importance of security in cloud adoption decision-making

4.4.1.5 Relationship between knowledge of cloud computing and cloud adoption

The regression analysis conducted on the dataset revealed some interesting insights regarding the relationship between cloud adoption and knowledge of cloud computing. The analysis yielded a multiple R-value of 0.63620901, indicating a moderate positive correlation between the variables. This suggests that as individuals' knowledge of cloud computing increases, their likelihood of adopting cloud technologies also tends to increase. The coefficient of determination (R^2) was found to be 0.404761905, indicating that approximately 40.48% of the variability in cloud adoption can be explained by knowledge

of cloud computing. This suggests that knowledge of cloud computing plays a significant role in determining the level of cloud adoption among the respondents.

Further examination of the coefficients reveals that the intercept term, representing the expected cloud adoption value when knowledge of cloud computing is zero, is 0.46875. This implies that even without any knowledge of cloud computing, there is still a baseline level of cloud adoption. The coefficient for the variable "Knowledge of Cloud Computing" is 0.53125, indicating that, on average, for every one-unit increase in knowledge of cloud computing, cloud adoption is expected to increase by 0.53125 units. This highlights the positive impact of knowledge in driving cloud adoption.

Multiple R	0.636209
R Square	0.404762
Adjusted R Square	0.397131
Standard Error	0.31963
Observations	80

Table 3: Regression Analysis 1

	Coefficients	*Standard Error*	*t Stat*	*P-value*	*Lower 95%*	*Upper 95%*	*Lower 95.0%*	*Upper 95.0%*
Intercept	0.46875	0.056503	8.295995	2.51E-12	0.356261	0.581239	0.356261	0.581239
Knowledge of cloud computing	0.53125	0.072945	7.282857	2.27E-10	0.386027	0.676473	0.386027	0.676473

Table 4: T-Test Result (Relationship between knowledge of cloud computing and cloud adoption)

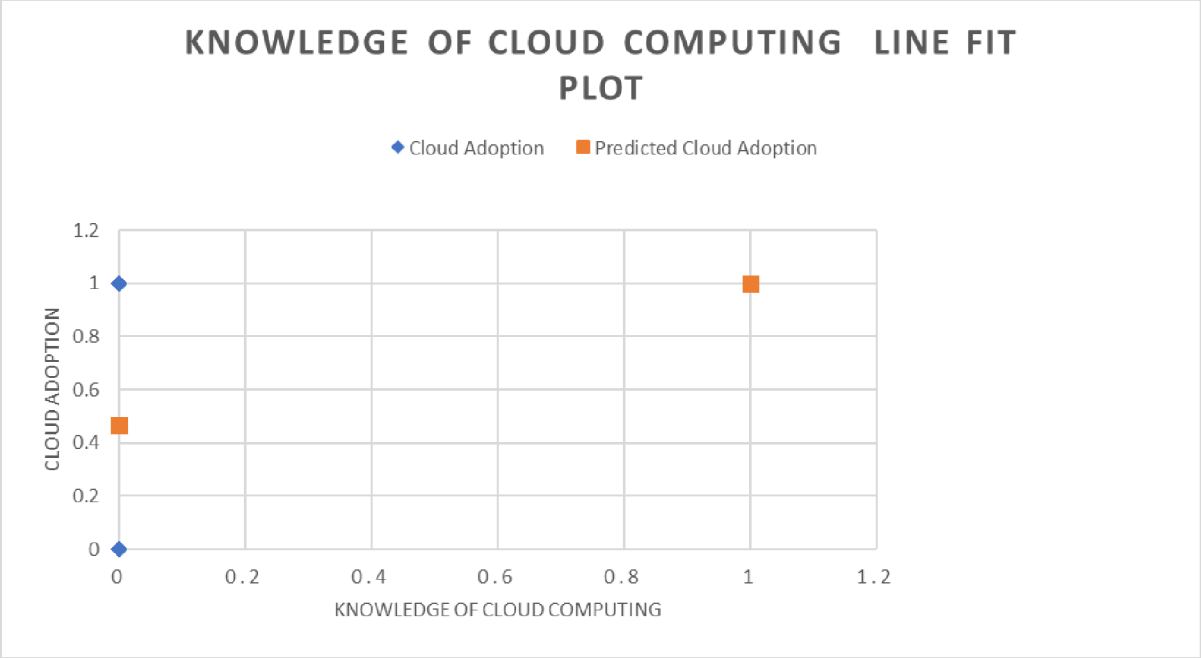

Figure 8: Knowledge of Cloud Computing Line FIT Plot

4.4.1.6 Relationship between security importance and cloud adoption

Another regression analysis was done to see if respondents with higher importance to security had any relationship with the cloud adoption. The regression analysis results indicate that the model is statistically significant (F = 7.509917446, p = 0.007292489), demonstrating that the independent variables included in the model collectively have an impact on the dependent variable. The "Security Importance" variable shows statistical significance (t = 2.740422859, p = 0.007292489), indicating a positive relationship with the dependent variable. A coefficient of 0.275058275 suggests that a one-unit increase in "Security Importance" corresponds to a 0.275058275 unit increase in the dependent variable. The R-Square value of 0.071177361 reveals that the independent variables explain approximately 7.12% of the variance in the dependent variable. It's worth noting that the adjusted R-Square value of 0.061699579 is slightly lower, suggesting that the model's explanatory power is limited. Therefore, additional factors not accounted for in the model may contribute to the remaining variance.

SUMMARY OUTPUT	
Regression Statistics	
Multiple R	0.266791
R Square	0.071177
Adjusted R Square	0.0617
Standard Error	0.415782
Observations	100

Table 5: Regression Analysis 2

	Coefficients	*Standard Error*	*t Stat*	*P-value*	*Lower 95%*	*Upper 95%*	*Lower 95.0%*	*Upper 95.0%*
Intercept	0.545455	0.088645	6.153244	1.66E-08	0.369541	0.721368	0.369541	0.721368
Security Importance	0.275058	0.100371	2.740423	0.007292	0.075876	0.474241	0.075876	0.474241

Table 6: T-Test Result (Relationship between security importance and cloud adoption)

Figure 9: Security Importance Line Fit Plot

4.4.2 Factors Influencing the Selection of Cloud Vendors and their Security Considerations

4.4.2.1 Relationship between type of data stored in cloud and security accreditation expected by the cloud service provider

After creating a contingency table, chi-square test was performed and below are the results:
Chi-Square Statistic: 15.676
Degrees of Freedom: 12
p-value: 0.207

The chi-square test results provide information about the relationship between the variables "Data type stored in cloud" and "Security accreditations expected from CSPs."
In this case, the obtained p-value is 0.207. The p-value represents the probability of observing the data or more extreme data under the assumption that the variables are independent (i.e., there is no association between them).

Since the p-value is more significant than the typical significance level of 0.05, we do not have sufficient evidence to reject the null hypothesis, which states that there is no association between the data types stored in the cloud and the security accreditations expected from CSPs.

Based on the provided data, we do not have enough evidence to conclude that the choice of security accreditations expected from CSPs is significantly related to the cloud data type.

4.4.2.2 Data type stored in the cloud and expected security accreditation

Another analysis was done to see if any particular security accreditations were expected for types of data stored in the cloud and a pivot table was created and which shows valuable insights into the relationship between different data types and their relevant security accreditations. Among the data types, financial data has the highest count with 36 instances, primarily associated with PCI DSS (8 cases) and HIPAA (10 cases). The intellectual property follows with a total count of 23 instances, mainly associated with PCI

DSS (10 cases) and SOC 2 (4 cases). PII (Personally Identifiable Information) has a count of 22 cases and is primarily associated with SOC 2 (9 instances) and PCI DSS (6 cases). Health records, with a count of 19 cases, are closely linked to ISO 27001 (7 instances) and Other (specify) (7 cases). The most prominent security accreditations overall are PCI DSS (24 cases), HIPAA (20 cases), and SOC 2 (20 cases). ISO 27001, with a count of 20 cases, appears relatively evenly distributed across various data types, while Other (specify) has the lowest count with 16 cases, suggesting it is less frequently associated with the listed data types. These insights shed light on the patterns and associations between specific data types and their corresponding security accreditations.

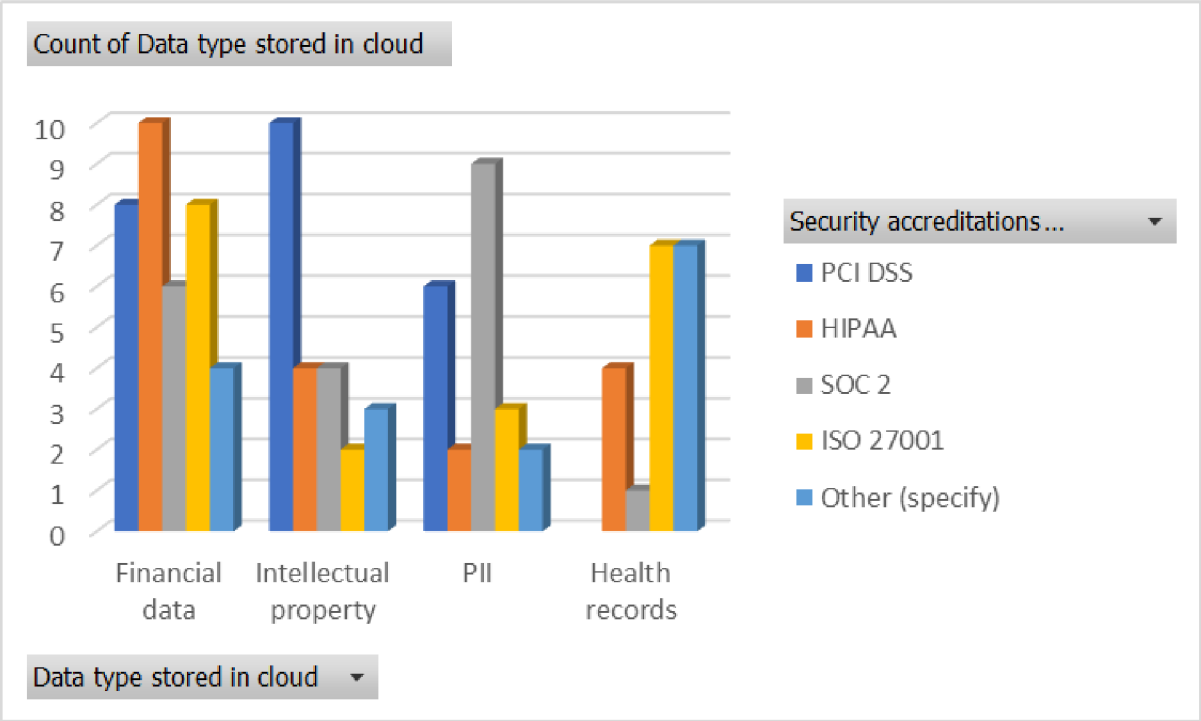

Figure 10: Relationship between different data types and their relevant security accreditations

4.4.2.3 Security factors influencing cloud vendor selection

Respondents were asked which security factors they would consider most important when choosing a particular vendor for cloud services.

