Designing Secure Cloud Architecture in AWS to Mitigate Data Breach Risks

Upesh kumar Rapolu

Houston, USA
Upeshkumar.rapolu@gmail.com

Abstract

This research paper has provided a vivid explanation of how to construct a secure cloud architecture in AWS to mitigate the high chances of data breach risks. This secure cloud architecture has been paramount as it has supported a robust platform for hosting applications and underlying the overview in an ethical sense. This has been curated to support more advanced security measures leading to the protection of sensitive data. Furthermore, the research has also navigated with steps which are used to minimise the chances of data breach risks such as augmentation of data loss prevention tools, adequate training to the employees, conducting regular security audits and fostering continuous security testing which has helped to synchronise to lower the risks that are intertwined with data breaches.

Keywords: AWS, Data Breach, Cloud Architecture, Cloud Security, Cybersecurity

I. INTRODUCTION

The following research paper will provide a nuanced understanding of designing a secure cloud architecture in Amazon Web Service also abbreviated as “AWS”. At the same time, it often uses robust data encryption that will enable service-side encryption (SSE) by the usage of AWS Key Management Service. However, this will set the stage by protecting the transmitted data among AWS and clients[1]. This will result in financial losses and reputational damage for the organisations. Furthermore, in order to minimise these, creating a secure cloud architecture will aid in lowering the chances of data breaches. Thus, the architecture will harness the best practices and security tools used by AWS to control the amount of data breaches.

Figure 1: Amazon Web Service

II. DESCRIBING AN OVERVIEW OF SECURITY IN AWS

This section describes the intricate role and function of security in Amazon Web Service in an explicit manner. The clients stand to be vital for protecting and securing their applications. This helps to limit the security services in AWS which ultimately impacts on elevating the overall security. It encompasses several elements such as Encryption, Identity and Access Management, DDoS Protection, Network Security Controls and Monitoring and Logging[2]. The first element is encryption poses an important stage that is used to protect the transmitted data within AWS services and clients by the utilisation of Secure Sockets Layer (SSL) and Transport Layer Security (TLS). This also harnesses Amazon Web Service Certificate Manager for the management of SSL or TLS certificates. The second element which is Identity and Access Management is also considered to be an essential tool used by AWS. This is because it caters access to the cloud resources and determines necessary actions which need to be taken to lower the percentage of data breaches[3]. The third element involves the implementation of DDoS Protection which uses services such as AWS Shield with content-delivery network services like Amazon CloudFront. This aids in shielding the application and databases from DDoS attacks. The fourth element which is Network Security Controls has the probability to implement firewalls followed by intrusion and prevention systems (IDPS) and Virtual Private Networks thereby identifying the risks at the initial stages and applying necessary actions to mitigate those risks ethically.

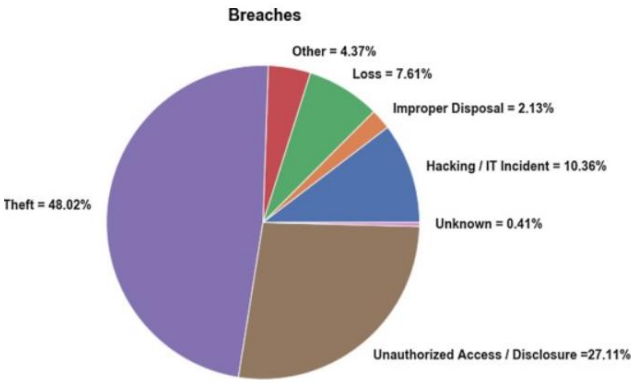

Figure 2: Distribution of Breaches Applied to Human Factors

III. ILLUSTRATING A SECURE CLOUD ARCHITECTURE IN AWS

The following section delves deep into portraying a secure cloud architecture in AWS which plays a crucial character and is termed to be of immense relevance. It contains several components that are used to define the design principles. Firstly, the application of a network security design tends to separate public-facing web servers from application servers and database layers[4]. It is used to host web servers with the help of a private subnet. This is then designated by the application of database servers. Secondly, the architecture incorporates access controls like IAM roles for EC2 instances to allow permission to temporary access to AWS resources. Catering with a centralised IAM policy proves to strengthen the security policies in the organisations. This is attained by the utilisation of an elastic load balancer over the internet. Additionally, organising data classification assessments needs extra protection for the identification of confidential information[5]. Thus, it makes sure that all the data is encrypted at rest by Amazon S3, EBS and Encryption and also by integrating HTTPS in case of transit. The fourth component which is application security provides protected coding practices to construct resilient applications. This consists of processes such as

