MANAGING CYBER THREATS AND VULNERABILITIES OF DATA ON CLOUD: BEST PRACTICES AND MITIGATION STRATEGIES

Asma Hafeez

Enrollment No: 01-246182-002

Supervisor: Dr Zahoor Sarwar

A thesis submitted to the Department of Software Engineering, Faculty of Engineering Sciences, Bahria University, Islamabad in the partial fulfillment for the requirements of a Master degree in Engineering Management

April 2021

Approval Sheet

Thesis Completion Certificate

Scholar's Name: **Asma Hafeez** Registration No: **01-246182-002**
Programme of Study: MS Engineering Management
Thesis Title: Managing Cyber Threats and Vulnerabilities of Data on Cloud: Best Practices and Mitigation Strategies

It is to certify that the above student's thesis has been completed to my satisfaction and, to my belief, its standard is appropriate for submission for Evaluation. I have also conducted plagiarism test of this thesis using HEC prescribed software and found similarity index at 12% that is within the permissible limit set by the HEC for the MS/MPhil degree thesis. I have also found the thesis in a format recognized by the BU for the MS/MPhil thesis.

Principal Supervisor's Signature: ___________________________

Date: 7 April, 2021 Name: Dr. Zahoor Sarwar

Certificate of Originality

This is to certify that the intellectual contents of the thesis *Managing Cyber Threats and Vulnerabilities of Data on Cloud: Best Practices and Mitigation Strategies* are the product of my own research work except, as cited property and accurately in the acknowledgements and references, the material taken from such sources as research journals, books, internet, etc. solely to support, elaborate, compare and extend the earlier work. Further, this work has not been submitted by me previously for any degree, nor it shall be submitted by me in the future for obtaining any degree from this University, or any other university or institution. The incorrectness of this information, if proved at any stage, shall authorities the University to cancel my degree.

Signature: ______________________ Date: 7 April, 2021

Name of the Research Student: Asma Hafeez

ABSTRACT

Cloud computing is coming forth as one of the most efficient, adaptable and fastest internet technologies in the industry. The focus of this paper is to bring to light the best strategies to manage the security threats associated with data on Cloud Computing. Qualitative research methodology was applied to get a better insight into the purpose and its complications. Qualitative research method of "Interviews" was applied on the paper by conducting several semi-structured interviews with Small and Medium Enterprises (SMEs) to retrieve requested Data. Several recommendations were presented for successful implementation of Cloud Computing along with mitigation strategies of security threats. Research was limited to organizations operating in Islamabad. Due to ongoing pandemic majority interviews were taken on calls which may result in an interviewee being biased and interpreting the questions according to their own understanding. With this research, Businesses and enterprises can use the findings to secure their online presence relating to Cloud Computing to ward off potential security threats and planned cyber-attacks

DEDICATION

I dedicate this thesis to my parents & teacher with lots of love and gratitude.

You all are the supreme factor contributing to my academic accomplishments.

Acknowledgments

In the name of Allah, the Most Gracious and the Most Merciful.

From the deepest of my heart, I would like to thank Almighty ALLAH for the unconditional love He has shown me throughout my life and strength He has provided me to cope with any challenges that came across in my life.

I would like to thank and appreciate the effort of my supervisor Dr. Zahoor Sarwar who has shown his devotional commitment towards the accomplishment of this dissertation. His professional guidance, overwhelming attitude and irresistible support has made this dissertation a possibility within limited span of time allowed.

I would also like to thank my family, as I am very grateful for their love and support through every thick and thin phase of my life. My family has been the prime reason behind the success and achievements that I have in my master's degree. I owe a great debt of gratitude to my parents for their continuous support and for being my motivation throughout my life. I would like to appreciate the supporting effort of my graduate friends who has helped me a lot throughout my graduate degree.

- Asma Hafeez

Table of Contents

Abbreviations

SaaS	Software as a Service
IaaS	Infrastructure as a Service
PaaS	Platform as a Service
ERP	Enterprise Resource Planning
CRM	Customer Relationship Management
AWS	Amazon Web Service

CHAPTER 1: Introduction

1.1 Introduction

To define Cloud Computing in the simplest of terms, it means storing and accessing data over the internet as compared to a computer's hard drive.

Cloud computing has its perks for its ever-growing popularity among Small and Medium Business (SMB) Enterprises as well as gigantic organizations which includes convenient data sharing, quick data distribution and enhanced IT services. It is in process of replacement of hardware as it helps to share resources like applications or data over the internet. In contrast to that, cloud computing comes with the benefit of not having to pay any upfront costs. Moreover, there is no need to own an elaborate IT infrastructure but instead, pay for the service as and when they use it. This not only saves physical warehouse space and rent, but it also reduces maintenance costs, rent expenses and security expenses. This, in turn, paves the way for the cloud computing services providers to benefit from economies of scale, considering that they can render their services to a wide customer base.

The most popular definition of cloud computing is provided by The National Institute of Standards and Technology (NIST), which defines "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models" [1] [2].

There are three service models, namely, Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). They are also known as SPI models. On the other hand, Private cloud, Public cloud, Hybrid cloud and Community cloud are the four deployment models. The five essential characteristics of cloud computing are on-demand self-service, broad network access, resource pooling, rapid elasticity and lastly measured service. [1]

The most prominent names in the market with regards to cloud computing service providers are: Amazon, DropBox, Microsoft Azure, Google Cloud, IBM Cloud, & Apple iCloud. All the above-mentioned service providers allow the users to store as well as access data regardless of the geographical differences via the Internet with or without certain fee. Cloud computing provides customizable and efficient services to access and use applications according to customer's requirements, allowing the customers to freely customize their data and its storage. It also helps to provide a platform to its customers to design infrastructure or applications based on their requirements. The cloud environments ensure the impact of shared assets for its end clients. Cloud providers uses multitenancy to emerge the idea of sharing. Cloud suppliers ideally keep up organization framework, storages, and application software's that advance dependability, execution, and convenience. A particularly sharing of assets could settle data security, integrity, and privacy. [30]

Along with the benefits cloud has to offer, its side threats are posed as well. Biggest threats and vulnerabilities being faced by cloud users include ever-growing requirement of configuration options and their complexity, lack of continuous scanning due to the ease with which applications can be introduced in an environment as it may leave behind older versions of server being accessible alongside the latest version. Threats also include issues such as interconnectivity of cloud and its functions, although a beneficial aspect of cloud but an easy threat due to the hacker having easy access to all functions at once, lack of obedience to policies by the employees and cloud users, high usage of default code templates to develop infrastructure. Furthermore, excess privilege being provided in cloud due to lack of acceptance by many, causing a smaller number of people having high privileges to multiple interconnected modules of cloud, data loss with no chances of recoverability and system vulnerability occurring due to exploitable bugs in programs which may allow hackers to infiltrate and access sensitive information or even crash the service operations.

On the other hand, numerous security specialists are dealing with finding better security solutions. Despite the fact that security is improving step by step yet at the same time security managers are discovering multiple approaches by hackers to exploit cloud environments [31]. Therefore, it is imperative to design a strategy that protects your data stored in a cloud environment from security breaches. Basic elements to be included in the strategy should be to authenticate all users who have access to cloud, apply roles or menus to each user in order to limit their access, authenticate all software and its changes, formalize the process of any user requiring access beyond their roles/menus provided to them, monitoring all logs and activity, encrypt all valuable data and regular checkups for any vulnerabilities.

1.2 Motivation for Study

Cloud computing is gaining name as a practical safety measure for online data storage in various industries. Its processes and substructure are designed to tackle online security liabilities and threats bearing minimum cost. The focus in this research will be figuring out security liabilities in a cloud environment along with possible measures to counter them using qualitative analysis.

The reason behind choosing cloud computing services as a study topic is its rising popularity because of its amiable and cost-efficient nature. Almost all businesses and industries look for innovative means to boost their profits without spending much therefore cloud computing is a viable finding to their search. [2] Microsoft Azure, AWS and Salesforce are few of the cloud computing services that know how to cater to the demands of different enterprises using their various resources. Clients mostly interrogate about the level of security a cloud service can offer before availing their services. Cloud service providers (CSP) find it difficult to promote their services to users as they are extremely cautious in selecting a cloud service to protect their data and are not ready to settle for less. [3] Therefore, it is important to evaluate the safety threats and weaknesses in a cloud computing network.

1.3 Problem Statement

Many issues are surfacing using cloud computing, highlighting the security breach and theft cases of data. Moving organization's critical applications and resources full of sensitive and private information to cloud with no control and management of their own data is the major concern of many organizations.

1.4 Research Questions

The research questions addressed through this research work are:

RQ$_1$: What policies do CSPs need to nullify security threats related to online data storage?

RQ$_2$: What are the likely approaches to tackle the trials of cloud security?

RQ$_3$: What are the most efficient strategies to manage cloud computing security risks?

RQ$_4$: How does an enterprise handle weakness in their cloud infrastructure?

RQ$_5$: What are the strategies or procedures that can improve security offered by cloud computing?

1.5 Aims and Objectives

1.5.1 Aim

The purpose of the study is to find security vulnerabilities of applications in cloud computing identified by CSP's implementation of five cloud computing characteristics discussed in literature review. It also highlights security threats and challenges for adopting cloud computing.

1.5.2 Objectives

- To analyze policies CSPs need to nullify security threats related to online data storage.
- Identifying approaches to tackle the trials of cloud security.
- To identify most efficient strategies to manage cloud computing security risks.
- To collect guidelines enterprises, apply to handle weaknesses in their cloud infrastructure.
- To identify strategies or procedures that can improve security offered by cloud computing.

1.6 Significance of Study

IT sector plays an important role in technological development of a developing country. This study recommends how various Businesses and enterprises can use the findings to secure their online presence relating to Cloud Computing to ward off potential security threats and planned cyber-attacks. This study proves significant in helping firms operating in Cloud Computing to understand their current position and make correct decisions based on the recommendations. Through this study, stakeholders of Cloud Computing sector have the ability of understanding that which key areas were significant in impacting and can pose as a potential loophole for hackers to exploit. Through this study, suggestions have been made by people actually working with the Cloud Computing environment. Meanwhile, this study provides a direction for the managements of Cloud Computing firms towards making their company secure and safe for online presence when interacting with Cloud Computing. Furthermore, this study provides a foundation based on which research students can enhance their knowledge and perform further research in future to have detailed investigation of potential flaws, loopholes and threats mentioned by respective Interviewees. Finally, this study proves significant for IT students in improving their knowledge and understanding about the literature topic.

1.7 Outlines of the study

The research process is conducted in an organized and systematic manner. Table 1.1 illustrates the study format, which is presented and documented in five chapters.

Table 0.1 Structure of the study

Chapter	Description
Chapter One	This chapter discusses complete overview of the thesis. It provides the overview of the topic, motivation for the study and problem statement followed by the research questions and the aims and objectives.
Chapter Two	In this chapter, background of cloud computing is discussed. It also contains information about five characteristics of cloud model, cloud service models, deployment models and related work and threats and recommendations.
Chapter Three	Chapter Three provides an overview of the research methodology, design and approach adopted for this study.
Chapter Four	This chapter presents the analysis of the data collected. It provides analysis of interviews and its results.
Chapter Five	The last chapter includes recommendations, conclusion and future work.

CHAPTER 2: Literature Review

2.1 Background and History of Cloud Computing

Cloud computing is an ever-evolving internet technology that originated first in 1960s on mainframe systems. The network diagrams used to explain the concept envisioned internet as clouds hence the technology was named cloud computing. [4]. Technologies like Grid computing, Virtualization and Clustering etc. are at the center of cloud computing networks which not only facilitate low service rates but also take care of maintenance cost of their core informational centers. [4]

The advent of cloud computing wouldn't have been possible, without the development of Advance Research Projects Agency Network (ARPANET). It helped to improve interconnection of systems which was needed to connect multiple computers for sharing resources and gradually it led to the invention of Internet. Continuous research in the field of data storage made room for expanded services of Grid Computing, Cloud Computing and Application Service Provision (ASP) [5]. Cloud service networks have switched from interconnected servers to shared resources that provide convenient accessibility regardless of the user's location.

The big pioneers today in cloud computing entered the market in various years. In 1999, Salesforce.com initiated the provision of applications to users by the usage of a website. The applications were sold and distributed to the organizations using the Internet, and this way cloud computing was initiated by salesforce. Whereas in 2002, Amazon entered the market with Amazon Web Services, providing simple services such as storage and human intelligence. However, Elastic Computer Cloud was launched in 2006 which was open for commercial use by the general public. By 2007 binge watching series and movies became a trend when Netflix launched its video streaming website. IBM joined the competition with SmartCloud meanwhile Apple launched the popular "iCloud". Around the same time, Oracle released its own Cloud. Coming to 2008, Google entered the market using Google Apps which were used to provide cloud computing enterprise apps. In 2010, Microsoft entered the market with the launch of Windows Azure, with many other competitors behind the lines.

Users must trust their cloud computing providers in SaaS model to ensure the protection of their data from prying eyes. The dependency on someone else makes clients insecure about the safety of their data and operation of computing application as they are unaware of the security measures enforced by the providers. [11] SaaS allows customers to replace the outdated version of their application with new version. Therefore, secure data migration is prioritized to preserve the credibility of the cloud computing application. The SaaS software provider prefers hosting application on its private server though third-party involvement via infra-structure services is also a popular alternative. [12] One way to minimize new ventures in infrastructure facilities and entertaining better services is pairing cloud computing with pay-as-you-grow method. No industry, business and enterprises can accumulate profits without IT services and internet connection in today's world of technology. Data sharing and processing in guise of transactions and record keeping using pricing info is treated as a strategic move that is protected as per compliance policies. Though, service providers of SaaS protect data from different clients by storing them in their data center. Things differ when your SaaS service provider is using a public cloud computing service where confidential and insignificant data is treated as same. Cloud computing service providers facilitate easy data availability by making it accessible via different locations. On-premise model is more acceptable among enterprises as their stays within the confines of their network and adhere to their policies. Therefore, SaaS is viewed as a security liability by enterprises as they are unaware of the provider's privacy policy related to their data. They worry over possible loopholes in their security network and application designs to steer clear of fiscal and legal accountabilities.

2.2 Cloud Computing – Official Definition

National Institute of Standards and Technology (NIST) defines cloud computing as "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [1].

The above definition explains that cloud computing is highly scalable that helps organizations to minimize expenses spent on dealing with resource management and lessens the strain on users that handle cloud computing networks. The huge advantage to users or organizations using cloud computing is that it saves time and cost which can be used in carrying out other strategies and tasks. The definition provided by NIST is meant for comparison at a broad level with regards to cloud and its services and the strategies for deployment, and also to provide a simple baseline of what exactly is cloud computing and the best usage of cloud computing to reap maximum benefits it has to offer.

Organizations using and preaching this definition provided by NIST have a tool in their hands to determine the extent to which they must implement the technology in order to meet the minimum requirements and characteristics of cloud. It is important to know because the adoption of cloud with proper measures will allow the organizations to reap fruits cloud has to offer which includes savings of expenses, energy, and empowerment of customer. Also, the usage of the definition and implementation of its true meaning will also assist in evaluation of security properties.

2.3 Five Characteristics of Cloud Model

Following are the five indispensable characteristics that are part of NIST's cloud model:

- ***On-demand self-service:***

  Cloud service providers can assist you in cloud computing without needing you to interact with them personally. This means, clients can provision extra computing services (virtual machine and database assistance etc.) for themselves without interacting with the service providers. It eliminates the need for human intervention or human administrators at all levels which in turn allows the users to utilize the cloud services at the infrastructure, platform, or application level without any issue. It means the users can be self-sufficient to provide, monitor, and manage computing resources as per their needs. It may include web self-service portals in the shape of a user-friendly interface in order to access the organization's accounts to monitor their cloud services, the usage of cloud, as well as to provide and de-provide services as per the requirements of the organization.

- ***Broad network access:***

  Cloud service providers establish their computing resources over a network that can be accessed via diverse platforms. These networks are mostly spread over high broadband communication links such as worldwide web or the local LAN networks for exclusive cloud portals. Cloud services pay attention to the networks they've established for their clients especially on their latency and bandwidth to maintain their quality of service.

This is the most important factor for all the organizations which require time sensitive applications and data for their success. Cloud service has the capability to provide its services over network and is accessible through typical mechanisms that promote the use of multiple internet-dependable devices like smartphones and laptops.

This has enabled the organizations and its employees to have access to all the data from anywhere they are geographically which in turn has eliminated the simple yet longing requirement of the employee being present physically where the hardware is accessible in order to work. This has in turn proved yet again that cloud computing is assisting organizations indirectly in increasing their profitability.

- ***Multi-tenancy and resource pooling:***

  The IT resources, such as: networks, servers, storage, applications, and services are communal across several applications and inhabitant in an indifferent manner. Numerous organizations are given cloud services from the same physical source.

  Cloud service providers can use a single infrastructure and application to share their computing resources because of their multi-tenant model. Many may view multi-tenancy as a security liability, but the model has so far safeguarded their users' personal data. To explain multi-tenancy further, consider an example of a high earning company where employees share a building, but they all have their own workspace and privacy within that infrastructure.

  On the other hand, resource pooling is when several organizations are provided services from the same existing physical resources. For this to occur smoothly and successfully, the service providers' resource pool is required to be extremely large as well as flexible sufficiently to provide services to multiple clientele and their necessities and also to ensure economies of scale. As it arrives to resource pooling, resource allocation should definitely not affect performances of the core applications of the client's organizations.

- ***Rapid elasticity and scalability:***

  Cloud computing service providers can easily provision resources for their customers whenever and however they need them. Their systems succumb to business demands intentionally and sometimes automatically hence they provision or de-provision their computing resources. Note that the provisioned resources are neither limited nor bound to any time restrains.

The greatest benefit cloud computing has to offer is its ability to provide extremely quick resources as soon as the demand or need arises (depending on network and bandwidth limitations of the clients). As quick as it is to access the resources, on the other hand their removal is also quick once the resources are no longer needed or they need to be eliminated from the cloud. The resources of cloud computing are able to rapidly scale up and down and even automatically (depending on the circumstances) in line with the demands of the client's business needs, hence being the most vital feature of cloud computing in this era. The usage of cloud, its capacity as well as its expenses can be measured high or low without any further contracts or possible penalties.

In other words, elasticity in cloud computing is defined as organizations being able to perform provision and de-provision of resources of cloud computing at a very high speed. This is in relation to providing or de-providing to the storage or virtual machines or the applications being used by the clients.