When it comes to choosing a vendor, several security factors play a crucial role in decision-making. Among the identified security factors, strict data protection and privacy regulations hold significant importance, with a count of 24 instances. This highlights the

emphasis placed on vendors' ability to comply with rigorous regulations to safeguard sensitive information. Adherence to regulations and certifications is another critical factor, with a count of 27 instances. This indicates that organizations prioritize vendors who possess recognized certifications and demonstrate a commitment to maintaining compliance standards. Disaster recovery and incident response skills are also highly valued, as evidenced by a count of 25 instances. Organizations seek vendors with robust plans and capabilities to mitigate potential risks and efficiently respond to incidents. Finally, the importance of regular audits and open security procedures is evident, with a count of 24 instances. This signifies the emphasis placed on transparency and accountability in vendor security practices. Considering these factors enables organizations to make informed decisions and ensure that their chosen vendors align with their security requirements.

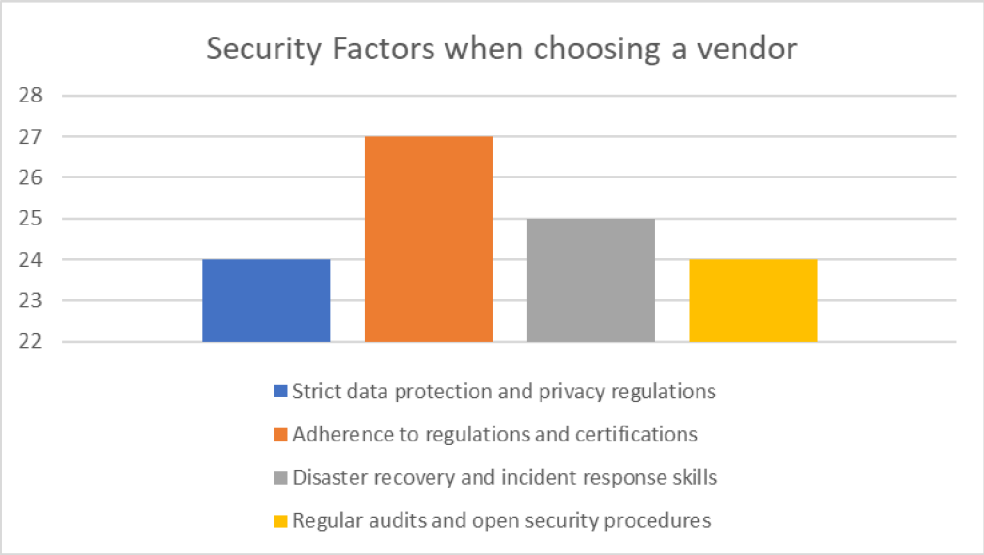

Figure 11: Security factors when choosing vendor

4.4.3 Confidence/Trust in CSPs and Concerns with Cloud Service Providers (CSPs)

4.4.3.1 Concerns of cloud security in CSPs

Respondents were asked some questions to evaluate their trust, perceptions, or concerns about security implemented by the CSPs.

Several observations can be made based on the line chart representing the percentage of respondents with high concerns about different aspects of CSPs. The chart shows that 31%

of respondents have high concerns about cloud-based data privacy, indicating a significant level of worry regarding the security and confidentiality of their data stored in the cloud. Additionally, 34% of respondents express high concerns about the physical security of cloud data centres, highlighting the importance of robust measures to protect the physical infrastructure where their data is housed.

However, the most notable finding from the chart is the high percentage of respondents, at 85%, expressing concerns about insider threats. This indicates that a large majority of the sample population is worried about the potential risks posed by individuals within the CSP organization who may have unauthorized access to sensitive data. This finding emphasizes the need for strong security protocols and measures to mitigate insider threats and maintain trust in CSPs.

These findings emphasize the importance of addressing these concerns to foster trust and ensure the security of data within the cloud environment.

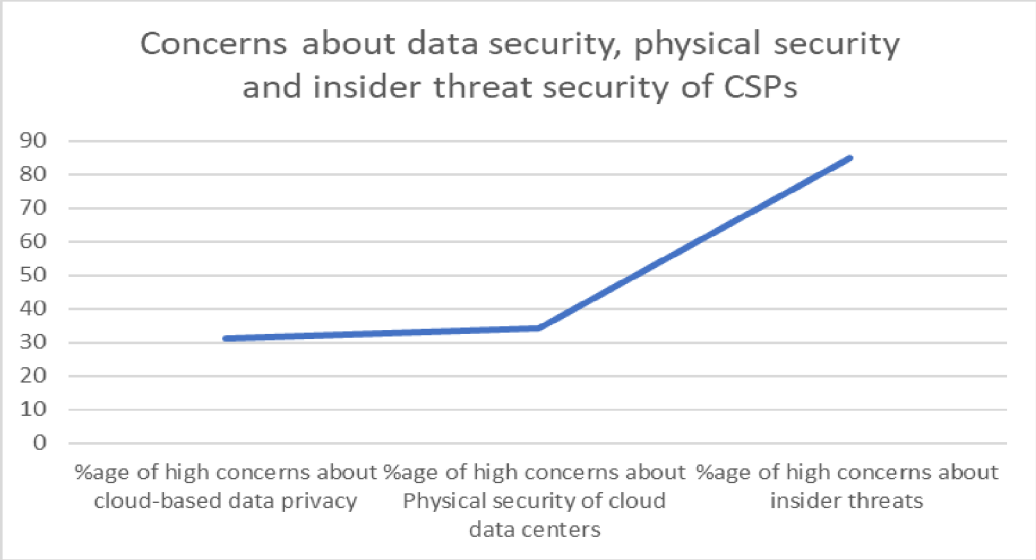

Figure 12: Concerns regarding security implemented by the CSPs

4.4.3.2 Confidence in CSPs to secure cloud and security measures offered/implemented and overall ability to handle different aspects of cloud security

Based on the provided data, a notable pattern emerges when examining the percentage of respondents with high confidence in different aspects of CSPs. Among the respondents, 41% expressed high confidence in the security measures implemented by CSPs. This suggests that a significant portion of the sample population believes that CSPs have

effective security measures in place to safeguard their data and protect against potential threats.

Furthermore, a substantial majority of 73% of respondents exhibit high confidence in the CSPs' ability to protect their data. This indicates a strong level of trust in the measures implemented by CSPs to ensure the security and integrity of the data entrusted to them. However, the data point for high confidence in CSPs' ability to recover from a disaster is relatively lower at 24%. This suggests that a significant number of respondents may have reservations regarding the CSPs' preparedness and effectiveness in recovering data in the event of a disaster or system failure.

Interestingly, 61% of respondents expressed high confidence in the CSPs being honest about handling security matters. This demonstrates that a majority of the sample population believes that CSPs are transparent and trustworthy in their approach to handling security concerns and communicating them to their customers.

In summary, the data reveals a positive trend of high confidence in the security measures and data protection ability of CSPs. However, there is room for improvement in instilling confidence in the CSPs' ability to recover from disasters. The majority of respondents also trust that CSPs are honest about their handling of security matters. These findings highlight the importance of continuous efforts by CSPs to enhance disaster recovery capabilities and maintain transparency in order to foster trust among their customers.

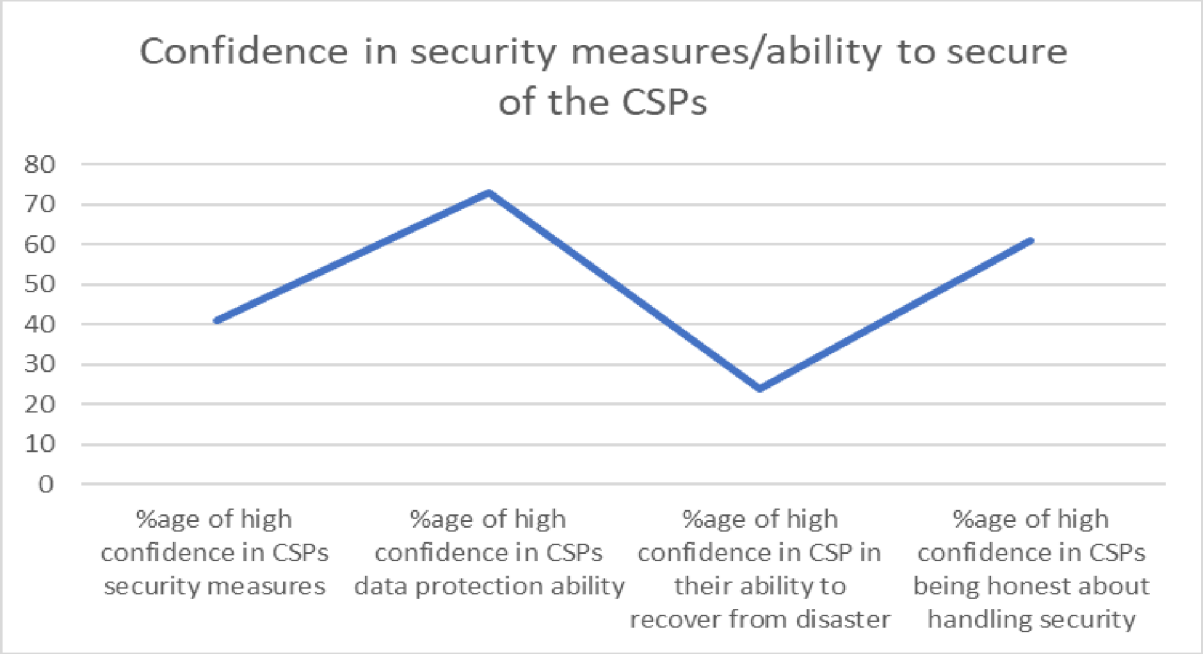

Figure 13: Confidence in security measures

4.4.3.3 Cloud security vs On-premises solutions security

Respondents were also asked if they think that the cloud offers more security than their on-premises solutions and it was noted based on the calculations, a significant percentage of respondents, specifically 84%, agree that cloud solutions offer more security compared to their on-premises counterparts. This finding suggests that a large majority of the sample population perceives the cloud as a more secure option for storing and managing their data, surpassing the security provided by traditional on-premises solutions.

