

STUDY OF CLOUD COMPUTING SECURITY MEASURES AND RISKS.

Rakesh L. Patil, Asst. Professor, Tilak Maharashtra Vidyapeeth, Pune
SudhirSoman, Asst. Professor, Tilak Maharashtra Vidyapeeth, Pune

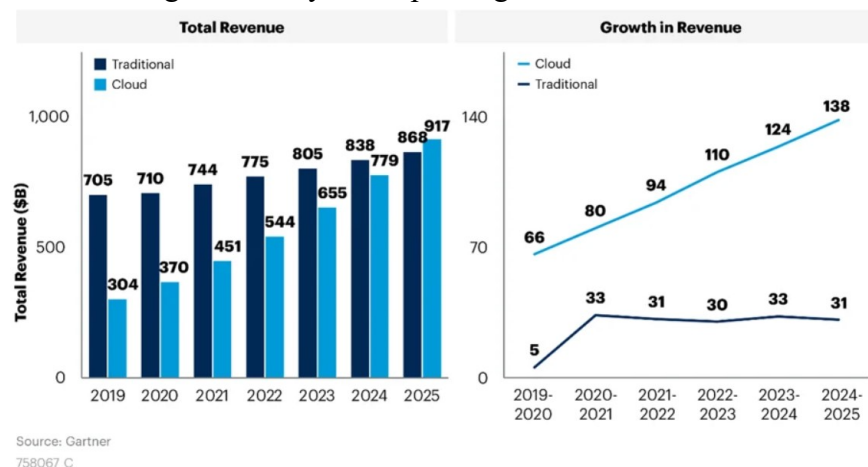
ABSTRACT:

The work environment of today can be anywhere. Enterprise mobile security solutions that facilitate the flexible delivery of apps, content, and resources across devices and guarantee a strong cybersecurity posture are essential for a secure mobile workforce, as stated by CIOs, CISOs, and their teams. In order to safeguard against sophisticated threats like ransomware and phishing and to effectively address any vulnerabilities, these leaders require strategic options for mobile security threats and prevention, regardless of whether they are supporting bring your own device (BYOD), choose your own device (CYOD), or a corporate-liable environment. These alternatives include containerisation of mission-critical resources, security policies, behavioural analysis, and risk insights. In this paper we are going to understand and learn about how Microsoft azure is providing cloud security to its customers, Azure AI shared responsibility model.

Keywords: Cloud Computing, Cloud Security, AI Responsibility model.

INTRODUCTION:

Cloud computing is the pay-per-use online access to a variety of computing resources, including software, hardware (real or virtual servers), data storage, networking, application development tools, and AI-powered analytic tools. Customers can enjoy more scalability and flexibility with this strategy than with traditional on-premises infrastructure. Cloud computing abilities are currently in high demand due to the current increase in the need for cloud computing services. Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) [1] are the three primary service model types that it offers. Because cloud services are now being used by businesses of all sizes, from small to large, they choose between several cloud types such as public, private, hybrid, and community clouds based on their needs. Cloud computing has become a game-changer in the ever-evolving world of technology, revolutionising how companies run and maintain their IT infrastructure. A recent analysis from Gartner® indicates that the move to cloud computing is gathering unparalleled speed, with projections indicating that by 2025, over half of commercial IT investment in important market categories will move to the cloud. Technology and service providers face both possibilities and problems as they adjust to the shifting market dynamics brought about by this rapid migration to the cloud.



<https://www.gartner.com/en/newsroom/press-releases/2022-02-09-gartner-says-more-than-half-of-enterprise-it-spending>

UNDERSTANDING THE SECURITY CHALLENGES:

Many businesses that use the cloud to store data and execute apps are quite concerned about cloud security. Numerous public cloud services are multi-tenant settings, which raises the risk of a breach since data from several clients is housed on a single server. Because so many businesses keep sensitive data on the cloud, cybercriminals are more motivated to try to get past cloud service providers' security measures in order to obtain or pilfer important data. [2] In order to fortify cloud computing security, cloud service providers implement a range of procedures, rules, and technologies to prevent data theft, loss, or disruptions due to cyberattacks. These may consist of security compliance and monitoring, user identification and access management systems, and data encryption. The shared responsibility paradigm is among the main security issues with cloud computing. In a cloud context, the customer and the cloud service provider (CSP) share responsibility for security. [3] The customer is in charge of protecting their data, apps, and user access, while the CSP is in charge of protecting the underlying infrastructure, which includes the actual data centres and network infrastructure. If not fully understood, this shared responsibility paradigm may cause confusion and security weaknesses. To safeguard their data from illegal access or breaches, customers must make sure the proper security measures are in place. These measures include robust authentication procedures, data encryption, and access controls. The dynamic nature of cloud infrastructures presents another difficulty. Because cloud resources can be supplied or de-provisioned on demand and are very scalable, it can be difficult to keep visibility and control over the entire infrastructure. Due to its dynamic nature, there is also a chance of configuration errors or other weaknesses that might be used by bad actors. Furthermore, the danger of data leakage or unauthorised access is introduced by the multi-tenancy characteristic of cloud computing. The data and workloads of numerous customers are housed on the same physical infrastructure in a shared environment, which raises the possibility of insider threats and expands the attack surface.

PRINCIPAL DIFFICULTIES WITH CLOUD SECURITY:

With a little reworking, enterprises frequently "lift and shift" their on-premise workloads and infrastructures to the cloud. Still, it is not feasible to move to the cloud with the legacy security paradigm and technologies alone. This is a result of the need to develop new security strategies and reconsider all security procedures in the context of the cloud.

- **The rate of change**
The cloud environment is dynamic and rapidly evolving. It happens as a result of on-demand resources and optimized provisioning procedures. Traditional security tools frequently cannot handle this "chaos" because of how much the current security management and security controls are weakened by this rate of change.
- **The fleeting nature of cloud networks**
Modern virtual instances actually spin up just as fast as they can be destroyed. Organizations have lost their ability to clearly define the boundaries of their workloads, networks, and responsibilities as a result of the use of cloud environments. Consequently, since the perimeter has vanished, the conventional perimeter-based security solutions are no longer functional.
- **The complexity of the cloud**
The security and compliance issues posed by even a basic cloud-based operation are considerable. not to mention the hybrid or multi-cloud deployments that add even more

complexity to the cloud. When there are several cloud entities, event logs, configuration files, and networks present, utilizing older data security solutions to analyze security incidents might be difficult or even impossible.

SHARED RESPONSIBILITY MODEL: KEY CHALLENGES TO CLOUD SECURITY :

Businesses aggressively embrace new digital technology in order to reconsider their processes in response to contemporary needs. Cloud-based workload and infrastructure migration from on-premises systems is one of the most popular digital transformations. The constant need for easily deployable and quickly scaled computation and network resources is met by cloud services. They do, however, also provide a new set of security concerns for cloud computing and call into question established security methodologies.

According to NIST, cloud computing is a methodology that allows for easy, on-demand, and widespread network access to a shared pool of quickly provided and released programmable computer resources with no involvement from service providers or management. The following qualities are involved in cloud computing:

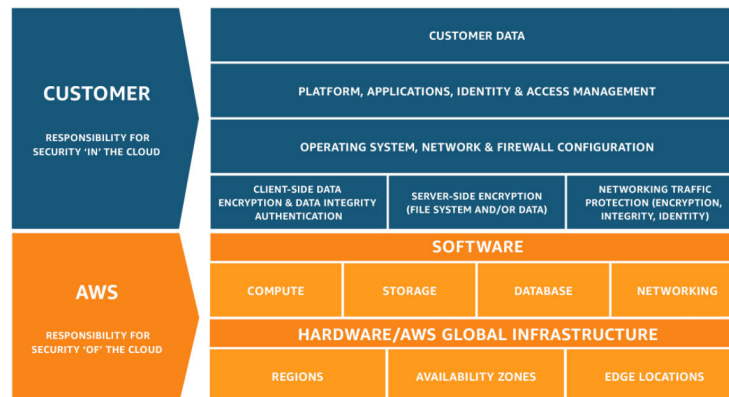
- On-demand self-service – Users are able to supply their own cloud's computing services and capabilities. [4]
- Broad network access – Any device, including mobile ones, can access any cloud service. [4]
- Resource pooling – Multiple users can be served by providers thanks to the multi-tenant concept.
- Rapid elasticity – Resources are available for consumers to access, shrink, or expand in proportion to their usage or release.
- Measured service – Service fees are determined by the needs of the user.

WHAT IS THE SHARED RESPONSIBILITY MODEL? :

The shared responsibility model is a framework that delineates the respective responsibilities of the cloud service provider (CSP) and the client with regard to safeguarding various components of the cloud computing environment. Security of the underlying infrastructure is often the responsibility of the CSP, while customers are responsible for protecting their data and apps housed in the cloud. All networking equipment and data centers must be kept secure by CSPs. They also take care of maintaining the dependability and availability of the cloud services in addition to patching and updating operating systems. This is referred to as the "cloud security" obligation. Customers are responsible for maintaining user accounts and credentials, encrypting data while it's in transit and at rest, configuring safe access restrictions, and putting application-specific security measures in place. This task is referred to as "security in the cloud". Few people are aware of these obligations. Just 13% of companies are aware of their cloud security duties, despite the fact that 98% of them report having had a cloud data breach in the previous 18 months. Erroneously, a lot of businesses depend on their CSPs for application security and data protection. Getting this knowledge gap closed is crucial to meeting your cloud security responsibilities. [5]

The shared responsibility paradigm includes controls like administration, operation, and verification in addition to IT infrastructures. Companies can take over some operating controls from their cloud providers, assume complete responsibility for others, and inherit operating controls from them. These are a few instances of shared accountability for controls. Physical and environmental controls that an organization inherits from its cloud provider are known as inherited controls. Shared Controls: Part of the control is shared by the customer and the cloud provider. Shared controls could be things like patch

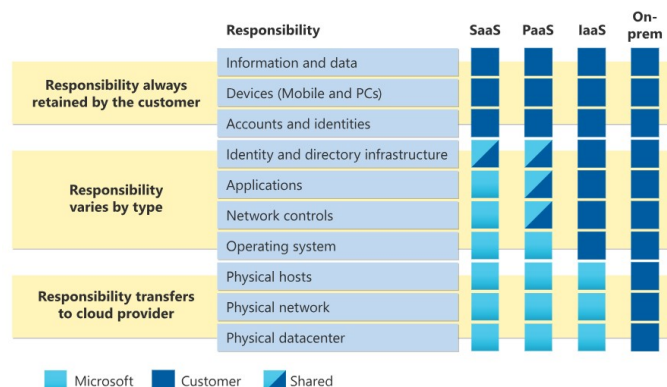
management, configuration management, and awareness and training programs. Controls that are "customer specific" mean that customers are solely responsible for their implementation and management. Organizations are in charge of controlling access and safeguarding communications with outside parties, for example.



(Source: <https://aws.amazon.com/compliance/shared-responsibility-model/>)

BOUNDARIES OF RESPONSIBILITY: SAAS, IAAS, AND PAAS :

The limits of responsibility serve as the foundation for the second popular method of applying the shared responsibility paradigm. Specifically, accountability varies based on the cloud deployment level and includes software as a service (SaaS), infrastructure as a service (IaaS), and platform as a service (PaaS). IBM Cloud, Google Cloud, and Microsoft Azure all frequently employ this strategy: Within an Infrastructure-as-a-Service (IaaS) paradigm, the provider is in charge of the physical layers and the client and provider jointly manage the host infrastructure and network security. The customer bears all liability for the remainder. While the provider in a PaaS architecture maintains complete control over host infrastructure and network security, it also shares accountability with the client for application and access control. Within Software as a Service (SaaS) framework, the provider assumes complete accountability for application controls, while the customer and the provider share responsibility for client/endpoint protection and access control. The sharing of responsibility boundaries is illustrated graphically in Figure 2:



(Source: <https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility>)

Vulnerabilities in the cloud shared responsibility model:

Vulnerabilities in the cloud shared responsibility model typically stem from misunderstandings or gaps in accountability between cloud service providers (CSPs) and cloud customers. Here are a few key vulnerabilities:

1. Misconfigurations: Both CSPs and customers have responsibilities for configuring security settings. Misconfigurations, such as leaving storage buckets or databases publicly accessible, can lead to data breaches.

