International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2021): 7.86

Analyzing Data Security Issues in Cloud Platforms Like AWS

Mohammed Sadhik Shaik

Sr. Software Web Developer Engineer, Computer Science
Germania Insurance, Melissa, Texas, United States of America
mshaik0507[at]gmail.com

Abstract: ***Computing cloud services occurs during the transfer of services from a local machine to a remote server on a distributed platform. Platform as a service (PaaS), software as a service (SaaS), and infrastructure as a service (IaaS) are just a few of the many offerings from cloud service providers. The cloud server offers a variety of services, including data storage, resource sharing, and virtual computing. In the course of technically handling the difficulties, more infrastructure-related issues pop up. There are potential security dangers that users face when sending data using specific programs. Security concerns, such as denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks, vulnerabilities in network communication, privacy concerns, incorrect cryptographic algorithm selection, and incorrect network design, are other internet dangers that might impact cloud services. Find out what kinds of attacks are possible on the cloud distributed platform when you use specific services. With an emphasis on data privacy in the cloud, we must ensure the services' security through authentication, access control, and data integrity. Confirm the existence of different cloud platform assaults and enhance the security events detected at the network layer. With the help of the AWS platform, the system can tailor its solutions to meet the needs of each client while also bolstering the cloud's security core in accordance with all applicable regulations (Vaibhav Sharma, et. al., 2020). Then, to safeguard the organization's data, components, and devices, AWS uses its datacentre to its full potential. Then, when paired with supply chain management, the cloud services offered by AWS can help the consumer.***

Keywords: Denial of Services, Distributed System, Cloud Services, Attacks, AWS

1.Introduction

The most important question to ask is, "What is cloud computing?" Through the use of cloud computing, users no longer need to invest in costly and specialized hardware in order to have remote access to powerful computer resources and related services. Plus, the main perk of cloud computing is that you only have to pay for what you use. Thanks to its scalability, affordability, and adaptability, the cloud is revolutionizing the way information technology is managed. In the next two to three years, the global cloud computing industry is expected to surpass $800 billion, according to recent forecasts [1,2]. Several old ideas and technologies are the bedrock upon which cloud computing is built. Early on in the history of distributed computing, renowned computer scientist J.C.R. Licklider proposed a "Intergalactic Computer Network" in the 1960s, which would have enabled distant access to data and programs. Grid computing first appeared in the 1990s as a method to execute computationally heavy jobs by combining resources located in different physical locations.

A framework for managing computational grids was given by the Globus Toolkit, which was created by Carl Kesselman and Ian Foster. Utility computing, which provided access to computing resources on a pay-as-you-go basis, also came into existence during this period. Benefits of on-demand resource rental were demonstrated by Sun Microsystems and Amazon's utility computing models. Changing the way computer resources are allocated and used, the term "cloud computing" emerged in the middle of the 2000s. With the introduction of Infrastructure as a Service (IaaS) in 2006, Amazon Web Services (AWS) began offering online networking, storage, and virtualized servers. Cloud computing, with its scalability and adaptability, shook up the hosting industry. Cloud computing was defined in 2011 by the National Institute of Standards and Technology (NIST) as a way to standardize computational resources that provide on-demand network access to a shared pool of programmable computers. Universality and ease of use were highlighted by NIST in their model. A lot of research has looked at many perspectives on cloud computing, which has helped shed light on its possibilities and repercussions.

1.1. Cloud Security Frameworks

Ability of Framework

Protecting the privacy, authenticity, and accessibility of sensitive company information while it is stored in the cloud is the primary goal of cloud security frameworks [3]. Undertook a rigorous analysis of the efficacy of new security frameworks in boosting cloud security. The study's overarching goal is to improve cloud security posture by analyzing and evaluating different cloud security standards and frameworks. Several prominent cloud security frameworks were investigated in depth by the writers. These included the Cloud Security Alliance (CSA) Security Guidance, the NIST Cloud Computing Security Reference Architecture, and the ISO/IEC 27017:2015 Cloud Security Controls. Important cloud security considerations like data protection, access management, encryption, and incident response were the basis for evaluating these frameworks. By comparing the two frameworks, the study exposed their respective advantages and disadvantages. Insights into the specific security measures and suggestions offered by these standards were provided, enabling readers to understand their relevance and use in different cloud deployment models. New security frameworks were also compared to previous standards in the study [5].

