A Survey on AWS Cloud Computing Security Challenges & Solutions

Shilpi Mishra
Department of CSE
Arya College of Engineering and Research Centre,
Jaipur, Rajasthan, India
mishra.shilpi20@gmail.com

Dr. Manish Kumar
Department of CSE
Arya Institute of Engineering & Technology,
Jaipur, Rajasthan, India
manishkrmukhija82@gmail.com

Niharika Singh
Department of CSE
Arya College of Engineering and Research Centre,
Jaipur, Rajasthan, India
0511niharikasingh2000@gmail.com

Stuti Dwivedi
Department of CSE
Arya College of Engineering and Research Centre,
Jaipur, Rajasthan, India
dwivedistuti2014@gmail.com

2022 6th International Conference on Intelligent Computing and Control Systems (ICICCS) | 978-1-6654-1035-9/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICICCS53718.2022.9788254

Abstract: **Amazon offers a comprehensive range of IT solutions to let businesses construct their private virtual clouds and maintain total control over their infrastructure. It is possible to use Amazon Web Services for both businesses and IT projects. Security professionals are drawn to the cloud because of its cost savings and efficiency, but it also poses numerous security and compliance issues. EC2 instances, which claim to make cloud computing safe for highly regulated companies, have been introduced as part of Amazon Web Services' (AWS) effort to relieve business security and compliance issues with cloud computing. Cloud computing has its drawbacks; however, these drawbacks also provide an opportunity to study a variety of cloud computing-related topics. The security and privacy of data stored and processed on cloud service providers' servers is a major concern. Several studies on cloud computing security and privacy are reviewed in this study. A better knowledge of cloud computing's security problems has been shown and the techniques and solutions which have been used by the cloud service sector have been highlighted in this article. The objective of this report is to shed light on immerging cloud services market and the different upcoming challenges like network issues.**

Keywords: **Amazon Web Services, Cloud Computing; Storage Security; Cloud Storage; Data Privacy; Cloud Security.**

I. Introduction

AWS (Amazon Web Services) provides a highly available and reliable cloud computing platform with scalability, allowing users to create a broad variety of applications. AWS places a high priority on ensuring the security, integrity, and availability of its customers' systems and data. Maintaining customer trust and confidence is also a priority.

Companies may utilize AWS to develop cost-effectively applications and services that are flexible, scalable, and reliable by providing computational power, storage, content delivery, and other features. With Amazon Web Services (AWS) self-service, customers may take control of their internal processes while still being ready to respond to external requests as they arise.

'AWS' stands for Amazon Web Services, which is a set of online cloud computing [1] services provided via the internet by Amazon's website. Amazon S3 and Amazon EC2 are two of the most often utilized services here. According to the service's pitch, it is easier, cheaper, and quicker than setting up a physical [2-3] server farm to provide enormous amounts of processing power.

There are numerous Availability Zones [4] in each region, each of which is a separate data center where AWS services are offered. To avoid the spread of outages across Zones and availability Zones, they have been segregated. It's possible to set certain services (e.g. Dynamo DB, S3) to be replicated across Availability Zones to prevent service outages.

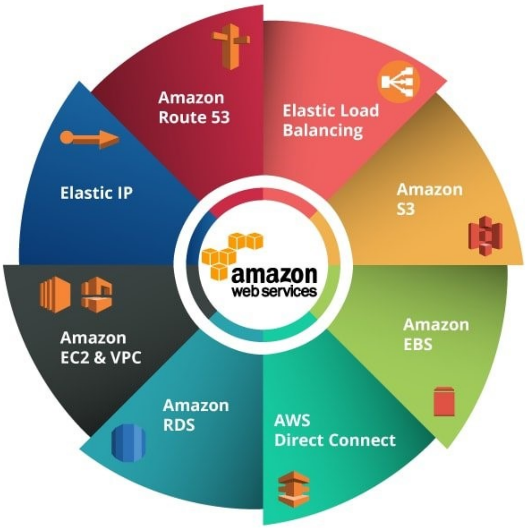

Fig. 1: Architecture of AWS. Source: AWS Tutorial For Beginners & Experts: Learn In 3 Days - ACTE

II. Services Of AWS

Templates from Amazon services such as VPC, EC2, Elastic Beanstalk, and others may be included in the creation of a cloud with a single click using the cloud formation feature. An application and IT infrastructure can be replicated with a few clicks.

To accommodate enormous simultaneous demand, a user may employ a content delivery platform like video and music to distribute extensively consumed digital products through Cloud Front.

