International Journal for Research in Engineering Application & Management (IJREAM)
ISSN : 2454-9150 Vol-04, Issue-12, Mar 2019

MGM-PAY

Secure Mobile Transaction using Multilevel Authentication

[1]Prof. Yogesh Shahare, [2]Aashish Prakash Patil, [3]Saurabh Gulab Zote, [4]Yash Vivek Dhuri,
[5]Pranay Tanaji Gade

[1]Professor, [2,3,4,5]UG Student, Dept. of IT MGM CET, Kamothe, Mumbai University, Maharashtra, India.

ABSTRACT - Mobile banking application and E-payment wallets are most important applications in today's world. Mobile banking service is made available by most of the banks all over the globe. The customer can manage all the banking services on their mobile banking application without going to bank office physically. That's why the security of mobile banking application for authorization of the user should be taken into account and the various combined methods for application login and transaction should be implemented. This research paper will introduce mobile banking application login and OTP code scanning methods. During our researches, we developed an Android based mobile banking application using MD5 algorithm to grant access to mobile banking application login and transaction process. We performed a sample test for this application, and it was found to be very secure and user friendly.

Keywords: Mobile Application Payment, OTP Authentication, OTP Code scanning, two-way authentication, MD5 Algorithm, Encryption.

I. INTRODUCTION

The use of the smart phones in today's world is increasing rapidly and gained a growth in mobile commerce and mobile banking in India. Mobile banking plays an important role between customer and e-commerce service. Mobile banking allows the user to pay anywhere at any time. Banking services through mobile banking application are offered by bank after obtaining permission from department of payment and settlement system, reserve bank of India.users . Mobile banking is made available from customers mobile network. The user virtually accesses the banking services such as obtaining account information, financial transaction and transfer money and make payments through mobile banking application.

These services are improved with the options for checking account balance, obtain mini statement and third-party transfer.

II. LITERATURE SURVEY

Lupu, Catalinand Vasile-Gheorghita Gatian proposed the security enhancement technique for online banking authentication process. This process was not feasible for mobile banking and also it requires special biometrics device for OTP code-based authentication.[1]

Same research was the performed by Venugopal Hridya and N. Viswanathand they proposed good method with more secure authentication mechanism. The only defect in this method was that based on the feature set from multiple data files. So, it was consuming more time for authentication and was not suitable for mobile banking. [2]

Then Yildirim,Nilay and Asaf Varol implemented a two way authentication scheme for mobile banking but without any security feature at the payment time and also main issue in implementation. And, it was working for some particular devices.[3]

As revised, the research by Plateaux & Aude "One time biometrics for online banking & electronic payment authentication" provides concept off security of one-time biometrics. This concept requires authentication by the bank and also with the user. [4]

"Usable security of authentication process" by Althobaiti,Maha M..,&Pam Mayhew says & analysis many security mechanism for authentication process & at the end they conclude OTP code scanning is more effective as compared to other biometrics technique. [5]

THE PROBLEMS WITH PASSWORDBASED AUTHENTICATION

Password based authentication is one of the most effective approaches to authenticate a user in various mobile application. But there are also many problems with password-based authentication system & risks associated with using passwords as an authentication mechanism for enterprise applications is not completely secure. One of the main problems with this password-based authentication is that many users don't know how strong their password should be? Extra rules to make your password strong drive call volumes to help desks proportionately. This problem can also result in IT & management letting password standards slip & as a result password of short length & complexity tend to happen such as simple 8-character

 DOI : 10.18231/2454-9150.2019.0241

words. This password can be easily cracked in few minutes, so they prove ineffective. And those passwords should also be less predictable by machines. There are many ways of cracking the password like Guessing, Brute Force Cracking, Dictionary Attacks or some other common methods.[9]

Downside:

- Security vs Ease of use for password
- Single high value target
- Does not provide strength identity
- Weak & susceptible to numerous attacks
- Shoulder Surfing Attack

III. SYSTEM ANALYSIS AND DESIGN

OTP CODE MODALITY: The most used type of modality is OTP code. The other types of modalities include fingerprinting, vascular, retina and facial recognition. There are two types of biometrics such as behavioral biometrics and physical biometrics. Behavioral biometrics are related to the behavior of a person and it can be used for validation. Physical biometrics are related to the structure of the body and it can be used for identification. Biometric system components consist of sensor, signal processing methods, storage, compare algorithm and decision-making process. First the sensor collects the data and converts information to a digital form. Algorithms perform quality control operations and generate the OTP Code structures. Then the data storage keeps information that new OTP Code sample/structure to one or more structures in data storage. Finally, decision making uses the generated information from the matching component to make a system level decision. [8]