When speaking with regards to scalability in cloud computing, the Capex is reduced thoroughly for the client of cloud services, reason being if just in case the client needs further storage or more services in accordance to its business needs, the cloud service providers can easily provide the client with their required demands within a few days' time without any hassle. Scalability's features are that it is planned, and it grows gradually. This means that the organizations are steadily planning for further capacity and the cloud being able to meet the requirements within a timely manner.

Just-in-time (JIT) service is a perfect example for some organizations which require the elasticity and flexibility which cloud can offer in order to scale up or scale down the resources in the cloud. A simple example can be taken of a client with an immediate requirement for increasing services of the cloud to meet the requirements of a newly opened service which deals with on-spot customers, this would conclude as the cloud elasticity. Whereas, if a client requires asset tagging functionality in its system for a new project, it was planned slowly and gradually, hence it is referring more towards scalability.

Another benefit which is provided by cloud's quick elasticity and scalability is the testing of applications. For instance, if an organization needs certain modules of its applications to be tested at developer stage before it is rolled out to live production stage, it can be performed, checked and have it running within a very short timeline as compared to dealing with hardware.

To conclude the rapid elasticity and scalability feature of the cloud, when and if the organizations require for something to be tested, for cloud services to instantly increase or decrease, it can happen in an instant. Also, it saves a lot of expense in terms of paying only for the services the organizations require, as well the capital expenditures being eliminated which come along with hardware and its maintenance.

- ***Measured service:***

  Cloud service providers can monitor the usage of their resources according to their diverse services. Hence, all types of resources (virtual or cloud based) are monitored and controlled for their usage. [1]

  In order to further discuss this feature, whenever the cloud resources are utilized, it is tracked for each and every application as well as its occupancy. This produces helpful results for the users as well as the cloud service providers to keep a track with regards to what services have been used and which services weren’t. This feature is used for multiple purposes such as keeping logs, producing final billing without any disagreements between the user and service provider and lastly, effective use of the cloud resources.

  This feature has enabled cloud services to be extremely economical as the billing is generated as per the charges on a per-use basis (in most cases) as services are being monitored and measured on the basis of how much the client has used the cloud services. Just like you would think of electricity bills, cloud computing usage is also metered, and organizations simply pay for what they have used. This in turn enables optimization of the usage of cloud resources by tracking its usage in a consistent manner. This means, that the usage of cloud resources is constantly being measured, monitored and reported by the service provider to the client which increases transparency. The “Pay for what you use” model is highly being preferred and utilized by the organizations which prefer cloud computing and its services.

2.4 Cloud Service Models

There are the following three types of cloud service models:

- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Software as a Service (SaaS)

2.4.1 Infrastructure as a Service (IaaS)

When cloud service providers allow clients to run applications and operating systems on their underlying infrastructure via resources like storage, networks and processing then the service is called IaaS. The system has hypervisors and virtualized resource layers that run on virtualization technology.

IaaS, famously acknowledged as Hardware as a Service (HaaS), is a computing infrastructure managed through the internet. The chief benefit of utilizing IaaS is that it helps the cloud computing users to evade the expenses and complications of acquiring and handling the physical servers. It permits the clients to safely outsource their entire information technology infrastructures including servers, networks, storage and various other types of resources. For the clients, this is available to them using the infamous "pay as per usage model" as compared to the older ways of service hosting where the information technology infrastructures used to be rented out in order to outsource them successfully. The traditional way had a big disadvantage for customers having to pay a fixed amount regardless of the actual usage. But now, due to the IaaS, clients can not only customize their configurations as per their needs, but also will no longer be charged for services not being utilized by them. With the introduction of IaaS, the need to maintain a whole IT infrastructure has been eliminated, saving time, space and money.

There are three models in which IaaS is offered to the clients: **public, private**, and **hybrid** cloud. When it comes the private cloud, the infrastructure is setup at the customer's provided location. On the other hand, public cloud is setup at the vendor's location. Lastly, the hybrid cloud includes the infrastructure to be available in both locations.

Best examples: Amazon Web Services and Microsoft Azure.

2.4.2 Platform as a Service (PaaS)

While using PaaS, consumers don't have to install any tool or application in their devices to deploy their application on a cloud infrastructure. Clients have no control over the middle layer of SPI system, yet they can use the servers (LAMP) provided by cloud service providers for the deployment of their applications. In other words, PaaS is utilized by the programmers to develop, test, run, and manage their applications as per their need.

Platform as a Service (PaaS) delivers an environment for runtime which in turn enables the programmers to not only develop applications but deploy them as well after sufficient testing, with ease. Just like IaaS, this is available to programmers using the infamous “pay as per usage model” and having ease of access by simply accessing the internet. Another feature in PaaS is in accordance to Iaas, which is, flexible scalability where programmers’ demand the scaling up and down as per their requirements without having to worry or make expenses for upgrades of the hardware. PaaS has a massive support available for web applications which includes servers, storage, development tools for programmers, management system for database etc.

Best examples: Google App Engine, Force and Azure.

2.4.3 Software as a Service (SaaS)

When a third-party cloud service provider allows their consumers to use applications (emails, software etc.) available on their cloud infrastructure via web browsers then the service is called SaaS (Software as a Service). Clients can access these applications through different devices despite being exposed to several potential threats. In other words, it is a software to host the applications in cloud, creating ease of access for users to access the applications by simply having a stable internet and a browser, which in turn means that no installation of the application is needed in the hardware being used by the users. SaaS is popularly called an "**On-Demand Software**" as well.

Big range of Services offered by SaaS Providers

- If a user is seeking to start a brand-new business, SaaS is able to provide services which are core for any business including Enterprise Resource Planning (ERP) system, Customer Relationship Management (CRM) system, system to maintain sales and record expenses.
- SaaS may also provide applications for management of documents in order to easily create, maintain and change the documents created by the users.

- A platform to maintain social media in order to handle and gather publicly available data.
- Mailing services.

Characteristics of SaaS

The following are the key characteristics of SaaS -

- SaaS is centrally managed from one location
- SaaS is hosted through a server which is remote
- Easily available through internet connection
- Automatic updates; hence removing any hassle with regards to hardware and its management
- Just like Iaas & Paas, it uses the infamous "pay as per usage model".

Best Examples: Google Apps, Dropbox and Slack.

Advantages and Benefits

The following are the key benefits of SaaS

- It is available to users at a very low cost, mainly because users may purchase the services through subscription which is charged either month wise or for the entire year as compared to the traditional ways of purchasing software which were based on licenses which huge initial costs and service level agreements expenses.
- One of the services offered by SaaS include a feature for many numbers of users to use one application.
- Since SaaS is based on remote server, the clients are not required to make heavy expenditures for hardware.
- Speaking about traditional methods of accessing software, they require proper hardware, installations, expense for maintenance and overall set-up costs. When it comes to SaaS and its feature of being remotely available, all above activities are no longer needed. The only expenses due to SaaS are the billing sent by vendors using the model "pay as per the usage"
- In order to remain competitive in the market, it is important for most businesses to have the latest hardware and updated version of software which costs the

organizations each time there is new update in the market as it requires IT support team and their salaries. SaaS eliminates this need as maintenance is the responsibility of SaaS provider.

- It is easy for clients to access the services provided by SaaS on multiple platforms such as PCs, laptops, phones etc.
- Integration of SaaS with most popular software is easy due to its usage of standard APIs.

Disadvantages

The following are the disadvantages of SaaS

- It is considered safe when all is being managed in-house, however cloud today is as secure as in-house management. However, there is still a risk being posed to all the data stored by client on SaaS provider’s cloud.
- The performance of the data and applications and their response may be affected due to multiple reasons such as high latency, slow or unstable internet connection, issues from the SaaS provider’s side which can cause delays while using the application through cloud as compared to application being deployed locally. Hence SaaS may require lots to be in check if the business requirement is for applications to respond within milliseconds.
- SaaS becomes unavailable almost completely if there is any instability in internet.
- Just like IaaS and PaaS, SaaS also faces immense difficulty with vendor switching due to client’s large amounts of data and application residing with the vendor within one type of SaaS and its transfer, conversion and exporting would become very hectic.

2.5 Vulnerabilities and Threats in SaaS Cloud Service Model:

Vulnerabilities and threats are two different terms but are often used interchangeably in research papers and articles for readers’ convenience. A threat is a planned attack on private information and capitals related to either commercial or personal interests with the purpose of exploiting the stolen data. Vulnerability in a computing system is a form of leak in your house’s plumbing system that damages your house’s infrastructure from within. An attacker can easily hack into your cloud computing system and misuse your data if there is a leak in its defense. [14]

Following are some of the threats and vulnerabilities commonly reported in SaaS Cloud Service Model.

Examples of Threats, Vulnerabilities & Risks

APIs is a gateway to SaaS cloud services therefore they should be free of all vulnerabilities and weaknesses. Lack of data validation, authorization check and weak passwords are some possible security hazards related to API. Any weakness in your SaaS cloud service's interface or API can jeopardize your personal and professional interests.

You can never purge your data stored online once it reaches the World Wide Web therefore choose your cloud computing service wisely. Moreover, there is no guarantee that the service providers that are backing your data will not use it for other purposes. They also don't take responsibility of data available on their network since they don't have any means to track its location. Lack of encryption and decryption in your SaaS cloud system for data dispensation, storage, and allocation puts your assets in jeopardy. [28]

Virtual machines are also part of cloud computing system and pose several security risks if left unchecked for vulnerabilities. They may open hidden networks in the system that allows an attacker to intervene in the system's infrastructure. Lack of management in transfer of resources as well as uncontrolled relocation of virtual machines hinders secure cloud data storage. If we judge by the past incidents, then VMs and hypervisor are the most vulnerable part of any cloud computing system. [27]

The most common threat faced by SaaS cloud computing service is hijacking which becomes easy when you have a weak password. Hijackers leak confidential information, modify transaction and interfere in your data inputs either for their personal gain or for their client. Data scavenging is another threat that puts your data at risk if you don't deal with your old devices carefully. These scavengers can retrieve deleted data from your old devices if you fail to use the right method to purge it from their memory completely.

Servers are important to manage traffic and requests for resources in a SaaS cloud system. Any person with ill intentions can impersonate authorized personnel or an individual to enter protected channels and steal data. There are also techniques like SQL that helps malicious users to manipulate data available on cloud servers.

Some also use virtual machines to enter computing servers and cloud storage infrastructure to exploit private information. VM migration is a risky operation that allows attackers to access confidential data illegally as well as relocate servers from one system to another.

SaaS cloud computing system is always at the risk of being infiltrated by hijackers, spammers, and criminal code authors that take advantage of the anonymity offered by the system. They also allow customers and IT services to operate under a solitary administrative domain therefore criminals find it easy to be the mole in these systems.

A cloud service is an amalgam of various technologies and servers therefore it has components that are questionable for a vast majority online. Since most public clouds offer reduced costs therefore, their services are interrupted by unauthorized and unidentified profiles more often. [14]

Loss of data is considered one of the most commonly faced risk yet the biggest one for any organization becoming prey to it. It can lead to data being leaked as well. To define loss of data in a few words, it is the deletion, corruption or leaking of sensitive data. The cause of the abovementioned factors can be either due to power failure, corruption of data center and the hardware, wrong installation of software or simply a malicious person with the intent to misuse the data they got their hands on.

SaaS cloud computing’s main feature is its high dependency on access to an internet connection, therefore it is very important to ensure that application programming interfaces being utilized by external users, are highly secured as application programming interfaces are the most comfortable means to make cloud accessible to users. However, mainly in public cloud, the cloud is based on a publicly accessible domain which makes it easy for people with malicious intents to access these domains in order to either harm or hack the interface and hack less or no secured application programming interface.

Breach of data is one of the biggest concerns for organizations as it means confidential or sensitive data being in view, easily accessible or even stolen by hackers with the intent to misuse the data or even sell it on the black market.

One very big risk faced by organizations using SaaS cloud services with the help of SaaS cloud service providers is that it’s not a very easy task to switch from one SaaS cloud service provider to another. The reasons for change could range from dissatisfactory services or risk of SaaS cloud service provider not doing a very good job with regards to security and the organization fears for their sensitive data. Reason why switching the SaaS cloud service providers isn't a very easy task is because it will require transfer of huge amounts of data from one vendor to the other. Another reason being that platforms used by each of the SaaS cloud service provider might not be same or compatible which will make it even harder to shift all the data as it might require some sort of conversion in its format which may even cause data loss, breaches in security as well as corruption of data rendering it useless.

In order to maintain cloud in-house, the organization requires an IT department with skilled personnel who can handle the cloud with regards to its migration, integration and operation for continuous provision of cloud services as an entity's operations are highly dependent on it if the data is present in the cloud. If the organization requires scaling up and down of resources, the IT personnel should be able to manage it accordingly without having to corrupt any software or facing down-time in hardware.

Spectre and Meltdown are two variations of basically the same vulnerability which is known to have affected almost every computer chip which has been manufacture in the past 20 years. It is known to be easily exploited which causes data leakage no matter the level of protection applied on that data. It can be found in PCs, mobile phones, tablets and as well as cloud which allows sensitive data to be stored in the memory of other programs running whether actively or in the background, making it easily accessible and exploitable. Data may include storage of passwords, credit card info, documents, emails etc.

The SaaS cloud can be a big target of Denial of Service (DOS) attackers. To define Denial of Service in a conclusive manner, it is an act to send large amounts of traffic or data that might crash the whole system to ensure that the machine or server being utilized for operations either shuts down or crashed, facing downtime. It ends up rendering the server to hand or crash for users intended to use it. Users may include employees, members and such people who access the server for particular reasons such as accessing data, working or bank account holders wanting to perform transactions. Denial of Service attack does not necessarily lead to loss of data nor it is considered as “hacking”. But it does lead to crashes or down time which may result in the organization in spending lots of time and money in order to make a recovery or get rid of the Denial of Service attack. Denial of Service attacks can be usually found targeting banking sector, governments and such, where every second counts.

To further discuss what type of Denial of Service attacks are faced by cloud servers of the organization, one type is flooding and other is crashing. Flood attacks, if defined in easy words, it’s when the attackers send too much traffic to the system which causes the loading time to extend to the point where system eventually fails to run. When the Denial of Service attack is focused on crashing, the process includes targeting the vulnerabilities or existing bugs and exploiting them in a way which crashes the server or the system being targeted, rendering it unusable till fixed.

One commonly known issue faced by SaaS cloud users is their accounts getting hacked. It could be due to carelessness of the individual, weak password, not changing passwords often, sharing the details with unauthorized individuals or even after taking all measures, hackers still finding a way to access the account. This results in unauthorized activities being performed by the account hijacker in the name of the authorized user, leaving undetectable traces.

2.6 Suggested Measures to Cater Threats and Vulnerabilities in SaaS Cloud Service Model

People feel unsure about using SaaS Cloud Service Model for data storage because of security liabilities. They don’t know much about the SaaS cloud environment therefore they have concerns about security, data protection, and cloud computing. Following list includes answers to some of their concerns as explained by experts of the field as well as precautions and some advices:

- *Take All Measures*

  A security breach is inevitable for a SaaS cloud computing service therefore you must be prepared for it by taking all the measures possible to ensure that all steps possible were taken by you to ensure maximum security, leaving no loop holes behind for hackers to manipulate or take advantage of.

- *Back-up Plan*

  Not all SaaS cloud service providers back up your data stored online. Hence it is considered a good practice to ensure that you have made up a secure back up off your own, depending on the preference of hot site and cold site. This will ensure that just in case there is a case of data loss, you will be able to recover it fully instead of requesting cloud service providers for your data. Also, one can never be sure how secure the backup is just in case your cloud service provider has kept one, hence it is always better to keep a backup of your own where you follow all required standard operating procedures to ensure maximum safety and minimal chances of backup destruction. This will help the organization get back to their operations just in case SaaS cloud server crashes or faces down time. However, a separate back up of your own will require extra costs and hardware.

- *Double Authentication and its Benefits*

  Choose double authentication and IP location method to access SaaS cloud servers and applications. Double authentication, also known as two-factor authentication has multiple benefits to be reaped. A simple example of two-factor authentication is accessing a server or cloud not only requiring your user name and password, but also requiring a one-time password being sent to your registered phone number or email address, without which you may not be able to log in to the system or perform vital activities. Benefits which two-factor authentication has to offer include:

  - the biggest reason why two-factor authentication is used is to improve security. A hacker may have got their hands on your user ID and password however it wouldn't be very easy to access the second form of security, being an SMS on your registered number or email or even both.
  - Identity theft is mitigated to some extent due to two-factor authentication. If identity theft occurs, chances are the organization will lose their customers and reputation in the market. Old customers stop relying and new ones would rather go to the competitors. Such news is always posted online hence this would jeopardize an organization's credibility throughout the years.
  - Today's generation is very habitual of having resources which are easy to access or on their fingertips. With the help of two-factor authentication, resources can be made accessible on multiple devices without having increased security issues and vulnerabilities.

- *Data Encryption and its Benefits*

  Influence data encryption and translate it whenever possible for backup. Data encryption is a method which translates data in a form of code so data becomes accessible by only limited number of people who have the decryption password. Even if data breach does occur, the hackers will not be able to decrypt the information with ease, rendering the data they acquired, useless for them. Benefits of data encryption include:

- Encryption is comparatively a very easily available and less costly security measure which even a layman may use due to some free software available. For the level of security encryption provides, it justifies the price required to be paid for it.
- In some countries, law of security and privacy of data is required the organizations to encrypt their data and its considered mandatory. If the organization faces a data breach and it is found that the data was not encrypted, it may lead to regulatory fines and non-compliance of laws.
- Encryption of customer data can increase the trust of customers on that organization as nothing matters more than privacy to any individual. This in turn can increase reputation of the business in the market and increase customer loyalty.

- *Minimal Human Interaction*

  It is recommended that minimizing human interaction is another way to eliminate security threats. As it may not seem like a very viable option, but it may reduce the information one may produce during the conversation that can create security threats or a target for hackers. Hence it may be important for high level personnel to keep in check whom they talk to and what do they talk about without revealing any details which may cause data breach.

- *Strong Standard Operating Procedures*

  Standard operating procedures are utilized in order to document and give a structure to business processes. Whether the organization is small or large, following standard operating procedures reduces the risk of potential breach or data loss of the SaaS cloud. Having strict standard operating procedures is beneficial in many ways as mentioned below:

  - Standard operating procedures can significantly show reduction of errors in daily activities if they are being followed properly by the personnel
  - Standard operating procedures improve the accuracy of data being input and data used in the outputs, putting data less at risk.

