ADDIS ABABA UNIVERSITY

SCHOOL OF GRADUATE STUDIES

COLLEGE OF NATURAL SCIENCES

DEPARTMENT OF COMPUTER SCIENCE

ONLINE DIGITAL PAYMENT SYSTEM

YITBAREK ZEWDE

A PROJECT SUBMITTED TO

THE SCHOOL OF GRADUATE STUDIES OF ADDIS ABABA UNIVERSITY
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE
OF MASTER OF SCIENCE IN COMPUTER SCIENCE

November 2013, Addis Ababa

ADDIS ABABA UNIVERSITY

SCHOOL OF GRADUATE STUDIES

COLLEGE OF NATURAL SCIENCES

DEPARTMENT OF COMPUTER SCIENCE

ONLINE DIGITAL PAYMENT SYSTEM

By: Yitbarek Zewde Kelbore

Advisor: Dida Midekso (PhD)

Approved by Board of Examiners:

Name	Signature
1. Dr. Dida Midekso, Advisor	_____
2. _____	_____
3. _____	_____

ACKNOWLEDGMENT

First of all, I would like to thank the Almighty God for his love and kindness in bestowing me health, strength, patience and protection throughout my study. Furthermore, I would like to express my gratitude to my advisor, Dr. Dida Midekso, for his guidance, support and his continuous enthusiasm and encouragement throughout the project. I pay respect and express appreciation to him because of his guidance, advice, consistent supervision as well as moral support.

Also, I like to thank the participants in my usability testing process, who have willingly shared their precious time during the process of filling in questionnaires.

Last but not least, I would like to thank my family, friends and colleagues for supporting me spiritually throughout my life.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

3DES – Triple Data Encryption Standard

AES – Advanced Encryption Standard

API – Application Programming Interface

ASP – Active Server Pages

D-Birr – Digital Birr

EPS – Electronic Payment System

HTML – Hyper Text Markup Language

IDE – Integrated Development Environment

ISO – International Organization for Standards

NIST – National Institute of Standards and Technology

PDS – Personal Digital Assistant

RSA – Rivesh Shamir Aldermen

SET – Secure Electronic Transaction

SHA – Secure Hashing Algorithm

SQL – Structured Query Language

UML – Unified Modeling Language

XHTML – Extensible HTML

XML – Extensible Markup Language

Abstract

Due to the expansion of the Internet throughout the world, payment systems are growing in number aiming to automate the process of buying and selling goods online. These systems have shown that it is possible to save time, resource and cost of transactions carried out using traditional paper based payment systems. Payment in all online payment systems is carried out using credit cards. However, in Ethiopia the use of credit card is very minimal. In this project work an Online Digital Payment System is designed and implemented by considering problems related to the minimal use of credit card based online payment systems in Ethiopia. Three-tier system architecture is chosen as architecture of the system. To reduce the complexity of the system, it is decomposed into four sub systems (Administration sub system, User sub system, Security sub system and Shop sub system) which run on different tiers. Payment models for buying and selling items and bonds have also been designed and implemented. Digital Birr, a payment code digitally signed by system provider (i.e. a Bank), is used as a means of paying for goods. Bond related transactions are carried out using Digital Bond, a bond payment code digitally signed by system provider. XHTML is used to present the contents on the client web browser. The dynamic parts are implemented using JavaScript, for client-side scripting and ASP.NET (C-Sharp), for server-side scripting. Finally, the Online Digital Payment System prototype evaluation is conducted using questionnaire by involving 30 different users from 5 different banks (6 users from each banks) using random selection. The results have shown that the Online Digital Payment System saves time, resource and cost of using paper based payment systems; it is easy to use and is secure. It is also seen that the system is a low-cost system to work with compared to credit card based systems.

Key words: Digital Birr, Digital Bond, Online Payment, Online Shop, Digital Signature

CHAPTER ONE

INTRODUCTION

1.1 Overview

Since the explosion of the Internet, more and more people are being part of the users due to the convenience of the services delivered through the Internet. The Internet has connected people around the world and subsequently enabled businesses to offer products and services around the globe without being physically present in front of the consumers or potential consumers. As time goes by, the Internet has become a part of the daily life, which demands more and more applications being created and services being made available to make full use of the infrastructure [1]. Consequently, electronic transactions have become possible and are being implemented for different applications. In today's rapidly changing marketplace, if financial institutions focus their strategy on creating novel approach for electronic payments (e.g. online payment system), they will be more likely to improve the profitability of their payment operations.

An online payment strategy has the potential to pay enormous long term financial and risk management benefits by reducing paper-based transactions [8]. Electronic transactions mainly save time, a valuable resource in business world. Additionally, as electronic systems are cheaper to operate, financial institutions can possibly reduce the cost of resources imposed by paper based transactions. The capability to pay electronically coupled with a website is the engine behind electronic commerce. Electronic commerce has been facilitated by automatic teller machines (ATMs) and shared banking networks, debit and credit card systems, electronic money and stored value applications, and electronic bill presentment and payment systems.

Mobile payments are a natural evolution e-payment schemes that will facilitate mobile commerce. Mobile payment or m-payment may be defined as any payment where a mobile device is used to initiate, authorize and confirm an exchange of financial value in return for goods and services. Mobile devices may include mobile phones, PDAs, wireless tablets and any other device that connect to mobile telecommunication network and make it possible for payments to be made [9].

In most electronic payment systems, credit cards are used as payment tools to purchase items online [12]. To pay using a credit card, a user must submit his/her credit card number, name, and card expiry date. Up on a successful validation of the information submitted, the merchant delivers goods and/or services.

1.2 Statement of the Problem

According to Mandana Jahanian Farsi [3], the present day payment systems fall into two large categories: account-based systems and token-based systems. Token-based systems such as paper cash, pre-paid phone cards, do not identify its users. Account-based systems such as checks, credit cards or bank accounts are better ways of payment as it is able to identify the users. However, when we come to payment through the Internet, it is impossible to implement using checks or bank accounts. Hence, an online payment using a credit card is the easiest and comfortable way to pay for goods and services online [4].

