International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 06 | June - 2022 Impact Factor: 7.185 ISSN: 2582-3930

SECURITY CHALLENGES AND SOLUTIONS ON CLOUD COMPUTING

Vinay Madhubabu Gouda

MASTER OF COMPUTER APPLICATION (MCA)

Audyogik Shikshan Mandal's

Institute of Management & Computer Studies (MCA Institute) (IMCOST)

UNIVERSITY OF MUMBAI

Abstract

In the previous couple of years, cloud computing has been included in various fields and industries, from Health Science and Medical to Military Arm forces, which has been scrupulously followed by exploring related multi-technologies within the industry and academic levels. Many enterprises and computing model companies have shifted from on-site or on-premises infrastructure to remote datacenters which is accessible via internet and managed by cloud service providers such as Azure, AWS, Google Cloud, IBM Cloud, etc. However, this drastic shift in computing technology introduces security concerns to individual and enterprise companies. To extend cloud development, Integration and deployment, these security concerns must be rigorously reviewed and addressed.

Cloud computing is defined as a brand new technology to deliver services within the name of cloud or remote through internet. This technology transformed over traditional data processing system to store large amount of data. Cloud computing provides the user the ability to access information anytime from anywhere remotely. Cloud is definitely useful for business that might not afford for hardware and maintenance team to work by 24 hours to keep the business alive. Because the data is within the cloud stored in various places not locally or company's private area. The data will be exposed for attacking from hackers and business enemies. In this paper, I tried to demonstrate the security challenges and issues caused by nowadays industries, while addressing various key topics such as vulnerabilities, threats and mitigations, and cloud models.

Keywords: Security, Internet, Cloud, Business

1. Introduction

Cloud computing is a model for rapid, on demand and desirable network access to a shared and different network. Configurable computing resource pool (e.g., networks, servers, storage, software, and services) that includes configurable computing resources. With minimum management efforts or service provider collaboration, it can be easily and quickly provisioned and published on the network. Many of us are going to see a drastic change in

IT industry in our lives and the market demand. Current development in the world of computation may have remarkably altered the way computing, as well as definition of Capital Expenditure in computing. In cloud computing network, the services are generally in the on premise or network of someone else and accessed cloud users remotely. Configuration and management is performed remotely, meaning that a personal data, confidential data and other items need to be sent to a cloud infrastructure for processing, and the output is returned. Upon completion of the requested processing in certain incidents, it might be appropriate or at least flexible for a person to store data on remote network cloud servers. This includes the following three situations that are of special interest in the organizational context of cloud computing:

• Transmission of confidential & private data to the cloud server.
• Transmission of information from the cloud servers to the computers of the clients.
• Storage of confidential private data of customers on cloud servers that are remote servers not managed by customers.

Both above three cloud computing situations are severely harmful to security breaches that make study and investigation on the security aspects of cloud computing practice an essential. There have been a different types that are being used in the cloud storage, but the simple principle remains the same – infrastructure, or service stay remotely place with someone else's ownership, and customers uses it for the time and pay how much they use it infrastructures.

The research discussed in this paper is formatted with a view to defining the solutions to cloud security problems and queries that are necessary to be contemplate in this paper. The importance of security in cloud computing, security challenges, threats, attacks, solutions, and critical analysis of existing solutions was considered in the context of the debate of this article.

2. Background

2.1 Cloud overview

Cloud providing structural models are featured by the ownership, size and access. It tells the concept of the cloud. The greater a part of the associations are need to execute cloud since it decreases the consumption and controls cost of activity. Cloud computing began its base within the mid of 2007 and is developing quickly till now. It`s different highlights that make clients have to change to the distributed computing environment. A number of these highlights are examined beneath:

Convenience:

There is no compelling reason to claim and appear after requirement, programming and different assets and properties by the cloud client. The cloud administrations are straight forwardly gotten to utilizing an online browser. No additional resources are expected to run and execute in the cloud administration. A fundamental work area with typical web network is adequate.