  - Following standard operating procedures also ensure that all functions were being dealt securely, ensuring less chances of data breach or loop holes left behind for attackers to manipulate.

- *Preparation for Future Potential Breaches and Loss*

  Data breach can occur anytime without a warning. After ensuring everything is secured fully to its possible extent, an organization should prepare for a data breach regardless. Data breach may affect the organization, the clients or even both. Hence both should be prepared to face the data breach and the possible losses beforehand. Recommended steps to prepare for it may include:

  - Understand the risk, its type, nature, probable loss (whether quantitative or qualitative) and other factors which make the risk a "risk" for the organization involved. To understand the risk, a few things should be figured out such as, data and its type being collected by the organization, understanding how the data is collected or retrieved, the timing of the data being collected, what use the data is being put to, access control list which has access to sensitive data, the basic flow of the data, as in, how to data flows from one system to the other, the safeguards or standard operating procedures put in place in order to protect the data and the legal implications on the organization as well the obligations with regards to collection, usage and distribution of the data in case a breach occurs either by the organization itself or the external parties involved.
  - Having a team is great but having the right team is essential. Data breach itself is a difficult issue to deal with however a good functioning team is essential in order to respond to the breach timely, dealing with delays, breakdowns and protecting the data in time. Ideally, the team should include people from various backgrounds and experiences such as IT, HR, PR, finance, senior members of the organization, as well as managers of various systems running in the organization. Not having the right team might cause various issues for the organization while the data breach is happening as it could lead to losses which are unimaginable with lots of costs to be able to recover everything back.

- Securing the data as well as consistently monitoring it as a preventive measure. The organization must have a clear view as to where they stand with regards to how well their information technology department is securing the data being collected and used by the organizations personnel, the policies of the organization and the employees with high level access to sensitive data and their management and lastly, if any past incidents have occurred, what measures the organization has taken to fix the issues. Apart from all measures that have been taken by the organization in order to protect the data, one measure is most undermined usually by the organizations, which is, training the high-level personnel dealing with sensitive data present in the cloud. Training shall include how to mitigate risks, what are the potential risks and their estimated loss, how to react during the breach, how to recognize a threat and informing the right personnel in order to deal with the breach as soon as possible.

When the breach has occurred in the SaaS cloud, there are a few steps recommended to the organizations:

- The decided and approved plan should be implemented accordingly as it may protect the organization from data loss and expenses.
- The insurance company should be informed immediately as most policies have a very small timeframe to contact and inform the insurance companies in order to be able to claim the insurance. If missed out on the deadline, the organization may face huge losses as insurance must be covering lots of expenses to be incurred. Organizations shouldn't hesitate or wait till the extent of breach is decided, it is highly recommended to inform and keep the insurers timely informed about each update regarding the breach. Any action or words may render the insurance to become void or not applicable on the breach, hence the personnel dealing with insurers must know what they are speaking about and what should they inform regarding the breach.

        - Organizations must be able to resolve external queries and problems thoughtfully with detailed proper responses as they can help in avoiding litigations against the organization. This can be either done by having a reliable spokesperson from within the organization or hiring of a public relations firm to assist with the situation.

- 24-hour monitoring services assist the organizations in securing the data. SaaS cloud monitoring service is a type of service that delivers cloud monitoring and management functions for monitoring cloud founded platforms, servers, IT Infrastructure and others. Cloud monitoring offers a wholly managed cloud monitoring facility for cloud. Cloud monitoring is mostly found in SaaS based clouds which has a sole purpose of monitoring and detecting issues with regards to performance or other across the whole cloud. Reports are later issued with statistics of performance reflecting the reports to the admins of the cloud server in order for them to review and find any issues possible. Cloud monitoring has helped the admins of SaaS cloud server in various ways however a few are very important for the cloud admins.
    - All the functions for monitoring SaaS cloud founded platforms, servers, IT Infrastructure are monitored for their performance and any lack thereof is reported immediately. It covers the whole infrastructure of the cloud, leaving no aspect behind which in turn helps the administrators of the cloud knowing that cloud is functioning fully.
    - Monitoring services of the cloud has a certain level it expects the cloud infrastructure to perform at. Therefore, it ensures the infrastructure is performing at its optimal level. Just in case it is not, the admins of the cloud are informed through the reports.
    - Immediate reporting of the issues can cater lots of damage which could’ve occurred if the cloud admins had not been informed timely and the remedial actions were not performed immediately. SaaS cloud monitoring services has the capability to inform the cloud administrators either through emails, message on cell phone, dashboard reports or any other possible manner which is the quickest to reach the admins of the SaaS cloud.

- Be ready to respond to any security breaches in time. Timely response to SaaS cloud breaches can save lots of damage quantitatively and qualitatively. If the breach is dealt with timely, organizations may not even find the need to shut down their operations completely, saving further loss from happening. In order to respond timely and effectively, preparation beforehand is the key. Ways an organization can prepare before the breach are as follows:
    - Timely response can firstly occur only when there was a breach response plan setup and practiced as well as informed to the relevant personnel. Relevant personnel will be identified as the incident response team who will include various people from various backgrounds and departments, internal as well as external to the organization facing the breach. The departments which they may belong to include HR, legal department, IT, security, internal PR etc. Whereas when speaking about external to the organization, the team should contain lawyers from a law firm, spokesperson from PR firm and security teams of relevant organizations. All should be told and trained as to how to execute the breach response plan of the cloud. Demo sessions may also be needed in order to focus on perfect execution. There should be a way to communicate each person involved in the incident response team immediately using the means most convenient and immediately accessible by the team no matter what time of the day it is and where they are geographically.

- Web Access Firewalls (WAF) is an advanced firewall technology that can help organizations protect the data stored online on SaaS cloud. Its main function is to protect web applications by filtering as well as monitoring traffic between it and the Internet. On one hand a proxy shields an organization’s machine’s identity by utilizing a midway, on the other hand web access firewall is a type of reverse of the functions of a normal proxy which includes shielding the server from revelation by having organizations pass through the web access firewall before even being able to reach the server. In web access firewall, there is an option to define the filters to push out all kinds of malicious traffic. These are called policies and maybe altered as per the needs of the organization. These policies maybe quickly altered even during the cloud breach to completely limit any kind of traffic to penetrate the SaaS cloud. Web access firewall has three types:

- Allow List web access firewall: It allows only the filters which have been applied in the web access firewall policies. If any traffic that doesn't comply with the filters, it will be pushed away. An example can be such as a party having a designated guest list and only people's name appearing on the guest list can make it to the party.

- Block List web access firewall: It disallows and protects only against known attacks or known malicious traffic updated in the data base. The data base needs to be kept updated to ensure that the latest known malicious traffic is blocked from penetrating the cloud servers. An example can be such as a party having a dress code, without which one cannot be allowed into the party. If the guests appear breaching the dress code policy, they cannot enter the party.

There are three ways web access firewall can be implemented in the organizations, each of them having pros and cons.

- Network based web access firewall: A lot of hardware needs to be purchased for network-based web access firewalls, hence making them expensive to purchase in the first place then expenses to maintain them, their physical security and their maintenance. They are installed on the premises of the organizations which means it also requires a designated storage.
- Host based web access firewall: It is integrated with the organization's SaaS cloud. It is comparatively less costly than the network-based web access firewalls however it has its own disadvantages such as it may not be compatible with the SaaS cloud's infrastructures hence making it difficult to implement it, maintenance costs which will be required from the organization and reliance on the host. However, another benefit includes that customization is very easily performed on it as it does not require the organization itself to perform the deed of increasing or decreasing resources and hardware in order for their requirements of customizations.
- Cloud based web access firewall: It is considered as the most viable and inexpensive option as compared to Host based web access firewall and Network based web access firewall. It is one of the easiest ways to implement on the cloud infrastructure of the organization. The costs include the month wise or year wise billing sent to the organization for the services of Cloud

based web access firewall by the SaaS cloud service provider. With regards to updated threats, it is the responsibility of the SaaS cloud service provider to ensure all data base is updated hence keeping the block list web access firewall most effective. Which means the organization is no longer responsible for the updates. However, the biggest disadvantage is complete reliance on a third party, facing consequences if the cloud service provider faces down time for any reason and trust that the malicious traffic will not pass through.

- Organizations can benefit from things like micro-segmentation, layering and application services in a SaaS cloud environment.
  - Micro-segmentation, to be defined in simplest of terms, is a type of security of network, that enables the division of data center of the cloud into different segments from top level to bottom level (an individual’s work load) and then define the security policies and the levels to be applied at each segment in order to ensure that each segment is secured and secured up to the level of the data needs the security, varying from sensitive data to common data. Micro-segmentation is used to assist the information technology department of the organizations to allow flexibility with the security policies and their application to the data center of the SaaS cloud as compared to the expensive and overly complex way of buying and applying physical firewalls in order to achieve the same concept of segmentation and security of the data. Due to micro-segmentation, it gets harder to breach the cloud security for the malicious attackers.
  - The layers of protection needed in SaaS cloud are important for security purposes of the data on the cloud. This could include small yet very effective steps for example, when an employee leaves the organization, paperwork and off boarding process should and must include revoking of all access on the very same day, preferably in the same hour they end their work at. It will be the information technology department’s responsibility as well as human resources department to inform the information technology department timely. But if under any case it seems impossible to implement such step as soon as possible (as per the above recommendation), then a system should be implemented which performs the actions. Having accounts (especially of

administrators or important personnel of the organization having access to the SaaS cloud at a very sensitive level) opened even after they have left the organization can put the risk on organization either by the same employee or employees around them who can for some reason access their account on the cloud, leaving no real traces behind as to who caused the mishap or breach to occur. Such a simple mistake can leave the organization high and dry.

Another great example of keeping the security tight is to ensure the main account (also known as the main administrator account or root account) should be kept as secured as possible and should have one designated owner in order to ensure that the actions are only being performed by that one person. The root account can perform all or any actions in the SaaS cloud, without needing a single approval or permission, without informing any other admins of the cloud, which can be very disastrous to the organization. Having backups is essential but ensuring the safety of the cloud account maintaining that backup is the key to security of the backup. It does not necessarily mean that a breach is supposed to happen for the backup account to come in use. There could be data loss due to other reasons such as an employee accidentally deleting an entire block of data base. The security policies being followed to keep the root account safe and secure should also be applied with the same dedication to the backup account as it can be the biggest key during disaster recovery process. It should be ensured that backup is being maintained and updated daily, and if failure to do so, there should be some sort of notification system set up which indicates the failure in backup immediately to a few personnel either through email or message alert on cellphones in order to ensure a quick communication to fix the issue immediately as even one day of data loss can render the organization to fall in jeopardy.

2.7 Deployment Models

There are the following 4 types of cloud which can be deployed by the organization according to their needs and business model:

- Public Cloud
- Private Cloud
- Hybrid Cloud
- Community Cloud

2.7.1 Public Cloud

This type of cloud service is designed for public use and the service providers are keen on facilitating their clients with benefits like reduced costs and multiple servers. Amazon Cloud service is one of the best public cloud platforms available in the market that promotes confidentiality and integrity. In other words, public cloud utilizes pay as per usage model for billing and is wide open to manipulate and access information using the internet. The resources of a public cloud are handled by Cloud SP. (Service Providers)

Best Examples: IBM SmartCloud, Microsoft, Google App.

2.7.2 Private Cloud

The private cloud infrastructure is not meant for general public. Despite sharing resources, it provides isolated servers for its clients. Most organizations use this type of cloud to manage their various customers' servers without threatening their privacy. Third party involvement and off-site relocation is a likely alternative in case of a security breach. In other words, private cloud is also identified as an internal cloud as well as corporate cloud. The management of data centers for the private cloud and its responsibility rests with the organization. It may rest with the third party which is highly dependent on what the organization decides who should manage the data centers and their data. The deployment of private cloud is used by tools of opensource namely Openstack and others.

Best Examples: HP Data Centers and Microsoft.

2.7.3 Hybrid Cloud

A hybrid cloud service is a cross between two or more cloud computing services (private, community, public). It takes care of data collaboration, allocation and storage with the help of standardized technology. In short, Hybrid Cloud is a combination of the public cloud and the private cloud. With private cloud being fully secure and public cloud having relatively less security and privacy, hybrid being both of them has security level half-way as the servers which are public can obviously be accessed by the general public.

Best Examples: Gmail, Google Applications and Google Drive.

2.7.4 Community Cloud

When organizations have same goals and concerns then they come together on a shared cloud computing platform to promote a community. These services operate on offsite channels and help organizations manage their policies and ongoing missions by securing their data. In other words, community cloud permits systems and services to be reachable by a number of organizations to share the data between them which is useful for all to collect and use. With regards to its ownership, management as well as operations, there can be a number of possibilities such as one or multiple organizations of that shared cloud or even a designated cloud service provider as well as lastly, a combination of both.

Best Example: Community cloud used by healthcare sector.

2.8 Security Issues in Cloud Computing – Famous Instances

Almost all cloud computing services promise protection against cyber threats and attacks, but the disposition of their aptitude isn't as reliable as one would think. *Almost a decade ago, several leading cloud service providers experienced unexpected security breaches in their system. Amazon's Simple Storage Service malfunctioned twice in early and mid-2009. Cloud service sites that lack backup storage servers were brought to a halt because of these incidents. Google Docs faced their biggest dilemma in early 2009 when their clients' personal and private data became available for public access. The most trusted email portal Gmail also experienced uninterrupted security breach for almost 4 hours. In May 2009, VMware's virtualization software designed for Mac users experienced several security breaches. Microsoft's cloud computing portal – Azure – went offline for almost a day without any security wall in place to fend off cyber threats. Things can get complicated for service providers if their systems are exposed to outward threats for too long. Link Up was forced to shut down their cloud services since they lost 45% data of their users.* [1]

Biggest Security Cloud Computing Data Breaches of the Century

- Microsoft

  In 2010, configuration issues caused data breach for Microsoft. The breach was caused by users not included in the authorized control list of cloud services could access all contact details of all the employees of Microsoft in the offline address books. Non-authorized users included customers of Microsoft as well. It was fixed within two hours of the breach but being a renowned company like Microsoft has its disadvantages due to expectations of the community.

- Dropbox

  A popular online cloud service drop box being used by many for free or for a fee faced a breach in the year 2012. Hackers got access to over 68 million usernames and password including email IDs which concluded over 5 GB’s of data. The compromised details were sold on the dark web for bitcoins worth over $1000. Dropbox took the initiative of truthfully informing their customers about the unknown breach and requested all users to change their credentials.

- National Electoral Institute of Mexico

  In April 2016, 93 million voters lost their details required during registration to the hackers. The breach happened due to National Electoral Institute of Mexico using a cloud server which was illegal and insecure outside of the country.

- LinkedIn

  LinkedIn became prey of the hackers back in 2012 as well as in 2016. In 2012, 6 million username and passwords were compromised but in 2016, 167 million usernames and passwords were stolen and was sold on dark web. To cater the problem, LinkedIn introduced two-way authentication for all users.

- Apple – iCloud

  The breach affected all data stored in iCloud however it was more of a targeted breach where celebrities faced leakage of their personal photos over the internet.

- Yahoo

  In 2013, user IDs, passwords, date of birth and secured question answers were leaked of over 1 billion users of yahoo. All the data was stored on cloud service being used by Yahoo.

- Republican National Committee

  This data breach incident is similar to National Electoral Institute of Mexico where data of voters was breached of 198 million individuals. The data included all private information of individuals including their race as well as which political party they voted for.

2.9 Related Work

Security in cloud computing is the top concern today for every organization implementing their applications on cloud. Different methods and techniques have been proposed in literature review in order to handle security breaches. Following is the brief discussion on these methods and techniques

- P.S. Suryateja, provided an overview of numerous threats and vulnerabilities which can act as a guide to evaluate security risks to decision makers in organizations. [7]
- Sugandh Bhatia, Rajinder S. Virk, discussed various tools and techniques for the implementation of security mechanism in the cloud services. [8]
- Muhammad Aamir Nadeem, performed surveys in his paper to identify the weaknesses in Cloud architecture, internet protocols, operating system and application software, and in crypto system. He further explains that the threats and vulnerabilities to Cloud are the concerned issues which if successfully overcome can make Cloud a digital platform or fort for its users. [9]
- LufungulaOsembe, proposed viable mechanisms to address the security challenges faced in the adoption and usage of cloud computing. The proposed framework provided the guidelines that can be further developed in order to reinforce compliance and minimize the impact of security challenges in cloud computing. [10]
- Nalini Subramanian, Andrews Jeyaraj, discussed the security challenges that are faced by cloud entities. Cloud computing is failing to take the leading spot as a data protection alternative because of various security reservations. New cloud computing models can work on the liabilities present in the previous models without changing the significant features of the existing model. Cloud environment is not stable enough to accept new technologies without the possibility of a security breach therefore users need to be cautious while introducing new technologies in it. This study details on the possible security issues that users might have to face in a service delivery model. [13]
- Naseer Amara, Huang Zhiqui, Awais Ali, have put forward grave concerns of not having any strict and reliable security standards for CC. According to them, even after developing multiple tools and models, CC is not secure. [14]

- Deyan Chen & Hong Zhao reveals that despite generating high revenues, cloud computing services lack in securing your data as well as maintaining privacy. They advise on prioritizing the protection of your privacy and security and isolation of confidential data from the public servers. [26]
- Jaydip Sen addresses regulatory, security and privacy concerns related to cloud computing services and recommend possible strategies and solutions to resolve them. He further suggests that transparency is needed to ease over the apprehensions of organizations and individuals over possible data breaches. [28]
- Muhammad Aamir Nadeem reveals that virtualization is what runs all cloud computing systems therefore weaknesses in virtual machines jeopardizes the whole infrastructure of cloud storage. [27]
- Anjana&Ajit Singh expressed that the involvement of third parties in resourcing puts cloud computing services at risk. They discussed all security concerns related to SaaS, PaaS and IaaS in a qualitative analysis report and propose Cryptofunctions, Cloud Identity Management and Virtualization in Cloud infrastructure as possible solutions to minimize security risks in cloud computing systems. [28]
- N. Chandramouli and B. Manjuladiscusses previously employed strategies and solutions to resolve security issues related to privacy and data protection in cloud computing system. [27]

CHAPTER 3: Research Methodology

3.1 Research Design

Exploratory research is used to solve a problem not clearly defined using qualitative research methodology. By definition, qualitative research refers to a market research focusing on gathering data through open-ended questions. This method is not only about “what” people think but also “why” they think so. Primary data is collected through qualitative semi-structured interviews. These interviews conducted have explored the companies who have implemented cloud computing on their applications. Secondary information is on literature review. It identified the challenges and hurdles in the way of implementing cloud computing and how does certain threats and vulnerabilities affect the cloud security. One-on-one interviews were conducted to identify gaps as conducting in-depth interviews is one of the most commonly used research methods.