You may gather, evaluate, and analyze metrics linked to cloud resources using Cloud Watch. As your virtual infrastructure becomes more complex, it is quite beneficial.

Known as "NOSQL" systems because they don't utilize SQL as their primary query language, a new class of database systems has arisen in the last few years. Large data sets that can grow horizontally without any human involvement are quite popular.

It is possible to create the backbone of a virtual network using Amazon's Elastic Compute Cloud (EC2).

There are occasions when a developer has to temporarily store a big quantity of data without committing it to a database. In applications with a large number of transactions, this is a common occurrence. The Elastic cache service[5] from Amazon is ideal for storing massive, yet transitory, data sets in in-memory storage.

Elastic Beanstalk [6] is a programming framework that may be used to manage all of the numerous services that are required.

To slice and dice the different data sets one has saved in any of the Amazon data storage services, one may use Amazon Elastic Map Reduce (EMR).

A framework for managing users who will have access to your Amazon services, IAM (Identity and Access Management) is provided by Amazon. For instance, if you wish to provide one user administrative access to Dynamo DB data and another user access to an EC2[6] server instance, you'll need to set up both of those instances using EC2.

If you aren't quite ready to embark on the NoSQL bandwagon, the Amazon RDS should feel at home. SQL query language and tools are used to build a scalable database system, which should be known to any database administrator.

This is Amazon's scalable DNS system, Route 53. Instead of utilizing your domain registrar's tools to create DNS names[7] for computers, you must use Route 53 to keep track of your DNS zones and subzones.

This service, Simple Email Service (SES), is ideal if you anticipate sending a large number of emails. It's far easier to utilize this service than to set up your outgoing email servers.

Administrators and developers may use SNS to send out SMS and email notifications. The Amazon cloud[8] provides an easy approach to incorporating alerts without having to worry about the specifics of multiple SMS and email systems and gateways.

SQS - In certain cases, separate applications (or application components) need to communicate with one other. A message queuing system is a great approach to do this.

S3 - The Simple Storage Service you might think of this as your Drop-Box or other Internet storage service. Your company's security rules will be satisfied with this method of storing sensitive data.

It's fairly uncommon for highly distributed systems[7] to break down enormous issues into smaller, more manageable chunks of labor, known as "tasks." Schedule, manage and set up tasks relevant to your huge distributed process using SWF service application components.

To use Amazon's Storage Gateway service, you'll need a PC and an Internet connection, as well as a physical device in your infrastructure. Using it for disaster recovery and backup archiving is a no-brainer.

Amazon EC2's Virtual Private Cloud (VPC) enables you to create a private network of Amazon EC2 server instances.

Fig. 2: Different AWS services. Source: Amazoncloudlinux.com

III. General Security Measures

AWS incorporates security into its services in line with industry standards and provides documentation on how to make use of the security tools. When creating an application environment, customers should make use of AWS security capabilities and best practices. AWS places a high priority on protecting the privacy, integrity, and availability of its customers' data, as well as retaining their trust and confidence. Following are some of AWS's methods for protecting the cloud infrastructure:

A. Credentials and Certifications

Amazon Web Services (AWS) has successfully passed numerous SAS70 Type II assessments and currently releases a Service Organization Controls 1 (SOC 1) report, which is issued under both SSAE 16 and ISAE 3402. Along with its

ISO 27001 accreditation, AWS has been verified by the Payment Card Industry (PCI) as a Level 1 service provider for data security (DSS). Regarding public sector certifications, AWS has been granted FISMA Moderate permission by US GSA and has been designated as the platform for applications with ATOs under DIACAP.

B. Physical Security

For many years, Amazon has designed and built large-scale data centers. The AWS infrastructure is housed in data centers owned and operated by Amazon across the globe. It is only individuals inside Amazon who have a valid business need to know the location of Amazon's data centers who are given this information. To prevent illegal entry, the data centers are physically guarded by several methods.

C. Secure Services

Services that are safe and reliable. The AWS cloud is designed to be safe at every level. Unauthorized access or use is prevented while still providing clients with the degree of freedom they expect.

D. Data Privacy

In today's world, the security of the data is very needed for those different techniques. Encryption and hiding are used [9-12]. Personal and commercial data may be encrypted [13-14] in the AWS cloud and backup and redundancy processes for services can be published so that clients can secure their data and keep their applications operational.

IV. Infrastructure Security Of AWS

As a result of shifting IT infrastructure to Amazon Web Services (AWS), a new paradigm of shared accountability emerges between the two parties. Amazon Web Services (AWS) may decrease the operational load by managing and controlling all aspects of a service's infrastructure, from its host operating system and virtualization layer to its physical security. Additionally, users are in charge of maintaining and configuring the AWS-provided security group firewall, as well as the guest OS system (with any necessary updates and security patches). If you're concerned about security and/or compliance, you may employ technologies like host-based firewalls, intrusion detection, or encryption to help.

