Secure Authentication in Online Banking and ATM Transaction

[1]Mohammad John Saida, [2]Pragada Lakshmi Venkata Narasimha Sai, [3]Patibandla Phani Teja, [4]Seedirala Gopinath, [5]Yatham Badri

[1]Assistant Professor, KKR&KSR Institute of Technology and Sciences, Guntur, AP, India

[2,3,4,5] B.Tech (CSE), KKR &KSR Institute of Technology and Sciences, Guntur, AP, India

***Abstract*— This study examines the misconception of security in Automated Teller Machines of Banking sector. There is an immense growth in number of publics using Automated teller Machine and Online Banking every day. Even though technological developments like mobile banking and internet banking have helped in completely reforming the banking sector, ATM remain to be an important factor in the sector. Banking services provided by ATM are subject to proper authentication of user by sending OTP to subjected user registered mobile number. The scenario described below shows how OTP based authentication is not safe and portrays a clear picture of the need for enhanced need for authentication.**

INTRODUCTION

The Financial sector is one of the major fastest growing industries in the world economy. The development of the financial sector in a country is dependent on the progress of various intermediary banking and non-banking institutions in the country. Hence there is a prerequisite for banking sectors to divert their objectives from their existing goal of consistent profits to growth-oriented, future plans. This can be achieved by the banking sector by adopting technology which result in innovation. One such innovation is Automated Teller Machine (ATM) which is widely accepted by all banks.

Also, Online banking is a highly profitable channel for financial institutions. It provides customers convenience, flexibility and can be provided at a lower cost than traditional branch banking. Online banking has grown and flourished over the years but is now facing major challenges due to various attacks. Online banking now needs to pay attention to aspect of confidentiality, integrity and authentication. A well-known safeguard for Online banking and ATM transaction authentication is by is using passwords and PIN (Personal Identification Number) respectively.

LITERATURE RIVIEW

"Online Banking System using Mobile OTP with QR-Code"

[1] This explains paper explains implementation details of online banking authentication system. Security is associate vital issue for online banking application which might be enforced by varied web technologies. To eliminate threat of phishing and to substantiate user identity we have a tendency to use concept of QR-code. QR-code need to be scanned by user mobile device to extract the OTP which is hided in it.

EXISTING SYSTEM

The existing system of verifying users in ATM and online banking is SMS based OTP Authentication. When engaging in an online transaction whereby the service is required, an OTP will be sent to the registered mobile number of the user via SMS. User must input the OTP in order to complete the transaction thereby verifying their identity. A OTP once utilized cannot be used again, although it has various ups there are some downs also which we will discuss below:

DISADVANTAGE

1. SIM Swap Security Risk:

SMS OTP authentication relies on user mobile number, so the system is vulnerable to so called attack "SIM Swap". To launch this attack, a hacker obtains personal information from the user through methods such as phishing then the attacker convince the victims mobile operator to switch to new sim informing the original one was broken or lost etc., which gives them access to all OTP's

2. Malware Security Risk:
The malware now had more advanced functionalities, and among them was the ability to steal OTP authentication codes. The malware can be entered to user's device by various third-party applications which are prone to security issues.

3. Additional Problems with SMS OTP:

- The SMS transmission delay represent one of the major limitations for transaction.
- Network coverage problem does not allow customers to complete an authorized transaction.
- Cost associated with SMS is more when compared to the statistics of banks transaction.

PROPOSED SYSTEM

Initially at the time of account creation a screen containing user identity as QR-Code is displayed indicting account is created successfully. So, user need to scan their QR-Code in their respective authenticator app for further usage.

The proposed system mainly focuses on security and authentication for processing a transaction. To ensure this we use authenticator for verifying the identity, when user tries perform a transaction. Instead of regular SMS OTP the user needs to enter the secure authentication code which is displayed in the Authenticated app at the time of ongoing transaction. To make an understanding of this scenario take a regular ATM money withdrawal as example, when user enters the pin and select withdrawal option as a service an SMS will be generated and sent to the registered mobile number of the user. As discussed, SMS OTP is prone to various types of attacks, so here we use authenticator embedded in banking application instead of SMS OTP. While the transaction is ongoing the user needs to enter OTP which is generated by Authenticator to complete it.

ADVANTAGES

1. Network Independent:
Since the codes are not delivered over the mobile network, hackers can't intercept the codes that way. The result is that even if they were to reroute your number, they still wouldn't receive the codes.

2. Expire quickly:
Major benefit of authenticator apps is that their codes expire quickly. A new code is usually generated every 30 seconds.

3. Faster:
When compared to normal OTP delivery using carrier there may be delay in reaching the intended target, whereas in authenticator codes are generated from the app itself and doesn't rely on carrier which makes it faster.

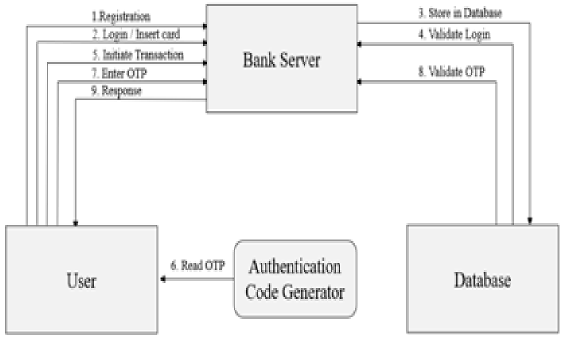
MODULES

1. Account creation and Device registration:
Initially user is entitled to give his details for account creation after that a screen containing user identity QR-Code is displayed which is to be scanned by the user to register his device and for further authentication purposes.