ONE TIME PASSWORD: We have OTP for receiver authentication for several years and the accuracy using OTP Code must be very high compared to other biometric technologies. OTP Code scanning is one of the most used and popular technologies. OTP Code then refers to automatic authentication of receiver. Automatic OTP Code authentication is one of the most robust technology among the other technologies which are either currently available or under research. [7]

IV. PROPOSED SECURED OTP CODE

AUTHENTICATION: This project is to generate OTP Code identification possibilities in Mobile Banking. The Banks are now securing the mobile banking with Unique Ids and Passwords for every user. But still there are many aspects and risks for mobile banking. So, improving the existing security is very important. This evolution must be done someday. Now there are devices that have camera inbuilt, for Login and sending payment with OTP Code verification. This verification can also be added to Mobile Banking applications. During our study in this paper, we were able to develop a Java based android application that can:

1. acquire the OTP Code of the receiver;
2. do the enrollment and store the structure in a database;
3. do the verification of the user and then perform the transaction/payment.

We have implemented two factor authentications for login that means just after opening the application, the user will enter username and password and then next step will be OTP Code authentication. After the correct authentication process, user will be sent to the Home screen of the Mobile banking application.

V. PROPOSED SYSTEM

The proposed system has the following steps:

1) The user has to register by visiting the Admin page.

2) A registration form captures a minimum of the following:

• A user names.

• Unique UID No.

• Contact Number and Email ID

3) Generating OTP Code using username.

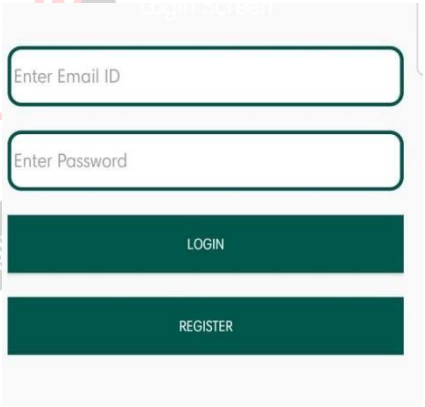

Figure 1: OTP Code Generation

4) Please enter OTP Code using the android App for Payment process.

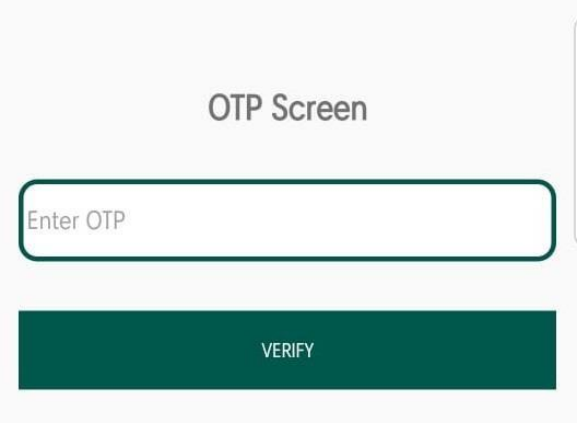

Figure 2: OTP Code Scanning

 DOI : 10.18231/2454-9150.2019.0241

5) The user will receive OTP code on registered mobile no., and he will have to share the code with end person for completing the payment process.

The proposed system as an end user be following:

From a user 's viewpoint the system appears user friendly and there is no password to remember.

The user account however becomes tied to the installed application that they used when they followed the OTP Code value.

Student have to visit the admin page for the new registrations with college ID, the admin will require basic details for generating a unique user id and password which he can use to pay for the canteen bills, college fees or any kind of payment within the institute with only OTP Code and OTP.

This application will save time as well as the queue for the payment and make paperless transactions in college thus reducing paper waste and well as cost of paper.

VI. IMPLEMENTATION

This is main screen of the android application. Users can login into application using their existing username and password.

This is main menu of the Android Application.