Diminished expense:

For making a path into a business, cost efficiency is needed for framework is decreased by moving to the cloud. As registering compute power, storage and required assets are utilized from cloud; cost to shop the products over the period is incredibly influenced. It`s beneficial for the associations if the assets are required by them only for little span. So as hostile possessing them cloud is a superior choice for a business.

Multi-Tenure:

A single information server, compute power are shared among various number of clients by utilizing virtualization. This is called as a Multi-tenancy, allows productive usage of resources.

Hardware and Site independency:

The cloud services are hosted within the web and may be access through web browsers. So, it means people can have the benefit of the services anytime from anywhere. Moreover, many companies can maintain the resources remotely through internet.

Reliability:
Numerous resources are accessible like figuring compute power, Storage and network so forth for offering types of assistance to the cloud customers. Likewise, the information might be put away in various areas by owners. This excess as far as information stock piling and other resource empowers arrangement for debacle recuperation and accomplishes unwavering quality and accessibility of information just as administrations.

2.2 Types of cloud

2.2.1 Private cloud

It is also called inside cloud. This stage for distributed computing is executed on cloud based secure climate and it is protected by a firewall which is administered by the IT Team that has a place with a specific professional support team. Private cloud allows just the granted clients or private clients and gives the association to the clients more prominent power over their information and data. The actual PCs and servers might be arranged inside or remotely datacenters they give the resources from a particular pool to the private cloud. Organizations having unexpected incidents or dynamic needs, activities which are related to administration requests, uptime necessities and IT Service Management are more qualified to receive private cloud. In private cloud there is not much requirement for additional security, security guidelines and data transfer capacity restrictions that can be available in a public cloud region. Customers and Cloud service providers have a control of the improved framework and managed security, since client's entrance and the organizations utilization are limited. Probably the best model is Microsoft Azure.

2.2.2 Public cloud

It is a kind of cloud providing services in which the cloud administrations are conveyed over an organizations that is open and accessed over remotely for public usability. This model is in realm noticeable of cloud providers. In this the cloud model featured as a organization offers, varieties of assistance and managed framework to different region clients.

Clients do not have any power over the area of the foundation (Infrastructure are owned by cloud providers). There might be almost no or no difference among public and private basic plan aside from the security level that are offered for different departments given to the public cloud support teams or channels like communities or third party venders by the cloud service providers. Public cloud is appropriate for business requirements and load which are monitored and supervised. Because of the capital expenditure (CapEx) overheads and operational cost (OpEx), the public cloud model is conservative and stable. Providers may offer the free assistance or permit strategy like compensation per client. The expense is shared by all the clients in broad of daylight cloud. It gives advantage to the clients by accomplishing economically scale up. Public cloud datacenters are accessible over the internet for example of a public cloud is Google or Google Cloud.