Qualitative research methods are usually created and utilized in a way that it helps show true perception, view and opinion of the targeted audience in relation to the topic in question. Hence, it can be said that the results which are derived from qualitative research methods are more descriptive and the conclusions can be produced very easily with the data in hand collected from various methods. Qualitative research methods are originally inspired by the sciences focusing on social as well as behavioral conducts. In today’s era, it is not very easy to understand what the humans genuinely feel, think and perceive about something. That is where Qualitative research methods comes in, with the sole purpose for the researcher to gain better clarity about the topic in question as it makes the targeted audience be more descriptive about the topic they are being asked to communicate about.

This paper has chosen the Qualitative research method of “Interviews”. It is the most common Qualitative research method and most effective for several reasons. It includes an activity of conducting a personal interview that is carried on one-to-one at a time. It is focused mainly on a method that is based on conversations and it promotes an opportunity for the researcher to gain as many deep details as possible from the target audience with regards to the topic in question. As mentioned above, this method was chosen for its advantages, one of them mainly being that the one-on-one interviews provide a great opportunity to the researchers to gather accurate data with regards to what the respondents truly believe in and what motivates them. If well prepared enough to know what type of questions one must ask, it can greatly help in collection of raw yet meaningful and highly useful data for the research.

Interviews allow a great ground to play on as from jumping to one topic to the other, follow up questions can be produced from the answers given by the respondents that can lead to unique answers with great details that can make the research very unique and exquisite. Qualitative research is yet to be performed on this topic, hence making it a unique method for the topic to be discovered and researched upon.

Some of the characteristics of qualitative research methods are mentioned below:

- Qualitative research methods allow data to be collected there and then, exactly where the targeted audience is working or experiencing any issues, hence making it data collected in real-time.
- Qualitative research methods have lots of methods to gather the same data. A researcher can use any or all methods that can provide the best and maximum information about. Ways of Qualitative research methods include interviews, observing the targeted audience, any documents audience might be able to provide with and so on.
- Qualitative research methods are mainly famous for making it easy for researchers to solve extremely complex issues by arranging and managing the data collected by them into meaningful information which can easily be understood by layman who is reading the research for learning purposes.
- Qualitative research methods usually rely on communication. Communication brings in personalization which helps in developing trust with the researcher then the information which is provided by the target audience has a lot of truth to what they are saying including genuinely good opinions as well as bad opinions regarding the topic in question.

The reasons mentioned above are as to why the Qualitative research methods were preferred.

3.2 Respondents

Several semi-structured interviews were conducted with Small and Medium Enterprises (SMEs), cloud workers and security management team to acquire appropriate data from four major companies.

3.3 Sample Size and Sample Technique

Companies providing cloud services as SaaS (Software as a Service) were considered for collecting data. Key information is gathered via purposive sampling technique. One can choose any sample that they deem appropriate for the purpose of their study. Purposive sampling technique will be used to select a group of participants who have the knowledge to answer the interviews questions. Theoretical sampling will be done based on theoretical saturation.

The paper has chosen purposive sampling which has other names such as judgmental, selective or subjective sampling. It is completely reliant on the researcher and their judgement when it chooses the sampling units to be researched upon. The sample size is comparatively small but meaningful as well as sufficient enough to extract data from. The main purpose of this type of sampling is to select units from the whole population in order to create samples which are not random. It allows the researcher to openly pick and choose particular characteristics in the unit which will assist the most in research and will help answer the questions in mind of the researcher, hence allowing the research to go more as planned and focused as possible. This helps removal of excessive unrequired data which other units may have provided if the sampling technique was focused on "random". One very common issue or weakness pointed out by most is that the samples chosen during purposive sampling does not represent the population in true and view, however, it is not considered an issue for the qualitative method researchers as it allows the researchers to have a choice made by them to choose the samples which best represent their topic of choice.

The reasons why purposive sampling was chosen is because of the advantages that it has to offer, some of them being:

- It is popularly known that qualitative method of researching and purposive sampling go hand in hand, complementing each other. The qualitative research designs can be conducted in various ways, most of which can be conducted using purposive sampling. The designs used in qualitative research require a unique type of strategy for sampling in order to gather the data which is focused on answering the questions of the research topic.
- The qualitative method researchers cannot take information from chosen samples and make general claims about the entire population in question however purposive sampling provides research logical and analytical ways to justify their researched samples and generalize the information.
- Different types of purposive sampling techniques can be used for one research to create the best conclusion.

- Purposive sampling is flexible enough to save time and money of the researchers as they can choose the samples as per their convenience and geographical limitations.
- Researchers can target niche demographics to obtain specific data points.
- It is very much allowed during purposive sampling to choose the target audience from a diverse range who are all relevant to the topic being researched. Purposive sampling is designed in a way to benefit the researchers to gain as much information as possible for the topic in question. For example, if the researcher requires to know opinions (whether good, bad or neutral) about the researched topic, the same questions can be asked from multiple people belonging to that community in order to support the conclusion being made by the researcher as it can be said that it represents the general public.
- If the researcher wants to find out how a change or any issue affects the average person, then it would require the researcher to conduct the research with people who fit into a defined median from the researcher's demographic studies, hence, helping the researcher find the averages in the data through purposive sampling.
- On the other hand, purposive sampling not only allows to seek the median perspective, it also has the flexibility to allow the researcher to gather information of extreme perspectives, which may be very important for a qualitative researcher.
- Purposive sampling allows the researcher to take the whole population as a sample in order to gain everyone's perspective for the research.

3.4 Data Collection

There are numerous methods to collect data like surveys, questionnaire, case studies and experiments. The survey method was used and has help in successfully collecting primary data by conducting semi-structured interviews. Semi structured interview guide is attached as Appendix A & B. In these questions all the required information was asked from Cloud Security manager team in the firms regarding importance of cloud security, management of critical challenges, threats and vulnerabilities faced by implementing cloud computing on their applications. Most of the interviews have been conducted face to face. However, few interviews were conducted by phone because of location of some companies and busy routine of respondents. Interview timings ranged from 15 minutes to half an hour. Bilingual (English & Urdu) interviews were conducted as per the interviewee's convenience for data analysis. It was notified to the participants that they can participate by their own will and if any time they want to withdraw, they can. The participants were guided, and interviews were scheduled a week before to make sure the availability of the participants. The participants were inquired regarding the management of application that are placed on cloud. What were the challenges faced and how did they manage it? Moreover, what are their mitigation strategies that are implemented to control the future threats or vulnerabilities of applications on cloud.

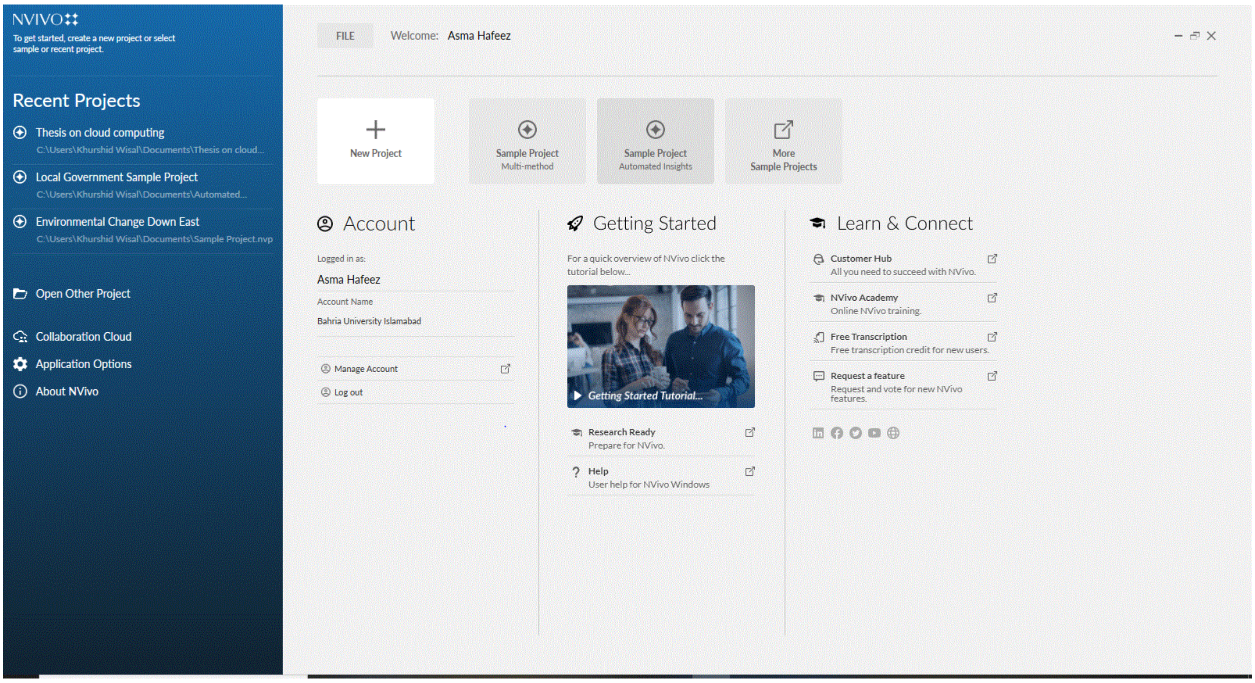
3.5 Data Analysis

After data has been collected, sorted and aligned accordingly, Data analysis tool i.e. NVivo (a software befitting for qualitative research) was used to analyze the collected data. QSR International fashioned this software program to examine vague writing, audio, video in addition to images as well as interviews and journal articles. The outcomes were analyzed and compared with cloud computing service delivery model (SaaS).

In this study the analysis of the data has been conducted with the framework of grounded theory that is widely used for qualitative data analysis. "Grounded theory is a research design where the "inquirer generates a general explanation of a process, an action, or an interaction shaped by the views of the large number of participants" [29].

Mainly grounded theory is used to build a theory based on opinions and thoughts of people however it is also helpful in generating concepts. Categories and concepts are key elements in grounded theory, so as a strategy in qualitative data analysis it works better in generating concepts than theory.

This qualitative analysis has been done with computer software that is used for qualitative data analysis Computer-assisted qualitative data analysis software, or CAQDAS namely NVivo. The interface of the software is shown in figure 3-1.



To get started, create a new project or select sample or recent project.

Welcome: Asma Hafeez

Logged in as: Asma Hafeez

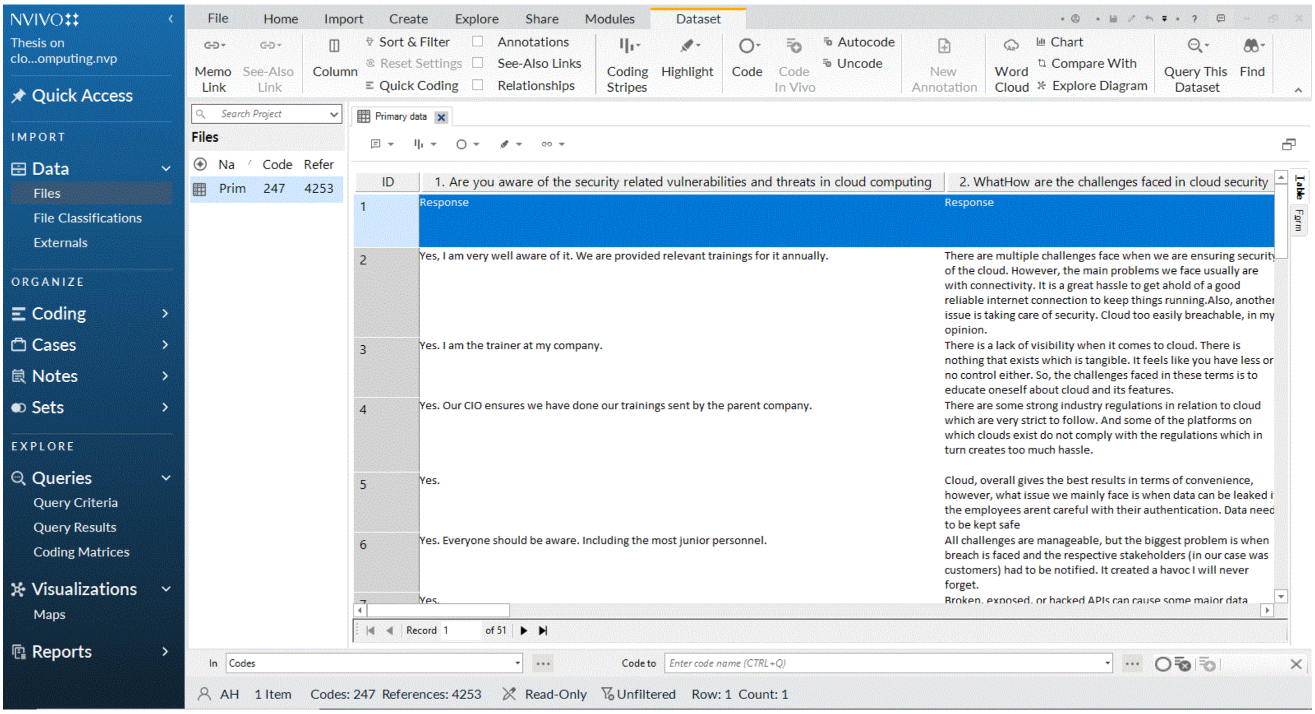
Account Name: Bahria University Islamabad

For a quick overview of NVivo click the tutorial below...

NVIVO
Recent Projects
Thesis on cloud computing
C:\Users\Khurshid Wisal\Documents\Thesis on cloud...
Local Government Sample Project
C:\Users\Khurshid Wisal\Documents\Automated...
Environmental Change Down East
C:\Users\Khurshid Wisal\Documents\Sample Project.nvp
Open Other Project
Collaboration Cloud
Application Options
About NVivo
FILE
New Project
Sample Project
Multi-method
Sample Project
Automated Insights
More
Sample Projects
Account
Manage Account
Log out
Getting Started
Getting Started Tutorial...
Research Ready
Prepare for NVivo.
Help
User help for NVivo Windows
Learn & Connect
Customer Hub
All you need to succeed with NVivo.
NVivo Academy
Online NVivo training.
Free Transcription
Free transcription credit for new users.
Request a feature
Request and vote for new NVivo features.

Figure 3-1 NVivo Software Interface

Despite using the software the analyst has to organize, interpret, code and then retrieve the data. After collection and transcription of data it was compiled in MS excel sheet. Then the excel sheet was imported to NVIVO as shown in the figure 3-2 so all the interviews were saved under the file name “Primary Data” in step one.



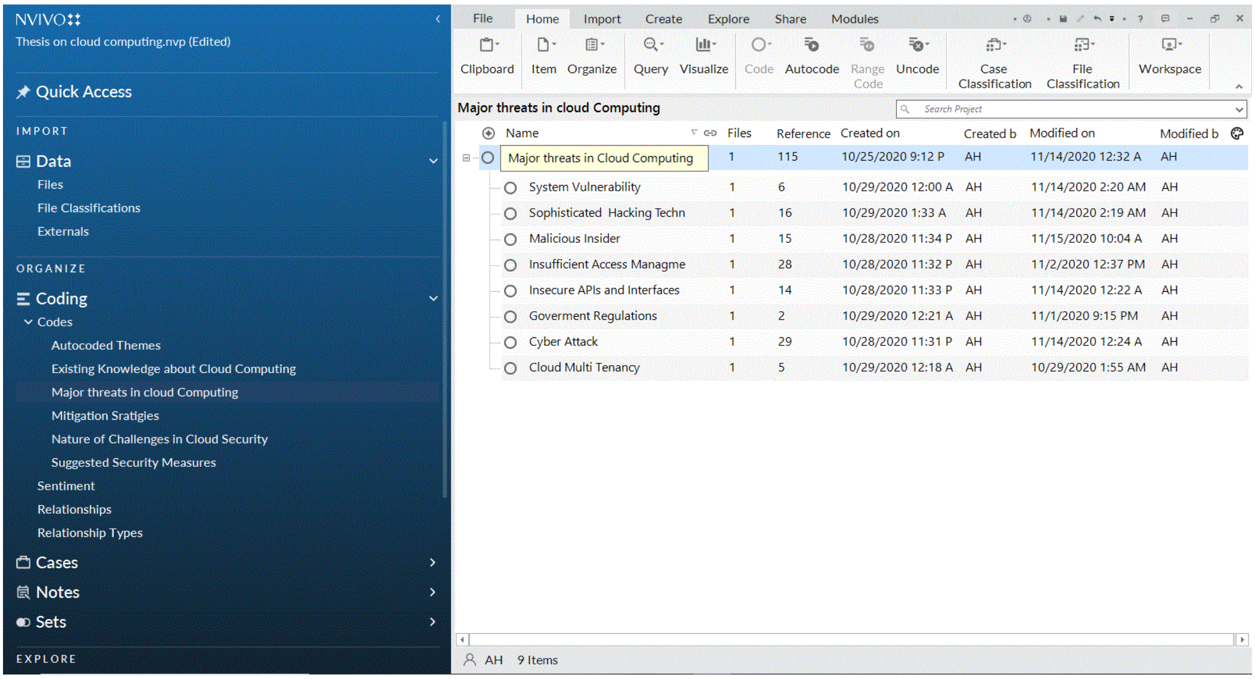
ID	1. Are you aware of the security related vulnerabilities and threats in cloud computing	2. WhatHow are the challenges faced in cloud security
1	Response	Response
2	Yes, I am very well aware of it. We are provided relevant trainings for it annually.	There are multiple challenges face when we are ensuring security of the cloud. However, the main problems we face usually are with connectivity. It is a great hassle to get ahold of a good reliable internet connection to keep things running.Also, another issue is taking care of security. Cloud too easily breachable, in my opinion.
3	Yes. I am the trainer at my company.	There is a lack of visibility when it comes to cloud. There is nothing that exists which is tangible. It feels like you have less or no control either. So, the challenges faced in these terms is to educate oneself about cloud and its features.
4	Yes. Our CIO ensures we have done our trainings sent by the parent company.	There are some strong industry regulations in relation to cloud which are very strict to follow. And some of the platforms on which clouds exist do not comply with the regulations which in turn creates too much hassle.
5	Yes.	Cloud, overall gives the best results in terms of convenience, however, what issue we mainly face is when data can be leaked i the employees arent careful with their authentication. Data need to be kept safe
6	Yes. Everyone should be aware. Including the most junior personnel.	All challenges are manageable, but the biggest problem is when breach is faced and the respective stakeholders (in our case was customers) had to be notified. It created a havoc I will never forget.
7	Yes.	Broken, exposed, or hacked APIs can cause some major data

Figure 3-2 Excel sheet imported in NVivo

Coding being the central part in grounded theory took place as the second step. Coding in qualitative data analysis serve the purpose of managing data, this management of data took place in three steps

- *Open Coding:* At this stage data is break down, examine and compare. This process concedes concepts that are later grouped and convert into categories.
- *Axial coding:* At this stage data is put back together in new shape by making connection between categories.
- *Selective coding:* This stage refers to the process of selecting the core category and relating it to other categories systematically.

