SECURE MULTIPLE BANK TRANSACTION LOG: A CASE STUDY

Amol Bhatnagar[1], Shekhar Tanwar[2], R. Manjula[3]

[1]*Student, Computer Science & Engineering, VIT University, Tamil Nadu, India*
[2]*Student, Computer Science & Engineering, VIT University, Tamil Nadu, Indi*
[3]*Professor, Computer Science & Engineering, VIT University, Tamil Nadu, India*

Abstract

This work will demonstrate a case study of a secure multiple bank transaction log. In particular we have implemented and evaluate a multiple bank transaction maintenance log. In this application we have implemented a transaction catalog which will maintain the transaction log from various bank in which the user has accounts. In this application we have identified a set of security issues and have applied the appropriate approach to minimize these security issues.

Keywords: *Security, Mobile databases, Server, Consortium, MySQL database, Mobile device, Third party auditor.*

----------***----------

1. INTRODUCTION

The use of mobile devices is increasing day by day. Every day there is an increase in the processing and computation power of the mobile devices and new technologies are being implemented to support the growing need of the mobile technology. Now database management is not only limited to the field of web technology but has expanded itself to cover mobile technologies as well. We have developed an application that comprises of a central database connected through a server to consortium of different banks and a number of autonomous mobile users with a mobile application.

One of the most important issue of concern in this application is providing sufficient security and privacy of the user data. Security issues of data flow through mobile devices are of prime importance as this involves the consortiums of different banks which will be carrying the important private data. We have come up with a solution that will ensure the security of the user data through an additional layer of security that we will discuss in the later part.

2. SECURE TRANSACTION LOG

We have considered the following system to maintain a secure transaction of multiple banks; our application is basically divided into three parts:

- A mobile device running on the Android Platform.
- A mobile database maintaining the transaction log.
- A third party Auditor for additional layer of security
- A PHP based web server.
- Assumed bank consortium.

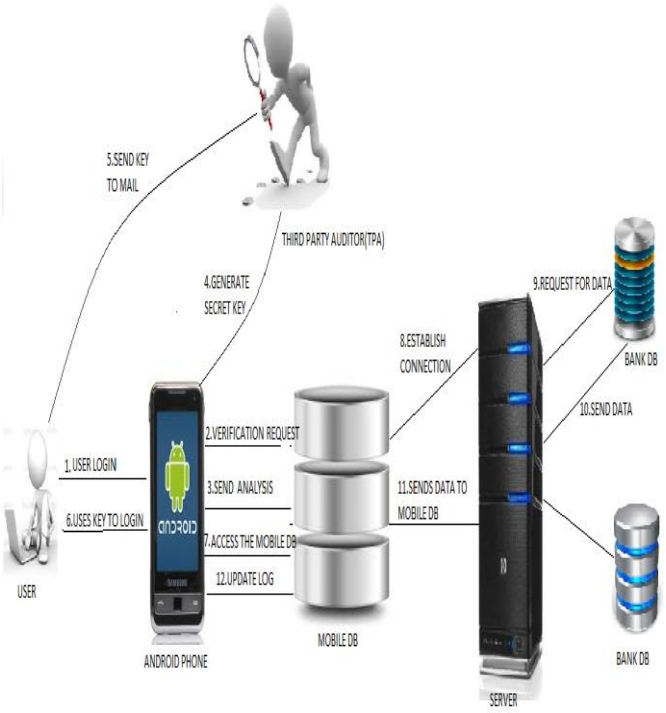

Fig-1: Secure transaction log of different bank

2.1. Mobile Device

The application running on the mobile device comprises of an interactive user interface. This user interface is compatible to all the android versions in the market. Through this user interface, user can interactively maintain their transaction log both in offline and online modes [2].

When the client is operating in offline mode then the client has a privilege to maintain the transaction log manually without

having connected to the server. This approach has several advantages compared to orthodox approach where there is no local storage available on the mobile device.

- Reduced dependency on network usage: As this application can work in an offline mode, thus it helps in reducing the dependency on network usage.
- Immediate access: Except for the synchronization of the latest entry, this application has access to all the previous transaction, enabling user the immediate access to all his transaction.
- Energy efficient: Once synchronized this application will update and maintain the transaction log locally on the mobile database, thereby reducing the need to synchronize and use the mobile hardware every time to access the transaction.