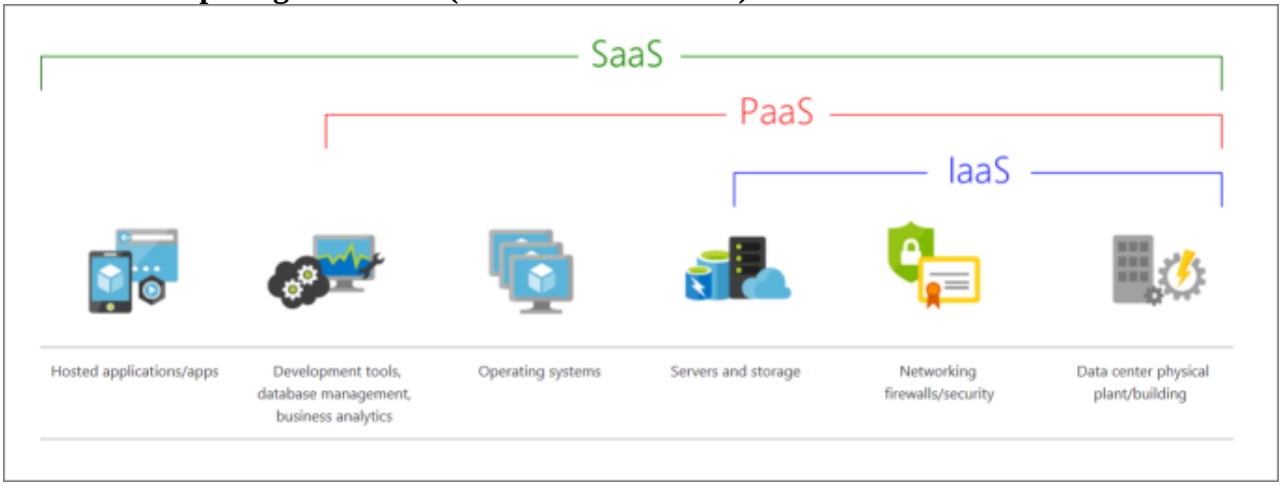
2.2.3 Hybrid Cloud

It is a kind of distributed computing, which is synchronized and coordinated. It could comprise two types of cloud (public and private) and with same or different cloud providers, for example both of the blend of private, public cloud that is bound together to work for singular client. Different departments or teams or cloud providers are equipped for convergence, disconnection and defeating limits by the cloud providers; hence, it can be classified into public, private cloud. It permits the client to expand the limits and resources just as the ability to adopt, Management and customization with another cloud administration. In a half and half cloud, the assets or resources are overseen either op-premises or by Cloud providers. It is a differentiation between two stages wherein the remaining activities is managed between the private and the public cloud according to the requirements and request of client association. Assets which are automated like turn off events and test remaining tasks at hand can be remain on-premises in the public cloud that has a place with an outsider or cloud provider.

While the remaining tasks or burdens are basic or easy to keep housed inside. Associations may lead to utilize the crossover cloud model for preparing large information and coordination. Half and half cloud providers has

highlights like adaptability and security.

2.3 Cloud computing as services (cloud service models)



2.3.1 Infrastructure as a Service (IaaS)

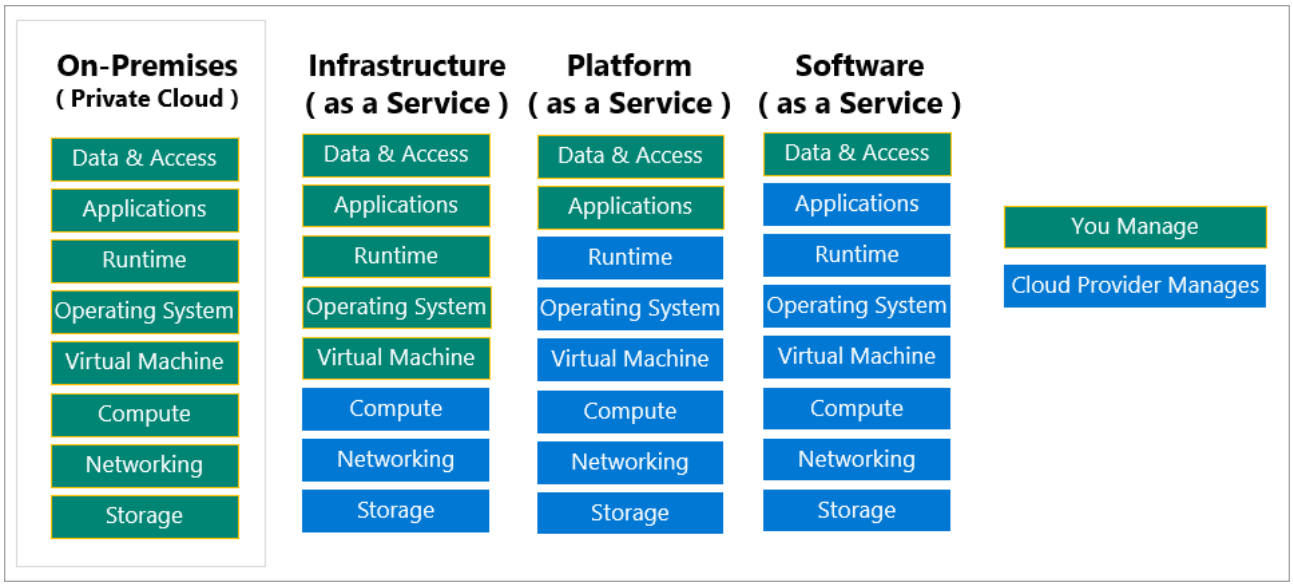
This cloud service model is the nearest to managing physical servers, a cloud provider will keep the hardware up-to-date and latest as per new launches, but operating system maintenance and network configuration is up to the client as the cloud tenant. For example, GCP virtual machines are fully operational and the virtual compute power and devices running in Google cloud datacenters. The benefits of this cloud service model is a fastest deployment of new compute devices and resources. Configuring a new virtual machine is normally faster than acquiring, installing, and setting up a physical server.

