

Texas A&M University-San Antonio

Digital Commons @ Texas A&M University-San Antonio

Masters Theses

Student Works

Spring 5-20-2023

SECURITY CHALLENGES IN CLOUD COMPUTING

Sashikumari Ramayan Singh
ssing05@jaguar.tamu.edu

Follow this and additional works at: https://digitalcommons.tamusa.edu/masters_theses

Recommended Citation

Singh, Sashikumari Ramayan, "SECURITY CHALLENGES IN CLOUD COMPUTING" (2023). *Masters Theses*. 15.
https://digitalcommons.tamusa.edu/masters_theses/15

This Thesis is brought to you for free and open access by the Student Works at Digital Commons @ Texas A&M University-San Antonio. It has been accepted for inclusion in Masters Theses by an authorized administrator of Digital Commons @ Texas A&M University-San Antonio. For more information, please contact deirdre.mcdonald@tamusa.edu.

SECURITY CHALLENGES IN CLOUD COMPUTING

A Thesis by

Sashikumari Ramayan Singh

Supervisor

Dr. Lo'ai Tawalbeh

Submitted to the Office of Graduate Studies

Texas A&M University – San Antonio

in partial fulfillment of the requirements for the degree of

MASTER OF COMPUTER SCIENCE

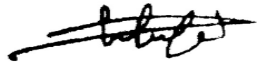
MAY 2023

Major Subject: Computer Security

SECURITY CHALLENGES IN CLOUD COMPUTING

A Thesis by
Sashikumari Ramayan Singh

Approved as to style and content by:



Dr. Lo'ai Tawalbeh, Ph.D.
Thesis Chair



Dr. Kevin Barton, Ph.D.
Committee Member



Dr. Izzat Alsmadi, Ph.D.
Committee Member

Theresa Garfield, Ed.D.
(Interim Dean of Graduate Studies)

MAY 2023

ABSTRACT

SECURITY CHALLENGES IN CLOUD COMPUTING

MAY 2023

Sashikumari Ramayan Singh

Graduate Thesis Chair: Dr. Lo'ai Tawalbeh

A ground-breaking technique called cloud computing is revolutionizing how business hardware and software are designed and purchased. Customers can access a shared computer resource pool on-demand or on a pay-per-use basis using a cloud computing paradigm. Since the introduction of this cutting-edge technology, trends of adopting cloud computing in IT businesses have been growing. In the upcoming few years, this new development in industrial technology will continue to expand and develop their e-governance. Cloud-based computing provides consumers and companies various advantages in terms of capital investment and operating cost reductions. Even with these benefits, cloud computing adoption is nevertheless constrained by a number of issues. Security is an important issue that is frequently considered. The computer model has a detrimental impact without this crucial element, which results in on a personal, moral, and financial level, misery.

Due to its many benefits over traditional computing, the majority of businesses are quickly moving to the cloud. Even with these benefits, cloud computing adoption is nevertheless constrained by a number of issues. Security is an important issue that is frequently considered. The computer paradigm has a detrimental impact without this essential component, which leads to suffering on the personal, ethical, and economic levels.

According to Cisco, cloud data centers will handle over 93% of workloads by 2021. Even a few nations have started to develop their own governmental global public clouds. In 2020, the majority of educational institutions (60%) and account breach (33%) were impacted by phishing efforts. Consumers, according to Gartner, more than 95% of cloud security issues are caused by this. If specific security precautions are not implemented, more frequent cyberattacks might result in serious material harm.

Keywords: Cloud Computing. Threats, Vulnerabilities, Security, Challenges, Monitoring, Security Alliance, Attacks.

DEDICATION

I would like to dedicate this thesis to my parents, who gave the little they had to ensure I would have the opportunity of an education. Their efforts and struggles have allowed me to have a key to unlock the mysterious of our world and beyond.

I would also like to thank my Professor Dr. Lo'ai Tawalbeh, Dr. Kevin Barton and Dr. Izzat Alsmadi who guided me throughout the process.

ACKNOWLEDGEMENTS

The person in charge, Dr. Lo'ai Tawalbeh, who enabled me to complete this task, deserves acknowledgement and my sincere gratitude. I was able to complete all the phases of writing my thesis thanks to his direction and counsel. Additionally, I want to express my gratitude to the members of my committee for allowing my defense to be a fun experience and for their insightful remarks and recommendations.

Additionally, I want to express my gratitude to my entire family for their unwavering support and tolerance as I conducted my research and wrote my thesis. Your supplication for me has kept me going so far.

Finally, I want to express my gratitude to God for guiding me through all of the challenges. Every day, I have felt your guiding. I was able to complete my degree thanks to you. For my future, I'll continue to put my confidence in you.

CONTENTS TABLE

ABSTRACT.....	I
DEDICATION.....	II
ACKNOWLEDGEMENT.....	III
CONTENTS TABLE	IV
FIGURES LIST	VIII

CHAPTER 1: Introduction.....	1
1.1 Research Problem.....	3
1.2 Aim.....	3
1.3 Research Objective.....	3
1.4 Research Question.....	4
1.5 Structure of Thesis.....	4
CHAPTER 2: Background of Cloud Computing.....	6
CHAPTER 3: Review Literature.....	10
3.2 Cloud Computing – Types of Cloud Computing.....	13
3.2.1 Cloud Based Upon Location.....	13
3.2.2 Cloud Based upon Service.....	17
3.3 Cloud Provider.....	23
3.3.1 Need of Cloud Provider.....	24
3.4 Important features of Cloud Computing.....	28
3.5 Cloud Service Level Agreement (SLA).....	30
3.5.1 Cloud Computing Monitoring and SLA Auditing.....	30
3.5.2 SLA auditing presumptions.....	31
3.5.3 Brief Description of the Proposed Architecture.....	32
3.6 Prototype.....	35
3.6.1 Creation of prototypes.....	35
CHAPTER 4: Methodology.....	38
4.1 Cloud Security Alliance (CSA).....	38
4.2 CSA Cloud Control Matrix (CCM).....	39
4.3 Shared Responsibility Model.....	39
4.3.1 Software as a Service (SAAS).....	40
4.3.2 Platform as a Service.....	40

4.3.3	Infrastructure as a Service.....	40
4.4	Cloud Security Models.....	41
4.4.1	Conceptual model or frameworks.....	42
4.4.2	Controls Model or frameworks.....	42
4.4.3	Reference Architecture.....	42
4.4.4	Design Patterns.....	42
4.5	Cloud Security Process Model.....	42
4.6	Cloud Security Challenges and its Proposed Solution.....	43
4.6.1	Data Breaches.....	43
4.6.2	Misconfigurations and inadequate change control.....	43
4.6.3	Lack of cloud security Architecture and Strategy.....	45
4.6.4	Insufficient identity, credential, access and key management.....	46
4.6.5	Account Hijacking.....	47
4.6.6	Insider Threats.....	47
4.6.7	Insecure interfaces and APIs.....	48
4.6.8	Weak Control Plane.....	49
4.6.9	Metastructure and Applistructure failures.....	49
4.6.10	Limited Cloud Usage Visibility.....	50
4.6.11	Abuse and nefarious use of cloud services.....	51
4.7	Cloud Security Goals.....	52
4.7.1	Data Privacy.....	52
4.7.2	Data Integrity.....	52
4.7.3	Data Confidentiality.....	53
CHAPTER 5:	Survey and Data Report.....	54
5.1	Virtualization in cloud computing.....	54
5.1.1	Virtualization.....	54
5.1.2	Hypervisor.....	54
5.1.3	Multitenancy.....	55
5.1.4	Service-oriented Architecture.....	55
5.2	Cross- Case Research.....	56
5.2.1	Hacked Accounts.....	56
5.2.2	Traffic Overflow.....	57
5.2.3	Attack on Wireless Local Area Network.....	58
5.2.4	Attack on XML Signature Wrapping.....	59
5.2.5	Malware of Injection.....	59
5.2.6	Attack through social engineering.....	61

5.2.7	Third-Party Service Provider.....	63
CHAPTER 6:	Conclusion and Future Scope.....	65
REFERENCES	68
VITA	74

FIGURES LIST

Figure 1	Evolution of cloud and its Service
Figure 2	Cloud Computing Architecture
Figure 3	Cloud Deployment Model
Figure 4	Cloud Public Model
Figure 5	Private Cloud
Figure 6	Hybrid cloud
Figure 7	Community Cloud
Figure 8	Cloud Service Model
Figure 9	Infrastructure as a service
Figure 10	Platform as a Service
Figure 11	Examples of SAAS
Figure 12	Cloud Provider Market Ratio
Figure 13	Characteristic of Cloud Computing
Figure 14	Model for architectural auditing and SLA monitoring for cloud computing
Figure 15	An example of a timestamp that was noted by inspectors while making a webpage request
Figure 16	Prototype Architecture
Figure 17	Shared Responsibility Model
Figure 18	Model for CSA's Cloud Security Management Process
Figure 19	Cloud Security Challenges
Figure 20	Multitenancy is abstracted in service-based cloud systems through virtualization
Figure 21	Total Malware Infections 10 years
Figure 22	Breach Incidents type in Social Engineering

CHAPTER 1: Introduction

The term “cloud computing” itself was coined in 1996 within a Compaq internal document. Simply put, cloud computing is the delivery of computing services—including servers, storage, databases, networking, software, analytics, and intelligence—over the Internet (“the cloud”) to offer faster innovation, flexible resources, and economies of scale.

Many definitions have been provided to describe cloud computing. According to definitions, cloud computing is the most recent state-of-the-art method that can offer a flexible IT architecture so that consumers are not required to own the infrastructure supporting these services. This incorporates capabilities that facilitate multi-tenancy and great scalability. Cloud computing also cuts down on capital expenses. This method is independent of user location and device.

The main benefits of cloud computing are great adaptability and scalability in organizational resources for good dependability, peak time demand, and availability of assets may be utilized at all times, from anywhere, with no expense for managing and installing the hardware and software infrastructure.

The fundamental requirement for businesses and government organizations to satisfy and execute e-Government with the least amount of downtime is 24x7 infrastructure availability. The term "cloud computing" refers to the delivery of applications, platforms, and infrastructure as services via the Internet using hardware and software in the data centers that host these services. If a company shares its sensitive data with geographically distinct cloud platforms, security is a top issue. When an organization switches to using public cloud services, a cloud services provider (CSP) is meant to have control over the computer system infrastructure. Due to the modern technology that is a major source of new vulnerabilities, such establishments may lose control over how they safeguard their computer environment and become concerned about the related secrecy and safety.

Cloud computing provides users with a sense of a network-based environment, allowing them to share computations and resources from any location in the world. The National Institute of Standards and Technology (NIST) describes cloud computing as "a template for delivering the appropriate and when required internet access to a shared pool of quickly manipulable programmable grids, servers, amenities, storage, and software." 2009; P. Mell and T. Grance. On-demand self-service, defined performance, high-speed network access, and accelerated elasticity. Additionally, there are four deployment options available: community, private, hybrid, and public clouds. public, private, communal, and hybrid clouds.

This approach is then coupled with the three service models: platform as a service (PAAS), infrastructure as a service (IAAS), and software as a service (SAAS). The essential foundation is provided by the NIST definition of cloud computing, which highlights characteristics including geographic distribution, homogeneity, virtualization, and service orientation. When implementing cloud service models at all levels, security issues must be taken into account. When the tales are compared, the browser comes out on top due to its heavy reliance. The lower tiers, in comparison, place more of an emphasis on online services. There is a decrease in overall operating expenses and investments, as well as increased productivity and scalability across all levels. Hybrid, communal, private, and public cloud service models may be utilized, depending on the demands of the customer.

By utilizing techniques like firewalls and virtualization, the Cloud Service Providers (CSPs) have pledged to guarantee the data security over stored data of cloud customers. Due to network weaknesses and CSPs' complete control over cloud apps, hardware, and client data, these measures would not completely safeguard the data. Before hosting may earn data privacy and confidentiality against CSP, sensitive data must be encrypted.

Businesses that move their systems to cloud providers entrust them with the duty of managing their data and carrying out mission-critical tasks. A means of ensuring that the outsourced service complies with the specifications established by the contractor is the Service Level Agreement (SLA). The cloud provider is required to uphold the SLA, which may be represented by QoS measurements or other agreed-upon indications.

The purpose of this research is to examine security issues and difficulties linked to cloud-based vulnerabilities and threats using a real-time experimental architecture with vulnerability scanners and penetration testing that facilitates application deployment. The virtual machine is explored, and significant security issues related to it are discussed. Additionally, the causes of cloud vulnerabilities are discussed, which facilitates the identification and evaluation of security threats.

1.1 Research Problem

One of the top emerging technologies for the accessibility of computing resources is cloud computing. In terms of security and resource sharing, cloud computing provides consumers and companies with a number of advantages. Any component in the cloud that has its security compromised might cause disaster for the company (the client) and damage to the provider. In order for suppliers and end users to be aware of the main security risks connected with cloud computing, it is necessary to identify the most vulnerable security vulnerabilities in cloud computing. Despite the availability of these advantages, there are several challenges that limit the use of cloud computing. Security is a crucial concern that is constantly taken into account. Lack of this essential component has a detrimental effect on because of harm to individuals, society, and business as a whole as a result of the computer model. I'll focus on and investigate the security issues that cloud entities encounter in my research.

1.2 Aim

The aim of this research is to follow and analyzes down the cloud computing architecture into four categories: 1) cloud deployment methods, 2) cloud service model, 3) cloud fundamentals, and 4) cloud security.

1.3 Research Objective

The goal of this investigation is to examine security concerns and issues in terms of cloud-specific vulnerabilities and threats utilizing a real-time experimental setup with vulnerability

scanner, which also makes it easier to deploy apps. This report addresses the problems with cloud data storage, including data breaches, data theft, and cloud data unavailability. Regarding security and privacy, there are several challenges that must be resolved in a cloud computing environment. This thorough survey article tries to elucidate and examine the numerous unresolved problems impeding the acceptance and spread of cloud computing, which have an impact on the various stakeholders connected to it.

1.4 Research Question

- 3 How can security problems in cloud computing be resolved? is the key query.
- 4 How can cloud computing consumers know that there are no security or availability concerns with their data?
- 5 Is their information secure? is a question everyone asks.

1.5 Structure of thesis

CHAPTER 1: Introduction

It provides a summary of the development of computing from mainframes to the cloud. It also outlines the objectives and restrictions of the research that relates to this study.

CHAPTER 2: Background of Cloud Computing

In this section we can see the background of the cloud also with the time frame we can see the development in this field according to time.

CHAPTER 3: Review Literature

The architecture of cloud computing is summarized in this chapter. It defines some fundamental terms and technology used in cloud computing.

CHAPTER 4: Metholodgy

The security issues associated with cloud computing are described. In this chapter we will describe the problem and solution which are proposed by Organization.

CHAPTER 5: Survey and Data Report

The study and discussion based on the security issues found in the cloud computing environment are described

CHAPTER 6: Concluding Statements and Future Scope

The findings and recommendations for further study are presented and we will wrap up our thesis by providing some recommendations for probable directions that cloud researchers in the future may go with their study.

CHAPTER 2: Background of Cloud Computing

In the 1950s, the idea of cloud computing was first suggested. As professionals plan and calculate temporary resources, cloud computing companies may construct data centers for a reasonable price. Computing is made efficient via cloud technology.

According to Qi Zhang, Lu Cheng, and Raouf Boutaba (2010), cloud computing combines a number of already available technology to handle company differently and efficiently. According to Rabi Prasad Padhy, Manas Ranjan Patra, and Suresh Chandra Satyapathy (2011), users don't need to be professionals in managing cloud infrastructure. Cloud computing is used by both large and small businesses, including Microsoft, IBM, Facebook, Yahoo, Google, Oracle, and others. The flexibility, portability, scalability, and capital investment benefits of cloud computing are balanced by its drawbacks in terms of security and stability as well as the lack of a clear baseline. Cloud data management and other difficult research questions in cloud computing (Deyan Chen, Hong Zhao, 2012). Access control, virtual machine migration, platform management forms, security, data encryption, interoperability, and service level agreements (Rabi Prasad Padhy, ManasRanjanPatra, and Suresh Chandra Satyapathy, year 2011).