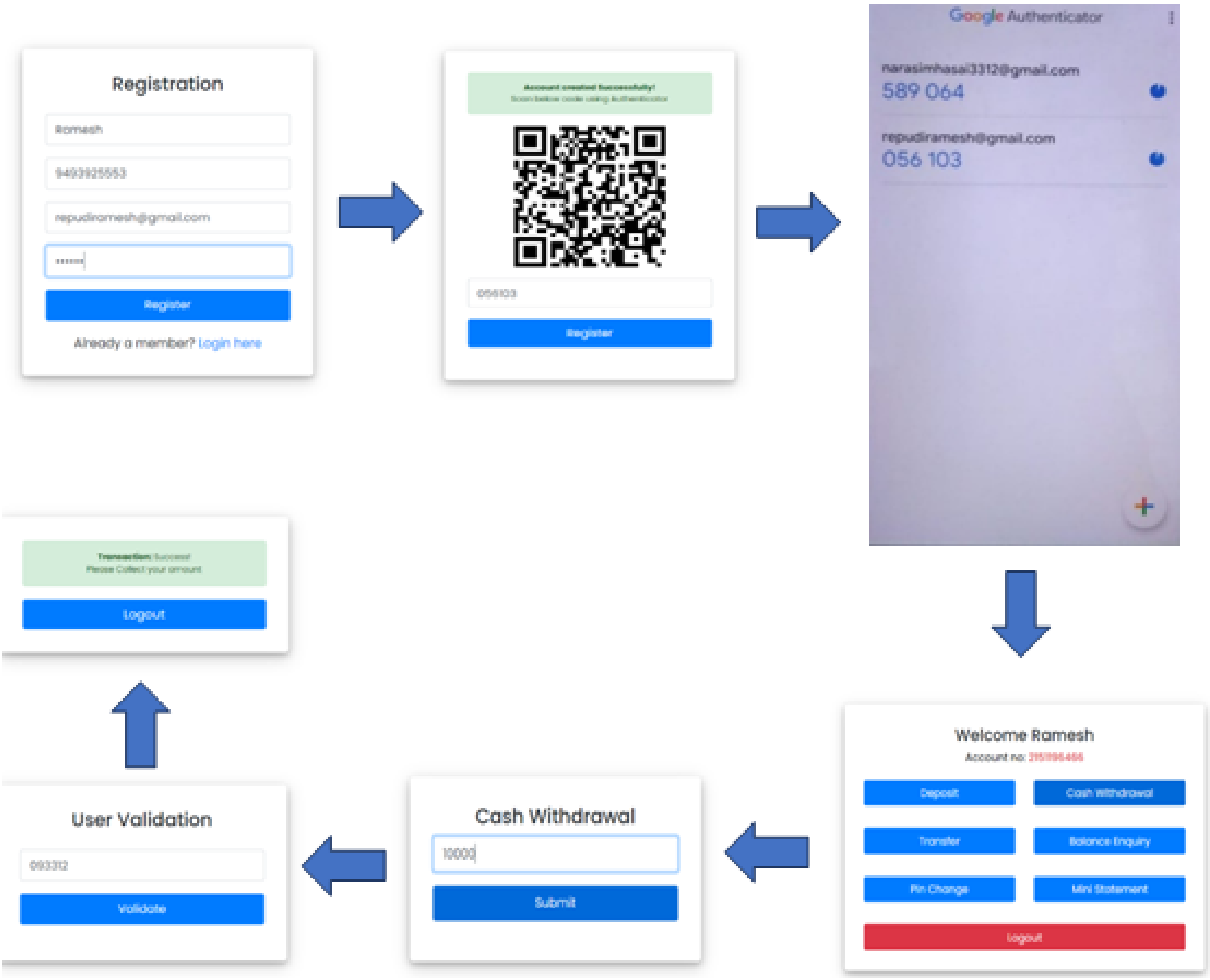
2. Transaction Initiation:
So, when the user enters his login credentials or insert his ATM card and initializes an online transaction or select withdrawal service the system navigates to verification screen where the user is entitled to enter the code generated in Authenticator app.

3. User Authentication:
Finally, the user needs to enter the authenticator generated secured code as OTP at the verification screen to complete the ongoing transaction securely.

ARICHITECTURE DESIGN



OUTPUT SCREEN:



Registration

Ramesh

9493925553

repudiramesh@gmail.com

Already a member? Login here

Account created Successfully!
Scan below code using Authenticator

056103

Google Authenticator

narasimhasai3312@gmail.com
589 064

repudiramesh@gmail.com
056 103

Welcome Ramesh
Account no: 2151195466

Cash Withdrawal

10000

User Validation

093312

Transaction Success!
Please Collect your amount

CONCLUSION

There must be a separate section for this authentication mechanism in the respective mobile banking application so that there is greater chance for maintaining confidentiality, integrity and non-repudiation for users. Proper infrastructure development of this scenario can show great results in banking sector in future.

REFERENCE

[1] Amandeep Choudhary, Shweta Rajak, Akshata Shinde, SiddeshwarWarkhade, Prof. F.S.Ghodichor, "Online Banking System using Mobile-OTP with QR-code", ISSN (Online) 2278-1021, Lonavala, Pune, India.