Integrated Approach for Increasing Security Level in Money Transactions through the Internet with GPS enabled Mobile Phones

C.S Rathnayake.
M.Sc Student (Geographical Information Systems & Remote Sensing)
Post Graduate Institute of Science (PGIS)
The Faculty of Science
The University of Peradeniya
Peradeniya
Sri Lanka
csaman@gmail.com

Introduction:

In early days people exchanged goods to carry out business transactions. Now in the modern world money is again disappearing and is being replaced by virtual money or E- Money (Digital Money).Modern Banking has rapidly changed because of e-Banking & e-Commerce.

Money transactions on the internet are always exposed to risks and Banks have to implement various security measures to avoid frauds.
The main purpose of the paper is to propose increase of security for internet-based transactions by using Global Positioning System (**GPS**) enabled mobile phones.

Customer can ask for additional security specifying that he requires additional security for his/her internet-based money transactions. The customer can instruct the bank to allow transactions only when he/she is within a geographic region or in a specific location. Bank can track the customer from his **GPS** enabled mobile phone and authorize his transaction by verifying by his local grid coordinates.

As an example if he has selected Sri Lanka as his geographic region the system will allow him to do transactions only when he is in Sri Lanka. System will track down his global position by checking his GPS enabled phone messages

Methodology:

Bank uses the normal customer database and an integrated **GIS** database to check location data and compares this information with data transmitted by **GPS** enabled mobile phone.

System Architecture

Actors Identification

1.Authorized User
The most active user of the system. Authorized users do money transactions on the Internet.

Use Case Diagram

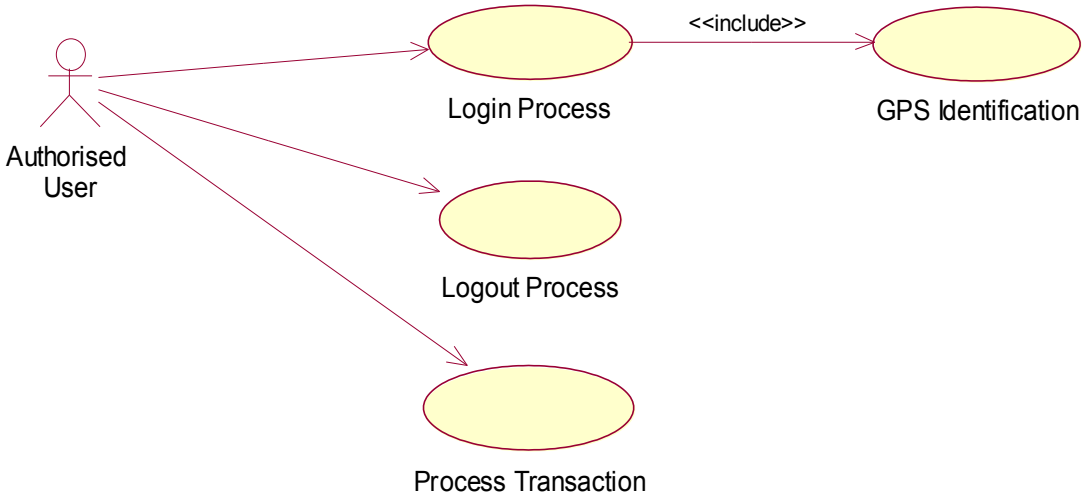


Diagram 1

Use Case Specifications

1. **Use Case Name – Login Process**

   Initial login process by using user ID and password to use the Internet Banking.

   Flow of Events

   1.1. Basic Flow

   This use case begins by presenting a log-in screen to the user as the initial screen of the system. The user is presented with provision to enter username, password to log in. The user enters his user ID, password and selects the desired program. Those data are validated. (If unsuccessful login, alternate flow 1.2 (a) is executed) After a successful login, the user will be redirected to get the GPS validation.

   1.2. **Alternate Flows**

   a) Login Unsuccessful

   The user can re-enter the login details, or terminate the use case.