penetration testing and identification of security issues. The fifth component, incident response planning plays a crucial character in developing an incident response plan boundering the necessary roles and responsibilities. This poses an essential for the establishment of communication protocols whenever there is a chance of a data breach. Thus, to overcome this, drill needs to be performed regularly to stay aware and ready to tackle this kind of breach.

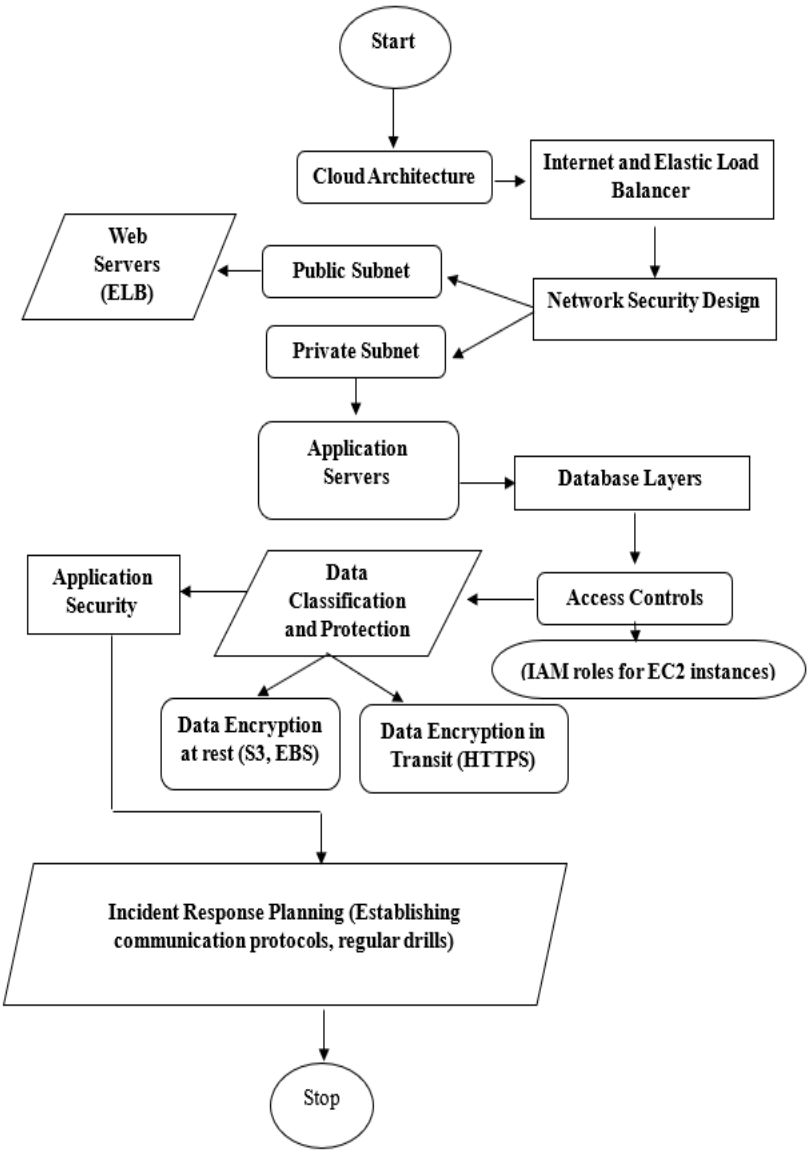

Figure 3: Demonstrating Secure Cloud Architecture in AWS

IV. MINIMISING THE RISK ASSOCIATED WITH DATA BREACHES

This section illustrates the steps required to minimise the risks associated with data breaches. These steps are explained below.

