**Educational Administration: Theory and Practice**
2019, 25(4), 782-789
ISSN: 2148-2403
https://kuey.net/

**Research Article**

# Securing The Perimeter Shared Responsibility Models In Cloud Vs. On-Premises Environments

Rajashekar Reddy Yasani[1*] ,Karthik Venkatesh Ratnam[2]

[1*]Senior Security Engineer Independent Security Researcher Boston, MA Cloud Security, Cloud Computing, Cyber Security rajshekaryasani@gmail.com
[2]Cloud Engineer, Devsecops ( cloud security) Independent Security Researcher Dallas,TX karthikratnam1@gmail.com

***Citation:*** Rajashekar Reddy Yasani, et al (2019), Securing The Perimeter Shared Responsibility Models In Cloud Vs. On-Premises Environments , *Educational Administration: Theory and Practice*, 25(4), 782-789
Doi: 10.53555/kuey.v25i4.7975

**ARTICLE INFO**

**ABSTRACT**

A complex infrastructure of many interconnected devices is what makes cloud computing possible and allows it to deliver the services that customers require. The building blocks of cloud computing are several kinds of adaptable distributed systems that can be linked in various ways and utilised for various tasks. Businesses are rushing to switch to cloud networks because of all the advantages, including low costs, scalability, reliability, and flexibility. Cloud networks are vulnerable to many network attacks and privacy problems, despite the fact that cloud computing's primary benefits are encouraging facts. The features of cloud computing, such as multi-tenancy and third-party managed infrastructure, necessitate an identity and access management system. The problem of ensuring secure access to cloud resources has been taken up by numerous experts in both academia and industry. Authentication, access control, security, and cloud services are all covered thoroughly in this essay, along with their respective issues and solutions. Focussing on cloud services, security concerns, and identity and access management, this study compares and contrasts current approaches from the viewpoints of cloud service providers and cloud consumers.

**Keywords:** Cloud networks, Authentication, On-Premises Environments.

## 1. INTRODUCTION

Networks, servers, storages, services, and applications are all parts of the cloud, which allows users to access these resources easily and whenever they need them [1]. People talk a lot about cloud computing, and it's already used in a lot of businesses. Cloud service providers (CSPs) are liable for managing identities and other cloud-related elements. However, many instances of data leakage have their origins in weaknesses in identity management systems [2]. Security for cloud services relies heavily on IAM, or identity and access management. Users seeking a more flexible and granular method of access control will find that the present identity management system, with its primary emphasis on CSPs, falls short of their expectations.
Cloud computing can take place in three primary forms: private, public, and hybrid/federated. Customised to fit the specific needs of a firm, a private cloud is ideal for large-scale businesses. The infrastructure support for different organisations is facilitated and managed by a third party in a public cloud environment. Several businesses can cut costs on service by sharing the same resources in a public cloud, often known as a multi-tenant environment. Hybrid or federated cloud architectures combine public, private, and on-premises cloud resources. Cloud computing also includes the concept of multi-provider clouds, which are configurations that share the workload among multiple cloud providers. Cloud computing enables mobile cloud services to disseminate applications to mobile devices, while IoT cloud services are customised to handle and analyse data derived from IoT devices. To back up these services, there are other cloud environments to choose from as well. Three primary models of cloud computing are infrastructure as a service (IaaS), software as a service (SaaS), and platform as a service (PaaS). Because of the service-oriented architecture, database-as-a-service (DbaaS), identity-as-a-service (IDaaS), and anything-as-a-service (XaaS) are all possible cloud services [3]. Business and academic resource management have both been enhanced by cloud computing. A cloud system's dynamic nature is shown by the vast number of users, devices, networks, organisations, and resources that are periodically connected to and disconnected from it.

Several criteria are considered in order to ascertain the optimal choice for the mandatory implementation of the cloud service model. Considerations like as scalability, interoperability, control of service, and flexibility are crucial [4]. In order to keep data and resources safe in the cloud, which can be somewhat complicated to use, a robust authentication and authorisation method is required. Management of identities, risks, trust, compliance, data security, privacy, transparency, and data leakage are just a few of the many problems that can develop in a cloud setting when a good technique is not in place [5]. Another factor to think about is the security risks and complexity of cloud systems. Cloud service providers (CSPs) and other entities outside of an organization's control store and handle user data, which creates challenges with transparency and control. These specific security concerns are slowing the adoption of cloud systems, despite the cloud's assured and attractive advantages. Despite these issues, the company is still hesitant to upload their sensitive identity data to the cloud [6].

