Encrypting Data of Banking Database deployed in Cloud

Dhanushree R[1], Chethana M[2]

[1]*M.Tech Student, Department of Information Science and Engineering,*
[2] *Assistant Professor, Department of Information Science and Engineering*
[1]*dhanuramanna@gmail.com,* [2]*chethanamallika@gmail.com*
Bangalore Institute of Technology, Bangalore, India.

Abstract

Banking application need not be only the application used by the customers always. The application used within the bank to maintain the records of their customers are also referred as Banking application. Now a day most of the application are moved into the cloud to ensure the accessibility anywhere. But the problem in cloud is securing the data, Since the Cloud Service Provider(CSP) has provided many security measures to protect the user data, which is not sufficient for the user to trust those securities to ensure extra security the user has to implement some more efficient security measures. The data need not always be attacked when it's at motion even data at rest can also be attacked. The data which is at database are sensitive data which are related to the customers can be attacked if un authorized person gets the access to the system. Hence maintaining the security for these data of the customers become more efficient. In this project the frame work has been defined to secure the data which is going to be stored in the database as soon as the data is created, this is possible with the help of implementation of the AES encryption technique to the data before storing into the database to secure the data from the attackers.

Keywords: Banking application, Cloud Platform, Database security, encryption, decryption.

I Introduction

There was lot of demand for identification of new system to replace the traditional banking system, which actually uses relatively long time and a complicated process to maintain the records, these records were initially noted on the paper and later they were scanned and that scanned copy were verified and placed in the local server which was centrally placed and then the papers were re-stapled kept at record room. There were other challenges faced during this time, Quality of the scanned copies were not so good which would many time leads to data loss, rescanning of data was another issues where the same data was duplicated and created a mess in calculations, and there was no such concept like

only authorized person has to use that system like every employee can work with which ever system which lead to a problem of data integrity. This problem was overtaken by the cloud computing where the banking application will be place at cloud for computation. The confidential data of the banks would have now moved from physical location to third party cloud supplier, hence the trusting the cloud service provider becomes a main concern. However, the cloud service provider says they provide best security measures, its user responsibility to ensure the protection of data stored by them on the cloud by providing more security. One of the best ways to secure the data stored in the database is to encrypt the data before storing them at the database. To achieve this AES algorithm has been used with the 256-bit key which would undergo 14 rounds of encryption intern securing the data.

II Related Works

In this paper they have discuss the necessity of database encryption and made an in-depth review of various database encryption scheme and compare their] results on the basis of advantage and disadvantage. [1]

Implement cryptographic methods suitable for a database with the help of algorithm which has a few securities measures used for the encryption may involve in higher level of encryption/decryption time depending on the key size, which would gradually lead to the substantial decrease in the performance on large set of data. [2]

This paper will show the framework that is used for sharing secure sensitive data between the banks, using variable AES instead of normal AES for securely storing the data, each block of data to get encrypted new sub key will be generated in variable AES when compared to Normal AES. Normal AES uses same key for all block of data. Hence the data will be more secured in variable AES compared to Normal AES. [3]

The systematic arrangement of data in a container is referred as database. To protect the data in the database, collective measure are taken which is referred as Database security, data will be protected against the illegitimate users or attackers. Six types of different methods have been proposed in this paper to ensure the secure way of storing the data and retrieving in an effective and convenient way. [4]

III Proposed System

In this proposed system the main target is to protect the sensitive data of the banks by encrypting the data before storing into the database in the cloud. The application will be deployed in the cloud using EC2 instances. The front end of this application will be designed using HTML, CSS, JavaScript, JQuery etc. In this proposed system the database has been created for the banking application which is already deployed in cloud. In this project encryption is done only for the transactional table stored in the database. Which would consist of the Transactional-ID, Account number, Amount transacted, Transactional-time, Transactional-Date for future references. As shown in the figure 1.1, user interacts with the application which is deployed in the cloud, database will be created according to the requirements in the cloud and then it will be connected to the java application using JDBC.