Similar codes were placed under single node and that node was named according to the central idea of the codes. This coding process help in identifying relevant themes in the study that ultimately leads to certain concept in the study. Process of coding is shown in figure 3-3.

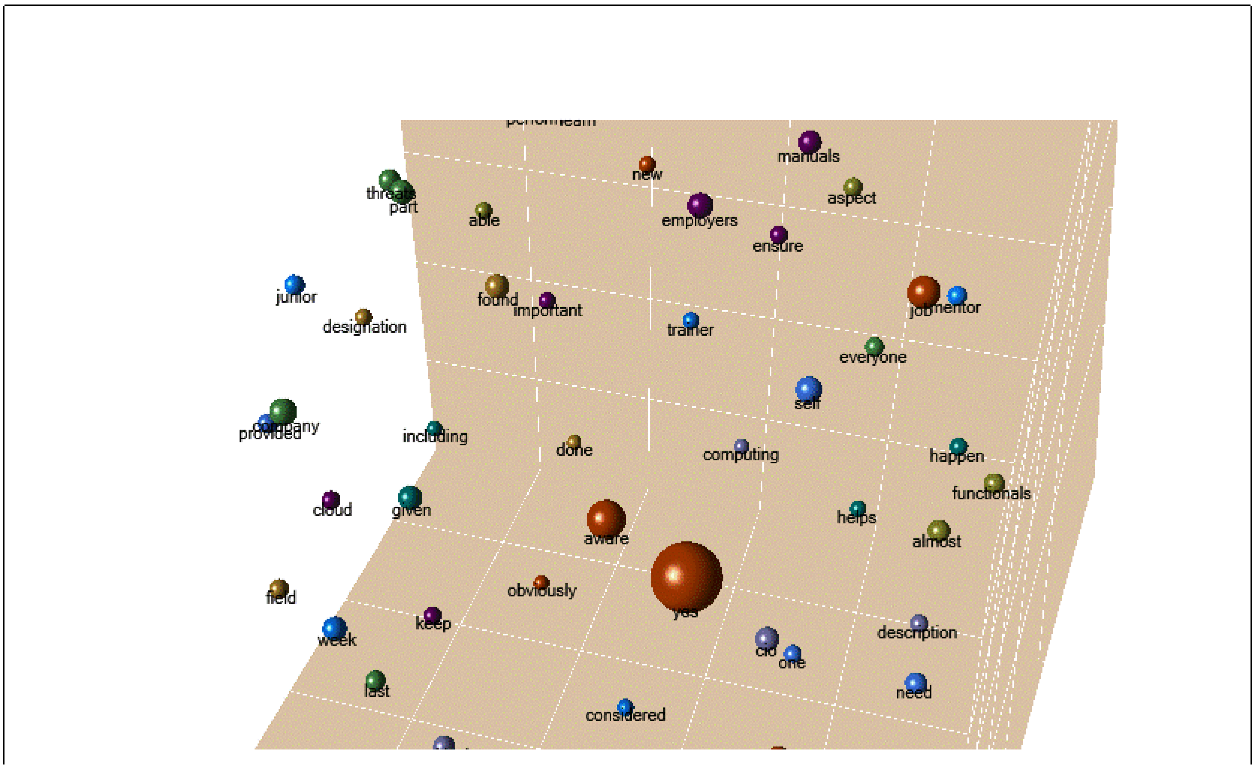


Major threats in cloud Computing

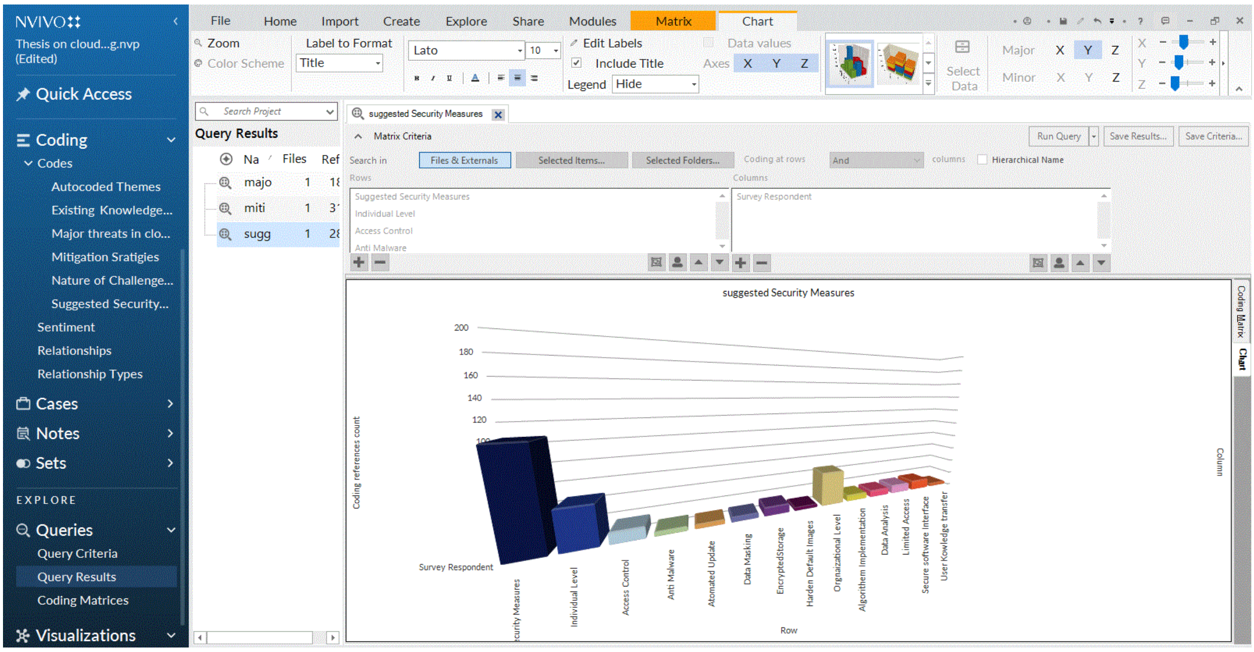
Name	Files	Reference	Created on	Created b	Modified on	Modified b
Major threats in Cloud Computing	1	115	10/25/2020 9:12 P	AH	11/14/2020 12:32 A	AH
System Vulnerability	1	6	10/29/2020 12:00 A	AH	11/14/2020 2:20 AM	AH
Sophisticated Hacking Techn	1	16	10/29/2020 1:33 A	AH	11/14/2020 2:19 AM	AH
Malicious Insider	1	15	10/28/2020 11:34 P	AH	11/15/2020 10:04 A	AH
Insufficient Access Managme	1	28	10/28/2020 11:32 P	AH	11/2/2020 12:37 PM	AH
Insecure APIs and Interfaces	1	14	10/28/2020 11:33 P	AH	11/14/2020 12:22 A	AH
Goverment Regulations	1	2	10/29/2020 12:21 A	AH	11/1/2020 9:15 PM	AH
Cyber Attack	1	29	10/28/2020 11:31 P	AH	11/14/2020 12:24 A	AH
Cloud Multi Tenancy	1	5	10/29/2020 12:18 A	AH	10/29/2020 1:55 AM	AH

Figure 3-3 Coding in NVivo

In order to extract results from this data we run different Queries to understand different patterns exist in our data. We used word frequency query that explain how often the word or it synonyms and phrase have been used. It is also used to explore the data and generate work of visualization for presentation and knowing about most frequently used words.



We use other queres like matrix coding query to know the comparison, convergence and divergence in our data furthermore it helps us in cross tabulating our data, mostly our major themes versus our survey respondents. Here we mostly rely on coding references keeping in view the nature of our data so the number shown in the ribbons refer to number of idea or a word used in that context by the respondents which lead us to understand the intensity of the views and opinion of the respondents.



Na	Files	Ref
majo	1	18
miti	1	3'
sugg	1	28

Rows: Suggested Security Measures, Individual Level, Access Control, Anti Malware

Columns: Survey Respondent

Figure 3-4 Matrix coding query

To visualise our data more clearly we use project maps, project map helps us in developing pattern representation, its coding and the connection within the study. The project map also enables us to see the comparison between two things the process can be seen in figure 3-5.

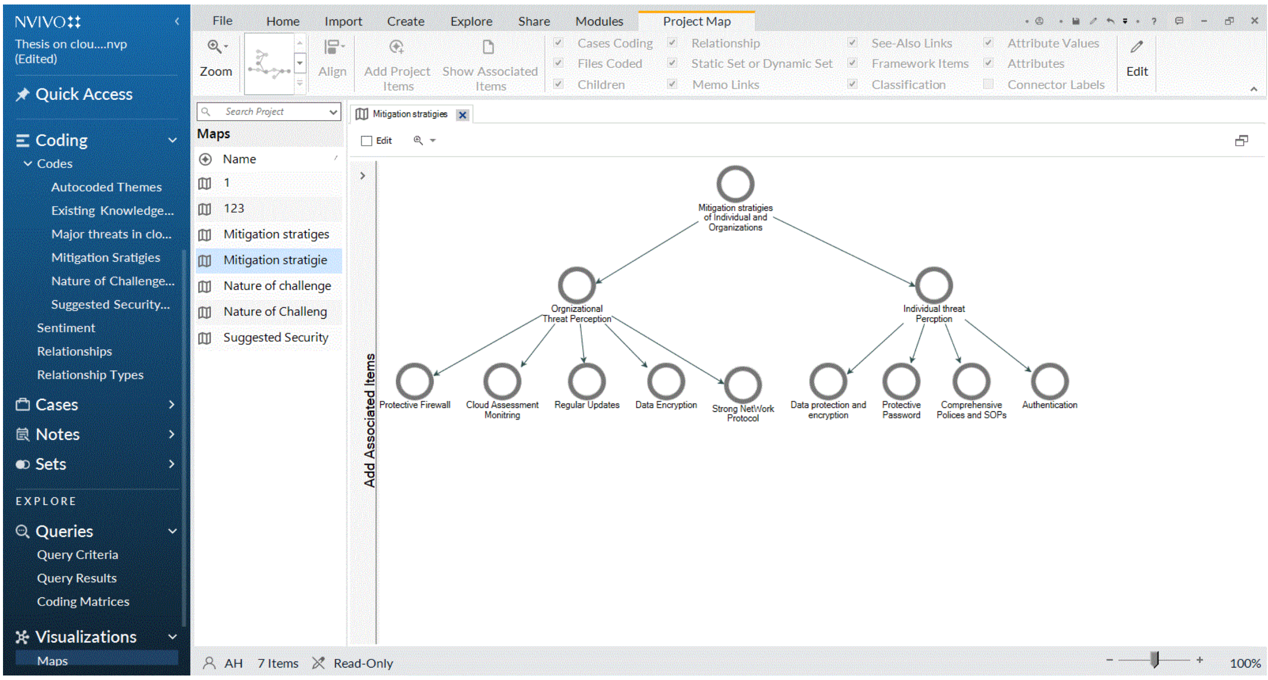


Figure 3-5 Project Map

All these results were exports to the study and were discussed /explained according to the outcome of the software. Lastly, on the basis of these results, findings were generated.

Chapter 4: Presentation of Results

4.1 Overview of the Chapter

This chapter covers the presentation of overall study results. It contains the benefits of cloud implementation. Challenges and hurdles being faced due to cloud. Key factors for managing cyber threats and vulnerabilities of data on cloud: best practices and mitigation strategies.

4.2 Location of Companies

For this research, interviews are conducted within Islamabad with 4 companies working on cloud computing. Total of 50 respondents were interviewed.

The responses below are provided by the Cloud Security Management team of the organizations during the interview for the research.

4.3 Existing knowledge about cloud Computing

General understanding about cloud computing is existing to optimum degree the results showed that word cloud is clearly visible that almost all the respondents are well aware. The reason of sufficient awareness about cloud computing is that all the key informants were expert in the field so they were quite able to respond the basic question about awareness of the study. As a result, the researcher got almost hundred percent result.

Most of respondents reply in “yes” only to the question however others reply that they are well aware, getting relevant trainings annually, bi annually while some have completed their trainings recently. Few of the informants were trainer on the subject by themselves while some were researcher and having teams to lead and teach. The respondents assert that the CIO ensures the conduct of training by every relevant employee even by the most junior person in the company they let us know they have a mentor to keep them aware about all of it. Highlighting the importance of the training respondents called it critical and most important for the fulfillment of their duties. Some called it prime responsibility, a basic feature, important aspect and crucial for job requirements. It is part of my job description to keep myself updated with latest threats express a respondent while other called it basic requirements for my designation and other wise doing their job will become impossible. Hence the researcher got sufficient knowledge about the primary understanding of the respondents that help in constructing the idea of hundred percent knowledge of the subject.

4.4 Nature of Challenges in Cloud Computing

Assessing security issues in cloud computing the researcher flowed a systematic approach of principal of gradation that is from simple to complex, so key informants were investigated generally regarding the challenges in cloud computing to which the respond was that there are multiple challenges face when we are ensuring security of the cloud. However, the main problems we face usually are with connectivity. It is a great hassle to get ahold of a good reliable internet connection to keep things running. Also, another issue is taking care of security. While some expressed that there is a lack of visibility when it comes to cloud. There is nothing that exists which is tangible. It feels like you have less or no control either. So, the challenge faced in these terms is to educate oneself about cloud and its features. There are some strong industry regulations in relation to cloud which are very strict to follow. And some of the platforms on which clouds exist do not comply with the regulations which in turn create too much hassle.

Some of the data collection participants share their views that Cloud, overall gives the best results in terms of convenience, however, what issue they mainly face is when data can be leaked if the employees aren't careful with their authentication. Data needs to be kept safe. They also share about the big problems and the incident of breach they experienced said "All challenges are manageable, but the biggest problem is when breach is faced and the respective stakeholders (in our case was customers) had to be notified. It created a havoc I will never forget".

Keeping in view their responses major themes extracted from the data are shown below in the project map.

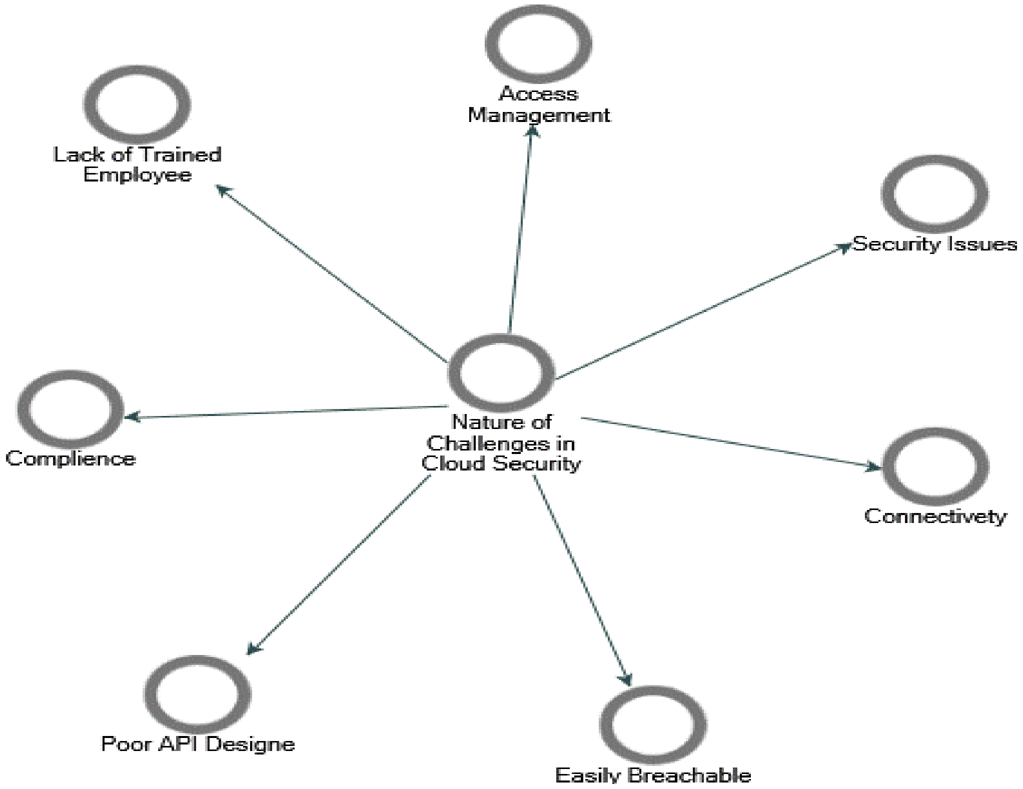


Figure 4-1 Challenges in Cloud Security

Regarding access management, they share that there are too many reasons which threaten the credibility of cloud but ignorance of taking access controls seriously or unauthorized access to customer and business data is the biggest problem nowadays. The access control of the users is a huge duty and access of sensitive information falling in hands of unauthorized individuals or access falling into the wrong hands with regards to sensitive information such as customer’s credentials is great challenge.

From authentication and access control to encryption and activity monitoring, the Software user interfaces (UI) and API's must be designed to protect against both accidental and malicious attempts to protect the security policy. Therefore, to design these interfaces is very challenging.

Describing security issues and poor API design it is said that Privacy and security issues are the biggest challenges and we face them in multiple ways, however the security and availability of general cloud services are dependent on the security of these APIs which shows its importance.

