Cloud Security: The Future of Data Storage

Parv Bajaj, Ritika Arora, Mehak Khurana, and Shilpa Mahajan

Abstract In this modern era, all the organizations seem to be shifting their data and services to cloud because of the increase in information leaks and data thefts. It has become easier for intruders to break into the organization's data stored locally. As cloud provides a significant hike in security levels, it is slowly turning into the future of data storage. It has become crucial to acknowledge the issues regarding cloud security. Cloud security is the security of all the services provided by the cloud—storage, servers, networking, and databases. In this paper, the issues related to the same are covered along with the mitigation proposed to deal with those problems. The key to the overall security of the cloud is identity access management (IAM). IAM is inherently more secure than a simple username and password combinations because of the profile of information IAM collects. It can make access to data and networks a much more convenient process.

Keywords Identity and access management · Cloud service models · Authorization · Cloud security

1 Introduction

Cloud security refers to the security dedicated towards protecting cloud computing systems from intruders. This involves keeping data safe and private across online applications, and platforms. Ample amount of security is provided by the cloud providers as end-users trust them with their personal data. Client's trust is a key component in their business. Cloud security methods are used to keep client's data safe and private. It will be wrong to say cloud security entirely depends on the cloud provider because some part of it is certainly in the end user's hand.

P. Bajaj (✉) · R. Arora · M. Khurana · S. Mahajan
The NorthCap University, Gurugram, India
e-mail: mehakkhurana@ncuindia.edu

S. Mahajan
e-mail: shilpa@ncuindia.edu

K. Khanna et al. (eds.), *Cyber Security and Digital Forensics*,
Lecture Notes on Data Engineering and Communications Technologies 73,
https://doi.org/10.1007/978-981-16-3961-6_9

Cloud security consists of:

- IAM
- Data security
- Policies
- Data retention
- Legal compliance.

The security guidelines focus on these three phases:

Phase 1: Understanding cloud usage and risk assessment.
Phase 2: Protecting the cloud.
Phase 3: Responding to cloud security issues.

These guidelines are related to protecting the hosts running the computer instances and the network these instances are connected to. This is where IAM plays the most important role because in order to secure the network, managing users and their access privilege are necessary. The protection of cloud data assets is done through encryption of all the data present in cloud storage.

The currently used cloud environments are:

- Public cloud services are offered by third-party datacenter provider to end-user. Public cloud offers resource pooling, self-service, service accounting, multi-tenancy to manage the solutions, deployment, and securing the resources and applications.
- Private clouds are deployments set up within the organization's firewall (on-premises datacenters) and traditionally run by on-site servers. Some of the benefits of a public cloud computing environment, such as elastic on-demand capacity, service-based access, and self-service provisioning are offered [1]. Private cloud is suitable when the traditional requirements, such as control, security, and resiliency, are more emphasized by an organization with the restricted and designated user access and authorization.
- A hybrid cloud is a combination of an interoperating public and private cloud. This is the model where consumer takes the noncritical application or information and compute requirements to the public cloud while keeping all the critical information and application data in control. It is an intermediate step in the evolution process, providing businesses an onstage from their present IT conditions into the cloud environment. A hybrid cloud provides you with resources of public cloud for small projects at a cheaper rate than if you use data center's IT infrastructure. With this, you do not invest much in the resources you need on a temporary basis.
- A community cloud is the cloud managed by groups of people, communities, and agencies especially government to have common interests—such as maintaining the compliance, regulation, and security parameters—working on the same mission.
- Shared private cloud is a shared compute capacity with variable usage-based pricing to business units that are based on service offerings, accounts

datacenters. It requires an internal profit center to buy infrastructure made available through account consolidations.

2 Cloud Service Models

Before we dive into cloud security, it is necessary to study about cloud service models. Clouds will transform the IT industry and profoundly affect how we live and how businesses operate. Cloud computing:

1. Offers the scalable compute model to be accessed from anywhere.
2. Offers you with simplified service delivery.
3. Disaster recovery.
4. Provides dynamic infrastructure for upcoming technologies data center.

Some say it is grid or utility computing or software-as-a-service, but it is all three of those combined—software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS).