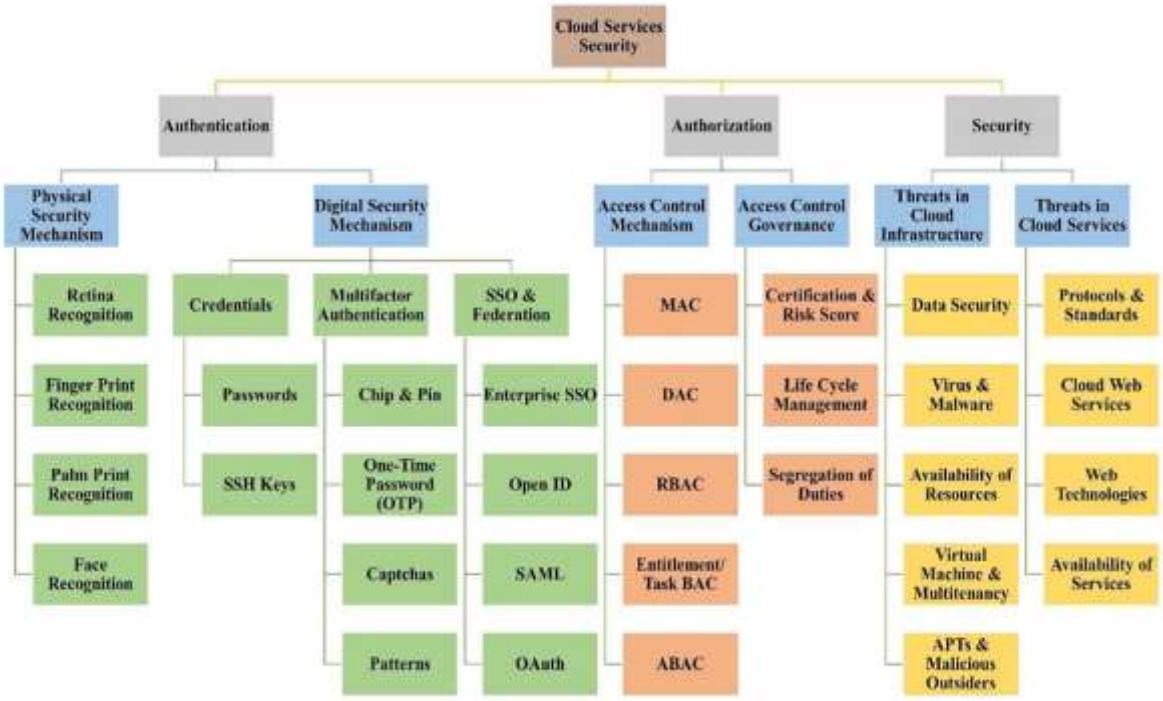


**Fig. 1**. Cloud service security taxonomy.

In a cloud computing model, organisations or external providers handle data storage and processing. The supplier of the service is liable for ensuring the safety of the cloud infrastructure and any information or programs stored therein. Verify that the authentication credentials you use are secure [7]. Many security concerns raise red flags regarding the potential for third party providers, who may be malicious attackers in their own right, to store and access data on the cloud. Despite the availability of standards and best practices to address these security concerns, cloud service providers are reluctant to implement them on their networks [8].

Identity and access management is one of the best ways to measure cloud services. These days, no cloud security solution is complete without Identity and Access Management (IAM). Authentication, authorisation, storage provisioning, and verification are just a few of the many duties performed by Identity and Access Management (IAM) systems in relation to cloud security. Protecting users' identities and attributes is the job of identity and access management systems, which screen users to verify their authorisation to access the cloud. In addition to helping with the management of rights, IAM solutions ensure that only authorised users can access data stored in the cloud [9]. Many companies are increasingly using Identity and Access Management solutions to further secure their cloud-based sensitive data. In Fig. 1 we can see a classification system for the safety of cloud services.