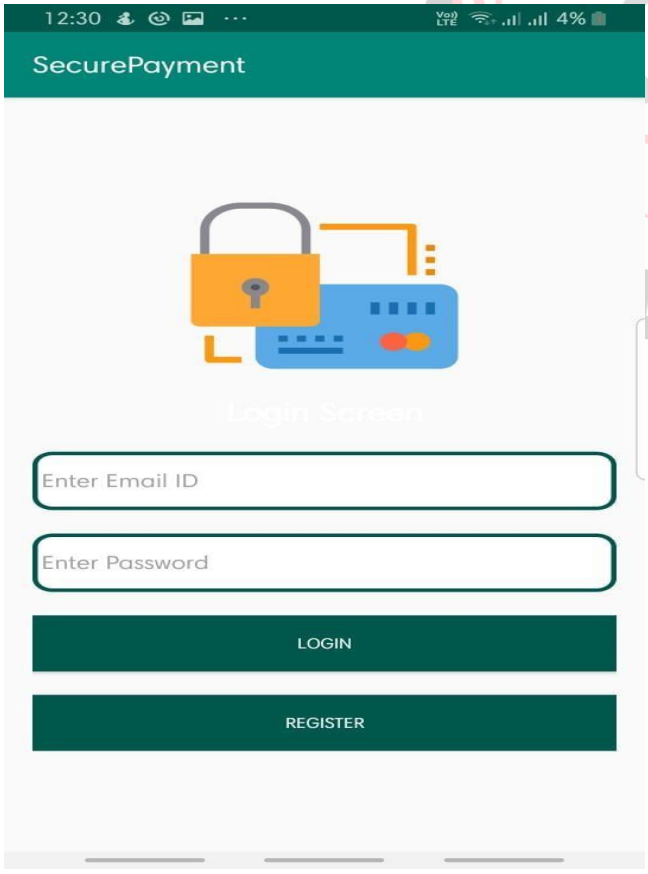

Figure 3: Login Screen

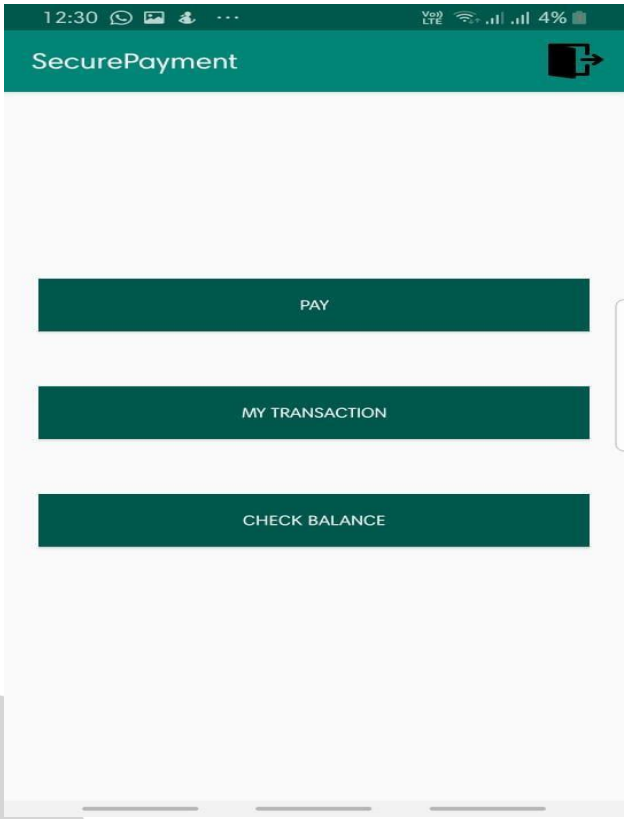

Figure 4 : Main Menu

User can do multiple operations as he wishes.

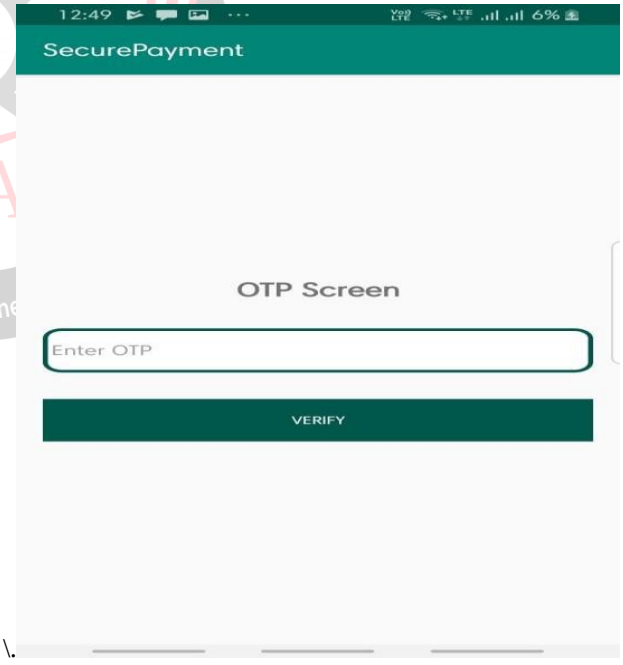

Figure 5: OTP Code Scanner

Once user completes the payment, he will be given popup regarding successful payment