This high level of agreement highlights the confidence and trust placed in cloud service providers (CSPs) when it comes to security measures. It indicates that respondents believe that CSPs have robust security protocols, technologies, and expertise to protect data in the cloud environment more effectively than they can achieve with their own on-premises systems.

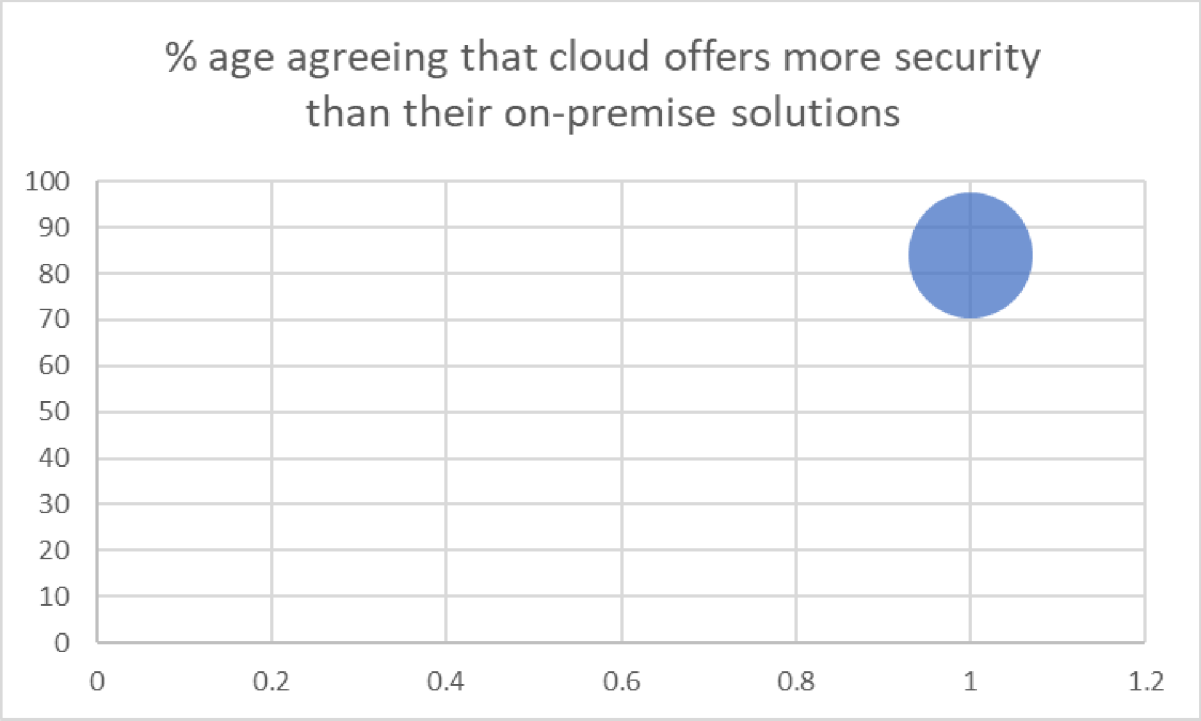

Figure 14: Cloud security vs On-premises solutions security

4.4.4 Knowledge and Awareness of Cloud Security

Respondents were asked yes or no regarding.

1. Their knowledge of cloud computing
2. Their awareness of the cloud security shared responsibility model
3. Knowledge of security or data breach instances involving CSPs
4. Knowledge of serverless computing and its impact on security

4.4.4.1 Knowledge area analysis

In the given dataset, the respondents were assessed on their knowledge in various areas related to cloud computing and security. Among the respondents, 79 individuals demonstrated knowledge of cloud computing, indicating a relatively high level of understanding in this area. However, the knowledge of cloud computing shared responsibility model was observed in only 24 respondents, suggesting a lower awareness of the shared responsibilities between cloud service providers and customers in ensuring security. Similarly, only 10 respondents displayed knowledge of security or data breach instances involving cloud providers, indicating a relatively limited understanding of the potential risks and breaches in the cloud environment. Knowledge of serverless computing

and its impact on security was observed in 35 respondents, reflecting a moderate level of familiarity with this aspect. Notably, none of the respondents exhibited knowledge of zero-trust security and its relation to cloud computing, indicating a complete lack of awareness in this domain. These findings highlight the varying levels of knowledge and understanding among the respondents in different areas of cloud computing and security, indicating potential areas for improvement and further education.

Knowledge area	Count of Respondents
Knowledge of cloud computing	79
Knowledge of cloud computing shared responsibility model	24
Knowledge of security or data breach instances involving cloud providers	10
Knowledge of serverless computing and impact on security	35
Knowledge of zero-trust security and relation to cloud computing	0

Table 7: Knowledge level of cloud computing

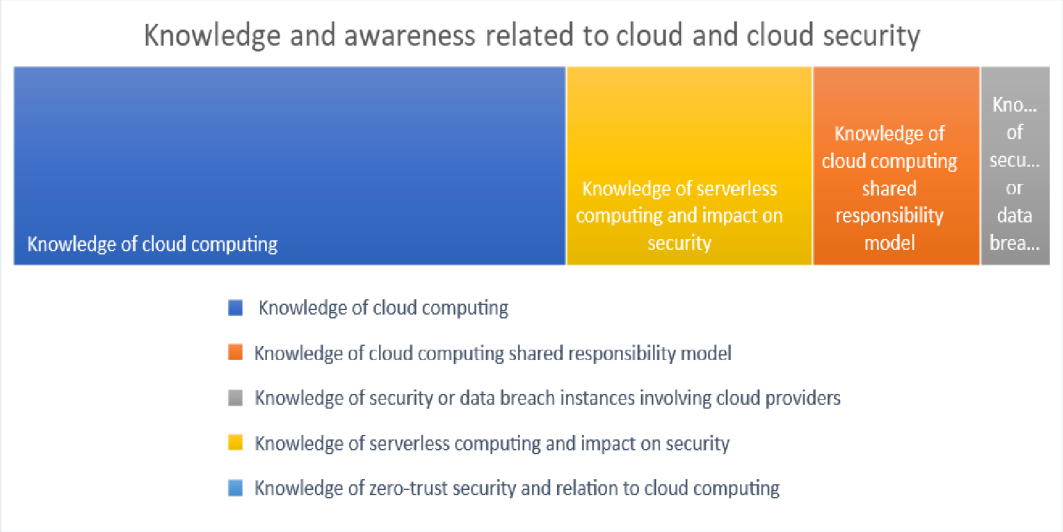

Figure 15: Knowledge and awareness related to cloud & cloud security

4.4.4.2 Impact of knowledge and awareness of cloud security on the occurrence of security breaches

For this analysis, we classified the population into high knowledge and low knowledge groups. It was assumed that the high knowledge group is those who had understanding in all or at least 3 areas.

The t-test will help us determine if there is a significant difference in breach occurrence between the high-knowledge and low-knowledge groups. The null hypothesis (H0) assumes that there is no significant difference between the two groups, while the alternative hypothesis (H1) assumes that there is a significant difference. Using the provided breach occurrence data, we'll conduct an independent two-sample t-test. Performing the t-test, we obtain the following results:
t-value: -1.4966 p-value: 0.1381
With a p-value of 0.1381, which is above the commonly used significance level of 0.05, we fail to reject the null hypothesis. This means that there is not enough evidence to conclude that there is a significant difference in breach occurrence between the high-knowledge and low-knowledge groups.

4.4.5 Implementation of cloud security defensive measures

The respondents were surveyed regarding their implementation of various cloud security defensive measures. The purpose of this analysis is to investigate the potential impact of adopting these defensive measures on reducing cloud breaches and incidents.

4.4.5.1 Frequency of Audits and Occurrence of Cloud Security Breaches or Incidents

We aim to examine the statistical relationship between the frequency of audits and the occurrence of cloud security breaches or incidents. To achieve this, a contingency table was constructed, as shown below:

	Security Incident or Breach: No	**Security Incident or Breach: Yes**
Frequency of Audit/Evaluation: 1	**35**	**26**
Frequency of Audit/Evaluation: 0	**5**	**34**

Table 8: Occurrence of Cloud Security Breaches or Incidents

Note: Frequency of Audit/Evaluation: 1 means regularly
Frequency of Audit/Evaluation: 0 means occasionally

Using this contingency table, we conducted a chi-square test of independence to assess the association between the frequency of audits and the occurrence of cloud security breaches or incidents.

The expected frequencies for each cell were calculated based on the row and column totals, as well as the grand total. Subsequently, the chi-square test statistic was computed by

summing the contributions from each cell, which were determined by comparing the observed and expected frequencies.

The calculated chi-square value was found to be 15.869. With one degree of freedom (df), we compared this value to the critical chi-square value at a significance level of 0.05. The critical chi-square value for df = 1 was determined to be 3.841.

