**IFSC 3360: System Analysis and Design**

**Final Project Report**

**Mobile banking application using two factor authentications**

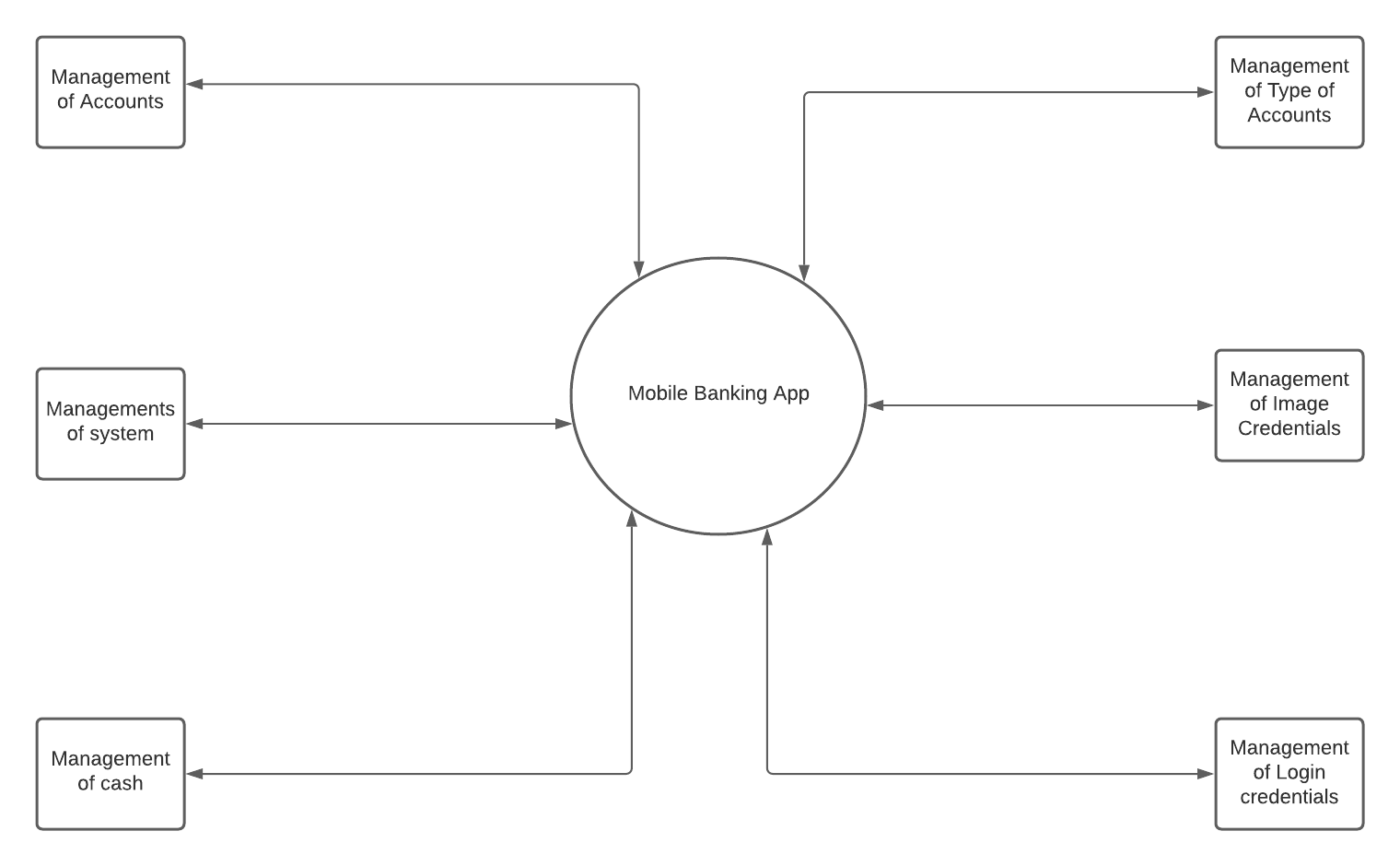
**Divyajitsinh Mahida**

# Introduction

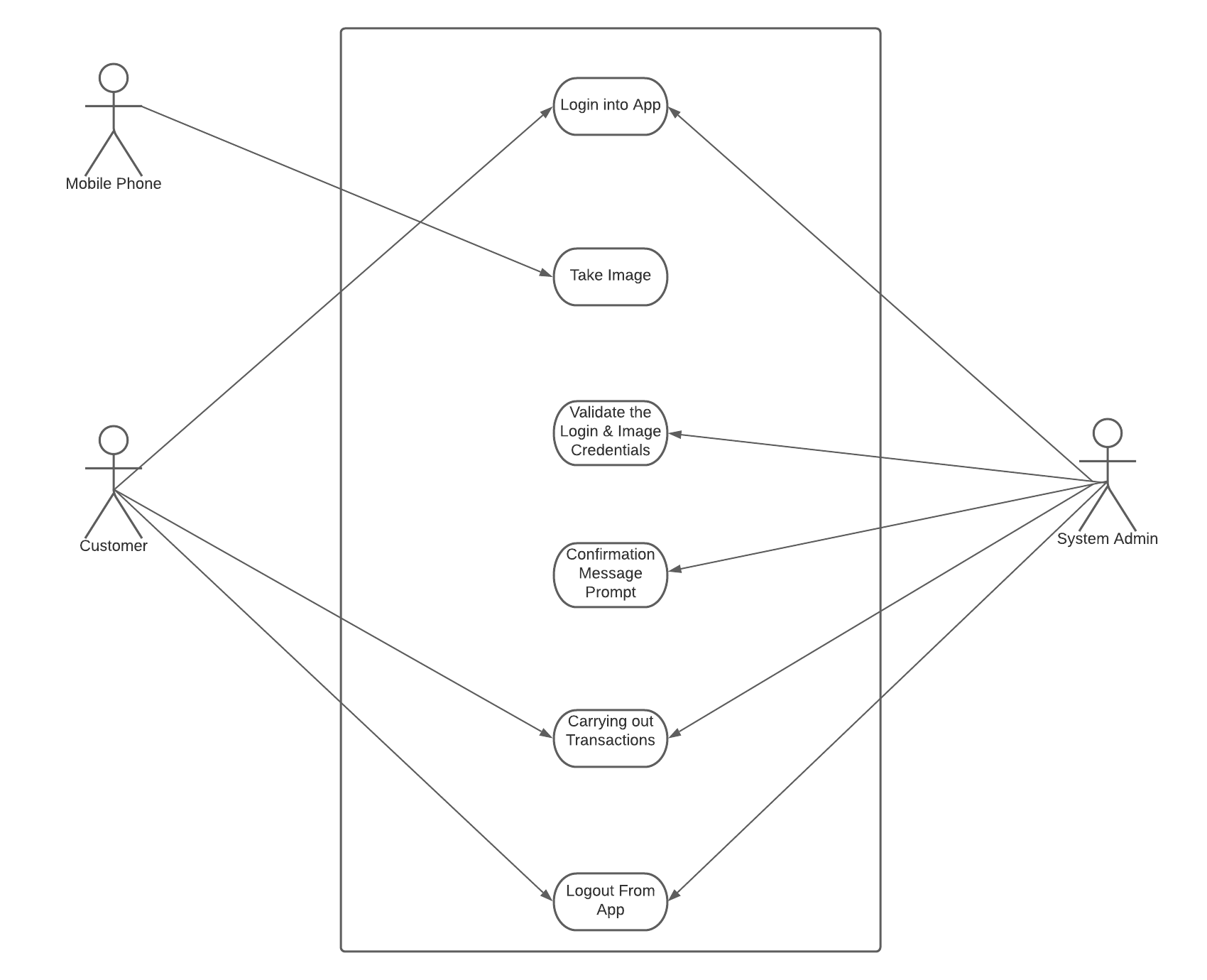
* So many of the peoples have a bank account in an android or an IOS phone. The idea here is, whenever a user enters in Mobile App of bank, he/ she has to enter login id and password with one more security label as Capture his/her picture. Then the picture is to be send to the database of the bank then confirmation to the login page and to the bank will be generated and if valid, user will get enter in the app otherwise it shows message that you are not authorized user try again. Major concern related to existing Mobile Banking application is “How to make Application Secure?” So as per Security is concern, we need to provide proper Authentication which is always costlier and major security flaw in the system. So, idea here is to implement security to the Mobile Application by capturing the user image and validating with the database to ensure the authentication of the process. This way your face can only open the app.
* I am improving the existing system. I do have knowledge about IOS face is security, but my idea is to capture the user photo. The application will capture the photo every time you try to login for the authorization.
* Because now days so many people are hacking into bank application to steal their money. Right now, the bank application is not that safe, but if we apply the photo security, it can improve the safety and security of your money
* The system will capture the user photo every time whenever they try to login there bank mobile application, and that photo will go to bank database to verify the user photo. If the photo matches, the app will let the user in.
* Most importantly in this kind of authorization no one will be able to hack or fraud the system with the other faces.
* After looking at the bank database the system will allow you to login in the bank mobile app.
* Every time this photo two factor authentication will require to login in to bank mobile application.
* We need this system because nowadays the mobile banking application is not safe. You can see articles regarding the security of the mobile banking application. Of the 781 data breaches tracked in the United States last year, 71 were banking-related, according to the [Identity Theft Resource Center](http://www.idtheftcenter.org/ITRC-Surveys-Studies/2015databreaches.html). Though that might appear to be a low incidence, it is double what was reported the previous year. **Fake banking apps are another major threat.** They look like the real apps of major banks, and they are designed to trick users into entering their login credentials. According to the FBI, this hacking technique represents “one of the fastest growing sectors of smartphone-based fraud.” If we use the system which I made, it will decrease lots of risk of hacking. Because my system will take live photos and will match the database of bank and then it will let you in. Its so much safer and better then right now face id or fingerprint authentication.

# 2. System Requirements Model

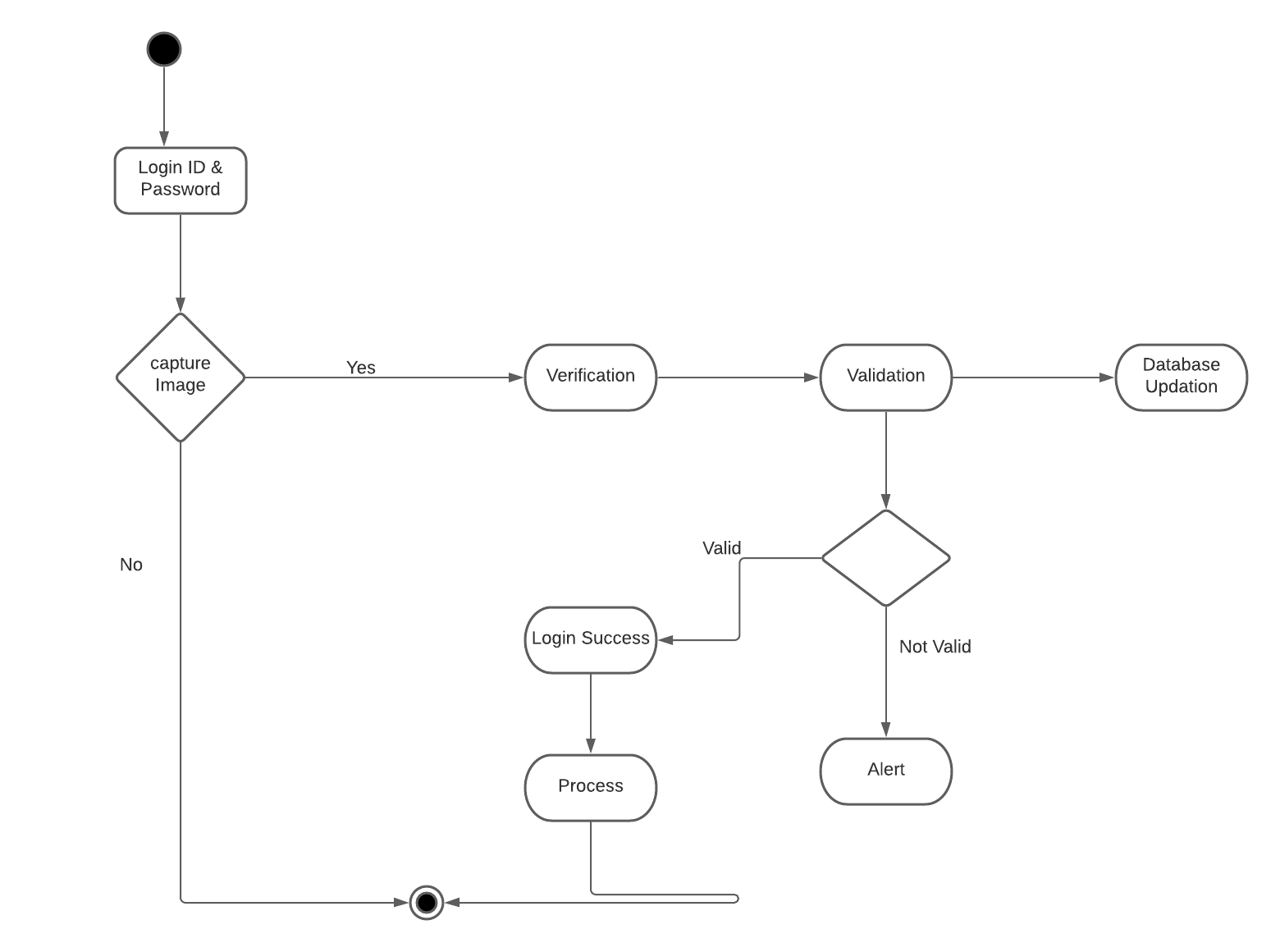
* Provide snapshots of DFD diagrams with brief high-level descriptions.



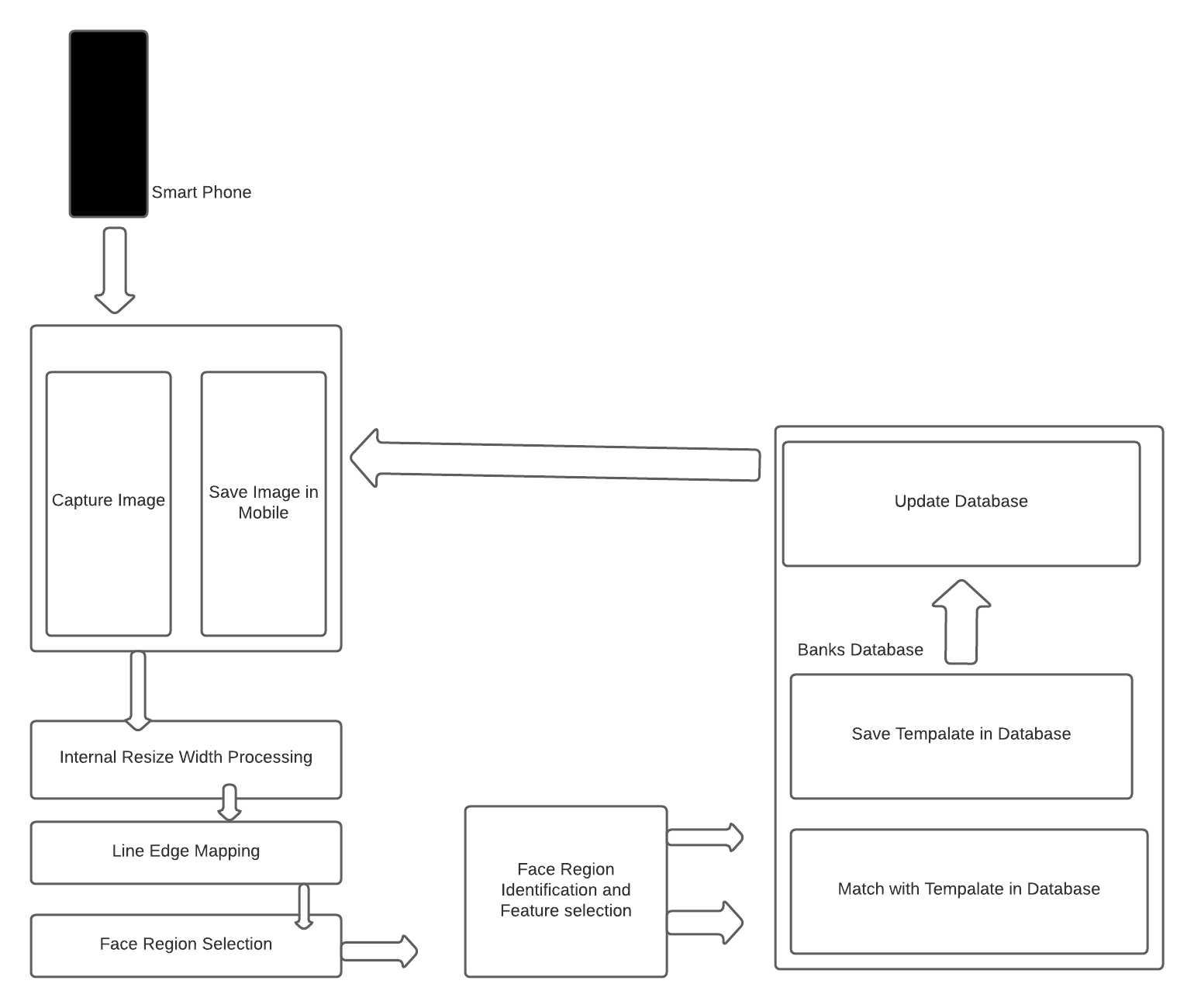
- Provide snapshot of the UML use case diagram of the entire system and a brief high-level description.



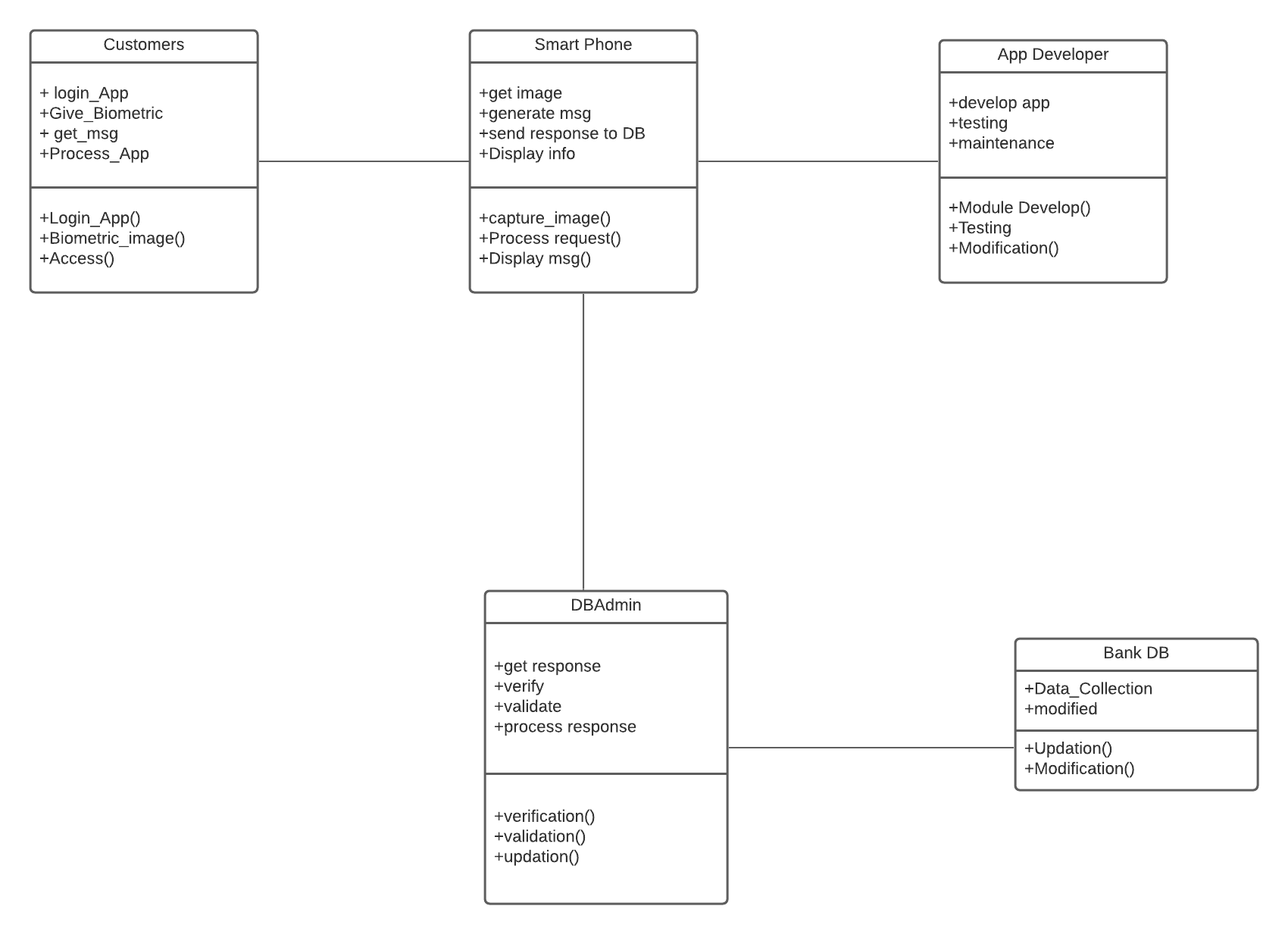
* Provide main/success scenarios, alternate scenarios, pre-conditions, and post-conditions for all the use cases.
* Here there are three actors namely: 1) Mobile Phone, 2) Customer, 3) System Admin
* Mobile Phone takes care of “Take Image” system use case.
* While Customer and System Admin must interact co – operatively in other use cases for a smooth experience
* Provide snapshot of the system sequence diagram (SSD) of the entire system and a brief high-level description.
* You can see in the sequence diagram the phone will capture the photo of the user and then if the photo is correct the system will verify and validate the photo in the database of the bank. After it gets valid it will let the user to login. And if the photo does not verify the user will get alert that the photo is not valid, and it will not let the other user log in.



* Provide snapshots of all sequence diagrams (SD) and brief high-level descriptions explaining how it realizes the use case scenario for which the particular sequence diagram was designed.
* You can see in the interaction diagram that the smart phone will capture the photo of the user, then the phone will save the photo in the database after capturing the photo the photo will go to bank database got face region selection, after the photo identify in the database the photo will update the bank database with new photo of yours. It will have the users all the photos as validation. Each photo of the user will update the bank database for the security. The interaction diagram will explain how does the use case scenario work with phone, customer, and system admin.



* Provide a snapshot of the class diagram for the entire system with a high-level description. Also explain the rationale of the associations, dependencies, and inheritance relationships using an example.
* The system consists of four classes namely Customers, Smart Phone, App Developer, DB Admin and Bank DB. Their attributes and functions are mentioned in the diagram. Class diagram is the fundamental building block of conceptual design of object-oriented modelling and data modelling. You can see in the class diagram that dependencies will be on the customer which will let the user login App and giving their biometric image. The smart phone will get the image and it will send it to the bank database for the verification also it will send it to the app developer for the modification and update. Finally, the photo will be verified in the bank database and it will give access to the user.



# 3. Lessons Learned

* If I has another shot, I have would have done this, Biometrics systems have found a worldwide use in branch banking, but still biometric technologies are evolving and emerging towards a large scale of use. Attempts are also being made to standardize common software interfaces to enable sharing of biometric templates and to permit the effective comparison and evaluation of different biometric technologies. Biometric systems still face the major challenge of securing the user's template. The templates represent the user’s personal characters and hence pose a threat to invading one's privacy if not stored properly. Also storing the template in a centralized database paves for attack and compromise. Biometrics does have a promising future in the next generation authentication and security systems. By adding more specific feature according to the need of security in mobile baking application can be enhanced by the developer. Because it is proven that every human has different retina no of the human has same retina. So, if we follow this idea no one would ever be able to hack into our any kind of systems.