2. Lack of visibility: Customers might assume that CSPs handle all security aspects, leading to a lack of visibility into their own responsibilities. This can result in oversight of critical security measures on the customer's end.

3. Data breaches: Due to the shared responsibility model, data breaches can occur if either the CSP or the customer fails to adequately secure their portion of the infrastructure. Attackers may exploit vulnerabilities in one party's security measures to gain access to sensitive data.

4. Compliance issues: Compliance requirements vary depending on the industry and region. Failure to understand and fulfill compliance obligations on both sides can result in regulatory fines and legal consequences.

5. Limited control: Customers may have limited control over security measures implemented by the CSP, leading to concerns about data protection and compliance with internal policies.

The accidental exposure of 38TB of data by Microsoft AI researchers is a significant incident. It highlights the importance of robust data security measures, especially when handling large volumes of sensitive information. This breach underscores the need for continuous vigilance and stringent protocols to safeguard data privacy and prevent unauthorized access. Microsoft must take immediate steps to address this breach, mitigate any potential harm, and reinforce their data protection measures to prevent similar incidents in the future. [6]

CONCLUSION:

In cloud computing, the shared responsibility approach has various benefits. It assists in resolving security issues by outlining the obligations of the service provider and the user in precise terms. This approach guarantees the implementation of data protection protocols, including access control policies established by developers to thwart illegal access. It also improves data accountability by enabling consumers to keep an eye on how much data they utilize and fostering confidence in cloud service providers. The shared responsibility model also promotes moral behavior by providing avenues for ethical activity, conforming to social norms, and providing workable solutions to enhance moral behavior. Furthermore, by defining dependence connections for better implementation and building a trustworthy chain of trust, it helps create accountable cloud services. In general, the cloud computing industry's shared responsibility paradigm encourages security, responsibility, and moral conduct online. To mitigate vulnerabilities, it's crucial for both CSPs and customers to clearly understand their respective responsibilities and implement robust security measures. This includes regular security assessments, ongoing monitoring, employee training, and collaboration between the CSP and the customer to address any security gaps. Additionally, leveraging tools for cloud security management and automation can help streamline security processes and improve overall resilience.

REFERENCES:

- 1) Janet Julia Ang'udi. (2023), Security challenges in cloud computing: A comprehensive analysis. World Journal of Advanced Engineering Technology and Sciences, 2023, 10(02), 155–181
- 2) Shakeel Juman TP Shakeel Juman TP, (2020), Advantages and Security Challenges of Cloud Computing– Overview, International Journal of Computer Science and Mobile Computing, Vol.9 Issue.12, December- 2020, pg. 76-85
- 3) PanJun Sun, Security and privacy protection in cloud computing: Discussions and challenges, Journal of Network and Computer Applications, Volume 160, 2020, 102642, ISSN 1084-8045, <https://doi.org/10.1016/j.jnca.2020.102642>.
(<https://www.sciencedirect.com/science/article/pii/S1084804520301168>)
- 4) Alghofaili, Y.; Albattah, A.; Alrajeh, N.; Rassam, M.A.; Al-rimy, B.A.S. Secure Cloud Infrastructure: A Survey on Issues, Current Solutions, and Open Challenges. Appl. Sci. 2021, 11, 9005. <https://doi.org/10.3390/app11199005>
- 5) <https://www.esg-global.com/hubfs/ESG-Infographic-DP-Cloud-Strategies.pdf>
- 6) <https://www.techtarget.com/searchsecurity/news/366552399/Microsoft-AI-researchers-mistakenly-expose-38-TB-of-data>