Some of the respondents have the views that security controls are there obviously but when there is inconsistency in them, that will guaranteed threaten the credibility and sensitive data is always under attack so protecting it at all costs is how we face challenges. Besides controls made for security that aren't applied properly can pose challenges.

Broken, exposed, or hacked APIs were also under discussion of the respondents and it is asserted that it can cause some major data breaches while poorly designed APIs and open Ports or Public IPs could lead to misuse or—even worse—a data breach. Hence preventing them is how we face challenges.

Highlighting the importance of the issue it is explained that security and availability of general cloud services are dependent on the security of these APIs, similarly APIs that aren't designed too well can create lots of issues for cloud so it needs to ensure all APIs are properly fixed. Furthermore, the security and availability of general cloud services are dependent on the security of these APIs. Therefore, to manage these API's are challenging and can affect cloud if poorly designed.

Lack of trained employees as a challenge was also highlighted that finding well trained, experienced and expert employees are difficult to find so it is a challenge for organizations, there is also a risk of data leak due to carelessness of employees. Cloud security is condition with employee's professionalism, and skills it was highly suggested for the organization to hire certified and well trained employees. Other challenges such as breaching, compliance and connectivity were also discussed as challenges by the interview participants.

4.5 Major threats in Cloud Computing

After discussing general challenges some of the biggest and major threats were identified as theme. These challenges are considered most frequent and often easily occurring. According to data results cyber-attack is the largest threat while other threats like Insufficient Access Management, Insecure APIs and Interfaces, Sophisticated Hacking Techniques and System Vulnerability are discussed as well. The frequency of views of respondents can be seen in chart and the table.

4.5.1 Cyber attacks

A lot of things have improved in recent times but currently the biggest threat is security as hackers are getting more and more sophisticated so Cyberattacks nowadays is the biggest threat. Some of participant shared their experience said that

"We have faced cyberattack in 2016. It had lots of consequences".

Nowadays, cyberattacks are increasing in numbers, the situation can be observed in the increased number of frequency of respondent views, and they are more intense in nature and mostly happen to companies.

According to the respondents Data breach is one of the biggest threats on cloud computing where an attack can affect sensitive information such as health, financial, personal identity and other restricted information which can be stolen or misused by an unauthorized user.

4.5.2 Insufficient Access Management

According to data results insufficient access management is consider another major threat to cloud security. It is observed that the cloud storage protection mechanisms mostly provide Authenticated access. While not having the protection mechanism in place, credibility might be threatened.

There are too many reasons which threaten the credibility of cloud. Unauthorized access to customer and business data is the biggest problem nowadays. Furthermore, ignoring the principle of least access privileges, lack of consistent security controls, access falling into wrong hands with regards to sensitive information such as customer's credentials are security threats.

The access control of the users is a huge duty and sadly it's not followed through as it should be,

ACLs have information of users and their level of access and hence maintaining that helps with facing challenges besides infrastructure and data Security also needs to be controlled through the proper implementation security tools and access policies and by restricting sensitive data to approved storage and use Data Loss Prevention (DLP) solutions to enforce these restrictions. However, access control should be maintained very properly by the IT department but even that sometimes lacks some check and balance.

A respondents share his/her view that "In my opinion if your company relies on a third party or someone else to look after their data stored in the cloud, this can be the biggest issue. I'm unsure where this amount of trust comes from, but I advise against it all the time."

As cloud storage protection mechanisms mostly provide Authenticated access so most of the threats easily get mitigated.

4.5.3 Sophisticated Hacking Technique

Another threat posing to the security of cloud storage is sophisticated hacking technique, hackers and their hacking techniques is the most challenging threat in cloud computing

It is noted that hackers are the tiring problem while taking care of cloud security explain their sharpness. It is expressed that they are one step ahead of any technology devised to keep cloud safe, hackers and their skills that grow over time and their software are getting advanced day by day.

Talking about the issues it is also observed that young ambitious hackers are posing sever threats and exploiting the data. There are software and spywares handled by extreme experts to breach cloud. The technology is getting smarter and so are these people. So hackers are the biggest issue nowadays. No matter how secure we make the cloud, there always comes out that one hacker who can bypass it.

4.5.4 System Vulnerability

The issue of System vulnerability is a pertinent threat and cloud providers prefer if you use their predefined template images which can contain vulnerabilities that will be visible/present in all cloud workloads, so vulnerability in the underlying cloud infrastructure is also a significant risk to cloud storage leased by clients.

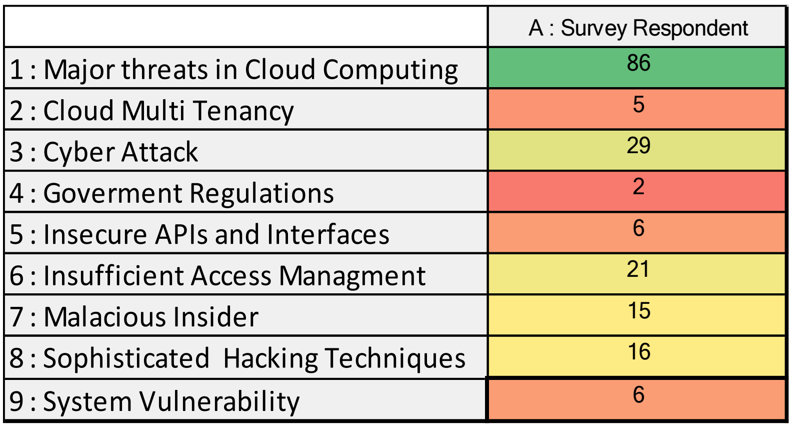
4.5.5 Malicious Insider and Cloud Multi Tenancy

Malicious Insider can also create problems for security, the issue comes from people within the organization, such as employees, business associates, who have inside information concerning the organization's security practices, data and computer systems, so insider threat is believed as the biggest threat to any organization.

Employees who have privileged access have bigger responsibilities. But the principle of least privileges is ignored which in turn creates threats the situation is further deteriorated when data of the organization being leaked or getting in hands of people not allowed by company. Moreover, lack of staff with the skills to secure cloud data and infrastructure or security controls not being implemented as suggested are the existing threats.

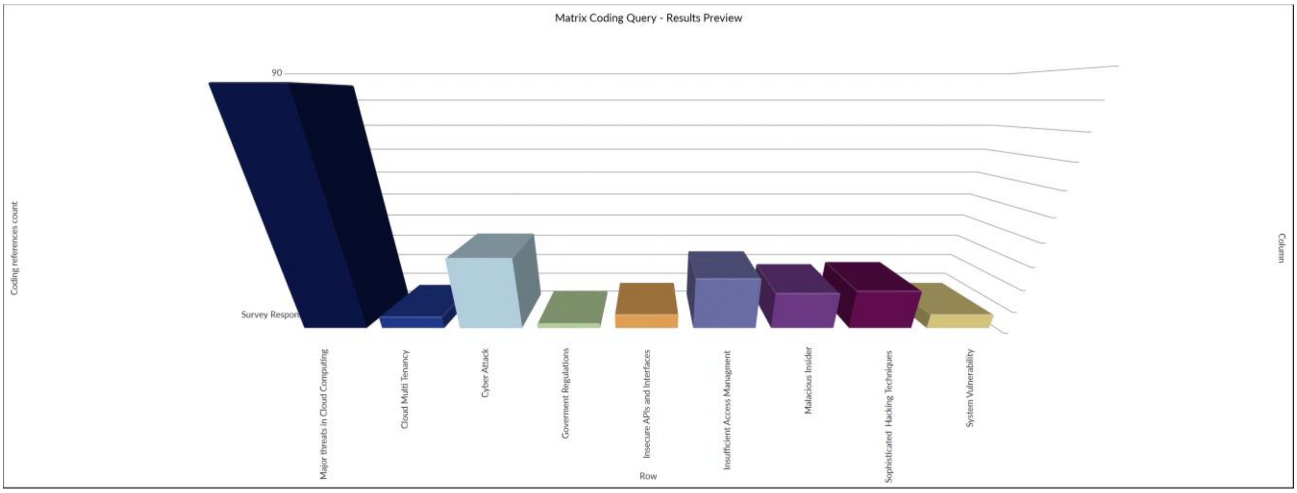
Cloud Multi Tenancy can be understood as a threats that come from people already having access to the cloud. Cloud storage providers don’t build specific servers for each user; the server space is shared between different customers as needed so that can create an issue for security.

Other treats in in this regard like *Government intrusion* and *lacking of standardization* can threaten the cloud, however standardization of policies and rules really manage everything itself for cloud.



	A : Survey Respondent
1 : Major threats in Cloud Computing	86
2 : Cloud Multi Tenancy	5
3 : Cyber Attack	29
4 : Goverment Regulations	2
5 : Insecure APIs and Interfaces	6
6 : Insufficient Access Managment	21
7 : Malacious Insider	15
8 : Sophisticated Hacking Techniques	16
9 : System Vulnerability	6

Table 4-1 Frequencies of Major threats



4.6 Mitigation strategies of Individual and Organizations

Having considerable exchange of views on general and specific threat perception on individual and organizational level, existing mitigation strategies were extensively discussed on individual as well as organizational level. The said strategies and security measures are largely in practice on organizational and individual level. Responses of participants are discussed under the following heading as shown in the map.

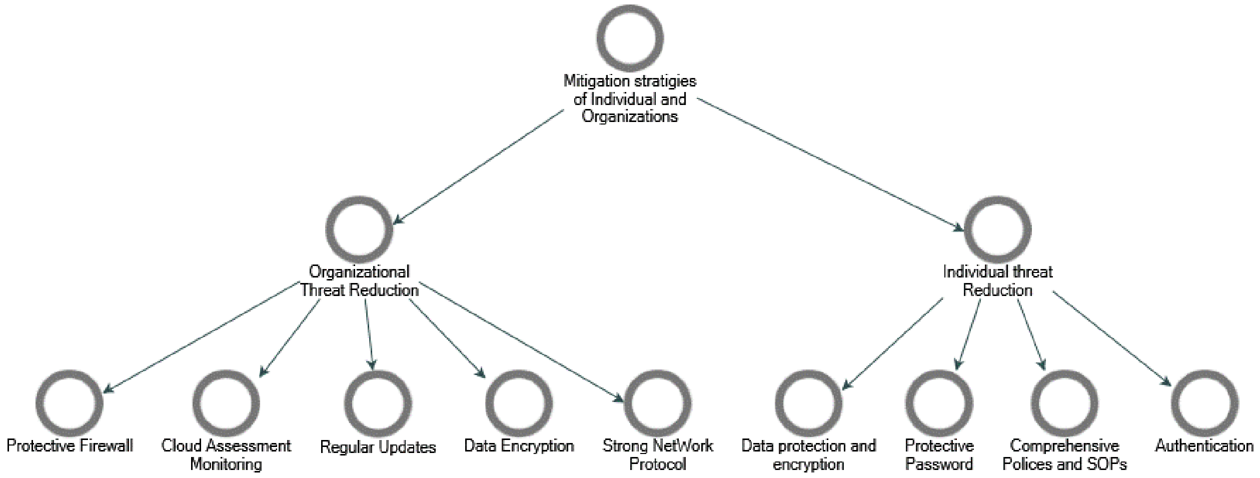

Mitigation stratigies of Individual and Organizations
Organizational Threat Reduction
Individual threat Reduction
Protective Firewall
Cloud Assessment Monitoring
Regular Updates
Data Encryption
Strong NetWork Protocol
Data protection and encryption
Protective Password
Comprehensive Polices and SOPs
Authentication

Figure 4-2 Mitigation Strategies on Individual and Organizational Level

4.6.1 Individual Threat Reduction

On individual level threats reduction and mitigation strategies were discussed under the following heading

4.6.1.1 Data protection and encryption

Data encryption is the cheapest way to secure any data. All data whether it is at rest, not being used or whether it's in transit being sent to someone else. The encryption software is already installed in all the computers in some company.

It is suggested that Individuals, can and should only access tabs and folders which are provided to them whereas management should ensure that data is protected. Sharing of folders (Necessary Folders Only) should be restricted/ tightened in order to ensure the data protection while strong encryption of cloud services and their usage is what individuals can do for starters.

It is further suggested that as an individual we ensure that employee's data is encrypted whether it's saved or in transit. Sharing of folders (Necessary Folders Only) should be restricted/tightened in order to ensure the data protection and individuals should avoid bypassing this. An employee should encrypt their data whether they are using it or not so data encryption is mandatory.

4.6.1.2 Comprehensive Polices and SOPs

Whole set of policies and SOPs are present which should be followed by the department heads and each of their employees. Individuals should read the user agreement to find out how your cloud service storage works, instead of clicking “I accept”. There is a whole guidance book for all procedures which also includes how to request for permission to access data. Individuals should follow that to maintain security. The employees receiving access should go through the company’s SOPs and company's SOP should be strictly followed in order to allow access to employees.

4.6.1.3 Authentication

There are multiple software running on the laptops and PCs of the employees which are duly authenticated for the protection purpose and any changes made to them are authorized by security lead besides it is important that accessing cloud should first get authenticated through proper channels. It is a considered opinion that insider as threats is the biggest issue, so authentication is highly required.

It is also believed that care should be taken during the input which means, to secure the first very step. In the case for cloud security, any employee who is about to get access to the cloud environment, authenticate each user timely and enforce these employees to keep their username and password safe.

Regarding *password security*, the participants shared that there is an IT Security Risk Management (ITSRM) manual in the company. It defines the basic password that is needed to access any application or cloud. I just believe that individuals should follow the password policy mentioned. It is ensured and advised to Use twelve character passwords with special characters like in the policy besides manuals have defined rules to create passwords. Individuals should follow the rules.

Having an IT security risk and management manual with policies for passwords is highly recommended so individuals can follow basic policies to help secure the password.

4.6.2 Organizational Threat Reduction

Measurements that are taken under consideration on organizational level as discussed in the table are under the following headings.

4.6.2.1 Cloud Assessment Monitoring

Organizations have to make sure and analyze information that will access their data services (abnormal users' patterns) to avoid data breach.

Before adding the cloud services to an organization, it is very important for cloud assessment to occur and find the risks.

Implementation of incident reporting system is one way some companies are working on in order to allow all users to be able to report threats. Surveillance network is the practice that is followed in some organization while CASA is the reporting system for various types of incidents besides IRS named SOR is used at some companies. Some organization takes security threats very seriously. For that very purpose, it is believed that before adding the cloud service, cloud assessment should be performed to evaluate the risks and mitigate them timely. Once again, secure the input, it brings the best output.

4.6.2.2 Protective Firewall

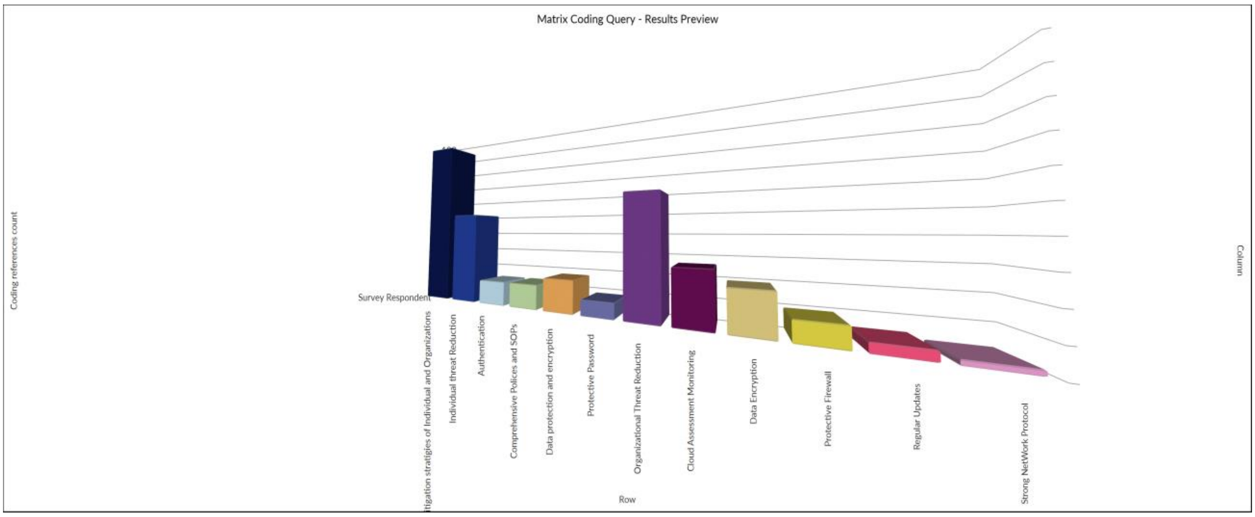
Many organizations have a firewall installed. They monitor and control all kinds of traffic as well to ensure safety. Installation of network firewall and implementation of security control on all network devices for monitoring and controlling inbound and outbound traffic is sufficient to handle the threats.

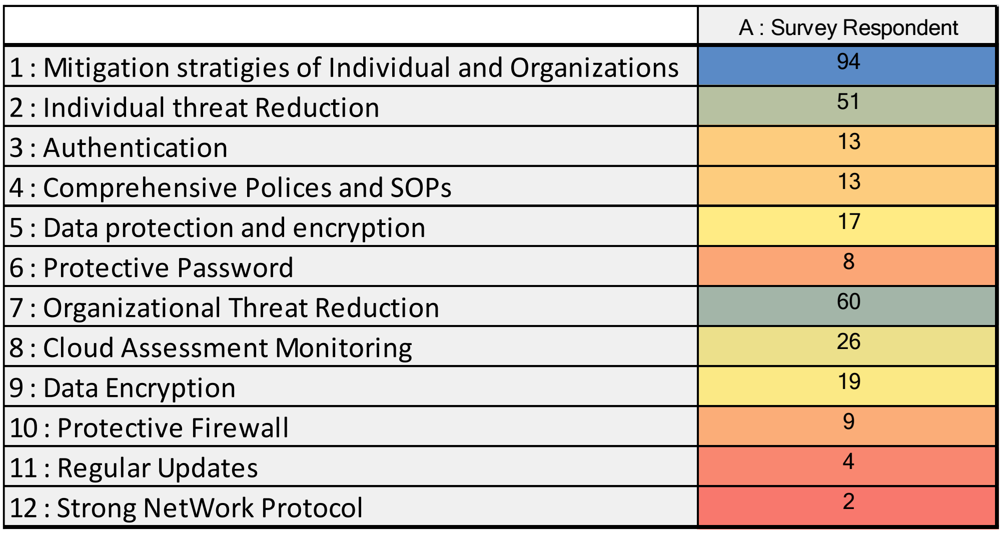
Few organizations take security threats very seriously. For that very purpose, they have always suggested and ensured that cloud is only being used for general purposes, for all functions that do not include anything sensitive. Whereas it is also recommended to have a local facility built up in a separate room which should only be utilized for sensitive data.