Considering that the calculated chi-square value (15.869) exceeds the critical chi-square value (3.841), we reject the null hypothesis of independence. These results provide evidence to support the hypothesis that there is a statistically significant association between the frequency of audits and the occurrence of cloud security breaches or incidents. In conclusion, the analysis suggests that adopting a higher frequency of audits may reduce cloud security breaches or incidents. Further research and examination of other factors are recommended to gain a more comprehensive understanding of the relationship between defensive measures and cloud security outcomes.

4.4.5.2 Effectiveness of security measures in preventing breaches

During the survey, participants were inquired about the security measures they employ, which included options such as data encryption, access management, multi-factor authentication (MFA), and regular security evaluations and audits. An interesting observation was made regarding the occurrence of breaches in relation to the implementation of these measures.

It was observed that the cases with the lowest number of breaches were associated with a higher adoption rate of data encryption both in transit and at rest, as well as the management of access restrictions and permissions. These measures were found to be implemented more frequently by the respondents.

On the other hand, despite some instances where breaches were not reported, regular security evaluations and audits were perceived to be the least effective among the implemented measures. This suggests that their implementation alone did not consistently lead to a significant reduction in the occurrence of breaches.

Overall, the findings highlight the importance of implementing robust security measures such as data encryption and access management, which have demonstrated a positive

impact in preventing breaches, while also underscoring the need for further investigation into the effectiveness of regular security evaluations and audits in the specific context examined.

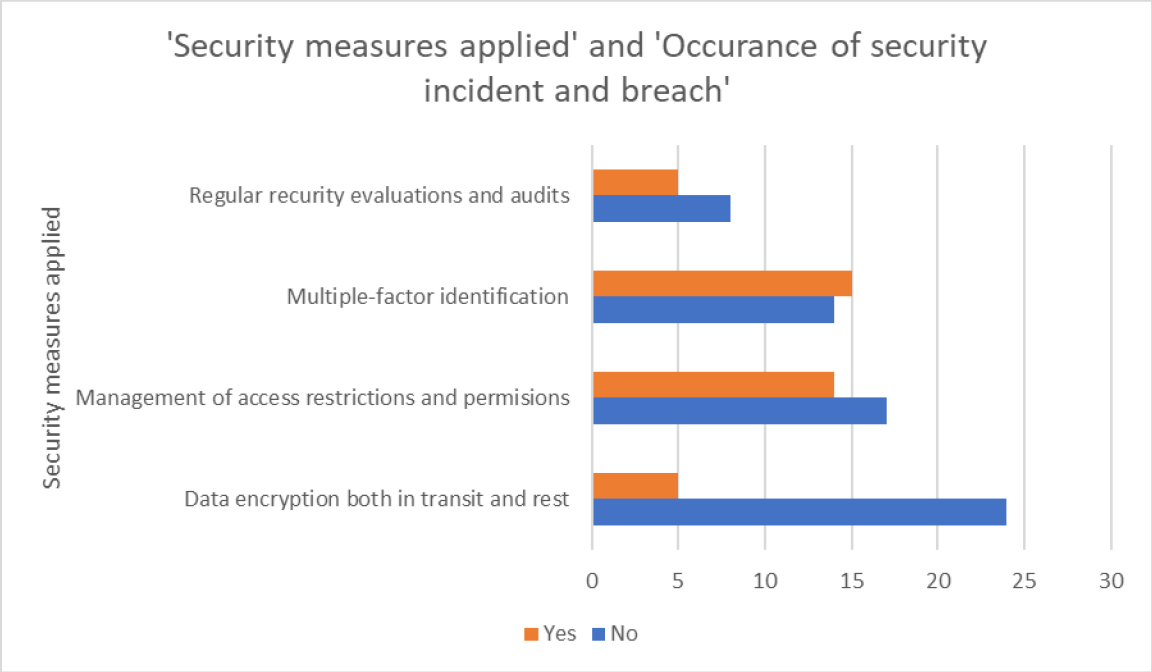

Figure 16: Security measures applied and occurrence of security breaches or incidents

4.4.5.3 Relation between Data confidentiality and security measures implemented

Respondents were asked what kind of confidential information they store in the cloud and furthermore, analysis was done if the confidentiality levels of data influenced or encouraged certain types of security measures.
A contingency table was created to analyse the relationship:

Data Confidentiality	**Security Measure implemented**				
	Multiple -factor identification	Regular security evaluations and audits	Data encryption both in transit and at rest	Management of access restrictions and permissions	Grand Total
Financial data	9	10	6	12	37
Intellectual property	9	3	5	6	23
PII	3	7	10	2	22
Health records	6	5	3	4	18
Grand Total	**27**	**25**	**24**	**24**	**100**

Table 9: Security Measure for Cloud Implementation

The analysis reveals a correlation between the type of confidential information stored in the cloud and the security measures implemented. Among the respondents, 37 out of 100 store financial data in the cloud. For this type of sensitive information, access restrictions and permissions are the most common security measure implemented by 12 organizations. Encryption measures, both in transit and at rest, are adopted by 10 organizations, followed by regular security evaluations and audits implemented by 6 organizations.
Similarly, 23 respondents store intellectual property in the cloud, with encryption being the most prevalent security measure implemented. Multiple-factor identification is

implemented by 6 organizations, while access restrictions and permissions are employed by 5 respondents. For personally identifiable information (PII), 22 organizations reported storing such data in the cloud. Encryption is the most implemented security measure for PII, with 10 organizations using it. Access restrictions and permissions are employed by 7 respondents, while multiple-factor identification is implemented by 3 respondents. Health records are stored by 18 organizations in the cloud, with access restrictions and permissions being the primary security measure implemented by 6 organizations. Encryption, multiple-factor identification, and regular security evaluations and audits are employed by 5, 4, and 3 respondents respectively.

In summary, organizations recognize the importance of tailoring security measures to the specific nature of the confidential data stored in the cloud. By implementing appropriate security measures, such as access restrictions, encryption, multiple-factor identification, and regular security evaluations and audits, organizations can effectively protect their sensitive information and maintain data confidentiality.

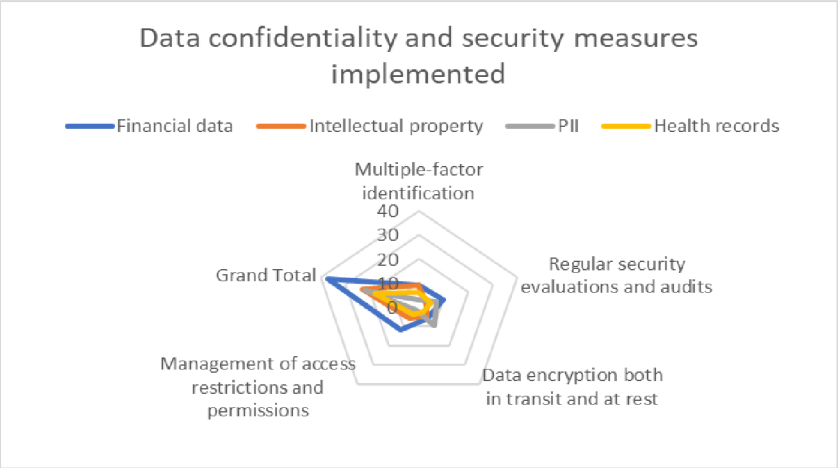

Figure 17: Data confidentiality and the security measures implemented

4.4.6 Challenges for SMEs when implementing cloud security solutions

Small and Medium-sized Enterprises (SMEs) face unique challenges when it comes to implementing cloud security solutions. Despite their limited resources and budgets, SMEs must navigate regulatory and compliance requirements, address a lack of internal knowledge, and ensure the availability of necessary materials. The survey results indicate that SMEs encounter significant difficulties in terms of both regulatory and compliance

issues and a lack of internal knowledge, with 13 and 15 respondents, respectively, expressing concerns in these areas. Although budgetary and material constraints are comparatively lower for SMEs, these organizations must still carefully consider how to allocate their limited resources to effectively address their cloud security needs.