John McCarthy first proposed the concept of cloud computing in the 1960s with the intention of making technology accessible to the general public for financial gain and practical use. The 1990s saw the term "cloud" being applied to expansive networks like ATM networks. Telecommunications companies currently provide better-quality, more affordable Virtual Private Network (VPN) services. Cloud computing is an ancient notion since it relies on tried-and-true ideas and best practices. In cloud computing, we host programs and data on remote servers through the Internet. In 2009, Pearson talked about privacy concerns. when using the cloud. In 2009, Enisa offered cloud security risk evaluation. In 2006–2007, Amazon introduced Amazon Web Services (AWS), which is based on server virtualization technology.

In July 2010, Rackspace Hosting and NASA announced OpenStack, an open source cloud computing platform. On March 1, 2011, IBM unveiled the IBM SmartCloud architecture in

support of Smarter Planet. On June 7, 2012, Oracle released the Oracle Cloud. Every security concern is carefully evaluated, described, and handled (Al Morsy, M. Grundy & I. Mueller, 2010). Cloud computing enables the storage of data on remote sites to preserve sensitive data while maximizing the use of resources (Kevin Hamlen, Murat Kantarcioglu, Latifur Khan, and Bhavani Thraisingham, 2010). To address the different security concerns identified, a security architecture system is developed. Rajasekhara Rao Kurra, Dayanand Sagar Kukkala, V.P. Krishna Anne, 2011). A key advantage of disaster recovery is that services like AWS are only accessible when we need them, and we only pay for what we need.

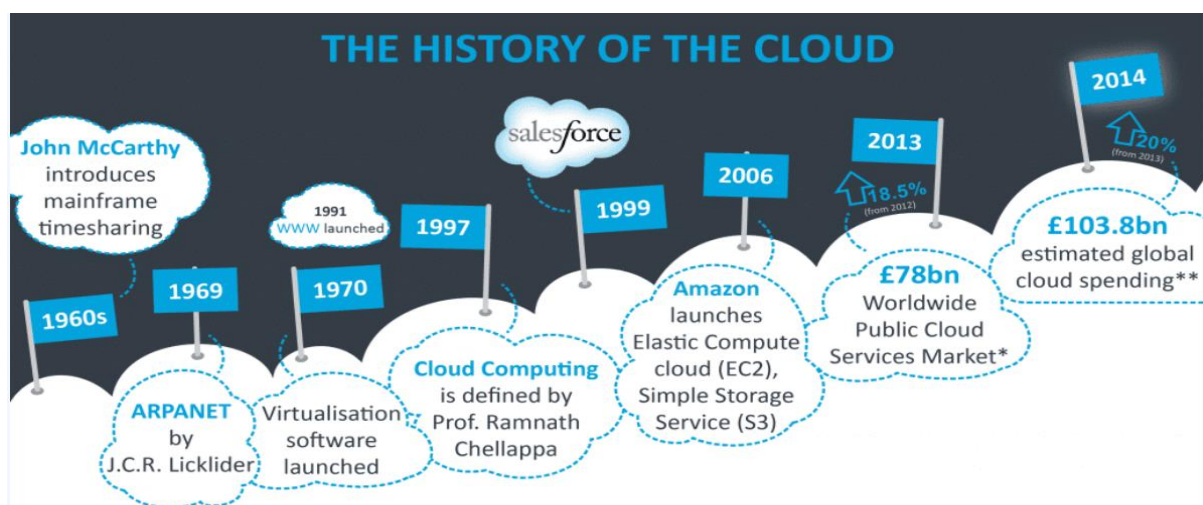


Figure 1: Evolution of cloud and its Service

In 2017, Pamela Carvalho wrote a paper Multi cloud Application Security Monitoring. In this paper, Threat detection system is used to identify possible attacks in cloud computing systems. Also considered possible strategies and techniques to detect malicious insider attacks (Pamela Carvalho, Ana R. Cavalli, Wissam Mallouli, Erkuden Rios, 2017). MUSA EU, a security platform to monitor applications deployed onto multi cloud environment in cloud providers servers is proposed. Deviations in server level agreements are detected with the help of proposed system to protect the heterogeneous platform from any attacks. The results are positive. In 2017, Yibin Li addressed about security and privacy concerns in cloud computing faced by government sectors and private financial industries in the paper intelligent cryptography approach for secure distributed big data storage in cloud computing (Nishit Mishra, Tarun Kumar Sharma, Varun Sharma, Vrince Vimal, 2017).

This paper focused on ways to protect the data from cloud operators by intelligent cryptography approach. The data files are segregated and stored in different locations in distributed manner in servers. In such a way Account Hijacking is less possible. An alternative method was also proposed to identify if the data split is required as it takes more operation time. The model is named as Security-Aware Efficient Distributed Storage (SA-EDS). Many algorithms were taken into consideration to implement the model. The approach has shown better results in terms of security and effectiveness of data storage in cloud. It was depicted that the computation time is shorter than other current approaches. In 2017, Nishit Mishra proposed a cloud security model to illustrate the necessities for every business and government agencies to protect the data stored in cloud domain and data integrity. The author proposed an efficient way to store the data by cryptography methods to overcome DDoS attack. The approach was a complex calculation which is difficult for attackers to predict the way to intrude into the cloud system (LiYibin. KeKe gai, 2017).

Two schemes: Encryption and Decryption methodologies were proposed for data security. Author addressed many new technologies like Big Data and Internet of Things also facing security challenges which can be resolved by the proposed methodology. In 2018, Gagangeet Singh Aujla proposed a secure storage, verification and auditing (SecSVA) of big data in cloud environment (Gagangeet Singh Aujla ; Rajat Chaudhary ; Neeraj Kumar ; Ashok Kumar Das ; Joel J. P. C. Rodrigues (2018).

This method includes deduplication framework based on attribute for cloud data storage, identity verification and authentication of data based on Kerberos process and Hash tree based methodology for auditing data onto the cloud in order to avoid Insecure Application Programming Interface(APIs). The author illustrated that analysis shows proposed methodology can provide secure auditing with integrity in any cloud environment. In 2019, K Latha proposed a technique for security in data storage and distribution in multi cloud environment. A prototype was developed by the author to avoid major concerns that arise by internal or cloud hackers from accessing the critical information like medical and personal data and to safeguard data security, confidentiality and authenticity (Latha, K., Sheela,2019).

A novel approach called block based data security using Galois field is carried out to achieve protection of cloud data in multi cloud environment to avoid intentional or unintentional data breaches in cloud. To simulate multi cloud, Amazon Simple Storage service (S3) and drop box was utilized. The results show efficiency in data security and efficient method to hide data from attackers. In 2019, Murtadha Arif illustrated a web client application approach for securely storing the application in cloud, it guarantees confidentiality and integrity of data that is stored in cloud database against insider attacks (Murtadha Arif Bin Sahbudin ; Riccardo Di Pietro ; Marco Scarpa, 2019).

Several experiments were conducted to test security of data using web applications in real time multi cloud environment. Performance is evaluated by measuring response time, start and end time of the user request for downloading and uploading the data from cloud. It has shown effective results for the proposed method by which the Insecure API problem is kept away. In 2020, G.Viswanath concentrated on providing algorithm for securely storing big data in multi cloud storage environment. The author developed a framework to restrict insider attacks, Tampering attacks and DDOS attacks. Various approaches like data uploading, slicing, indexing, encryption, decryption. Retrieval, merging process (Viswanath, G., Krishna, P.V., 2020).

Hybrid encryption algorithm, combination of Feistel algorithm and Advance Encryption Standard algorithm was implemented for encryption process and the same is used for decryption process but in reverse manner to store big data storage in cloud. The results were shown with high performance and security using simulation analysis in real time cloud environment. In 2020, P. Blessed Prince proposed a privacy enforced model for Health care system which uses Privacy Rating (PR) based approach to provide privacy access control to data owner to achieve data privacy, high confidentiality data integrity and availability (Prince, P.B., Lovesum, S.P.J., 2020). in cloud data through proper access management technique.

In this model the Privacy rating is measured for both data and end user to provide access to any user requested data. The author implemented discrete mathematical modeling to overcome system overhead during access granting mechanism. The results showed that privacy rating policy is governing body for all other access control methods and well suited for control over data.

CHAPTER 3: Review Literature

In this section we will explain about the Cloud Computing Architecture and its working. Apart from this we will be explaining some fundamentals terms and technology which are related to cloud computing.

When discussing cloud computing settings, the term "cloud architecture" refers to how different cloud technology elements, such as hardware, virtual resources, software capabilities, and virtual network systems, interact and communicate. It serves as a roadmap for the most effective approach to strategically integrate resources to create a cloud environment for a particular business purpose. The front end and the back end are separated into two sections.

Front end: This category includes all endpoint hardware, software, and services such web servers, client-side interfaces, mobile devices, laptops, and networks. For instance, front-end cloud services include Google, Firefox, and Microsoft Edge.

Back end: The back end includes everything else not included in the front end, such as servers, big storage devices, managing applications and services, security, etc. Back-end cloud services include, for instance, Microsoft Azure, Google Cloud, and Amazon Web Services.

The below image for cloud computing is a perfect and detailed explanation of it. and it has basically five elements of cloud computing and the term Services it is sub-divided into different three category such as (IAAS, PAAS, SAAS)

5.2 Elements for the cloud computing are as follows:

1. Management
2. Application
3. Storage
4. Services
5. Security

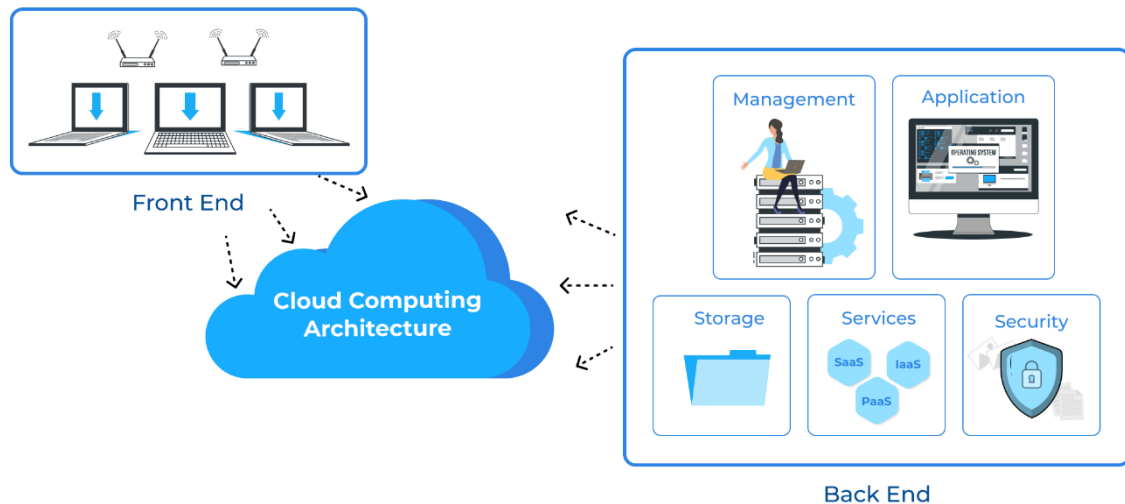


Figure 2: Cloud Computing Architecture

1. Management

Resources must be handled in real time in accordance with user needs for cloud service models. To organize communication between the backend and frontend cloud architecture components and distribute resources for certain activities, management software, sometimes referred to as middleware, is crucial. In addition to middleware, management software will provide features for data integration, application deployment, use monitoring, and disaster recovery.

2. Application

This might be anything, from the platform to software. System and application software are both successfully and efficiently managed through the cloud. Clients and end users can get the information they require with the aid of the application. Users may immediately engage with the program and complete required activities thanks to cloud computing design.

3. Storage

Data storage is a significant challenge. Data storage frequently becomes a taxing process, even with so many enormous physical storage devices and specialized storage units. This issue

has been substantially overcome by cloud computing. As long as you're connected to the internet, it's incredibly simple to access data like files, movies, and documents that are saved in the cloud. Microsoft Azure Storage, Amazon S3, Oracle Cloud Storage, and others are some of the most used cloud storage systems.

4. Services

The service, which manages all the actions carried out on a cloud computing system, is the brains of the cloud architecture. It controls which resources, such as storage, application development environments, and web applications, you have access to. It is divided into three different services such as:

- I. IAAS (Infrastructure as a Services)
- II. PAAS (Platform as a Services)
- III. SAAS (Software as a Services)

5. Security

One of the most crucial parts of the cloud computing architecture, especially in the present, is this one. Security plays a significant role in the shift that many small, medium, and large enterprises are making to entirely cloud-based services. The following are a few of the most fundamental and common measures used by cloud service providers:

- Data with limited client access
- Ongoing security examinations
- Advanced authentication
- Multiple forms of permission

3.2 Cloud Computing – Types of Cloud Computing

We all know cloud computing have different types, which can be describe into two parts. Such as the cloud which is based on location and the cloud which is based upon the services. So lets see the

3.2.1 Cloud Based upon the location

- I. Public Cloud
- II. Private Cloud
- III. Hybrid Cloud
- IV. Community Cloud

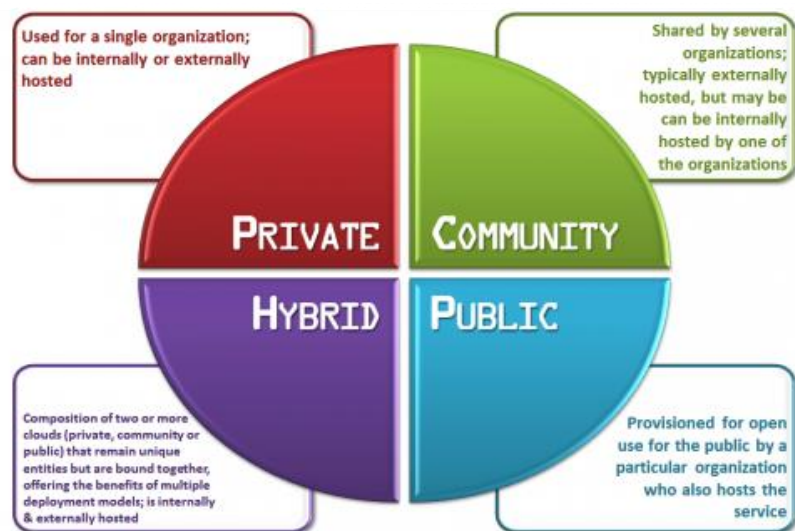


Figure 3 : Cloud Deployment Model

I. Public Cloud

Public cloud refers to an environment where the whole computer infrastructure is housed on the premises of the provider of the cloud service. As a result, the consumer and the site remain distinct, and he has no actual power over the infrastructure.

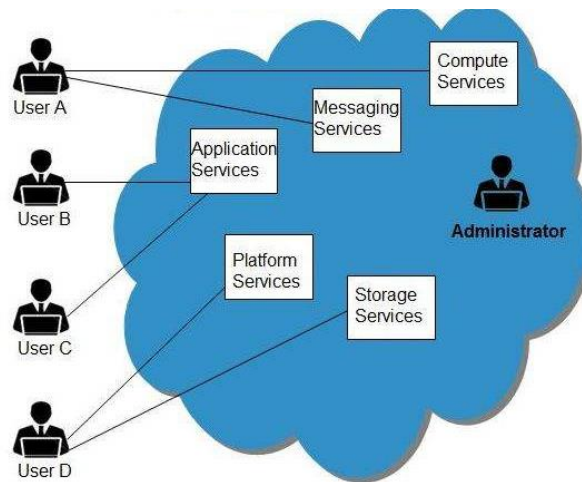


Figure 4: Public Cloud Model

Public clouds are the most performant because to the usage of shared resources, but they are also the most susceptible to numerous threats. As we go on public cloud it has its own pro and cons which are as follows:

The Benefits

- I. **Virtually limitless resources** - we can rapidly furnish a limitless quantity of resources.
- II. **Scalability and Elasticity**: we can adjust your resources to match demand fluctuations and peaks, and only pay for what you utilize.
- III. **Pay as you go** - No capital expenditures, just a monthly bill

Drawbacks

- I. **Lack of Perceived Degradation Benefits on Investment** - we can that seen huge organizations that avoid clear of public cloud since it is believed that the degradation benefits on capital investments are greater than the benefits realized on cloud-based operational expenses.
- II. **Compliance** - It's possible that public cloud service providers do not adhere to every regulatory requirement that a firm has.