But the cost of building and running the credit card infrastructure is something which needs an emphasis to deal with [11]. Staring from paying the experts who run the credit card infrastructure to printing the plastics, to mailing the statements, to running the computers that keep track of every cardholder's balance, to taking the many phone calls which cardholders place to their issuer, to protecting the customers from fraud rings, it needs a huge amount of fund. In addition to that, credit card fraud has been a major issue for financial institutions, since the very moment credit cards were introduced [13]. The cost of combating credit cards fraud is also another overhead for any institution in charge.

In Ethiopia, almost all transaction payments are carried out manually, through the process of cash payment, which yields inefficient usage of time and resource. It is difficult for an online person (a person on the Internet) to browse and buy goods (such as electronic books, music, movies, software) and services using his/her personal computer. Additionally, buying and selling of bonds is another area of transactions that needs to be automated. In finance, bond is a debt security, in which the authorized issuer owes the holders a debt and, depending on the terms of the bond, is obliged to pay interest to use and/or to repay the principal at a later date, termed maturity [2].

Recently, credit cards are being introduced in Ethiopia. However, credit cards providers in Ethiopia do not allow use of credit cards for online payments. The main reasons here are the issues related to security, cost of developing a system and lack of awareness towards the applicability of credit cards for online payment in Ethiopia. Hence, the researcher is motivated to design and implement a non-credit card online payment system.

1.3 Objectives

1.3.1 General Objective

The general objective of this project work is to design and implement an Online Digital Payment System.

1.3.2 Specific objectives

The specific objectives of the project work are to:

- Conduct literature review
- Explore and adopt related works and algorithms on online payment
- Develop a prototype
- Evaluate the prototype

1.4 Scope and limitations

This project work automates the payment process without the use of credit cards. In addition, the proposed system only considers transactions related to financial bonds and non-tangible items such as computer programs, music files, movies and electronic books.

1.5 Methodology

Methods that are needed to achieve the objectives of the project are discussed in sections below.

1.5.1 Literature Review

Different literatures that are considered to be relevant for the project are reviewed to get better understanding of the area and to have detailed knowledge on the various techniques that are essential for online payment systems.

1.5.2 Development Language and Tools

In this project, ASP.NET web development language is applied. This is due to its flexible and secure natures. Additionally, JavaScript will be used for implementing client-side functionalities such as encrypting sensitive data to be sent over the network, decrypting an encrypted data received from the network and so on. The backend database server is implemented using Microsoft SQL Server 2005. Microsoft Visual Studio 2008 is used as an IDE (Integrated Development Environment) for the development of the Online Digital Payment System prototype.

1.5.3 Evaluation

After the implementation of the prototype, the usability test will be conducted with selected users as it can assure whether the objectives of the project are met or not.

1.6 Application of Results

The result of this project work can be used by so many financial institutions including banks, credit delivery institutions, and development associations. Bond selling organizations can use the result of this project to automate and easily manage selling-buying transactions. Private trading centers will play a very crucial role in achieving the advancement of manual payment transactions. Those who want to buy a bond for some purpose will not be expected to go to overcrowded financial institutions rather they can buy a bond code from nearby trading shops and register it to the remote database administrated by the financial institution.

Additionally, the result can also be used by any legal trading companies as the proposed system helps them to sell their non-tangible items online. They can easily reach their customers through the Internet.

1.7 Document Organization

The remainder of the report is organized as follows. Chapter Two discusses literature review for the understanding of basic concepts related to mobile payment systems, security aspects of web-based payment systems, and credit card and its usage in web-based payment technologies. Chapter Three focuses on the analysis of Online Digital Payment System by identifying the functional and non-functional requirements. The design aspects of the proposed system are discussed in Chapter Four. Issues related to deign goals and constraints of the proposed system are clearly presented in this Chapter. Chapter Five discusses system development tools like development IDE, Microsoft SQL

Server 2005, development markup and scripting languages, and encryption libraries used for the development of the system. A prototype of Online Digital Payment System is also presented. In Chapter Six, the evaluation of Online Digital Payment System, which is conducted by actively involving different users, is presented and the evaluation of the usability of the prototype is presented based on the data collected from the participants. Finally, Chapter Seven gives conclusion of this project and points out future works related to the Online Digital Payment System.

CHAPTER TWO

LITERATURE REVIEW AND RELATED WORK

2.1 Literature Review

Along with the information technology, the high-speed development of the use of Internet has caused the possibility of online electronic payment systems to become widely used. In the electronic payment practice, the online electronic payment is a way of using electronic payment tools (such as credit cards) for the purpose of buying and/or selling items online on the Internet [14].

Additionally, the Internet has become an essential tool for commerce and financial services. With the help of new communication technologies, these services have experienced tremendous growth. They are becoming more and more accessible to customers, regardless of their location. An inhibiting factor for this growth is the fear of fraud and sensitive data theft, which is widespread among the general public due to the insecure and unreliable nature of the Internet [15].

According to Jan L. Camenisch [16], the number of private and corporate financial transactions that are done electronically is growing rapidly. From a user's point of view, efficiency and flexibility are clear advantages of existing and emerging electronic payment systems. Due to technical progress and new developments in cryptography, these systems offer also a high level of security.

Under this chapter various literature studies related to online payment systems, system security and online payment models are discussed.

2.1.1 Credit Card

A credit card is the most popular payment method used in Internet shopping. The idea of credit card payment is to buy first and pay later [17, 18]. The cardholder can pay at the end of the statement cycle or he/she can pay interest on the outstanding balance. Usually, a credit card-based electronic payment system involves five parties: cardholder, merchant, acquirer bank, issuer bank, and financial institution. The Internet is an open system and the communication path between each other is insecure. All communications are potentially open for an eavesdropper to read and modify as they pass between the communicating endpoints. Therefore, the payment information transmitted between the cardholder and the merchant through the Internet is dangerous without a secure path. Secure Socket Layer is a good example to secure the communication channel. Besides the issue of insecure communication,

there are a number of factors that each participant must consider. For example, a merchant is concerned about whether the credit card or the cardholder is genuine. There is no way to know the consumer is a genuine cardholder. As a result, the merchant is incurring the increase in losses due to cardholder disputes and frauds. On the other hand, cardholders are worried about the theft of the privacy or sensitive information such as the credit card number. They don't want any unauthorized usage of their credit cards and any modification to the transaction amount by a third party. These security issues have deterred many potential consumers from purchasing online. Existing credit card-based EPSs solve the problems in many different ways. Some of them use cryptography mechanisms to protect private information. However, they are very complicated, expensive, and tedious. Some electronic payment systems use the certificate authority model to fulfill the authentication, integrity, and no repudiation security schemes. However, each participant requires a digital certificate during the payment cycle. These certificates are issued by independent certificate authorities but the implementation and maintenance cost of this model is very high. In addition, the validation steps of certificate-based systems are very time-consuming processes. It requires access to an online certificate server during the payment process. Moreover, the certificate revocation list is a major disadvantage of the Public Key Infrastructure based certification model. The cardholder's certificate also includes some private information such as the cardholder's name. The requirement of a cardholder's certificate means software such as e-Wallet is required to be installed on the cardholder's computer. It is a barrier for the cardholder to use Certificate-based payment systems.