2.Literature Review

In an effort to address the problems and mitigate the risks associated with cloud security, a number of different approaches have been proposed and implemented. A few instances are provided here. Encryption and Key Management: Encrypting data both while it is stored and while it is in transit is an effective way to keep illegal access from occurring. When it comes to preserving the security of encryption technologies, having the appropriate key management solutions is absolutely necessary [6]. Identity and Access Management (IAM): Having reliable IAM solutions is critical for managing user identities, roles, and permissions. The principle of least privilege, when put into practice, helps reduce the likelihood of potential risks. It is [7]. Security for Virtualization: It is vital to properly secure the virtualization layer in order to prevent attacks that target weaknesses in the hypervisor or instances of virtual machines [8].

Security solutions that are Exclusive to the Cloud The utilization of cloud-native security solutions has the potential to improve threat detection and response within the cloud environment. Real-time monitoring is provided by a variety of tools, including AWS GuardDuty and Azure Security Center. In the realm of security monitoring and incident response, the utilization of all-encompassing security monitoring technologies and processes enables the identification of security issues and the prompt implementation of appropriate responses. Continuous monitoring, log analysis, and threat intelligence are all essential components in the process of identifying and mitigating security breaches [9]. Standards and Certifications for Cloud Security: Standards and certifications for cloud security that are recognized by the industry offer a framework for analyzing and ensuring the security of cloud services. [10] Organizations are able to evaluate the security capabilities of cloud service providers with the use of standards like as ISO 27001, CSA STAR, and FedRAMP. Organizations can benefit from conducting regular security audits and assessments because they help them detect vulnerabilities and ensure that they are in compliance with security standards. Independent audits, penetration testing, and vulnerability scanning are all components of a proactive security plan [11].

Both the implementation of secure configurations for cloud services and the strengthening of the underlying infrastructure in order to reduce the risk of potential vulnerabilities [12]. In spite of the fact that the preceding literature has been found to contain a few holes. In cloud security research, one of the gaps that has to be filled is the demand for a comprehensive understanding of the growing dangers and threats that are associated with cloud systems. In order to stay one step ahead of potential threats, it is necessary to do ongoing research because the cloud ecosystem is continually evolving, which results in the development of new attack vectors and vulnerabilities [13]. One of the problems with cloud security is that there are not enough consistent standards or regulatory frameworks. This makes it difficult to maintain compliance and excellent security across a wide range of cloud service providers (CSPs) and businesses thanks to the issues that this presents. In order to build standardized frameworks that are capable of satisfying the requirements for security and compliance, it is required to conduct relevant research. One of the most significant shortcomings of cloud computing is that it does not provide any options for auditing or transparency.

Due to the fact that organizations usually have little insight into the security measures that have been implemented by CSPs, this might hinder the effectiveness of monitoring and incident response efforts. Regarding accountability and culpability in the event of a security breach or data loss, the shared responsibility model of cloud computing raises challenges that need to be addressed. The establishment of legislative frameworks for responsibility and the determination of the level of duty that exists between customers and CSPs is a challenge that persists over time. In order to implement proactive security measures, having effective threat intelligence is essential. The availability of comprehensive threat intelligence that is specific to cloud systems is lacking, however, and this is a gap in the market. There is a need for research to improve threat intelligence techniques that are specifically geared to cloud-based adversaries.

AWS Security Risks: Best Practices & Instructions

One of the most well-known and prominent hyper-scale public cloud providers is Amazon Web Services (AWS). Infrastructure, platforms, and software as a service solution are offered by AWS, which operates 38 data centers globally and delivers more than 200 services. A great deal of complexity has been introduced to the AWS cloud by the extensive and adaptable nature of AWS services. Also, from sole proprietors and small businesses to multinational conglomerates, AWS wants its platform to be available to all. As a result, AWS implementations may face security vulnerabilities due to the mix of accessibility and complexity. Data compromise, service interruption, and reputational harm could occur if threat actors exploit these vulnerabilities without mitigation. Here we'll take a look at seven of the most prevalent security threats to AWS and how businesses may protect themselves from them.

AWS Security Risk #1: Misconfigurations

Misconfigurations, such as inadvertently enabling all Internet traffic to an EC2 instance or making an S3 bucket with sensitive data publicly accessible, are the leading cause of AWS security breaches. In this group of AWS security concerns, items arise from unintentional misconfigurations or wrong settings caused by ignorance. For instance, when first learning how to use AWS, many people set up IAM permissions for resources like S3 buckets that are too liberal. This applies to both users and roles. Tools and procedures to identify, avoid, and fix misconfigurations are the defenses against this AWS security risk. Here are three measures that businesses can use to lessen their vulnerability:

- Make sure your AWS setups are consistent and safe by using Infrastructure as Code technologies such as AWS CloudFormation and Terraform.
- Make use of compliance technologies that can detect and notify you of potentially unsafe setups in real-time.

- Assess the safety, speed, resilience, and efficiency of your application and infrastructure with the help of the AWS Well-Architected Framework.

AWS Security Risk #2: Credential leaks

There have been multiple high-profile AWS breaches due to compromised credentials. While compromised credentials like usernames and passwords do make the rounds, the most common information stolen by malicious actors are the secret access keys and programmatic AWS access key IDs. These sensitive keys are frequently lengthy strings of letters and numbers, and the access they grant might not be immediately obvious to everyone. Users risk inadvertently pushing them to a public code repository, public document, or shared storage space (like an S3 bucket) without realizing it. When hackers get their hands on them, they can use them to access or change resources in the compromised AWS account. Figure 1 shows Credentials stored in publicly accessible data repositories can be stolen and used.

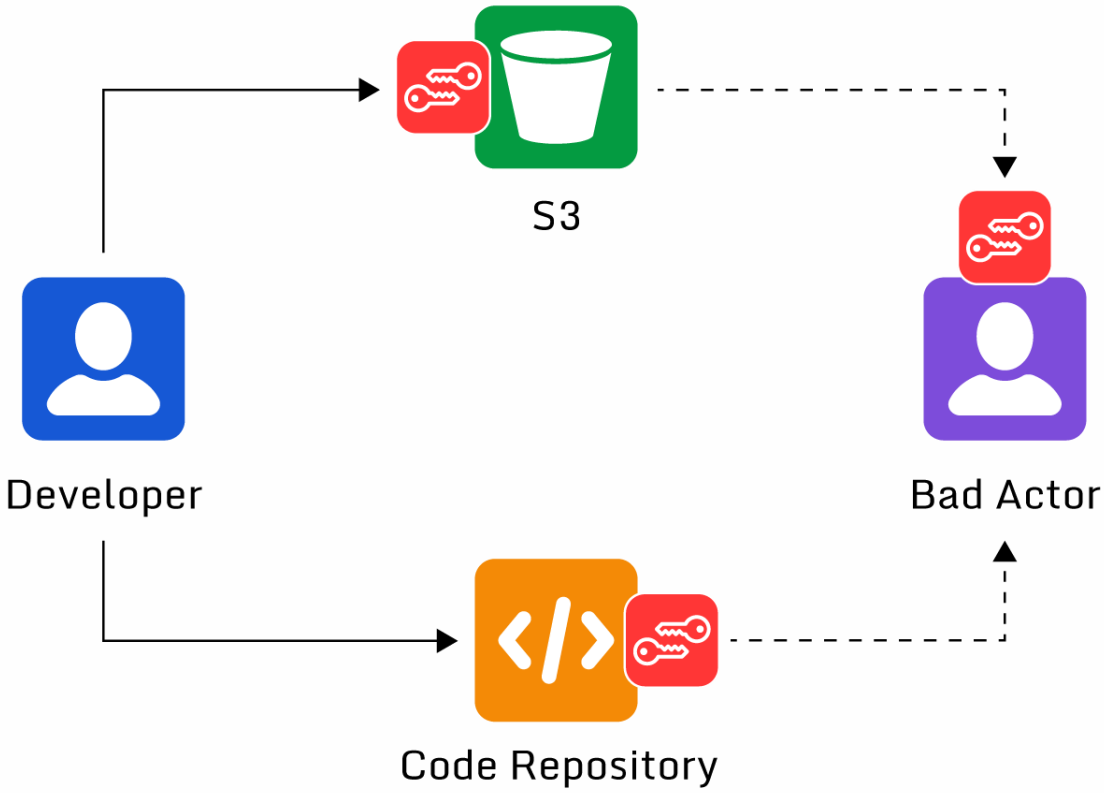

Figure 1: Credentials stored in publicly accessible data repositories can be stolen and used

Fortunately, this AWS security vulnerability has multiple viable solutions.

- Password management methods and strong passwords should be enforced. Password sharing, minimum length requirements, and the use of a secure password management solution are all secure password management practices that organizations should adopt.
- Turn on MFA (multi-factor authentication): This will help, but it won't stop credential leaks in and of itself. Yet, multi-factor authentication does aid in preventing the use of compromised passwords.
- Regularly rotate keys: An attacker may only use sensitive keys for a limited length of time if they are not rotated regularly. This helps keep systems secure and follows the principle of least privilege.
- Use permissive AWS access keys sparingly, unless absolutely necessary (such as when taking IAM responsibilities).
- Make use of tools that actively monitor: To prevent keys from being committed to code repositories or stored in public shared storage, protective monitoring techniques are useful. To keep an eye out for this and other forms of personally identifying information, Amazon Macie can monitor S3 buckets.

AWS Security Risk #3: Data encryption

Data must be encrypted before being sent over a public network like the Internet; this much is obvious. For these kinds of tasks, VPNs and protocols like HTTPS are already standard. Nevertheless, encryption plays an equally important role in private networks. Hackers have stolen millions of records containing client data that is not encrypted. Data encryption would have made it considerably more difficult for unauthorized parties to access the information. Data can be encrypted both while it is in transit across AWS's network and while it is at rest within their services, which helps to reduce this risk. Built-in encryption is available for the majority of AWS services through the AWS Key Management Service (KMS). Customers can generate their own unique key and then import it into the service, making it even more secure. By assigning these keys to certain users or roles, we can make sure that only authorized users and programs may decrypt the data.

AWS Security Risk #4: Insufficient logging

An important part of being observable and having a good security posture is logging well. Logs make it possible to identify threats and analyze attacks after the fact. A lot of companies, regrettably, don't use enough AWS logging policies. CloudTrail, AWS's default logging service, only records management events and deletes them after 90 days. While these records can be useful in certain situations, there are times when it's required to go further back in time to find certain actions. Additional events that aren't logged by default include data access information and logs that reveal suspicious behavior.

When utilizing AWS services, it is important to examine additional logging systems such as S3 access logs, VPC flow logs, and service integration with Amazon CloudWatch. If you don't set up extra logging, you might not be able to find out where a security incident came from and fix it so it doesn't happen again. Therefore, make sure you set up sufficient logging in your AWS account, and then store these logs in S3 for later use in analysis. In addition, each application should have its own set of logging parameters and have the ability to link with a central repository, such as Amazon CloudWatch, when it is built or installed (for example, in an EC2 instance). Last but not least, businesses should be proactive in their alert settings and respond swiftly to any questionable activity.

AWS Security Risk #5: Inadequate monitoring and reporting

In spite of its importance, logging is merely the beginning. For the purpose of threat detection and insight extraction, organizations must analyze log data. In order to address operational concerns before they affect customers, many organizations employ operational monitoring. Weak security monitoring is more common, which is a shame. This means that breaches can be undiscovered for a long time, even months or even years, and that any malevolent action could go unnoticed.

A number of AWS services, including Security Hub, GuardDuty, Inspector, and Macie, are available to assist with security-related log data analysis. The combination of these tools allows for the reporting of threats, analysis of those threats, and the remediation of data and application issues. Figure 2 shows Amazon Macie findings after a scan of S3 buckets.