2. **Use Case Name – GPS Identification**

   This is the step that system checks customers Global Positioning System coordinates and matches with his given geographic region or the location.

   Flow of Events

   2.1. Basic Flow

   After initial login process before continuing to the money transaction system generates an automated SMS to the customer telling him “You are going to do a transaction we need your location verification”.

To continue the money transaction process customer needs to reply this SMS to the Banking system with a specified time period. This SMS will be stamped with his location data. It means (**X, Y**) local grid coordinates.

2.2. **Alternate Flows**

a) **Time out.**
If the user is unable to response the system generated SMS, user will be automatically logged out. Transaction will be terminated.

b) **Location Mismatched.**
If the user's Global position is not matched with his security specified position, user will be automatically logged out.

2.3. Special Requirement

Bank has to negotiate with Mobile service providers to maintain a SMS service with Global Positioning System (GPS). SMS response by the customer has to be stamped with the local grid coordinates. Then banking system matches with the given region by the customer to apply the security.

3. Use Case Name – Logout Process

Log out by the system is done by the user after doing transaction successfully or abandon it.

Flow of Events

3.1. Basic Flow

The user does log out after doing the transaction successfully**.**

4. Use Case Name – Transaction Process

After verification user ID and password and GPS location system allows to do the transaction.

Flow of Events

4.1. Basic Flow

After verification user ID and password and system waiting for the SMS response and checks GPS location system then if the location matches allows doing the transaction

