Secured Data Storage in Google Cloud

S.SABARI VASAN*1, I.GOLDA SELIA*2

(1)M.Tech student in Computer Science and Engineering,

(2)Assistant professor in Information Technology,

Dr. MGR Educational & Research Institute University, Chennai, TamilNadu, India.

Abstract: **Cloud Computing is an emerging technology in today's computer revolution. It has various benefits such as resource sharing, easy to use, highly accessible, and pay per usage, though there are some drawbacks, one of them being security. It makes the users a fear in fully accessing or using the cloud computing services. It is the responsibility of the cloud service provider (CSP) to provide security to the data that is to be stored in an unsecured location on internet. In this paper, it is proposed to encrypt the data to be stored on the cloud.**

Keywords: **cloud computing, cloud security, data security, Google cloud.**

I. Introduction

The revolution of computing leads to cloud computing with these offerings such as Bare Operating System, Web or Portal Infrastructure, Web Services, Database Services, Customizable Application Service which has several benefits such as highly scalable, highly available, dynamically allocate resources, performance, low cost (pay only for the resources that is used). With these features, the security for data that is to be stored on the cloud is a drawback. The cloud service provider provides authentication and some security to its services [1] although it will also have threats, there is a need to protect the data that is to be stored in the cloud.

The cloud service provider has provided authentication and security methods but there are security loop holes in it [2], such as Insecure Interfaces and APIs, malicious insiders, Data Loss or Leakage, Account or Service Hijacking. There is a possibility of data stored on the cloud to be vulnerable. To overcome this data security issue the user can encrypt the data and store it on the cloud.

In this paper, the data security for the cloud is implemented using the Google Cloud SQL [3] and Advanced Encryption Standard (AES) [4]. The Google Cloud SQL is a web service that allows users to create, configure, and use relational databases that resides in Google's cloud. The users are allowed to fully-manage the services that maintain, manage, and administer their databases, and allow the user to focus on their applications and services.

The Advanced Encryption Standard (AES) is a specification for the encryption of electronic data. AES is based on a design principle known as a substitution-permutation network.

Outline of this paper:

The remainder of this paper is organized as follows. Section 2 introduces the basics and features of Google Cloud SQL, Advanced Encryption Standard and Google AppEngine. Section 3 elaborates on the process of data encryption and decryption to the data that is to be stored in the database. Section 4 summarizes the paper.

II. Basics and Features

A. Google Cloud SQL

Cloud SQL is a web service in the cloud computing provided by Google. It is an Infrastructure as a Service (IaaS) that allows users to create, configure, and use relational databases that is available in the Google cloud. It is a fully-managed service the user can maintain, manage, and administer their databases which is stored in the cloud, allowing users to focus on their applications and services.

Features:

1) Easy to use

A graphical user interface (GUI) that allows the user to create, configure, manage, and monitor their databases in the cloud.

2) Fully managed

The Cloud Service Provider takes care of the tasks like replication of data, patch management, or backups.

3) Highly Available

The user data are replicated across multiple geographic regions, so the services are available, and user data is preserved, incase if the datacenter becomes unavailable. The user Databases can be created and replicated in datacenters either in Europe or United States. User can choose whether to use synchronous or asynchronous replication.

4) Integrated with Google App Engine and other Google services

Application integration with Google App Engine and other Google services enables the user to work across multiple products easily, get more value from the data, move user's data in and out of the cloud, and get better performance.

B. Advanced Encryption Standard (AES)

The Advanced Encryption Standard is a specification for the encryption of electronic data. AES is based on a design principle known as a substitution-permutation network, and it is efficient and fast. That works both in software and hardware. AES uses a fixed block size of 128 bits. The key sizes used in it are 128, 192, or 256 bits. The key size used for an AES cipher specifies the number of repetitions of transformation rounds that converts the user input, called the plaintext, into the final output, called the cipher text. The numbers of cycles of repetition are as follows:

Table 1, Key Size and numbers of cycles of repetition

Key Size	No Of Cycles
128 bit	10
192 bit	12
256 bit	14

In each round there is more number of processing steps, in which one that is specific for encryption key itself and a set of reverse rounds are applied to transform cipher text back into the original plaintext using the same encryption key.

