A Proposal for Smart Authentication mechanism in the Locker System

[1]Suganthy. A, [2]Surendar. K

[1,2]Department of Banking Technology
[1,2]Pondicherry University

Abstract: This paper aims in exploring the security system of the lockers available in banks and proposes a smarter security system. The proposed model uses a smarter application for authenticating the user using biometric authentication mechanism for using the locker system. The system also provides a passcode for the user to use the locker system and this passcode acts as one time code for the user to use the locker system. Whenever the user uses the locker system, the user has to request the passcode from the system using the mobile request and the user has to submit the same to the system. This system provides a higher security mechanism for authenticating the user.

IndexTerms – **Smart Locker, Smart application, Secure Locker System.**

I. INTRODUCTION

Banking industries in India are adopting to the technological advancements and they are providing their banking services to the tech-savvy customers. The technological inclusions in the banking services benefitted the customers of the banks in multiple ways. Banks have adopted the information technology services in their business process in a phased manner. In the initial days, banks started to automate all the banking process and later they wanted to provide their services to their customers using information technology. Over a period of time, banking customers adopted the technological advancements and they started getting benefits out of the digital services provided by the banking systems. With the help of the information technology, banks have implemented various applications for the benefit of their customers.

Today, banking services are available to the customers in a more convenient way and the customers need not go to the banks for getting the bank services. Banks have implemented multiple service delivery channels and some of them are introduction of ATM, online banking, mobile banking, SMS services etc. and these delivery channels benefits the customers in a number of ways. It reduces the time for delivering the services to the customer by avoiding the customers to stand in a long queue in the banks for getting some of the services like withdrawal, deposits etc.

The remainder of this paper is organized as follows: section II of this paper aims in exploring the security system available in the locker system of the banks. Section III explains the proposed model of the system with smart authentication system and section IV concludes the paper.

II. LOCKER SYSTEM IN BANKS

Apart from providing financial services to the customers, banks are providing locker facilities to their customers where the customers could safeguard their valuable things. Banks are providing these locker facilities on rental basis to their customers and it's the duty of the banks to safeguard the lockers from attacks by the attackers. Currently the lockers in banks are protected with the help of various security protection mechanisms and these security mechanisms are mostly based on traditional way of safeguarding the lockers.

Present locker system functions in the following way, when a customer wants to get the locker facility, the customer has to approach the banks and they get the locker and the customer will be provided with a key for using the locker system. Two keys will be used for operating the locker system in most of the cases and Figure 1 shows a picture of a traditional locker system. Whenever the customer wants to use the locker for keeping his valuable assets or to take any asset from the banks, he has to approach the officials of the concerned banks where the locker is available and only with their concerns the customer should open the locker using the key available with the customer. The officials of the banks will maintain the other key using which the locker could be opened, so for opening the locker system, both the keys are used and this mechanism gives an initial way of protecting the locker system.

Figure 1: Locker System

Security features of the traditional locker system

The security of the traditional locker system used in banks are as follows:

- The use of two keys for the operation of the locker system will help to serve the basic security operations [2].
- Installation of CCTV's in the locker room will help to monitor the activities of the people entering in the room where the locker systems are placed [3].
- Maintaining the log details of the people entering in the locker room.
- Maintaining the registry.

The security features involved in the traditional locker system is vulnerable to attacks by the attacker. Because of the threats involved with the traditional locker system, the reputation of the organization which maintains the locker will be spoiled. This paper proposes a smarter locker system which is explained in the below section of the paper.

III. A PROPOSAL FOR SMARTER LOCKER SYSTEM

In the traditional locker system, authenticating the user of the locker follows a manual process and leads to the misuse of the system by the attacker. Hence this paper proposes a smart authentication mechanism which avoids the use of manual process for identifying the customer using the system.

The proposed model for authenticating the user has the following steps:

- The user of the locker has to send a request for accessing the locker using the mobile.
- The locker system from the bank side has to verify the request from the user and it should provide a passcode to the requested user.
- The user after reaching the locker has to provide the passcode to the system for using the locker.
- The proposed model uses biometric authentication mechanism for identifying the user.
- Once the user is identified using biometric mechanism and the passcode provided by the user, the system should allow the user to use the locker system.

