iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** V **Month of publication:** May 2020

DOI: http://doi.org/10.22214/ijraset.2020.5179

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue V May 2020- Available at www.ijraset.com

A Geo-Location Authentication Application for Mobile Banking

Supritha[1], Jeevan[2], Spoorthi B[3], Ashika A[4], Sowmya K[5]
[1, 2, 3, 4]*Computer Science and Engineering Department, Srinivas institute of technology, Valachil*
[5]*Assistant Professor, Computer Science and Engineering Department, Srinivas institute of technology, Valachil*

Abstract: ***Mobile banking is a service provided by banks that allows its customers to conduct financial transactions using mobile application . Our application allows the users to conduct banking activities by checking balances or making payment through a Smartphone. One of the most challenging issues in mobile transaction is to provide the security to personal data. Everyday new challenges come in security and many technologies are working to resolve the issues and challenges. Accessing mobile transaction services through mobile application are unsafe because someone might misuse the data. The common attacks targeted on Mobile transaction application are man in the middle attack, phishing attack etc. Hence an application called GeoPay is developed for secure mobile banking. GeoPay application is implemented for both Real time and Non-Real time using Android Studio. In addition to the existing two factor authentication scheme using user ID, password and OTP, the face detector and geo location is used to authenticate the user.***
Keywords: face recognition, banking application, GPS location, pattern matching.

I. INTRODUCTION

One of the most common authentication mechanism is based on the use of password. People generally choose weak passwords and use the same ones for multiple services. As a result, accounts get hacked, people lose money, and privacy is breached etc. In order to counter those problems, security critical services, such as online banking, started to use multi-factor authentication solutions. For example, pattern matching, face recognition, OTP based authentication,

The use of more than one factor has been observed to be more secure than depending only on a single factor. Most solutions depend on factors that fall under three categories, namely: (1) what you know e.g. password, personal identity number (PIN), (2) what you have e.g. smart cards, token, etc., and (3) what you are e.g. biometrics, such as fingerprints, voice recognition, palm scanning or retinal scans. Even though these factors are sufficient for most cases, there is still additional room for improvements and alternatives. One of these factors is user's location. There are several existing systems that utilize location information to provide authentication and authorization solutions. However, these solutions usually require a specially designed infrastructure and Special devices that can used to determine their location

II. LITERATURE REVIEW

Nowadays wireless network and mobile technology are interconnected together to make the human life easier. This section of surveys shows various author approaches and their discussion.

Rohit Joshi proposed a Location based authentication system in which Location is used as an authentication factor. It is used for enhancing the security of banking using mobile applications.

Existing system do not provide high level authentication. It only provides user credentials i.e. username and password. Existing systems do not have any GPS location privileges ,face recognition and depends on basic three factors: what you know (secret), what you have (token), and what you are (biometrics). This Application will make use of the basis of Shamir's Algorithm for Secure Fund Transaction.

The data are being cached, or copied, and archived by the Cloud Service Providers (CSPs), more often without users authorization and control. The Self-destructing data mainly aims to protect the user data's privacy. All the data and their copies become destructive or unreadable after any user specified time, without any user intervention. Moreover, the decryption key is being destructed after the user-specified time.

Prince Gupta, Mahendra Hinde proposed a Location Based Authentication for E-Banking . Reliable client authentication and the data protection are still major concerns for banking transaction because authentication factors are open for hackers. This project reviews techniques that use location as authentication factor, and makes recommendation that how location can be used to enhance the security of a banking using smart phone application requiring robust client authentication and lastly how secret key using an AES algorithm for secure fund transaction. Author speaks about major terms such as Authorization, IMEI ,GPS. The system provides high level security by adding GPS location along with user credentials, i.e. username and password and also checks GPS location on timely basis to secure the data from unauthorized access, it uses self-destructing keys, which expires after some time making this system more secure.

Satpute Pooja, Gunjal Ashwini, Tidake Bharati, Mulay Shital, Prof.Pawar S.E proposed a Secured Bank Authentication Using Geo-Location Based System. Global Positioning System is used for tracking a location of the user. According to location of the user, user will be allowed to login into the system.

The user location should match each time when user want to access the system. To secure the textual password from the attack, system uses a sharing algorithm to create the share. The sharing algorithm deals with Image Processing and Visual Cryptography. In sharing algorithm, Signature of the user is processed and signature is taken as input which is then divided into different number of shares. One share is stored in the bank database and all other shares are given to the user. The user needs to provide his shares during every transaction and those shares are over lapped with the already existing bank shares and the share entered by a user. Share stored in the bank database is compared using correlation technique. If a higher correlation coefficient is achieved, then the verification is succeeded.