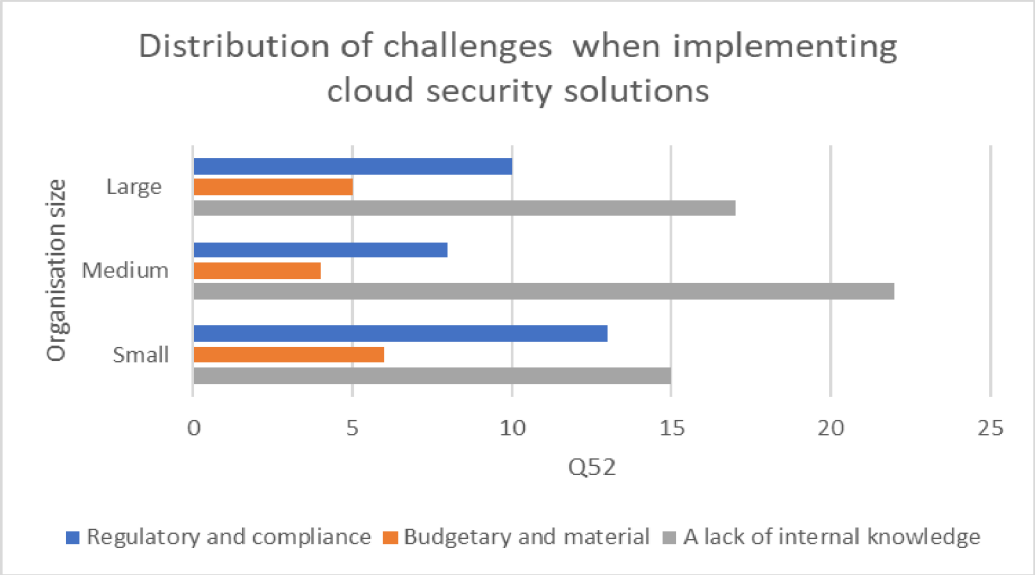

Figure 18: Challenges for SMEs when implementing cloud security solutions

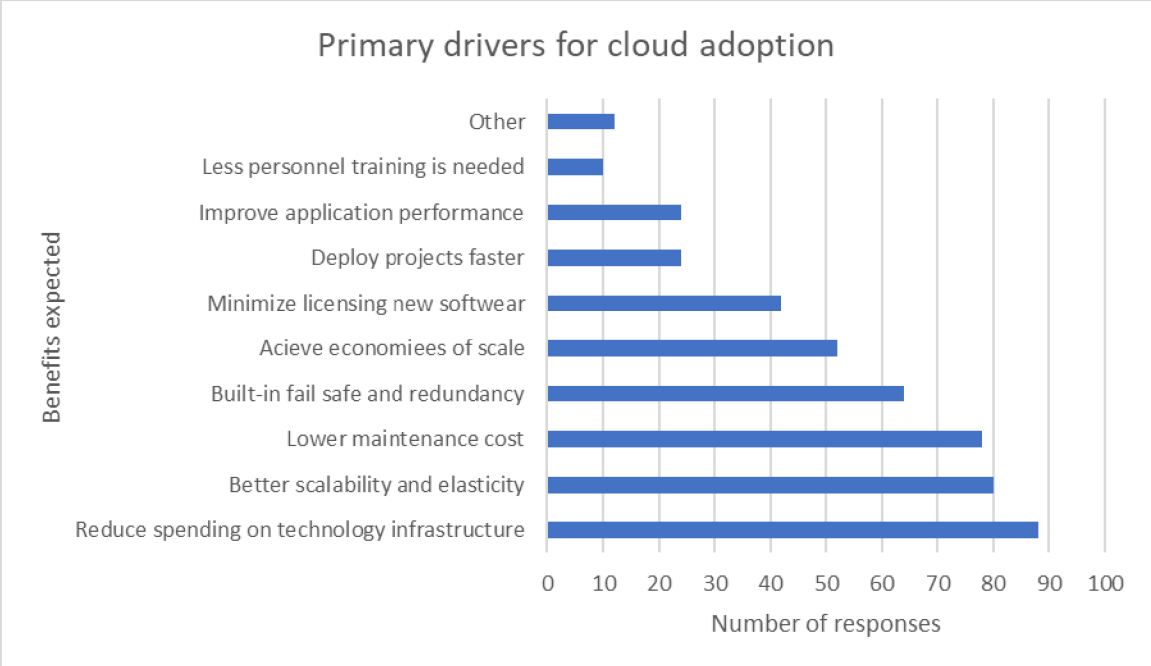

Figure 19: The primary drivers for cloud adoption

The benefits of cloud computing would motivate SMEs to embrace it right away for business expansion and reducing the cost. There are some potential reasons that may lead to cloud computing adoption for SMEs in Bangladesh. The bar chart in figure 19 shows that benefits of cloud adoption expectation are 88 % for reduce spending on technology infrastructure, followed by 10 % lower maintenance cost, and 80 % for better scalability and elasticity in the top lists. Redundancy and software licensing are also major driving forces. But it is evident that SMEs encounter a variety of challenges both from the inside and the outside. Therefore, a realistic information is needed about this technology to increase user awareness and ensure that everyone especially managers and owners of small and medium-sized businesses fully understand its benefits.

4.4.7 Future Trends and Expectations in cloud computing security

In the content analysis of open-ended responses, the following themes emerged regarding future trends in cloud computing security: 1) The growing use of AI and ML (mentioned by 38 respondents), 2) A stronger focus on data privacy (mentioned by 33 respondents), and 3) Stricter laws and compliance (mentioned by 26 respondents). These findings indicate a recognition of the importance of AI/ML, data privacy, and regulatory compliance in shaping the future of cloud security. Other mentioned themes included the adoption of Zero Trust Architecture, DevSecOps integration, and AI/ML for threat detection, highlighting the industry's interest in advanced technologies.

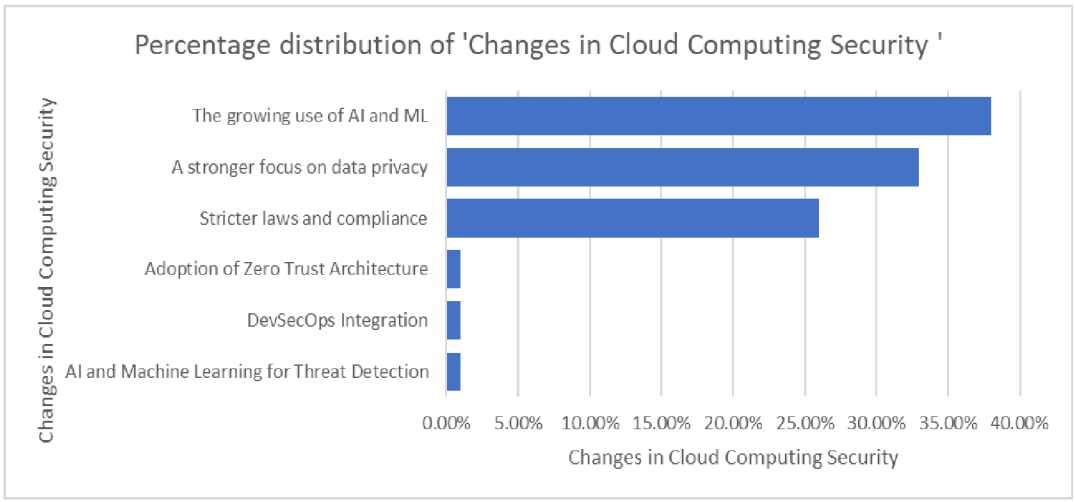

Figure 20: Future Trends and Expectations in cloud computing security

5. Results and Discussion

The findings from the practical will now be discussed in this chapter with particular attention on the cloud computing adoption, benefits, security concern and challenges. The main objectives of this study is to provide a foundation of knowledge and awareness regarding how the security measure was influencing in cloud adoption decision-making; determining the factors that influencing most of the businesses organizations when weighing economic benefits and the risks. These goals have been achieved. Prospective cloud users and cloud service providers may both utilize the information covered in this chapter for building future cloud use plans, and customize their services offering from a more user-oriented perspective.

Benefits of Cloud Adoption

The analysis of literature review offered background information on the present trend of cloud adoption with economic benefits. According to the survey data analysis, the respondents believed that the major advantage of using cloud computing would be lower IT cost and pay-as-you-go pricing strategies, including infrastructure, scalability and flexibility. The survey finding indicates that 35% of organizations prioritize cost-saving pay-as-you-go pricing strategies and IT infrastructure, scalability and flexibility are valued by 27% of organizations.

Cloud Security Concern and Challenges

Cloud security is considered one of the greatest challenges both service providers and customers. It is regarded as the main concerned by 90% of respondents. The main concerns with cloud include data privacy and security, integration with existing systems, regulatory compliance, and data mobility/vendor lock-in. The survey finding indicates that the highest average score of 25 indicating a significant emphasis on security. It is quite obvious that security issues of cloud computing are an important issue that cannot be overstated owing to threats from both inside and outside of cloud environments. Thus, cloud service providers should improve their service offerings in this area as well.

Based on the findings we can conclude that cloud users do not have a positive outlook on cloud security, because there are a lot of unidentified risk variables in the cloud environment and customers see the security of cloud computing as being inadequate. 31%

of respondents have high concerns about cloud-based data privacy, indicating a significant level of worry regarding the security and confidentiality of their data stored in the cloud and 34% of respondents express high concerns about the physical security of cloud data centers. However, the most notable finding from the chart is the high percentage of respondents, at 85%, expressing concerns about insider threats. Therefore, users of cloud computing services are concerned with their security and not yet completely convinced by the security measures provided by the cloud service providers.

Knowledge and Awareness of Cloud Security

The survey revealed that respondents had a high degree of security awareness related to cloud computing and security. Among the respondents, 79 individuals demonstrated knowledge of cloud computing, indicating a relatively high level of understanding in this area.

Challenges of Cloud Computing for SMEs

Most of the respondents think that SMEs should embrace cloud computing in Bangladesh, because it can bring a tremendous benefit on SMEs. Despite their limited resources and budgets, SMEs must navigate regulatory and compliance requirements, address a lack of internal knowledge, and ensure the availability of necessary materials. The survey results indicate that SMEs encounter significant difficulties in terms of both regulatory and compliance issues and a lack of internal knowledge, with 13 and 15 respondents, respectively, expressing concerns in these areas.

Finally, the survey findings indicate that security is the biggest concern of all the factors to determine the performance and growth of cloud computing. The purpose of this thesis is to determine the current security risks associated with cloud computing clearly explained how these risks influence organizations' cloud adoption decisions. So cloud-based systems need to be more consistens for tailoring security measures in order to make the cloud more secure and reliable. By implementing appropriate security measures, such as access restrictions, encryption, multiple-factor identification, and regular security evaluations and audits, organizations can effectively protect their sensitive information and maintain data confidentiality. As a result, the issue of cloud computing security, threats and challenges will remain relevant.

6. Recommendation

The following recommendations have been made based on the key findings of this study in the context of ICT specially for SMEs. Thes recommendations are applicable for cloud service users or planning to adopt cloud computing in the future.

It is quite clear that security concern of cloud computing is an important issue that cannot be underrated owing to threats from both inside and outside of cloud environments. So, it is important to verify the service provider's capabilities like feedback from existing customer and reliability before migrating to any cloud services. Information regarding audits details and incident reports can help to identify the best service provider from the other vendors.

Before using a cloud provider, users should verify the following aspects of their cloud provider including data, infrastructure, applications as well as internal and external security. Cloud service provider must follow strong industry-level security standards, regulatory compliance, and customer requirements for gaining customers' trust.

Cloud service providers should have provided the most up-to-date and effective security measures for their customers. Service providers have the responsibility to make sure that appropriate security and isolation measures are implemented to reduce the risks that users offer to one another; when it comes to data loss, misuse, or violation of privacy in the cloud.

Multilayer security protection: A knowledgeable client is aware of the importance of multilayer security and how it protects customers' private information and resources. On the contrary, cloud security can be maintained with defense-in-depth, continuous monitoring, along regular trainings, and risk assessments.

Many new clients are attracted to cloud computing as it is becoming popular day by day, but they are reluctant to migrate it. Cloud technology will not move to the next level, if these factors are not improved. Cloud service providers need to take the greater responsibility to maintain the long-term security of the cloud environment.