2.1.2 Cryptography

Cryptography is a way for two communicating parties (systems) to communicate secretly over an insecure channel without an opponent understanding what is being transmitted. In cryptography there are two main activities, encryption and decryption [19]. The data transferred from one system to another over public network can be protected by the method of encryption. On encryption, the data is encrypted or scrambled by any encryption algorithm using a 'key'. Only the user having the access to the same 'key' can decrypt or de-scramble the encrypted data. This method is known as private key or symmetric key cryptography. There are several standard symmetric key algorithms defined. Examples are AES, 3DES etc. These standard symmetric algorithms are proven to be highly secured and time tested. But the problem with these algorithms is the key exchange. The communicating parties require a shared secret, 'key', to be exchanged between them to have a secured communication. The security of the symmetric key algorithm depends on the secrecy of the key. Keys are typically hundreds of bits

in length, depending on the algorithm used. Since there may be a number of intermediate points between the communicating parties through which the data passes, these keys cannot be exchanged online in a secured manner. In a large network, where there are hundreds of system connected, offline key exchange seems too difficult and even unrealistic. This is where public key cryptography comes to help [20].

Public Key Cryptography

Using a public key algorithm, a shared secret key can be established online between communicating parties without the need for exchanging any secret data. In public key cryptography, each user or the device taking part in the communication has a pair of keys, a public key and a private key, and a set of operations associated with the keys to do the cryptographic operations [20, 21]. Only the particular user/device knows the private key whereas the public key is distributed to all users/devices taking part in the communication. Since the knowledge of public key does not compromise the security of the algorithms, it can be easily exchanged online. A shared secret can be established between two communicating parties online by exchanging only public keys and public constants if any. Any third party, who has access only to the exchanged public information, will not be able to calculate the shared secret unless it has access to the private key of any of the communicating parties.

One-Way function

In public key cryptography, keys and messages are expressed numerically and the operations are expressed mathematically [20, 21]. The private and public keys of communicating parties are related by the mathematical function called the one-way function. One-way functions are mathematical functions in which the forward operation can be done easily but the reverse operation is so difficult that it is practically impossible. Hashing algorithms, such as SHA-1 [22], are used to digest the message using one-way function implementation. Generally, one-way or hash functions are characterized by the following properties:

- It is computationally infeasible to find a message *m* that corresponds to a known output of hash function *h*.
- It is computationally infeasible, given message *m* and hash function *h* to find $m' \neq m$ such that $h(m) = h(m')$

- Given a hash function *h*, it is computationally infeasible to find any two different input values *m* and *m*', such that *h(m) = h(m')*

Key Agreement

Key agreement is a method in which the system communicating in the network establishes a shared secret between them without exchanging any secret data [20, 21]. In this method, the systems that need to establish shared secret between them exchange their public keys. Both the systems on receiving the other system's public key perform key generation operation using its private key to obtain the shared secret.

Since it is practically impossible to obtain private key from the public key, any middleman, having access only to the public keys, will never be able to obtain the shared secret. During the key exchange process the public keys may pass through different intermediate points. Any middleman can thus tamper or change the public keys to its public key. Therefore, for establishing shared secret it is important that system A receives the correct public key from system B and vice versa. Digital Certificate helps to deliver the public key in authenticated method [20].

Digital Signature

Using Digital signature a message can be signed by a system using its private key to ensure authenticity of the message [23]. Any system that has got access to the public key of the signing system can verify the signature. Thus, the system receiving the message can ensure that the message is indeed signed by the intended system and is not modified during the transit. If any data or signature is modified, the signature verification fails [22].

2.1.3 RSA

RSA is a public-key cryptosystem that offers both encryption/decryption and digital signatures (authentication). Ron Rivest, Adi Shamir, and Leonard Adleman developed RSA in 1977. RSA stands for the first letter in each of its inventors' last names. It mainly has three steps; key generation, encryption and decryption [24].

RSA Key Generation

The RSA key generation is used to generate private and public keys using large prime numbers. The main steps are:

- Take two large primes, p and q, and compute their product $n = pq$;
- Choose a number e less than n and relatively prime to $(p-1)(q-1)$, which means e and $(p-1)(q-1)$ have no common factors except 1.
- Find another number d such that $(ed - 1)$ is divisible by $(p-1)(q-1)$. The values e and d are called the public and private exponents, respectively.
- The public key is the pair (n, e); the private key is the pair (n, d).

It is currently difficult to obtain the private key d from the public key (n, e). However if one could factor n into p and q, then one could obtain the private key d. Thus, the security of RSA is based on the assumption that factoring is difficult. The discovery of an easy method of factoring would "break" RSA.

RSA Encryption

RSA can also be used to encrypt a text. To encrypt message m, the sender S creates the cipher text c by exponentiating: $c = m^e \bmod n$, where e and n are receiver R's public key. Then S sends c to R.

RSA Decryption

RSA decryption is used to recover an encrypted data back. To decrypt cipher c, the receiver R also exponentiates: $m = c^d \bmod n$, the relationship between e and d ensures that R correctly recovers m. Since only R knows d, no one else can decrypt this message.

RSA Digital Signature

Suppose the sender S wants to send a message m to a receiver R in such a way that R is assured the message is both authentic, has not been tampered with, and from S. S creates a digital signature s by exponentiating: $s = m^d \bmod n$, where d and n are S's private key. S sends m and s to R. To verify the signature, R exponentiates and checks that the message m is recovered: $m = s^e \bmod n$, where e and n are S's public key.