Activity Diagram

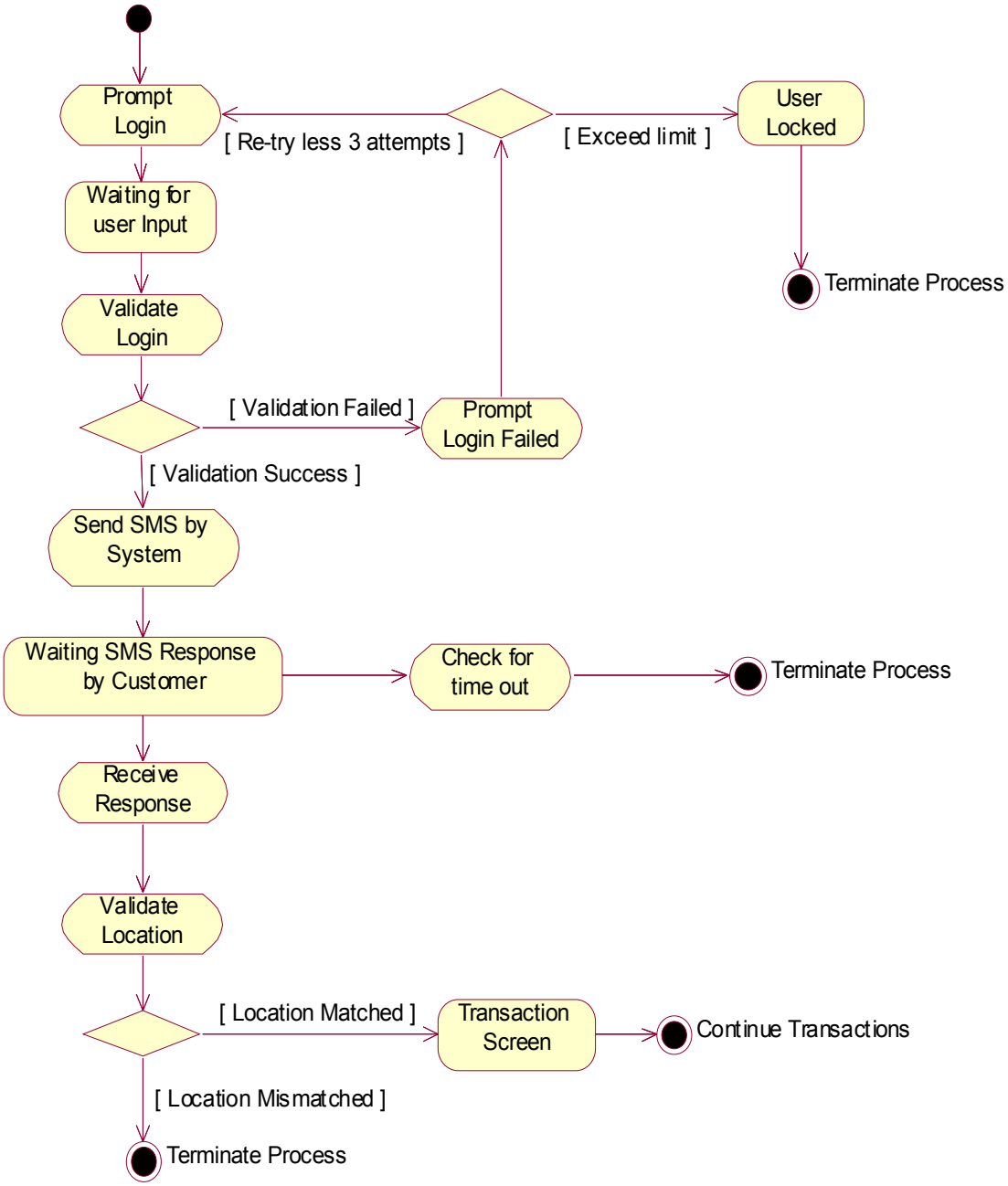
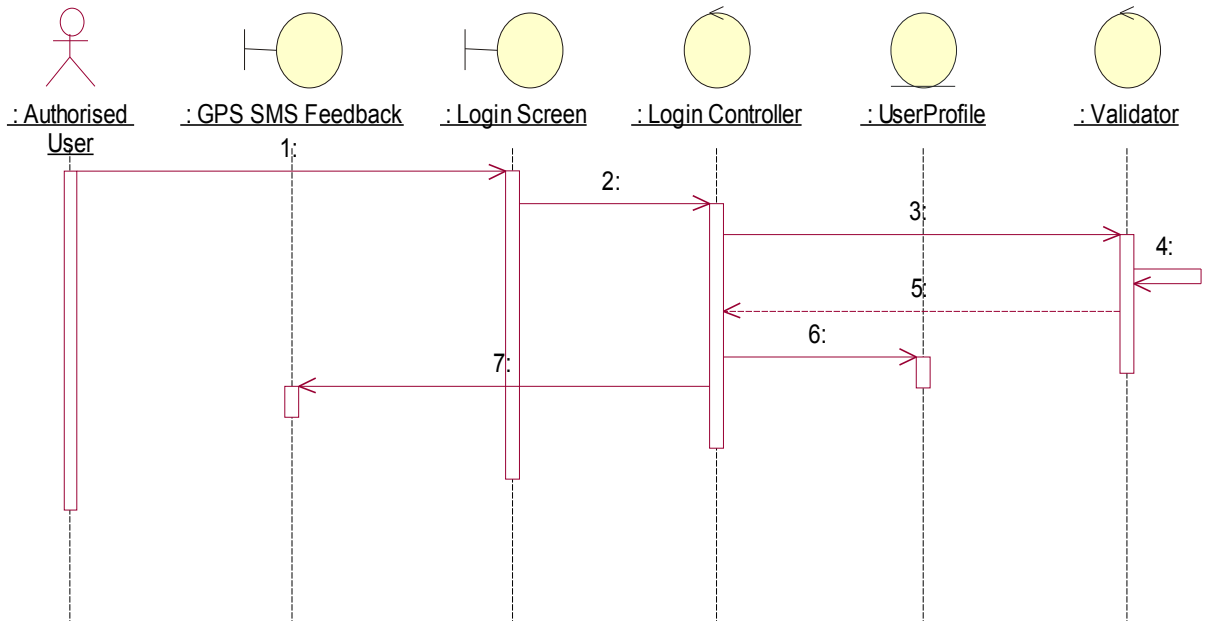