The majority of security breaches have been occurred due to improper or restricted access controls. Hence, limited access controls to cloud resources should be implemented by

cloud providers. Nevertheless, it is important for both cloud providers and consumers to consistently verify if their software is up to date, because outdated software might be a target for attackers as it is easy to carry out attacks using known weaknesses.

Many of the cloud users think that adopting cloud is more secured, effective, and economical. The majority of them lack comprehensive understanding of cloud computing as well as they are unable to evaluate the potential risks associated with cloud migration. In addition, it important to educate them by offering trainings and security awareness programs for a secure cloud computing environment. Both cloud service providers and users should work together to share responsibility for privacy and data security.

Small and medium-sized businesses (SMEs) need to take the initiative to educate their employees and staff members about cloud security risks and threats. According to research, information security is most threatened by the individuals who use and manage technology. That is why it is important to be aware normal users of information systems about the risks to information security that they represent, in addition to the technological protections in place.

7. Conclusion

It has become more clear after completing this thesis that cloud computing indeed has immeasurable benefits not only to the computing field, but also many organizations, and users in the context of ICT. Therefore, small and medium-sized enterprises can take advantage of a number of benefits provided by cloud computing. These benefits can be achieved through cloud computing's economies of scale and flexibility. So Cloud computing can be a good option for SMEs considering the current state of resources availability and IT demands in Bangladesh. The key findings of this research is that cloud adopting in SMEs would have enhanced better service delivery as well as higher productivity and efficiency. However, a great deal of awareness needs to be raised by the service providers for SMEs in order to take advantages of the numerous benefits from cloud computing.

On the other hand, potential benefits and flexibility offered by cloud computing comes with different threats, security risks and challenges. This research has explored the advantages of cloud computing as well as the numerous security issues and challenges that come with it. Data security and privacy are the main concerns along with regulatory compliance, data location, and trust in the cloud environment, because the huge amount of data and resources are accessible in the cloud which makes it easier for attackers to take advantage of it. So, it is the responsibility of cloud service providers as well as customers to provide efficient security both inside and outside of the cloud and how they addressing the need of security issues in cloud environment. Some important measures have to be taken **in order to make the cloud more** reliable, scalable, and affordable from the service providers such as access restrictions, encryption, multiple-factor identification, regular security evaluations and audits. This study enables cloud users to make well-informed decisions by understanding the risks and threats before transferring their organization's data to the cloud as well take necessary precautions.

Finally, it can say that cloud computing can bring positive economic, functional, and additional security benefits for companies especially for SMES and IT firms if it is implemented and designed appropriately. With IT giants such as Google, Amazon and even Microsoft are competing to expand their market share in providing cloud services.

8. References

ADAM, I.O. and Musah, A. Small and medium enterprises (SMEs) in the cloud in developing countries: A synthesis of the literature and future research directions. *J. Mgmt. & Sustainability*, 2015. Vol. 5, p. 115.

ALBESHRI, A. Boyd, C. and Nieto, J.G. A security architecture for cloud storage combining proofs of retrievability and fairness. In *3rd International Conference on Cloud Computing, GRIDS and Virtualization, 2012.* pp. 30-35.

ALSAEED, N. and Saleh, M. Towards cloud computing services for higher educational institutions: Concepts & literature review. In *2015 international conference on cloud computing (ICCC)*. IEEE, 2015. p. 1-7.

AMAZON. About Amazon Web Services. [online]. 2022. [Accessed 25 February 2021]. Available from: http://aws.amazon.com

ARDAGNA, C.A. Asal, R. Damiani, E. and Vu, Q.H. From security to assurance in the cloud: A survey. *ACM Computing Surveys (CSUR)*, 2015. Vol. *48*(1), pp.1-50.

ATTRAPADUNG, N. Herranz, J. Laguillaumie, F. Libert, B. De Panafieu, E. and Ràfols, C. Attribute-based encryption schemes with constant-size ciphertexts. *Theoretical computer science*. 2012. Vol. *422*, pp.15-38.

BARR, R. Qualys Inc. How to gain comfort in losing control to the cloud. 2013.

BEHL, Akhil. and Kanika, Behl. An Analysis of Cloud Computing Security Issues. 2012. IEEE proceedings World Congress on Information and Communication Technologies, pp.109-114. ISBN: 978-1-4673-4805-8.

BIKRAM, B. Safe on the Cloud. A Perspective into the Security Concerns of Cloud Computing. 2009. Vol. 4. p. 34-35.

BOT, A.G. Menendez, M.E. Neuhaus, V. Mudgal, C.S. and Ring D. The comparison of paper-and web-based questionnaires in patients with hand and upper extremity illness. 2013. *Hand*, *8*(2), pp. 210-214.

BRYMAN, A. and Cramer, D. Quantitative data analysis with SPSS 12 and 13: A guide for social scientists. Psychology Press, 2005.

Bryman, A. and Cramer, D. Quantitative data analysis with SPSS 12 and 13: A guide for social scientists. Routledge, 2004.

BUYYA, R. and Murshed, M. 2002. Gridsim: A toolkit for the modeling and simulation of distributed resource management and scheduling for grid computing. The Journal of Concurrency and Computation: Practice and Experience (CCPE), 2002.

BUYYA, R. Vecchiola, C. and Selvi, S.T. Mastering cloud computing: foundations and applications programming. Newnes, 2013.

CAFARO, M. & Aloisio, G. Grids, clouds and virtualization. Dordrecht: Springer Varelag. 2010.

CISCO Annual Internet Report: Global Internet adoption and devices and connection, 2018–2023 White Paper. [Online]. 9 March 2020. [Accessed 8 December 2022]. Available from: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

CLOUD Academy. San Francisco: Cloud Academy. 2016. [Accessed 23 December 2022]. Available from: http://www.cloudacademy.com

CREEGER, M. 2009. CTO roundtable: cloud computing. Communications of the ACM. 2009. Vol. 52(8), p. 50-56.

CRESWELL, J. W. Research designs: Qualitative, quantitative, and mixed methods approaches. California: Sage, 2009. P. 20, 86.

DAWSON, C. Practical Research Methods. How To Books Ltd. 2002. p. 20-79.

DILLON, T. Wu, C. and Chang, E. Cloud computing: issues and challenges. In 2010 24th IEEE international conference on advanced information networking and applications (AINA). Ieee, 2010. p. 27 -33.

ELINOR, M. Cloud computing security forecast: Clear skies. [online]. 27 January 2009. *News. cnet. com.* [Accessed 17 April 2022]. Available from: *http://news. cnet. com/8301-1009_3-10150569-83*

ESWARAN, S. and Abburu, S. Identifying data integrity in the cloud storage. *International journal of computer science issues (IJCSI)*. 2012. Vol. *9*(2), p.403.

EUROPA. *What is an SME?*. Europa.eu [online]. 2014. [Accessed 3 March 2022]. Available from: https://single-market-economy.ec.europa.eu/smes/sme-definition_en

FINN, A. Vredevoort, H. Lownds, P. and Flynn, D. *Microsoft private cloud computing*. John Wiley & Sons, 2010.

FOX A, Griffith R, Joseph A, Katz R, Konwinski A, Lee G, Patterson D, Rabkin A, Stoica I. Above the clouds: A berkeley view of cloud computing. Dept. Electrical Eng. and

Comput. Sciences, University of California, Berkeley, Rep. UCB/EECS. [online]. 10 February 2009. p. 1-8. [Accessed 14 February 2021].
Available from: *http://www2.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf*

FOX, A. Griffith, R. Joseph, A., Katz, R. Konwinski, A. Lee, G. Patterson, D. Rabkin, A. and Stoica, I. Above the clouds: A berkeley view of cloud computing. *Dept. Electrical Eng. and Comput. Sciences, University of California, Berkeley, Rep. UCB/EECS*. 2009.
Available from: https://www2.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html

GHANAM, Y. Emerging issues & challenges in cloud Computing—A hybrid approach. Journal of Software Engineering and Applications. [online]. 26 November 2012. [Accessed 28 October 2022]. Vol. 5(11), p. 923-937. DOI 10.4236/jsea.2012.531107.
Available from: https://www.scirp.org/pdf/JSEA20121100011_55442678.pdf

GHAURI, P. N., & Grønhaug, K. *Research Methods in Business Studies: A Practical Guide*. London: Pearson Education, 2005.

GRAY, D.E. Doing research in the real world. *Doing research in the real world*. London, 2021. pp.1-100.

HAN, Y. Cloud storage for digital preservation: optimal uses of Amazon S3 and Glacier. *Library Hi Tech*. 2015.Vol. *33*(2), p.261-271.

Hashim, M.K. and Abdullah, M.S. A proposed framework for redefining SMEs in Malaysia: One industry, one definition. *Asian academy of management journal*, 2000. Vol. *5*(1), pp.65-79.

HAYES, B. Cloud computing. In: ACM New York, NY, 2008.HOBSON, D. Into the Cloud We Go..... *Cloud Computing Journal.* 2009. *Vol. 2, Issue 3*, p. 8-9.

HORRIGAN, J. B. Cloud computing' takes hold as 69% of all internet users have either stored data online or used a web-based software application [online]. 12 September 2008. pewresearch.org. [Accessed 12 May 2022].
Available from: https://www.pewresearch.org/internet/2008/09/12/cloud-computing-takes-hold-as-69-of-all-internet-users-have-either-stored-data-online-or-used-a-web-based software-application/

HUTH, A. and Cebula, J. The basics of cloud computing. *United States Computer*. 2011. pp.1-4.

IANKOULOVA, I. and Daneva, M. Cloud computing security requirements: A systematic review. In *2012 Sixth International Conference on Research Challenges in Information Science (RCIS)*. IEEE, 2012. p. 1-7.

JIANG, Jianchun, and Weiping, WEN. The information security problems of cloud computing environment. *Netinfo Security*. 2010. Vol. 10.2, p. 61-63.