2.1 SAAS

In software as a service model, it is not required to install an application instead you can reliably access it via the Internet. It saves you from complex software and hardware management. A third-party provider hosts it on the internet, and it can be used by various customers. These applications are not actually managed by your company but by the software provider itself. It is more convenient as it relieves you from a pestering of software maintenance, network security, data availability, infrastructure management, and all other operational issues involved with keeping applications up and running. SAAS model onboard has the largest market share in cloud security.

2.2 PAAS

Platform as a service (PaaS) is more of a complete development and deployment environment in cloud security. In this platform-as-a-service (PaaS) model, the developers hire almost everything they need to design an application, depending on a cloud provider for development tools, infrastructure, and operating systems. The PaaS provider makes available everything like servers, networks, storage, operating system software, databases at their centralized data center. The user can purchase

the resources as per need from a cloud service provider on a pay-as-you-go basis and access them over a secure Internet connection.

2.3 IAAS

Infrastructure as a service model hosts applications on the public cloud and private cloud rather than in a traditional on-premises data center. The application is made available to users on-demand while it is being fully controlled by the cloud service provider (CSP) itself. The enterprises hire servers for computation and storage in the cloud environment. Infrastructure as a service is highly flexible as you need to purchase only the components you need according to your needs and demand and scale them up or down based on your business needs. Infrastructure as a service model is identical to utility computing, the user gets the resources on the rental basis and pays only for the resources he uses like power, data storage space, etc., on your business needs (Fig. 1).

3 Threats in Cloud Security

3.1 Data Breaches

The risk of a data breach is not new to cloud security, but it consistently ranks as a top threat to cloud customers. Common data breach exposures incorporate personal information, such as social security numbers, credit card numbers, and healthcare histories of customers, as well as corporate information, such as customer lists and software's source code [2].

Mitigation:

You can encrypt the data using data-at-rest and data-in-transit security. Traffic monitoring technique (log management to identify unreliable IP addresses) is also

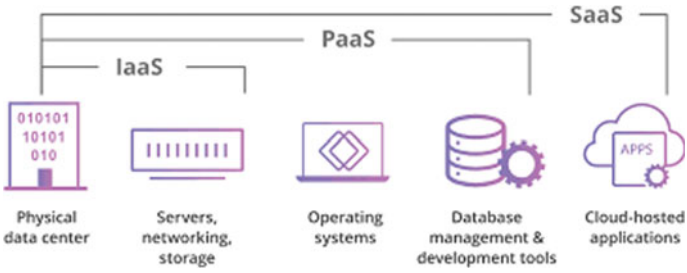

Fig.1 Cloud services models

advisable to prevent data breaches. Implementation of data access governance and establishing data remediation workflows to secure data.

3.2 Insecure APIs

The APIs are delivered by the cloud service providers to software developers to build the interfaces and with these interfaces; they can interconnect to the cloud services. Unique characteristics of API leave the door wide open for threats. The difficulties like anonymous access, reusing passwords, or tokenization could hamper the cloud services and could restrict logging, monitoring capabilities, and API dependencies which could result in DDoS attack or repudiation attack.

Mitigation:

Testing techniques that mimic an outsider attack which targets specified API endpoints and aim to break the security and get access to company's sensitive data. API keys must be protected and not reused.

3.3 Denial-Of-Service Attacks (DoS/DDoS)

A denial of service (DOS/DDoS) attack is an attempt to tie up a website's resources so that users who need to access the site cannot do so. It generally makes a website service unavailable by overwhelming it with traffic from multiple sources. These are usually launched by bots or malware from hundreds of infected hosts. Application-level DoS/DDOS attacks can easily manifest themselves as high-volume Web page reloads, XML* web services requests [3]. This attack consumes all available resources in the Web server such as memory, CPU, space in disk and indirectly abuses the functioning of the website.

Mitigation:

Implement firewalls and allowing only legitimate IP addresses or blocking ones from known attacker is one of best ways to mitigate DDoS attacks. These attacks can be nullified by rate-limiting the amount of traffic available to a specific network interface controller. The impact of DDoS attack can be reduced by filtering requests upstream, long before it reaches the target network.

3.4 Misconfigured Cloud Storage

Misconfigured cloud storage is when there are critical gaps in your cloud security that leave your organizational data at risk. It happens when you make errors while

configuring the security controls, or you forget to implement them at all. One of the repeated misconfigurations grants public access to storage buckets. These buckets are often vulnerable because of authentication methods such as passwords, making them available to everyone and prone to attacks. Although, access to these storage buckets is one of the examples of the type of misconfiguration. Organizations face innumerable types of misconfigurations as they drift to public IaaS cloud environments [4].