 DOI : 10.18231/2454-9150.2019.0241

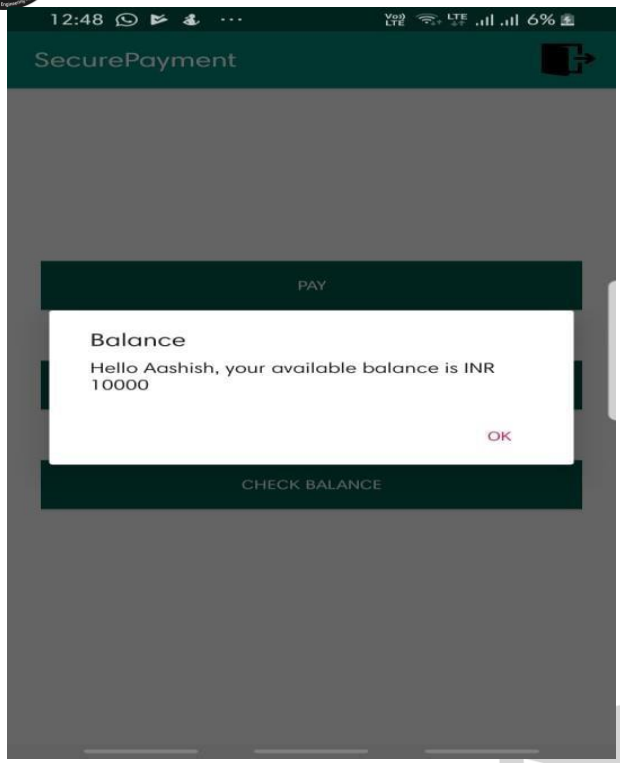

Figure 6: Payment Success

VII. CONCLUSION

Using one-time password eliminates the need of remembering the password, but it is an overhead of using a new password every single time of user logins. The above application takes the advantage of this facility as well as makes it easier for a user to use $_{his}$ OTP Code

The process of System embedding OTP into OTP Code in a cryptic approach and the pertinent application decoding the corresponding code makes the process effortless for the user to make payment. This system covers two key points of any authentication system i.e. "what should you know?" and "what you already have?", while the user just need to carry his OTP

Code and phone to be today's basic need. It makes registration simpler and reduces it to one step which is beneficial for user. Although verifying the user's UID number is mandatory requirement.

OTP Code Based payment, as a mode of Password-less Login at institute level implementations is uncommon because it doesn't have to rely on any Third-party Authentication or Authorization. It should however be easier for many users and has the potential for better security for most users as well. It is also no_t harder to implement than a Properly implemented password-based authentication system.

REFERENCES

[1] Shraddha Naik, Monam Pandey, Ashish Patil "OTP Code based authentication system for websites".

[2] Venugopal, Hridya, and N. Viswanath. "A robust and secure authentication mechanism in online banking." Green Engineering and Technologies (IC-GET), 2016 Online International Conference on. IEEE, 2016.

[3] Yıldırım, Nilay, and AsafVarol. "Android based mobile application development for web login authentication using fingerprint recognition feature." Signal Processing and Communications Applications Conference (SIU), 2015 23th. IEEE, 2015.

[4] Dr. Gomathy Thyagarajan "MOBILE BANKING – A REVIEW "International Journal of Management and Social Science Research Review, Vol.1, Issue.14, Aug – 2015

[5] Lokesh Sharma and Manish Mathuria "Mobile Banking Transaction Using Fingerprint Authentication".

[6] Lupu, Cătălin, Vasile-GheorghiţăGăitan, and ValeriuLupu. "Fingerprints used for security enhancement of online banking authentication process." Electronics, Computers and Artificial Intelligence (ECAI), 2015 7th International Conference on. IEEE, 2015.

[7] Renjie Weng – "Password-less login Everywhere, Journal of Stevens Institute of technology, Hoboken, NJ07030".

[8] Kirit Saelensminde and Prof. Veera Boonjing - "A simple password less authentication system for web sites, Seventh International Conference on Information Technology IEEE paper.

[9] Plateaux, Aude, et al. "One-time biometrics for online banking and electronic payment authentication." International Conference on Availability, Reliability, and Security. Springer International Publishing.

 DOI : 10.18231/2454-9150.2019.0241