

Secure Mobile POS System

A point of sale application for secure financial transactions in a mobile business environment

KAZI MASUM SADIQUE



**KTH Information and
Communication Technology**

Master of Science Thesis
Stockholm, Sweden 2013

TRITA-ICT-EX-2013:77

To my parents

Acknowledgements

At first I would like to thank to my respective supervisor, Professor Dr. Sead Muftic, for his guidance, advice and valuable feedback time to time to complete my thesis.

Thanks to my wife Mst. Sabina Yesmin for her help and patience throughout the thesis. Also for her review of a draft copy of this report, which contributed to my understanding of the written word and the overall readability of this text. All grammatical and spelling mistakes are my own.

Thanks to my two sons, Kazi Sadin Yousuf and Kazi Sabin Yousuf, for their patience and tolerance of my long hours absent from home.

Thanks to my parents, brother and sisters, whose constant love and support and encouragement for my higher education.

Thanks to my all the friends who help me during my research work with their valuable suggestions.

Finally, I would like to thanks to God for his blessings, that he gave me chance to study and completed my degree in KTH.

Kazi Masum Sadique

Stockholm, Sweden

Abstract

The use of smart phones has changed the lifestyle of the society. Almost all kind of useful tools you can find on your smart phone. People used to buy goods every day. And for the purchase of goods they must pay. Security is very important while payment is concern. In this thesis we have designed and demonstrated a mobile phone application that can be used for a small shop or a big market. For any kind of commerce application, three different kind of entities are mostly involved: the customer, the sales person, and the management of the shop. Our designed mobile application has three different interfaces for three different kind of users: Manager Interface, Employee Interface, and Customer Interface. An interface for the system administrator is also designed, which should be used as an desktop application on the point of sale server. This application is flexible with capabilities of different payment options. Our proposed design can be implemented in any smart phone environment for example Android, iOS or Windows phone. This design provides availability, confidentiality, and integrity of payment data.

Keywords: mobile point of sale, POS, secure financial transactions, m-commerce.

Abbreviations and Acronyms

APDU	Application Protocol Data Unit
API	Application Programming Interface
CA	Certificate Authority
DB	Database
DES	Data Encryption Standard
DS	Digital Signature
DSA	Digital Signature Algorithm
FIPS	Federal Information Processing Standards
HTTPS	Hypertext Terminal Protocol Secure
HTML	Hyper Text Markup Language
IDMS	Identity Management Server
IP	Internet Protocol
IPS	Identity Provider Server
MAC	Message Authentication Code
NSA	National Security Agency
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKC	Public-Key Cryptography
PKI	Public Key Infrastructure
POS	Point of Sale
RSA	Rivest, Shamir and Adleman
SHA	Secure Hash Algorithm
SA	Strong Authentication
SSL	Secure Socket Layer
SECLAB	Security Laboratory
TCP	Transmission Control Protocol

Table of Contents

Acknowledgements	iv
Abstract	vi
Abbreviations and Acronyms	viii
List of Figures	xiii
Chapter 1: Introduction and Scope	1
1.1 Overview	1
1.2 Problem Statement	2
1.3 Scope	2
1.4 Goals and Purpose	2
1.5 Research Methodology	2
1.6 Limitations.....	3
1.7 Audience.....	3
1.8 Thesis Organization.....	3
Chapter 2: M-Commerce Systems and Related Standards.....	4
2.1 M-Commerce Systems	4
2.1.1 M-Payments.....	4
2.2 Security Issues	4
2.2.1 Communication Security	4
2.3 Related Standards.....	5
2.3.1 Public Key Cryptography	5
2.3.2 CA Server	5
2.3.3 FIPS 196.....	5
2.3.4 NFC Technology	6
2.3.5 SAFE (Secure Application for Financial Environments)	6
2.4 Analysis of the Existing Applications	7
Chapter 3: System Design and Architecture	8
3.1 Roles.....	8
3.2 POS System Component	8
3.2.1 Manager Service Package.....	8
3.2.2 Employee Service Package.....	9
3.2.3 Customer Service Package	9
3.2.4 Main Server Management Package	10

3.2.5 Inventory/Database.....	10
3.2.6 Three Different Android User Interfaces.....	10
3.2.7 Windows Application for POS Administrator.....	10
3.3 System Architecture	10
3.3.1 Internal Architecture of the POS System	11
3.4 Message Transaction Cycle.....	12
3.4.1 Message Flow for the Customer's Mobile Application	13
3.4.2 Message Flow for Employee's Mobile Application	14
3.4.3 Message Flow for Manager's Mobile Application	16
3.4.4 Message Flow for the Administrator Windows Application.....	17
3.5 Use Cases	18
3.6 Object Based Model	19
3.7 Security Requirements	20
3.8 Security Features Analysis	21
3.8.1 Authentication	21
3.8.2 Confidentiality.....	21
3.8.3 Integrity	21
3.8.4 Non-repudiation.....	21
3.8.5 Authorization.....	21
Chapter 4: System Implementation and Demonstration.....	22
4.1 Development Environment.....	22
4.1.1 Java Technology.....	22
4.1.2 Android SDK.....	22
4.1.3 MySQL Server	22
4.1.4 PHP.....	22
4.1.5 Eclipse IDE.....	22
4.1.6 NetBeans IDE.....	23
4.2 Demonstration	23
4.2.1 POS Application for A Customer.....	23
4.2.2 POS Application for Employees	32
4.2.3 POS Application for Managers	33
4.2.4 Admin Application	34
Chapter 5: Conclusions and Future Work	37
5.1 Conclusions	37

5.2 Future Work	37
References	xv

List of Figures

Figure 2.1 Mutual Authentication using FIPS 196 Protocol [14].....	6
Figure 3.1 System Architecture of the Mobile POS System.....	11
Figure 3.2 Internal Architecture of the POS System.....	12
Figure 3.3 Message Transaction Cycle.....	13
Figure 3.4 Message Flow for Customer Application.....	14
Figure 3.5 Employee Application Message Flow.....	15
Figure 3.6 Message Flow for Manger's Application.....	16
Figure 3.7 Message Flow for the Admin Application.....	17
Figure 3.8 Use Cases of the System.....	18
Figure 3.9 Object Based Model of the System.....	20
Figure 4.1 Customer Login Screen.....	24
Figure 4.2 Main Screen for the Customer.....	24
Figure 4.3 Food List Screen.....	25
Figure 4.4 Single Food Item.....	26
Figure 4.5 Add Food to Order.....	26
Figure 4.6 Complete Order Screen.....	27
Figure 4.7 Order List Screen.....	27
Figure 4.8 Unpaid Orders List.....	28
Figure 4.9 Unpaid Single Order Detail.....	28
Figure 4.10 Payment Type Selection Screen.....	29
Figure 4.11 Credit Card Payment Option Details.....	30
Figure 4.12 Payment Confirmation Screen.....	30
Figure 4.13 Paid Order List.....	31

Figure 4.14 Paid Single Order Details.....	31
Figure 4.15 Unpaid Order List.....	31
Figure 4.16 Select Single Order for Payment.....	31
Figure 4.17 Employee Login Screen.....	32
Figure 4.18 Main Screen for Employees.....	33
Figure 4.19 POS Settings Screen.....	33
Figure 4.20 Device ID Configurations.....	33
Figure 4.21 POS Version Configurations.....	33
Figure 4.22 Manager's Login Screen.....	34
Figure 4.23 Main Screen for Managers.....	34
Figure 4.24 Admin Login Screen.....	34
Figure 4.25 Manager Registration Screen.....	35
Figure 4.26 Employee Registration Screen.....	36

Chapter 1: Introduction and Scope

This is an introductory chapter of this thesis. This chapter starts with the overviews of this research, where the area of research and its scope has been introduced. Then it describes the problem statement of this research, the goals and purpose, and the research methodology of this research. This chapter ends with limitations of the research, the audience of the research, and the organization of this thesis.

1.1 Overview

Rapid enhancements in mobile telecommunication technology and mobile handset technology have improved user experience. Now mobile phones are capable to process instruction faster as they are having powerful processor [7]. Also wireless communication technology has enhanced to 4G wireless broadband technology [8]. Current smart phones are capable to provide all the features of a desktop computer. All users of mobile phones are moving forward towards smart phones to make their life easy. As a result, the research and development of smart phone applications has opened a new field of study [9]. The m-commerce systems support sales and marketing of goods through the use of mobile phones [10]. Sales of goods over Internet through the use of mobile phones introduced the need of payment for the purchases of goods through the use of the same technology. As a result, a new payment method has been introduced, namely mobile payment or m-payment. The m-payment is the process of payment through the use of mobile device and wireless environment [9][10]. A POS system is involved in sale of goods and to register sales and payment information to a server [11]. Currently, there are several research projects concerned with secure mobile payment system, but none of them focused on a standalone mobile application that can be used as mobile POS system. And will also be capable to provide secure financial transaction features, which leads us toward the problem definition described in the next section.

1.2 Problem Statement

There are several proposed mobile point of sale architectures and designs. But, none of them has provided complete solution for all the roles (customers, sales person and managers) involved in any business organization where sales is the main concern. Also, the proposed solutions are not scalable with multiple types of payment capabilities. Therefore, the objective of this research is to design, implement and test a secure mobile point of sale application that provides interface for all the involved entities.

1.3 Scope

This thesis report describes a generic solution for any kind of business organization interested to enhance their business experience by using mobile technology. We have designed our application to provide support for different types of financial transaction capabilities. The scope of this thesis is to demonstrate a B2C (business to customer) mobile transactions using a mobile POS system.

1.4 Goals and Purpose

The goals of this research are to find out the critical issues for mobile financial transactions and to design a complete mobile point of sales application that can be used within any kind of business environment, where financial transactions are involved. As we mentioned above, mobile financial environment and its related fields are problematic. Our intention is to design an architecture that should be secure and also generic for any business environment and any kind of mobile platform.

1.5 Research Methodology

The research has been performed by following the Hypothetical-deductive module[5] and also the qualitative case study research methodology [6]. Design of the new architecture based on hypothesis and this hypothesis has been created after the case study of different existing secure financial transaction applications. After analyzing the existing problem situation and existing solutions, we have designed a new architecture that have been partly implemented and tested.

This research project has been organized in several steps, which are as follows:

- First, study the existing problem area and the existing solutions within the area.
- Secondly, analysis of those solutions in respect to problem area.

- Thirdly, design a new architecture that can improve the discussed problem area.
- Fourthly, implement a new secure application based on the proposed new architecture.
- Finally, analyze the proposed solution with respect to security vulnerabilities.

1.6 Limitations

Due to time limitations all the designed modules of the mobile application are not implemented.

1.7 Audience

Target audience of this thesis report includes small and large business organizations, those who are interested to improve their sales experience with the new mobile point of sale technology. Also financial organizations which want to enhance their banking facilities with the business organizations using mobile transactions. This thesis will also be helpful for future research within the field of secure mobile financial transactions and secure mobile point of sale systems.

1.8 Thesis Organization

The structure of this thesis report is the following:

In Chapter 1 we have described the current situation of Point of Sale (POS) systems and mobile financial transactions. We have mentioned the problem area within the mobile transactions. Also the goals and purpose, the research methodology, the limitations have been discussed. At the end, we have mentioned target audience and the structure of this thesis.

In Chapter 2 we describe the area of research in detail. We have also mentioned the related standards for this research.

In Chapter 3 we give the detail design and system architecture of the Secure POS System. We have also analyzed the security features of the proposed system.

In Chapter 4 we describe current implementation and demonstration of the secure mobile POS system.

In Chapter 5 we present conclusions and future work within the research area.

Chapter 2: M-Commerce Systems and Related Standards

In this chapter the m-commerce systems has been described. Also the related standards that have been directly and indirectly used in this research are described.

2.1 M-Commerce Systems

An m-commerce system is defined as a system which is involved in money transactions over the wireless environment [10]. In an m-commerce system the business is performed using mobile devices. An m-commerce system can have the same types of business transactions like the e-commerce system. The main transaction types are as follows:

B2B (business to business): A B2B transaction is performed when two different business organizations make transaction between them. For example, a B2B transaction could be between restaurant and a grocery shop. A restaurant can make order and pay bills to a grocery from whom they buy fresh goods to make the food.

B2C (business to customer): The B2C transaction is performed when a business organization makes transaction with a customer. A B2C transaction could be between a restaurant customer and the restaurant itself.

2.1.1 M-Payments

m-payment is the payment system that uses mobile environment to make any kind of payment [10]. It could be an electricity bills or a restaurant bills that a customer can pay using his mobile device.

2.2 Security Issues

Security is a very crucial issue while payment data need to be transferred between different entities of the payment system.

2.2.1 Communication Security

In this application users and server communication will be established via communication link through Internet. But, Internet channel is not a secure network. We can use HTTPS (Hypertext Terminal Protocol Secure) for getting a trustful and secure network. HTTPS provides encrypted communication in a insecure channel. It is a combination of HTTP with

the SSL/TLS protocol [13]. HTTPS uses a certificate which is a public key certificate and contains public key. And the certificate is signed by the trusted Certificate Authority (CA). A secure tunnel is established between user and a communication server. HTTPS ensures protection from eavesdropping and man-in-the-middle (MITM) attack.

2.3 Related Standards

In this section we have described the related standards that are used for design and implementation of a secure mobile POS system.

2.3.1 Public Key Cryptography

There are two main types of cryptography mechanisms, such as symmetric key cryptography and asymmetric or public key cryptography. For message encryption and description, both sender and receiver use the same secret key in symmetric key cryptography mechanism. Key management is a big problem of symmetric key cryptography when it communicates in an insecure channel. But, public key cryptography has solved key management problem. In public key cryptography, sender and receiver use different keys for message encryption and description process: private key and public key are used in this mechanism. Private key is used to keep privacy of the owner. The reason for this is that only private key owner knows the key. Public key cryptography is used in key management process and also in signature of application [13].

2.3.2 CA Server

CA (Certificate Authority) has an authority that issues digital certificates to web clients and servers. Many public key infrastructure (PKI) use CA. The provider information of the digital certificate requester is verified by the CA in a PKI [14].

2.3.3 FIPS 196

FIPS (Federal Information Processing Standards) is a standard for strong authentication protocol which gives secure authentication in the field of public key cryptography. This protocol is used for mutual authentication process. Using this protocol with mutual authentication process, we can prevent masquerade, password compromise, and replay attacks[14]. Authentication protocol is described in Figure 2.1.

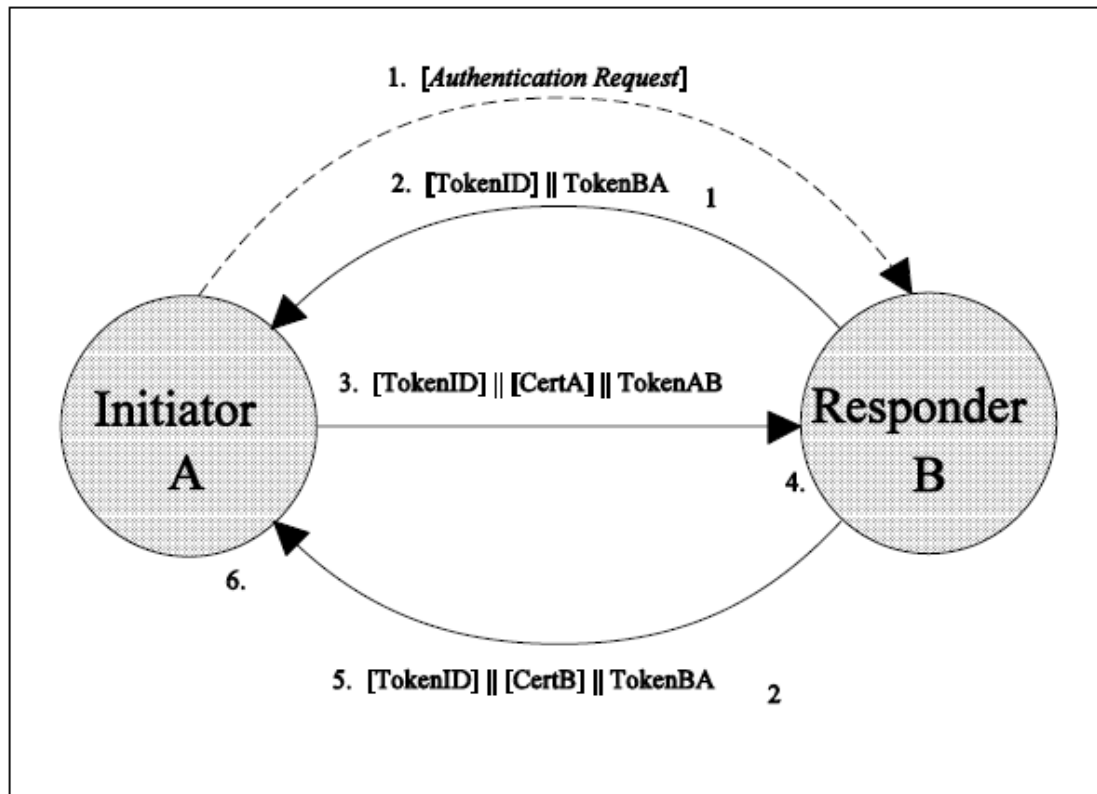


Figure 2.1 Mutual Authentication using FIPS 196 Protocol [14]

2.3.4 NFC Technology

NFC (Near Field Communication) a connectionless communication process that allows communication between devices, like smart phone and tablet. The new smart phones are mostly NFC enables phones [15].

2.3.5 SAFE (Secure Application for Financial Environments)

SAFE is a secure, reliable and convenient application that provides mobile financial transactions. SAFE performs various type of financial transactions like m-Banking, m-Commerce, m-Ticketing, m-Parking, m-Loans etc by using mobile phone or other hand-held devices. It performs transaction between multiple banks, person to person, client to merchant payments, and also non-banking mobile applications. SAFE system also supports to use mobile prepaid accounts. It is one of the main feature of SAFE system [2] [3].

Different types of participant provide different type of services in SAFE system. Banks provide registration, certification and financial services, security services providers provide security services and clients initiate or receive financial transactions. All participants need to be registered with the SAFE system. All participants' registration data is stored in IDMS

(identity management system) server. All identifications information data in IDMS is encrypted to prevent the identity theft attack .Every participant has certificate in SAFE system, based on registration stored in IDMS server. Certificate issued by CA server and the certificates are storied in mobile phone or smartcard. SAFE system uses public key cryptography for security of all transaction. After registration, certification and issuance of smart cards, SAFE system is prepared for doing various financial transactions in security way [1][2][3].

Our application is a continuation of the SAFE application so here we will follow the Generic, Secure, and Modular methodology for the development of secure mobile application.

2.4 Analysis of the Existing Applications

Several research projects have been done on mobile payment systems. But, not that many researches are focused on a generic model for the POS system.

Allan P. et al. [11] has done their research on ‘Designing a Secure Point to Sale System’. In their research they have designed point of sale system based of common criteria. This is mostly a theoretical research. The good thing of the POS system model with input and output data flow. In input data flow, POS application has bar code scanner, keyboard and payment terminal and for output data flow it has printers and display. But it is based on implementation and evaluation of design system. Also, the designed POS system is not for mobile environment.

Another research by Carl and David [7] described ‘A Secure Wireless Point of Sale System’ where researchers have described mobile POS system using the Infra-red. They have described wireless POS system, but they use a stationary device in POS of this research.

All other articles that we have studied are only about secure mobile financial payments. None of those researches was done for designing a new flexible, user friendly and mobile POS application.

Chapter 3: System Design and Architecture

In this chapter we describe the proposed system architecture. The details of this architecture have also been described here. At the end of the chapter, the proposed solution has been analyzed in respect to security.

3.1 Roles

A POS System includes different entities. The possible roles working in a POS environment are as follows [11]:

Customer: Customers are the buyer of goods. Customers make orders for goods and pay for goods.

Sales Person: Sales persons use POS device to select goods and to make bills for the customer. Sales person also requests payment to the customers.

Manager: Managers are authorized persons who check the inventory, add/modify items in the inventory, and check financial transactions.

Administrator: Administrators are used to install, maintain and configure POS system. In some cases administrators also add users to the systems. An administrator needs to be a trusted person.

3.2 POS System Component

Depending on the roles stated above, we have considered the following components in our designed POS system. In this section we describe different component of the secure mobile POS system with their functionalities.

3.2.1 Manager Service Package

Manager service package performs operations that could be done by the managers. Manager service package consists of the following functionalities:

- Login/Logout
- View the Inventory
- Add Employee (Add Emp)

- Add Item to the Item list (Add Menu Item)
- View Sales Report
- View/Modify Employee List

3.2.2 Employee Service Package

Employee service package includes the operations that could be done by the employee of any business organization. The functionalities for an employee package are as follows:

- Login/Logout
- Make order for the Customer (Order)
- Modify the existing order (Add to Order)
- Print a check (Print a check for an order)
- Pay for a customer
- Add new Customer (EditCustomer)
- View Member Information (Member Search)

3.2.3 Customer Service Package

Customer service package includes the following functionalities:

- Login/Logout
- View the Food menu
- Make order from Mobile Device (Order)
- Modify existing order (Add to Order)
- Make payment online
- View/Recall an old order (Recall an Order)
- View/Print Check online (Print a check for an order)
- Make Payments using the same Application

- Become a Member of the Shop (Edit Customer)

3.2.4 Main Server Management Package

The main server management package handles communication and security issues of the system. Several communication and transactions are performed by this package.

3.2.5 Inventory/Database

Inventory/database holds the information about the items that are sold in that business. It also keeps record of transactions. Transaction information are saved in transactions database. The information about the users are kept in the IDMS database.

3.2.6 Three Different Android User Interfaces

We have designed and developed three different mobile applications for three different kinds of users. Customers, employees and managers have their own applications to access the POS server.

3.2.7 Windows Application for POS Administrator

For admin user we have developed a Windows based application. Admin users use that application to add or modify user information to the Local IDMS Server.

3.3 System Architecture

System architecture of our designed POS system is given in Figure 3.1. In our design the admin user uses stationary computer to enter user data to the local database. Managers use their smart phone or tablet devices to login to the POS system. Employees also use mobile devices. In some cases employees may have extra POS device for handling the payment by the customer. Employee's mobile device should have NFC (near field communication) capabilities to handle mobile payment from the customer with NFC enables mobile devices. CA server provides certificates to the entities. Our designed system is connected to the SAFE system. If a user has a SAFE account, then he/she can pay their bills using their SAFE account. The designed system is also connected to the bank IT server to handle payment of the customer.

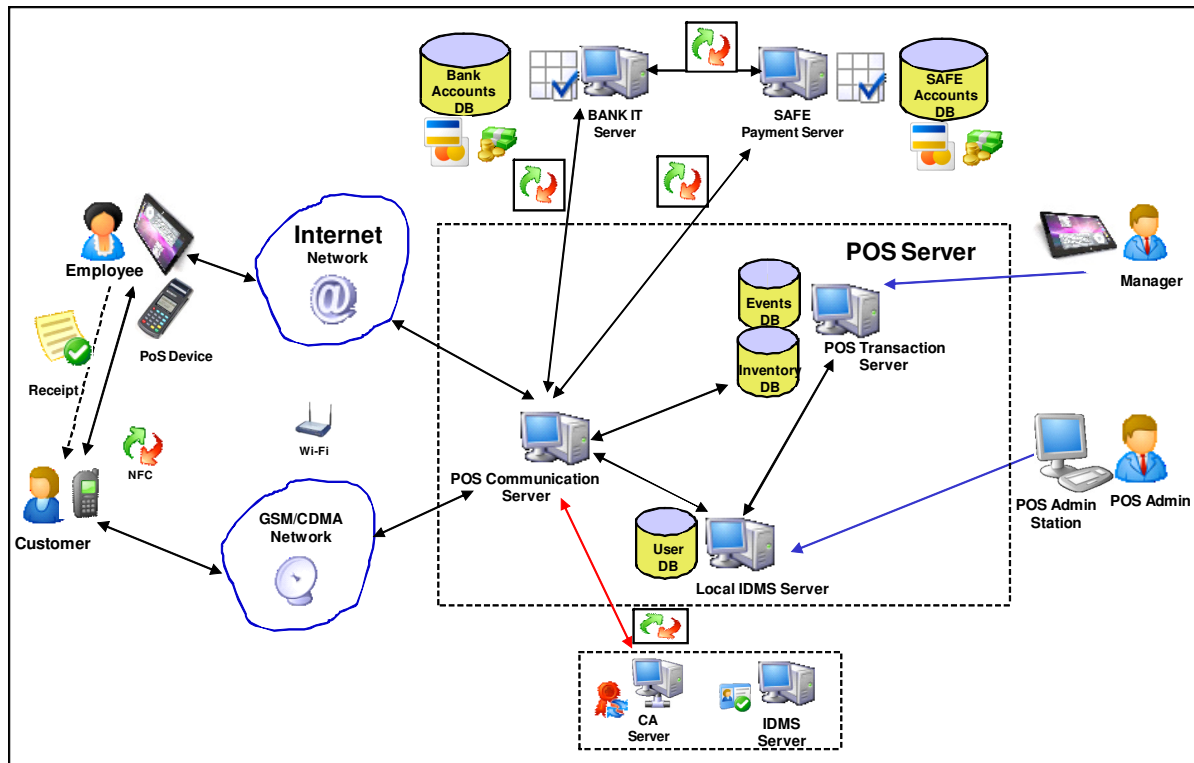


Figure 3.1 System Architecture of the Mobile POS System

3.3.1 Internal Architecture of the POS System

The internal architecture of our designed POS server is given in Figure 3.2. POS server includes the following components.

- Inventory
- IDMS database
- Security Manager
- Transaction manager
- Communication Manager
- Admin Service API
- Manager Service API
- Employee Service API
- Customer/Client Service API

The three mobile client applications (Manager application, employee application and customer application) connect to the system through their respective APIs.

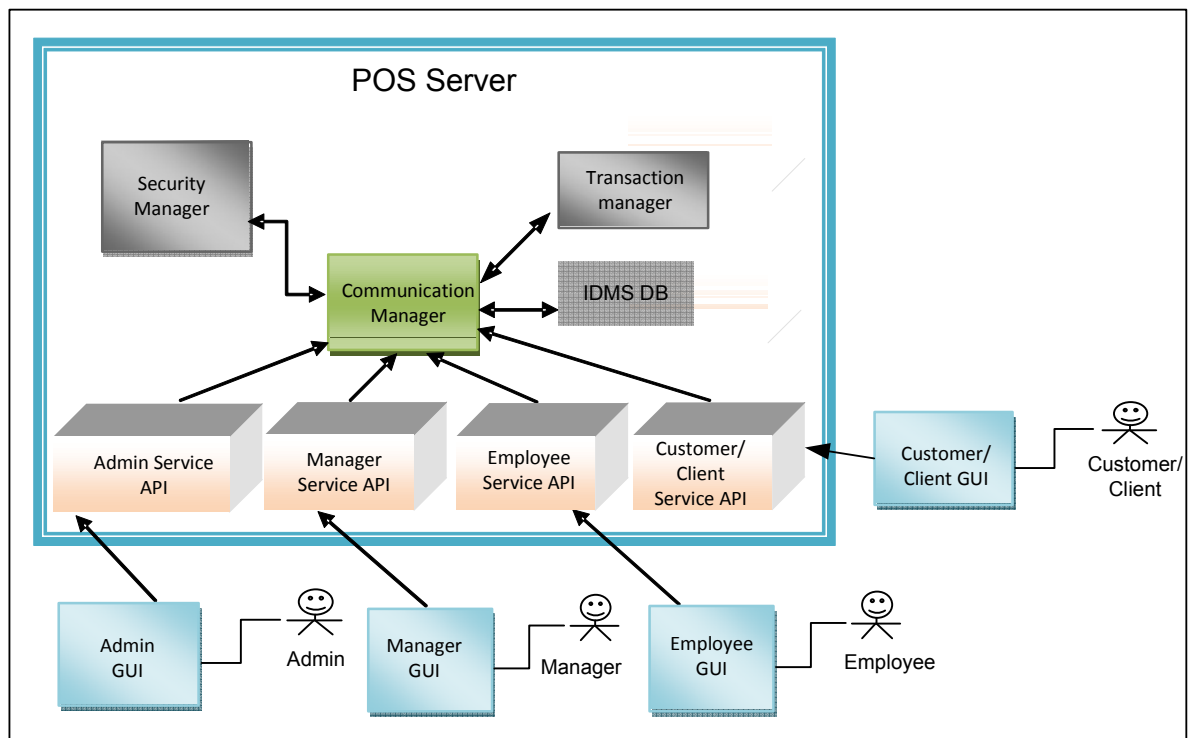


Figure 3.2 Internal Architecture of the POS System

3.4 Message Transaction Cycle

Message transaction cycle is shown in Figure 3.3. We have considered a situation where a customer pays his/her bills using SAFE account. Generalized common message flow between the customer, our designed POS server, and the SAFE server is the following:

1. Request for registration/authentication
2. Registered/authenticated
3. Request for services
4. Service response
5. Request for payment
6. Payment confirmation

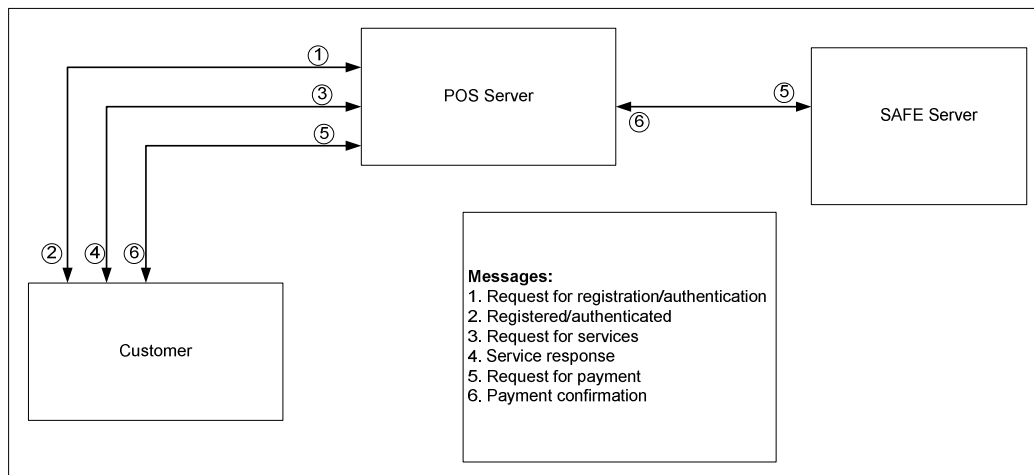


Figure 3.3 Message Transaction Cycle

Message flow diagram for each of the entities is described below.

3.4.1 Message Flow for the Customer's Mobile Application

Customers use mobile devices to see the goods at a store. Message flow is shown in Figure 3.4. Common messages for the customer's mobile application are:

1. Customer searches for goods

At first, customers search for goods at the inventory of the store. They send request for goods list and get back the goods list.

2. Customer orders for goods

With this message, customer sends order to POS server. Customers select the goods and quantities using their mobile device and send the list of goods selected for the order.

3. Customer pays bills

Customer pays bills for the ordered items using mobile client. The customer can pay using their SAFE account (if they have any) or they can use their own bank account to pay the bills. In some cases the customer can also pay bills using their mobile operator. In that case the bills are paid using customer's prepaid/postpaid mobile account.

4. Server sends payment confirmations

The server sends payment confirmation to the customer for a successful/unsuccessful payment.

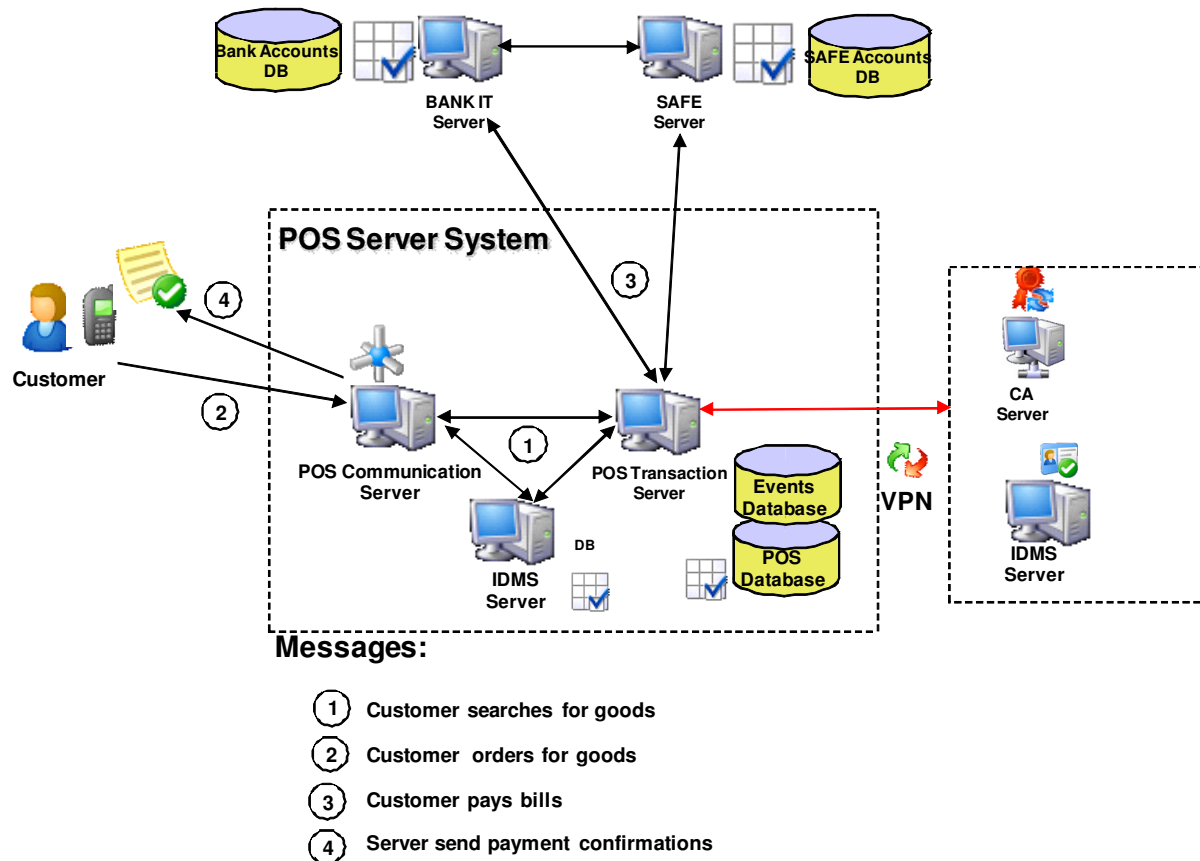


Figure 3.4 Message Flow for Customer Application

3.4.2 Message Flow for Employee's Mobile Application

The message flow for employee's mobile application is shown in Figure 3.5. Common messages for the employee's mobile application are:

1. Employees search for goods

When a customer comes to a shop and request for goods to the employee. After that, employees search for the goods to the inventory of the store and get back the list of items.

2. Employees order for goods

With this message, employees send order to POS server. Employees select the goods and quantities using their mobile device and send the list of goods selected for the order.

3. Employees send bill to customer

When order is complete, then employees send bill to customer using NFC based mobile devices. In some cases, bill may be sent over Bluetooth connection, depending on the requirement of the users.

4. Customer uses their NFC mobile phone for payment

Customer uses their NFC mobile phone for payment of bill, received in the previous message from the employee's mobile device.

5. Server sends the payment confirmation

After getting the payment confirmation from the payment servers, the POS server sends payment confirmation to the employee's mobile device.

6. Employee sends the payment receipt to customer's mobile

When the employee gets the payment confirmation from the POS server system, then he/she sends the receipt to the customer's mobile device using NFC or Bluetooth technology.

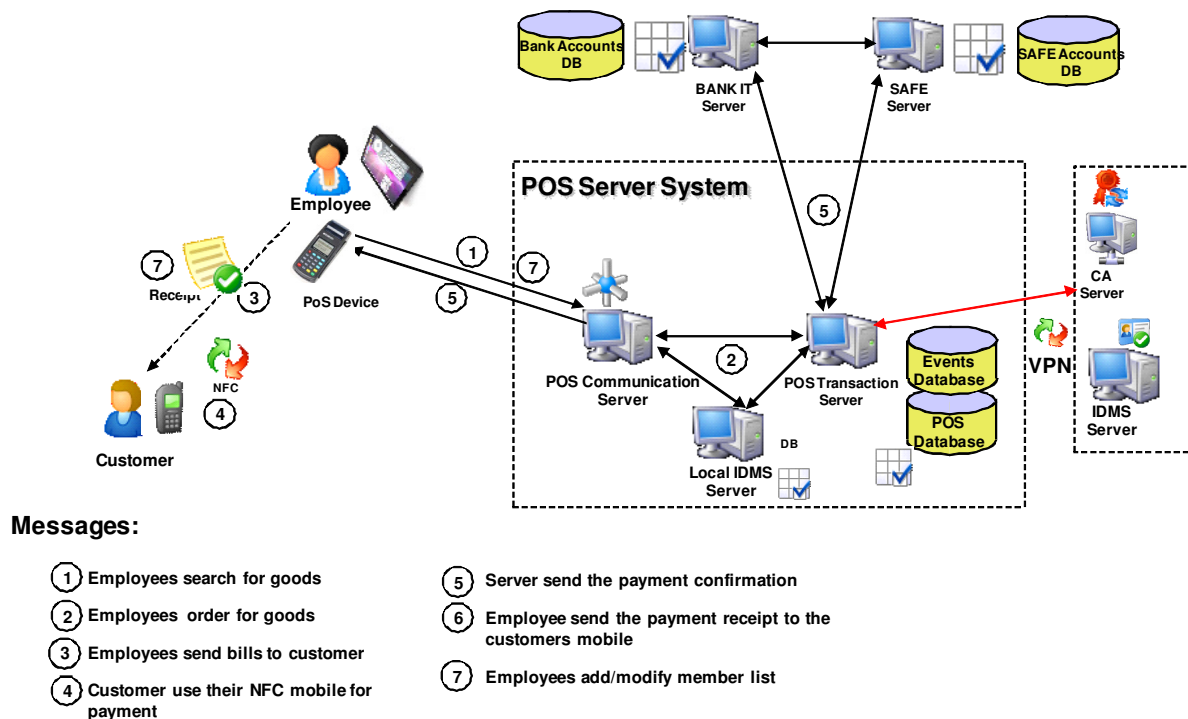


Figure 3.5 Message Flow for Employee's Application

7. Employees add/modify member list

When a customer wants to be a member of the store and make a request to the employee, then the employee add the member to the store's member list. In case of any modification request from the members employees also modify member's information.

3.4.3 Message Flow for Manager's Mobile Application

Message flows for manager's mobile application is shown in Figures 3.6. Common messages for manager's mobile application are: .

1. Add items to the inventory

Managers of the stores add/modify items to the inventory. The message in between the server and the client's mobile device is quite state forward. The managers sends the add item request to the server and the server sends confirmation of successful add/modify of items to the inventory.

2. Check sales report

Managers check sales report of the store by this message. Manager's mobile device sends a request for the report of sales to server and the server sends the report.

3. List transactions

Managers can ask the server for a list of transactions. The manager's mobile server sends a request to POS server for the list of transactions and server sends the transaction list to the manager's mobile device.

4. Add/modify employee's information

Manager's may be interested to add/modify the information of employees. In that case manager's mobile device send message to the POS server. POS server sends the confirmation of add/modify employees information to manager's mobile device.

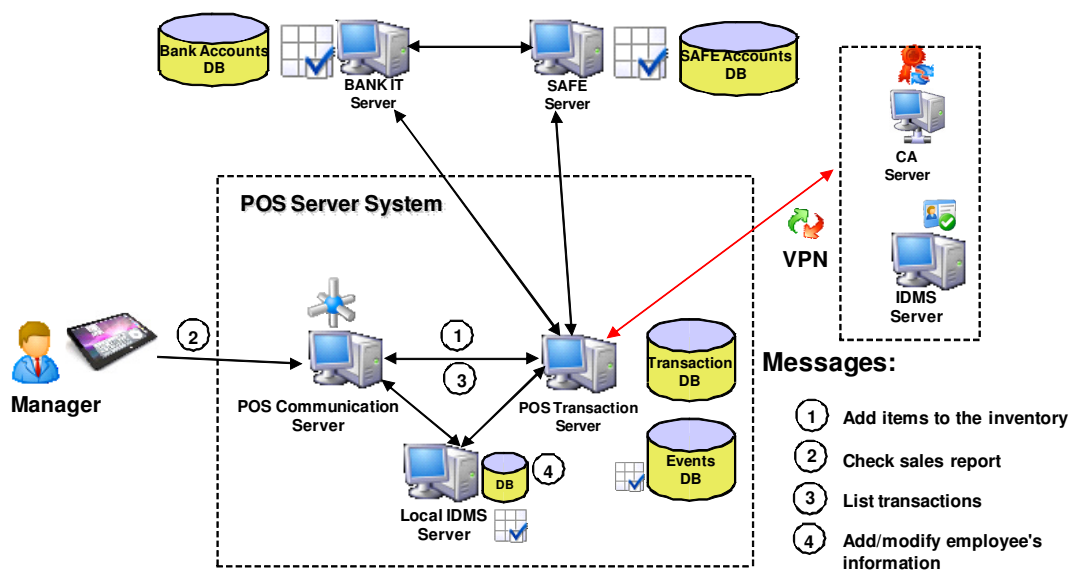


Figure 3.6 Message Flow for Manger's Application

3.4.4 Message Flow for the Administrator Windows Application

Figure 3.7 shows message flow for the admin user application. Common messages for the administrator's application are:

1. Add/modify manager's information

Administrator of POS system add/modify manager's information to POS server using this message. POS server sends response of success/failure of requested modification.

2. Add/modify employee's information

Administrator of the system also add/modify employee's information to POS server. POS server confirms success/failure of requested modification.

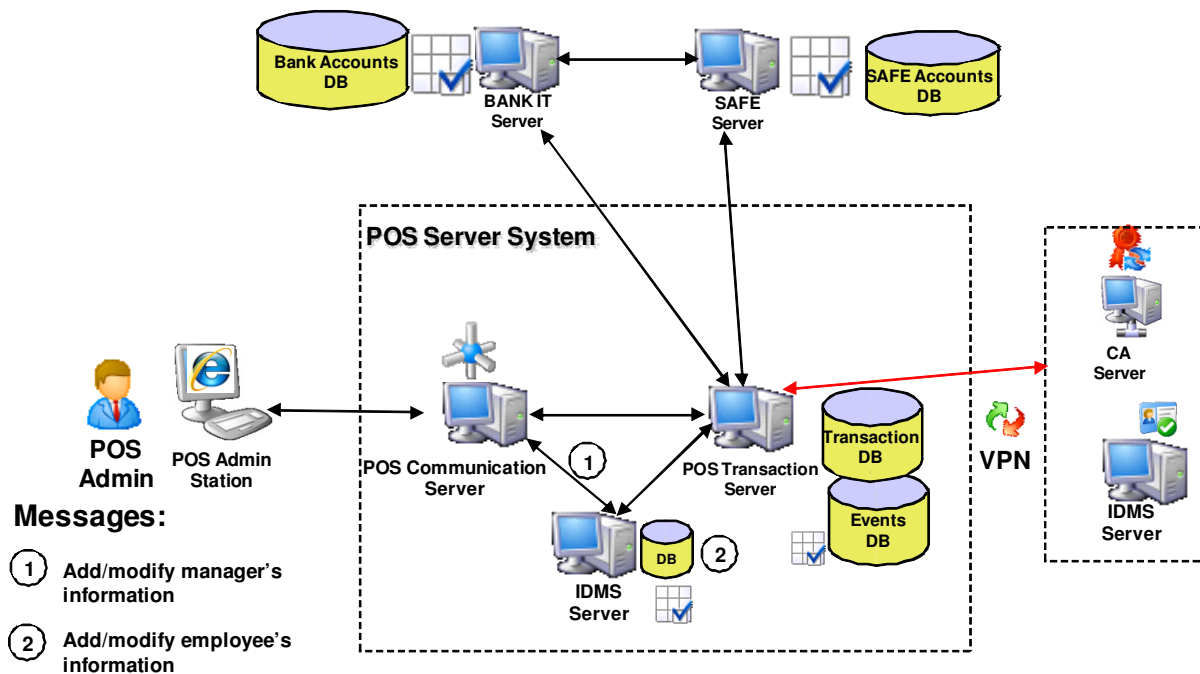


Figure 3.7 Message Flow for the Administrator's Application

3.5 Use Cases

Use Cases diagram shows overall uses of the mobile POS system. The different operation performed by customers, employees, managers and administrators are clearly shown in Figure 3.8.

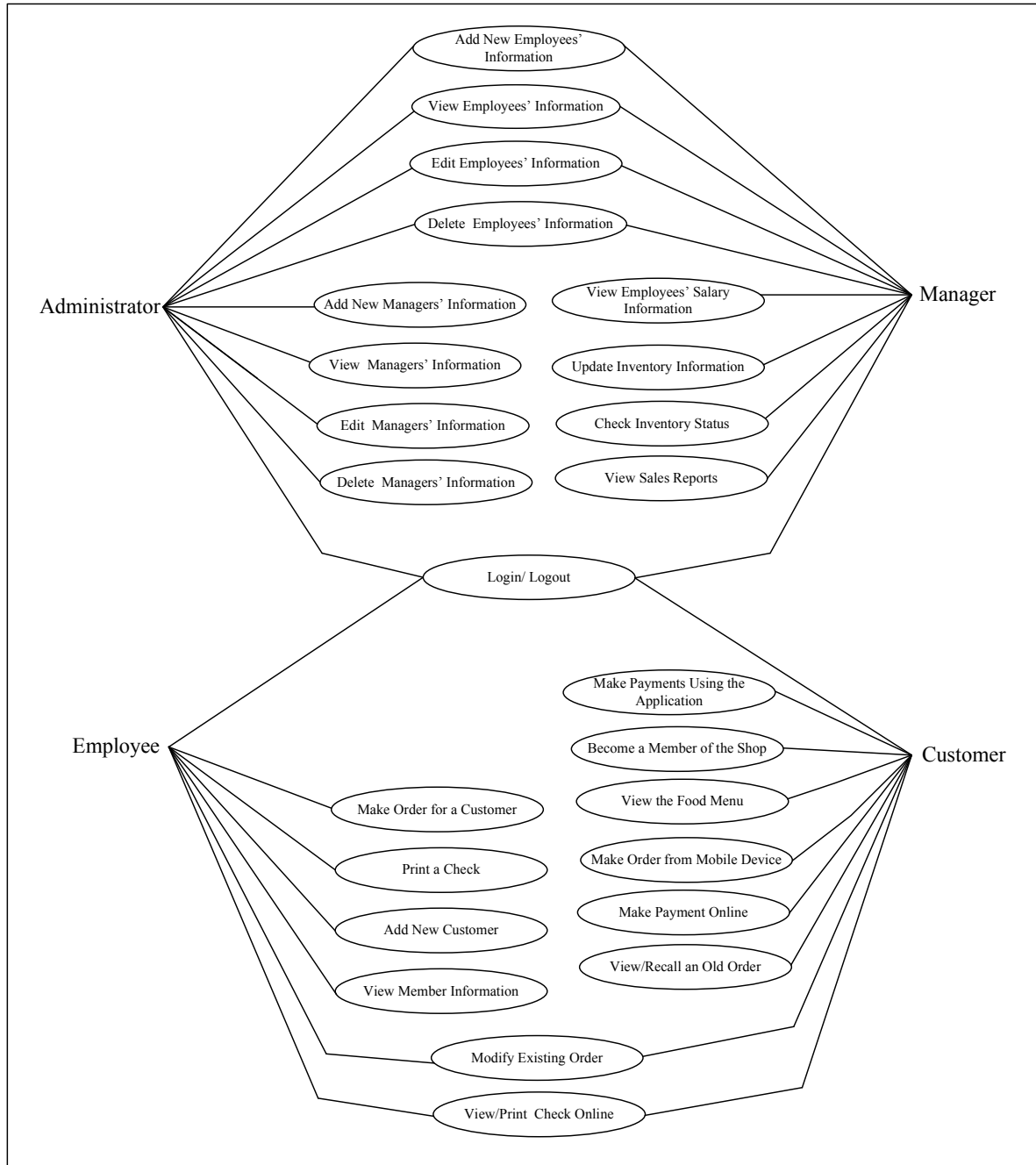


Figure 3.8 Use Cases of the System

3.6 Object Based Model

Object based framework of the proposed payment system using SAFE server is shown in Figure 3.9. There are six main component of the model: Mobile Client, POS Server, SAFE Server, Trusted Certificate Authority, Restaurant's Bank, and Customer's Bank. All these components are connected through Internet. Trusted Certificate Authority, SAFE server and the banks are connected to each other by secure virtual private network connection.

Mobile Client Application, POS Server, and SAFE Server has their own security manager. Those security managers are responsible for authentication, key management and certificate management.

Mobile client has user interface manager object, which handles all factors related to user interface of the application. Communication manager object in mobile client and connection manager object in POS server are responsible to handle the communication between these two modules. The concurrency manager in POS server handles concurrent access to inventory by different users of the mobile application.

Log manager in SAFE server keeps log of transactions. Trusted Certificate Authority issues certificate to users. Customer's bank and restaurant's bank are also connected to the POS server and SAFE system for financial transactions in between them.

In case of transaction through SAFE server, mobile POS server communicate with the SAFE server for payment process. In other case, when a payment is not done using customer's SAFE account, POS server directly communicate with bank's IT server. Request manger object in POS server checks the request type and decide the process of communication to other organizations (SAFE server, bank's IT server etc).

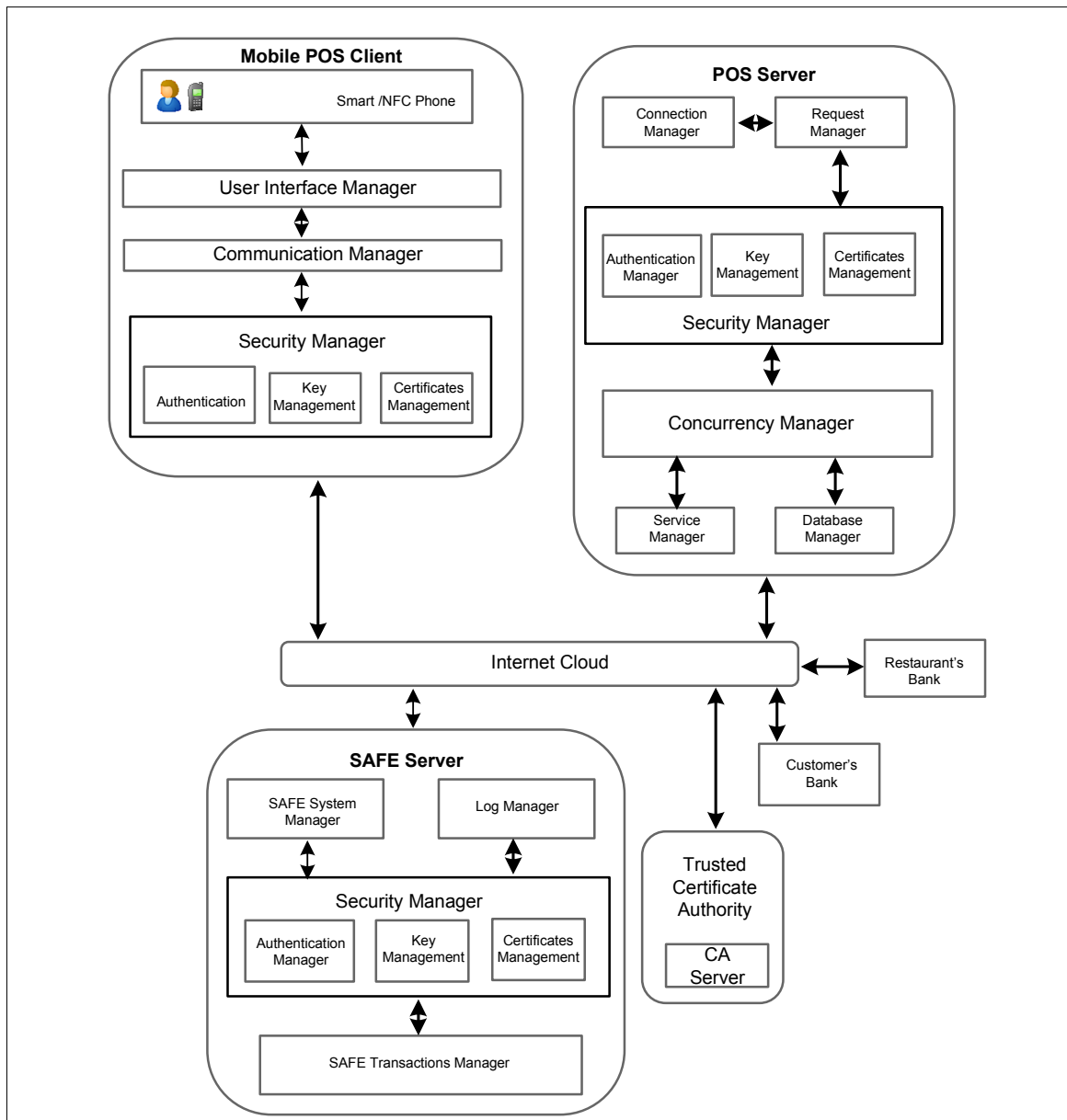


Figure 3.9 Object Based Model of the System

3.7 Security Requirements

There are several security requirements that need to be fulfilled for any secure application. Security requirements are: authentication, confidentiality, integrity, availability, authorization, and non-reputation [8]. All these security requirements are also considered as security challenges [9]. In the next section we have analyzed all these security requirements in respect to our designed mobile POS system.

3.8 Security Features Analysis

In this section we have provided the security analysis of the designed POS system.

3.8.1 Authentication

We have used mutual authentication between mobile client and the payment server of the bank or the SAFE server. Because mutual authentication is a strong authentication that prevents different attacks, like masquerade, password compromise, replay attacks etc. The CA server issues certificates. Customers use their certificates and digital signatures to confirm payments.

3.8.2 Confidentiality

Communication between mobile client and payment server is performed by the SSL/TSL protocol through a secure channel. Also, we have used access control mechanism to ensure the confidentiality of the data.

3.8.3 Integrity

Customers generate their digital signatures by using their private keys. Messages are signed by the sender's private key. And only the respective receiver knows the sender's public key which have been shared before transaction data are transferred. The attacker doesn't know the private key of the customer. If the attacker can eavesdrop the data on its way and modify it and sign it and send it to the receiver, that will not work. Because the receiver will verify digital signature of the sender and digital signatures will not be the same, which confirms the integrity of the payment information.

3.8.4 Non-repudiation

The payment information is transferred in between the customer and the payment server by using PKI. Private key of the customer and the payment server only the respective entities which insure the non repudiation of the system.

3.8.5 Authorization

In our designed mobile POS system, different kind of users has different roles. It is very important to have proper authorization of the users depending on their roles. We have used role based access control method for the authorization of the users to their respective access area.

Chapter 4: System Implementation and Demonstration

In this chapter the development environment of the implemented application based on the proposed architecture has been described. We have also included screenshots of the implemented application with description of them.

4.1 Development Environment

In this section we have described different development tools and environments, which have been used for the implementation of the secure mobile point of sale application.

4.1.1 Java Technology

We have used Java technology to develop the admin application for the Windows environment. Security features are also developed using Java cryptographic extensions [4].

4.1.2 Android SDK

Three mobile applications (customer application, employee application and manager application) are implemented using Android SDK tools. Android SDK is a very powerful tool for developing mobile applications that can be used on Android mobile phones [20].

4.1.3 MySQL Server

In this demo application we have used MySQL as our database server. The reasons for choosing MySQL server is because it is open source and also light-weight [16].

4.1.4 PHP

We have used PHP for the communication between MySQL database and mobile client application to save and retrieve data from MySQL database server. We have used PHP, because it is one of the best choices to communicate with MySQL database server [17].

4.1.5 Eclipse IDE

Android applications are implemented using Eclipse integrated developing environment. Eclipse IDE is a powerful tool for Android applications development. Eclipse is a plug-in based developing environment, where you just add the Android plug-in to develop your Android application [18].

4.1.6 NetBeans IDE

We have used NetBeans IDE to develop graphical user interface (GUI) for Windows based admin application. It is very easy to develop GUI with the help of NetBeans IDE [19].

4.2 Demonstration

In this section we have provided screenshots of the developed prototype for mobile POS system. We have demonstrated three different mobile applications used by different entities using the POS System. We have also provided screenshots of the Windows application used by POS Admin.

We have considered a restaurant to demonstrate our designed POS system. Mobile POS Applications are the following:

1. POS application for the customer
2. POS application for an employee
3. POS application for manager

4.2.1 POS Application for A Customer

The screenshots for the customer application is provided here. In this demo we have considered that a customer could be a registered member of a restaurant or he/she may not be a member. The customers can search foods in the restaurant's POS database, select items, make order, and pay bills.

4.2.1.1 Customer Login Screen

Customer login screen allows registered customer to login into the system. If a customer is not registered member, he/she can just click login to use the applications. The registered member may get some extra benefits on price, depending on organizational rule. Figure 4.1 shows login screen for the customer.

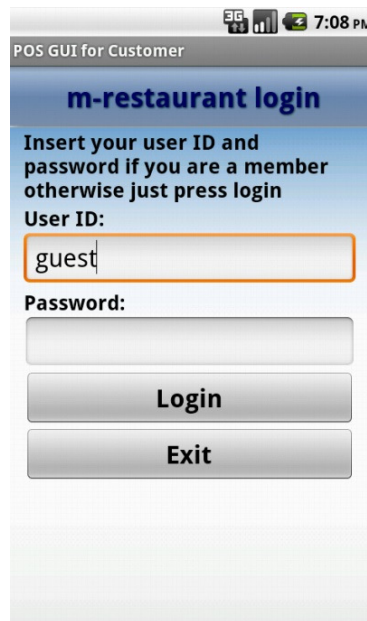


Figure 4.1 Customer Login Screen

4.2.1.2 Customer Main Screen

Customer's main screen for mobile POS is given in Figure 4.2. Customer has four options to choose in this screen. Customer can create order, list previous orders, request payments, and select the membership option to become a member of the restaurant. Membership options is for becoming a member of the shop. If a user is not a member of that shop, then he/she will have to enter some data at the next step of the membership options. It can also be used for modifications of membership information for a registered member of a shop.

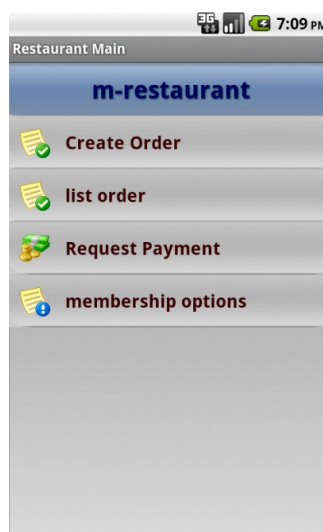


Figure 4.2 Main Screen for the Customer

4.2.1.3 Food Menu Screen

If a customer selects Create Order option, then he/she will be redirected to the Food List, where they can select food to add them in their order. Figure 4.3 shows Food List Screen.



Figure 4.3 Food List Screen

4.2.1.4 Single Food Item

Figure 4.4 shows single menu item detail. If the user selects a single item in the item list, then single food item detail is shown. In this screen the customer can enter the number of items that he/she wants to buy. He/she can also calculate total cost of items that he/she wants to buy. Add to Order button allows the user to add the item to the order list. The customer can also select the complete order to add the order to the order list and to go to the order confirmation screen.

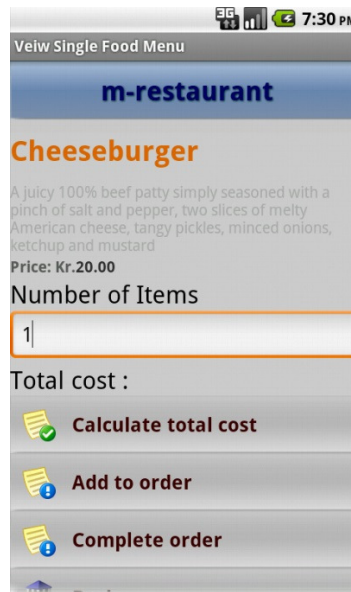


Figure 4.4 Single Food Item

4.2.1.5 Add Food to Order

If customers select the Add to Order option at the single food detail screen, then they will be redirected to the 'Add Food to Order' screen (shown in Figure 4.5). This screen is quite similar to the food list screen, but here at this screen the customer has the option to go to the Order Completion screen directly.



Figure 4.5 Add Food to Order

4.2.1.6 Complete order screen

Before writing order list to the database, the application asks for a confirmation from the customer (Figure 4.6). In this screen the user can select a ordered item from the list and can

modify or delete item from the list. The customer can also add more items using the Add More Items button.

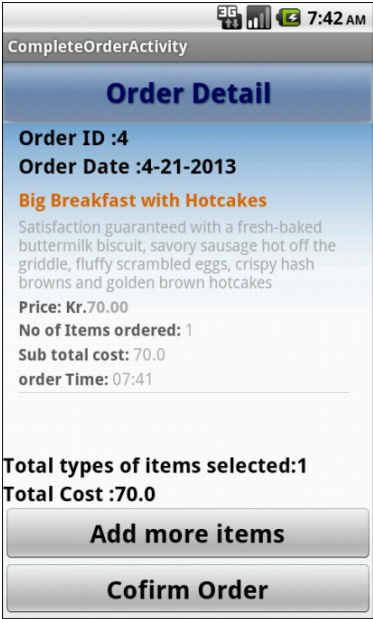


Figure 4.6 Complete Order Screen

4.2.1.7 Order List

At the restaurant's main screen, if the customers select the order list, then they will be redirected to the Order List Screen (Figure 4.7). At this screen the customer can see the paid and unpaid orders separately or together in the same list.

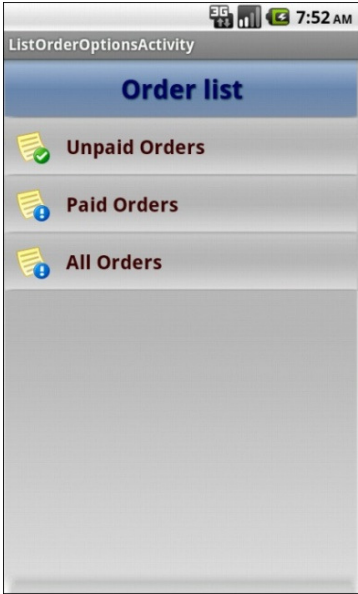


Figure 4.7 Order List Screen

4.2.1.8 Unpaid Order List

Figure 4.8 shows Unpaid Orders List, where we can see that there are two orders that are unpaid in our demo application.

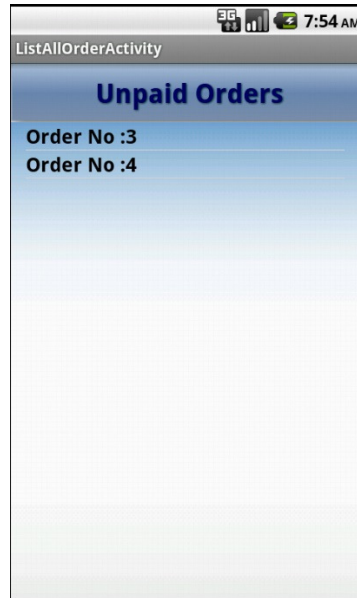


Figure 4.8 Unpaid Orders List

4.2.1.9 Single Unpaid Order Detail

Figure 4.9 shows Unpaid Single Order Detail. Customer can choose the 'Pay Order' button to go to the Payment Type Selection screen.

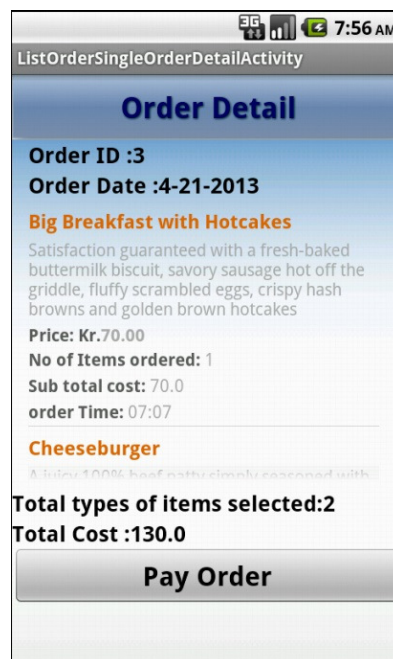


Figure 4.9 Unpaid Single Order Detail

4.2.1.10 Payment Type Selection Screen

Figure 4.10 shows the screenshot where we have three different payment options. The customer can choose the option that he/she wants to use to pay his/her restaurant bills. If the customers select credit card payment option, then they will be redirected to the Credit Card Payment Screen (Figure 4.11). If the customer wants to pay using his/her SAFE account then they have to select 'Pay by m-Wallet' option. In this case the customer needs to have an account with the SAFE System [15]. In some cases the user may like to pay the bills using his or her mobile account. Then he/she has to select 'Pay Using Mobile Account' option. While a payment through the mobile account is involved, the sales organization needs to have an account with the mobile operator to get the payment through the customers' pre-paid or post paid mobile account.

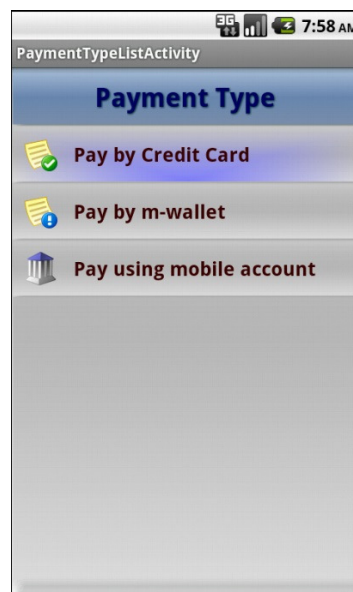


Figure 4.10 Payment Type Selection Screen

4.2.1.11 Credit Card Payment Option

If the customer selects the credit card payment option, then he/ she will be shown similar screen like Figure 4.11. In this screen customers can insert their card information and then they will have to perform challenge/response procedure to confirm the payment.

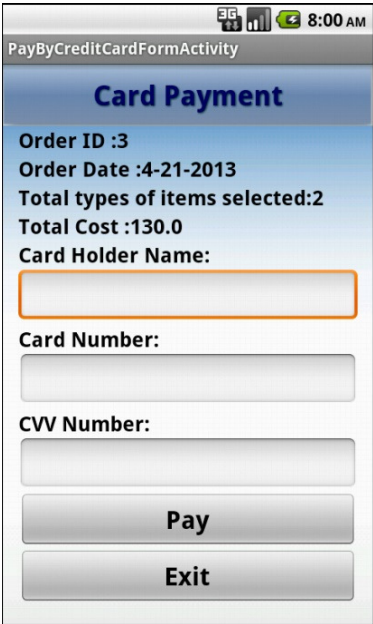


Figure 4.11 Credit Card Payment Option Details

4.2.1.12 Payment Confirmation Screen

Figure 4.12 shows Payment Confirmation screen where the customers get the confirmation of their payments.

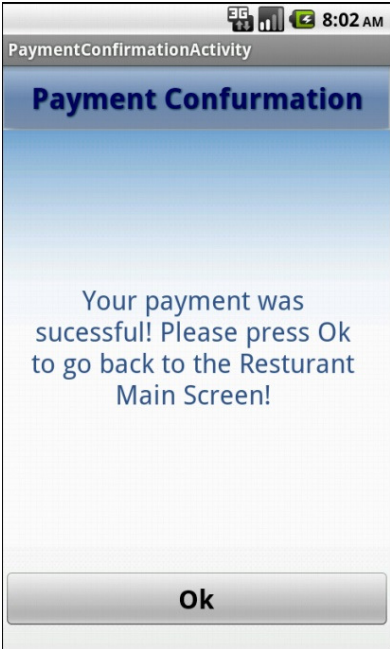


Figure 4.12 Payment Confirmation Screen

4.2.1.13 Paid Orders List

Figure 4.13 is the screenshot of the paid orders list. If the customer wants to recall the paid order, they will be redirected to this screen. Figure 4.14 shows the details of a single paid order.

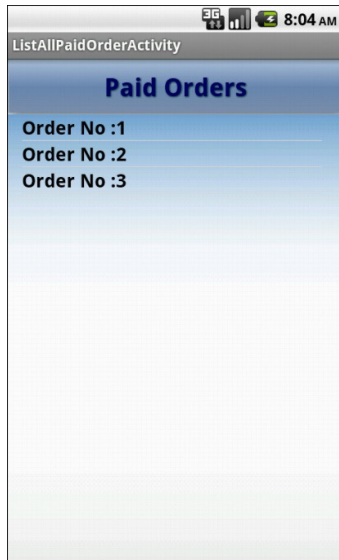


Figure 4.13 Paid Order List

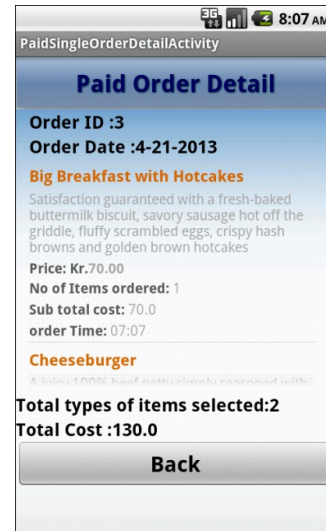


Figure 4.14 Paid Single Order Details

4.2.1.14 Request Payment Options

If the customer selects Request Payment option, he/ she will be redirected to an unpaid order list, shown in Figure 4.15. User can select any unpaid order to pay. Figure 4.16 shows the selected unpaid order details. Customer can go to the payment screen by pressing 'Pay Order' button.

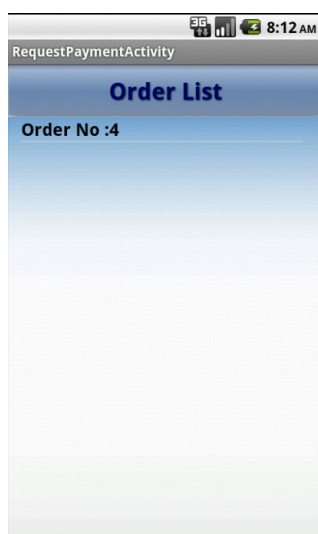


Figure 4.15 Unpaid Order List

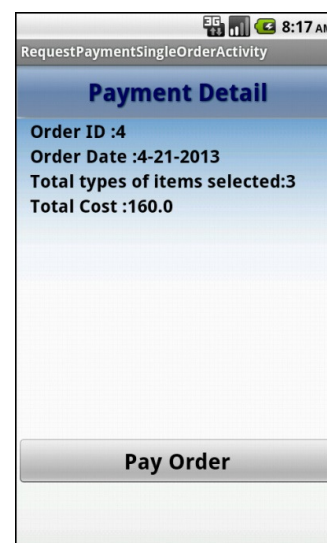


Figure 4.16 Select Single Order for Payment

4.2.2 POS Application for Employees

POS application for employees enables business organization to handle sales through the sales persons. Here the employees login to the POS server to have access to the item list. The details of the employee application with the screenshots are given bellow.

4.2.2.1 Employee Login

Employee must login to the POS system in order to access items list. Employee Login Screen is shown in Figure 4.17.



Figure 4.17 Employee Login Screen

4.2.2.2 Main Screen for Employees

After successful login into the system, the employee will be redirected to the main screen. The main screen for the employee application is shown in Figure 4.18. The main difference between employee's application and customer's application is the payment method. In a employees POS client application the employee sends the bills to the customer's mobile device/smart phone through NFC technology. And the customer pays their bills using their NFC enabled mobile phones. Customers have different payment options to pay their bills, as we have described in the payment section for the customer. In the employee POS client application the employee can add/edit member information for the member of the store. The members are registered customers. The members can have extra facilities compared to normal customers, depending on the requirement of the sales organization. Another difference between the customer's application and the employee's application is the POS settings. The

POS Settings screen is shown in Figure 4.19. In the POS settings option the employees enter their device id and the version of their client software.

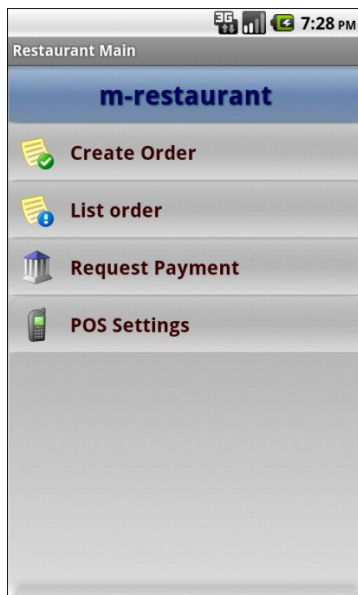


Figure 4.18 Main Screen for Employees

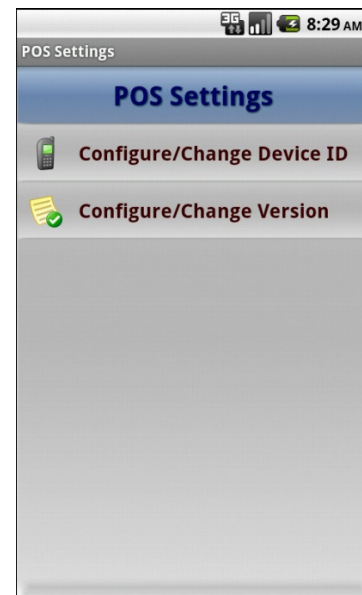


Figure 4.19 POS Settings Screen

4.2.2.3 Device ID and POS Version Configuration

Figure 4.20 shows device ID configuration screen and Figure 4.21 shows POS version configuration screen.



Figure 4.20 Device ID Configurations

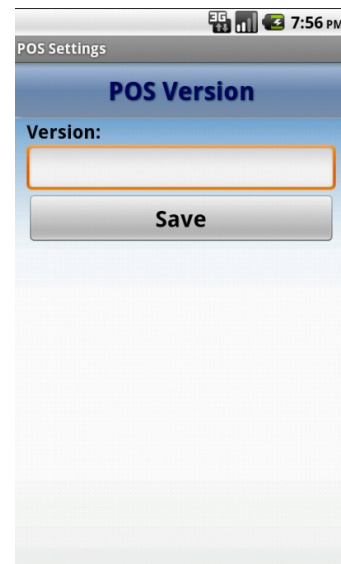


Figure 4.21 POS Version Configurations

4.2.3 POS Application for Managers

Managers of a sales organization also have a mobile application. Managers login screen is shown in Figure 4.22. After successful login into the system, managers are redirected to the

main screen for managers, which is shown in figure 4.23. Managers can view or modify the inventory by selecting 'Inventory' option at the main screen. They can also check sales reports by choosing 'List Transactions' option. The "POS System" is the option for the configuration of the POS system.

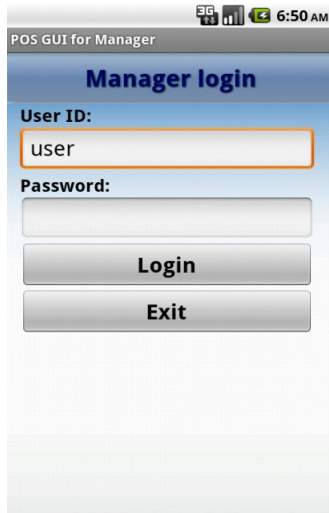


Figure 4.22 Manager's Login Screen

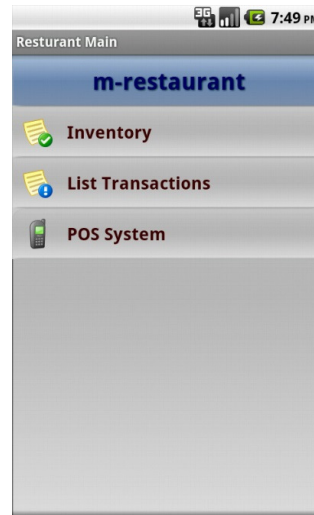


Figure 4.23 Main Screen for Managers

4.2.4 Admin Application

We have developed a Windows based application for the administrator of the mobile POS system. The Admin login screen is shown in Figure 4.24. The admin users install and configure the POS system. They are also responsible to add and modify managers and employees of the POS system.

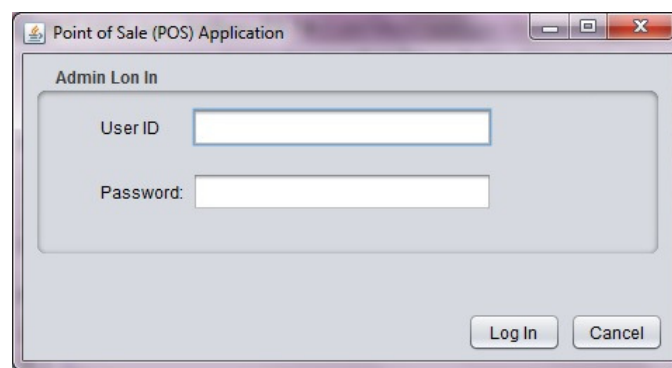


Figure 4.24 Admin Login Screen

The screenshot shows a window titled "Point of Sale (POS) Application" with a "Manager Registration Form" inside. The form is organized into two main sections: "Manager Data" and "Manager Address".

Manager Data Section:

- Manager ID:
- First Name: Last Name:
- Gender: Male Female
- Phone no: Email:
- Wage:

Manager Address Section:

- Address Line 1:
- Address Line 2:
- City: City Code:
- State: Country:

At the bottom right of the form, there are two buttons: "Register" and "Cancel".

Figure 4.25 Manager Registration Screen

Manager registration screen is shown in Figure 4.25. Admin users play a vital role for the business organization. The admin person needs to be a trusted person.

The screenshot shows a window titled "Point of Sale (POS) Application" with a sub-header "Employee Registration Form". The form is organized into two main sections: "Employee Data" and "Employee Address".

Employee Data Section:

- Employee ID: 0
- First Name: [Text Field]
- Last Name: [Text Field]
- Gender: Male Female
- Role Name: Waite (Dropdown Menu)
- Phone no: [Text Field]
- Email: [Text Field]
- Wage: [Text Field]

Employee Address Section:

- Address Line 1: [Text Field]
- Address Line 2: [Text Field]
- City: [Text Field]
- City Code: [Text Field]
- State: [Text Field]
- Country: [Text Field]

At the bottom right of the form, there are two buttons: "Register" and "Cancel".

Figure 4.26 Employee Registration Screen

The employee registration screen is shown in Figure 4.26. The admin users enter all these data to POS system. In some cases the data about the employees can be inserted by managers.

Chapter 5: Conclusions and Future Work

In this chapter, our research has been concluded. Also future scopes of research within the area have been discussed.

5.1 Conclusions

After analyzing the problem area, we have designed and implemented our secure mobile POS application. Designed application will increase mobility for users of the POS application. In our example, as we have described a restaurant mobile POS application, we can consider the flexibilities of it. A **manger** can access the inventory as well as the sales report of the restaurant, while he is not at the office. **Employees** can use mobile device while they are standing besides customer add getting order from them. **Customers** can use their mobile application to make the order to a restaurant for home delivery of their food. In a residential hotel the customer can also make order using their mobile phone to the restaurant of the same hotel to get their food delivered to their room. The designed application is secure enough, because we have fulfilled all the security features that need to be considered, while developing secure mobile application.

5.2 Future Work

In this thesis we have mentioned several payment methods within our design, but not implemented. Future research and development work can be done with different payment methods introduced in the design section of this thesis. Also, we have tested the application within the SecLab environment. The same application can be tested within the real m-commerce environment, what also opens a new research scope.

References

1. Mavridis, Ioannis; Pangalos, G.; Koukouvinos, T.; Muftic, S., "A secure payment system for electronic commerce," *Database and Expert Systems Applications, 1999. Proceedings. Tenth International Workshop on* , pp.832,836, 1999
URL: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=795290&isnumber=17217> [Online] [Cited: 3rd, April 2013]
2. Feng Zhang; Muftic, S.; Schmöelzer, G., "Secure service-oriented architecture for mobile transactions," *Internet Security (WorldCIS), 2011 World Congress on* , pp.133,138, 21-23 Feb. 2011
URL: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5749898&isnumber=5749844> [Online] [Cited: 3rd, April 2013]
3. F. Zhang, 'Security Application for Financial Environment (SAFE) system', Royal Institute of Technology (KTH), Stockholm, Sweden
4. Abbasi, A.G.; Muftic, S.; Schmöelzer, G., "A model and design of a security provider for Java applications," *Internet Technology and Secured Transactions, 2009. ICITST 2009. International Conference for* , pp.1,7, 9-12 Nov. 2009
URL: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5402592&isnumber=5402499> [Online] [Cited: 3rd, April 2013]
5. Scientific method, <http://philosophy.hku.hk/think/sci/hd.php> [Online] [Cited: 24th, March 2013]
6. Qualitative Case Study Methodology: Study Design and Implementation for Novice Researchers, *The Qualitative Report*, Volume 13, Number, 4 December 2008 544-559
URL: <http://www.nova.edu/ssss/OR/OR13-4/baxter.pdf> [Online] [Cited: 24th, March 2013]
7. Debono, C.J.; Busuttil, D., "A secure wireless point of sale system," *EUROCON - International Conference on Computer as a Tool (EUROCON), 2011 IEEE* , pp.1,4, 27-29 April 2011
URL: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5929195&isnumber=5929030> [Online] [Cited: 4th, April 2013]
8. Nguyen, T. N T; Shum, P.; Chua, E. H., "Secure end-to-end mobile payment system," *Mobile Technology, Applications and Systems, 2005 2nd International Conference on* , pp.4, 15-17 Nov. 2005
URL: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1656771&isnumber=34698> [Online] [Cited: 4th, April 2013]
9. Manvi, S. S.; Bhajantri, L.B.; Vijayakumar, M.A., "Secure Mobile Payment System in Wireless Environment," *Future Computer and Communication, 2009. ICFCC 2009. International Conference on* , pp.31,35, 3-5 April 2009
URL: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5189737&isnumber=5189730> [Online] [Cited: 5th, April 2013]

10. Antovski, L.; Gusev, M., "M-payments," *Information Technology Interfaces*, 2003. ITI 2003. Proceedings of the 25th International Conference on , pp.95,100, 16-19 June 2003
URL: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1225328&isnumber=27508> [Online]
[Cited: 4th, April 2013]
11. Pedersen, A.; Partner, N.; Hedegaard, A.; Sharp, R., "Designing a secure point-of-sale system," *Information Assurance, 2006. IWIA 2006. Fourth IEEE International Workshop on* , pp.15 pp.,65, 13-14 April 2006
URL: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1609999&isnumber=33798> [Online]
[Cited: 5th, April 2013]
12. S. Britto R. Kumar, S. Albert Rabara, and J. Ronal Martin. 2009. MPCS: a Secure Mobile Payment Consortia System for higher educational institutions. In *Proceedings of the 2nd International Conference on Interaction Sciences: Information Technology, Culture and Human (ICIS '09)*. ACM, New York, NY, USA, pp. 571-579. URL:<http://doi.acm.org/10.1145/1655925.1656029>
13. Vesna Hassler. *Security Fundamentals for E-Commerce*. Computer Security Series. Artech House, second edition, 2000.
14. W. Stallings, *Network Security Essentials*, Low price edition, Pearson Educations, 2000
15. Ali, T.; Awal, M.A., "Secure mobile communication in m-payment system using NFC technology," *Informatics, Electronics & Vision (ICIEV), 2012 International Conference on* , pp.133,136, 18-19 May 2012
URL: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6317453&isnumber=6317321>
[Online] [Cited: 15th, April 2013]
16. Why MySQL, <https://www.mysql.com/why-mysql/> [Online] [Cited: 15th, April 2013]
17. What is PHP, <http://www.php.net/manual/en/intro-what-is.php> [Online] [Cited: 16th, April 2013]
18. Why use Eclipse?, <http://www.eclipsezone.com/eclipse/forums/t100199.html> [Online] [Cited: 18th, April 2013]
19. NetBeans IDE, <https://netbeans.org/features/index.html> [Online] [Cited: 20th, April 2013]
20. Android, the world's most popular mobile platform, <http://developer.android.com/about/index.html>
[Online] [Cited: 20th, April 2013]