Algorithm:

Step 1: KeyExpansion

The round keys are derived from the cipher key using Rijndael's key schedule.

Step 2: Initial Round

AddRoundKey: Each byte of the state is combined with the round key using bitwise XOR.

Step 3: Rounds

SubBytes: A non-linear substitution step where each byte is replaced with another according to the lookup table.

ShiftRows: A transposition step where each row of the state is shifted cyclically a certain number of rounds.

MixColumns: A mixing operation which operates on the columns of the state, combining the four bytes in each column.

AddRoundKey

Step 4: Final Round (no MixColumns)

SubBytes

ShiftRows

AddRoundKey

Performance Features:

High speed and low RAM requirements are criteria for the AES selection process. Thus performance of AES is more efficient in hardware, which varies from 8-bit smart cards to high-performance computers.

C. Google App Engine

Google App Engine allows user to run web applications on Google's infrastructure. App Engine applications are easy to build, maintain, and scale as user traffic and data storage increases. With App Engine, there are no servers to maintain: users can upload their application, and it's ready to serve their needs.

Users can develop their application for the Java runtime environment using common Java web development tools and API standards. The application interacts with the cloud environment using the JavaServlet standard, and uses common web application technologies such as HTML, Java Server Pages (JSPs).

III. Implementation

This paper relies on the Google Cloud SQL. To access the Google cloud SQL the user needs to create an account [5] in it to provide the necessary details and billing information. This will provide the user to select specific resources and pay as they use.

The Cloud SQL is provided by Google which is the Cloud Service Provider (CSP). The CSP has various authentication and security but it is not safe to store data in a third party location. The data is encrypted and stored. The encryption algorithm used to encrypt the data is Advanced Encryption Standard.

The cloud SQL can be accessed by using web browser or by using Eclipse API which allows the user to create their programs that can be executed on the cloud. The programming languages support by it is JAVA AND PYTHON. The AES has been implemented using the JAVA.

The Eclipse API should be first configured with the Google by installing the plug-in which will gives the user to interact and access data with the cloud.

Procedure:

Step 1: Create a Google account.

Step 2: Request for necessary resources (Cloud SQL) that is required and select the resource usage amount.

Step 3: Create database with the necessary tables.

Step 4: Configure the Eclipse API to access the services in the cloud.

Step 5: Create a user interface application to the database in Cloud SQL using Eclipse API.

Step 6: Create code for the AES algorithm in java.

Step 7: Create an AppEngine application to execute the code in cloud.

Step 8: Encrypt the data using code.

Step 9: Store the encrypted data in respective tables in the database.

Step 10: Decrypt the data whenever required to access the database.

IV. Conclusion

In this paper the AES algorithm has been implemented to store data in the Google Cloud SQL. This will provide security to the data stored in an untrusted third party location in the internet and it will also provide a trust management between the user and the Cloud Service Provider. The user can get additional security by encrypting the data along with the CSP data securities such as data backup, data recovery, authentication etc.,

The encryption of data will add an additional security to the data stored in the cloud and only the user can be able to access the data whenever and wherever required. The user can also share the data to others by using the key used for encryption.

REFERENCES

[1]https://cloud.google.com/files/GoogleCommonSecurity-WhitePaper-v1.4.pdf

[2] https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

[3] https://developers.google.com/cloud-sql/

[4] http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

[5] https://developers.google.com/cloudsql/docs/before_you_begin

Authors Profile

(1)Author S.SABARI VASAN is an M.Tech, student in Computer Science & Engineering, Dr. MGR Educational & Research Institute University, Chennai, TamilNadu, India.

E-mail - vasan_sabari@yahoo.co.in

(2)Author I.GOLDA SELIA is an Assistant Professor in Information Technology, Dr. MGR Educational & Research Institute University, Chennai, TamilNadu, India.

E-mail - golda_selia@yahoo.co.in