2.2. Mobile Database

Basically the mobile database is used to maintain the transaction log. The mobile database consists of two tables i.e. transaction and accounts, the transaction table is responsible of holding all the transaction from the different banks and account table maintains the information about the different accounts which the user had registered on this application [1]. Moreover the updation made through the transaction would be reflected back in the accounts table as well.

2.2.1. Security Issue

This application will provide two fold security i.e.

- The user level security.
- Network connection security.

2.2.1.1. User Level Security

As this application consists of sensitive data there is a need of providing two layers of security. The first layer of secure access consists of providing the propriety use of passwords security, this phase will enables user to create a password protected environment and will restrict the malicious use of information by the other user as the password is only known to the authorizing user.

Due to the modernization of different cryptographic techniques, the security through password is no moreover a secure access [7]. Thus to overcome this issue, there is a need of providing a more efficient, reliable and robust algorithm of supporting the futuristic need of security. One of these algorithms which we have implemented is providing the application with a third party auditor (TPA). Before allowing access to the application, the TPA will authenticate the user by a secret key which will be send to the authorized email of the user. This secret key will consists of pseudo randomly generated alphanumeric characters of length 6 or more, there by restricting the unauthorized access to the user data.

2.2.1.2. Network Connection Security

To maintain the efficient transaction log, the mobile database and the central database have to be synchronized at a particular time. This synchronization of both the databases is implemented in the system software of the mobile device and is performed on the HTTP protocol to serve the synchronization at a specific time [4]. Using HTTP protocol has the significant advantages, which will provide a wide range of protocol for the synchronization operation and a minor disadvantage of lower performance than the other protocols for the database synchronization operation. More precisely we have used secure HTTP protocol (HTTPS) to achieve the synchronization between the mobile database and the central database [10]. The reason for choosing HTTPS is as follows:

- HTTPS ensures authentication of the server computer.
- HTTPS ensures authentication of the client computer.
- Secure transfer that is confidentiality of the data that is transferred.

2.3. Third Party Auditor

As this application includes the high sensitive data of the user thus there is a need to provide the additional layer of security to the user. This addition layer of security ensures the integrity of the user and prevents the access to confidential user data by an unwanted user. This third layer of security that is third party auditor will ensure more restricted access to the application by the following way.

Before allowing access to the application, the TPA will authenticate the user by a secret key which will be send to the authorized email of the user. This secret key will consists of pseudo randomly generated alphanumeric characters of length 6 or more, there by restricting the unauthorized access to the user data [9]. The secret key generation involves the java.util.UUID library and generates and 128 bit key which we have limited to 6 bit of length only. This secret key length can be controlled according to the level of the security demanded by the user.

2.4. A Web Server

A web server is behaving as a portal to provide synchronization of mobile database and the central database.

2.5. Assumed Bank Consortium

It consists of a database which contains the table holding the various transactions being carried out by the user. On polling the database picks up the latest row entered into the database and update this row to the mobile database thus updating the transaction log [3].

3. ARCHITECTURE

The architecture of secure transaction log maintenance is shown in figure 2.This application works on the Client Server Architecture. The Client side of the application basically consists of three important modules i.e. Mobile Database, Application Interface and the User Interface. The Application Interface provide the user the interactive way of communicating with the mobile database, basically the application interface provides the end to end communication link that is used to transfer data between the mobile database and the user interface [5].

Basically the client side is a mobile application with a graphical user interface that used to provide an interactive way of maintaining a transaction log of the user. The mobile database is a small database on the client side i.e. mobile device which reflects the specific past of the bank database.

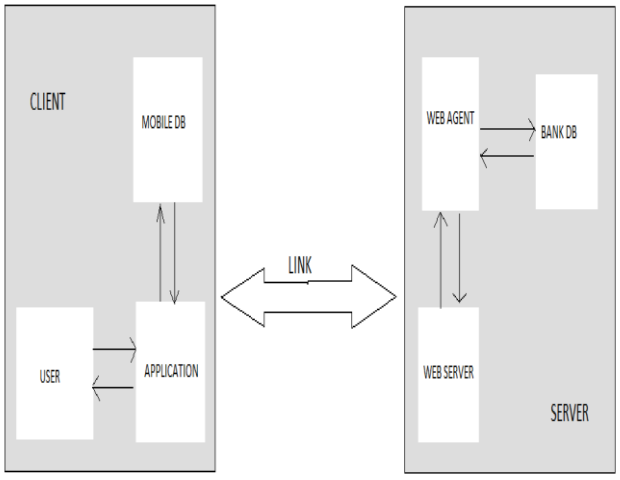

Fig-2: Architecture of the application

The server side of the application also has three main components i.e. web server, web agent and bank database. The bank database provides the transaction information updated by the specific bank according to the user activity [6]. The web agent connects the web server to the bank database; basically the web agent provides the end to end connection between the web server and the web database.