2.3.2 Platform as service

Platform as service (PaaS) is a sort of distributed computing administrations or a managed hosting environment that gives a stage that permits the clients to create, run, and test applications without having to worry about the infrastructure, physical hardware and software requirements. One need not be worried about lower level components of hardware infrastructure, storage and datacenters, security and networking this is accomplished by the cloud specialist from cloud providers. Client developers deal with the applications. Applications utilizing PaaS acquire cloud trademark and agreements, For example, GCP App engine services provides a managed hosting and distributed computing environment where developers or programmers can upload their web applications code, without having to worry about the physical hardware and software requirements. This model benefits since it diminishes the measure of coding, automates business strategy, and help in moving applications to hybrid or PaaS model.

2.3.3 Software as services

Software as services (SaaS) is developing rapidly. In this cloud service model, the cloud provider manages all characteristics of the application environment, such as compute power, networking resources, datacenters or storage, and applications. The cloud tenant or client only needs to provide their information to the application managed by the cloud provider. SaaS applications can be run from an online browser and no need to download, however this requires account or access. The cloud provider furnishes the customer requirements with the capacity to send an application on a cloud. Because of this web conveyance model SaaS eliminates the need to create and run applications on single PC. SaaS providers typically offer program-based graphical user interface. APIs are typically similar made accessible for engineers and developers. For example, GSuite provides a fully working version of Google Apps such as gmail, office, maps, drive that runs in the cloud. All you need to do is create your account, and Gsuite takes care of everything else and provides usability.



Advantages

No CapEx- Clients do not have up-front costs.

Agility- Applications can be accessible quickly and remotely, and it can be deprovisioned whenever needed.

Management- The shared responsibility model applies to the clients, manages and maintains the resource services they have provisioned, and the cloud provider owns and manages the cloud infrastructure hardware behalf of clients.

Consumption-based model for IaaS- Organizations pay only and billed for what they use and operate their provisioned under an Operational Expenditure (OpEx) model.

Skills- No deep technical skills are required to deploy, use, and gain the advantages of a public cloud. Organizations can utilize the skills and expertise of the cloud provider professionals to ensure workloads are secure, safe, and highly available on the cloud and in the remote locations.

Cloud benefits- Organizations can utilize the skills and expertise of the cloud provider professionals to ensure workloads are secure, safe, and highly available on the cloud and in the remote locations.

Flexibility. IaaS is the most flexible and adaptable cloud service because the clients have control to configure and manage the hardware running your application.

Pay-as-you-go model- Users or clients pay for the software they have used on a subscription model, mostly monthly or yearly, regardless of how much they used the software.