## 2. LITERATURE REVIEW

The term “authentication” refers to the procedure whereby one entity verifies another. It checks if the applicant or the person seeking access are eligible. A piece of software or the whole piece of software is typically responsible for performing the authentication procedure [10]. Common authentication methods in a network setting include login credentials, third-party authentication, biometric authentication, graphical passwords, basic text passwords, 3D password objects, and digital device authentication. The aforementioned

authentication procedures can be used alone or in conjunction with one another by a cloud system [11]. At the moment, an identity management system is used to authorise permission to access the cloud.

Physical security measures, such as biometrics and access cards, prevent unauthorised individuals from gaining access to cloud resources and facilities. Businesses have recently taken an interest in cloud data centres (CDCs) because of the 24/7 accessibility they provide their clients. Because CDCs centralise all servers, networks, and applications, data can be accessible from anywhere at any time. To ensure the safety of data centres, access cards and biometric identification technologies including fingerprint, iris, retina, face, and palm print recognition can be employed. Protecting sensitive information from prying eyes requires stringent physical security measures for data centres, in addition to usage and governance rules.

Digital authentication devices and biometric access control systems are the current physical security measures in use [12]. The possession of proper credentials demonstrates one's rank, access privileges, and entitlements. It proves that the user has a right to or merits the use of the resource or service in question. Credentials like one-time passwords, patterns, and captchas are examples of traditional system security measures. Many cloud service providers offer authentication management solutions, the most common of which being Microsoft Active Directory (AD) and the Lightweight Directory Access Protocol (LDAP).

Third-party vendors or the company's own network administrators handle LDAP and AD server management in cloud computing [13]. When more than one application is installed on these older credential management systems, the maintenance burden on the cloud rises. Anyone who joins or leaves the company must have their account added, disabled, changed, or removed. Regarding provider-side credential management, a credential reset vulnerability exists due to weak password recovery techniques. In the event that credentials are compromised, malicious redirection, data monitoring, and manipulation in the cloud are all possible outcomes [14].

One way that the Secure Shell (SSH) protocol identifies the SSH server is through challenge-response authentication or public-key cryptography. One great thing about SSH keys is that they allow you to authenticate with the server without sending your password over the network. This makes it such that hackers can't decipher the password.

With SSH keys, brute force attacks that try to guess credentials during authentication are rendered useless. SSH agents allow users to connect to servers without having to remember several passwords. The private keys are stored by the SSH key agent, and they are provided to the SSH client programs. The encryption of these private keys requires a password, which must be entered each time you want to establish a connection to the server. To proceed to the authentication phase of each SSH call, you must know the password used to decrypt the private key. The passphrase is only required while the agent is adding private keys to its store.

This effort is tailored to assist devices that frequently establish SSH connections. The SSH agent starts running automatically as soon as the login is started and continues running during the session. The primary issue with SSH keys is that, without properly protecting the private keys, the security is no better than credentials. Cloud web service authentication often makes use of static credentials and SSH key techniques.