Mitigation:

Cloud security configurations must be double-checked upon setting up a particular cloud server. This should be understood that configurations are part of security. A third-party security tool should be used that can look at configurations constantly. It provides a constant check and alerts you when things are misconfigured. Outside security testers should be hired to ensure that everything is configured correctly. Sometimes audits can find things that a client may overlook. The stuff being uploaded on the storage should be checked for hidden malwares.

4 Identity and Access Management

Identity and access management refers to the ability to manage user identities and their privileges to access the resources. IAM is the first step to make an organization effective in communication, reliability and securing sensitive data. Identity is the necessity for the foundation of identity and access management. It lubricates the path of providing user's privacy and secure guarding their sensitive information from data theft using identity. Identity plays a crucial role in this heterogeneous cloud environment. IAM strategies have been an important facet of IT platform as it helps to make work possible. IAM as a framework consists of policies which authenticate and authorize user to access a specific resource.

IAM ensures that you as an identity are accessing the appropriate resource at the right point of time securely and you are right person to access it with the help of these two components:

- Authentication.
- Authorization.

Within **authentication**, applications recognize you as a person by looking at your identity cards, digital certificates, etc.

Within **authorization**, applications check what permissions you have to perform actions in that specific environment considering roles, attributes of your identity, or other affiliations to decide if you are authorized to have access to a particular resource. Both these calls help to reduce the load of help desks and maintain the user's privacy. Main functionalities required from an IAM system are:

- An individual may have multiple accounts requiring PINs or passwords.
- Authentication of the user is done by a unique ID provided by IAM system.
- For authentication purpose, complexity of passwords are determined; SSO techniques and OTPs are used to prevent stealing of passwords.
- IAM manages log activity so no suspicious activity passes unnoticed resulting in preventing identity thefts.
- IAM lets individuals manage their personal and confidential data and lets organizations modify data of their employees.

IAM stops threatening activities with the help of techniques like log management, machine learning, and other algorithms. It maintains policies to make users comply with security agreement of the companies.

5 Authentication

The methods to determine that someone is who they claim to be. The most commonly used authentication method is the log-on credentials. But using passwords alone for authentication is increasingly regarded as insecure since passwords are easy for hackers to crack using various attacks (Fig. 2).

5.1 Single Sign-On (SSO)

SSO is an Internet access management tool that allows a user to log in to one of an organization's portal and automatically be logged in to a designated set of other properties. For example, when you log in to Google, you are automatically logged in to your Gmail and YouTube accounts. For users, since they do not have to keep track of different credentials for every application, SSO reduces friction. For organizations, SSO helps in collecting valuable insights about client's behavior and

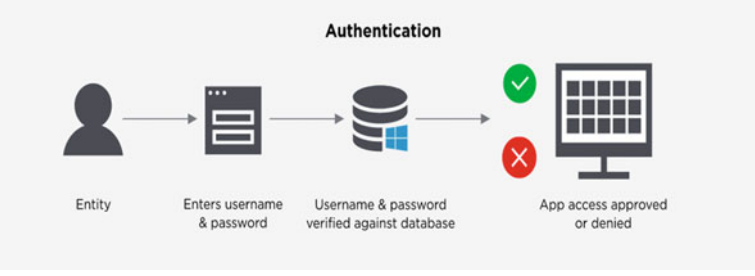

Fig. 2 Authentication basic concept

preferences since it tracks them as they move from one application to another, connected by a single login.

5.2 Multi-Factor Authentication (MFA)

Implementing multi-factor authentication is crucial to protect your organization's data and crucial information from malicious intrusions. Every IAM platform offers some form of MFA. However, it is equally crucial to customize MFA with the appropriate level of security. IN B2C contexts, you need to consider UX (user experience) and try not to create unnecessary friction for users who do not want to be subjected to heightened scrutiny every time they log in. For IAM in workplace, you may want more stringent multi-factor authentication, since the consequences of an unauthorized party gaining access to your private network can be so devastating. A modern IAM solution will allow you to implement MFA only when it is needed. This can be accomplished through step-up authentication or adaptive authentication in which users only trigger MFA if they are trying to access sensitive data or their behavior is flagged as risky.