II. Private Cloud

Private cloud refers to the network's (cloud infrastructure) use by only one client or business. Despite being distantly located, it is not shared with anybody else. If the cloud is hosted by a third party. A more expensive alternative available to businesses is an on-premise private cloud, which gives them physical control over the infrastructure but is also more expensive.

When using a private network, the security and control levels are at their maximum. However, if the business is required to invest in an on-premise cloud infrastructure, the cost savings may be small.

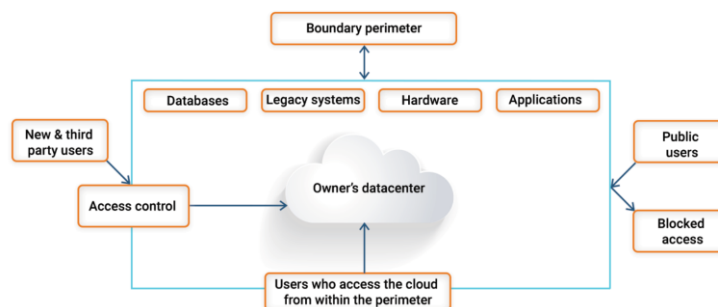


Figure 5: Private Cloud

The Benefits

- I. **Security** - Because the data is stored on-site, there is a sense of security among the companies.
- II. **Compliance** - Businesses can adhere to the compliance requirements set out by their respective sectors and corporate governance frameworks.

Drawbacks

- I. **Costs** - Organizations must pay for the up-front purchase of hardware, storage, and networking resources, as well as ongoing maintenance costs for each resource.
- II. **Complexity** - Complex virtualization of hardware resources makes the deployment and maintenance of private clouds challenging.

III. Hybrid Cloud

Through the use of a network connection, the public cloud and private cloud environments are combined to create the hybrid cloud, which enables the exchange of data and applications across them.

The Benefits

Flexibility - Businesses may employ a variety of public and private clouds to benefit from both deployment strategies. We can launch an application on a private cloud and burst it to a public cloud to handle peaks in demand.

Drawbacks

Deploying a hybrid approach is difficult since each supplier has different criteria.

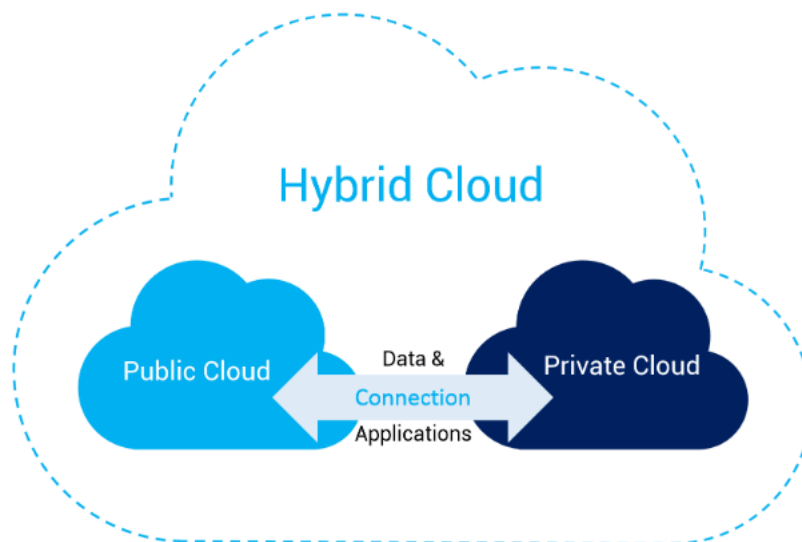


Figure 6: Hybrid cloud

IV. Community Cloud

Community clouds refer to shared infrastructure amongst businesses, typically with shared data and data management issues. A community cloud, for instance, may be owned by the government of a particular nation. Community clouds may be found inside or outside the building.

The greatest choice for using cloud computing is the public cloud if you are a startup or small business. Without making any upfront payments, you get pay-as-you-go access to the top resources available. Additionally, you reduce the amount needed to be spent on resource upkeep.

It makes sense for major businesses to take use of their hardware infrastructure investments already made and to install a private cloud on top of them.

For Large businesses purpose hybrid cloud is always a better choice as it is use for a variety of purposes, including cloud bursting, storage and archiving, development and testing on public clouds, and production on private clouds, among others.

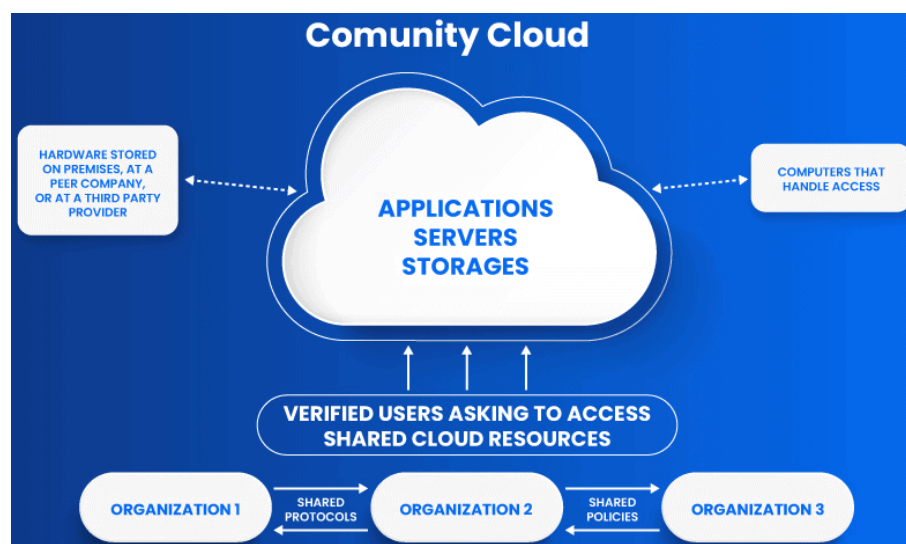


Figure 7: Community Cloud

After getting into the features and drawbacks for the deployments modes we can understand that each and every model has its own pros and cons so the user can select the cloud depending upon their organization need and requirements.

3.2.2 Cloud Based Upon the Services

The three primary cloud computing service model subcategories are SaaS, PaaS, and IaaS. All three are accessible through an online browser or through mobile apps that are available

online. Instead of creating offline, then sharing online, the team may work together online thanks to the cloud service architecture.

- I. IAAS (Infrastructure as a Services)
- II. PAAS (Platform as a Services)
- III. SAAS (Software as a Services)

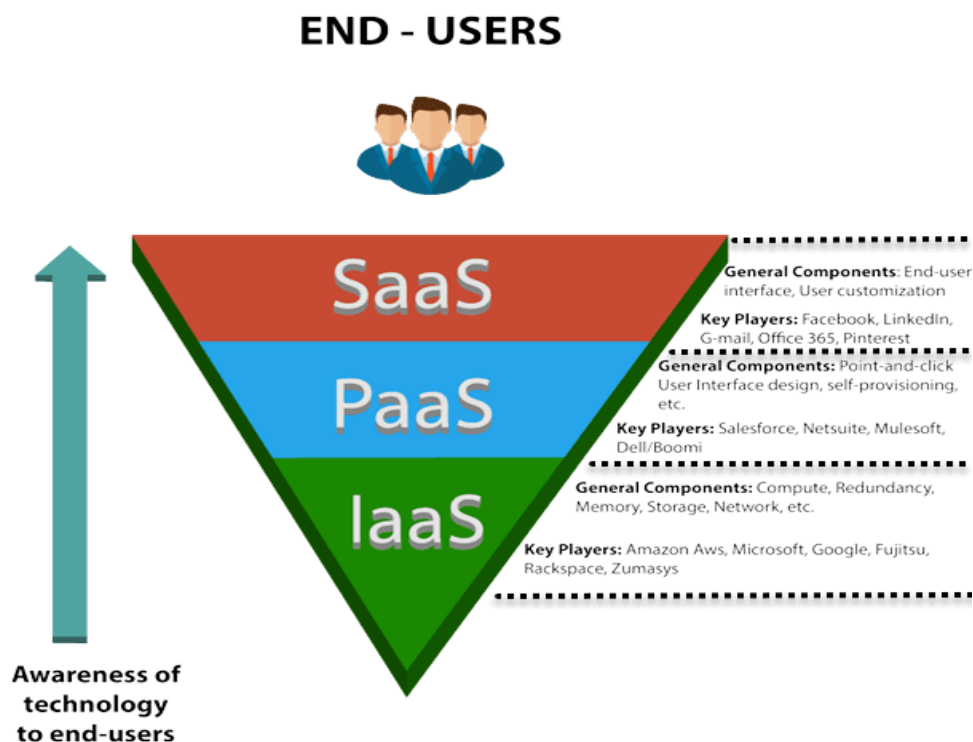


Figure 8: Cloud Service Model

I. IAAS (Infrastructure as a Services)

IaaS is a cloud computing service that provides on-demand access to networking, storage, and computing resources. Typically, it operates on a pay-as-you-go system. Instead of purchasing the hardware entirely, businesses may acquire resources as they are needed.

The on-premises data center, servers, storage, networking equipment, and the hypervisor (virtualization layer) are all hosted by the IaaS cloud vendor.

The fundamental building elements for web application are contained in this Model. It offers total control over the hardware (storage, servers, virtual machines, networks, & operating systems) that powers your application. we have the most flexibility and administrative control over the IT resources with the IaaS approach.

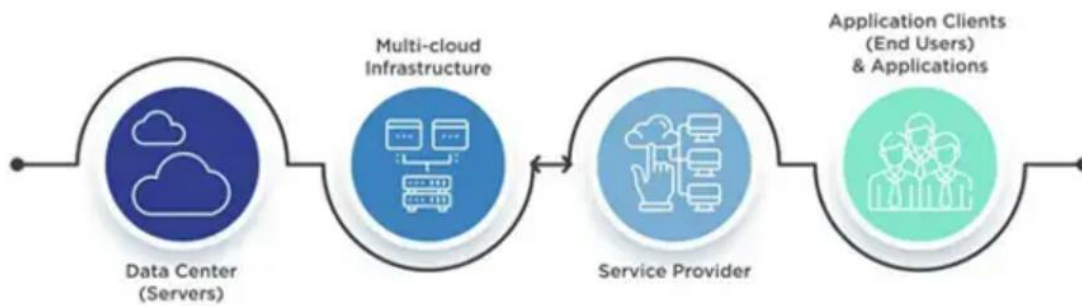


Figure 9: Infrastructure as a Service (IaaS)

IaaS features

- The resources are offered as a service.
- Service scalability is quite high.
- vibrant and adaptable API-based access and GUI for cloud service models
- Automate administrative employment opportunities

IaaS benefits

1. The deployment of servers, networking, and storage can all be automated with ease.
2. Hardware purchases may be made based on use.
3. The underlying infrastructure is entirely under the clients' control.
4. The resources can be deployed by the supplier at any moment to a customer's environment.
5. It may be sized up or down according to user need.

IaaS disadvantages

1. We must make sure that operating systems and applications are reliable and offer the highest level of security.

II. PAAS (Platform as a Services)

PaaS (Platform as a Service) offers a cloud computing architecture for the development and deployment of software applications. It is a platform for the distribution and administration of software applications. This adaptable cloud computing architecture grows automatically as needed. While the developers just manage the application portion, it also oversees the servers, storage, and networking. It provides a runtime environment for tools used in the deployment and development of applications.

All the facilities needed to enable the intricate life cycle of creating and delivering web applications and services only for the Internet are provided by this model. Developers may create, launch, and manage programs quickly using this cloud computing architecture without having to create and maintain the infrastructure or platform.

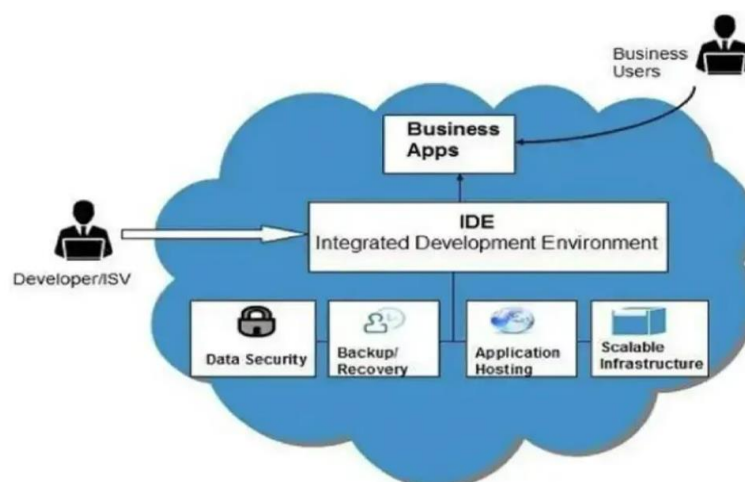


Figure 10: Platform as a service (PAAS)

PaaS features

1. Builds on virtualization technology, making it simple to scale up (Auto-scale) or down computer resources in accordance with the requirements of the enterprise.
2. Support a variety of frameworks and programming languages.

3. Connects to databases and online services.

PaaS Benefits

1. Simple, affordable app creation and deployment
2. SaaS programs may be modified by developers without the difficulties of software upkeep.
3. Automate Business Policy
4. simple transition to a hybrid model
5. It enables application development without the burden of a supporting operating system or cloud infrastructure.
6. It allows developers the flexibility to concentrate on the architecture of the application while the platform handles the language and the database
7. Working together on a same project with multiple developers is beneficial.

PAAS Drawbacks

1. The architecture of the program is not under user control; only its code is.
2. Users of the app may occasionally be exposed to security risks since the PaaS provider retains their data.
3. Selecting the appropriate services is crucial since vendors provide different degrees of service.
4. The ecosystem require for development environment may change if we run the danger of lock-in with a vendor.

III. SAAS (Software as a Services)

A web-based deployment technique called program as a Service (SaaS) makes the program available via a web browser. Users of SaaS software don't have to be concerned about the product's hosting location, operating system, or even the programming language used to create it. With an internet connection, any device may access the SaaS program.

Users of this cloud service type are always using the most recent software version. Maintenance and support are handled by the SaaS provider. Users do not have any control over infrastructure under the SaaS model, including storage, processing power, etc.



Figure 11: Examples of SAAS

SaaS features

1. It is run out of one main site.
2. Directly hosted on a distant server.
3. It may be reached via the Internet.
4. Updates to hardware and software are not the responsibility of SaaS users.
5. Pay-per-use is the method of payment for the services.

Benefits of SaaS

1. The main advantage of SaaS is that it is simple to set up and ready for use right away.
2. It is less expensive than software that is installed on-site.
3. Since the software is often included in a SaaS subscription or purchase, we don't need to manage or upgrade it.
4. It won't make use of local resources, such as the hard drive usually needed for desktop program installation.

5. It is a type of hosted cloud computing service that offers a wide variety of capabilities and services.
6. Web-based software applications are simple for developers to create and deploy.
7. It is simple to access with a browser.

SaaS Drawbacks

1. It is not feasible to "patch" an integration on your end because integrations are up to the supplier.
2. SaaS technologies might become incompatible with existing gear and software in company.
3. Data may be jeopardized if any leaks happen since you depend on the SaaS provider's security procedures.

3.3 Cloud Provider

The term A CSP (cloud service provider) can be defined as is a third-party firm that offers scalable computing resources, such as cloud-based compute, storage, platform, and application services, that organizations may use on demand across a network.

Cloud Computing it provides the flexibility, scalability, resilience, and security that business demands require without worrying about the physical limitations of your own on-premises servers or investing a lot of resources into setting up, managing, and maintaining an in-house data center, cloud computing is quickly replacing on-premises servers as the model of choice for accelerating digital transformation and innovation.

For internal services and commercial applications, we can rent services from a CSP on their infrastructure, which we can share with other people or businesses, as opposed to developing our own.

Building, managing, and delivering both small- and large-scale online and mobile apps is made possible by cloud service providers. To speed up development, they provide clients a variety

of online tools, including big data analytics, IoT, computing, and more, through virtual server hosting.

Most cloud services come with plug-and-play features, letting need utilize only the parts that require at the time they require them.