V. BEST SECURITY PRACTICES

Everyone is worried about safety in a multi-tenant setting. Every layer of the cloud application architecture should be protected by security measures. The service provider, of course, takes care of physical security, which is still another advantage of utilizing the cloud. The user must ensure network and application-level security. Securing cloud applications on Amazon Web Services (AWS) is addressed in detail in this section. Basic security should be implemented first using the tools and features listed above, and then further best practices should be implemented using conventional ways.

TABLE 1: ADVANTAGES AND DISADVANTAGES OF AWS[21]

Advantages	Disadvantages
User-friendly	Lack of Experts
Scalable and Elastic	Price Variations
Cost-effective	General issues
Secure	Limitations

A. Protect Transit Data

Encrypt the server instance if the data is secret or critical. VeriSign or Entrust are examples of third-party certification authorities that must be used. To encrypt data in both routes, the shared session key generated from the server's public key is used to verify its authenticity to the browser. Businesses should use network security protocols such as gateways and network management to safeguard data in transit. These will aid in the protection of networks used to transfer data against virus assaults or intrusions. Avoid using reactive security to safeguard your data. Rather than that, discover at-risk information and take proactive efforts to safeguard it. It is critical for businesses to incorporate information security measures in their cyber security choices, which notify users or encrypt sensitive data. The business should establish procedures for categorizing and evaluating all data, regardless of its location. Policies are required to guarantee that proper safeguards are in place both during the data's storage and during its access.

B. Protect Data Stored

Individual files should be encrypted before being uploaded to the cloud if users are worried about sensitive or confidential data being stored there. For example, before saving the data as Amazon S3 objects, it may be encrypted using any open source or commercial PGP-based tools, and it can be decrypted after download. Building HIPAA-Compatible Applications 20, which must hold Protected Health Information, typically necessitates this approach (PHI). File encryption on Amazon EC2 is dependent on the operating system being used. Encrypting data while it's in transit or at rest is a difficult task no matter what operating system or technology a user uses. For example, if a user loses their password, they'll lose all of their data permanently. As a result, it is essential that you thoroughly research the key management capabilities of any goods you are considering purchasing.

C. Protect Credentials of AWS

Access keys and X.509 certificates are two different forms of security credentials provided by Amazon Web Services (AWS). Access key ID and secret access key are two elements of the AWS access key. To authenticate a request made over the REST or Query APIs, the user must use his or her secret access key to compute a signature. Sending queries via HTTPS protects against in-flight tampering.

D. Manage Multiple Users

As part of AWS IAM, users may establish several Users and control the rights for each of these Users in their AWS account. Using AWS Services, a User has a unique set of credentials that may be used to log in. This removes the need to provide user credentials and makes it simple to grant or deny a user's access. Security best practices such as least privilege may be implemented by issuing unique credentials to every user in an AWS account and only allowing the authority to access the AWS Services and resources necessary for each user to accomplish their job.

V. Conclusion

Cloud computing has experienced explosive growth in recent years, notably for commercial online applications. The on-demand, pay-as-you-go concept allows for a more versatile and valuable way of gaining access to computing capacity.Elastic Compute from Amazon Organizations is rapidly adopting cloud services like IBM's Smart Cloud to manage their IT infrastructures and the online services they provide. Computing power may now be acquired with relative ease. Using cloud-based apps, a user may simply purchase the product online and start and shut down virtual images. Sharing and creating virtual photos with other users is one of the most popular features of cloud-based popular services.

The rise of cloud computing has made it possible to research all aspects of cloud computing. Cloud computing has five main characteristics, three service models, and four ways to put it in place. Research into safe cloud storage is complicated by the fact that users' data may be kept in multiple places for either redundancy or because the service is provided by a chain of service providers. We looked at the security measures taken by the biggest cloud service provider, Amazon web services AWS. We looked at their infrastructure security and the security best practices that AWS uses.

References

[1] Foster, I., Zhao, Y., Raicu, I., Lu, S, “ Cloud computing and grid computing 360-degree compared”, Grid Computing Environments Workshop, GCE ’08, p. 1-10, 2008.

[2] Takabi, H., Joshi, J., Ahn, G.J., “Security and privacy challenges in cloud computing environments. Security Privacy”, IEEE, vol. 8, issue. 6, pp. 24-31, 2010.