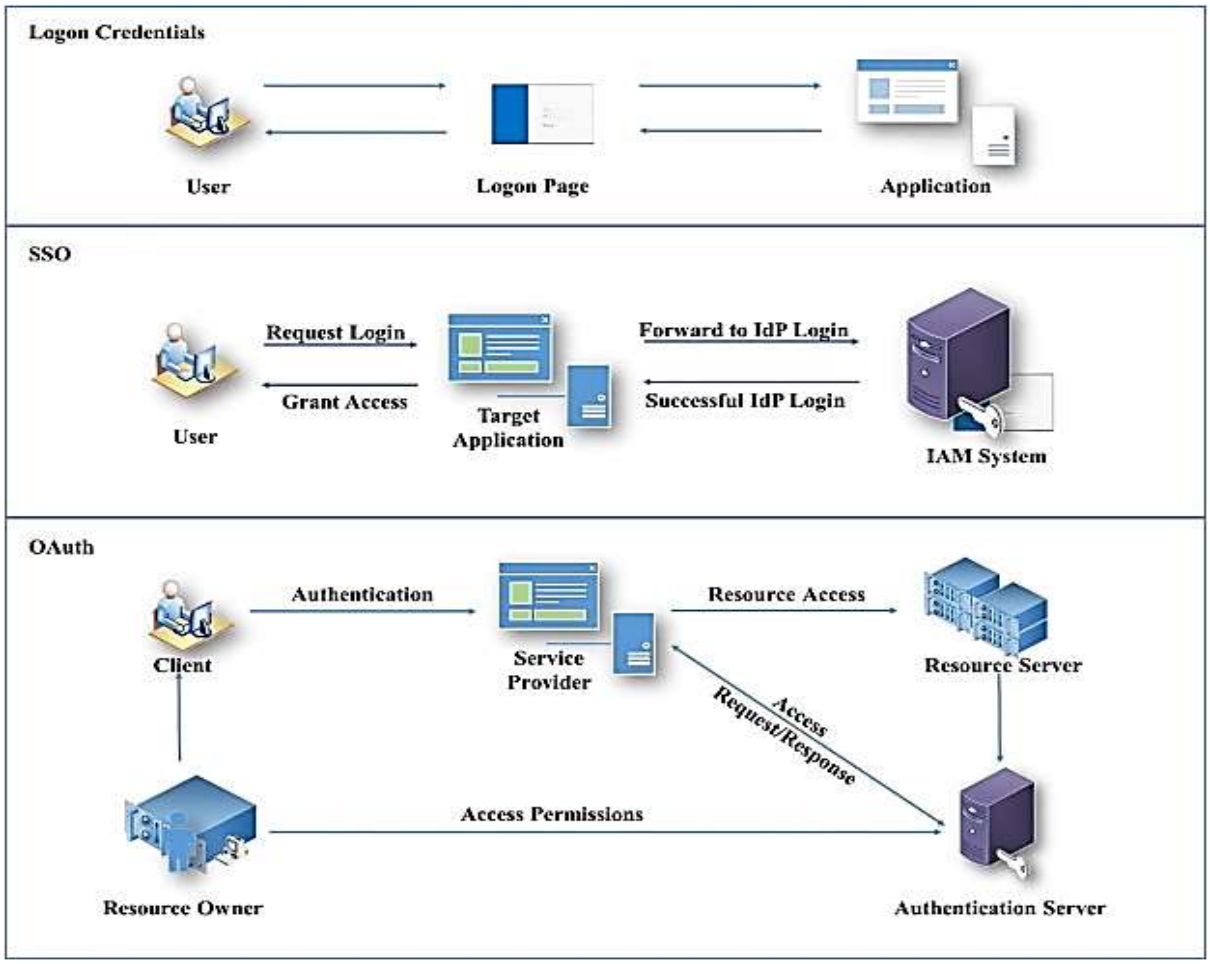


**Fig. 2.** Investigating various authentication methods in a cloud setting.

Traditional methods of authentication may not work when authenticating users remotely. One way to reduce software piracy is to implement centralised monitoring for authentication when visiting SaaS applications. Many login credentials are required since cloud consumers sometimes subscribe to multiple services [15]. Having a single user manage a huge number of credentials becomes a nightmare because of this. As a potential option, one may employ single sign-on procedures. With the help of single sign-on (SSO) provision, cloud users can access all of their applications and services with just one password. Maintaining a single credential for each user ensures uninterrupted and secure services. In order to access various web services hosted in the cloud, customers do not have to repeatedly enter their credentials [16]. With the help of SAML, OAuth, and OpenID, the Identity Provider (IdP) can share authentication and authorisation information with the Service Providers (SPs), allowing for Single Sign-On (SSO), as shown in Figure 2.

## 3. THE SHARED RESPONSIBILITY MODEL IN THE CLOUD

Gartner predicts that user mistake will account for the vast majority of cloud security incidents up to 2025. In particular, for cloud customers, this kind of number can be startling, frightening, or otherwise concerning. Cloud computing is challenging because it is an unstoppable force with exponentially complicated dynamics. Maybe we should reevaluate the rules for cloud configuration and figure out why customers might easily fail to adequately secure their cloud, rather than blaming them when things go wrong. The good news is that if customers are clear about what they are accountable for protecting in the cloud, a significant chunk of that 99% of failures can be avoided. The Shared Responsibility Model, then, comes into play.

What is the Shared Responsibility Model?

The shared responsibility model is followed by cloud service providers and specifies who is accountable for what in a cloud environment. This includes infrastructure, data, identities, workloads, networks, settings, and much more besides.

The CSP and the consumers each have a part to play. The model of shared responsibility is defined differently by each supplier. Prior to delving into the fundamentals of two leading cloud providers, it is important to grasp the historical backdrop of the shared responsibility model.

Why the Shared Responsibility Model is Important

There is a growing demand for cloud providers to guarantee secure environments as more and more organisations move their operations to the cloud. In the past, businesses were solely liable for the security of

their own datacenters, networks, and infrastructure. Now the burden has changed because we contract out the administration of a significant amount of gear. When you work with a service provider, you get a solid foundation upon which to build your company. The cloud provider's duty has grown significantly in the wake of landmark incidents like the notorious Azure CosmosDB managed database service vulnerability. From that point on, cloud service providers like Microsoft Azure, Amazon Web Services (AWS), and Google Cloud Platform (GCP) have gone to great lengths to guarantee their clients' environments are completely secure.
However, there is a limit to this promise, and a boundary was thus established. The emergence of the shared responsibility model occurred when cloud providers, with AWS as a prime example, released a transparent roadmap outlining the extent to which they will oversee and control their customers' environments. The group came to the opinion that cloud security is largely the provider's job, with a little bit of a customer shoulder.
Benefits and Challenges of the Shared Responsibility Model
Reducing operational strain on your organisation is the most apparent benefit. Cloud security is a joint effort between you and your CSP, but managing the underlying hardware and software is easier with them. In a perfect world, security would be at an all-time high if you and your CSP both knew and fulfilled your roles. On the other hand, the model is not without its potential difficulties. To begin, it's important to understand that different clouds have distinct duties because each CSP has their own unique model. This is especially true when working with multiple clouds at once. The second thing to keep in mind is that the services you're looking at, such IaaS and PaaS, have distinct responsibility management. Last but not least, there is potential for misunderstanding because certain things are subjective. It can be challenging to stay on top of your responsibilities and follow through adequately with all this variety and intricacy.

## 4. AWS SHARED RESPONSIBILITY MODEL

Since AWS does not have complete control over its customers' AWS usage, the company pays close attention to the security of its infrastructure. This includes safeguarding its computing, storage, networking, and database services from attacks. The safety of the programs, hardware, and buildings that house AWS services is entirely on AWS. Elastic MapReduce, WorkSpaces, AWS DynamoDB, RDS, Redshift, and other AWS managed services have their security configurations handled by AWS as well. It is ultimately the duty of AWS users to ensure the secure utilisation of unmanaged services, albeit this varies every AWS service. In particular, it is the responsibility of the customer to turn on multi-factor authentication, particularly for Identities with the most extensive IAM permissions in AWS, even though AWS has installed various safeguards to prevent unauthorised access to AWS, such as multi-factor authentication.The default security settings for AWS services are also among the most insecure. Therefore, as a low-hanging fruit to accomplish their half of the AWS shared responsibility model, companies should prioritise enhancing the default AWS security settings and specifically designing your cloud.