Thus, encryption and authentication take place without any sharing of private keys: each person uses only another's public key or their own private keys. Anyone can send an encrypted message or verify a signed message, but only someone in possession of the correct private key can decrypt or sign a message.

2.2 Related Work

In this section systems related to our work are discussed.

2.2.1 Secure Electronic Transaction

Jan L. Camenisch, et al [16], have shown that secure payment systems are critical to the success of electronic transactions. There are four essential security requirements for safe electronic payments: Authentication, Encryption, Integrity and Non-repudiation. Encryption is the key security schemes adopted for electronic payment systems, which is used in protocols like SET. SET is not a payment system by itself rather it enables users to employ the existing credit card payment infrastructure on an open network in a secure manner. The purpose of the SET protocol is to establish payment transactions that provide confidentiality of information; ensure the integrity of payment instructions for goods and services order data; authenticate both the card holder and the merchant. There are four main entities in SET: Card holder (customer), Merchant (web server), Merchant's Bank (payment gateway, acquirer) and Issuer (card holder's bank).

The cardholder encrypts the payment information using his/her private key, which also means that he/she has digitally signed the payment. Then he/she re-encrypts the digitally signed payment using a randomly generated symmetric encryption key to ensure message confidentiality. Finally he/she encrypts the message with the merchant's public key, creating a secure "digital envelope" and sends it to the merchant.

The merchant opens the "digital envelope" using the merchant's private key. Note that only the intended merchant can open the envelope. Then he/she checks the cardholder's digital signature by using the cardholder's public key. Finally, he/she decrypts the payment information using the symmetric key attached by the cardholder.

Despite being very secure, SET has not been a success in e-commerce environments. The main reason attributed is the overheads associated with SET are heavy [6].

2.2.2 Mobile Payment Systems

According to Tomi Dahlberg, et al [25], mobile payment may be defined as any payment where a mobile device is used to initiate, authorize and confirm an exchange of financial value in return for goods and services. The realization of mobile payments will make possible new and unforeseen ways

of convenience and commerce. Because of the fading use of cash, mobile devices provide the potentials to develop new substitute payment approaches for low-value transactions using financial service stations. Additionally, the need of a cost-effective means to charge payments in m-commerce environment can be achieved by mobile payment systems [5].

Performing payment transactions in wireless environments mainly suffers from resource limitations of mobile devices and characteristics of wireless networks (high latency, vulnerability to eavesdropping, etc.) [7].

2.2.3 Digital Cash

Digital cash is a payment system which enables a secure off-line transaction without revealing the payers identity. Digital cash can be used both as paper cash and electronic money since it keeps its users anonymity and enables off-line transactions. It is portable and at the same time offers the ability of electronic transactions [3].

People like to use paper cash because it is easy to carry around. They can make a payment with the received cash and they don't need to ask a third party like a bank to perform their payments. Paper cash can, however, be stolen or lost and no one compensates for the lost or stolen money.

Credit cards reduce risk of losing cashes for people, but by using electronic money people are in the risk of losing their privacy. Annually, credit card companies and banks lose large sums of money since they are required to compensate for lost cards and the costs associated with fraud and human error. In light of the explosive increase of electronic services such as Internet, the need for more efficient electronic payments has become an essential fact. Digital cash offers a solution to the problems of paper cash and today's credit cards; it is secure and protects people's privacy. The customer can use digital cash to pay over the Internet without the involvement of a bank during their payments.

General Structure of Digital Cash Transactions

There are three different types of transactions during a digital cash procedure [4]:

a) Withdrawal, in which a sender transfers some of his/her money from his/her bank account to his/her wallet
b) Payment, in which a sender transfers money from his/her wallet to the receiver.

c) Deposit, in which the receiver transfers the money he/she has received to his/her bank account.

As shown in figure 2.1, in a digital cash system, we have three kinds of actors:

- A financial network (Bank).
- A payer or consumer.
- A payee or a shop.

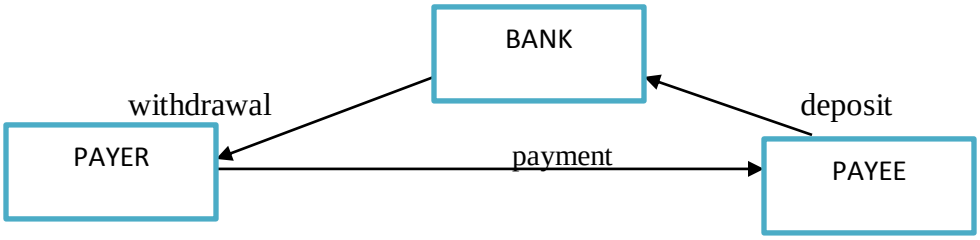

Figure 2-1: Digital Cash Transaction

2.2.4 eBay

eBay is an online auction and shopping website in which people and businesses buy and sell a broad variety of goods and services worldwide. Founded in 1995, eBay is one of the notable success stories of the dot-com bubble; it is now a multi-billion dollar business with operations localized in over thirty countries. eBay expanded from its original "set-time" auction format to include "Buy It Now" standard shopping; online event ticket trading; online money transfers (via PayPal) and other services [26].

Any user who wants to buy items from eBay must have an eBay account first. Once the account is created eBay offers two types of purchase options:

Place a Bid

When the buyer places a bid, he/she need to enter the maximum amount he/she is willing to pay for the item. eBay will bid incrementally on behalf of the buyer, based on pre-set bid increments.

Buy it Now

This time, a buyer can simply click on the Buy It Now Button at the bottom of the listing of items on eBay website. No bidding or waiting necessary.

How the buyer pay for an item depends on the payment methods accepted by the seller. The seller may offer the following payment methods: PayPal, ProPay, Skrill, Merchant Credit Card (Sellers can accept credit card payments to their Internet merchant account directly through eBay checkout by providing their payment gateway account information) and Payment up on pickup (buyer pays when he/she pick up the item). Generally, payment is carried out using credit cards.

2.2.5 Amazon

Amazon.com, Inc. is an American multinational electronic commerce company with headquarters in Seattle, Washington, United States. It is the world's largest online retailer. The company also produces consumer electronics - notably the Amazon Kindle e-book reader - and is a major provider of cloud computing services [27].