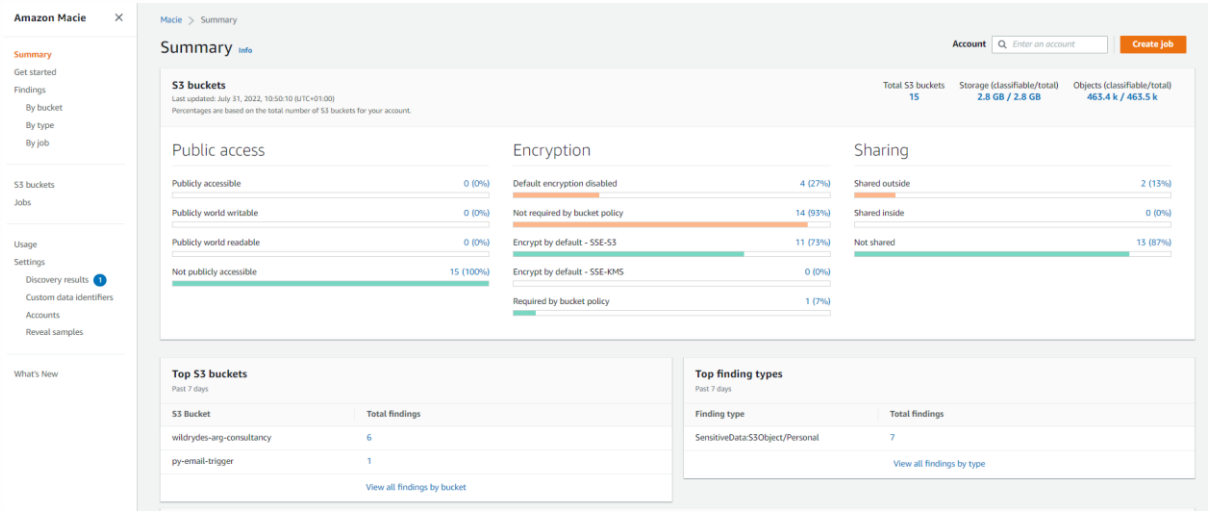

Figure 2: Amazon Macie findings after a scan of S3 buckets

AWS Security Risk #6: No strategy or recovery plans

A cloud-specific security plan is frequently overlooked by organizations. Because cloud security presents unique issues compared to on-premise security, this is a poor decision. Although it does require some expertise and work, it is possible to achieve better IT security in the cloud than on-premises.

It is common practice for public cloud services to be automatically accessible over the internet. There must be measures in place to ensure the security of apps and data kept on AWS. With AWS, you can improve your standard security measures with features like built-in monitoring solutions for operations and protection and the ability to automate problem remediation.

It is also important to have a strategy in place for dealing with various situations. Among the most important things to think about is what to do in the event that a system is compromised. Even worse, what happens if an unauthorized user discloses their credentials?

After an incident has occurred, it is too late to ask these questions. You can limit or avoid data loss and reputational harm by documenting and testing your processes to guarantee rapid remediation as soon as practicable. To aid you in planning and building a strong procedure, AWS offers a Security Incident Response Guide.

AWS Security Risk #7: Shadow IT

The scalability and ease of use of public cloud systems make resource deployment a breeze. As a result, departments or even individual employees can easily use AWS cloud

services to store data, interact internally, and build or deploy applications possibly without a proper security overview or controls.

The public cloud makes high-end IT services available to everyone. Security safeguards can easily be circumvented in the absence of adequate planning and supervision. Cloud management and governance solutions are necessary for gaining insight into and command of deployed resources, in addition to well-defined business policies. To facilitate this governance process, AWS offers tools like Control Tower, Organizations, and Service Catalogue. When it comes to protecting multi-cloud and hybrid cloud settings, security professionals are left to fend for themselves because cloud-native products are designed to work with just one cloud provider. The native tools likewise have little features and functionality, which is understandable given their age. Open-source Cloud Security Posture Management (CSPM) technologies, including Paladin Cloud's Open-Source Community Edition, were born out of this gap. Common vulnerabilities across various cloud providers and data center infrastructure can be easily monitored with this free tool's pre-configured settings. In the event that it identifies a security vulnerability, it performs predetermined corrective measures and provides visualization through an up-to-date user interface.

3.Conclusions

Finally, after much research, analysis, and evaluation, a number of important findings and implications have surfaced. Throughout this chapter, we investigated well-known cloud security frameworks such as the NIST Cloud Security Framework, the CSA STAR, ISO/IEC 27017, COBIT5, and the AWS Well-architected framework. When it comes to safeguarding cloud computing systems, these frameworks provide helpful rules and controls for dealing with important security issues and making sure that data and resources are available, secure, and secret. As far as cloud security frameworks are concerned, the research showed that there are a number of options to address the unique challenges of safeguarding cloud systems. There are advantages and disadvantages to each framework. It becomes apparent by comparing and contrasting multiple frameworks that no one framework can completely satisfy all requirements for every cloud deployment, as each framework has its own set of restrictions and drawbacks. A company's specific needs, regulatory mandates, and comfort level with risk should be carefully considered while deciding on a framework or combination of frameworks. In addition, the study shed light on common problems and vulnerabilities in cloud security. Some instances include poor security measures, insider threats, unauthorized access, APIs that aren't safe, and data breaches.

References

[1] Marston, S.; Li, Z.; Bandyopadhyay, S.; Zhang, J.; Ghalsasi, A. Cloud computing—The business perspective. Decis. Support Syst. **2011**, 51, 176–189. [**Google Scholar**]
[2] Weinhardt, C.; Anandasivam, A.; Blau, B.; Borissov, N.; Meinl, T. Cloud Computing—A Classification, Business Models, and Research Directions. Bus. Inf. Syst. Eng. **2009**, 1, 391–399. [**Google Scholar**]
[3] Bhushan, K.; Gupta, B.B. Security challenges in cloud computing: State-of-art. Int. J. Big Data Intell. **2017**, 4, 81–107. [**Google Scholar**]
[4] Di Giulio, C.; Sprabery, R.; Kamhoua, C.; Kwiat, K.; Campbell, R.H.; Bashir, M.N. Cloud Standards in Comparison: Are New Security Frameworks Improving Cloud Security? IEEE: Honololu, HI, USA, 2017. [**Google Scholar**]
[5] Armbrust, M.; Fox, A.; Griffith, R.; Joseph, A.D.; Katz, R.; Konwinski, A.; Lee, G.; Patterson, D.; Rabkin, A.; Stoica, I.; et al. A view of cloud computing. Commun. ACM **2010**, 53, 50–58. [**Google Scholar**]
[6] Amara, N.; Huang, Z.; Awais, A. Cloud Computing Security Threats and Attacks with Their Mitigation Techniques. In Proceedings of the 2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), Nanjing, China, 12–14 October 2017. [**Google Scholar**]
[7] Mohanan, S.; Sridhar, N.; Bhatia, S. Comparative Analysis of Various Cloud Security Frameworks. In Proceedings of the 6th International Congress on Information and Communication Technology, London, UK, 25–26 February 2019. [**Google Scholar**]
[8] Popa, D.; Cremene, M.; Borda, M.; Boudaoud, K. A security framework for mobile cloud applications. In Proceedings of the 11th RoEduNet International Conference, Sinaia, Romania, 17–19 January 2013. [**Google Scholar**]
[9] Ukil, A.; Jana, D.; Das, A. A Security Framework in Cloud Computing Infrastructure. Int. J. Netw. Secur. Its Appl. **2013**, 5, 11–24. [**Google Scholar**] [**CrossRef**]
[10] Hashizume, K.; Rosado, D.G.; Fernández-Medina, E.; Fernandez, E.B. An analysis of security issues for cloud computing. J. Internet Serv. Appl. **2013**, 4, 1–13. [**Google Scholar**] [**CrossRef**]
[11] Grobauer, B.; Walloschek, T.; Stocker, E. Understanding Cloud Computing Vulnerabilities; IEEE: Piscataway, NJ, USA, 2011. [**Google Scholar**]
[12] Rodero-Merino, L.; Vaquero, L.M.; Caron, E.; Muresan, A.; Desprez, F. Building Safe PaaS Clouds: A Survey on Security in Multitenant Software Platforms. Comput. Secur. **2012**, 31, 96–108. [**Google Scholar**]
[13] Tsochev, G.R.; Trifonov, R.I. Cloud computing security requirements: A Review. IOP Conf. Ser. Mater. Sci. Eng. **2022**, 1216, 012001.