DOI: https://doi.org/10.31410/ITEMA.2023.35

ONE Security Solution in a Cloud Environment

Marija Zajeganović[1]
Milan Pavlović[2]
Nenad Kojić[3]

Received: December 22, 2023
Accepted: February 11, 2024
Published: May 28, 2024

Keywords:
Security;
Cloud;
Services;
Virtualization

Creative Commons Non Commercial CC BY-NC: This article is distributed under the terms of the Creative Commons Attribution-Non-Commercial 4.0 License (https://creativecommons.org/licenses/by-nc/4.0/) which permits non-commercial use, reproduction and distribution of the work without further permission.

Abstract: *Over the past decade, cloud computing and virtualization have become one of the areas that increasingly capture the attention of the IT world. The significance and advantages of cloud platforms compared to traditional infrastructure systems are numerous. On the other hand, due to the openness of many services to the public network and the need for certain services to be accessible exclusively through secure and private networks, security in the cloud becomes a highly significant issue. In the first part of the paper, an overview of cloud service delivery models will be provided. The authors will then elaborate on some core cloud services and their security aspects in detail. Additionally, security mechanisms in a virtual private cloud will be explained.*

1. INTRODUCTION

Irrespective of the industry type or company size, whether it's a corporation or a startup, the capabilities of cloud technology have proven highly effective. An increasing number of companies are recognizing the significance and benefits of cloud platforms over traditional infrastructure systems. This has resulted in a significant rise in cloud migrations and an uptick in the utilization of cloud services. Due to the openness of many services to the public network, as well as the need for certain services to be available exclusively through a secured and private network, prioritizing security in the cloud has become crucial. The number of cyberattacks is increasing, and so are the resources invested in security. Numerous providers offer a diverse range of cloud services and infrastructures to users globally around the world. Azure Web Services is first cloud provider, started business in 2006. The three biggest cloud providers are Amazon Web Services (AWS), Azure, Google Cloud Platform.

This paper will present an overview of the cloud concept and cloud architecture, followed by an overview of cloud core services and their security aspects, and finally, as an example of a security solution in a cloud environment, security mechanisms in a virtual private cloud will be presented.

2. CLOUD COMPUTING CONCEPTS AND ARCHITECTURES

The principles underlying cloud computing include virtualization, scalability, flexibility and adaptability, pay-as-you-go model and high availability. Virtualization allows physical resources, such as servers and network infrastructure, to be shared and used in multiple ways. Virtualization enables better use of resources and greater flexibility in adapting resources to user

[1] The Academy of Technical and Art Applied Studies Belgrade, Department School of Information and Communication Technologies, Starine Novaka 24, Belgrade, 11000, Republic of Serbia

[2] The Academy of Technical and Art Applied Studies Belgrade, Department School of Information and Communication Technologies, Starine Novaka 24, Belgrade, 11000, Republic of Serbia

[3] The Academy of Technical and Art Applied Studies Belgrade, Department School of Information and Communication Technologies, Starine Novaka 24, Belgrade, 11000, Republic of Serbia

OPEN ACCESS

needs. Scalability provides the ability to quickly and easily scale resources. Users can easily increase or decrease capacity according to their current needs, thus achieving more efficient use of resources. Flexibility and adaptability allow users to connect to resources and services through the network from any location and various devices. Users can customize their resources, applications and settings according to their needs and preferences. One of the main advantages of cloud computing is the pay-as-you-go model where users only pay for the resources and services they actively use, eliminating the need for substantial investments in expensive infrastructure. This model enables better cost control. Cloud providers usually guarantee high availability of their services through redundancy and data distribution across multiple locations. This ensures that applications and data are available to users at all times, even in the event of hardware failure or problems at one location.

The definition of cloud computing (Mell & Grance, 2011) that received industry-wide acceptance was composed by the National Institute of Standards and Technology (NIST). "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models."

The five essential characteristics are on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service. The three service models are Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) as shown in Figure 1. The four deployment models are private cloud, community cloud, public cloud and hybrid cloud.