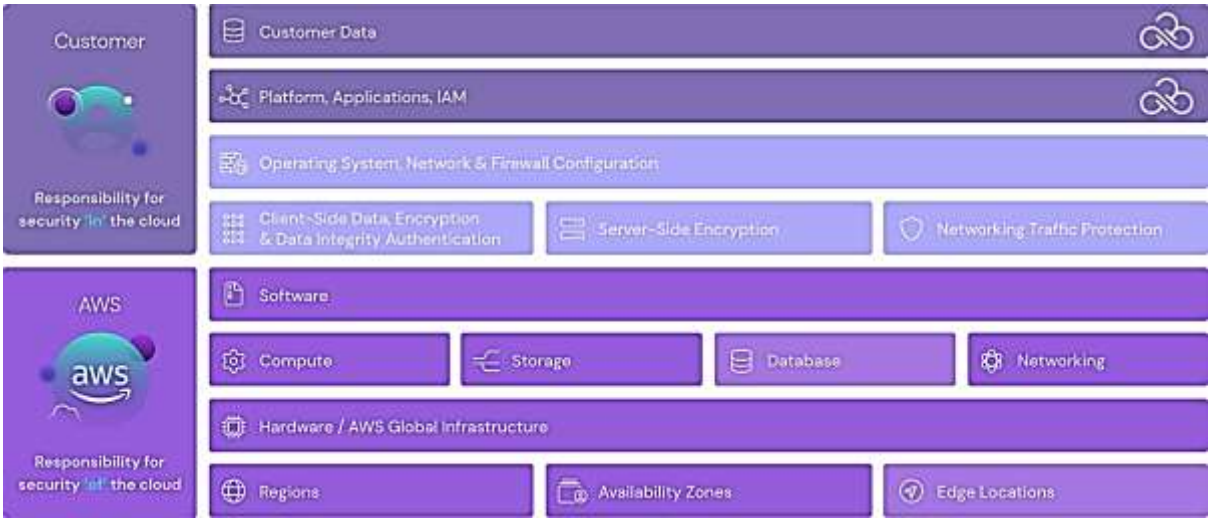


**Fig 3:** AWS Shared Responsibility Model

### Azure Shared Responsibility Model

By preventing unauthorised access to its compute, storage, networking, and database services, Azure prioritises the safety of its underlying infrastructure. The safety of the computers, networks, and other infrastructure components that house Azure services is another responsibility of Azure. Security is a top priority when configuring Azure managed services. This includes AKS, Container Instances, Cosmos DB, SQL, Data Lake Storage, Blob Storage, and many more.
Security for everything that an Azure customer creates, uses, or instantiates is the customer's responsibility in their own cloud. Whether Azure users are utilising SaaS, PaaS, or IaaS services determines this duty. With an on-premises data centre, the customer has full ownership of the stack, according to Microsoft. Some tasks are

handed off to Microsoft Azure when you migrate to the cloud. The following graphic shows the customer's and Microsoft's respective responsibilities:

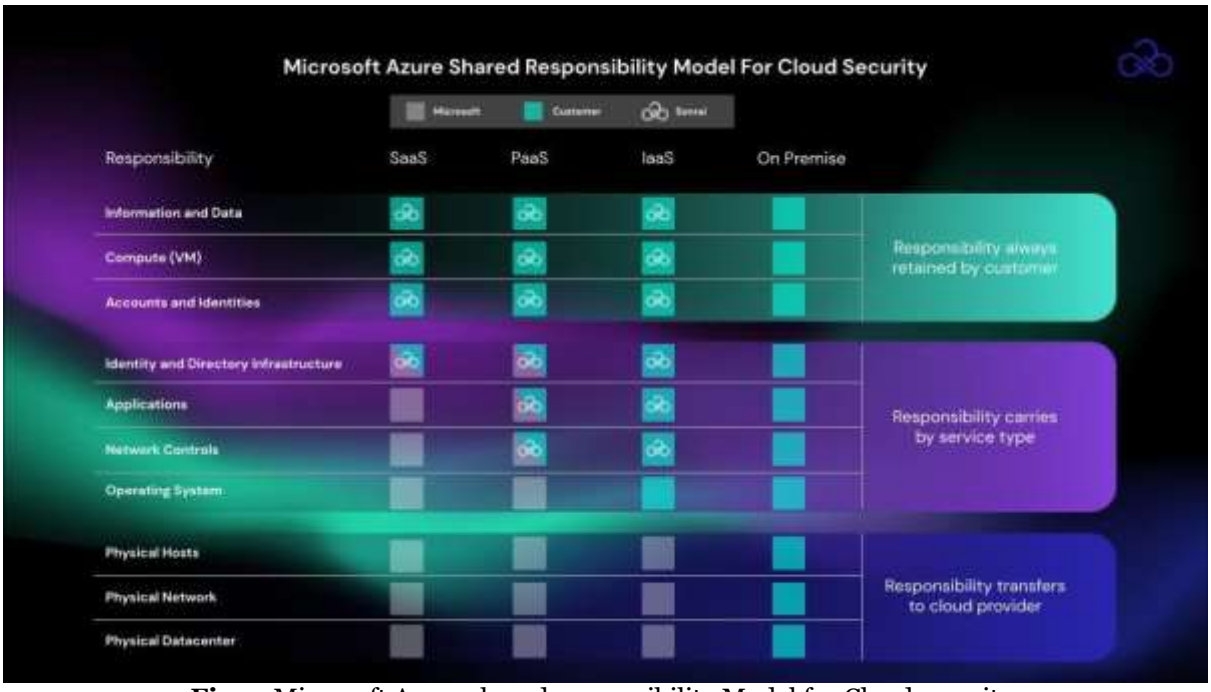


**Fig 4:** Microsoft Azure shared responsibility Model for Cloud security.

The responsibility for the security of the client's data and identities, as well as the cloud components under their control, lies with the customer, according to Microsoft's unambiguous definition. Following this, the Azure Shared Responsibility model specifies the four duties that the client is inevitably responsible for:

- Data
- Endpoints
- Account
- Access Management

## 5. GOOGLE CLOUD PLATFORM (GCP) SHARED RESPONSIBILITY MODEL

Google Cloud identifies many domains as follows: content; consumption; deployment; identification; operations; network security; data and content; networking; storage and encryption; and hardware. They also set the boundary based on the service you're using. Infrastructure as a service (IaaS) providers argue that users should pay the lion's share of the cost for services like Compute Engine, Cloud Storage, Cloud DNS, Cloud VPNs, etc., while they take care of infrastructure security and hardware. Platform as a service (PaaS) models, like BigQuery and Google Cloud Platform (GCP), more fairly divide up the tasks of application level management, data and identity protection, and the use of the same physical hardware and infrastructure by both the customer and GCP, with the latter also providing extra network controls. Software as a service providers (SaaS) like Google Workspace highlight their own efforts and responsibilities, while customers are only held accountable for the data and controls they opt to store in the service.


**Fig 6**: Googles responsibility.

Best Practices for Implementing the Shared Responsibility Model

**Review the SLA:** It is important to carefully check your SLA to understand what you are agreeing to, as responsibilities can vary depending on the cloud. Now is the moment to clear up any confusion and work together with your provider to reach a mutual understanding. Read each one if you're using many clouds.

**DevSecOps**: A commitment to the ongoing lifecycle of security is implicit in a DevSecOps mindset. Security shouldn't be an afterthought; thinking about it while you build can help you detect issues earlier and streamline your procedures.

**Focus on data:** You should always prioritise the security of your data regardless of the cloud service provider (CSP) or service you use (IaaS, PaaS, etc.). To establish a solid foundation, you should centre your strategy around your company's core operations and then expand outside. Data sensitivity should inform data classification, policy enforcement, and plan customisation.

**Keep communication open:** Mail from your service provider may arrive at any time. Updates to services or new features that could impact your security duties are among the many changes they make. If you are unsure of something, don't be afraid to ask for clarification. The security community should be your ally.

**Outsource a trusted security partner:** To ensure that you fulfil your obligations under the Shared Responsibility Model, there are resources available to assist you. Consider solutions like Cloud Workload Protection, Cloud Security Posture Management, and Cloud Infrastructure Entitlement Management. These will help with identity and permission security, critical asset lockdown, application and workload security, and secure configuration enforcement, respectively.

## CONCLUSIONS

Companies can reduce their capital and operating expenditures using cloud service, making it a significant paradigm for digital solutions. Concerns about security are high due to the fact that this technology is multi-tenant and depends on other parties to manage the cloud infrastructure. This article reviewed and analysed the current situation of cloud security, potential dangers, and mitigation strategies with a focus on identity and access management, security, and services. From both academic and business vantage points, this study

evaluates a variety of topics along with their most popular mechanisms, the main problems with each mechanism, and suggestions for improvement. It is evident that existing frameworks for this field require development in light of the numerous cloud services and identity and access control techniques evaluated; this, in turn, suggests avenues for future research to develop more appropriate methods.