4.6.2.3 Regular Updates

Regular vulnerability patching and monitoring are important steps taken by organization while a network which is always under check and balance. Some organizations follow two main practices, one being constant patching of any issues found and monitoring throughout the month is also a best practice. Other measurements like strong network protocol and data encryption are also some measures as some respondents shared that for security, we implement SSH (Secure Shell) and reverse SSH, for connectivity and reliability we rely on good service providers like AWS.

Further it is suggested that choosing a cloud service, whether it's an IaaS, PaaS, or SaaS solution, it's important to check the user access controls that come with the solution.





	A : Survey Respondent
1 : Mitigation stratigies of Individual and Organizations	94
2 : Individual threat Reduction	51
3 : Authentication	13
4 : Comprehensive Polices and SOPs	13
5 : Data protection and encryption	17
6 : Protective Password	8
7 : Organizational Threat Reduction	60
8 : Cloud Assessment Monitoring	26
9 : Data Encryption	19
10 : Protective Firewall	9
11 : Regular Updates	4
12 : Strong NetWork Protocol	2

4.7 Suggested Security Measures on Individual Level

Finally, respondents put forward some security measures that could manage data breach and cloud vulnerability in organizational as well as individual level besides individual efforts that can enhance the security of the cloud are also widely discussed. Themes have been extracted from data which enlighten us about the security measures on individual level are Access Control, Encrypted Storage, Data Masking, Automated Update and Anti Malware.

4.7.1 Access Control

On individual level access control is mostly discuss by the respondents during the study. It is suggested that Access control on all types of data should be implemented and employees who are duly authorized should be able to access them with limits implemented on their profiles similarly read and write profiles for tables and columns should be defined separately. While ensuring that access is applied to control data and access is given to upper management mostly is very fruitful in this regard.

According to some respondents the efforts are not sufficient when they say that individuals can do a lot but do nothing at the same time. Hence, it is believed that as the cloud security team, it should ensure at our part that individuals are securing the cloud. Some team member's asserts that they define separate read and write profiles for databases, tables and columns, scanning and monitoring of cloud. This ensures that data on the cloud is heavily protected.

In a nutshell access control should be implemented on data and sensitive data should only be given to employees who are duly authorized.

4.7.2 Encrypted Storage

Secondly encrypted storage is also considered an important step to enhance security of the cloud hence encrypting sensitive data is one of the most effective method to secure the data on cloud so the sensitive details should be kept on local storage available physically instead of cloud. Furthermore, encryption of storage is the most preferred option for the organization's cloud workloads

4.7.3 Data Masking

Data masking is another helpful remedy for protection of cloud security. The study suggests that Data masking should be performed by all individuals however you must ensure that database supports it well enough. Besides, data masking is taught to employees during trainings while other respondents reported that just employing data masking is pretty helpful and easy.

4.7.4 Anti-Malware

Performing regular backups of sensitive data and using anti-viruses or firewalls can protect data on cloud from security threats. It is considered that no matter how much secure the data is on cloud, it will still be at a huge risk of getting infected by malware. Therefore, using Anti-spy or anti-virus can help protect the sensitive resources on cloud. It is suggested that Approved Anti-Virus systems "Symantec End Point Protection" should be installed on all the servers.

4.7.5 Automated Update

Maintenance of cloud servers is very important to protect resources on Cloud. Download latest security updates on operating system and automate updates so system could be automatically updated to defend any security risk. Moreover, automate software updates and regular scan your cloud servers. Lastly, maintaining strong configuration management with frequent and automated scanning of templates, and hardening the default images is one way individuals can help in protection of data on cloud.

4.8 Suggested Security Measures on organizational level

Security measures proposed in this for organizational level security are very pertinent some handful points come forward from the views of the respondents. The suggestions were categorized in the following themes with respect to the intensity of the frequency of the coded views.

4.8.1 Secure software Interface

Most effective thing is the detailed implementation of strong API access control. Usage of a good and decent security model of software interfaces can save the cloud from lots of vulnerabilities similarly two-factor authentication is a very useful tool to secure anything, even access to cloud. There are standardized API frameworks available. Their usage helps manage the vulnerabilities

4.8.2 Limited Access

Organizations must restrict access to data and maintain adherence to industry standards and compliance besides access is to be given to individuals on certain protocols namely need-to-know and need-to-access.

Strong authentication methods and limited access of most people along with encrypted transmission should be practiced. Similarly, it is important to disable all other user accounts (later on after the system gets fixed, enable these user accounts, change their passwords and create new user profiles).

4.8.3 Data Analysis

Some suggestions put forward regarding analysis of the data in order to protect the cloud storage so it is considered that analysis of data protection during run time is extremely important while some suggested that during run time, data protection should be analyzed and evaluated.

It is believed that ensuring the input is correct and has worked like a charm. So, in this case as well, while one is designing and running the cloud, the data is analyzed for maximum protection. If the data being input in the organization is free from malwares or spywares, cloud will no longer be vulnerable.

4.8.4 Algorithm Implementation

Focusing on promoting cloud security some respondent thought that most effective thing is the detailed implementation of strong API access control. Teams required for performing detailed penetration testing, strong implementation and good algorithms of hashing for data protection.

4.8.5 User Knowledge transfer

Keeping in view the challenge of unaware customer the participants suggested to conduct trainings and provide self-reading manuals to all the users of cloud to understand the importance of security for cloud and its safety. Security awareness should be provided to contractors, employs and third-party users and everyone else involved.

4.9 Miscellaneous suggestions

Some ideas shared by respondents during interviews other than coded themes are also worth adding to the study.

- Infrastructure and data Security also needs to be controlled through the proper implementation security tools and access policies and by restricting sensitive data to approved storage and use Data Loss Prevention (DLP) solutions to enforce these restrictions

- All the victims of a breach should be informed timely however they can backlash through lawyers and suing us
- There are multiple challenges faced when we are ensuring security of the cloud. However, the main problems we face usually are with authentication. Employees are not careful at all when it comes to their ID and passwords. Also, access control should be maintained very properly by the IT department but even that sometimes lacks some check and balance.
- In few companies, integration of cloud with other cloud service provider's help ease the burden.
- Challenges can be eliminated by simple authentication process and ensuring access control.
- It is always recommended and preferred that experienced individuals should be added to the cloud team.
- An individual can follow the process of hiding original data with modified content.
- Data should be controlled and given to authorize personnel only.
- Specific Users should be able to access the systems while protecting the integrity and security of the system
- It is strongly discouraged to use the web browsing on any of the live application system if it becomes unavoidable (in some circumstances to test/verify the application locally) than never respond to pop-up windows.

Chapter 5: Conclusion and Future Work

5.1 Overview of the chapter

This chapter illustrates the summary of the study and suggests recommendations for successful implementation of cloud services in Pakistan along with the management and mitigation of cyber threats it poses. It also explains the future direction and limitations of the current study.

5.2 The conclusion of Study

This study has examined fully as to how beneficial cloud is however it poses cyber threats no matter how much security is implemented throughout the organizations. The primary data for this study was collected through semi-structured interviews from cloud security management team of the organizations who have the responsibility of securing the cloud environments. The companies included medium and small sized industries. The results showed that cloud's implementation has proven to be great regardless of the threats it poses.

Research was conducted to gather the data from security team and those who are directly involved in cloud server management of the organizations. Several issues were highlighted such as lack of skilled labor who understand and can tackle the cloud server, uneducated manpower, along with integration of cloud with any other cloud service provider, troubleshooting connectivity issue, such as ping command that does not exist in many service providers and most importantly privacy and security issues.

This research contributes to the positives of cloud implementation in an organization and it proves that companies can take full advantage of the benefits of cloud has to offer along with managing cyber threats and vulnerabilities of data on cloud: best practices and mitigation strategies and this research will help managers and CEO's to better understand the success factors and challenges in the way of cloud implementation. The threats being faced by cloud is just not focused to Pakistan, it is an issue being faced all over the world, yet they are still manageable and fixable.

5.3 Recommendations

The study presented several recommendations for successful implementation of cloud. It is rather a new concept or foreign concept in Pakistan for now. First step is to give awareness to people regarding what cloud servers are and what threats can be faced after its implementation. Once people understand the concept, they will be compelled to implement the safety measures to protect the data in cloud. The biggest flaw in Pakistan is that trainers are hired that they give lectures or presentations and then leave. On-field trainers should be brought in that know how to actually implement safety measures, what one must do in case of a breach, how to report a potential breach and such necessary actions.

Further recommendations that a company may take were building the local facility for sensitive data, using cloud for general purposes, installation of network firewall and implementation of security control on all network devices for monitoring and controlling inbound and outbound traffic, regular vulnerability patching and monitoring, implementation of incident reporting system, no personal device connectivity to local LAN by physical protection measures on all official's network and edge devices, surveillance network, building up the secure usage procedure and implementation of encryption for communication. Secondly encrypted storage is also considered an important step to enhance security of the cloud hence encrypting sensitive data is one of the most effective method to secure the data on cloud so the sensitive details should be kept on local storage available physically instead of cloud. Furthermore, encryption of storage is the most preferred option for the organization's cloud workloads. Also, performing regular backups of sensitive data and using anti-viruses or firewalls can protect data on cloud from security threats. It is considered that no matter how much secure the data is on cloud, it will still be at a huge risk of getting infected by malware. Therefore, using Anti-spy or anti-virus can help protect the sensitive resources on cloud. It is suggested that Approved Anti-Virus systems "Symantec End Point Protection" should be installed on all the servers.

More recommendations in order to protect data on cloud were to always harden the default images once they are employed, always prefer encrypted storage option for your workloads, always prefer to keep legally privileged data (i.e. account numbers, credit card info etc.) on premise storage, employ access control on data (i.e. specific tables, or certain columns of table) only for authorized personnel only, define separate read and write profiles for databases, tables, columns etc. and employ data masking if the database supports it.

As mentioned above, individuals should be trained and controlled by IT to ensure cloud is secure on their part such as encrypt both data at rest and data on transit, apply passwords policies, apply access policies, sharing of folders (necessary folders only) should be restricted/tightened in order to make sure the data is protected, use of DLP (data loss prevention software), regular data backups, authenticate all people accessing the network, authenticate all software deployed on the machines and all changes to such software, formalize the process of requesting permission to access data or applications and log all user activity and program activity, also analyze the actions for unexpected behavior.

Lastly, for readers of this research, general overview of the security practices as recommended by professionals whom we conducted interviews with include AWS security groups, system's firewalls, server's users and groups, antivirus systems (Symantec Endpoint Protection) and security systems (Trend Micro or Sophos etc.) should be used for security hardening, specific users should be able to access the systems while protecting the integrity and security of the systems, these users should only be granted with minimum access needed to accomplish the particular task, the users under special cases be allowed to place the "approved executable" on the servers, users access should be logged, rules should be configured to control the inbound traffic of instances and a separate set of rules are configured that control the outbound traffic, for public access address range(s) should be configured and only allowed destination range(s) should be added in the white listings and rest of the world is blocked, firewall configurations should be backed up and stored in a secure location and firewall rules should be reviewed on a weekly basis.

5.4 Study Limitations

There are some limitations also associated with this study. The collected data should be taken with caution because few interviews conducted for this research cannot represent opinions, issues and recommendation of the entire population. Moreover, the research is limited to organizations located in Islamabad.

This research uses interview technique for data collection. The issue this year regarding interviews was the pandemic situation due to Covid-19 and the lockdown for which interviews were taken in restricted time and with proper covid-19 precautions. Few interviews were one to one whereas majority interviews were taken on calls.

One more issue regarding interview method on call is that interviewers may understand questions differently and transcribe questions in their own ways. An interviewee can be biased on their views. And lastly, due to time constraints, fewer numbers of companies and interviewees were considered.

5.5 Future Work

This research has considered organizations based in Islamabad whereas future research can target other cities and foreign countries. Results of different organizations based in different cities/countries can provide more detailed understanding of cloud threats and vulnerabilities. Researchers may even create a questionnaire based on this research and conduct qualitative analysis and compare results with ease. This research only considered medium to low level organizations. Future research can include more High-level organizations. This research uses interview method; future research can use data collection techniques which qualitative research methods allow. Further research can consider higher number of interviews for more detailed results for the research.

References

[1] Peter Mell, and Tim Grance, “The NIST Definition of Cloud Computing,” Version 15, 10-7-09, http://www.wheresmyserver.co.nz/ storage/media/faq-files/cloud-def-v15.pdf.

[2] Musa, F. A. and Sani, S. M. (2016) ‘Security Threats and Countermeasures In Cloud Computing’, International Research Journal of Electronics & Computer Engineering, 24.

[3] Liu, Y. et al. (2015) ‘A Survey of Security and Privacy Challenges in Cloud Computing: Solutions and Future Directions’, Journal of Computing Science and Engineering, 9(3), pp. 119–133. doi: 10.5626/JCSE.2015.9.3.119.

[4] B.R. Kandukuri, VR Paturi, and A. Rakshit.Cloud security issues.In Services Computing, 2009.SCC'09. IEEE International Conference on, pages517-520, 2009

[5] Goran Novkovic “Five characteristics of cloud computing” https://www.controleng.com/articles/five-characteristics-of-cloud-computing/

[6] P.S. Suryateja (2018) “Threats and Vulnerabilities of Cloud Computing: A Review”, International Journal of Computer Sciences and Engineering, Volume-6, Issue-3, E-ISSN: 2347-2693.

[7] Sugandh Bhatia and Rajinder S. Virk, “Cloud Computing Security, Privacy And Forensics: Issues And Challenges Ahead”, International Journal of Research Trends in Engineering and Research, Volume 04, Issue 03; March - 2018 [ISSN: 2455-1457]

[8] Muhammad Aamir Nadeem, “Cloud Computing: Security Issues and Challenges”, Journal of Wireless Communications 1 (1): 10-15, 2016 | https ://lsp.institute [ISSN: 2377-3308]

[9] LufungulaOsembe, “A Review of Security Challenges in Cloud Computing Adoption: A Conceptual Framework on Early Adopters of Cloud Computing as a Technology Model”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 7, Issue 5, May 2017 [ISSN: 2277 128X]

[10] Kumar, R., & Goyal, R. (2019). On cloud security requirements, threats, vulnerabilities and countermeasures: A survey. Computer Science Review, 33, 1–48. doi: 10.1016/j.cosrev.2019.05.002

[11] Kumar Patel, Antonina Alabisi, “Cloud Computing Security Risks: Identification and Assessment”, Journal of New Business Ideas & Trends Vol. 17 Iss.2, September 2019, pp. 11-19.

[12] Nalini Subramanian, Andrews Jeyaraj, “Recent security challenges in cloud computing”, Computers and Electrical Engineering 71 (2018) 28–42

[13] Naseer Amara, Huang Zhiqui, Awais Ali, “Cloud Computing Security Threats and Attacks with their Mitigation Techniques”, 2017 International Conference on Cyber-Enabled

Distributed Computing and Knowledge Discovery 978-1-5386-2209-4/17 $31.00 © 2017 IEEE DOI 10.1109/CyberC.2017.37.

[14] Tarek Radwan, Marianne A. Azer, Nashwa Abdelbaki, "Cloud computing security: challenges and future trends" Int. J. Computer Applications in Technology, Vol. 55, No. 2, 2017

[15] https://phoenixnap.com/blog/cloud-security-threats-and-risks

[16] Hong, J. B., Nhlabatsi, A., Kim, D. S., Hussein, A., Fetais, N., & Khan, K. M. (2018). Systematic Identification of Threats in the Cloud: A Survey. Computer Networks. doi:10.1016/j.comnet.2018.12.009

[17] Anjana, & Singh, A. (2018). *Security concerns and countermeasures in cloud computing: a qualitative analysis. International Journal of Information Technology.* doi:10.1007/s41870-018-0108-1

[18] Rath, A., Spasic, B., Boucart, N., &Thiran, P. (2019). *Security Pattern for Cloud SaaS: From System and Data Security to Privacy Case Study in AWS and Azure. Computers, 8(2), 34.* doi:10.3390/computers8020034

[19] Neupane, R. L., Neely, T., Calyam, P., Chettri, N., Vassell, M., &Durairajan, R. (2018). Intelligent defense using pretense against targeted attacks in cloud platforms.Future Generation Computer Systems. doi:10.1016/j.future.2018.10.004

[20] Domingo-Ferrer, J., Farràs, O., Ribes-González, J., & Sánchez, D. (2019). *Privacy-preserving cloud computing on sensitive data: A survey of methods, products and challenges. Computer Communications, 140-141, 38–60.* doi:10.1016/j.comcom.2019.04.011

[21] Zeng, W., &Germanos, V. (2019). Benefit and Cost of Cloud Computing Security. 2019 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI). doi:10.1109/smartworld-uic-atc-scalcom-iop-sci.2019.00093

[22] R. Wang. (2017) "Research on Data Security Technology Based On Cloud Storage," Procedia Eng. 174: 1340–1355.

[23] Q. N. Naveed and N. Ahmad. (2019) Critical Success Factors (CSFs) for Cloud-Based. pp. 140–149.

[24] A. D. Kozlov, and N. L. Noga.(2018) "Risk Management for Information Security of Corporate Information Systems Using Cloud Technology," Elev. Int. Conf. Management large-scale Syst. Dev. (MLSD). pp. 1–5.

[25] D. Chen and H. Zhao, "Data Security and Privacy Protection Issues in Cloud Computing", Tarjomefa.com, 2020. [Online]. Available: https://tarjomefa.com/wp-content/uploads/2017/07/7186-English-TarjomeFa.pdf. [Accessed: 27- Apr- 2020].

[26] N. Chandramouli, B. Manjula , "A Study on Data Security and Privacy Protection Issues in Cloud Computing," International Journal of Computer Sciences and Engineering, Vol.5, Issue.9, pp.164-170, 2017.

[27] M. Nadeem, "Cloud Computing: Security Issues and Challenges", Journal of Wireless Communications, vol. 1, no. 1, 2016. Available: 10.21174/jowc.v1i1.73 [Accessed 28 April 2020].

[28] Anjana and A. Singh, "Security concerns and countermeasures in cloud computing: a qualitative analysis", International Journal of Information Technology, vol. 11, no. 4, pp. 683-690, 2018. Available: 10.1007/s41870-018-0108-1 [Accessed 28 April 2020].