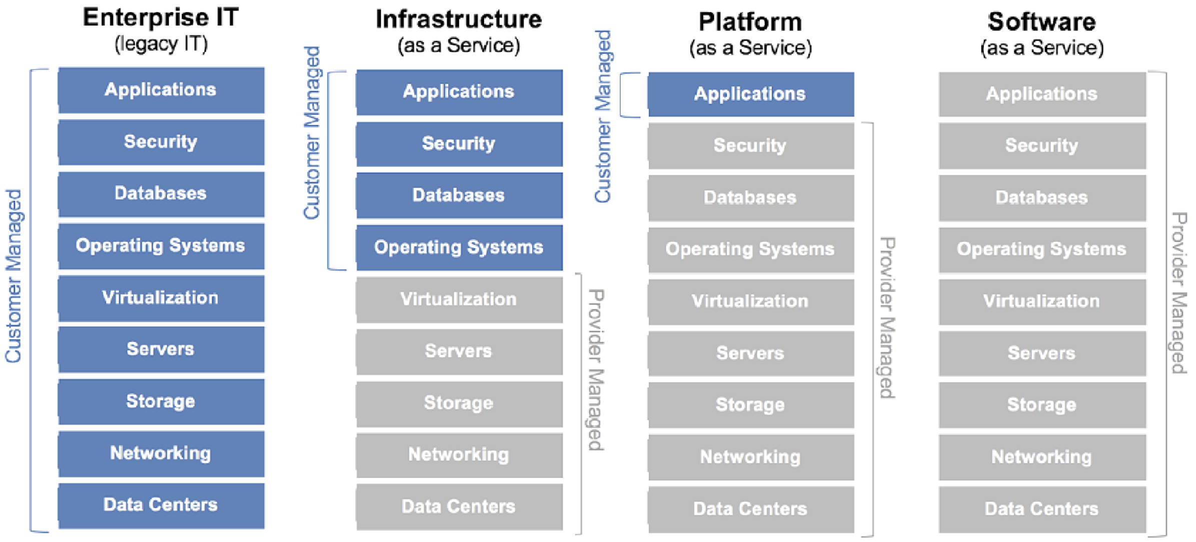

Figure 1. Cloud computing services defined by the NIST

Source: General Services Administration, n.d.

In Software as a Service (SaaS) model, the cloud provider assumes responsibility for granting access to applications and services, such as email, communication tools, and Office 365, all delivered over the internet. Users are relieved from managing any aspect of the cloud services, except for limited user-specific application settings. Their primary obligation is to provide their data.

For Platform as a Service (PaaS) model, the cloud provider is accountable for offering users access to development tools and services required for application delivery. Typically, these users are programmers who may exert control over the configuration settings of the cloud provider's application hosting environment.

In Infrastructure as a Service (IaaS) model, the cloud provider is tasked with providing IT managers access to network equipment, virtualized network services, and supporting network infrastructure. This cloud service allows IT managers to deploy and run software code, encompassing operating systems and applications.

None of the mentioned solutions is an ideal solution for every company, and most companies tend to change their cloud philosophy over five years.

Cloud service providers have extended this model to also provide IT support for each of the cloud computing services. For businesses, IT as a Service (ITaaS) can extend the capability of the network without requiring investment in new infrastructure, training new personnel, or licensing new software. These services are available on demand and delivered economically to any device anywhere in the world without compromising security or function and we also have a new model SECurity as a Service (SECaaS) (Theodoropoulos et al, 2023).

3. CLOUD CORE SERVICES AND THEIR SECURITY ASPECTS

Cloud core services serve as the foundational elements and resources that support the infrastructure of cloud platforms. They play a crucial role in the development and administration of various cloud-based applications and solutions. Security is a critical aspect of cloud core services, given the imperative to protect the cloud environment from potential threats and vulnerabilities. Key dimensions of cloud core services include physical security, data encryption, identification and authentication, access control, security monitoring, and measures for redundancy, as well as disaster recovery.

Identity and Access Management (IAM) stands as a vital element within cloud core services, serving as a foundational service enabling organizations to manage and regulate access to their cloud resources and services. IAM plays a foundational role in upholding the security and compliance of cloud-based environments. IAM identities, encompassing both human users and non-human entities like applications, services, or systems, are entities capable of making requests to access cloud resources. The significance of IAM services lies in their ability to finely control privileges and compel users to adhere to security policies. IAM policies define the permissions and access control rules for resources (Mell & Grance, 2011). These policies are attached to IAM identities and resources, specifying what actions are allowed or denied. Some of the features of the IAM service are centralized identity management, granular access control, multi-factor authentication, access delegation, auditing and activity monitoring.

IAM identities offer security mechanisms, including authentication and authorization, ensuring that only authorized users can access specific resources. Additionally, IAM identities support access delegation of access and facilitate compliance with data protection regulations and rules. These identities play a crucial role in precisely defining access rights, roles, and privileges, enabling organizations to effectively manage and control resources and data within the cloud infrastructure. User accounts, representing individuals within an organization or team, receive specific types of access and can be organized into user groups. User groups serve the purpose of grouping user accounts to grant privileges at the group level.

IAM policies play a key role in ensuring security and managing access in a cloud environment. They allow administrators to grant specific privileges to users or groups of users. This may include access to certain resources, services, or functionality. Granting privileges can be based on roles, business needs, or other factors. IAM policies can be designed to ensure compliance with data protection laws and regulations. For example, policies can ensure that only certain users have access to sensitive or regulated data. Also, policies may require the use of certain security mechanisms such as multi-factor authentication or data encryption. Policies are attached to identities and define the exact range of privileges that an identity can share within the system as shown in Figure 2.

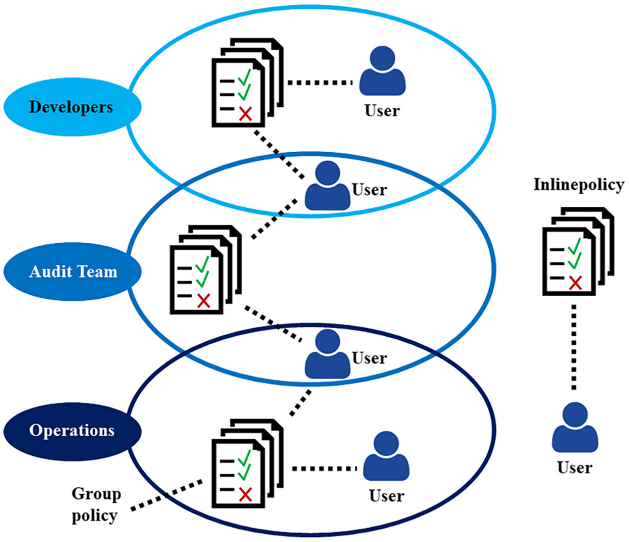

Figure 2. The way policies function within different user groups

Source: Own research

Multi-factor authentication (MFA) is a security mechanism that requires individuals to provide two or more separate factors to verify their identity during the authentication process. This additional layer of security makes it significantly more difficult for unauthorized users to gain access to an account or system (Kunduru, 2023). MFA devices can be physical and virtual. The essence of MFA is that even if user content is stolen, an attacker cannot access the service. In the event of an attempt to find a six-digit code using the "Brute-force" technique, logging into the service will soon be blocked and additional identity verification will be required. Multi-factor authentication is a perfect blend of what the user needs to know (credentials) and what the user has (device MFA).

Amazon Elastic Compute Cloud (Amazon EC2) is a web service offered by Amazon Web Services (AWS) that provides resizable compute capacity in the cloud. In simpler terms, it allows user to rent virtual servers on a pay-as-you-go basis. EC2 provides various mechanisms for security and access control, such as defining security groups that define rules for incoming and outgoing network traffic, integration with AWS IAM for managing identities and access rights, as well as the ability to use keys for data encryption.

Amazon Elastic Block Store (Amazon EBS) is a cloud-based block storage service provided by Amazon Web Services (AWS). EBS is designed to provide scalable and durable block-level storage volumes that can be attached to Amazon EC2 instances, making it a critical component for storing and managing data in the AWS cloud. One of the key functionalities of EBS is the ability to encrypt data at the disk level. Users can encrypt EBS volumes to protect data from unauthorized access.

4. SECURITY MECHANISMS IN A VIRTUAL PRIVATE CLOUD

The virtual private cloud architecture establishes a private cloud with underlying infrastructure that belongs to a public cloud provider but that is exclusively dedicated to one specific cloud consumer for whom the private cloud is delivered. This can be useful for an organization that wants to have a private cloud but does not have the necessary infrastructure to support it on-premise (Erl & Baecelo 2023). Virtual private cloud (VPC) represents a logical virtual private network in which cloud users implement their infrastructure. In many of its elements, VPC resembles the traditional network infrastructure of data centers, but with almost unlimited possibilities for scalability and expansion. A VPC is divided into multiple availability zones. It consists of many network components such as a router, internet gateway, and NAT gateway.