5.3 Anomaly Detection

In the past few years, identity has become a preference for hackers to break into systems. Credential stuffing attacks, brute-force attacks and even highly targeted phishing campaigns are all attempts by hackers to break in through an organization's front door: the login box. These attacks can be devastating, leading to legal fallout, huge spikes in traffic that crash applications and most of all, stolen data. IAM solutions are designed to get in front of those issues through anomaly detection. There are multiple ways identity access management systems can help to detect and mitigate malicious attacks. For example, by detecting attacks by monitoring signals such as the velocity of traffic, detection of login patterns that differ from a user's routine (such as location and browser), use of devices and IP addresses with a poor reputation, or use of a breached password.

5.4 OpenID

OpenID is a protocol which allows users to be authenticated by cooperating sites—RP (relying parties) using a third-party identity vendor. It is an open standard authentication protocol. A relying party (RP) is a service that depends on a third-party identity provider to identify and authenticate a user who is requesting

access to a digital resource [4]. OpenID supports single sign-on services by allowing users to sign in to multiple websites and web services using just one identity.

5.5 Federated Identity

While in single sign-on, the tool lets users log in to different properties or brands owned by a single organization; federated identity does the same thing across multiple organizations. The example of federated identity we see in real life is through social login, in which you can use your Google, Facebook, or Apple ID to log in to a wide range of apps. Federation is built on trust, so when you order from a food delivery app with your Samsung pay ID, you are not ordering from Samsung but indicating that the app trusts Samsung enough to take their word that you are who you claim to be.

5.6 SAML

SAML works by transferring the client's identity from the identity provider to the service provider. This is done via an exchange of digitally signed XML documents [5].

5.7 OAuth

OAuth offers one-way authentication. It is an open-standard authorization framework that allows a user to grant a third-party website access to the user's protected resources, without necessarily revealing their long-term credentials or even their identity [6]. Commonly used by consumer applications and services, so users do not have to sign up for a new username and password. Some examples of OAuth in real world are when you go to log on to a website and it offers one or more ways to log on using another website's logon—"Sign in with Google" or "Log in with Facebook".

6 Authorization

Authorization is the module that is used to determine users' privileges for a particular resource which usually includes system data, files, network services, etc. To explain it better, we can look at some examples: privilege to access any service at all, to access any service with a well-stated write access, to access only a part of the network service or permission to get into whole cloud console. Authorization in

Fig. 3 Authorization basic concept

organizations is usually achieved by access control policies or access right delegations. Access control policies can be defined as—only the authorized clients will be able to access both the resources and services. Authorization is based on complex access control mechanisms which keep record of user attributes like session id, personal information, etc. It helps in safeguarding sensitive information and reducing security risks (Fig. 3).

6.1 Access Control Mechanisms

6.1.1 MAC (Mandatory Access Control)

Mandatory access control sets up access policies and states security attributes for the clients where the system provides users with access rights. The access policies are handled by the director, and the users are not given the rights to set, alter, or repeal permissions. When a user tries to access any program, the operating system examines the user's security attributes and decides whether the access can be granted or not. The system verifies the credentials of every individual when any resource is accessed by them. All the security measures are forced by the kernel itself. The system provides access to users based on their clearance level. This type of access control is implemented on systems with high security such as army systems or bank systems. In mandatory access control model, security labels are assigned to every file system object (determines whether it is confidential, secret, etc.). The classification label is maintained by the operating system. If a client wants to access a confidential or a secret file, he must have a secret clearance or high clearance level [5].

6.1.2 DAC (Discretionary Access Control)

In the discretionary access control model, power lies in the hands of owner of the resource; he decides who can have access to a specific object. In DAC, controls are

discretionary as the users can access a file on identity basis. The file owner has the authority to change the permissions of the file. The owner can grant access to other clients as per the requirements. Discretionary access control offers a high level of security to data networks of company [7]. DAC minimizes threats and attacks by setting up a firewall with a well-organized IP-tables rules. Unauthorized users are blind to resource characteristics, such as file size, file name, and directory path. All operating systems like Windows, UNIX, and Linux use discretionary access control. DAC provides more flexibility as compared to MAC and is labor-intensive.