[3] Himanshu Arora, Monika Mehra, Pramod Sharma, Jaisika Kumawat, Jyoti Jangid, "Security Issues On Cloud Computing", Design Engineering, pp. 2254-2261, 2021.

[4] Li, M., Yu, S., Ren, K., Lou, W., Hou, Y., “Toward privacy-assured and searchable cloud data storage services Network”, IEEE, Vol. 27, issue. 4, pp. 56-62, 2013.

[5] Bracci, Fabio, Antonio Corradi, and Luca Foschini, "Database security management for healthcare SaaS in the Amazon AWS Cloud." In 2012 IEEE Symposium on Computers and Communications (ISCC), pp. 000812-000819, 2012.

[6] Amazon web services team, creating hipaa-compliant medical data applications with aws. http://media.amazonwebservices.com/AWSH $IPAA$W $hitepaper$ F$inal.pdf$; 2009 − 04 − 01.

[7] Amazon web services: Overview of security processes. http://aws.amazon.com/security/; June 2013.

[8] Naresh Kumar, M., Sujatha, P., Kalva, V., Nagori, R., Katukojwala, A., Kumar, M, “Mitigating economic denial of sustainability (edos) in cloud computing using in-cloud scrubber service”, Computational Intelligence and Communication Networks (CICN), 2012 Fourth International Conference on. 2012, p. 535-539. 2012.

[9] G. K. Soni, A. Rawat, S. Jain and S. K. Sharma, "A Pixel-Based Digital Medical Images Protection Using Genetic Algorithm with LSB Watermark Technique", Springer Smart Systems and IoT: Innovations in Computing, pp. 483-492, 2020.

[10] Himanshu Arora, Manish Kumar and Sanjay Tiwari, "Improve Image Security in Combination Method of LSB Stenography and RSA Encryption Algorithm", International Journal of Advanced Science and Technology, vol. 29, no. 8, pp. 6167-6177, 2020.

[11] G.K. Soni, H. Aroa, B. Jain, "A Novel Image Encryption Technique Using Arnold Transform and Asymmetric RSA Algorithm", Springer International Conference on Artificial Intelligence: Advances and Applications 2019 Algorithm for Intelligence System, pp. 83-90, 2020.

[12] H. Arora, G. K. Soni, R. K. Kushwaha and P. Prasoon, "Digital Image Security Based on the Hybrid Model of Image Hiding and Encryption," 2021 6th International Conference on Communication and Electronics Systems (ICCES), pp. 1153-1157, 2021.

[13] S. Mishra, D. Singh, D. Pant and A. Rawat, "Secure Data Communication Using Information Hiding and Encryption Algorithms," IEEE 2022 Second International Conference on Artificial Intelligence and Smart Energy (ICAIS), pp. 1448-1452, 2022.

[14] Manish Kumar, Dr. Sunil Kumar, Dr. Harish Nagar, "Enhanced Text and Image Security Using Combination of DCT Steganography, XOR Embedding and Arnold Transform", Design Engineering, issue-3, page no- 732 – 739, 2021.

[15] Swati Bhargava, Manish Mukhija, "Hide Image And Text Using Lsb, Dwt And Rsa Based On Image Steganography", ICTACT Journal On Image And Video Processing, Volume: 09, Issue: 03, Pp-1940-1946, February 2019.

[16] S. Matted, G. Shankar and B.B. Jain, "Enhanced Image Security Using Stenography and Cryptography", Springer Computer Networks and Inventive Communication Technologies, vol. 58, 2021.

[17] Harish Nagar, Manish Kumar and Sunil Kumar, "Comparative Analysis of Different Steganography Technique for image or Data Security", International Journal of Advanced Science & Technology (IJAST), vol. 29, no. 4, 2020.

[18] Dr.Sunil Kumar and Dr. Harish Nagar Manish Kumar, "Comparative Analysis of Different Cryptography Technique for image or Data Security", Wesleyan Journal of Research, vol-13, issue-69, pp. 9-20, 2021.

[19] M. Kumar, A. Soni, A. R. S. Shekhawat and A. Rawat, "Enhanced Digital Image and Text Data Security Using Hybrid Model of LSB Steganography and AES Cryptography Technique," IEEE 2022 Second International Conference on Artificial Intelligence and Smart Energy, pp. 1453-1457, 2022.

[20] Jackson, Keith R., et al. "Performance analysis of high performance computing applications on the amazon web services cloud." 2010 IEEE second international conference on cloud computing technology and science. IEEE, 2010.

[21] Top 7 Benefits of AWS - Disadvantages of Amazon Web Services (intellipaat.com)