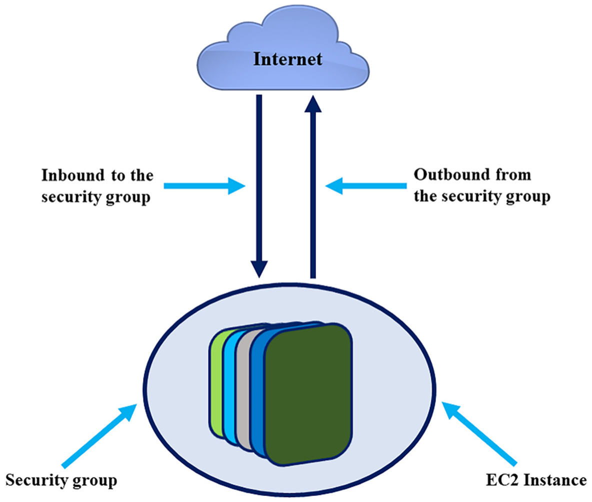
Internet
Inbound to the security group
Outbound from the security group
Security group
EC2 Instance

Figure 3. Inbound/Outbound security group rules

Source: Own research

Security groups represent the first level of protection. This is a type of firewall that controls inbound and outbound traffic at the EC2 instance level within the VPC as shown in Figure 3. Security groups contain only “allow rules”, while at the end there is always an “implicit deny rule”. When filtering traffic, it goes through all the rules in search of a permit rule.

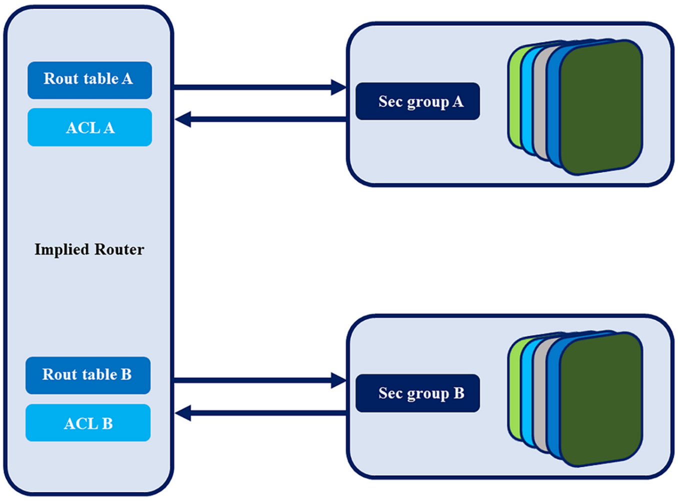

Figure 4. Security within a VPC

Source: Own research

Security groups are not the only type of protection. Access control lists (ACL) are responsible for protecting the third layer of the TCP/IP model. An ACL is a built-in feature within the default router, which is an integral element of every VPC as shown in Figure 4. ACLs use the stateless concept. In case inbound traffic is allowed, outbound traffic will not be allowed by default, but all outbound rules within the ACL will be taken into account. The same principle will be applied in the opposite direction of the network traffic. It goes through the rules until the moment of matching, and then apply the permit or deny rule. ACLs stand as a first line of defense for inbound traffic and a secondary line of defense for outbound traffic.

5. CONCLUSION

Cloud security is a shared responsibility between cloud providers and companies (users). Cloud providers are constantly improving and implementing advanced methods like encryption, firewalls, multiple levels of authentication and other security mechanisms to protect user data from unauthorized access. However, users also need to take on a large part of the responsibility, including implementing adequate security policies, regularly updating software, educating employees and implementing security protocols.

Based on all of the above, it can be safely concluded that sudden changes within the industry and all the improvements that come with them, bring more and more complex infrastructures that will require more and more complex security solutions.

References

Erl, T., & Baecelo, E. (2023). *Cloud Computing Concepts, Technology, Security, and Architecture*. Second Edition. Pearson.

General Services Administration. (n.d.). Cloud Security. CIC.GSA.gov. https://cic.gsa.gov/basics/cloud-security

Kunduru, A. R. (2023). THE PERILS AND DEFENSES OF ENTERPRISE CLOUD COMPUTING: A COMPREHENSIVE REVIEW. *Central Asian Journal of Mathematical Theory and Computer Sciences*, 4(9), 29-41.

Mell, P., & Grance, T. (2011). *The NIST definition of cloud computing.* NIST Special Publication 800-145. U.S. Department of Commerce

Theodoropoulos, T., Rosa, L., Benzaid, C., Gray, P., Marin, E., Makris, A., Cordeiro, L., Diego, F., Sorokin, P., Girolamo, M. D., Barone, P., Taleb, T., & Tserpes, K. (2023). Security in Cloud-Native Services: A Survey. *Journal of Cybersecurity and Privacy, 3*(4), 758-793. https://doi.org/10.3390/jcp3040034