This application has to use a communication link between the client side and the server side for maintaining the updated transaction log. The link is secured by HTTPS protocol but there is another way of establishing the link like JSON object

4. The MOBILE APPLICATION

We consider the following mobile application: In this application there is a read only client which is basically used to access the application, the viewer will provide the user with the different options like Add Account, Add transaction, View Transaction ,View Account and the web server connected with the bank database to provide the synchronization [8].

The Add Account feature in the application will provide a way to add the new account to the application, Add Transaction is used to add the transaction manually, View Transaction will provide the synchronized transaction log obtained from the bank database through a secure server connection and View Account will list all the account added by the user in this application.

Fig-3: The mobile application

5. CONCLUSIONS

Paper proposes the models which enables a user to maintain the secure multiple bank transaction log over a secure channel. This application will provide two fold security i.e. The user level security and Security of network connection. This will ensure the privacy and the protection of the user from unauthorized access.

FUTURE WORK

In particular we have developed a prototype of a mobile application which maintains a transaction log of the various transactions that a user makes in various bank accounts. We have identified a set of security issue in maintaining secure transaction log and had implemented an additional layer of security through a third interface that will ensure the authenticity of the user. In future work we will try to improve our models in respect of the security and performance issues also we propose to increase the efficiency of the fetching of the data from the database and making it more robust.

ACKNOWLEDGEMENTS

We would like to express our sincere gratitude to my guide and the other author of this paper for their valuable help.

REFERENCES

[1]. Rakesh Agrawal, Jerry Kiernan, Ramakrishnan Srikant, and Yirong Xu. Hippo-cratic databases. In 28th Int'l Conf. on Very Large Databases (VLDB), Hong Kong, 2002

[2]. Guy Bernard, Jalel Ben-Othman, Luc Bouganim, G´erˆome Canals, Sophie Chabri-don, Bruno Defude, Jean Ferri´e, St´ephane Gan¸carski, Rachid Guerraoui, Pas-cal Molli, Philippe Pucheral, Claudia Roncancio, Patricia Serrano-Alvarado, andPatrick Valduriez. Mobile databases: a selection of open issues and research directions. SIGMOD Record, 33(2):78–83, 2004.

[3]. Thomas Connolly and Carolyn E. Begg. Database Systems:A Practical Approachto Design, Implementation and Management 4th Ed. Addison-Wesley, 2005.

[4]. Microsoft Corporation. Step by step: Developing a sql mobile application withvisual studio 2005 and sql server2005, June2006.(http://msdn2.microsoft.com/enus/library/aa454892.aspx).

[5]. Georgios Drosatos. Data management on platforms with restricted computational resources Master's thesis, Dept. Electrical and Computer Engineering, School of Engineering, Democritus University of Thrace, Greece, 2006 Written in Modern Greek

[6]. Ramez Elmasri and Shamkant B. Navathe. Fundamentals of Database Systems, 4th Edition Addison-Wesley, 2004

[7]. Benjamin Halpert. Mobile device security In InfoSecCD '04: Proceedings of the 1st annual conference on Information security curriculum development, pages 99–101,New York, NY, USA, 2004. ACM Press

[8]. Sushil Jajodia. Database security and privacy ACM Comput. Surv., 28(1):129–131, 1996.

[9]. Sumit Jeloka. Oracle Database Security Guide Oracle Corp., Redwood City, CA,USA, February 2005. B14266-01

[10]. Abraham Silberschatz, Henry F. Korth, and S. Sudarshan. Database System Concepts, 5th Edition McGraw-Hill Book Company, 2005

BIOGRAPHIES

Manjula R, associate professor at VIT University. E-mail: rmanjula@vit.ac.in

Amol Bhatnagar, student of computer science engineering at Vellore Institute Of Technology, Vellore, Tamil Nadu. He is currently pursuing B.Tech in Computer science at VIT University. His current area of research includes Cloud Computing.

Email:amolmbd@gmail.com

Shekhar Tanwar, student of computer science engineering at Vellore Institute Of Technology, Vellore, Tamil Nadu. He is currently pursuing B.Tech in Computer science at VIT University. His current area of research includes Mobile application development.

E-mail: shekhart91@gmail.com