Diagram 2

Sequence Diagram fro Login Process (Success Path)

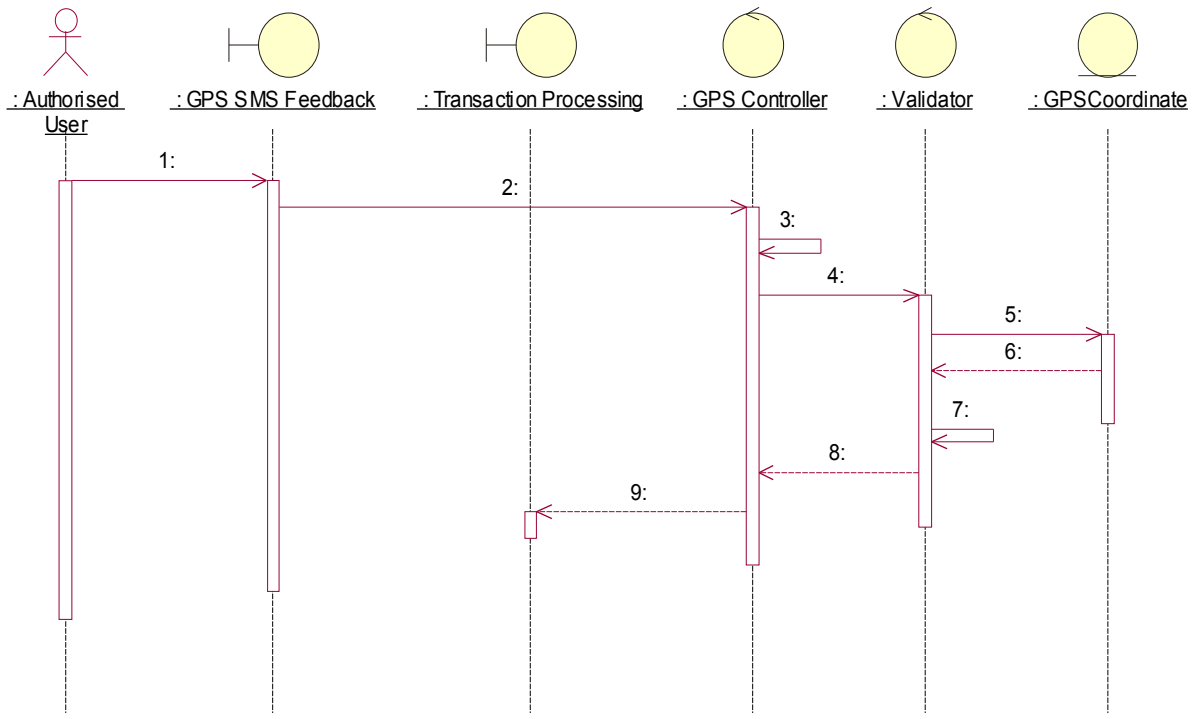


Sequence Diagram for Login Process (Success Path)

1. Accept User ID and Password
2. Send the User ID and Password
3. Send the User Id and Password for validation
4. Do User verification
5. Success feedback
6. Create User profile on success login
7. Send **SMS** for **GPS** verification

Diagram 3

Sequence Diagram for GPS Identification (Success Path)



Sequence Diagram for GPS Identification (Success Path)

1. Accept user **GPS** coordinates
2. Send coordinates to **GPS** controller
3. Check for the response time out
4. Send data for verification
5. Request user **GPS** information from database
6. Get user **GPS** information
7. Do **GPS** Validation
8. Validation feedback

9. Enable for transaction processing

Diagram 4

Findings & Discussions:

By adding this concept, additional security is included for the Internet-based money transactions.

Conclusions:

In very near future GPS enabled mobile phones will be popular. Then customers can use the GPS enabled facility to add additional security level to their accounts.