JOHNSTON, S. Cloud Computing Types: Public Cloud, Hybrid Cloud, Private Cloud. *Random rants about technology.* 2009. [Accessed 27 February 2021]. Available from: http://samj.net/2009/03/cloud-computing-types-public-cloud.html

JOINT, A. and Baker, E. Knowing the past to understand the present–issues in the contracting for cloud based services. *Computer Law & Security Review*. 2011. Vol. *27*(4), p.407-415. DOI 10.1016/j.clsr.2011.05.002

KHAJEH-HOSSEINI, A. Sommerville, I. and Sriram, I. Research challenges for enterprise cloud computing. *arXiv preprint arXiv:1001.3257*. 2010.

KHAJEH-HOSSEINI, A. Sommerville, I. Sriram, I. *Research Challenges for Enterprise Cloud Computing.* Submitted to the 1st ACM Symposium on Cloud Computing, SOCC 2010.

KHMELEVSKY, Y. and Voytenko, V. Cloud computing infrastructure prototype for university education and research. In *Proceedings of the 15th Western Canadian Conference on Computing Education*. 2010. pp. 1-5.

KHORSHED, M.T., Ali, A.S. and Wasimi, S.A. A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. *Future Generation computer systems.* 2012. Vol. *28*(6), pp.833-851. [Accessed 27 July 2021]. Available from: https://doi.org/10.1016/j.future.2012.01.006

KING, N.J. and Raja, V.T. Protecting the privacy and security of sensitive customer data in the cloud. *Computer Law & Security Review*.2012. Vol. *28*(3), pp.308-319.

KRUTZ, R.L. and Vines, R.D. Cloud Security: A Comprehensive Guide to Secure Cloud Computing. Wiley Publishing: *Inc. Indianapolis, Indiana 2010*.

KVETON, P. Jelínek, M. Klimusová, H. and Voboril, D. Data collection on the internet: evaluation of web-based questionnaires. *Studia psychologica*. 2007. Vol. 49, no. 1, p. 81-88.

Lakshmisri, S. MACHINE LEARNING ON NETWORK SECURITY, 2019.

LEE, G. and Nick, A. Cloud Computing: Principles, Systemsand Applications, (Computer Communications and Networks). London: Springer, 2010. ISBN 9781849962407.

MA, X. 2012, August. Security concerns in cloud computing. In *2012 Fourth International Conference on Computational and Information Sciences (ICCIS)*. IEEE, 2012. p. 1069-1072.

MACVITTIE, L. Load balancing is key to successful cloud-based (dynamic) architectures. *DevCentral Home*. 2009. [Accessed 31 March 2021]. Available from: http://devcentral.f5.com/weblogs/macvittie/archive/2009/01/23/loadbalancing-iskey-to-successful-cloud-based-dynamic-architectures.aspx

MALIK, M.I. Wani, S.H. and Rashid, A. CLOUD COMPUTING TECHNOLOGIES. *International Journal of Advanced Research in Computer Science*, *9*(2). 2018.

MCCARTHY, J. Speech given at MIT. *Time-Sharing Computer Systems*. 1961.

MELL, P. and Grance, T. The NIST definition of cloud computing. 2011. pp. 1–2, 2009.

MELL, P. Grance, T. The NIST Definition of Cloud Computing; NIST: USA, 2009. [online]. [Accessed 3 January 2021].

Available from: https://csrc.nist.gov/publications/detail/sp/800-145/final

MIKE, Fratto. *Private Clouds Will Change IT Jobs, Not Eliminate Them.* online]. 1 June 2012. Networks Computing. [Accessed 10 March 2023]. Available from: https://www.networkcomputing.com/cloud-infrastructure/private-clouds-will-change-it-jobs-not-eliminate-them

MIKE, Fratto. *The hybrid cloud: What is it, and how do you get there?*. [online]. 1 June 2012. Networks Computing. [Accessed 12 March 2023].

Available from: https://www.networkcomputing.com/cloud-infrastructure/hybrid-cloud-what-it-and-how-do-you-get-there

MOLLAH, M.B. Islam, K.R. and Islam, S.S. Next generation of computing through cloud computing technology. In *2012 25th IEEE Canadian conference on electrical and computer engineering (CCECE)*. IEEE, 2012. p. 1-6.

NARASIMHAN, B. *Cloud Computing Saving – Real or Imaginary?* [online]. 2009.Appirio. [Accessed 15 February 2022].

Available from: http://blog.appirio.com/2009/04/cloud-computing-savings-realor.html

NICK, A. and Gillam, L. *Cloud Computing: Principles, Systems and Applications*. London: Springer, 2010. p.361-372.

NIST. Cloud Computing Definition. [online]. 2021. [Accessed 25 August 2021]. Available from: http://www.nist.gov/itl/csd/cloud-102511.cfm

PAHL, C. and Xiong, H. Migration to PaaS clouds-Migration process and architectural concerns. In 2013 IEEE 7th International Symposium on the Maintenance and Evolution of Service-Oriented and Cloud-Based Systems. IEEE, 2013. p. 86-91.

PATTERSON, D. Rabkin, A. Ahmed, M. and Hossain, M.A. Cloud computing and security issues in the cloud. International Journal of Network Security & Its Applications. 2014. [Accessed 25 April 2022]. Available from: (IJNSA), 6(1):25-36. DOI: 10.5121/ijnsa.2014.6103 25.

PIERS, Wilson. Positive perspectives on cloud security. *Information Security Technical Report*, 2011.

OGIGAU-NEAMTIU, F. Cloud computing security issues. *Journal of Defense Resources Management (JoDRM)*. 2012. Vol. *3*(2), pp.141-148.

OLIVEIRA, T. and Martins, M.F. Understanding e-business adoption across industries in European countries. *Industrial management & data systems*. 2010. Vol. *110*(9), p. 1337-1354.

RAI, R. Sahoo, G. and Mehfuz, S. (2013). Securing Software as a Service Model of Cloud Computing: Issues and Solutions. *arXiv preprint arXiv:1309.2426.* International Journal on Cloud Computing: Services and Architecture. 2013. Vol. 3(4), 1-11. DOI 10.5121/ijccsa.2013.3401

RAULINE. The public cloud debate. Crn, (1307), 2011. p. 10.

RAMGOVIND, S. Eloff, M.M. and Smith, E. The management of security in cloud computing. In *2010 Information Security for South Africa*. IEEE, 2010. p. 1-7.

RITTINGHOUSE, J.W. and Ransome, J.F. Cloud computing: implementation, management, and security. CRC press, 2016.

ROUSE, M. (2012) Definition Community cloud. [online] 2012. Search Cloud Storage Tech Target. [Accessed 20 November 2021].

Available from: http://searchcloudstorage.techtarget.com/definition/community-cloud

SADIKU, M.N. Musa, S.M. and Momoh, O.D. Cloud computing: opportunities and challenges. *IEEE potentials*. 2014. Vol. *33*(1), p.34-36.

SHAIKH, F.B. and Haider, S. Security threats in cloud computing. In *2011 International conference for Internet technology and secured transactions*. 11 December 2011. IEEE. p. 214-219.

SATYANARAYANA, S. CLOUD COMPUTING: SAAS. Journal of Computer Science and Telecommunications. Vol. 4, No. 4, p. 76-79.

SELVIANDRO, N. Suryani, M. and Hasibuan, Z.A. Open learning optimization based on cloud technology: case study implementation in personalization E-learning. In *16th International Conference on Advanced Communication Technology*. IEEE, 2014. pp. 541-546.

SHIMBA, Faith. Cloud computing: Strategies for cloud computing adoption. 2010.

SINGH, S. and Jangwal, T. Cost breakdown of public cloud computing and private cloud computing and security issues. *International Journal of Computer Science & Information Technology*. 2012. Vol. *4*(2), p.17-31.

SINGH, S. Jeong, Y.S. and Park, J.H. A survey on cloud computing security: Issues, threats, and solutions. *Journal of Network and Computer Applications*. 2016. Vol. 75, pp. 200–222.

SME Foundation (2015). *International Journal of SME Development.* Vol. 01, issue. 01, Small & Medium Enterprise Foundation, Dhaka, Bangladesh. [Accessed 13 July 2021]. *Available from: http://www.smef.org.bd/v2/smef_download/journal.pdf*

STARKS, Christopher. *The History of Cloud Computing*. [online]. 28 March 2012. [Accessed 17 January 2022]. Available from: https://www.cetrom.net/resources/blog/uncategorized/the-history-of-cloud-computing

SRINIVASAN, S. ed. Security, trust, and regulatory aspects of cloud computing in business environments. IGI Global, 2014.

STOICA, I., Morris, R., Karger, D., Kaashoek, M. F., Balakrishnan, H. Chord: A Scalable Peer-to-peer Lookup Service for Internet Applications. *ACM SIGCOMM Computer Communication Review, 2002. Vol. 31(4), 149-160.*

SUBASHINI, S. and Kavitha, V. A survey on security issues in service delivery models of cloud computing. *Journal of network and computer applications*. 2011. Vol. *34*(1), pp.1-11.

SULLIVAN, T. The ways cloud computing will disrupt IT. [online]. 26 March 2009. cio.com. [Accessed 26 December 2022]. Available from:

https://www2.cio.com.au/article/296892/nick_carr_ways_cloud_computing_will_disrupt_it/

SURYA, L. (2019). Machine learning-future of quality assurance. *International Journal of Emerging Technologies and Innovative Research.* [online]. 4 May 2019. Vol.6, Issue 12, pp1078-1082. [Accessed 15 April 2022]. I*SSN*, 2349-5162. Available from: http://www.jetir.org/papers/JETIR1912145.pdf

SVANTESSON, D. and Clarke, R. Privacy and consumer risks in cloud computing. *Computer law & security review*, 2010. Vol. *26*(4), pp.391-397.

TADAPANENI, N. R. Different Types of Cloud Service Models. 2017.

TANG, Y. Lee, P.P. Lui, J.C. and Perlman, R. Secure overlay cloud storage with access control and assured deletion. *IEEE Transactions on dependable and secure computing*, 2012. Vol. 9 (6), pp.903-916.