3. Security on cloud

The information moved on the cloud is habitually seen as crucial to individuals with pernicious point. There is a huge demand of individuals information and possibly secure data that people store on their personal assets, and this information is as of now being moved and stored to the cloud. This makes it fundamental for the individuals to appreciate the wellbeing possibility that our cloud provider has set up, and it is comparably simple and easy to avoid any and all types of risks to ensure about our data. The essential thing has brought to research is the security venture that our cloud provider provision has set up. These vary from cloud provider to cloud provider and among the various kinds of features. Which type of encryption methodologies they provide? What methodologies for confirmation do they have set up for the real time environment that our data will be taken care properly? Will they have security firewalls for my data? Do they have fortification methods? In case client have an organizational cloud, what barrier are set up to keep our information safe and separate from
various other organization? Many cloud providers have standard rules and regulations or terms and conditions that may impact to these requests, anyway the individual customer will probably have never have anything trade

room in their cloud contract. An organizational customer may have fairly more data and space to analyze the arrangements and requirements of their concurrence with the provider and will have the chance to represent these requests during the provisioning. It is easy to pick a cloud provider that provide the security of our data as a huge concern and perturb.

Security in cloud computing is a major concern for clients or end users. Data in cloud should be stored in an encrypted format. To limit client from accessing the shared data directly, proxy services should be implemented. Despite how worry the clients are with their own data, by purchasing into the cloud they will give up some access or control to an external source. This detachment among the individuals and the actual datacenters of our data makes a perimeter. It may similar manner to make more data and space for an client to get to their information. Regardless, to misuse the advantages of the cloud, cloud providers brought to intentionally give up direct control of their data. A cloud provider probably has a huge demand of resources and influence than the ordinary customer to ensure about their personal assets and associations.

3.1 Threats in cloud computing and the Solutions

3.1.1 Authentications

Organizations on occasion battle with individual differences the board as they effort to achieve to allow permission for something suitable to the client's employment. They in some cases neglect to terminate client opportunity when a profession work changes, or a client leaves the organization. The Song of exercise through special force uncovered in necessary millions of client records, was the after effect of taken client techniques.

Solution: In Microsoft Azure, it provides passwordless authentication methods such as Windows Hello, FIDO2 security keys, and the Microsoft Authenticator app because they provide the most secure sign-in experience and commonly can use username & password. Azure AD Multi-Factor Authentication (MFA) adds additional security over the AD accounts only using a password when a user signs in. It is very simple to remove or delete the user or client accounts and permissions which are directly connected to Azure AD.

3.1.2 Data sections

Cloud cases face an outstanding number of corresponding dangers as current corporate organizations, however since a lot of data is put away on cloud workers, vendors have become a captivating objective. The seriousness of the damage will in general calculation upon the affectability of the data that is disclosed. Individual economically data grabs the features, however, get deeply in including government data, exclusive advantages can be more destroying. At the point when the data penetration happens, an organization might be open to legal activity. Penetrate examinations and client warnings can build up the most difficulty in expenses. indirect impacts may cause brand harm and loss of business can affect the organizations'.

Solution: Many cloud providers facilitate employees to work on client locations or either remote locations with a powerful VDI (Virtual Desktop Interface) where they are restricted by copy paste, transferring data to local machines or other places. For windows VDI users they restricted by group polices and Linux VDI users they restricted by ACLs, etc. So there is no chance to leakage or disclosure of organizations, govt., confidential data. They have implemented policies like penalties, punishment and jail if employee violates company rules and regulations.

3.1.3 Application APIs

Today each and every cloud organization and application presently offers APIs. IT industries utilizes these interfaces and APIs to oversee and communicate with cloud administrations, including those that offer cloud provisioning, the executives and checking. The security, safety and accessibility of cloud organizations calculate upon the security of the interface risk is expanded with outsiders who depend on APIs and extend on these interfaces, as organizations may need to remove more administrations and licenses. APIs and weak interfaces may open organizations to security and privacy related issues, for example, privacy, responsibility, accessibility APIs and interfaces are the especially not closed piece of the framework since they can be gotten to from open

Web.