Dipak Auti, Krishna Landage, Swapnil Chavan proposed a location based security for online transaction. Global Positioning System is used for tracking a location of the user. According to location of the user, user will be allowed to login into the system. The user location should match each time when user want to access the system.

To provide security from the textual password attack, system uses a sharing algorithm to create the share. The sharing algorithm deals with Image Processing and Visual Cryptography. In sharing algorithm, Signature of the user is processed and signature is taken as input which is then divided into different number of shares. One share is stored in the bank database and all other shares are given to the user.

The user needs to provide his shares during every transaction and those shares are over lapped with the already existing bank shares and the share entered by a user.Share stored in the bank database is compared using correlation technique. If a higher correlation coefficient is achieved, then the verification is succeeded.

III. EXISTING SYSTEM

In existing system we face new challenging issues to provide the security to the data access control. Everyday new challenges come in security and many technologies are working to resolve the issues and challenges. Existing system has authentication factors such as security pin, pattern matching, biometric authentication etc. In existing system, there exist attacks such as fishing attack and man in the middle attack. In normal transaction app anybody who knows the password can easily get into the app and perform transaction. This is very risky.

IV. PROPOSED SOLUTION

One of the most challenging issues in mobile banking is to provide the security to data access control. Security to banking application is briefly discussed and new authentication method are implemented into banking application. Along with security pin, pattern matching, biometric authentication, further authentication features like face recognition, location based authentication are added. If the location of the registered user does not match the location stored in the database then he will be asked a set of security questions, this further increases the security of our application.

A. ER Diagram

The ER model defines the conceptual view of a database. It works around real-world entities and the associations among them. At view level, the ER model is considered a good option for designing databases. An ER diagram has three main components: entities ,attribute, relationship.

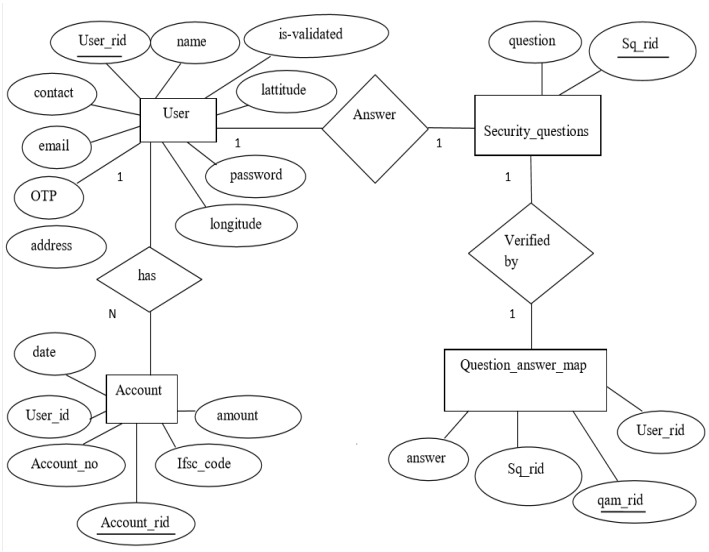


Fig 1: ER Diagram

The ER diagram representing the model of banking application. The entity-relationship diagram of geo-location authentication application for mobile banking shows all the visual instrument of database table and the relation between user, account, security_question, question_answer_map etc. etc. It used structure data and to define the relationship between the structured data groups of geo-location authentication application functionalities. The main entities of the geo-location authentication application are user, account, security_question, question_answer_map etc. one user can have N number of accounts. One user can answer one security question.Security question will be verified by question_answer_map.

B. Use Case Diagram

A use case diagram is a representation of a user's interaction with the system A use case diagram will describes the different types of users of a system and the various ways that they interact with the system. A use case diagram is a dynamic or behaviour diagram in UML. The use cases are represented by either circles or ellipses. Use case diagrams model the functionality of a system using actors and use cases. Use cases are a set of actions, services, and functions that the system needs to perform. Use case diagrams are valuable for visualizing the functional requirements of a system that will translate into design choices and development priorities. They also help identify any internal or external factors that may influence the system and should be taken into consideration.

The user inputs registration details to the system..The given input is then stored in the database. Thre username and password is used to login to the application. When a user login to the system email verification has to be done. The inputs are verified with database and access is granted to perform transactions.