Top threats to cloud computing: Cloud security alliance. [Online]. cloudsecurityalliance.org. [Accessed 19 April 2023]. Availbale from: https://cloudsecurityalliance.org/research/top-threats/

TENEYUCA, D. Internet cloud security: The illusion of inclusion. *Information Security Technical Report*. 2011. Vol. *16*(3-4), pp.102-107. [Accessed 27 December 2022]. Availbale from: https://doi.org/10.1016/j.istr.2011.08.005

VAQUERO, L.M. Rodero-Merino, L. Caceres, J. and Lindner. A break in the clouds: towards a cloud definition. *ACM sigcomm computer communication review*. 2008. Vol. *39*(1), pp.50-55.

VELTE, A.T. Velte, T.J. Elsenpeter, R.C. and Elsenpeter, R.C. Cloud computing: a practical approach. *McGraw-Hill Osborne Media, 2010.*

WANG, H. Integrity verification of cloud-hosted data analytics computations. 2012. p. 1-4. DOI 10.1145/2347673.2347678. ISBN 978-1-4503-1596-8

WALLIMAN, N. & Baiche, B. Your research project a step-by-step guide for the first-time researcher, SAGE Publications, London. Thousand Oaks. New Delhi, 2001.

WATSON, S.C. A primer in survey research. *The Journal of Continuing Higher Education*,1988. Vol. *46*(1), pp.31-40.

WEINS, K. Cloud computing trends: 2016 state of the cloud survey. *Right Scale*. [online]. 2016. [Accessed 8 December 2022]. Available from: https://go2.digitalrealty.com/rs/087-YZJ-646/images/Report_RightScale_2016_State_of_the_Cloud.pdf

WHITE, S.R. Hanson, J.E. Whalley, I. Chess, D.M. and Kephart, J.O. An architectural approach to autonomic computing. In *International Conference on Autonomic Computing, 2004. Proceedings.* IEEE, 2004. p. *2-9.*

WIDYASTUTI, D. and Irwansyah, I. 2018. Benefits and challenges of cloud computing technology adoption in small and medium enterprises (SMEs). *Bandung Creative Movement (BCM)*, *4*(1). 2018.

WINKLER, V. J. Securing the Cloud: Cloud computer Security techniques and tactics. Elsevier. 2011.

YU, S. Wang, C. Ren, K. and Lou, W. 2010, March. Achieving secure, scalable, and fine-grained data access control in cloud computing. In *2010 Proceedings IEEE INFOCOM.* Ieee, *2010.* p. 1-9.

ZHAO, W. Peng, Y. Xie, F. and Dai, Z. Modeling and simulation of cloud computing: A review. In *2012 IEEE Asia Pacific cloud computing congress (APCloudCC).* IEEE, 2012. p. 20-24.

ZHU, J. Cloud computing technologies and applications. *Handbook of cloud computing*, 2010. p.21-45.

ZISSIS, D. and Lekkas, D. 2012. Addressing cloud computing security issues. *Future Generation computer systems*, 2012. In Press: Corrected Proof. Vol. *28*(3), pp.583-592.

9. Appendix

Survey Questinnaire

(For this survey, N=100)

Cloud Computing

Dear Participant,

Thank you for assisting us with our research on the benefits, usage, adoption, security, and challenges of cloud computing. The only motivation for performing this research is to fulfill academic requirements. The confidentiality of the information you've provided is guaranteed. Please respond to the questions below if you want to share your ideas with the researcher.

Thank you very much.

1. What are the benefits and applications of the cloud in daily life and work?

a) Strong network connectivity
b) versatile and scalable architecture
c) Efficient resource allocation
d) Strict restrictions and security measures
e) Effortless compatibility and integration

2. Do you have any knowledge of cloud computing?

a) Yes
b) No

3. Have you used cloud computing within your company?

a) Yes
b) No

4. What are your company's critical benefits for embracing cloud computing?

a) Improved IT infrastructure scalability and flexibility
b) Cost-saving pay-as-you-go pricing strategies
c) Improved remote access and collaboration capabilities
d) Simplified business continuity planning and disaster recovery

5. What challenges did you encounter when setting up and managing cloud services?

a) Data privacy and security issues
b) Integration with currently installed on-site systems
c) Adherence to applicable industry regulations
d) Lack of data mobility and vendor lock-in

6. How essential was security in your company's decision to use cloud computing?

a) Extremely important
b) Important
c) Somewhat important
d) Not important

7. Have any security breaches or incidents occurred while using cloud services?

a) Yes
b) No

8. How confident are you in the security measures your cloud service providers have implemented?

a) Very confident
b) Somewhat confident
c) Not confident
d) Unsure

9. What confidential information or data does your company save in the cloud?

a) Personally identifiable information (PII)
b) Intellectual property
c) Financial data
d) Health records
e) Other (specify)

10. How much do you concern about cloud-based data privacy for your company?

a) Very concerned
b) Somewhat concerned
c) Not concerned
d) Unsure

11. What security measures does your company use to protect its data when utilizing cloud services?

a) Data encryption both in transit and at rest
b) Multiple-factor identification
c) Management of access restrictions and permissions
d) Regular security evaluations and audits
e) Other (specify)

12. Do you think the cloud effectively protects your company's data?

a) Yes
b) No
c) Unsure

13. How well do you recognize the cloud security shared responsibility model?

a) Very well
b) Somewhat well
c) Not well
d) Unsure

14. Have you encountered compliance or regulatory challenges when using cloud services?

a) Yes
b) No

15. Do your organization's security policies align with cloud computing practices?

a) Yes
b) No
c) Partially

16. How frequently does your company update and maintain its cloud infrastructure?

a) Regularly
b) Occasionally
c) Rarely
d) Unsure

17. How important is encryption for your organization's cloud-based data?

a) Very important
b) Important

c) Somewhat important
d) Not important

18. Have you ever experienced poor cloud service performance?

a) Yes
b) No

19. What are the most important factors to consider regarding security when choosing a cloud service provider?

a) Strict data protection and privacy regulations
b) Adherence to regulations and certifications of compliance
c) Regular audits and open security procedures
d) Disaster recovery and incident response skills
e) Other (specify)

20. Do you know of any security or data breach instances involving cloud service providers that might affect your business?

a) Yes
b) No

21. How confident are you that your cloud provider can recover from a disaster?

a) Very confident
b) Somewhat confident
c) Not confident
d) Unsure

22. What measures does your organization take to ensure data sovereignty when using cloud services?

a) Selecting cloud service providers with data centers in particular countries
b) Implementing service-level agreements (SLAs) with data residency requirements
c) Other (specify)

23. How do you evaluate a cloud service provider's dependability and credibility?

a) Examining their security audits and certifications
b) Examining client testimonies and references
c) Evaluating their financial stability and standing in the industry
d) Other (specify)

24. Is your organization concerned about vendor lock-in when using cloud services?

a) Yes
b) No

25. How does your company handle cloud-based identity and access management?

a) Implementing centralized permission and authentication systems
b) Implementing single sign-on (SSO) tools
c) Using RBAC (role-based access controls)
d) Other (specify)

26. Are you aware of any cloud data portability challenges that may impact your organization?

a) Yes
b) No

27. How important is the transparency of cloud provider security procedures for your company?

a) Very important
b) Important
c) Somewhat important
d) Not important

28. Do you understand serverless computing and how it affects security?

a) Yes
b) No

29. Have you encountered any problems with the multi-tenancy of cloud computing that can affect your company?

a) Yes
b) No

30. What security accreditations or requirements do you expect from your cloud provider?

a) ISO 27001
b) SOC 2
c) PCI DSS
d) HIPAA
e) Other (specify)

31. How frequently does your company evaluate or audit the security of its cloud infrastructure?

a) Regularly
b) Occasionally
c) Rarely
d) Never

32. Are you concerned about the physical security of the cloud data centers where your company's data is kept?

a) Yes
b) No

33. Do you utilize your company's third-party security products or services to improve cloud security?

a) Yes
b) No

34. How essential are continuous monitoring and warning systems for cloud security?

a) Very important
b) Important
c) Somewhat important
d) Not important

35. Have any challenges getting cloud services to work with your current security infrastructure?

a) Yes
b) No

36. Do you know of any challenges with cloud data loss prevention?

a) Yes
b) No

37. How does your company manage cloud data backup and recovery?

a) Regular backups to an alternative cloud service provider
b) Using the backup and recovery services offered by the cloud provider
c) Other (specify)

38. Do you concern that insider attacks could exist in cloud environments?

a) Yes
b) No

39. Do you think the cloud can offer more security than conventional on-premises solutions?

a) Yes
b) No
c) Unsure

40. What principal challenges do you encounter while implementing cloud-based security solutions?

a) Budgetary and material constraints
b) A lack of internal knowledge
c) Regulatory and compliance issues
d) Other (specify)

41. What benefits do you expect that can be the primary drivers for cloud adoption?

a) Reduce spending on technology infrastructure
b) Better scalability and elasticity
c) Lower maintenance costs
d) Built-in fail safe and redundancy
e) Other (specify)

42. Do you understand zero-trust security and how it relates to cloud computing?

a) Yes
b) No

43. How does your business ensure that its use of cloud services complies with data protection laws?

a) Reviewing audit reports and compliance certifications from cloud providers
b) Applying access controls and data encryption
c) Other (specify)

44. Do you have challenges with the elasticity and scalability of cloud resources?

a) Yes
b) No

45. Do cloud storage and file-sharing services make you concerned about the possibility of data leakage?

a) Yes
b) No

46. Do you think cloud service providers are honest about handling security?

a) Yes
b) No
c) Unsure

47. How does your company manage cloud forensics and incident response?

a) Creating a plan for handling incidents in cloud settings
b) Hiring emergency response services from other sources
c) Other (specify)

48. Do you know of any challenges with geographical limitations and data sovereignty in the cloud?

a) Yes
b) No

49. How does your company handle cloud security training and employee awareness?

a) Holding routine training sessions on best practices for cloud security
b) Offering instructional tools and resources
c) Other (specify)

50. What changes do you expect to see in cloud computing security over the next few years?

a) The growing use of cutting-edge security technologies like artificial intelligence and machine learning
b) Stricter Laws and compliance standards for cloud service providers
c) A stronger focus on data protection and privacy
d) Other (specify)