Augmentation of data loss prevention tools (DLP): Augmentation of data loss prevention tools is used to amalgamate processes and technology for mitigating data breaches and loss of confidential information[6].

Providing Adequate training to the employees: It is necessary to supplement with adequate training to the employees by conducting comprehensive training programs for preventing data breaches which are caused by humans.

Conducting regular security audits: Scheduling audits dailyfuels up the security postures of the cloud architecture and identifies any sort of misconfiguration and loopholes[7].

Fostering with continuous security testing: This section fosters continuous security testing that integrates into either the CI or CD pipeline with the segregation of tools such as AWS Inspector therefore automating security assessments of applications.

Figure 4: Highlighting the steps required to minimise the risk associated with data breaches

V. CONCLUSION

The research paper has concluded that the organisation has been heavily dependent on cloud services for safeguarding the data inside the cloud environments. It has made AWS cultivate robust security features which has aided in following the best practices. This has been achieved by the construction of an effective cloud architecture for mitigating data breach risks. As a result, this has allowed to fostering of complete cloud workload protection for safeguarding the application along with processes and resources thereby supporting each workload. Thus, this has proved to be advantageous in lowering the possibility of data breach risks.

Abbreviations and Acronyms

- AWS- Amazon Web Service
- SSL- Secure Sockets Layer
- TLS- Transport Layer Security
- DDoS- Distributed Denial of Service
- IAM- Identity and Access Management
- IDPS- Intrusion Detection and Prevention Systems
- CDN- Content Delivery Network
- DLP- Data Loss Prevention
- CI- Continuous Integration
- CD- Continuous Deployment
- EC2- Elastic Compute Cloud
- ELB- Elastic Load Balancer
- S3- Simple Storage Service
- EBS- Elastic Block Store

- HTTPS- Hypertext Transfer Protocol Secure

Units

- Here, the security metrics are measured in bytes for the transmission of the data.

Equations

- Encryption Strength: Strength= [$\log_2(K)$], where, K is the key length in bytes
- DDoS Detection: Effective Bandwidth= [Total Bandwidth - Attacker's Bandwidth]
- Risk Reduction Rate= [(Number of Breaches After Implementation / Number of Breaches Before Implementation) X 100]
- Vulnerability Detection Rate = [(Vulnerabilities Detected / Total number of vulnerabilities) X 100]
- Balancing load when using ELB: Load per Instance = (Total Incoming Request / Number of Instances)

ACKNOWLEDGEMENT

I sincerely acknowledge the guidance and support of all contributors whose valuable insights and encouragement helped me to complete this research project. I would also like to thank my professors for lending their precious time to the accomplishment of my research project successfully.

REFERENCES

[1] B. Ringlein, F. Abel, A. Ditter, B. Weiss, C. Hagleitner, and D. Fey, "System Architecture for Network-Attached FPGAs in the Cloud using Partial Reconfiguration," 2019 29th International Conference on Field Programmable Logic and Applications (FPL), pp. 293–300, Sep. 2019.

[2] J. B. Almeida et al., "A Machine-Checked Proof of Security for AWS Key Management Service," Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, Nov.2019.

[3] J. Backes et al., "Reachability Analysis for AWS-Based Networks," Computer Aided Verification, pp.231–241, 2019.

[4] J.-Y. Yu, S. Korea, and Y.-G. Kim, "Analysis of IoT Platform Security: A Survey," 2019.

[5] M. Gupta, J. Benson, F. Patwa, and R. Sandhu, "Dynamic Groups and Attribute-Based Access Control for Next-Generation Smart Cars," Proceedings of the Ninth ACM Conference on Data and Application Security and Privacy, Mar.2019.

[6] S. Mukherjee, "Benefits of AWS in Modern Cloud," SSRN Electronic Journal, 2019.

[7] S. Singh, I.-H. Ra, W. Meng, M. Kaur, and G. H. Cho, "SH-BlockCC: A secure and efficient Internet of things smart home architecture based on cloud computing and blockchain technology," International Journal of Distributed Sensor Networks, vol. 15, no. 4, p. 155014771984415, Apr. 2019.