3.3.1 Need of Cloud Providers

Numerous benefits of cloud computing are essential for keeping up with the technological advancements of contemporary applications. Following are a few advantages that cloud computing may provide to your company:

Save Money

You may save a ton of money using cloud computing platforms, especially on the initial purchase of servers and hardware for your business.

Rapidity

The bulk of cloud services are self-serve and pay-as-you-go, allowing you to quickly provide substantial amounts of computer resources.

Versatility

With cloud computing, we have the freedom to access resources whenever you need them. Set specific parameters to scale your capacity when demand rises and pump on the breaks when demand falls, as opposed to using a single threshold.

Protection

The majority of cloud platforms include a wide range of rules, technologies, and controls that safeguard your infrastructure, data, and apps from dangers, improving your overall security posture.

Trustworthy

To prevent any unneeded downtime, backup your environments in the cloud and receive on-demand access to data.

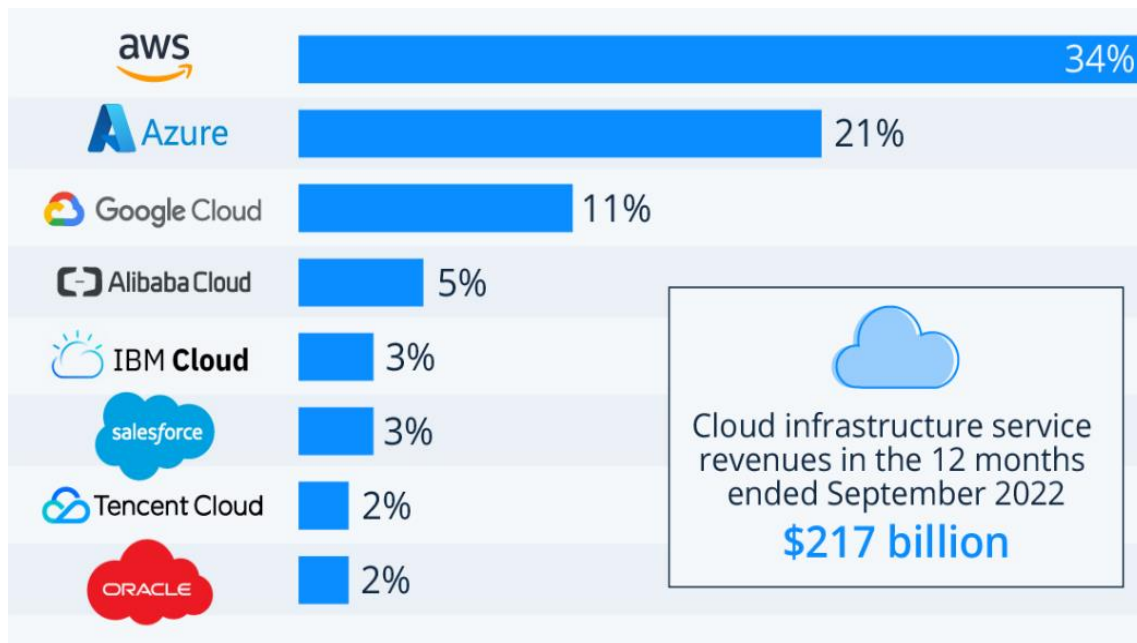


Figure 12: Cloud Provider Market Ratio

- **AWS (Amazon Web Services)**

Over 200 fully functional services are offered by Amazon Web Services (AWS), the most comprehensive and popular cloud in the world, from data centers located all over the globe. Millions of customers, including the biggest enterprises, the most effective governmental institutions, and the fastest-growing startups, utilize AWS to reduce costs, improve agility, and speed up innovation.

When compared to other cloud providers, AWS offers a significantly greater variety of services and features within those services, including cutting-edge technologies like artificial intelligence, machine learning, data lakes, and the Internet of Things, in addition to infrastructure technologies like compute, storage, and databases. As a consequence, migrating current programs to the cloud is easier, quicker, and more affordable, and we are able to build nearly anything.

Among these services, AWS offers the most complete capabilities. In order to choose the appropriate tool for the job at the best price and performance, for example, AWS provides the largest collection of databases that are designed especially for particular applications.

AWS is the largest and most active community, with millions of active customers and tens of thousands of partners globally. Customers of all sizes and from practically every industry, including startups, major enterprises, and governmental organizations, conduct every imaginable use case on AWS. The AWS Partner Network (APN) is made up of tens of thousands of independent software vendors (ISVs) and thousands of systems integrators who are experts in AWS services. To run on AWS, ISVs alter their technology.

AWS, which is intended to be both, is the most flexible and secure cloud computing platform currently available. Our core infrastructure satisfies the security requirements for the military, big banks, and other extremely sensitive organizations. More than 300 security, services, and features for governance and compliance are included in this extensive package of cloud security solutions. In addition to supporting 98 security standards and compliance certifications, AWS provides the ability to encrypt customer data across all 117 of the AWS services that host it.

Utilizing the most modern technologies, AWS enables you to experiment and build more quickly. We are continually accelerating our innovation process to produce wholly unique technologies that you can use to transform your business. As an illustration, AWS established serverless computing in AWS Lambda, a platform that enables developers to run their code without deploying or managing servers, was released in 2014 as part of this service. Amazon SageMaker, a fully managed machine learning service that enables inexperienced developers and scientists to use machine learning, is another AWS product.

AWS offers unmatched experience, maturity, dependability, security, and performance for your most important applications. For more than 16 years, AWS has been offering cloud services to millions of clients all around the world, covering a variety of use cases. AWS has the most large-scale operating experience of any cloud service.

AWS offers the greatest global cloud infrastructure. The AWS Region and Availability Zone architecture has been named by Gartner as the recommended technique for hosting business applications that require high availability.

- **Azure**

The Azure cloud platform is made up of more than 200 products and cloud services that can be used to develop new solutions, address current problems, and foresee the future. Use the preferred tools and frameworks to create, execute, and manage applications across various clouds, on-premises, and at the edge.

Obtain security that is built from the ground up, supported by a team of professionals, and proactive compliance that is trusted by businesses, governments, and startups.

We will meet you where you are, on-premises, across various clouds, and at the edge. Utilize services created for hybrid clouds to integrate and manage your environments.

Build how you want and deploy where you want with a dedication to open source and support for all languages and frameworks. Microsoft's ongoing innovation helps your progress today, and your future product concepts.

- **GCP (Google Cloud Platform)**

The Google Cloud is a collection of cloud computing services that utilizes the same internal infrastructure as Google's consumer products including Google Search, Gmail, and YouTube.

There are many services offered by Google Cloud, and the list is constantly expanding. Enterprises may combine these services in ways that provide them the infrastructure they want for building apps or running workloads on Google Cloud.

A group of cloud computing services are offered by Google under the moniker Google Cloud Platform (GCP). It is a public cloud computing platform with various services including

computation, storage, networking, application development, big data, and more that utilize the same cloud architecture as Google's internal products like Google Search, Photos, Gmail, and other end-user products.

Software developers, cloud administrators, and IT specialists can access GCP services through the Internet or a dedicated network connection.

3.4 Important Features of Cloud Computing

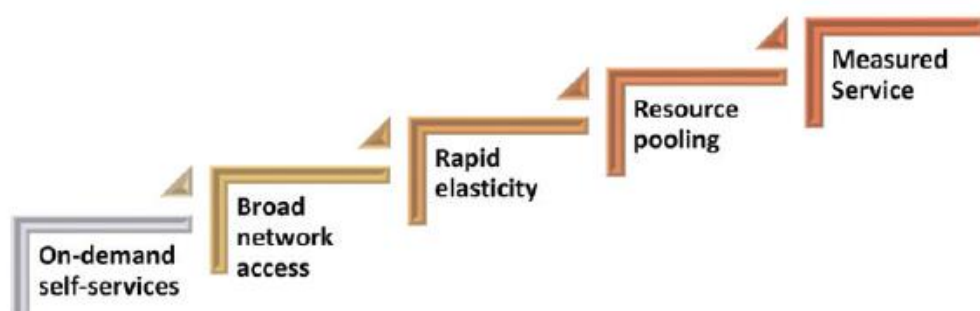


Figure 13: Characteristic of Cloud Computing

Resource Sharing

Information Technology Useful resources such as servers, networks, programs, and quotes a reprovided by some programs. A carrier of useful resources for the same body for many customers. (Al Selami, F. A. 2023).

In the cloud, several consumers can be served by a single instance of a software program. In other words, the cloud's resource pooling function entails adopting a multi-tenancy architectural model to pool the computing resources of a cloud provider to serve several clients. The cloud provider dynamically allocates and reallocates various physical and virtual resources in response to customer demand.

Rapid Elasticity

The benefits of cloud computing are to have IT assets that can scale and grow quickly with your needs. Whenever the person wants sacrifices, it is offered to them, and it grows rapidly as his needs are overcome (Al Selami, F. A. 2023).

When demand grows or falls, cloud resources are automatically supplied to scale in or out quickly. These provisionable resources might often appear to cloud users to be limitless and able to be purchased in any number at any moment.

Broad Network Access

Those services are typically supplied over desired devices and networks which are heterogeneous (Al Selami, F. A. 2023).

As a result, cloud resources are accessible through the network and may be used by a variety of thin- or thick-client devices, such as smartphones, laptops, and tablets

Measured Service

Pursuing the beneficial use of resources for each resident and software, it provides a version of the content used to the man or woman and the provider of beneficial resources. This is a conclusion drawn for several reasons, such as account monitoring and efficient use of beneficial useful resources (AlSelami, F. A. 2023).

A client only pays for what they utilize on the cloud. In order to accurately bill and be fairly charged, the supplier and the client can measure the storage levels, processing, bandwidth, and the number of user accounts. The customer and the service provider may both keep an eye on and manage the resources being used. This may be turned on or off by the user via a special web control panel. Transparency in transactions is provided by this.

On-Demand Self-Service

Cloud computing services require no human manager, and roles can provision, monitor and control computing properties as needed (AlSelami, F. A, 2023).

This is a feature of the cloud where a client may independently enable the consumption of computing resources, including server time and network storage, as needed automatically using an online control panel, without needing to manually coordinate with the service providers.

3.5 Service Level Agreement (SLA) for the cloud

As part of this service, AWS Lambda was introduced in 2014 and is a platform that enables programmers to run their programs without creating or managing servers. Another AWS offering is Amazon SageMaker, a fully managed machine learning service that makes machine learning accessible to novice developers and scientists.

For your most critical applications, AWS provides unequalled experience, maturity, reliability, security, and performance. AWS has been providing cloud services for more than 16 years to millions of customers worldwide, spanning a wide range of use cases. Of all cloud services, AWS has the most expertise operating at a big scale.

The best worldwide cloud infrastructure is provided by AWS. Gartner has identified the AWS Region and Availability Zone architecture as the suggested method for hosting enterprise applications that high availability is necessary.

3.5.1 Cloud Computing Monitoring and SLA Auditing

The assumptions, design, and key elements of the proposal are covered in this part, along with a discussion of anonymous auditing.

3.5.2 SLA auditing presumptions

The following principles serve as the foundation for the suggested architecture for SLA monitoring and auditing in cloud computing:

- The auditing information should be obtained from a third party or an unbiased organization that is trusted by all parties.
- The auditor develops the SLI and compares it to the SLO using data that the inspectors frequently collect from the client, contractor, and infrastructure supplier.
- Information gathered on the contractor and client environments may be compared with the provider measuring to identify and remediate a potential non-compliance with the SLA caused by elements internal to the cloud (under the responsibility of the contractor or the client. On the other side, information technology (IT) staff at contractors should be able to monitor customers' and contractors' activities within the cloud. This is because SLA can be severely impacted by external variables that have an adverse effect on clients' and service engineers' impressions of the cloud service (SaaS).
- Contractors and providers may be held accountable for their actions inside the cloud environment by collecting data.
- Processing spikes should be identified at runtime in order to support service maintainability.
- To aid in service maintainability, a live migration decision should be made appropriately.

3.5.3 Brief Description of the Proposed Architecture

Inspectors, auditors, and governance are the three elements of the auditing method shown in Figure 14. To acquire auditing information, the inspectors are deployed into the cloud entities' provider infrastructure (Inspector IaaS), contractor application side (Inspector SaaS, and the Inspector Service Provider (APP)), and client side (Inspector Client). Every inspector is responsible for compiling the data that will comprise a SLI or a section of one.

In order to compute the corresponding SLIs, the auditors get inspection data records while conceptually and physically staying outside of the cloud. It is possible for each SLI

or a collection of linked SLIs (i.e., those derived from the same data) to have a separate auditor. The auditor checks the computed SLI with the corresponding SLO failure to look for instances of respect the SLA.

The SLO values established by the auditors and the SLIs' evidence of SLA deviation are delivered to the governance side. The IT governance administrators can determine the underlying reasons of possible issues from each measurement record since they are aware of all SLIs created for each client. An auditing example for one kind of SLI for an APP is shown in Figure 14.

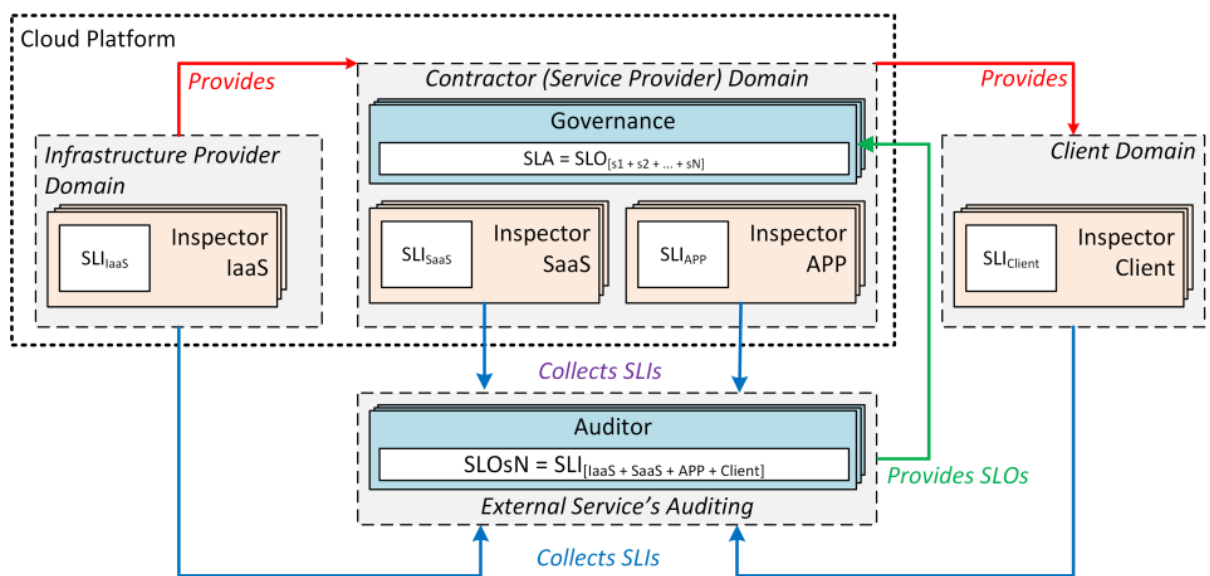


Figure 14: Model for architectural auditing and SLA monitoring for cloud computing

From the auditing records acquired, the governance mechanism may examine a certain provider's services and produce statistical statistics. In addition, the only people who can determine the causes of a SLA deviation are the governance administrators. The auditors are not given access to any information that identifies a specific consumer because the plan uses anonymized data to avoid conflicts of interest. The value of an indicator linked to a pseudonym in the proposal, which is employed to provide service clients anonymity, is the sole thing an inspector looks at [Zhang, J., Zhao, 2016]. The auditor who creates SLIs and challenges them with SLO characteristics for the same identity experiences the same thing. After that, the results are combined and made accessible for the governance process. The

identity can't be related to a practical Nevertheless, according to the inspector and auditor, entity identification. Only the governance administrator has access to the mapping between the client's real identity in the outside world and her pseudonym on the cloud computing platform. As a consequence, the recommended strategy naturally addresses conflicts of interest because an auditor can look at competing contractors but cannot tell who they are just by looking at their names.

We assume that the inspector source code for obtaining the indicators must acquire permission before to being launched in the collecting agents. The auditor has access to the source code at all times, and it is kept secure by creating cryptographic hash codes, for example. The inspectors' code should be developed as a reentrant program in this case, we advise [P. Qian, Z. Liu, Q. He, R. Zimmermann, and X. Wang, 2020].

Inspectors can start keeping an eye on the cloud infrastructure and its apps after the basic environment assumption for capturing auditing metrics has been constructed. The recommended design assumes that virtual machines be supplied in an infrastructure-as-a-service environment. Furthermore, the provided scenario is designed to communicate with web server-installed programs as an application method. (Figure 15) and a client-side interface server (SaaS).

On the infrastructure side, the Infrastructure Inspector (particularly Inspector IaaS, Figure 14) receives the IaaS's measurements of SLIs and data on the availability and use of virtual resources managed by the hypervisor. Figure 15 outlines the locations and responsibilities for timestamp collecting using a URL request as an example. The application on the client (represented as Inspector C in Figure 15), the application mechanism server (represented as Inspector SA in Figure 15), and the face server (represented as Inspector SI in Figure 14) are where inspectors conduct their online operations. On the basis of the inspectors' data, the auditors construct their SLI "response time to the client (end-user) per operation."

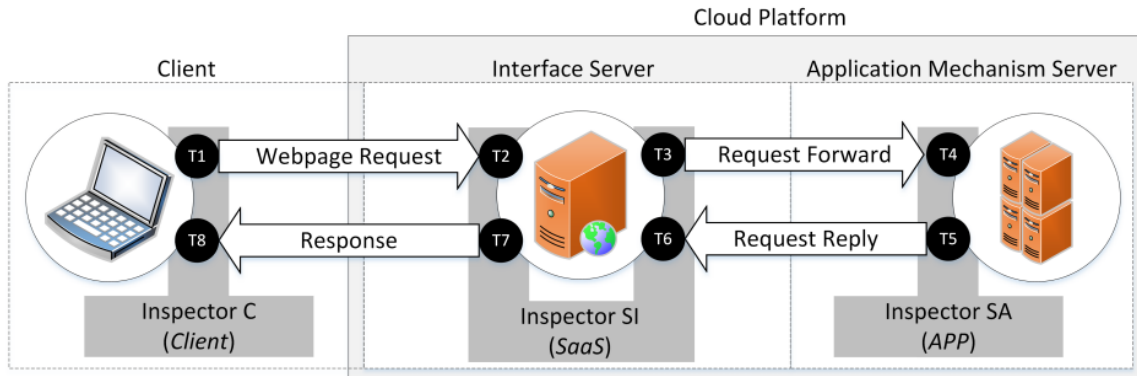


Figure 15: A timestamp that was seen by inspectors when requesting a website. At the client's end, Inspector C (the client) gathers SLI indications. SLI indications are gathered by Inspector SI (SaaS) from the server side of the interface. SLI indications are gathered by Inspector SA (APP) on the application side.

Inspectors gather the following timestamps:

- T1: the client-generated timestamp of the web page request, or the instant the program got the operation request;
- T2: The interface server's timestamp when it received the operation request.
- T3: the timestamp that was captured just before to the request being sent to the application mechanism server.
- T4: the moment the request for the procedure was made.
- T5: a timestamp that was added right before delivering the operation's outcome.
- T6: timestamp obtained immediately after the response from the application mechanism.
- T7: Timestamp just prior to the client receiving the response.
- T8: timestamp set as soon as the operation's results are received.

Gathering timestamps for each transaction that occurs at the client station (T1 and T8, Figure 15) is Inspector C's goal. The application inspectors working in the contractor application environment have unique duties. The Inspector SI (Figure 15), which is operating on the interface server, gathers timestamps when talking with the client and the application mechanism server (T2, T3, T6, and T7, Figure 14). When the Inspector SA (Figure 15) gets a request for an operation to be performed, the action is carried out on the application

mechanism server (Inspector SA) and a timestamp is recorded (T4, Figure 15), after which the client is contacted with a response (T5, Figure 15).

3.6 Prototype

We developed and tested a prototype of the architecture for multiparty cloud auditing to determine the project's feasibility.

3.6.1 Creation of prototypes

We developed the prototype as a web application for storing data on a private cloud infrastructure (on-premise) for later information retrieval (search engine, receiving messages with attachments for storage and indexing). We divided the application into an interface layer and an application mechanism. It is the responsibility of the interface layer to receive requests (web requests) from the client, transmit them, manage answers, and give processing requests to the application mechanism. To establish a search engine (application mechanism) that takes RESTful messages from the interface layer, stores the received document, and does other things, we set up an Elastic Search cluster [https://www.elastic.co/]. In order for you to later search through the stored documents, it builds an inverted index.

The servers are installed using the Eucalyptus HPE version 4.4 [https://github.com/eucalyptus/eucalyptus] in a LAN-based cloud computing environment. Each server runs the Ubuntu 16.04 operating system as a virtual machine (VM) with eight virtual cores and 16 GB of RAM. The interface server deploys RESTful web services using Apache Tomcat. The Elastic Search cluster is made up of a single virtual machine (VM).

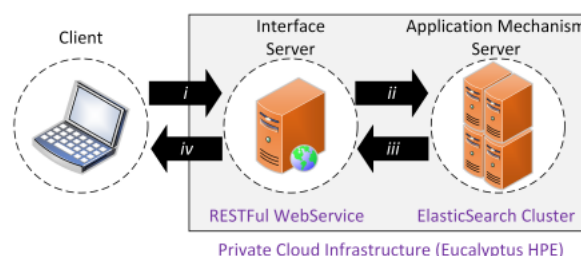


Figure 16: A prototype architecture that has been evaluated is as follows: The procedure goes as follows: i. Client delivers a file for storage; ii. Interface Server sends the file to the ElasticSearch cluster for indexing and storage; iii. ElasticSearch processes the request; Client is alerted; iv. Interface Server notifies Client when the file has been successfully stored.

When sending messages between the interface server and the application mechanism server, JSON is utilized as an alternative to XML (Extensible Markup Language). The Elastic Search cluster is also provided the queries in JSON format.

In order to obtain the SLI in Figure 14, Inspector IaaS connects to the hypervisor. Directly from the event generator available directly on the XenTrace subsystem,

XEN running a hypervisor on bare metal. The auditor gets the data and records the operation. The created Inspector IaaS uses the C programming language to save the collected data in text files for subsequent auditor consolidation.

Simply obtaining the CPU consumption for each server allows the Inspector IaaS in this prototype to detect the exhaustion of processing resources. But the hypervisor could offer metrics for Inspector IaaS's increased hardware resources. We make the decision to not include these additional data because we don't use them throughout the tests. The name of the environment in which the Java programming language was employed was sent to the inspector from the application service (SA).

Three situations were established on the SLA:

I. Basic Scenario

The servers' whole resource pool is readily available. The baseline SLI level for cloud infrastructure that was not impacted was determined using this scenario.

II. CPU Load Example

The processing power of both servers in this instance (Figure 15, Interface Server, and Application Mechanism Server) was compromised by a concurrent application load (multitenant interference). The concurrent demand within both server virtual machines is caused by a complex indexing process and a large-scale data search request on elasticsearch. The elasticsearch server is continuously asked to index a 10MB file, which increases the concurrent demand. Elasticsearch updates the pertinent entries in its inverted index in response to each request it gets. As a consequence, the CPU is used throughout our while

also creating an influence on research that is feasible. the steps taken during the development of a concurrent load for each request. The steps are repeatedly used throughout the studies. (Figure 15, the Tsi) SLIs should be affected by Tsa (Figure 15, the time needed by the Application Mechanism Server to process a request after it has been received and before it is sent to it). Largely loaded apps like virus scanners, big data frameworks, and real-time stream processing can also lead to this sort of issue. This hypothetical situation represents a real-world problem that cloud service providers are now facing when handling loads with short deadlines.

III. A scenario with network load

In this instance, all of the server resources could be managed, watched, and evaluated. We were in charge. using the Linux CBQ (Class-Based Queue) traffic shaping tool, the bandwidth. A 100 Mbps bandwidth between the client and the server was discovered. To identify a restricted bandwidth, utilize the Trd1 (Figure 15, the time between the Client submitting the request and the Interface Server receiving it) and Trd2 (Figure 15, the time between the Interface Server sending the answer and the Client receiving it) SLIs. During the experiment, the network bandwidth between a client and the servers was limited.

CHAPTER 4: Methodology

Almost all businesses have adopted cloud computing to varied degrees. The organization's cloud security plan must be prepared to defend against the main risks to cloud security, though, as a result of this use of the cloud. The way that businesses save, utilize, and exchange data, workloads, and software is constantly changing thanks to cloud computing. The amount of sensitive data that is potentially at danger is growing as a result of increased cloud usage globally.

Virtual private networks (VPN), firewalls, penetration testing, obfuscation, tokenization, and avoiding public internet connections are some techniques for providing cloud security.

Every day, security risks, dangers, and difficulties are faced by all businesses. There are more subtle differences between these phrases than most people realize. You can better secure your cloud assets if you are aware of the minute variations between them.

Despite the many benefits, moving a company's workloads to a publicly hosted cloud service exposes the company to additional data security threats that worry certain clients and IT departments at other companies. Data and software migration to the cloud presents new info-security problems.

Although it may appear straightforward, cloud security and compliance include everything a security team is now responsible for, just in the cloud. All of the conventional security domains are still there, but risks, roles, and how controls are applied vary often in a significant way.

The Cloud Security Alliance (CSA) turned to the experts to help resolve their cloud concerns. Security concerns were discovered by a working group comprising practitioners, architects, developers, and C-level personnel, who then had them examined by security experts.

In terms of cloud Computing Security there are few terms and technology which should be known and they as follow:

4.1 Cloud Security Alliance (CSA)

Its goal is to "promote the use of best practices for providing security assurance within cloud computing, and to provide education on the uses of cloud computing to help secure all other forms of computing." The Cloud Security Alliance (CSA) is a non-profit organization.

The CSA Enterprise Architecture develops a unified roadmap to satisfy corporate demands for cloud security. Risk managers must utilize this technique and set of tools to analyze the operational state of internal IT security and cloud provider policies. It enables security architects, enterprise architects, and risk management experts to meet a set of standard requirements.

4.2 CSA Cloud Controls Matrix (CCM)

A cybersecurity control architecture for cloud computing is called the Cloud Controls Matrix (CCM) by the CSA.

It is made up of 197 control goals that are organized into 17 domains and cover all important facets of cloud computing. It offers instructions on which security measures should be applied by which actor within the cloud supply chain and may be used as a tool for the methodical evaluation of a cloud deployment. The controls framework is regarded as a de facto standard for cloud security assurance and compliance since it is in line with the CSA Security Guidance for Cloud Computing.

4.3 Shared responsibility model

Although it may appear straightforward, cloud security and compliance include everything a security team is now in charge of, just in the cloud. All of the conventional security domains are still there, but risks, roles, and how controls are applied vary often in a significant way.

The components that each cloud actor is in charge of changing significantly, even as the overall scope of security and compliance remains constant. Different entities are usually in charge of implementing and managing various components of the stack in the cloud computing technology architecture. Security duties are thus divided among the companies involved and the stack as a whole.

The shared responsibility model is the term used to describe this. Consider it as a matrix of obligations that are based on service model, deployment model, and specific cloud provider and feature/product.

Security responsibility may be mapped to an actor's level of influence over the architectural stack at the highest level:

4.3.1 Software as a Service (SaaS)

Since the cloud user may only access and control how they use the program and cannot change how it functions, the cloud provider is mostly responsible for security. For instance, although the customer may only be able to control permission and entitlements, the SaaS provider is in charge of perimeter security, logging/monitoring/auditing, and application security.

4.3.2 Platform as a Service

The security of the platform is the responsibility of the cloud provider, and the user is in charge of everything that is implemented on the platform, including the configuration of any security measures that are made available. As a result, the duties are distributed more fairly. For instance, when utilizing a database as a service, the provider handles the basic configuration, patching, and security while the cloud user is responsible for responsible for maintaining accounts, choosing the security features of the database to utilize, and even determining authentication procedures.

4.3.3 Infrastructure as a Service

Similar to PaaS, the supplier is in charge of basic security, while users are in charge of everything they construct on the platform. This throws far more responsibility on the customer than PaaS does. For instance, the IaaS provider would probably keep an eye out for threats at their perimeter, but it is entirely up to the customer to establish and execute their virtual network security using the service's capabilities.



Figure 17: Shared Responsibility Model

When employing cloud brokers or other intermediates and partners, these responsibilities become much more intricate.

Knowing precisely who is in charge of what in any given cloud project is the most crucial security factor. It doesn't matter whether cloud provider offers a certain security measure as long as we are aware of what they do and how it works. If can't close the controls gap, we can select a new supplier or try to close it yourself. For IaaS, capacity to accomplish this is quite great; for SaaS, it is less so.

This is how a cloud provider and customer interact in terms of security. What action takes the provider? What should the consumer do? The cloud service provider allowing the consumer to act as they see fit? What is meant by the technology's specifications and the documentation, and what is guaranteed by the contract and service level agreements?

Two proposals are directly related to this shared responsibility model:

- **Cloud Provider**

In order for cloud consumers to make an educated choice, cloud providers should explicitly explain their internal security measures and customer security features. Additionally, providers need to properly plan and put in place such controls.

- **Cloud Consumer**

To track who is applying which controls and how, cloud users should create responsibilities matrices for each individual cloud project. This should also be in line with any requirements for compliance.

4.4 Cloud Security Models

Models for cloud security serve as tools for making security-related choices. Since "model" may be used in a lot of different ways, we've divided it into the following categories for our purposes:

4.4.1 Conceptual models or frameworks

Visualizations and descriptions that are used to teach cloud security ideas and principles are included in conceptual models or frameworks, such as the CSA logical model in this article.

4.4.2 *Controls models or frameworks*

Controls models or frameworks, like the CSA CCM, define and describe certain cloud security controls or types of controls.

4.4.3 Reference architectures

A reference design for IaaS security is an example of a standardized framework for implementing cloud security. They can be highly precise, down to particular buttons and functionalities, or quite abstract, almost conceptual.

4.4.4 Design patterns

Design patterns are reusable answers to specific issues. IaaS log handling is a case in point in security. They can be more or less detailed or abstract, down to common implementation patterns on certain cloud platforms, just as reference designs.

Depending on the objectives of the model's creator, the boundaries between these models frequently converge and overlap. Even combining all of them under the umbrella term "model" is certainly incorrect, but as the terms are frequently used interchangeably in different sources, it makes sense to do so.

4.5 Cloud security Process Model

While the exact cloud project will determine the implementation specifics, required controls, particular procedures, and multiple reference architectures and design models, there is a generally simple, high-level method for managing cloud security [Awadallah, R., & Samsudin, A. (2020)]:

1. Determine any current controls as well as any essential security and compliance needs.
2. Choose cloud service provider, models for deployment, and services.
3. Set the architecture in place.
4. Examine the security measures.
5. To find control gaps.
6. Create and put into place controls to close the gaps.
7. Control alterations throughout time.

Each project should be judged on its own merits because different cloud projects, even on the same provider, would probably employ wholly distinct sets of settings and technologies. For instance, the security measures for a project that is comparable but delivered on pure IaaS in one provider may appear extremely different.

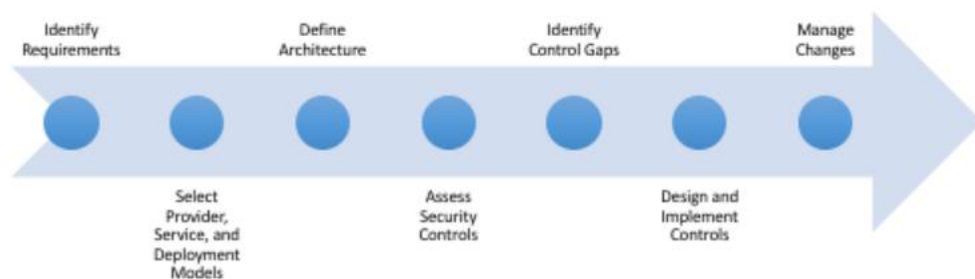


Figure 18: Model for CSA's Cloud Security Management Process

4.6 Cloud Security Challenges and its Proposed Solution

4.6.1. Data breaches

Breaches of information, which are the responsibility of both CSPs and their customers, were once again the biggest danger to cloud security in CSA's study this year. Over the past several years, the cloud has been blamed for a number of data breaches, Capital One's cloud misconfigurations being one of the most famous.

A data breach may bankrupt a business, ruining its reputation permanently, putting it in financial trouble owing to legal obligations, regulatory repercussions, incident response expenses, and diminished market value.

CSA suggested the following

- Identifying the value of data and the consequences of its loss.
- Encrypting data, and having a reliable, tried-and-true incident.

Response Approach

The following are specifications for the CSA Cloud Controls Matrix (CCM)

- Executing routines to ensure data input and output integrity.
- Using the least privilege principle to access control and creating rules and processes for safe data removal and destruction.

4.6.6 Misconfigurations and inadequate change control

Assets are subject to attack when they are configured improperly. For instance, the Capital One hack was linked to a web application firewall error that made Amazon S3 buckets vulnerable. Other significant causes of vulnerabilities include using default credentials and having too many permissions, in addition to insecure storage.

Related to this, cloud misconfigurations may be brought on by poor change control. Change control should be automated in on-demand, real-time cloud settings to facilitate quick change.

Misconfigurations, change control, and customer accountability are new to the list of cloud security threats.

CSA suggested the following

- Paying close attention to information available online.
- Identifying the commercial worth of data and the consequences of its loss; developing
- Establishing and keeping a reliable incident response strategy.

Response Approach

- Making sure that external partners follow the same change management, release, and testing processes as internal developers.
- Executing risk assessments on a regular basis.
- Providing security awareness training for employees, contractors, and third-party users.

4.6.7 Lack of cloud security architecture and strategy

Too many businesses adopt cloud computing without the necessary architecture or plan in place. Customers must comprehend the risks they face, how to migrate safely to the cloud (remember that this is not a lift-and-shift procedure), and the details of the shared responsibility model before making the switch to the cloud.

The customer is responsible for this danger, which is new to the list. Customers will be susceptible to cyberattacks without adequate preparedness, which might result in monetary losses, reputational harm, and legal and compliance problems.

CSA suggested the following

- Establishing and executing a security architectural framework.
- Ensuring the security architecture is in line with the business goals and objectives, and implementing continuous security.

Response Approach

- Ensuring that risk assessment policies incorporate appropriate updates to policies, procedures, standards, and controls.
- Planning, creating, and deploying network and system components, API designs and configurations, and business-critical/customer-impacting applications in accordance with established IT governance, service management policies, and capacity-level expectations.
- Limiting and keeping track of traffic between trustworthy and unauthorized connections in virtual instances and network settings.



Figure 19: Cloud Security Challenges

4.6.8 Insufficient identity, credential, access and key management

Identity and access management (IAM) problems are a key contributor to cybersecurity dangers in general and cloud security threats in particular. CSA recommendations state that this results from the following

- Inadequate credential protection
- Failure to generate an automatic cryptographic key, password, or rotating certification.
- Scalability issues with IAM
- multifactor authentication is not present
- Faulty passwords

Cloud usage compounds IAM problems. Defining roles and rights, provisioning and deprovisioning concerns, zombie accounts, superfluous admin accounts, and users evading IAM constraints all make it difficult to conduct an inventory, track use, monitor activity, and manage the sheer volume of required cloud accounts.

CSA suggested the following

- when two-factor authentication is used.
- Using stringent IAM rules for cloud identities and users.

- Utilizing central, programmable key management, rotating keys, and eliminating unneeded login credentials and access capabilities.

Response Approach

- Developing and sustaining key management policies, as well as identifying important managers.
- Defining, explaining, and assigning roles and duties for carrying out procedures' changes or terminations of employment.
- Executing prompt deprovisioning of user access to data and network components, whether by revocation or change.

4.6.9 Account Hijacking

The revelation, unintentional disclosure, exposure, or other breach of a cloud account that is essential to the use, management, or upkeep of a cloud environment is known as cloud account hijacking. If compromised, these extremely private and sensitive accounts might have grave repercussions.

Account penetration can result in data breaches and service interruptions due to phishing, credential stuffing, weak or stolen credentials, and faulty coding.

CSA suggested the following

- Keeping in mind that account hijacking entails more than merely changing your password.
- Using IAM and defense-in-depth techniques.

Response Approach

- Creating, preserving, and implementing an integrated business continuity strategy.
- Dividing the surroundings used for production and nonproduction.
- Keeping track of and updating compliance liaisons in case a forensic investigation calls for quick contact with law enforcement.

4.6.10 Insider threats

The hazards connected to staff members and other users accessing a company's network are not exclusive to the cloud. Insiders, such as current and former workers, contractors, and

partners, can result in data loss, system outages, decreased consumer confidence, and data breaches whether intentionally or negligently.

It is the customer's duty to resolve insider risks involving stolen or leaked data, credential problems, human mistake, and cloud misconfigurations.

CSA suggested the following

- Giving a security awareness course.
- Correcting faulty cloud servers.
- Limiting entry to vital systems.

Response Approach

- Requesting permission before moving or moving software, hardware, or data.
- Approving and revoking user access permissions on a regular basis.
- Separating networks, infrastructure, and multi-tenant apps from other tenants.

4.6.7 Insecure interfaces and APIs

Some of the most exposed elements of a cloud system are CSP UIs and APIs, which consumers use to engage with cloud services. Any cloud service's security is dependent on how well they are protected, which is the responsibility of both customers and CSPs.

Customers must be attentive in controlling, monitoring, and safely using what the CSA refers to as the "front door" of the cloud, and CSPs must make sure security is incorporated.

CSA suggested the following

- Maintaining proper API hygiene.
- Avoiding reusing API keys.
- Utilizing open and common API frameworks.

Response Approach

- Following industry-leading standards for designing, creating, implementing, and testing APIs as well as any relevant legal, statutory, and regulatory requirements.

- To avoid data leakage and manipulation, audit instruments that communicate with the company's information systems should be separated and given access controls.
- Limiting the use of utility programs that can override system, object, network, virtual machine, and application controls.

4.6.8 Weak control plane

The cloud control plane, which is new. It is the group of administrative consoles and interfaces that an organization uses to manage its use of the cloud. According to CSA, it also covers data duplication, transfer, and storage. A compromised control plane that was not adequately protected might result in data loss, regulatory fines, and other repercussions, as well as a damaged company reputation that could result in revenue loss.

CSA suggested the following

- Requiring CSPs to exercise reasonable controls.
- Carrying out research to check if possible cloud services have sufficient control planes.

Response Approach

- Developing infosec rules and procedures and making them accessible to internal staff and outside business contacts for evaluation
- Putting into practice and using defense-in-depth techniques to quickly identify and stop network-based assaults
- Creating guidelines for the handling, labeling, and security of data and data-containing items.

4.6.9 Metastructure and Applistruce failures

According to the CSA, the metastructure is "the protocols and mechanisms that provide the interface between the infrastructure layer and other layers" or, to put it another way, "the glue that binds the technologies and facilitates management and configuration."

The metastructure, often referred to as the waterline, serves as the boundary between CSPs and clients. There are several security risks present here, such as incorrect cloud app usage by users or bad API implementation by CSPs, according to the CSA. Such security issues might result in service interruptions and configuration errors, which could have a negative financial and data loss impact.

The phrase "the applications deployed in the cloud and the underlying application services used to build them" is used to define the term "applistructure." PaaS capabilities like message queues, AI analysis, and notification systems are a few examples. This research identifies a new threat, for which the customer and CSP have responsibilities.

CSA suggested the following

- Customers integrating features and controls in cloud-native designs.
- CSPs undertaking penetration testing and sharing findings with customers.
- CSPs giving visibility and disclosing mitigations to offset their tenants' lack of transparency.

Response Approach

- Creating and maintaining audit plans to manage interruptions in corporate processes.
- Employing encryption to safeguard data while it is being stored, used, and sent.
- Creating guidelines and practices for the management and storage of identification information.

4.6.10 Limited cloud usage visibility

Enterprise administrators have long been concerned about cloud visibility, but this report's CSA cloud security concerns list does not yet include it. According to CSA, poor visibility results in two major problems:

- When employees utilize programs that are not authorized by IT, this practice is known as shadow IT or unauthorized app use.
- Apps that have been approved by IT are misused in a sanctioned manner. This covers both users who are permitted to use the program and unauthorized users who access

it using stolen credentials obtained, for instance, through SQL injection or DNS assaults.

According to the CSA, this lack of visibility causes a lack of governance, knowledge, and security, all of which may lead to cyberattacks, data loss, and security breaches. It falls under the responsibility of both CSPs and clients.

CSA suggested the following

- Creating a top-down cloud visibility initiative.
- Requiring and enforcing mandatory corporate education on appropriate cloud usage guidelines.
- Need a cloud security architect or outside risk management to assess and approve any unapproved cloud services.

Response Approach

- Periodically undertaking risk evaluations.
- Educating all employees on their duties and responsibilities with regards to compliance and security.
- Creating and managing data flows, and performing inventory.

4.6.11 Abuse and nefarious use of cloud services

The cloud may be utilized for good, but attackers can also use it maliciously. SaaS, PaaS, and IaaS solutions used fraudulently have an impact on people, cloud consumers, and CSPs alike. Customers are particularly vulnerable to the exploitation of cloud services via the following: Disguised as originating from a CSP,

- Assaults that use distributed denial-of-service
- Phishing
- Click fraud
- cryptomining
- Brute-force assaults
- Hosted harmful or illegal content

A client unintentionally hosting malware, data loss, loss of cryptocurrencies or other payments made by the attacker, and other costs can result from compromised and misused cloud services.

The CSA advised CSPs to take extra care in spotting and thwarting such attacks using an incident response mechanism. Additionally, CSPs should provide their clients with monitoring instruments and controls, monitor apps and workloads in the cloud.

CSA suggested the following

- Monitoring cloud usage by employees.
- Employing technology for preventing data loss in the cloud.

Response Approach

- Using technology controls to mitigate dangers associated with mobile devices.
- Establishing limits and use rights for workstations, laptops, and other user- and enterprise-owned endpoints.
- Making and keeping a list of stores and applications that have been authorized.

4.7 Cloud Security Goals

The major reason why many businesses are taking their time adopting cloud computing is security concerns. In CSP computing, there are three significant legal issues that pertain to cloud-based services: Four cloud security solutions include cloud data visibility, control over cloud data, access to cloud data and applications, and compliance. Cloud computing provides security, but there is no 100% guarantee of security. Refined requirements to ensure cloud service security from CIA triad.

4.7.1 Data Privacy

Protecting sensitive customer data given by a third party is connected to data privacy. The third party that offers the cloud service and technical capability has control over the customer. The client's data privacy may be impacted by a breach of any signed contract with a third party.

4.7.2 Data Integrity

Maintaining the original data that is stored in many physical places on servers run and managed by numerous businesses all over the world is connected to data integrity. Additionally, it relates to the CSP's appropriate selection of the necessary data (in accordance

with the must be utilized in the computation requested by the client). As a result, it is a serious problem because the CSP cannot ensure the data's safety, which in some instances neither the CSP's data selection process nor the data that is put in their global data centers. itself.

4.7.3 Data Confidentiality

According to [A. Izang, Y. A. Mensah, O. J. Omotosho, and C. P. Obioma, 2016], the ability to link various cloud services has an impact on data secrecy. These are a few of the issues that have an influence on the management of cloud infrastructure. These are some of the other issues that outsourcing control to the CSP, which is referred to as a central administrative unit, raises.

It is among the greatest ways to secure data privacy, secrecy, and integrity, according to numerous studies.

CHAPTER 5: Survey and Data Report

5.1 Virtualization in cloud computing

Technologies that Support Cloud Computing Due to fundamental concepts like virtualization, multitenancy, and service-oriented architecture (SOA), cloud computing is now a real possibility. [S. Sengupta, V. S. Kaulgud, V. S. Sharma, A. Verma, and S. Kaushal, 2011] These processes allocate resources to consumers from a physical location.

5.1.1 Virtualization

Virtualization, which implies a flexible approach to computing, enables resource division in the cloud environment. Sharing resources is made possible by a virtual machine (VM) using a file usually known as an image, which may be developed by users or downloaded from the internet [H. Tabrizchi and M. K. Rafsanjani2020], [J. P. Barrowclough and R. Asif]. Any shared IT resource might really be virtualized to enable many users to access a single instance of the resource in practice. Virtualization of the desktop, network, storage, data, applications, CPU, and cloud are the most often utilized varieties. The incorporation of IaaS, PaaS, and SaaS models into cloud virtualization implies resource virtualization [IBM Cloud Education, 2021] through [M. I. Malik, A. Rashid and S. H. Wani, 2018]. Figure 20 illustrates an abstract picture of the service-based cloud computing architecture. In this idea, a hypervisor is used to distribute physical resources to a number of users across several layers as a result of virtualization.

5.1.2 Hypervisor

An OS-like component called a hypervisor (HV) or virtual machine monitor (VMM) functions similarly to an OS in a cloud environment. As a software layer that stands in between actual hardware and virtual machines, it maintains the multiple VMs and makes sure they have the resources they require. B. Asvija, R. Eswari, and M. B. Bijoy, 2019; J. P. Barrowclough and R. Asif, 2018]. It is possible to operate several VMs simultaneously on a single device thanks to HV technology. The two-type approach, which divides HV into baremetal and hosted varieties, has been shown to be the most common. While the second type operates directly on the raw hardware, the first sort runs as a software on the host OS, such as KVM, QEMU, and VirtualBox. include Xen and ESX.

For the latter category, direct resource communication significantly reduces latency. into the hosted and bare metal HV. Figure 20 depicts a bare metal HV, which eliminates the need for the host OS by translating user VM commands directly to the hardware.

5.1.3 Multitenancy

Program design known as "multitenancy" enables several users to access the same program instance at once. This method makes use of the same physical entities to serve end users across several virtual machines running on a single server. To deliver the promised services to numerous consumers, a Service-Oriented Architecture (SOA) makes use of a number of mediatory technologies, such as HTTP and Simple Object Access Protocol (SOAP). Figure 19 shows a potential resource virtualization that would result in the multitenancy situation shown. Through virtualization, physical instances like CPU and Memory are separated into shareable components in multitenancy and given to many clients. The performance of the shared resource would suffer from simultaneous access to one instance, but on the other hand, resource use would be maximized. Theoretically, separated userspace would guard against security problems like data leakage, but in practice, this is not the case, and the cloud paradigm would become more vulnerable as a result of this technology [R. Kumar and R. Goyal,2019], [B. Asvija, R. Eswari, and M. B. Bijoy, 2019].

5.1.4 Service-Oriented Architecture

Loosely connected components are used in Service-Oriented Architecture (SOA), which outlines a reusable software development process, to improve interoperability and reusability. The SOA design is well suited for emerging computing environments like service-based cloud computing because the independence of the services increases development agility. Target functionality are offered through service interfaces in this model. Typically, services are described using Web Service Definition Language (WSDL) standards and exposed via the SOAP or REST network protocols. The advantages of this software development paradigm are numerous. Due to the interface's loosely linked components, a user only requires the absolute minimum of information to use it. It is possible for the provider and customer to speak different languages, which makes things less dependable [IBM Cloud Education,2021], [S. Wang, Z. Liu, Q. Sun, H. Zou, and F. Yang2014].

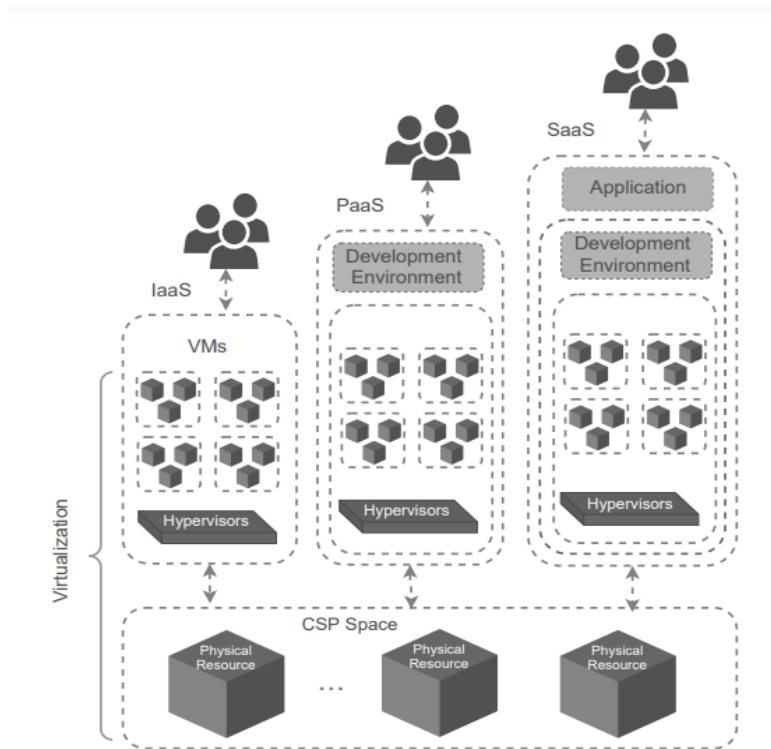


Figure 20: Multitenancy is abstracted in service-based cloud systems through virtualization

5.2 Cross – Case Research

In various real-life situations, the utilization of cloud computing and the actions that cause the association to decrease the event will be investigated. For each case, the specifics of the attack will be quickly established, and a discussion of those details will follow. Protocols for counteraction will also be looked at.

5.2.1 Hacked Accounts

Account hijacking is a risk when malevolent attackers access account credentials, which are extremely sensitive information and can lead to account breach [assets.extrahop.com, 2019].

Instagram (Chtrbox) has abused as of May 2019. Users can submit photographs and videos to Facebook owns the American social networking site Instagram. The information in Instagram's database, which includes display images, followers, and contact details such an email and a mobile number, is available without a password. Although the breach did not expose any financial information, it did provide access to contact information and a

geographic location that may not have been intended to be made public. The data of 49 million Instagram users is stored in an online database, according to security expert Anurag Sen. He then informed TechCrunch, who made contact with the owner of Chtrbox, a social media influencer marketing firm located in Mumbai that pays people to promote sponsored adverts. The research by TechCrunch claims that it got in touch with a few unconnected people whose information was in the database and got confirmation that they could be personally recognized and connected to Instagram accounts. The stolen information is subsequently said to have been made public and put up for sale using Bitcoins [U Verma, J. Lirk].

To stop this data leak, the cloud must have a far more flexible environment throughout development and runtime. Despite disregarding the idea of least benefit for optimal security needs, this method, Multi-factor authentication (MFA), regular key rotation, and a number of other crucial processes that have to be routine are among the best security safeguards for assets. Important insights helped businesses understand their cloud accounts, workloads, and container basis. Without it, the business is subject to information gaps that limit its ability to identify errors, ineffective procedures, or other problems that might quickly result in a breach [C. Pedigo, 2019].

5.2.2 Traffic Overflow

Attacks that overflow a network or service with traffic do so by sending a lot of traffic to a single server. Or, to put it another way, it stops responding to the genuine request just because more resources are being consumed by bogus traffic. This attack causes network congestion [York, D, 2010].

The telecom company OVH was the target of an assault in September 2016 that was 100 times more powerful than most of its sort. Almost the whole eastern United States saw a slowdown in internet speed. A 21-year-old college student from New Jersey created the Mirai Botnet, an Internet-connected gadget, together with his two buddies. Initially, they are attempting to advance in the computer game Minecraft. A network of zombie devices infected with malware that the owners of VDoS may control to launch DDoS assaults at will. That was a

newer Internet of Things zombie. It wasn't at all like a typical DDoS attack. IoT devices with default security settings given by the manufacturer were inspected by the new virus as The default passwords have scarcely ever been changed by users. Surprisingly, between 200,000 and 300,000 infections occurred across roughly 65,000 devices in under 20 hours, with the amount doubling every 76 minutes. This assault increased the speed from 10 to 20 gigabits per second to 50 gigabits per second [G. Graff].

The FBI, business researchers, and network service providers like Akamai created a number of honeypots, or hackable devices, to study how infected "zombie" devices communicated with Mirai's command and control server. Later, the Minecraft DDoS attack mitigation solution was provided by Internet host OVH's VAC service. The FBI then worked with academics from the corporate world to develop tools that enable them to keep an eye on traffic rerouting [G. Graff].

5.2.3 Attack on Wireless Local Area Network

In a wireless area network assault, an intruder gains access to the network of the authorized user and launches many attacks. For instance, man-in-the-middle, cipher, denial-of-service (DoS), and flooding attacks [M. Sri Lakshmi, Dr. S. Kumar,2014],[Soni M., Rajput B.S., Patel T., Parmar N. (2021)].

One guy from the ground hacked hundreds of aircraft in November 2017. Ruben Santamarta was able to see into airplanes that were flying hundreds of meters above him by taking advantage of a flaw in the satellite's technology. Some of them involve the largest airline in the world's commercial fleet. By breaking into onboard systems, researching Wi-Fi, and monitoring every passenger's linked gadget. He was able to spy because of flaws in the antennae that are transmitting data to the modem. The satellite communication equipment was converted by him into "radio frequency weapons" [T. Brewster].

There are several potential responses to this attack. The usage of firewall technology comes first. This can assist determine whether to restrict traffic after evaluating the incoming and outgoing traffic.

5.2.4 Attack on XML Signature Wrapping

In an XML signature wrapping attack, threat actors use application logic to inject phony elements and unaltered components into the message's structure. Additionally, by doing this, the attacker can access web service requests by impersonating a valid user. [M. Jensen, L. Lioa, S. Gajek, and J. Schneck].

In July 2019, data from Capital One, the country's second-largest banking company, was hacked. In this invention, customer personal identifying information from a rented cloud data server—including social security numbers, birth dates, email addresses, bank account numbers, and a sizable amount of credit card information—was discovered on Paige A. Thompson's GitHub account. The theft also affects 6 million Canadians and 100 million US consumers who have Social Insurance Numbers (SINs). During your cracking Capital One, Thompson used TOR and VPN I predator because these technologies are excellent in obscuring your trail. Even though a Web Application Firewall (WAF) was set up to safeguard the cloud, the breach nevertheless happened as a result of incorrect firewall settings. Following the incident, Capital One contacted law enforcement about the data theft, which assisted the FBI in pinpointing the attack. After resolving the configuration issue, Capital One immediately began working with federal law enforcement. The company provided free credit monitoring and identity protection to everyone through a variety of means and warned its users [C. Pedigo 2019].

Knowing your infrastructures well, configuring the cloud security appliance appropriately, and following general guidelines are suggested ways to this cloud assault. Only certain job responsibilities should be allowed for access, users, or applications. To avoid becoming more vulnerable to data breaches, Capital One Company could have kept and operated its data from many locations. [N.Hazut , H.Poston 2019,].

5.2.5 Malware of Injection

In malware injection, the attacker attempts to inject a malicious server or virtual machine. Attackers attempt to integrate a malicious service implementation module into a cloud system. The attacker must then behave as though the service is legitimate. After doing so successfully, the attacker's code begins to run and a genuine user request is sent to a malicious service implementation [R. Rao, Vaudha, S 2018].

Currently, malicious actors are using Amazon's cloud to host drive-by download sites and domain services. Additionally, researchers have looked at a variety of domains that are being used to spread malware through spam and phishing campaigns on Amazon's cloud infrastructure in order to steal sensitive data like banking credentials [D.Fisher 2011]. The goal of this assault, which had its origins in Brazil, was to steal client information from nine banks and solely target Brazilians. Malware disabled the regular operation of virus protection products and plugins that might secure the online banking system in order to boost its success rate. Also mentioned was the malware's theft of Microsoft Live Messenger's digital credentials and certificates [V. Zakorzhevsky 2011]. In addition, malicious programs placed onto victims' computers from attack websites containing the module that turned off the anti-virus software while acting as root. Similar to spamming efforts, these assaults start when consumers get emails with links that guide them to dangerous websites, raising serious security issues. Threat actors deployed various components during the breach that contained login details for nine Brazilian banks and two foreign institutions. In addition, hackers obtained eTokens used in an authentication process. [D. Bestuzhev 2011]. This hacking attempt mirrored earlier ones that had been made public for years.

One broad solution to this issue is to handle cloud-based email interactions with specialized anti-phishing software. The majority of hackers are for your money, identity, and financial information. Therefore, protecting business companies against phishing scams is an important step that must be performed. A protective system connected to the mail client as a centralized system on a server should be present on each host machine. With the use of that method, threats on the cloud mail system, spam emails, and spear-phishing efforts may be swiftly identified. These are frequently linked to email systems like Postbox, Inky, Outlook, Hiri, Notes, etc. and incorporated into group or individual virus prevention software. Furthermore, it is crucial for companies to create cloud-related solutions under the rigorous

supervision of intrusion detection systems. when intruders are found. Utilize an IDS (Intrusion Detection System) that can detect network activity and respond to abnormal insider behavior by taking action. One might get in touch with Amazon Web Services (AWS) to report such malicious behavior. The following webpage (<http://aws.amazon.com/security/vulnerability-reporting/>) allows users to report AWS vulnerabilities. After this attack, AWS deleted all the dangerous links.

2009 saw 12.4 million fewer malware injection instances than any other year. Between 2009 and 2012, the number of malware infections surged seven-fold. The number of malware injections climbed gradually throughout the same period, reaching 82.62 million in 2012.

The graph demonstrates that malware injections increased more fast in the years that followed. There were 165 million in 2013, and 702 in 2017, a significant growth. From this point on, the cases increased regularly until 2018.

The malware injections that occurred between 2009 and 2018, a ten-year span, are depicted in the following line graph:

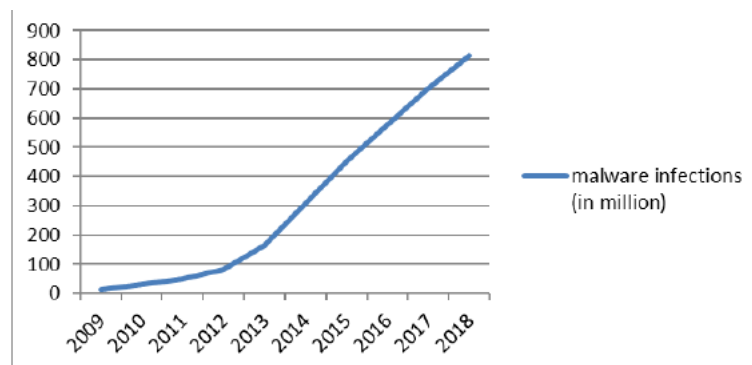


Figure 21: Total Malware Infections 10 years

5.2.6 Attack through social engineering

A social engineering assault needs human contact in which different individuals are tested to see whether they may be used as part of a trick to circumvent customary security protocols.

[I. Kotenko, M. Stepashkin, and E. Doynikova 2011][Soni M., Patel T., Jain A 2020].

Unintentionally, Apple technical support allowed hackers access to an iCloud account, and Amazon technical support assisted them in gathering a little amount of information—the four-digit credit card number. In other words, Apple deems protected to carry out the personal evidence while Amazon considers extremely four-figure non-essential in a user account that is adequate to disclose the entire image online. When information management weaknesses were discovered and the whole technological industry has been dealing with an outbreak of Discrepancy [wired.com 2012]. A person's digital life was in danger, and he lost all of the information associated with his Gmail, Twitter, and Apple ID. All of these were linked together by an apple ID, therefore the iCloud was also compromised.

When utilizing cloud storage and your data, you should be mindful of the following:

- Avoid keeping important information there and use different passwords for different websites in a way that cannot be tracked and read SLA (Service Level Agreement) will help you better understand how cloud storage services operate and what can and cannot be stored there.
- Use the most latest versions of email filters, firewalls, and anti-malware software to protect your devices. Think about a VPN.
- Regularly create backups to an external hard disk.
- Humans have become the weakest link in this form of attack because of a lack of awareness, thus they must train.
- The proliferation of shared human data on social networking platforms in recent years has made it legal for attackers to guess passwords or steal sensitive information from businesses through posts. The way to stop similar incidents from occurring is via awareness of secure system usage.
- Always keep two-factor authentication active to protect your account from outsider or illegal access.
- Change your password regularly and at erratic intervals [I. Kotenko, M. Stepashkin, and E. Doynikova 2011].

The pie chart below shows how social engineering breaches can occur in a variety of ways, including identity theft, unauthorized financial access, annoyance, and more:

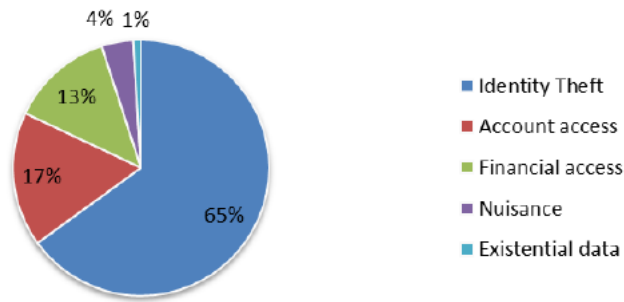


Figure 22: Breach Incidents type in Social Engineering

At first look, it is clear that identity theft accounts for the majority of social engineering attacks—2/3 of them—while existential data accounts for the smallest percentage. In addition, account and financial access are the elements that present in 17% and 13% of breach incidents, respectively. Furthermore, social engineering annoyance is aware of 4% of cases.

5.2.7 Third – Party Service Provider

The security issues mostly relating to third-party service providers were described by Mazhar et al. [M. Ali, S. U. Khan, and A. V. Vasilakos 2015].

The main security concerns with third-party CSPs are the points where virtualization, multitenancy, and shared resource pools come into play. The virtual network needs additional consideration, even if the study in this area mostly focuses on the communication and architectural views. A thorough, well-planned architecture is needed to control or monitor the traffic in order to stop information leakage, even though virtual devices were offered to protect the virtual network. Shared technologies like HV, VMs, and virtualization have opened up new security gaps for enemies. For VM security issues, rewriting the packets may provide a way to maintain a balance between privacy and monitoring.

Trusted computing is advantageous due to the tamper-proof key management. contender for offering an all-encompassing security solution for cloud computing [S. Cabuk, C. I. Dalton, A. Edwards, and A. Fischer 2008]. The CSP's policy will determine whether or not you receive the full benefits of the solution, even when the SLA provides a countermeasure for virtualization

and multitenancy. Examples of CSPs who are hesitant to provide all the necessary information for SLA transparency are Google and Microsoft [W. Halboob, H. Abbas, K. Haouam, and A. Yaseen 2014].

In above cases we have seen many of cloud security Real world scenario with the approach solutions. We can say that the security for the data in today's world is quite challenging and there are different ways from which we can secure our data.

CHAPTER 6: Conclusion and Future Scope

In conclusion, cloud computing is a relatively young technical innovation with enormous potential for global effect. It offers its consumers and companies a wide range of advantages. For instance, one of the advantages it offers to organizations is that it lowers operational costs by focusing more on the business itself and paying less on upkeep and software upgrades. However, there are still more difficulties that cloud computing must face. People have a lot of doubts about how safe and private their data is. Worldwide norms or laws do not apply to data delivered via cloud computing.

Cloud computing has the potential to be a disruptive factor through influencing the deployment and usage of technology, as we have pointed out throughout Thesis. The cloud could represent the next development in computer history similar to mainframes, minicomputers, PCs, servers, smartphones, and so on, and fundamentally altering how businesses handle their IT. Yes, there are still many unanswered questions about security in the cloud and how users and cloud service providers (CSPs) will handle problems and expectations, but to say that interest in cloud computing has grown would be a serious understatement.

It's impossible to resist the buzz around cloud computing. Consumers, companies, financial experts, and of course the CSPs themselves have all expressed interest in it. On the Internet, a search for "cloud computing" will turn up hundreds of articles describing, praising, mocking, and marketing the concept. The concept of cloud computing is so potent that, according to some, merely bringing it up might increase interest and generate more money for service providers. Amazon was a pioneer in cloud computing in December 2007.

Cloud computing has the potential to be a disruptive factor through influencing the deployment and usage of technology, as we have pointed out throughout Thesis. Be careful with rapid technological breakthroughs are resulting in a plethora of new technologies that have the potential to improve human life. However, one must exercise extreme caution to comprehend the security threats and difficulties posed by using these technologies. The same

applies to cloud computing. The main security issues and difficulties that cloud computing now faces are discussed in this thesis. Future leaders in the promotion of a safe, virtual, and financially feasible IT solution may emerge from cloud computing.