The major feature involved in this proposed model are

- The use of biometric authentication mechanism
- The passcode which serves the purpose for one time. Passcode will be used for one time only and it will be expired in a shorter span of time.
- The proposed system saves time for the user to stand in a queue if the locker system is requested by multiple users at the same time.
- The proposed system also saves the cost involved in employing a guard to assist the user to open the locker system.

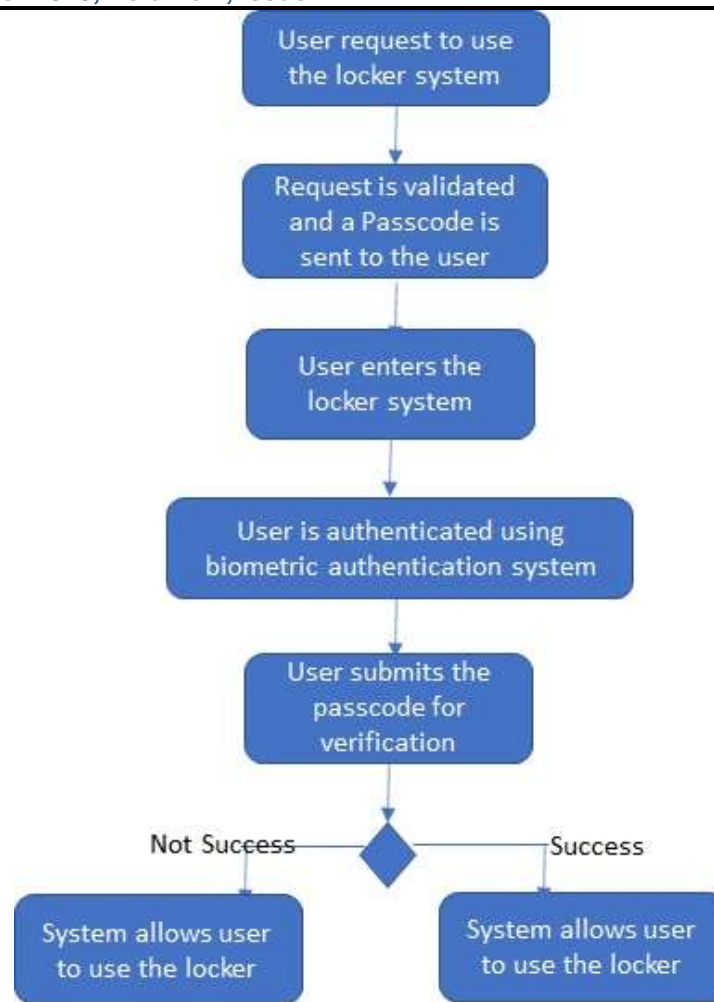The process flow involved in the proposed system is shown in Figure 1.

Figure 1: Process Flow of the proposed model

IV. CONCLUSION

This paper identified the difficulties involved in the current locker system in banks and proposed a smarter solution for banking system. The proposed model uses biometric authentication mechanism for identifying the user. The proposed model also provides a passcode to the user using which the user could access the system. This system eliminates the banker to verify the user and assisting the user to use the locker system. This system can be further enhanced using IOT and by providing more enhanced security features which completely avoids human involvement into the system.

REFERENCES

[1] A. Chikara, P. Choudekar, Ruchira and D. Asija (2020), "Smart Bank Locker Using Fingerprint Scanning and Image Processing," 6th International Conference on Advanced Computing and Communication Systems (ICACCS), pp. 725-728, doi: 10.1109/ICACCS48705.2020.9074482.

[2] Neeraj Khera, Amit Verma, (2014), "Development of an Intelligent System for Bank Securiety", 5th International Conference-Confluence The Next Generation Information Technology Summit (Confluence).

[3] A Gupta et al., (2016), "An Efficient Multistage Security System for User Authentication" International Conference on Electrical, Electronics and Optimization Techniques (ICEEOT).