[29] Creswell, J. W. (2013). Qualitative Inquiry & Research Design: Choosing among Five Approaches (3rd ed.). Thousand Oaks, CA: SAGE.

[30] Tanweer Alam (2020) "Cloud Computing and its role in the Information Technology", IAIC Transactions on Sustainable Digital Innovation (ITSDI) p-ISSN: 2686-6285 Vol. 1 No. 2 April 2020.

[31] Narendra Rao Tadapaneni, "Cloud Computing Security Challenges", Novateur Publications International Journal Of Innovations In Engineering Research And Technology [Ijiert] Issn: 2394-3696 Volume 7, Issue 6, June-2020.

Appendix A: Cloud Security Manager Questionnaire.

1. Are you aware of the security related vulnerabilities and threats in cloud computing?
2. How are the challenges faced in cloud security?
3. What threatens the credibility of Cloud storage?
4. Cloud computing services take care of your data in a cloud environment. What can you do as an individual to secure your online data?
5. What are the best practices / strategies followed by your organization to handle the security related threats?
6. What are the steps taken to handle security related cloud challenges?
7. What are the practices or guidelines that can enhance security in cloud computing?
8. What do you think is the biggest security threat of the Cloud?
9. How data breaches and cloud vulnerabilities are managed by organizations?
10. What can we do as an individual to protect our data on cloud?

Turnitin *Originality Report*

- Processed on: 09-Mar-2021 19:57 PKT
- ID: 1528388328
- Word Count: 21115
- Submitted: 1

Cyber *by Hafeez Asma*

Similarity Index

12%

Similarity by Source

Internet Sources:

10%

Publications:

6%

Student Papers:

8%

1% match (student papers from 05-Oct-2020)

Submitted to Indiana University on 2020-10-05

< 1% match (Internet from 14-Jul-2020)

https://www.javatpoint.com/cloud-service-models

< 1% match (Internet from 19-Aug-2014)

http://torchlms.com/learning-technology/benefits-of-software-as-a-service/

< 1% match (Internet from 01-Dec-2019)

https://cloudsecurityalliance.org/download/artifacts/top-threats-to-cloud-computing-egregious-eleven/

< 1% match (Internet from 02-Jul-2018)

https://www.diva-portal.org/smash/get/diva2:830115/FULLTEXT01.pdf

< 1% match (Internet from 29-Jun-2020)

https://www.coursehero.com/file/26777905/02CloudComputingpdf/

< 1% match (Internet from 02-Dec-2020)

https://wire19.com/10-biggest-threats-to-cloud-computing-2019-report/

< 1% match (student papers from 23-Jun-2020)

Submitted to Christchurch Polytechnic Institute of Technology on 2020-06-23

< 1% match (student papers from 21-Oct-2020)

Submitted to Bridgepoint Education on 2020-10-21

< 1% match (Internet from 11-Jun-2020)

https://www.richtmann.org/journal/index.php/ajis/article/download/10668/10290

< 1% match (student papers from 11-Jan-2013)

Submitted to London School of Business and Finance on 2013-01-11

< 1% match (Internet from 11-Dec-2018)

http://paper.ijcsns.org/07_book/201805/20180522.pdf

< 1% match (student papers from 18-Feb-2021)

Submitted to Liberty University on 2021-02-18

< 1% match (student papers from 13-Sep-2019)

Submitted to Study Group Australia on 2019-09-13

< 1% match (student papers from 04-Oct-2020)

Submitted to Victorian Institute of Technology on 2020-10-04

< 1% match (Internet from 20-Feb-2021)

https://www.secureworldexpo.com/industry-news/4-types-cloud-security-vulnerability-mitigation

< 1% match (student papers from 26-Sep-2011)

Submitted to Napier University on 2011-09-26

< 1% match (Internet from 04-Jul-2020)

https://www.ijiert.org/admin/papers/1591100560_Volume%207,%20Issue%206.pdf

< 1% match (student papers from 10-Nov-2014)

Submitted to VIT University on 2014-11-10

< 1% match (Internet from 24-Jul-2017)

https://sispress.org/journals/jowc/article/download/73/33

< 1% match (Internet from 19-Sep-2020)

https://www.ijcseonline.org/full_paper_view.php?paper_id=1449

< 1% match (student papers from 10-Oct-2020)

Submitted to Study Group Australia on 2020-10-10

< 1% match (student papers from 23-May-2010)

Submitted to Strayer University on 2010-05-23

< 1% match (student papers from 07-Jun-2017)

Submitted to Higher Education Commission Pakistan on 2017-06-07

< 1% match (Internet from 05-Sep-2017)

https://ijarcsse.com/docs/papers/Volume_7/5_May2017/SV7I5-0176.pdf

< 1% match ()

https://nsuworks.nova.edu/shss_dft_etd/46

< 1% match (Internet from 04-Oct-2020)

https://www.researchgate.net/publication/322408253_Cloud_Computing_Security_Threats_and_Attacks_with_Their_Mitigation_Techniques

< 1% match (Internet from 12-Dec-2020)

https://www.compuquip.com/blog/cloud-security-challenges-and-risks

< 1% match (Internet from 09-Dec-2019)

https://repository.nwu.ac.za/bitstream/handle/10394/33735/13126539%20Kumar%20R.pdf?isAllowed=y&sequence=1

< 1% match (student papers from 18-Jan-2021)

Submitted to Chester College of Higher Education on 2021-01-18

< 1% match (student papers from 15-Jun-2019)

Submitted to Ghana Technology University College on 2019-06-15

< 1% match (publications)

Tariq Ahanger, Abdullah Aljumah. "Cyber Security Threats, Challenges and Defense mechanisms in Cloud Computing", IET Communications, 2020

< 1% match (student papers from 07-Jan-2016)

Submitted to University of West London on 2016-01-07

< 1% match (Internet from 27-Dec-2014)

http://ijater.com/Files/686bc66b-692f-43a2-aea3-742fed64655e_ICETT_01_02.pdf

< 1% match ()

http://etd.uum.edu.my/4604/

< 1% match (student papers from 28-Apr-2019)

Submitted to Victorian Institute of Technology on 2019-04-28

< 1% match (student papers from 13-Nov-2020)

Submitted to Macquarie University on 2020-11-13

< 1% match (student papers from 11-Oct-2018)

Submitted to University of Johannsburg on 2018-10-11

< 1% match (Internet from 23-Feb-2021)

https://dokumen.pub/intelligent-systems-design-and-applications-16th-international-conference-on-intelligent-systems-design-and-applications-isda-

2016-held-in-porto-systems-and-computing-557-band-557-1st-ed-2017-9783319534794-3319534793.html

< 1% match (student papers from 22-Aug-2020)

Submitted to Study Group Australia on 2020-08-22

< 1% match (Internet from 09-Dec-2017)

http://ijarcs.info/si/Complete%20Issue.pdf

< 1% match (Internet from 06-Nov-2012)

http://liujintao.iwebs.ws/researchmethod.pdf

< 1% match (student papers from 30-May-2019)

Submitted to University of Sydney on 2019-05-30

< 1% match (student papers from 10-Dec-2019)

Submitted to CSU, Bakersfield on 2019-12-10

< 1% match (student papers from 21-Dec-2020)

Submitted to Ivy Tech Community College Central Office on 2020-12-21

< 1% match ()

http://etheses.whiterose.ac.uk/13677/

< 1% match (Internet from 24-Feb-2015)

http://hufee.meraka.org.za/Hufeesite/staff/the-hufee-group/paula-kotze-1/mariana-carroll-phd-thesis

< 1% match (Internet from 02-Mar-2021)

https://solutionsreview.com/cloud-platforms/7-cloud-storage-security-risks-you-need-to-know-about/#:~:text=%207%20Cloud%20Storage%20Security%20Risks%20You%20Need,o

< 1% match (Internet from 12-Nov-2020)

https://tutorsonspot.com/questions/bi-week-2-assignment-t5oj/

< 1% match (Internet from 14-Nov-2020)

https://ir.lib.nchu.edu.tw/handle/11455/21788?mode=full

< 1% match (Internet from 09-Apr-2020)

http://sersc.org/journals/index.php/IJCA/article/download/8395/4760/

< 1% match (Internet from 31-Oct-2020)

https://core.ac.uk/download/pdf/188769876.pdf

< 1% match (student papers from 10-Jan-2020)

Submitted to De Montfort University on 2020-01-10

< 1% match (Internet from 01-Apr-2020)

https://www.tandfonline.com/doi/full/10.1080/15267431.2019.1623220

< 1% match (Internet from 24-Feb-2019)

https://www.ijrter.com/papers/volume-4/issue-3/cloud-computing-security-privacy-and-forensics-issues-and-challenges-ahead.pdf

< 1% match (Internet from 28-Feb-2021)

https://www.ekransystem.com/en/blog/insider-threat-definition

< 1% match (Internet from 27-Feb-2017)

https://www.scribd.com/doc/287048738/Essentials-of-Cloud-Computing

< 1% match (Internet from 20-Aug-2020)

https://mafiadoc.com/business-information-management-and-the-cloud_5a1370951723dd586439beff.html

< 1% match (Internet from 09-Oct-2020)

https://cps-vo.org/book/export/html/12397

< 1% match (Internet from 09-Jan-2016)

http://www.itforce.ie/cloud-computing/benefits-of-cloud-computing/

< 1% match (publications)

Chellammal Surianarayanan, Pethuru Raj Chelliah. "Essentials of Cloud Computing", Springer Science and Business Media LLC, 2019

< 1% match (student papers from 05-Sep-2020)

Submitted to Middle East Technical University on 2020-09-05

< 1% match (student papers from 18-Mar-2019)

Submitted to Northern Melbourne Institute of TAFE on 2019-03-18

< 1% match (Internet from 11-Mar-2016)

https://ediss.uni-goettingen.de/bitstream/handle/11858/00-1735-0000-0022-605F-2/thesis1.pdf?sequence=1

< 1% match (Internet from 17-Feb-2021)

http://ijcttjournal.org/archives/ijctt-v57p111

< 1% match (publications)

Pradeep Kumar Tiwari, Sandeep Joshi. "A review of data security and privacy issues over SaaS", 2014 IEEE International Conference on Computational Intelligence and Computing Research, 2014

< 1% match (student papers from 23-Nov-2020)

Submitted to Royal Holloway and Bedford New College on 2020-11-23

< 1% match (Internet from 16-Feb-2020)

https://www.yumpu.com/en/document/view/2228020/mourning-rituals-and-practices-in-contemporary-

< 1% match (publications)

Maniah, Edi Abdurachman, Ford Lumban Gaol, Benfano Soewito. "Survey on Threats and Risks in the Cloud Computing Environment", Procedia Computer Science, 2019

< 1% match (student papers from 28-Nov-2020)

Submitted to Australian College of Business and Technology on 2020-11-28

< 1% match (student papers from 26-Dec-2011)

Submitted to Universiti Teknikal Malaysia Melaka on 2011-12-26

< 1% match (Internet from 13-Oct-2020)

https://www.ijcseonline.org/full_paper_view.php?paper_id=1799

< 1% match (Internet from 15-Aug-2018)

http://www.ijana.in/papers/V7I6-1.pdf

< 1% match (student papers from 02-Aug-2011)

Submitted to ABRS International Information and Consultancy on 2011-08-02

< 1% match (Internet from 03-Mar-2021)

https://www.cio.com/article/2380182/5-tips-to-keep-your-data-secure-on-the-cloud.html

< 1% match (student papers from 04-Nov-2020)

Submitted to South Bank University on 2020-11-04

< 1% match (student papers from 01-Dec-2020)

Submitted to Jacksonville State University on 2020-12-01

< 1% match ()

https://aptikom-journal.id/index.php/itsdi/article/view/103

< 1% match (Internet from 06-Dec-2020)

https://researchportal.northumbria.ac.uk/en/publications/using-computer-assisted-qualitative-data-analysis-software-caqdas-nvivo-to-assist-in-the-complex-process-of-realist-theory-generation-refinement-and-testing(172bae23-a210-45a4-91de-8940a442f623).html

< 1% match (publications)

Mohammed M. Alani. "Elements of Cloud Computing Security", Springer Science and Business Media LLC, 2016

< 1% match (Internet from 12-Nov-2020)

https://www2.slideshare.net/Agarwaljay/cloud-computing-simple-ppt-41561620

< 1% match (Internet from 03-Nov-2018)

https://eprints.soton.ac.uk/424740/1/EBRAHIM_Final_Thesis_22_7_18_PDF_1_.pdf

< 1% match (Internet from 08-Feb-2021)

https://pepper-mt.oise.utoronto.ca/data/note/715281/creswell_Qualitative_Inquiry_2nd_edition.pdf

< 1% match (Internet from 20-Jul-2016)

http://www.go4hosting.in/forum/viewtopic.php?f=8&sid=e913100d9bfd04eeb86a4fe4cdefd106&t=23435

< 1% match (Internet from 10-Aug-2020)

http://www.freepatentsonline.com/10489420.html

< 1% match (Internet from 06-Oct-2019)

http://www.conscientiabeam.com/pdf-files/eco/62/IJBEM-2019-6(4)-232-247.pdf

< 1% match (Internet from 18-Jul-2020)

https://mafiadoc.com/data-security-and-privacy-protection-issues-in-cloud-computing_5c5c1d45097c47075e8b46d3.html

< 1% match (Internet from 15-Apr-2018)

http://docplayer.net/8691723-Security-in-cloud-computing.html

< 1% match (Internet from 05-Feb-2019)

https://eprints.soton.ac.uk/419480/1/Final_thesis_after_corrections2.pdf

< 1% match (Internet from 21-Jul-2020)

https://scholarworks.waldenu.edu/cgi/viewcontent.cgi?article=2786&context=dissertations&httpsredir=1&referer=

< 1% match (Internet from 03-Jul-2020)

http://dspace.bu.ac.th/jspui/bitstream/123456789/4339/1/Yanfang%20Liu.pdf

< 1% match (publications)

Hamed Tabrizchi, Marjan Kuchaki Rafsanjani. "A survey on security challenges in cloud computing: issues, threats, and solutions", The Journal of Supercomputing, 2020

< 1% match (publications)

Jamaludin Jamaludin, Romindo Romindo. "Hybrid Cryptosystem Analysis by Using The Combination of Vigenere Cipher and RSA for Text Security", Proceeding on International Conference of Science Management Art Research Technology, 2020

< 1% match (Internet from 24-Mar-2015)

http://dsresearchcenter.net/PDF/V2_I5/07.pdf

< 1% match (Internet from 27-Sep-2020)

https://cwww.intechopen.com/books/cells-of-the-immune-system/introductory-chapter-development-of-neutrophils-and-their-role-in-hematopoietic-microenvironment-reg

< 1% match (Internet from 26-Feb-2021)

https://trueinfluence.com/timc-topic-dictionary/

< 1% match (Internet from 22-Jan-2021)

https://researchers.uq.edu.au/researcher/23703

< 1% match (publications)

De, Debashis. "Cloud Computing", Mobile Cloud Computing, 2016.

< 1% match ()

https://research.brighton.ac.uk/en/studentTheses/53c11a93-3d8d-4cbe-82df-deb34be6ab1f

< 1% match (Internet from 25-Aug-2020)

http://docplayer.net/13762783-Secure-virtual-machine-migration-in-cloud-data-centers.html

< 1% match (Internet from 09-Jan-2020)

http://docplayer.net/16429160-Top-threats-in-cloud-computing.html

< 1% match (Internet from 22-Mar-2016)

http://www.ijarcsse.com/docs/papers/Volume_3/11_November2013/V3I11-0211.pdf

< 1% match (Internet from 15-Feb-2017)

http://ukros.ru/wp-content/uploads/2016/03/ICCWS2016-Book-dropbox.pdf

< 1% match (Internet from 13-Jul-2013)

http://siteblog.aace.org/2009/09/18/cloud-computing-for-education/

< 1% match (Internet from 22-Aug-2020)

https://mafiadoc.com/issn-2141-0240_5baac875097c47b0568b46bc.html

< 1% match ()

https://ir.lib.uwo.ca/etd/2262

< 1% match (Internet from 20-Oct-2020)

https://www.scientific.net/AMR.905.687

< 1% match (Internet from 20-Feb-2017)

https://espace.curtin.edu.au/bitstream/handle/20.500.11937/1929/242438_De%20Maio%20C%202015.pdf?isAllowed=y&sequence=2

< 1% match ()

https://trepo.tuni.fi/handle/10024/116993

< 1% match ()

http://eprints.utem.edu.my/23441/

< 1% match ()

http://hdl.handle.net/10019.1/106060

< 1% match ()

http://hdl.handle.net/10500/19574

< 1% match (Internet from 21-Feb-2021)

https://www.cbinsights.com/research/report/microsoft-strategy-teardown/

< 1% match (Internet from 19-Jul-2020)

http://ugspace.ug.edu.gh/bitstream/handle/123456789/5557/Edward%20Nii%20Nuetey%20Noi_Comparative%20Study%20of%20the%20Experiences%20of%20NHIS%20Subscriber%20and%20Non-Subscribers%20in%20Accessing%20Health%20Care%20at%20the%20Ga%20East%20Municipality_2012.pdf?sequence=1

< 1% match (publications)

"Web, Artificial Intelligence and Network Applications", Springer Science and Business Media LLC, 2020

< 1% match (publications)

Wael Alnahari, Mohammad Tabrez Quasim. "Authentication of IoT Device and IoT Server Using Security Key", Research Square, 2021

< 1% match (publications)

Nahid Bohlol, Zohreh Safari. "Systematic parameters vs. SLAs for security in cloud computing", 2015 9th International Conference on e-Commerce in Developing Countries: With focus on e-Business (ECDC), 2015

< 1% match (publications)

José Francisco Enríquez de la O. "Decision-making and Strategic Management as Sources of Sustained Competitive Advantage in a High Cost Private Multi-campus University in México", Corvinus University of Budapest, 2017

< 1% match (student papers from 09-Mar-2012)

Submitted to TSU, University College on 2012-03-09

< 1% match ()

http://hdl.handle.net/10962/148574

< 1% match (publications)

Rakesh Kumar, Rinkaj Goyal. "On cloud security requirements, threats, vulnerabilities and countermeasures: A survey", Computer Science Review, 2019

< 1% match (publications)

"Recent Trends in Data Science and Soft Computing", Springer Science and Business Media LLC, 2019