Engineering and Scientific International Journal (ESIJ)
Volume 11, Issue 1, January – March 2024
ISSN 2394-7187(Online)
ISSN 2394 - 7179 (Print)

Cloud Computing and Cloud Security Issues and Threats in 2024

Dr .Srinivasa Rao Kadari
Assistant Professor of Computer Science, BJR Government Degree College, Ayanaguda, Hyderabad

Abstract — Cloud computing hides the details of the system implementation from the end users and developers. Applications runs on the undefined physical systems. Similarly, data is stored at undetermined locations. The systems administration is outsourced to others and accessed by the user globally. For the organizations making their transition to cloud, cloud security is an essential factor while choosing a cloud provider. The attacks are getting stronger day by day and so the security needs to keep up with it. For this purpose it is essential to pick a cloud provider who offers the best security and is customized with the organization's infrastructure. Cloud security has a lot of benefits cloud security has become a top priority for most industries operating in the cloud environment. Cloud service providers and adopters don't consider it as a discrete practice; instead, they embrace and consider it as a primary aspect of overall security practice and data protection strategy. From small and large to enterprise-level organizations, it has become a go-to solution for everyone at the current time. Automation and modern cloud technologies have made cloud security much more advanced and allow it to deal with security issues effectively. However, maintaining in-house cloud security was challenging, which is why many organizations emerged in the market to offer optimum cloud security solutions to everyone. Currently, many top organizations

Keywords: *Cloud Computing; Security Issues; Unauthorized Access; DoS; Threats.*

1. Introduction

Cloud computing refers to the on demand delivery of computing services such as applications, computing resources, storage, database, networking resources etc. through internet and on a pay as per use basis. At the present time the demand for cloud computing services are increasing with respect to that demand for cloud computing skills is also increasing. It provides three main types of service models i.e. SaaS (Software as a Service), PaaS (Platform as a Service) and IaaS (Infrastructure as a Service). With this as starting from small to large organizations have started using cloud services so depending upon their requirement they go for the different types of cloud like Public cloud, Private cloud, Hybrid cloud, Community cloud.

1.1 Security in Cloud Computing

Cloud computing which is one of the most demanding technology of the current time, starting from small to large organizations have started using cloud computing services. Where there are different types of cloud deployment models are available and cloud services are provided as per requirement like that internally and externally security is maintained to keep the cloud system safe. Cloud computing security or cloud security is an important concern which refers to the act of protecting cloud environments, data, information and applications against unauthorized access, DDOS attacks, malwares, hackers and other similar attacks. Community Cloud: These allow to a limited set of organizations or employees to access a shared cloud computing service environment.

1.2 Benefits of Cloud computing

It is accessible to all the users (proper credentials) without any restriction, using the cloud for applications is cost-efficient, Least the possibility of access failure due to non-dependency on a single machine, Cloud provides independence from machine access. URL gives access to infrastructure all the time, Real time user access. Multiple users can access the same application and can work on it (Example: Google Doc). Cloud is reliable for Backup and recovery since data storage is not server-specific, Cloud computing is the best platform to showcase your applications/software worldwide. Users can access your application & work on it using a single link, Flexibility to access it from anywhere makes it popular among users and service-providing industries.

1.3 Planning of security in Cloud Computing

As security is a major concern in cloud implementation, so an organization have to plan for security based on some factors like below represents the three main factors on which planning of cloud security depends.

- Resources that can be moved to the cloud and test its sensitivity risk are picked.
- The type of cloud is to be considered.
- The risk in the deployment of the cloud depends on the types of cloud and service models.

1.4 Types of Cloud Computing Security Controls

There are 4 types of cloud computing security controls i.e.

ISSN 2394-7187(Online)
ISSN 2394 - 7179 (Print)

- Deterrent Controls: Deterrent controls are designed to block nefarious attacks on a cloud system. These come in handy when there are insider attackers.
- Preventive Controls: Preventive controls make the system resilient to attacks by eliminating vulnerabilities in it.
- Detective Controls: It identifies and reacts to security threats and control. Some examples of detective control software are Intrusion detection software and network security monitoring tools.
- Corrective Controls: In the event of a security attack these controls are activated. They limit the damage caused by the attack.

1.5 Importance of Cloud Security

For the organizations making their transition to cloud, cloud security is an essential factor while choosing a cloud provider. The attacks are getting stronger day by day and so the security needs to keep up with it. For this purpose it is essential to pick a cloud provider who offers the best security and is customized with the organization's infrastructure. Cloud security has a lot of benefits –

- Centralized security : Centralized security results in centralizing protection. As managing all the devices and endpoints is not an easy task cloud security helps in doing so. This results in enhancing traffic analysis and web filtering which means less policy and software updates.
- Reduced costs : Investing in cloud computing and cloud security results in less expenditure in hardware and also less manpower in administration
- Reduced Administration : It makes it easier to administer the organization and does not have manual security configuration and constant security updates.
- Reliability : These are very reliable and the cloud can be accessed from anywhere with any device with proper authorization.

When we are thinking about cloud security it includes various types of security like access control for authorized access, network segmentation for maintaining isolated data, encryption for encoded data transfer, vulnerability check for patching vulnerable areas, security monitoring for keeping eye on various security attacks and disaster recovery for backup and recovery during data loss.

There are different types of security techniques which are implemented to make the cloud computing system more secure such as SSL (Secure Socket Layer) Encryption, Multi Tenancy based Access Control, Intrusion Detection System, firewalls, penetration testing, tokenization, VPN (Virtual Private Networks), and avoiding public internet connections and many more techniques.

But the thing is not so simple how we think, even implementation of number of security techniques there is always security issues are involved for the cloud system. As cloud system is managed and accessed over internet so a lot of challenges arises during maintaining a secure cloud. Some cloud security challenges are

- Control over cloud data
- Misconfiguration
- Ever changing workload
- Access Management
- Disaster recovery

1.6 Cloud Computing

Cloud computing is a type of technology that provides remote services on the internet to manage, access, and store data rather than storing it on Servers or local drives. This technology is also known as Serverless technology. Here the data can be anything like Image, Audio, video, documents, files, etc.

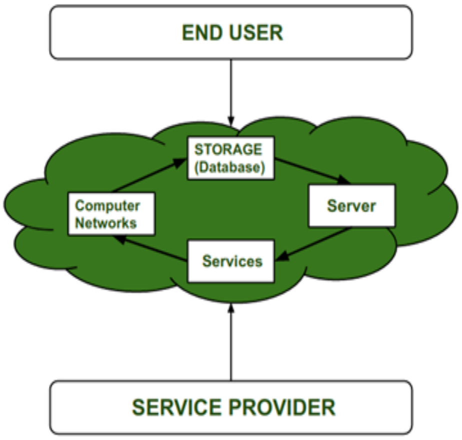

Fig.1: Remote Services of Cloud Computing

1.7 Need of Cloud Computing

Before using Cloud Computing, most of the large as well as small IT companies use traditional methods i.e. they store data in Server, and they need a separate Server room for that. In that Server Room, there should be a database server, mail server, firewalls, routers, modems, high net speed devices, etc. For that IT companies have to spend lots of money. In order to reduce all the problems with cost Cloud computing come into existence and most companies shift to this technology.

1.8 Security Issues in Cloud Computing

There is no doubt that Cloud Computing provides various Advantages but there are also some security issues in cloud computing. Below are some following Security Issues in Cloud Computing as follows.

DOI: 10.30726/esij/v11.i1.2024.111002

1.8.1 Data Loss

Data Loss is one of the issues faced in Cloud Computing. This is also known as Data Leakage. As we know that our sensitive data is in the hands of Somebody else, and we don't have full control over our database. So, if the security of cloud service is to break by hackers then it may be possible that hackers will get access to our sensitive data or personal files.

1.8.2 .Interference of Hackers and Insecure API's

As we know, if we are talking about the cloud and its services it means we are talking about the Internet. Also, we know that the easiest way to communicate with Cloud is using API. So it is important to protect the Interface's and API's which are used by an external user. But also in cloud computing, few services are available in the public domain which are the vulnerable part of Cloud Computing because it may be possible that these services are accessed by some third parties. So, it may be possible that with the help of these services hackers can easily hack or harm our data.

1.8.3 User Account Hijacking

Account Hijacking is the most serious security issue in Cloud Computing. If somehow the Account of User or an Organization is hijacked by a hacker then the hacker has full authority to perform Unauthorized Activities.

1.8.4 Changing Service Provider

Vendor lock-In is also an important Security issue in Cloud Computing. Many organizations will face different problems while shifting from one vendor to another. For example, An Organization wants to shift from AWS Cloud to Google Cloud Services then they face various problems like shifting of all data, also both cloud services have different techniques and functions, so they also face problems regarding that. Also, it may be possible that the charges of AWS are different from Google Cloud, etc.

1.8.5 Lack of Skill

While working, shifting to another service provider, needs an extra feature, how to use a feature, etc. are the main problems caused in IT Company who doesn't have skilled Employees. So it requires a skilled person to work with Cloud Computing.

1.8.6 Denial of Service (DoS) attack

This type of attack occurs when the system receives too much traffic. Mostly DoS attacks occur in large organizations such as the banking sector, government sector, etc. When a DoS attack occurs, data is lost. So, in order to recover data, it requires a great amount of money as well as time to handle it.

1.9 Main Cloud Security Issues and Threats in 2024

Almost every organization has adopted cloud computing to varying degrees within their business. However, with this adoption of the cloud comes the need to ensure that the organization's cloud security strategy is capable of protecting against the top threats to cloud security.

1.10 Misconfiguration

Misconfigurations of cloud security settings are a leading cause of cloud data breaches. Many organizations' cloud security posture management strategies are inadequate for protecting their cloud-based infrastructure.

Several factors contribute to this. Cloud infrastructure is designed to be easily usable and to enable easy data sharing, making it difficult for organizations to ensure that data is only accessible to authorized parties. Also, organizations using cloud-based infrastructure also do not have complete visibility and control over their infrastructure, meaning that they need to rely upon security controls provided by their cloud service provider (CSP) to configure and secure their cloud deployments. Since many organizations are unfamiliar with securing cloud infrastructure and often have multi-cloud deployments – each with a different array of vendor-provided security controls – it is easy for a misconfiguration or security oversight to leave an organization's cloud-based resources exposed to attackers.

1.11 Unauthorized Access

Unlike an organization's on-premises infrastructure, their cloud-based deployments are outside the network perimeter and directly accessible from the public Internet. While this is an asset for the accessibility of this infrastructure to employees and customers, it also makes it easier for an attacker to gain unauthorized access to an organization's cloud-based resources. Improperly-configured security or compromised credentials can enable an attacker to gain direct access, potentially without an organization's knowledge.

1.12 Insecure Interfaces/APIs

CSPs often provide a number of application programming interfaces (APIs) and interfaces for their customers. In general, these interfaces are well-documented in an attempt to make them easily-usable for a CSP's customers.

However, this creates potential issues if a customer has not properly secured the interfaces for their cloud-based

ISSN 2394-7187(Online)
ISSN 2394 - 7179 (Print)

infrastructure. The documentation designed for the customer can also be used by a cybercriminal to identify and exploit potential methods for accessing and exfiltrating sensitive data from an organization's cloud environment.

1.13 Hijacking of Accounts

Many people have extremely weak password security, including password reuse and the use of weak passwords. This problem exacerbates the impact of phishing attacks and data breaches since it enables a single stolen password to be used on multiple different accounts.

Account hijacking is one of the more serious cloud security issues as organizations are increasingly reliant on cloud-based infrastructure and applications for core business functions. An attacker with an employee's credentials can access sensitive data or functionality, and compromised customer credentials give full control over their online account. Additionally, in the cloud, organizations often lack the ability to identify and respond to these threats as effectively as for on-premises infrastructure.

1.14 Lack of Visibility

An organization's cloud-based resources are located outside of the corporate network and run on infrastructure that the company does not own. As a result, many traditional tools for achieving network visibility are not effective for cloud environments, and some organizations lack cloud-focused security tools. This can limit an organization's ability to monitor their cloud-based resources and protect them against attack.

1.15 External Sharing of Data

The cloud is designed to make data sharing easy. Many clouds provide the option to explicitly invite a collaborator via email or to share a link that enables anyone with the URL to access the shared resource. While this easy data sharing is an asset, it can also be a major cloud security issue. The use of link-based sharing – a popular option since it is easier than explicitly inviting each intended collaborator – makes it difficult to control access to the shared resource. The shared link can be forwarded to someone else, stolen as part of a cyber-attack, or guessed by a cybercriminal, providing unauthorized access to the shared resource. Additionally, link-based sharing makes it impossible to revoke access to only a single recipient of the shared link.

1.16 Malicious Insiders

Insider threats are a major security issue for any organization. A malicious insider already has authorized access to an organization's network and some of the sensitive resources that it contains. Attempts to gain this level of access are what reveals most attackers to their target, making it hard for an unprepared organization to detect a malicious insider.

On the cloud, detection of a malicious insider is even more difficult. With cloud deployments, companies lack control over their underlying infrastructure, making many traditional security solutions less effective. This, along with the fact that cloud-based infrastructure is directly accessible from the public Internet and often suffers from security misconfigurations, makes it even more difficult to detect malicious insiders.

1.17 Cyber attacks

Cybercrime is a business, and cybercriminals select their targets based upon the expected profitability of their attacks. Cloud-based infrastructure is directly accessible from the public Internet, is often improperly secured, and contains a great deal of sensitive and valuable data. Additionally, the cloud is used by many different companies, meaning that a successful attack can likely be repeated many times with a high probability of success. As a result, organizations' cloud deployments are a common target of cyberattacks.

1.18 Denial of Service Attacks

The cloud is essential to many organizations' ability to do business. They use the cloud to store business-critical data and to run important internal and customer-facing applications. This means that a successful Denial of Service (DoS) attack against cloud infrastructure is likely to have a major impact on a number of different companies. As a result, DoS attacks where the attacker demands a ransom to stop the attack pose a significant threat to an organization's cloud-based resources.

1.19 Main Cloud Security Concerns in 2024

In the Cloud Security Report, organizations were asked about their major security concerns regarding cloud environments. Despite the fact that many organizations have decided to move sensitive data and important applications to the cloud, concerns about how they can protect it there abound.

1.20 Data Loss/Leakage

Cloud-based environments make it easy to share the data stored within them. These environments are accessible directly from the public Internet and include the ability to share data easily with other parties via direct email invitations or by sharing a public link to the data. The ease of data sharing in the cloud – while a major asset and key to

ISSN 2394-7187(Online)
ISSN 2394 - 7179 (Print)

collaboration in the cloud – creates serious concerns regarding data loss or leakage. In fact, 69% of organizations point to this as their greatest cloud security concern. Data sharing using public links or setting a cloud-based repository to public makes it accessible to anyone with knowledge of the link, and tools exist specifically for searching the Internet for these unsecured cloud deployments.

1.21 Data Privacy/Confidentiality

Data privacy and confidentiality is a major concern for many organizations. Data protection regulations like the EU's General Data Protection Regulation (GDPR), the Health Insurance Portability and Accessibility Act (HIPAA), the Payment Card Industry Data Security Standard (PCI DSS) and many more mandate the protection of customer data and impose strict penalties for security failures. Additionally, organizations have a large amount of internal data that is essential to maintaining competitive advantage.

Placing this data on the cloud has its advantages but also has created major security concerns for 66% of organizations. Many organizations have adopted cloud computing but lack the knowledge to ensure that they and their employees are using it securely. As a result, sensitive data is at risk of exposure – as demonstrated by a massive number of cloud data breaches.

1.22 Accidental Exposure of Credentials

Phishers commonly use cloud applications and environments as a pretext in their phishing attacks. With the growing use of cloud-based email (G-Suite, Microsoft 365, etc.) and document sharing services (Google Drive, Drop box, One Drive), employees have become accustomed to receiving emails with links that might ask them to confirm their account credentials before gaining access to a particular document or website.

This makes it easy for cybercriminals to learn an employee's credentials for cloud services. As a result, accidental exposure of cloud credentials is a major concern for 44% of organizations since it potentially compromises the privacy and security of their cloud-based data and other resources.

1.23 Incident Response

Many organizations have strategies in place for responding to internal cyber security incidents. Since the organization owns their entire internal network infrastructure and security personnel are on-site, it is possible to lock down the incident. Additionally, this ownership of their infrastructure means that the company likely has the visibility necessary to identify the scope of the incident and perform the appropriate remediation actions.

With cloud-based infrastructure, a company only has partial visibility and ownership of their infrastructure, making traditional processes and security tools ineffective. As a result, 44% of companies are concerned about their ability to perform incident response effectively in the cloud.

1.24 Legal and Regulatory Compliance

Data protection regulations like PCI DSS and HIPAA require organizations to demonstrate that they limit access to the protected information (credit card data, healthcare patient records, etc.). This could require creating a physically or logically isolated part of the organization's network that is only accessible to employees with a legitimate need to access this data.

When moving data protected by these and similar regulations to the cloud, achieving and demonstrating regulatory compliance can be more difficult. With a cloud deployment, organizations only have visibility and control into some of the layers of their infrastructure. As a result, legal and regulatory compliance is considered a major cloud security issue by 42% of organizations and requires specialized cloud compliance solutions.

1.25 Data Sovereignty/Residence/Control

Most cloud providers have a number of geographically distributed data centres. This helps to improve the accessibility and performance of cloud-based resources and makes it easier for CSPs to ensure that they are capable of maintaining service level agreements in the face of business-disrupting events such as natural disasters, power outages, etc.

Organizations storing their data in the cloud often have no idea where their data is actually stored within a CSP's array of data centres. This creates major concerns around data sovereignty, residence, and control for 37% of organizations. With data protection regulations such as the GDPR limiting where EU citizens data can be sent, the use of a cloud platform with data centres outside of the approved areas could place an organization in a state of regulatory non-compliance. Additionally, different jurisdictions have different laws regarding access to data for law enforcement and national security, which can impact the data privacy and security of an organization's customers.

From a cyber-risk perspective and over the next 12 months, Indian organisations are most concerned around cloud-related threats (52%), attacks on connected devices (45%), hack-and-leak operations (36%) and software supply-chain compromise (35%).

DOI: 10.30726/esij/v11.i1.2024.111002

Almost half of respondents felt that the outcome of a cyber-attack could result in loss of customer data and revenue, followed by more than a third of them highlighting operations downtime to be a key outcome of a cyber-attack. Cyber budgets continue to rise. 99% of the respondents stated an increase in cyber budgets, out of which 50% of them envisaged an increase between 6% and 15% in the next 12 months.

1.26 Protecting the Cloud

The cloud provides a number of advantages to organizations; however, it also comes with its own security threats and concerns. Cloud-based infrastructure is very different from an on-premises data center, and traditional security tools and strategies are not always able to secure it effectively. For more information about leading cloud security issues and threats, download the Cloud Security Report.

2. Conclusion

Cloud computing will affect large part of computer industry including Software companies, Internet service providers. Cloud computing makes it very easy for companies to provide their products to end-user without worrying about hardware configurations and other requirements of servers. Cloud computing is used to provide pools and automated resources that can be accessed on-demand. Cloud computing setup is tedious, complicated. Cloud computing is highly scalable. Cloud computing requires many dedicated hardware. Cloud computing provides unlimited storage space. Large companies that have high download speed and high security as their main requirement finds virtualization as the best option The landscape of cyber-attacks is evolving every year, and there have been multiple critical attacks in the past few years. In 2024, businesses will come across many new cyber-attacks, and that is we present some cyber security trends that will help you stay ahead of emerging attacks.

References

[1] https://www.geeksforgeeks.org/security-issues-in-cloud-computing/
[2] https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/top-cloud-security-issues-threats-and-concerns/
[3] Cloud Computing: Concepts, Technology, and Architecture by Thomas Erl
[4] Cloud Computing- A hands on approachby Arshdeep Bahga & Vijay Madisetti
[5] https://computingforgeeks.com/top-open-source-cloud-platforms-and-solutions/
[6] https://www.educba.com/cloud-computing-service-providers/
[7] https://www.ubuntupit.com/best-cloud-os-the-experts-recommendation/
[8] https://www.outsource2india.com/software/azure-application-development-services.asp
[9] https://www.clouddefense.ai/cloud-security-trends/