Payment in Amazon is carried out using Amazon.com account which contains the shipping and payment information of the buyer. It is possible to pay with Amazon.com account on any online store or nonprofit website accepting Amazon Payments without having to re-enter credit card information which is already stored in Amazon.com account.

2.3 Chapter Summary

In all related works discussed above, online payment is carried out through the use of a credit card which is very expensive to implement its infrastructure and control fraud [11, 4].

Taking the above issues into consideration, we are seeking to design and implement a system that can facilitate online payment without the use of credit cards. Instead, Digital Birr and Digital Bond, a low budget payment code, are used. Electronic transactions are sensitive, can be interrupted easily unless a way for protection is not given a highly-coordinated attention. Hence, security will be a very crucial asset for the implementation of the proposed system and cryptographic primitives (encryption, digital signature, message digest) will be given very high attention while designing and implementing the proposed system.

CHAPTER THREE

SYSTEM ANALYSIS

3.1 Overview

This Chapter presents an overview of the proposed system and the system models using use case, class and sequence diagrams.

3.2 Overview of Online Digital Payment System

The Online Digital Payment System is intended to provide an environment by which buying and selling of non-tangible items and bonds online is possible without using credit cards.

3.2.1 Functional Requirements

In order to come up with a solution for the problems discussed in section 1.2 of chapter one, we need to develop a web-based online payment system with the following functional requirements:

- The system should be able to add new users and online shops with necessary information
- The system should generate necessary report about users, online shops, and market transactions.
- The system should be able to add items to online shops
- The system should allow any user to buy any non-tangible item from online shops
- The system should be able to generate D-Birr and Bond codes
- The system should allow buying and selling of D-Birr and Bonds
- The system should provide different access levels to the administrators, online shop owners and the users.
- The system should allow the users to search for necessary items

3.2.2 Non-Functional Requirements

Non-functional requirements are constraints on the operation of the system. This section discusses security requirements, performance requirements and reliability requirements.

Security requirements

Security requirements are important factors in this system as payment transactions are vulnerable to different kinds of attacks. To make sure that the system is secure enough, different security techniques will be implemented. These techniques include digital signature, password hashing, and public key cryptography based encryption and decryption. Form validation will be done during any input-based functions to insure that the data is valid and the system is not vulnerable for attacks such as SQL injection. Session variables will be assigned a fixed time to expire so that the system will not be vulnerable to attacks such as session hijacking and so on.

Performance requirement

Performance is the degree to which a system or component accomplishes its designated functions within given constraints, such as speed, accuracy, or memory usage. A performance requirement is a requirement that imposes conditions on a functional requirement; for example, a requirement that specifies the speed, accuracy, or memory usage with which a given function must be performed. Therefore, the system shall respond as fast as possible in generating report and performing other functionalities of the system.

Reliability

Reliability is one of the important attributes that every system should have. Therefore, our system needs to be reliable in a way that it must continue operating in the expected way over time. For this a thorough testing will be done.

3.3.Analysis Model

To produce a model of the system which is correct, complete and consistent we need to construct the analysis model which focuses on structuring and formalizing the requirements of the system. Analysis model contains three models: functional, object and dynamic models. The functional model can be described by use case diagrams. Class diagrams describe the object model. Dynamic model can also be described in terms of sequence, state chart and activity diagrams. For the purpose of this project we have described the dynamic models using sequence diagrams.

3.3.1 Use case Diagram

A use case diagram is used to describe the functionality of the system from an external point of view. The use case model is one which is considered as a functional model. Use cases of Online Digital Payment System are “Register Online Shop”, “Request Bond”, Request Digital Birr”, “Verify Shop”, “Generate Bond”, “Generate Digital Birr”, “Generate Report”, “Add Item”, “Sell Digital Birr”, “Sell Bond”, “Create Profile”, “Edit Profile”, and “Buy Item”. The actors are Administrator, User and ShopOwner.

3.3.2 Actor Description

Name: **Administrator**

Description: An administrator is a person who verifies the creation of online shops, generate D-Birr, Sell D-Birr for shops (both online and offline), generate transaction report and control overall system settings.

Name: **User**

Description: A user is a person that registers himself on the system and uses the functionalities of the system such as buy D-Birr, Buy items, edit his profile.

Name: **ShopOwner**

Description: A ShopOwner is a special user who is registered as an ordinary user and later creates his own online shop. This actor also uses the functionalities of the system such as buy D-Birr, Sell D-Birr, Sell items, Add new items.

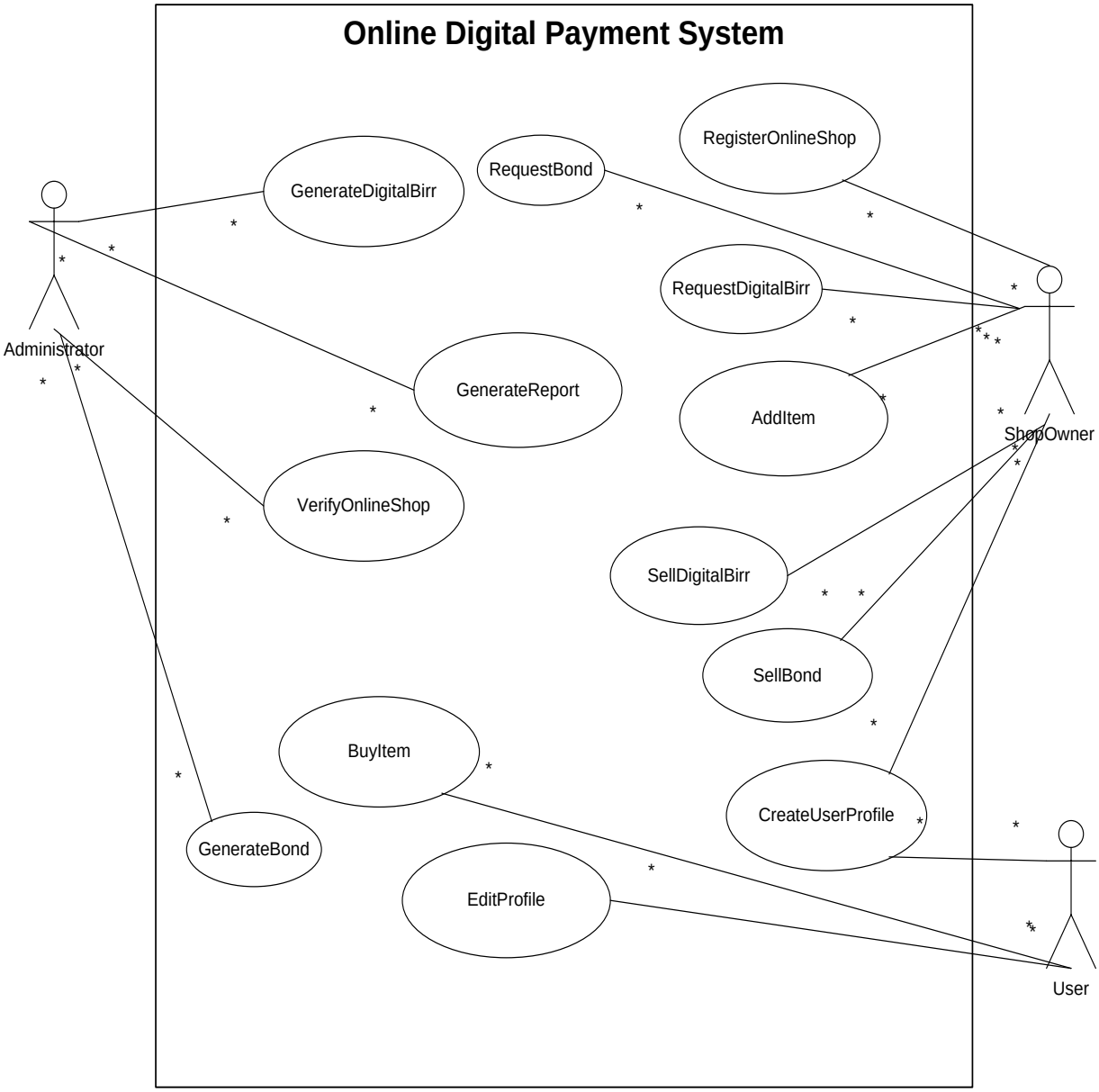

Figure 3-1: Use case diagram for Online Digital Payment System

3.3.3 Use Case Description

Name: GenerateDigitalBirr

Actor: Administrator

Description: To generate Digital Birr

Precondition: 1) Administrator must be logged in

2) A buyer (shop owner) must be a registered party and request must be sent

Flow of Events:

(1) A buyer (offline shop owner) wants to buy some amount of Digital Birr

(2) Administrator logs into the system [Alt 2]

(3) Administrator verifies that the requesting party is valid [Alt 3]

(4) Registration form will be given to the buyer

(5) The buyer completes the form that contains information like amount of Digital Birr, shop's ID and other details.

(6) Administrator checks whether the contents of the form is properly completed

(7) Administrator fills and submits the form to the system

(8) System registers the detail and generates Digital Birr

(9) Use case ends

Alternative Flow of Events

Alternative flow Alt 2: Administrator's password and/or ID is not valid

Alt 2.1. The system shows an error message

Alt 2.2. Use case ends

Alternative flow Alt 3: The buyer is not registered

Alt 3.1. The system shows an error message

Alt 3.2. Use case ends

Post Condition: Digital Birr generated and sold to buyer

Name: GenerateBond

Actor: Administrator

Description: To generate Digital Birr

Precondition: 1) Administrator must be logged in

2) A buyer (shop owner) must be a registered party and request must be sent

Flow of Events:

(1) A buyer (offline shop owner) wants to buy some amount of Bond

(2) Administrator logs in to the system [Alt 2]

(3) Administrator verifies that the requesting party is valid [Alt 3]

(4) Registration form will be given to the buyer

(5) The buyer completes the form that contains information like amount of Bond, shop's ID and other details.

(6) Administrator of the system checks whether the contents of the form is properly completed

(7) Administrator fills and submits the form to the system

(8) System registers the detail and generates Bond

(9) Use case ends

Alternative Flow of Events

Alternative flow Alt 2: Administrator's password and/or ID is not valid

Alt 2.1. The system shows an error message

Alt 2.2. Use case ends

Alternative flow Alt 3: The buyer is not registered

Alt 3.1. The system shows an error message

Alt 3.2. Use case ends

Post Condition: Bond generated and sold to buyers

Name: GenerateReport

Actor: Administrator

Description: To view which Digital Birr is sold to whom

Flow of Events:

(1) Administrator wants to view market transactions regarding Digital Birr

(2) Administrator logs in to the system [Alt 2]

(3) Administrator selects to view the required report

(4) System displays the appropriate report

(5) Administrator prints out the report

(6) Use case ends

Alternative Flow of Events

Alternative flow Alt 2: Administrator's password is invalid

Alt 2.1. The system shows an error message

Alt 2.2. Use case ends

Name: VerifyOnlineShop

Actor: Administrator

Description: To approve the creation of online shop

Precondition: 1) Administrator must be logged in

2) Online shop creation information must be submitted

Flow of Events:

(1) Administrator wants to verify an online shop

(2) Administrator logs in to the system [Alt 2]

(3) System displays a list of requests

(4) Administrator selects a request to approve

(5) Administrator approves the creation

(6) Approval information sent to ShopOwner

(7) Use case ends

Alternative Flow of Events

Alternative flow Alt 2: Administrator's password is invalid

Alt 2.1. System cannot display list of requests

Alt 2.2. Use case ends

Post condition: Online shop created

Name: CreateUserProfile

Actor: User

Description: To add new members of the system

Flow of Events:

(1) A user wants to be part of the system

(2) The user fills necessary information

(3) System validates input data [Alt 3]

(4) System create a profile for the User

(5) Use case ends

Alternative Flow of Events

Alternative flow Alt 3: Input data validation failed

Alt 3.1. System displays error message

Alt 3.2. Use case ends

Name: BuyItem

Actor: User

Description: To buy any items online from online shops

Precondition: A User must have bought enough amounts of Digital Birr to buy that item

Flow of Events:

(1) A User wants to buy an item

(2) The User logs into the system [Alt 2]

(3) The User searches an item he/she wants to buy [Alt 3]

(4) The system lists the item

(5) The User fills the payment form with Digital Birr [Alt 5]

(6) The User owns that item

(7) Use case ends

Alternative Flow of Events

Alternative flow Alt 2: The User is not registered

Alt 2.1. The system displays an error message

Alt 2.2. Use case ends

Alternative flow Alt 3: The item is not available

Alt 3.1. The system cannot list items

Alt 3.2. Use case ends

Alternative flow Alt 5: The amount of Digital Birr is not enough

Alt 5.1. The system displays error message

Alt 5.2. Use case ends

Post condition: The user bought the item

Name: EditProfile

Actor: User

Description: To modify the details of a user's profile

Precondition: The user must be logged in

Flow of Events:

(1) A User wants to edit the details of his/her profile

(2) The User logs into the system [Alt 2]

(3) The User selects an edit option

(4) The User edits his/her profile

(5) The system validate edited data [Alt 5]

(6) The system saves new profile

(7) Use case ends

Alternative Flow of Events

Alternative flow Alt 2: The User's password is invalid

Alt 2.1. The system displays an error message

Alt 2.2. Use case ends

Alternative flow Alt 5: Edited data validation failed

Alt 5.1. The system displays an error message

Alt 5.2. Use case ends

Post condition: User profile edited

Name: RegisterOnlineShop

Actor: ShopOwner

Description: To create new online shop (virtual shop)

Precondition: The shop owner must have valid TIN number and must be a registered user

Flow of Events:

(1) The User logs into the system [Alt 1]

(2) The User selects shop creation option

(3) The system displays a registration form

(4) The User fills and submits the form

(5) The system validates the form [Alt 5]

(6) The system sends the request to administrator

(7) Use case ends

Alternative Flow of Events

Alternative flow Alt 1: The user's password is invalid

Alt 1.1. User cannot create a shop

Alt 1.2. Use case ends

Alternative flow Alt 5: Form validation failed

Alt 5.1. The system displays an error message and the request is not sent

Alt 5.2. Use case ends

Name: AddItem

Actor: ShopOwner

Description: To add items to online shop

Precondition: The online shop must be verified and created

Flow of Events:

(1) The ShopOwner wants to add new item

(2) The ShopOwner logs into the system [Alt 2]

(3) The ShopOwner open his/her shop [Alt 3]

(4) The ShopOwner browse item and adds to shop

(5) System uploads item

(6) System displays the appropriate status

(7) Use case ends

Alternative Flow of Events

Alternative flow Alt 2: ShopOwner not registered

Alt 2.1. The ShopOwner cannot login

Alt 2.2. Use case ends

Alternative flow Alt 3: Shop not created

Alt 3.1. Shop cannot be opened

Alt 3.2. Use case ends

Name: SellDigitalBirr

Actor: ShopOwner

Description: Sell some amount of Digital Birr for users

Precondition: 1) The ShopOwner must be logged in

2) The buyer must be registered

Flow of Events:

(1) A User wants to buy digital birr

(2) The ShopOwner logs into the system [Alt 2]

(3) System displays a form containing details like buyers ID, amount of digital birr and so on

(4) The ShopOwner searches the buyers' ID [Alt 4]

(5) The ShopOwner fills digital birr selling form [Alt 5]

(5) System prints out a receipt

(6) Use case ends

Alternative Flow of Events

Alternative flow Alt 2: ShopOwner password is invalid

Alt 2.1. The ShopOwner cannot open his online shop

Alt 2.2. Use case ends

Alternative flow Alt 4: the buyer's ID is invalid

Alt 4.1. System cannot print out receipt and displays error message

Alt 4.2. Use case ends

Alternative flow Alt 5: the requested amount of Digital Birr is larger than the available amount

Alt 5.1. System cannot print out receipt and displays error message

Alt 5.2. Use case ends

Name: SellBond

Actor: ShopOwner

Description: Sell some amount of Bond for users

Precondition: 1) The ShopOwner must be logged in

2) The buyer must be registered

Flow of Events:

(1) A User wants to buy bond

(2) A ShopOwner logs in to the system [Alt 2]

(3) System displays a form containing details like buyers ID, amount of bond and so on

(4) ShopOwner searchs the buyers' ID [Alt 4]

(5) ShopOwner fills digital birr selling form [Alt 5]

(5) System prints out a receipt

(6) Use case ends

Alternative Flow of Events

Alternative flow Alt 2: ShopOwner password is invalid

Alt 2.1. The ShopOwner cannot open his online shop

Alt 2.2. Use case ends

Alternative flow Alt 4: the buyer's ID is invalid

Alt 4.1. System cannot print out receipt and displays error message

Alt 4.2. Use case ends

Alternative flow Alt 5: the requested amount of Bond is larger than the available amount

Alt 5.1. System cannot print out receipt and displays error message

Alt 5.2. Use case ends

Name: RequestDigitalBirr

Actor: ShopOwner

Description: Request for new Digital Birr codes

Precondition: The buyer must be registered and verified by system administrator

Flow of Events:

(1) The shop owner wants to request for digital birr

(2) The ShopOwner logs in to the system [Alt 2]

(3) System displays a form containing details like amount of Digital birr and so on

(4) The ShopOwner fills in the form and submits

(5) System submits the form

(6) Use case ends

Alternative Flow of Events

Alternative flow Alt 2: ShopOwner password is invalid

Alt 2.1. The ShopOwner cannot open his online shop

Alt 2.2. Use case ends

Name: RequestBond

Actor: ShopOwner

Description: Request for new Bond codes

Precondition: The buyer must be registered and verified by system administrator

Flow of Events:

(1) The shop owner wants to request for Bond

(2) The ShopOwner logs in to the system [Alt 2]

(3) System displays a form containing details like amount of Bond and so on

(4) The ShopOwner fills in the form and submits

(5) System submits the form

(6) Use case ends

Alternative Flow of Events

Alternative flow Alt 2: ShopOwner password is invalid

Alt 2.1. The ShopOwner cannot open his online shop

Alt 2.2. Use case ends

3.3.4 Sequence Diagrams

The sequence diagram is used to formalize the behavior of the system and to visualize the communication among objects of the system. It is the one that shows the dynamic model for this work. The sequence diagram for all use cases is shown in Appendix A.

3.3.5 Class diagram

The class diagram shown in Figure 3.2 describes the structure of the Online Digital Payment System using classes of the system.