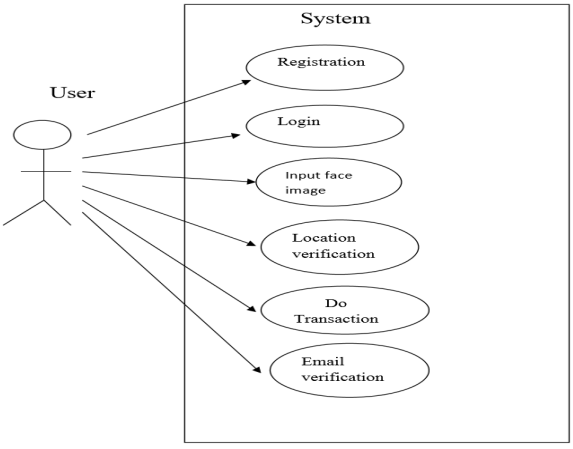


Fig 2: Use case Diagram

C. Sequence Diagram

Sequence diagram shows the participants in an interaction and sequence of messages flown among them. They also show the interactions of a system with its actors to perform all parts of use case. Each use case requires one or more sequence diagrams to describe its behavior. The user registers to the application by providing username ,password, security question and answers ,email id ,phone number and face dataset. The user inputs username and password to the system. The given input is then verified with database. The request is sent to scan the face. The face is verified with database if the face gets verified successfully ,then the registered location matched with current location .if the location is verified successfully then bank transaction will be performed. If the registered location is not verified successfully , then set of security questions will be asked for the user. the user needs to answer the questions. If the answer is right then he is allowed to perform transaction. Then user can fill the bank details like account number ,IFSC code, bank branch name etc, then proceed with the transaction.

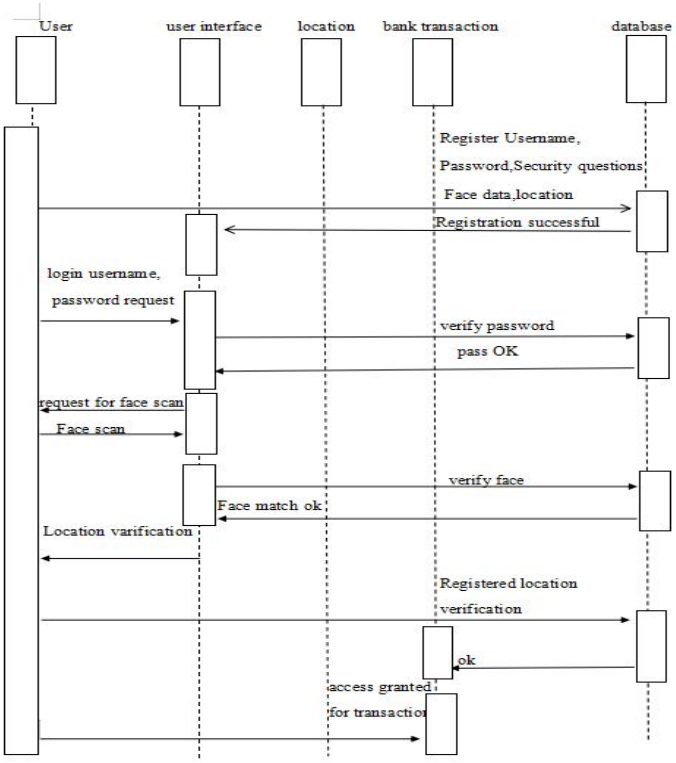


Fig 3**:** Sequence Diagram

V. EXPECRED RESULTS

If the users current location does not match with the registered location and if the users face is not recognized then the system will not allow the user to perform transactions. If both gets verified then user can begin histransaction.

VI. AKNOWLEDGMENT

We would like to thank, first and foremost, the almighty god, without his support this work would not have been possible. We would also like to thank all the faculty members of srinivas institute of technology, for their immense support.