Solution: Every cloud vendor offers various API security controls. AWS provides two services to control - API Gateway and AWS IAM - which you can use to establish safe and secure API connections and manage access to data and VMs. Azure offers the authorization keys, OAuth and JWTs, as well as client certificate authentication security controls. GCP offers OAuth 2.0, SAML policies, and API keys to strength the APIs.

3.1.4 Account logins

Giving false representation, Phishing, and programming issues are exceptionally widely spread today, and cloud organizations add another scope to the danger since attacker can listen on work, control exchanges, and changing information. Attackers might have chance to utilize the cloud application to delivering of different attacks.

Solution: Organizations should not allow sharing of record licenses among clients and profits and should get more power to mixed validation plans where they are accessible. Records must be observed with the aim that each exchange need to be followed to a human. The key is to shield account licenses from being taken.

3.1.5 DDoS attack

DDoS attack have been around for entirely a while and they get outstanding quality again on account of distributed computing since they mostly influence permission. Frameworks may run normally or essentially break. These DDoS attacks suffer-through a lot of handling power, a bill the client may at last need to pay. High-volume DDoS attacks are very quietly normal, yet organizations need to meanwhile know about shift and application-level DDoS attacks, which target on the Web worker and database slowness.

Solution: They are many security solutions provided to protect cloud from DDoS Attack such in Azure – Azure DDoS Protection which monitors & restricts the attackers in a network, AWS - Amazon CloudFront and Amazon Route 53 which mitigates the attacks, GCP - Google Cloud Armor which is network security service that offers defenses against DDoS and application attacks, and provides a rich set of WAF rules.

3.1.6 System bugs

Weaknesses in framework, available bugs in code had become the most important issue with the coming of distribution in distributed computing. Organizations share memory, databases and properties in near to each other, making new attack places. The cost of moderating framework weakness are slowly little closed with other IT needs. The cost of setting up IT cycles to discover and fix weaknesses is little when in compared with the expected loss.

Solution: Azure visual studio provides strong debugging and tips to improve and strengthen the code, AWS - Amazon ECS with AWS Fargate which provides debugging services in compute resources.

3.1.7 Inadequate diligence

Organizations bearing distributed computing without having total grip of the climate and harms related with it might experience an huge number of business, financial, specialized, legal, and consistence chances. cleverness is required whether the organization is trying to relocate to the cloud or assembling with another organization in the cloud. For example, organizations that ignore to inspect an agreement may not know about the vendor's risk in the event of data mischance or break. Operational and building issues could come up if an association improvement group is eager about with cloud advances as applications are spread to a specific cloud. An organization need to do satisfactory exploration preceding to moving to distributed computing as a result of the danger related with it.

Solution: Azure Cloud Services Due Diligence Checklist - accurately identify your objectives, goals and requirements before choosing a cloud service provider, Azure Board provides proven productivity tools. Get your work complete with simplest and modern agile tools like Kanban boards, backlogs, sprints, dashboards and scrum boards.

3.1.8 Database security

Programmers present in the past had erased from cloud to cause hurt to organizations and cloud server farms are as unprotected against destructive events as any office. Cloud suppliers may suggest spreading applications and

data over various ranges for better assurance. Everyday data reinforcement and off-site stockpiling are important with consumption of cloud conditions. The weight of forestalling information mischance isn't just of cloud specialist, yet additionally of information supplier. A client may struggle information before transferring it on the cloud, at that point that client must be minded so as to get the encryption key. On the off chance that the key is lost, at that point the data will be lost. Agreeable strategies multiple times indicate how long organizations must hold records of review and different archives. Losing such sensitive data may have genuine outcomes.

Solution: Azure SQL Database, newly created databases are encrypted by default and the database encryption key is protected by a built-in server certificate. GCP – Cloud SQL, Cloud Spanner, BigQuery, Cloud Bigtable, Firestore, Firebase realtime database, Memorystore, Google's encrypting SQL proxy.