6.1.3 RBAC (Role-Based Access Control)

Role-based access control is a way for organizations to manage and assign access privileges across the network in a structured way. RBAC grants permissions based on the employee groups and their subsequent roles. The duties for those groups of employees can be segregated and only the amount of access the groups needs to perform their jobs can be granted. Users may be assigned multiple roles as required. In RBAC, an employee's position determines the permissions they are granted and ensures that lower-level employees are not able to access sensitive information or perform high-level tasks. Organizations that utilize RBAC are better able to secure their sensitive data and critical application [8]. RBAC provide the organizations with some benefits like:

- The process of adding or changing roles of the employees is automated resulting in less paperwork, therefore, increasing in efficiency.
- In RBAC, the data access is appropriately managed resulting in overall better control of compliance efforts.
- RBAC reduces the possibility of data theft, breaches, and information leaks by ensuring that only authorized users have permission to access certain areas of the system.

6.1.4 ABAC (Attribute-Based Access Control)

Attribute-based access control provides access rights based on any type of attributes —environmental attributes, resource attributes, and user attributes.

- Environmental attributes are those that relate to environmental conditions. It includes the location of the data, time of access, and current organizational threat levels [9].
- Resource attributes can be used to enable access control that relates to a particular resource, such as an operating system or application. It includes things like resource owner, creation date, file name, and data sensitivity [10, 11].
- User attributes include things like the user's role, name, ID, and security clearance [12].

7 Conclusion

We can conclude that for digital success in the future, IAM with strong privilege access management is necessary. This paper summarized every security issue that might occur in cloud environment, proposed mitigation for those issues, and potential threats are discussed with an emphasis on IAM. If all these threats are acknowledged and provided mitigation methods are performed, the transfer from local storage to cloud storage can be carried out very smoothly. As with proper implementation of IAM, cloud is going to become the most secure place to keep confidential data, and all the organizations will be shifting to cloud for storage resulting in cloud becoming the future of storage.

References

1. Singh, A., Chatterjee, K.: Identity management in cloud computing through claim-based solution. In: 2015 Fifth International Conference on Advanced Computing and Communication Technologies (2015). https://doi.org/10.1109/acct.2015.89
2. Rowe, N.S.: The future of identity management (2018). Retrieved from https://techvisionresearch.com/
3. Mogull, R., Arlen, J., Gilbert, F.: Cloud Security Alliance. Security Guidance for Critical Areas of Focus in Cloud Computing, V2.1 (2009). http://www.cloudsecurityalliance.org/
4. Sharmaa, H.D., Dr. Dhoteb, C.A., Poteyc, M.: Identity and access management as security-as-a-service from clouds. In: 7th International Conference on Communication, Computing and Virtualization (2016)
5. Bresz, F., Renshaw, T., Jeffrey R., Torpey, W.: Identity and access management (2007). Retrieved from https://chapters.theiia.org/montreal/ChapterDocuments/GTAG%209%20%20Identity%20and%20Access%20Management.pdf
6. Dragoş, M.M.: Cloud identity and access management—a model proposal. Account. Manag. Inf. Syst. **11**(3), 484–500 (2012)
7. Indu, I., Anand, P.M.R.: Identity and access management in cloud environment: mechanisms and challenges (2015). Retrieved from https://www.researchgate.net/publication/325336543
8. Zhu, Y., Huang, D., Hu, C.-J., Wang, X.: From RBAC to ABAC: constructing flexible data access control for cloud storage services. IEEE Trans. Serv. Comput. (2015). https://doi.org/10.1109/tsc.2014.2363474
9. Mohammed, H.K., Hassan, A., Yusuf, D.M.: Identity and access management system: a web-based approach for an enterprise. Path Sci. **4**(11), 1–11 (2018)
10. Khurana, M., Singh, H.: Two level phase retrieval in fractional Hartleydomain for secure image encryption and authentication using digitalsignatures. Multimed. Tools. Appl. **79**(19), 13967–13986 (2020)
11. Khurana, M., Singh, H.: An asymmetric image encryption based onphase truncated hybrid transform. 3D Res. **8**, 1–17 (2017)
12. Rohilla, A., Khurana, M., & Singh, L.: Location privacy usinghomomorphic encryption over cloud. Proquest. Int. J.Comput. Netw. Inf. Secur. **09**(08), 32–40 (2017)