Figure 1: Class Diagram for User Interaction

Once the connection is done the AES algorithm will be implemented by call the API for AES algorithm in the program. Here in this program will be using 256-bit key length for AES algorithm. Secret key will be specified by the programmer for encryption program. When the data has been requested by the user the data which is stored at database will get decrypted. The figure 1.2 shows the data flow for this banking application, where user input entered at UI will be encrypted and stored at database and when retrieving back the data stored at database will be compared with the user input and the matched data will be displayed at user end.
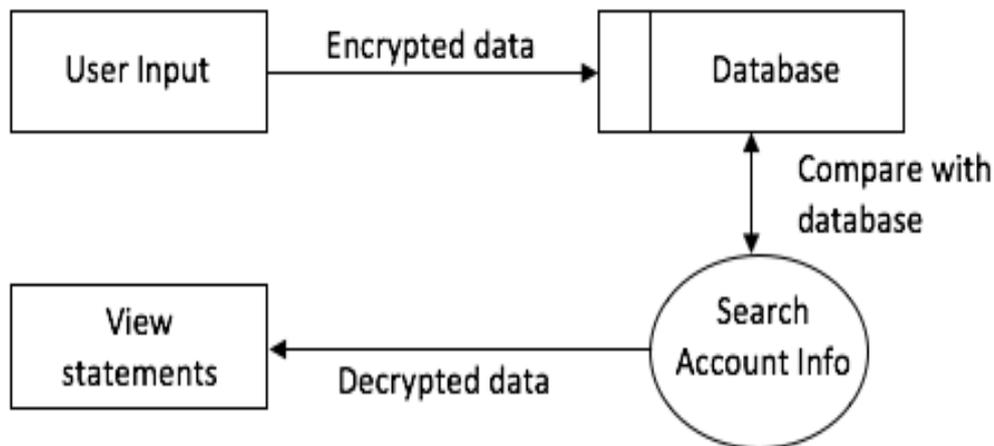
Figure 2: Data flow in the application

IV   Results

To view the database, the tool we have used is Xampp, through which cloud database can be viewed with the help of master credential of that database specified by the developer while creating that database in the cloud.

Figure 3: Table of savings account

The figure 1.3 shows the one of the table present in the database which relates to saving account. Here the customer details for savings account will be shown. The account number is the primary key attribute and the highlighted part which is one of the account number going to be encrypted in the transactional table.

Figure 4: Transaction example for amount is deposited to an account

The figure 1.4 shows the Deposit page for entering the account that need to be deposited in that account by specifying the account number. Once the Submit button for deposit is clicked it shows the pop-up box with the Transactional-ID which is going to be helpful in future references work of the banking staff.

Figure 5: Transaction table where data is encrypted

The figure 1.5 shows the one of the table present in the database which relates to savings account transactions. In this table Transactional-ID created when the transaction is successful will be the primary key for transactional table and account number which is a primary key of saving account table is going to be foreign key for transactional table. In this figure account number has been encrypted and stored.

V Conclusion and Future Enhancement

The database was made more secure to store data when compared to storing the data in the original format by using AES algorithm. This project has been implemented using Normal AES algorithm but Variable AES is more secure compared to Normal AES algorithm because Normal AES uses single key for the encryption of all the bytes of the plain text whereas Variable AES generate different keys for every 16 bytes of plain text and thus the data encrypted will be more secured. At present encryption has been applied to only on single attribute of the table present in the banking system and hence the encryption needs to be applied for all the attributes of the tables present in the database.

VI   References

[1] *R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, I. Brandic, "Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility, Future Generation Computer Systems", Vol. 25, No. 6, pp. 599-616, Elsevier Science, Amsterdam, The Netherlands, June 2009.* ⸎

[2] *Leymann, F.,"Cloud Computing: The Next Revolution in IT", In: Dieter Fritsch (Ed.), Proceedings of the Photogrammetric Week '09, September 7-11, Stuttgart, Germany, Wichmann Verlag, 3-12, 2009.* ⸎

[3] *An overview of the security concern in enterprise cloud computing, Anthony Bisong et. al., International journal of network security & its applications (IJNSA), Vol.3, No.1, January 2011, P.36*

[4] *T. M. Zaw, M. Thant and S. V. Bezzateev, "Database Security with AES Encryption, Elliptic Curve Encryption and Signature," 2019 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF), Saint-Petersburg, Russia, 2019, pp. 1-6.*