CSCI 5409

ADVANCE TOPICS IN CLOUD COMPUTING

DALHOUSIE UNIVERSITY

FACULTY OF COMPUTER SCIENCE

TICKET BOOKING SYSTEM

Security Consideration Critical Analysis and Response

GROUP – 8 ALPHA TEAM

DHRUV DOSHI	**Dh722257@dal.ca**
KISHAN KAHODARIYA	**Ks805556@dal.ca**
VISHAL RAKESH JAISWAL	**Vs98999@dal.ca**

As we have reached the business end of the development of the project, here in this document we are answering the security-related questions regarding the architecture and the design of the project.

HOW DOES THE APPLICATION ARCHITECTURE KEEP DATA SECURE AT ALL THE LAYERS?

The answer to this question is with the centralized database system. Here in the referred architecture, we are using a single encrypted database that stores all the data collected from the users alongside the hash generated by the algorithm to uniquely identify the entry of the database.

Making more consideration on the security aspect, every element in the application which requires the data need to go to the database layer to ask for access to the data, once they get permission to access the data, to use the information, they need to go through the decryption process. To have minimum exposure to the data the architecture we are using tries to minimize the access to the database by intermediatory saving the data in the S3 bucket till the information is processed once the data is ready to be stored then and only then is saved securely in the database.

The algorithms used in development are backed by SHA-256 encryption which is industry standard and to decrypt them without a relevant key is not viable.

VULNERABILITY OF THE DATA:

The data would be most vulnerable in the stage when getting the information from the client-side to the backend server page, this is the portion in which unauthorized access of information could take place, to resolve the issue we are targeting to send the data in the way that it is somewhat encrypted. As encrypting in SHA256 level on this data does not make any sense. To get more security we are saving the intermediatory information in a buffer like S3 and then after the process, we are transferring the data to the main database.

Alongside that AWS provides IAM and Cognito which would be used to check the user access and the authentication services, these services come up with security, Identify and compliance backed up by AWS.

To run the most advanced security check we will provide a provision in the documentation on how automated compliance check via AWS security hub should be triggered to maintain the zero-loophole system.

SECURITY MECHANISM USED TO OBTAIN UTMOST SECURITY:

As explained before that we are giving the provision for multiple cloud services to run automated compliance checks to find the vulnerability within the cloud system, alongside that the encryption constraints would also be maintained throughout the application.

AWS services are used to make the data secure.

[1]. **AWS Cognito:** Configuration compliance monitoring is a part of the AWS Cognito package which deals with the resource configuration alignment with the internal dependencies and the packages and compares it with the industry guidelines and the AWS recommendation for the same.

[2]. **Controlled S3 Public Access:** By blocking the public access to the S3 bucket we could narrow down the information breach from the cloud service. As the AWS platform states, "*Block Public Access is a good second layer of protection to ensure you don't' inadvertently grant broader access to objects than intended."[4]*

[3]. **Security assessments:** As mentioned before with the help of documentation there would be a provision that would guide the security assessment at a specific time. This could be done using AWS Security Hub or Amazon Inspector.

REFERENCE:

[1]. “Learn and use 13 AWS security tools to implement SEC recommended protection of stored customer data in the cloud | Amazon Web Services,” *Amazon Web Services*, 16-Jul-2020. [Online]. Available: https://aws.amazon.com/blogs/security/learn-and-use-13-aws-security-tools-to-implement-sec-recommended-protection-stored-customer-data-cloud/. [Accessed: 21-Nov-2021]

[2]. “Security information and event management | AWS Marketplace,” *Amazon.com*, 2012. [Online]. Available: https://aws.amazon.com/marketplace/solutions/security/siem. [Accessed: 21-Nov-2021]

[3]. “Data Privacy - Amazon Web Services (AWS),” *Amazon Web Services, Inc.*, 2021. [Online]. Available: https://aws.amazon.com/compliance/data-privacy-faq/. [Accessed: 21-Nov-2021]

[4]. “Security, Identity, and Compliance - Overview of Amazon Web Services,” *Amazon.com*, 2021. [Online]. Available: https://docs.aws.amazon.com/whitepapers/latest/aws-overview/security-services.html. [Accessed: 21-Nov-2021]

[5]. “Cloud Compliance - Amazon Web Services (AWS),” *Amazon Web Services, Inc.*, 2021. [Online]. Available: https://aws.amazon.com/compliance/. [Accessed: 21-Nov-2021]

[6]. “Security and Compliance - Overview of Amazon Web Services,” *Amazon.com*, 2021. [Online]. Available: https://docs.aws.amazon.com/whitepapers/latest/aws-overview/security-and-compliance.html. [Accessed: 21-Nov-2021]

[7]. Amazon Web Services, “What is AWS Security?” *YouTube*. 19-Jun-2020 [Online]. Available: https://www.youtube.com/watch?v=_2HFqANE4gw. [Accessed: 21-Nov-2021]

[8]. “Cloud Security Resources - Amazon Web Services (AWS),” *Amazon Web Services, Inc.*, 2019. [Online]. Available: https://aws.amazon.com/security/security-learning/?cards-top.sort-by=item.additionalFields.sortDate&cards-top.sort-order=desc&awsf.Types=*all. [Accessed: 21-Nov-2021]

[9]. “FAQ,” *Netwrix.com*, 2020. [Online]. Available: https://blog.netwrix.com/2020/07/02/cloud-data-security/. [Accessed: 21-Nov-2021]