VII. CONCLUSION

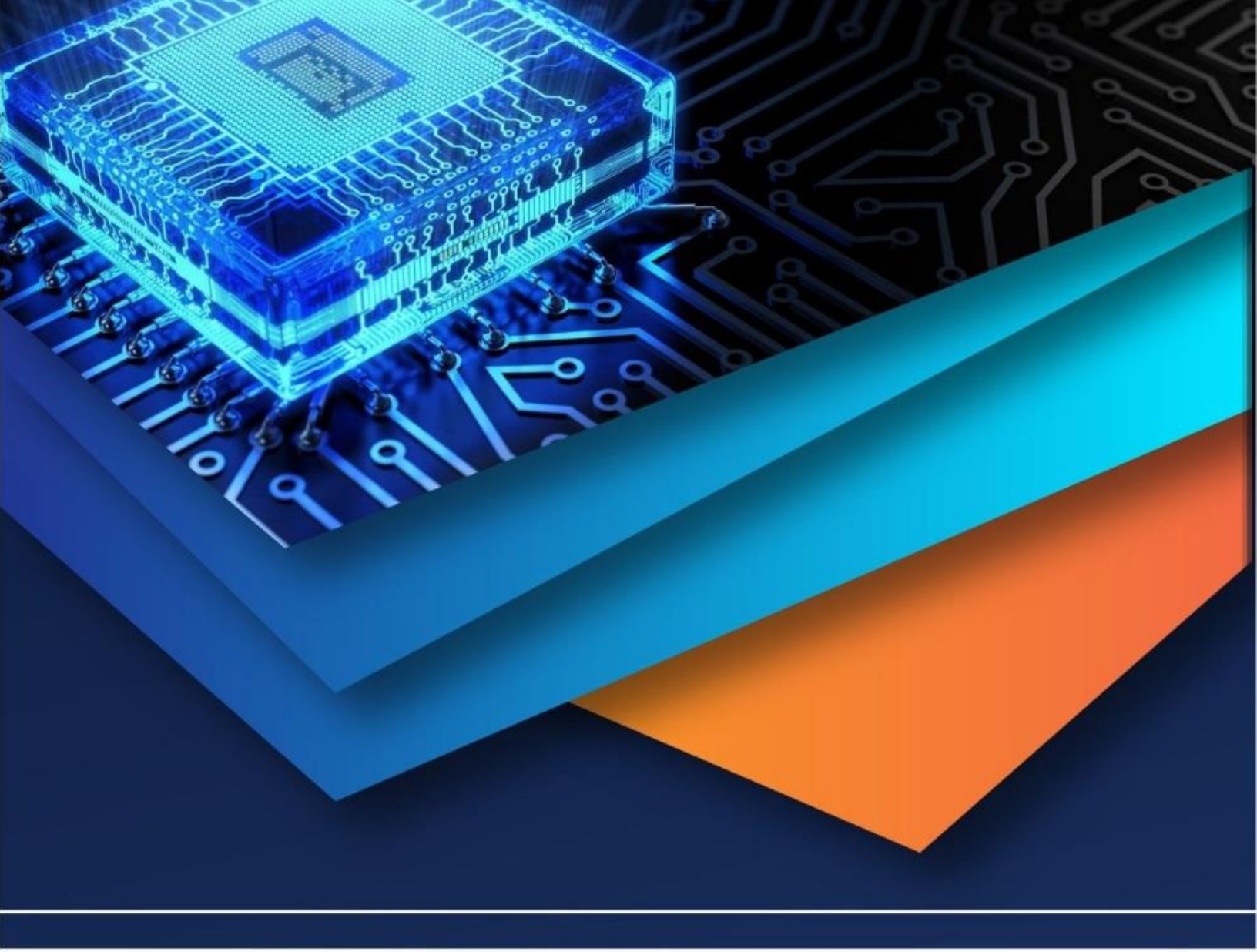
The mobile application, GeoPay extends secure transaction by using geolocation authentication and face recognition. The customer does not have to think twice while using the application due to its user friendly interface. This application provides additional authentication features unlike the other transaction applications. GeoPay includes security factors such as pattern matching ,security pin, face recognition, security questions as soon as the user tries to perform transaction other than the location registered. The user's privacy is given importance by all these additional security features.

Challenges faces are as follows

1) *Privacy and Security:* Invasion of personal data can be done in many ways, which involve application that first obtain access to transaction application, then start to monitor, control and tamper the personal information stored in the application. Transaction application often comes with never before known issues such as phishing attack, man in the middle attack, identity theft.

REFERENCES

[1] Rohit Joshi, "Location based authentication." International journal of latest trends in Engineering and Technology.
[2] Prince Gupta, Mahendra Hinde, "Location based authentication for E-banking" International journal of latest trends in Engineering and Technology.
[3] Satpute Pooja, Gunjal Ashwini, Tidake Bharati, Mulay Shital, Prof.Pawar S.E "Secured Bank Authentication Using Geo-Location Based System" International general for research in applied science and engineering technology April 2015.
[4] Dipak Auti, Krishna Landage, Swapnil Chavan, Dept. Of Computer Engineering K , Technical Campus Pune, India."Location Based Security for Online Transaction".International Journal of Innovative research in Computer and Communication Engineering 2016.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY