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

Cloud Computing Security Issues and Solutions

[1]SOURISH PAUL, [2]RAKSHITHA KIRAN
[1]PG SCHOLAR, [2]ASSISTANT PROFESSOR
DEPARTMENT OF MCA
DAYANANDA SAGAR COLLEGE OF ENGINEERING
AFFILIATED TO VTU, BENGALURU, INDIA

Abstract

Cloud computing is a recently developed computing model which comes from distributed computing, grid computing, virtualization technology, and many more computer technologies. Cloud computing is a technique to increase the capacity and add ability dynamically without spending on new infrastructure or licensing new software. The security issues of cloud computing and the techniques to overcome the issue have been discussed in this paper. The security issue of cloud computing is a significant problem and it can hamper the fast development of cloud computing. The basic security problem in cloud computing is service availability and data privacy. A single security technique cannot resolve the security problem of cloud computing, various traditional new strategies and technologies need to utilize together to protect the total cloud computing system.

I. Introduction

For both individuals and businesses, the "cloud" has become an essential aspect of daily life. Businesses, non-profits, and other organizations all use cloud computing services regularly to save time, money, and trouble administering an "on-premises" computer solution.

While the cloud has aided many businesses in gaining access to vital software tools, computing platforms, and services, it has also posed new cybersecurity risks.

II. What is Cloud Background?

The cloud symbol, which is frequently used to symbolize the Internet in flowcharts and diagrams, inspired the phrase cloud computing. Anything that includes offering hosted services via the Internet is referred to as cloud computing.

Services of Cloud Computing

- **Cloud Computing with SaaS** - A web-based interface is used to provide programs from a third party. The end-user only interacts with the specific application offered by the third party; all else is handled by the cloud service provider (CSP).
- **Cloud Computing using PaaS** - PaaS services provide end-users additional power and responsibility by offering a predefined operating environment in which they may design, test, and execute their apps. To put it another way, they provide a platform for users to build and execute cloud-based apps.
- **Cloud computing with IaaS** - This is the cloud computing service that gives the user the most freedom (and accountability). Users must control most elements of the computing environment, such as operating systems and security because the CSP is essentially delivering a distant data center with little setup. This is the closest experience cloud computing can deliver to administering an on-premises data center—albeit with the option to

adjust resource allocation up or down based on the user's needs each month.

III. Cloud Security and its importance

Cloud security could be a comprehensive term for the security controls, practices, and technologies that are used to safeguard the environment of cloud computing. These controls are classified into 3 categories:

- **Preventative Controls:** Cloud security controls obtain to reduce vulnerability along with close potential security gaps within the cloud infrastructure, which can contain things like firewalls, safe application use policies, and encryption solutions.

- **Controls for detection -** These measures identify ongoing or recently completed assaults, allowing automatic or manual cleanup to commence. Examples of detection controls include security information and event management (SIEM) systems (which are typically offered via SaaS models), anti-virus/anti-malware scanning tools, and even managed network security monitoring.

- **Corrective problems -** These settings are intended to repair the damage or bad consequences of an assault after it has occurred. Corrective controls might include remote data backups (to recover corrupted or destroyed files), virus/malware eradication tools, and managed security incident response services.

Cloud computing security is a group of safety features designed to shield cloud-primarily based infrastructure, applications, and information. These measures make sure the authentication of customers and devices, get right of entry to manage information and resources, and the safety of information privacy. Many users, however, underestimate the significance of cloud computing security. This is massive because of the truth they assume the CSP is accountable for cloud cybersecurity. Unfortunately, that isn't always the case. The majority of the time, the person of a cloud computing device is liable for any statistics breaches that occur. Because, even with the best security controls in place for preventing, detecting, and remediating breaches, if the end-user refuses to configure their cloud security strategy (or, worse, actively circumvents the CSP's security tools), the CSP is powerless to prevent a breach. While some cloud services make it much more difficult for end-users to adopt robust cloud security than others, it is always a concern.

IV. Challenges In Cloud Security

1. **Potential Intellectual Property Loss or Theft Regulatory -** Many businesses are concerned about intellectual property theft. According to WIPO figures, over 3.3 million patent applications were lodged in 2018. Because these IPs represent competitive advantages for the companies that own them, their loss or theft can have a substantial impact on market share as copycats reproduce goods and processes for less money because they don't have to cover development expenses.
2. **Compliance Violations -** Many firms must adhere to stringent compliance rules in their sector. However, a cloud computing service may not always fulfill an organization's stringent regulatory compliance criteria. If the cloud computing security concerns connected to the compliance requirement are not addressed, this might result in compliance violations.
3. **Cloud Environment Visibility is Reduced -** One of the most significant difficulties that

businesses have when using a cloud computing solution is that certain CSPs do not give insight into the cloud environment. This is most commonly an issue with SaaS systems—PaaS and IaaS solutions give more visibility because the customer is expected to handle their cloud configuration and administration.

4. **Cloud Environment Settings Have Less Control** - Along with less visibility, many cloud computing service customers report having less control over their computer settings when working in the cloud. This is particularly frequent with SaaS-type cloud solutions that provide a fixed application. IaaS and PaaS solutions often give far greater control.
5. **Spread of Lateral Attack** - If a cloud computing infrastructure lacks effective defense-in-depth measures, an attacker can easily spread from one job on the cloud to the next. This can result in several databases or cloud apps being compromised fast during a hack.
6. **Security has become more complex** - Companies that interact with numerous cloud service providers frequently complain about having to deal with various complex cloud security protocols. Some SaaS applications, for example, may demand multi-factor authentication through SMS text messages, whilst others may use various authentication techniques. This adds process complexity and makes it more difficult for end-users to employ various cloud solutions in their daily processes.
7. **Following a Breach, Notifying Affected Parties** - Another effect of less visibility into a cloud computing system is that identifying the parties impacted by a breach becomes more difficult. It's difficult to identify whose data was exposed without specific details of which databases and apps were impacted. This considerably complicates satisfying data breach notification obligations.

V. Overcoming Common Cloud Security Challenges and Issues

So, how can you solve some of the above-mentioned cloud computing security issues? While there is always some risk in any IT environment, there are steps that can be taken to reduce, if not eliminate, many of the issues listed above.

1. **Limit the number of cloud computing vendors you use** - One of the most difficult aspects of dealing with cloud-based solutions is that they can all have different security tools and processes, making them more difficult to manage. Finding ways to limit your selection of CSP vendors can be extremely helpful in this scenario. Consider sourcing as many cloud solutions as possible from a single vendor. However, this is often easier said than done.
2. **Check Your Access to Cloud Environment Information** - Because visibility is critical in cybersecurity, it is critical to confirm what information about the cloud environment you will have access to—preferably before signing an agreement. You can track and handle security more simply if you have better insight into the cloud environment.

3. **Verify Security SLAs** - Another item to look at before signing a contract with a cloud service provider is their security service level agreements. How fast will they address a security vulnerability once it is discovered? How long will it take to get everything back to normal? Who is in charge of informing impacted parties?

- Before signing an agreement, verifying these SLAs can assist guarantee that they.
- Meet your industry's cybersecurity criteria
- Will protect your business from untenably long service disruptions;
- Establish who is responsible for what follows a data breach.

4. **Consult a Cybersecurity Professional**- Consult a cybersecurity professional if you are ever concerned about whether a cloud solution has the necessary security protections to secure your organization's data, workers, and clients. Expert assistance can help you make a more educated decision that will help you secure your company more effectively in the long run.
5. **Examine Specific Security Measures** - How will the CSP stop attackers from entering your cloud environment? How will they stop attacks from propagating from one node on their network to another? It is critical to investigate the security measures provided by a cloud service provider to establish:

- How well-prepared they are to safeguard your data.
- their capacity to satisfy regulatory standards.
- and how simple or difficult it will be to integrate the solution into your current cybersecurity infrastructure.

It should be noted that not all cloud solutions have built-in security for the cloud computing environment. PaaS and IaaS solutions, in particular, will almost certainly leave it up to their customers to install the required security systems to protect the cloud environment.

VI. Conclusion

This paper summarizes, cloud security and its challenges. In recent times cloud computing is a new technological development which has the capacity to own an excellent impact on the globe. It has several advantages that it provides to users and businesses. The paper gives an insight of the common security measures undertaken to overcome security threats. Overall, the paper shows how important it is for the user to opt for a proper loud security provider.

Reference

[1] Top Threats to cloud computing, Cloud Security Alliance. March 2010(online).

[2] 'Cloud Computing: Virtual Cloud security Concerns', Winkler, Microsoft. 12 February 2012(online).

[3] 'Dark Cloud: Study finds security risks in virtualization', Hickey, Kathleen.

[4] "Securing the cloud: Cloud computer security techniques and tactics", Winkler, Joachim R (2011).

[5] https://en.wikipedia.org/wiki/Cloud_computing_security

[6] S. Lohr, Google, and I.B.M. join in "Cloud computing research", October(2007).