## REFERENCES


1. CSA, Security Guidance Critical Areas of Focus for Critical Areas of Focus in Cloud Computing V2.1, Cloud Security Alliance, No. 1, pp. 1–76, 2009. [Online] https://cloudsecurityalliance.org/csaguide.pdf.
2. S. Eludiora, A user identity management protocol for cloud computing paradigm, Int. J. Commun. Netw. Syst. Sci. 4 (2011) 152–163, https://doi.org/ 10.4236/ijcns.2011.43019.
3. S. Subashini, V. Kavitha, A survey on security issues in service delivery models of cloud computing, J. Netw. Comput. Appl. 34 (2011) 1–11, https://doi.org/ 10.1016/j.jnca.2010.07.006.
4. Wayne Jansen and Timothy Grance, Guidelines on Security and Privacy in Public Cloud Computing, NIST Special Publication, pp. 800-144, 2011. [Online] http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf.
5. S. Singh, Y.S. Jeong, J.H. Park, A survey on cloud computing security: issues, threats, and solutions, J. Netw. Comput. Appl. 75 (2016) 200–222, https://doi. org/10.1016/j.jnca.2016.09.002.
   Castiglione, A. De Santis, B. Masucci, F. Palmieri, A. Castiglione, J. Li, X. Huang, Hierarchical and shared access control, IEEE Trans. Inf. Forensics Secur. 11 (2016) 850–865, https://doi.org/10.1109/TIFS.2015.2512533.
6. M. Alizadeh, S. Abolfazli, M. Zamani, S. Baharun, K. Sakurai, Authentication in mobile cloud computing: a survey, J. Netw. Comput. Appl. 61 (2016) 59–80, https://doi.org/10.1016/j.jnca.2015.10.005.
7. [8] Z. Liu, J. Luo, L. Xu, A fine-grained attribute-based authentication for sensitive data stored in cloud computing, Int. J. Grid Util. Comput. 7 (2016) 237–244, https://doi.org/10.1504/IJGUC.2016.10001940.
8. D.H. Sharma, C.A. Dhote, M.M. Potey, Identity and access management as security-as-a-service from clouds, Procedia Comput. Sci. 79 (2016) 170–174, https://doi.org/10.1016/j.procs.2016.03.117.
   Singh, K. Chatterjee, Identity Management in Cloud Computing through Claim-Based Solution, in: 2015 Fifth Int. Conf. Adv. Comput. Commun. Technol., IEEE, 2015. doi:10.1109/acct.2015.89.
9. Butun, M. Erol-Kantarci, B. Kantarci, H. Song, Cloud-centric multi-level authentication as a service for secure public safety device networks, IEEE Commun. Mag. 54 (2016) 47–53, https://doi.org/10.1109/ mcom.2016.7452265.
10. H. Saevanee, N. Clarke, S. Furnell, V. Biscione, Continuous user authentication using multi-modal biometrics, Comput. Secur. 53 (2015) 234–246, https://doi. org/10.1016/j.cose.2015.06.001.
11. D.A.B. Fernandes, L.F.B. Soares, J.V. Gomes, M.M. Freire, P.R.M. Inácio, Security issues in cloud environments: a survey, Int. J. Inf. Secur. 13 (2014) 113–170, https://doi.org/10.1007/s10207-013-0208-7.
12. B. Grobauer, T. Walloschek, E. Stocker, Understanding cloud computing vulnerabilities, IEEE Secur. Priv. 9 (2011) 50–57, https://doi.org/10.1109/ MSP.2010.115.
    Khalil, M. Khreishah Azeem, Consolidated Identity Management System for secure mobile cloud computing, Comput. Networks. 65 (2014) 99–110, https://doi.org/10.1016/j.comnet.2014.03.015. [16] A.P. Méndez, R.M. López, G.L. Millán, Providing efficient SSO to cloud service access in AAA-based identity federations, Futur. Gener. Comput. Syst. 58 (2016) 13–28, https://doi.org/10.1016/j.future.2015.12.002.