4. Security challenges and solutions on cloud computing

4.1 Malicious attacking

Security issues can happen from both outside and inside the organizations. In a cloud environment, an insider can access and corrupt entire infrastructure or control or steal information. Frameworks that rely exclusively upon the cloud specialist co-operation for security are utmost serious issues.

4.2 Database backup

The cloud provider brought to guarantee that the backups of information is triggered that even security measures with all aspects. However, the backup information is commonly found in decoded or decrypted structure which can prompt abuse of the information by unapproved or not permitted individuals. In this way information backups lead to different security challenges. More the employee virtualization builds, a very problematic issue with backup and capacity is driven. Information reduplication is one of the solution for diminish backup and disconnected into large volumes.

4.3 Unencrypted data

Data encryption is a cycle that assists with illuminating different outside and malicious issues. Decoded information is truly powerless for weak information, as it doesn't give any security power. Decoded information can be shared to or by unapproved clients and the client data which prompts cloud employees to get away from different informational data to outside clients.

4.4 Flooding requests

In this type of attack, the intruder sends huge number of requests in the form of mails or service requests for assets on the cloud quickly so the cloud traffic gets overflowed with the large volume of requests. This delays or stops the cloud server not to responding to clients.

4.5 SQL injection attack

These attacks are known to be dangerous follow up on the cloud computing wherein a malicious code is embedded into a SQL code or request. This attack permits the intruder to increase unapproved admit the access to the data set and to other private or confidential data. SQL infusion can be utilized to attack any type of SQL information basis. The issue that SQL infusion and different intentions are conceivable is on the foundation that security is deficiently more noticeable being developed.

4.6 Internet browser

Clients or Users use web browsers or internet to send the data on network. These programs use internet protocols SSL innovation to clamber client's identity and credentials. Unfortunately, hackers or outsiders from the middleware may acquire or break these qualifications by utilizing sniffing bundles introduced on the delegate permits and damage the assets.

Solutions:

- Multifactor authentication and encryption mechanism are two of the security prevention that ensure protection against Malicious attack, Safe browsing and unencrypted data.

- Use Windows cloud defender and other antivirus protection tools and services to keep infrastructure safe and secure against threat attacks.
- Installing and use monitoring tools, threat detection tools in Cloud services.
- Make the infrastructure available all-time 24/7 as robost with availability sets and zones, disaster recovery in regional and globally.
- Cloud providers needs to ensure effective policies, and proper analysing, tracing, logging, auditing and monitoring of administrators and users activities.
- Eliminate unnecessary data to store in cloud, use auditing tools to keep secure Storage.
- Restrict unnecessary logins and permissions on cloud, use IAM roles and permission and AD roles and permissions to provide specific role to individuals.

5. Conclusion

Cloud computing has huge possibilities to keep safe and secure remotely, but the security issues installed in cloud computing approach are admissibly corresponding for its offered potential benefits and profits. Cloud computing is a gigantic opportunity and worthwhile choice both to the organizations and the individuals – either different people can have their own personal choices from Cloud computing. The immense prospects of Cloud computing can't be looked exclusively for the security challenges and reasons – the continuous observation, research and exploration for reliable and coordinated security mechanism for Cloud computing could be the main way of inspiration to future generations. Security for Cloud computing environment is a non-trading off prerequisite. It is unavoidable to turn into the ideal and constant way to deal with business development and processing in spite of the fact that the security limitations alongside various issues should be cleared for cloud computing to make it more preferable for business organizations and individuals.

6. Reference

1. Dhanamma SHANKAR Jagli Vivekanand Education Society's Institute of Technology “Cloud Computing and Security Issues”
2. Jawahar Alharthi, Dr.Sabah Alzahrani College of Computers and Information Technology, Taif University, Saudi Arabia, Vol 2, Issue21, 05 January 2021.
3. https://docs.microsoft.com/en-us/azure/
4. https://cloud.google.com/docs
5. https://docs.aws.amazon.com/