One of the major concerns that need to be addressed is data security in cloud. In particular data breaches are way up high, business, industries and organization are looking for overcoming those hindrances and protect their own data at the same time utilizes the features of emerging technology. It is therefore very much essential for researchers to concentrate more on cloud data security that will prevent hackers, intruders from getting access to sensitive data over the cloud.

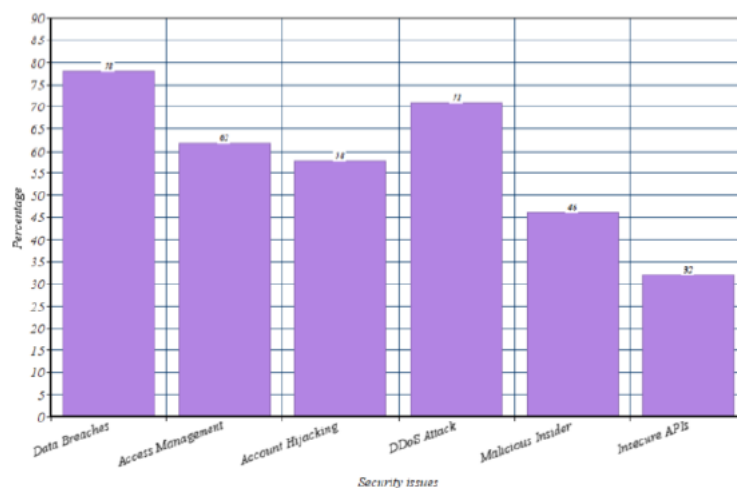


Figure 23: Data Breaches Statistics

Based on the study and insights obtained from various research papers, it shows many researchers have concentrated on internal hackers attack in data centers and few papers satisfy aspects like confidentiality, integrity of data in cloud environment. Better solution for data breaches is needed as data revolves around the cloud and everything has changed in pandemic situation with lot of internet users worldwide. In future, efficient algorithm for secure data storage and retrieval of data by end user for IOT based application can be addressed.

For the above question which were ask in the beginning of this thesis were tried to give the answer overall the research. On aspects of security is the primary aspects of every people .

How can cloud computing security issues be fixed? the crucial question. Before we can handle the security issue, we must first understand the weaknesses, risks, and hazards associated with cloud computing.

In addition to meeting legal security standards, essential security demands like availability, confidentiality, and transparency must also be taken care of. How can users of cloud computing be certain that their data is secure and always available?

Is their data protected? is a query that everybody has. The problems outlined in the core must be properly addressed. The security tree ensures that cloud computing security criteria are met when these core demands are appropriately handled.

The suggested architecture for the SLA in chapter 2 enables the governance team of the contractor to collect and evaluate quality of service indicators from the customer, supplier, and contractor for each monitored activity. As a result, we were better able to comprehend service delivery and the likely reasons for SLA deviations. Such data is crucial for service designers because it may spot bottlenecks brought on by outside variables. A request for a response from the individuals in control of these external components may be made in this situation, preventing changes to the SaaS application.

The availability and flexibility of hardware resources are both increased and administrative costs are significantly decreased thanks to virtualization. Virtualization, the foundation of cloud computing technology, is vulnerable to security risks, which include fast growth and widespread use of cloud computing. Analyzing the primary security risks that virtualisation technology faces and enhancing virtualization's security defenses are very important.

We now propose some more future works in this area.

References

1. Al Morsy. M. Grundy, J & Mueller, I. (2010). An analysis of the cloud computing security problem. 17th APSEC 2010. 30 November-03 December 2010.
2. Aziz, Abdul, and Hesham El-Rewini, Power Efficient Scheduling Heuristics for Energy Conservation in Computational Grids, Springer, 2011.
3. Abdul-Jabbar, M. D., & Aldeen, Y. A. A. S. (2023). State-of-the-Art in Data Integrity and Privacy-Preserving in Cloud Computing. *Journal of Engineering*, 29(1), 42-60.
4. Ahmed, A., Kumar, S., Shah, A. A., & Bhutto, A. (2023). CLOUD COMPUTING SECURITY ISSUES AND CHALLENGES. *Tropical Scientific Journal*, 2(1), 1-8.
5. AlSelami, F. A. (2023). Major Cloud Computing Security Challenges with Innovative Approaches. *Tehnički glasnik*, 17(1), 141-145.
6. Abeysinghe, S. (2011). "Cloud Computing Explained!" [Online]:
<http://blog.samisa.org/2011/07/cloud-computing-explained.html> [28/10/2013].
7. A Precise Model for Google Cloud Platform - 2018 IEEE by St'éphanie Challita, Faiez Zalila, Christophe Gourdin, and Philippe Merle.
8. Asma ben letaifa, Amed haji, Maha Jebalia, Sami Tabbane, —State of the Art and Research Challenges of new services architecture technologies: Virtualization, SOA and Cloud Computing||, International Journal of Grid and Distributed Computing 3(4), December 2010, 69-88.
9. A. Whitaker, M. Shaw, S. D. Gribble, —Denali: Lightweight virtual machines for distributed and networked applications||, Tech. rep. (Feb. 08 2002).
10. A Comparison between Google Cloud Service and iCloud-2019 IEEE by Hera Arif , Hassan Hajjdiab, Fatima Al Harbi2, Mohammed Ghazal
11. B. Siddhisena, Lakmal Wruasawithana, Mithila Mendis, —Next generation multi tenant virtualization cloud computing platform||, In: Proceedings of 13th International conference on advanced communication technology (ICACT), vol. 12, no.3; 2011. p.405–10.
12. B. T. Jijo, S. Zeebaree, R. R. Zebari, M. Sadeeq, A. B. Sallow, S. Mohsin, et al., "A comprehensive survey of 5G mm-wave technology design challenges," Asian Journal of Research in Computer Science, vol. 8, pp. 1-20, 2021.

13. D.Fisher "Attackers Using Amazon Cloud to Host Malware" Available: <https://threatpost.com/attackers-using-amazon-cloud-host-malware-060611/75306/> . Jun, 2011.
14. V. Zakorzhovsky "Monthly Malware Statistics" Available: <https://securelist.com/monthly-malware-statistics-june-2011/36360/>. June,2011.
15. D. Bestuzhev "Financial data stealing Malware now on Amazon Web Services Cloud". Available: <https://securelist.com/financial-data-stealing-malware-now-on-amazon-web-services-cloud/30647/>. Jun,2011.
16. I. Kotenko, M. Stepashkin, and E. Doynikova, "Security analysis of information systems taking into account social engineering attacks", IEEE 19th International Eurimicro Conference on Parallel, Distributed, and Network-Based Processing, 2011.
17. Soni M., Patel T., Jain A. (2020) Security Analysis on Remote User Authentication Methods. In: Pandian A., Senjyu T., Islam S., Wang H. (eds) Proceeding of the International Conference on Computer Networks, Big Data and IoT (ICCBi - 2018). ICCBi 2018. Lecture Notes on Data Engineering and Communications Technologies, vol 31. Springer, Cham. https://doi.org/10.1007/978-3-030-24643-3_60.
18. <https://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/> Jun,12.
19. M. Ali, S. U. Khan, and A. V. Vasilakos, "Security in cloud computing: Opportunities and challenges," Inf. Sci., vol. 305, pp. 357–383, 2015. [Online]. Available: <https://doi.org/10.1016/j.ins.2015.01.025>
20. S. Cabuk, C. I. Dalton, A. Edwards, and A. Fischer, "A comparative study on secure network virtualization," HP Laboratories, 2008.
21. W. Halboob, H. Abbas, K. Haouam, and A. Yaseen, "Dynamically changing service level agreements (slas) management in cloud computing," in Intelligent Computing Methodologies - 10th International Conference, ICIC 2014, Taiyuan, China, August 3-6, 2014. Proceedings, ser. Lecture Notes in Computer Science, D. Huang, K. Jo, and L. Wang, Eds., vol. 8589. Springer, 2014, pp. 434–443. [Online]. Available: https://doi.org/10.1007/978-3-319-09339-0_44
22. York, D. (2010). Control Channel Attacks. Seven Deadliest Unified Communications Attacks, 71–92. doi:10.1016/b978-1-59749-547-9.00004-1

23. G. Graff "How a Dorm Room Minecraft Scam Brought Down the Internet"
Available: <https://www.wired.com/story/mirai-botnet-minecraft-scam-brought-down-the-internet/>
24. M. Sri Lakshmi, Dr. S. Kumar - A Review on Wireless Network Attacks et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (2) , 2014, 2540-2542.
25. Soni M., Rajput B.S., Patel T., Parmar N. (2021) Lightweight Vehicle-to-Infrastructure Message Verification Method for VANET. In: Kotecha K., Piuri V., Shah H., Patel R. (eds) Data Science and Intelligent Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 52. Springer, Singapore. https://doi.org/10.1007/978-981-15-4474-3_50
26. T. Brewster "This Guy Hacked Hundreds Of Planes From The Ground" Available: <https://www.forbes.com/sites/thomasbrewster/2018/08/09/this-guy-hacked-hundreds-of-planes-from-the-ground/#38b0e08b46f2>
27. S. Gajek, M. Jensen, L. Lioa and J. Schneck, "Analysis of signature wrapping attacks and countermeasures", IEEE International Conference on Web Services, 2009.
28. C. Pedigo "The Biggest Cloud Breaches of 2019 and How to Avoid them for 2020"
Available: <https://www.lacework.com/top-cloud-breaches-2019/>
29. N. Hazut "Capital One Breach: How It Could Have Been Prevented" Available: <https://www.securitymagazine.com/articles/90832-capital-one-breach-how-it-could-have-been-prevented> Aug, 2019
30. H. Poston "Lessons learned: The Capital One breach" Available: <https://resources.infosecinstitute.com/lessons-learned-the-capital-one-breach/#gref>. Oct, 2019.
31. R. Rao, Vaudha, S. Bhat-International Journal of Innovative Research in Computer and Communication Engineering. Vol. 6, Issue 4, April 2018
32. IBM Cloud Education, "IaaS vs. PaaS vs. SaaS, understand and compare the three most popular cloud computing service models," 2021. [Online]. Available: <https://www.ibm.com/cloud/learn/iaas-paas-saas>

33. A. Rashid and A. Chaturvedi, "Virtualization and its role in cloud computing environment," *International Journal of Computer Sciences and Engineering*, vol. 7, no. 4, pp. 1131–1136, 2019.
34. M. I. Malik, S. H. Wani, and A. Rashid, "Cloud computing-technologies." *International Journal of Advanced Research in Computer Science*, vol. 9, no. 2, 2018.
35. B. Asvija, R. Eswari, and M. B. Bijoy, "Security in hardware assisted virtualization for cloud computing - state of the art issues and challenges," *Comput. Networks*, vol. 151, pp. 68–92, 2019. [Online]. Available: <https://doi.org/10.1016/j.comnet.2019.01.013>
36. R. Kumar and R. Goyal, "On cloud security requirements, threats, vulnerabilities and countermeasures: A survey," *Comput. Sci. Rev.*, vol. 33, pp. 1–48, 2019. [Online]. Available: <https://doi.org/10.1016/j.cosrev.2019.05.002>
37. S. Wang, Z. Liu, Q. Sun, H. Zou, and F. Yang, "Towards an accurate evaluation of quality of cloud service in service-oriented cloud computing," *J. Intell. Manuf.*, vol. 25, no. 2, pp. 283–291, 2014. [Online]. Available: <https://doi.org/10.1007/s10845-012-0661-6>
38. Cloud Security Alliance, "Top threats to cloud computing", Assets Extrahop , August 2019. Available: <https://assets.extrahop.com/pdfs/analyst-reports/CSA-Cloud-Computing-Top-Threats.pdf>
39. U Verma "instagram data breach" Available: <https://www.businesstoday.in/technology/news/instagram-data-breach-mumbai-based-chtrbox-leaks-private-data-of-social-media-influencers/story/348915.html>
40. J. Lirk "Database May Have Exposed Instagram Data for 49 Million" Available: <https://www.bankinfosecurity.com/database-may-have-exposed-instagram-personal-data-a-12503>
41. C. Pedigo "The Biggest Cloud Breaches of 2019 and How to Avoid them for 2020" Available: <https://www.lacework.com/top-cloud-breaches-2019/>
42. A. Izang, Y. A. Mensah, O. J. Omotosho, and C. P. Obioma, "Overview of Cloud Computing and Recent Addendum", *Journal of Communications Technology*,

- Electronics and Computer Science, Vol. 5, no. 5 pp. 26-32, 2016. DOI: 10.22385/jctecs.v5i0.93.
43. K. Muhammad, and Y. Z. Shao, "A survey on top security threats in cloud computing", International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 6, no. 3, pp.109-113, 2015. DOI: 10.14569/IJACSA.2015.060316
 44. S. Sengupta, V. S. Kaulgud, and V. S. Sharma, "Cloud computing security trends and research directions," in World Congress on Services, SERVICES 2011, Washington, DC, USA, July 4-9, 2011. IEEE Computer Society, 2011, pp. 524–531. [Online]. Available: <https://doi.org/10.1109/SERVICES.2011.20>
 45. A. Verma and S. Kaushal, "Cloud computing security issues and challenges: A survey," in Advances in Computing and Communications - First International Conference, ACC 2011, Kochi, India, July 22-24, 2011, Proceedings, Part IV, ser. Communications in Computer and Information Science, A. Abraham, J. L. Mauri, J. F. Buford, J. Suzuki, and S. M. Thampi, Eds., vol. 193. Springer, 2011, pp. 445–454. [Online]. Available: https://doi.org/10.1007/978-3-642-22726-4_46
 46. H. Tabrizchi and M. K. Rafsanjani, "A survey on security challenges in cloud computing: issues, threats, and solutions," J. Supercomput., vol. 76, no. 12, pp. 9493–9532, 2020. [Online]. Available: <https://doi.org/10.1007/s11227-020-03213-1>
 47. J. P. Barrowclough and R. Asif, "Securing cloud hypervisors: A survey of the threats, vulnerabilities, and countermeasures," Secur. Commun. Networks, vol. 2018, pp. 1–20, 2018. [Online]. Available: <https://doi.org/10.1155/2018/1681908>
 48. P. Qian, Z. Liu, Q. He, R. Zimmermann, and X. Wang, "Towards Automated Reentrancy Detection for Smart Contracts Based on Sequential Models", IEEE Access, vol. 8, pp 19685–19695, 2020
 49. F. Cai¹, N. Zhu¹, J. He¹, P. Mu¹, W. Li, and Y. Yu, "Survey of access control models and technologies for cloud computing", Cluster Computing, pp. 1–12, 2019.
 50. M. Masdari¹, and H. Khezri, "Efficient VM migrations using forecasting techniques in cloud computing: a comprehensive review", Cluster Computing, pp 1–30, 2020.

51. O. Fit'o and J. Guitart, "Business-driven management of infrastructure-level risks in Cloud providers", *Futur. Gener. Comput. Syst.*, vol. 32, pp. 41–53, 2014.
52. N. Li, H. Jiang, D. Feng, and Z. Shi, "Storage Sharing Optimization under Constraints of SLO Compliance and Performance Variability", *IEEE Transactions on Services Computing*, v. 12, pp 58–72, 2019.
53. Zhang, J., Zhao, X. Efficient chameleon hashing-based privacy-preserving auditing in cloud storage. *Cluster Computing*, v. 19, pp. 47–56, 2016.
54. "ElasticSearch – Open Source Search and Analytics", <https://www.elastic.co/>.
55. "Eucalyptus Cloud Platform", <https://github.com/eucalyptus/eucalyptus>.
56. Awadallah, R., & Samsudin, A. (2020, December). Homomorphic encryption for cloud computing and its challenges. In *2020 IEEE 7th International Conference on Engineering Technologies and Applied Sciences (ICETAS)* (pp. 1-6). IEEE.

VITA

I Sashi Kumari Singh was born in INDIA. I have done my Elementary schools from Nagpur city, which is also known as orange city (India). After completion of my graduation. I came to U.S.A to complete my master's in the field of Computer Science and I am doing my thesis in my last semester on the current topic.