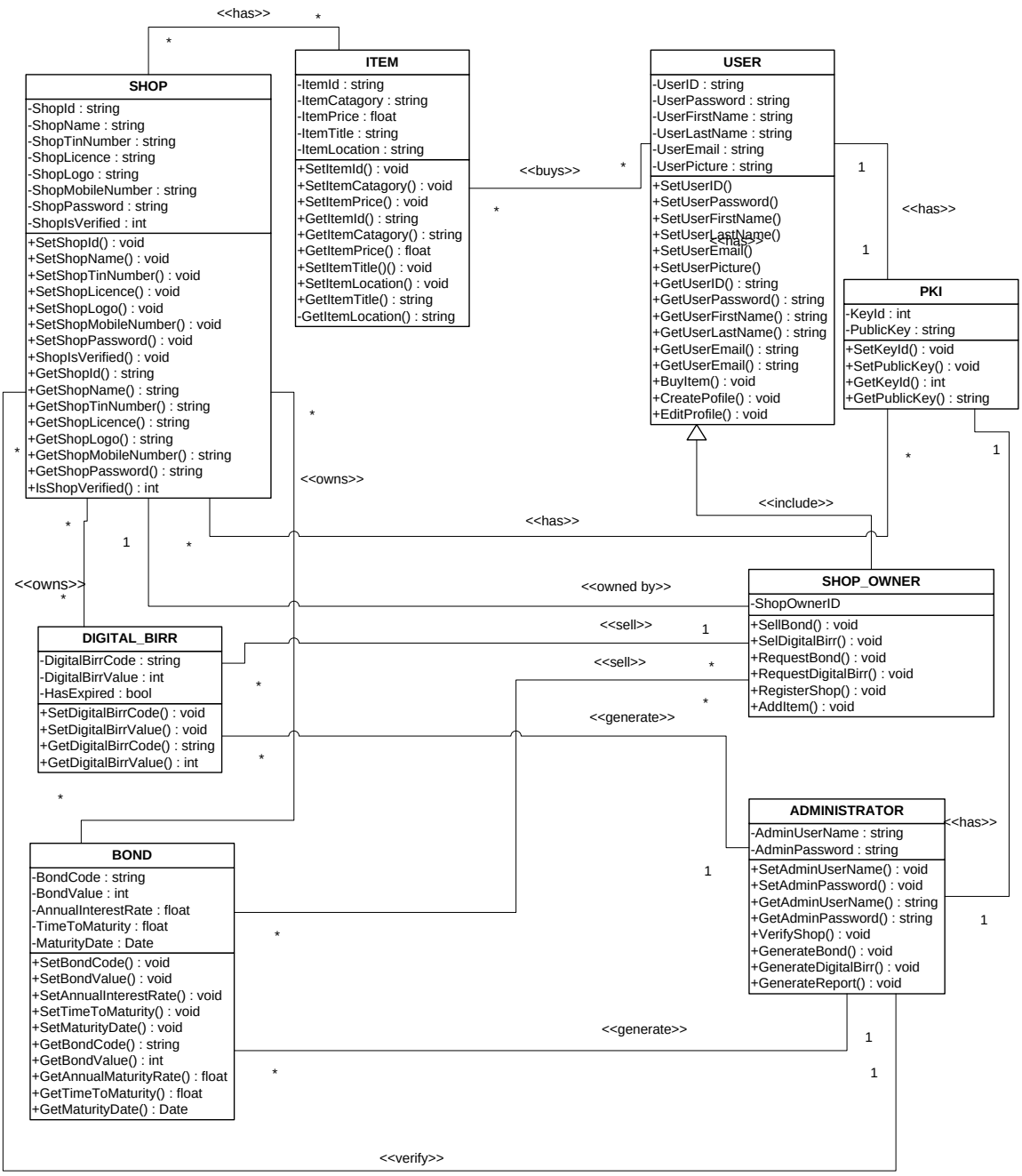

Figure 3-2: Class diagram for Online Digital Payment System

CHAPTER FOUR

SYSTEM DESIGN

4.1 Overview

In chapter three we have identified the functional and non-functional requirements of the system and produced the analysis model. In this Chapter, we discuss the design of the Online Digital Payment System. Particularly, we discuss the design goal of the system, the proposed software architecture for the system, sub-system decomposition, system deployment, database design and the user interface design.

4.2 Design goals

The design goal of a given system is derived from its non-functional requirements.

Generally, we consider the following design goals.

- Performance
- Dependability, and
- Maintenance

Performance

Performance of a system can be seen in terms of response time, throughput and memory handling. Every part of the system should have a fast response time (real time) with maximum throughput.

Dependability

The notion of dependability is broken down mainly into four fundamental properties: reliability, availability, confidentiality and integrity. Taking those in to consideration, it is expected that Online Digital Payment System will be operational when needed (availability), that it will keep operating correctly while being used (reliability), that there will be no unauthorized disclosure (confidentiality) or modification (integrity) of information that the system is using.

Maintenance

Maintenance mainly encompasses extensibility, modifiability, adaptability, portability, readability and traceability of requirements. The proposed system should be easily extensible to add new functionalities at a later stage as its design is based on object oriented approach. It should also be easily modifiable to make changes to the features and functionalities.

4.3 Architecture of the System

The architecture chosen for the system is a three-tier system architecture. The first layer runs on the client side (i.e. using web browsers), the second layer at the middle layer and the third layer will be the database system. The system will run using web technology.

Presentation Layer: it is a high-level layer through which the users can interact with Online Digital Payment System. It contains web browser along with java script cryptographic libraries for the purpose of implementing RSA, public key cryptography algorithm and SHA-1, hashing algorithm. Form validation functionalities also reside on this layer.

Business Logic Layer: the functional requirements of the system are implemented here on this layer. As per the request of the user (i.e. the request sent through the network), this layer triggers the corresponding functionality. It contains server-side scripting files (aspx and aspx.cs files) which can access the data storage layer.

Data Storage Layer: is it the back-end for Online Digital Payment System. It is used for persistent data management. Every data related to the system is stored on this layer. The data on this layer can only be accessed by business logic layer.

The overall architecture of Online Digital Payment System is developed as shown in Figure 4-1. There are four main components, Security Manager, User Manager, Shop Manager and Administrator. These components are further discussed in section 4.4.

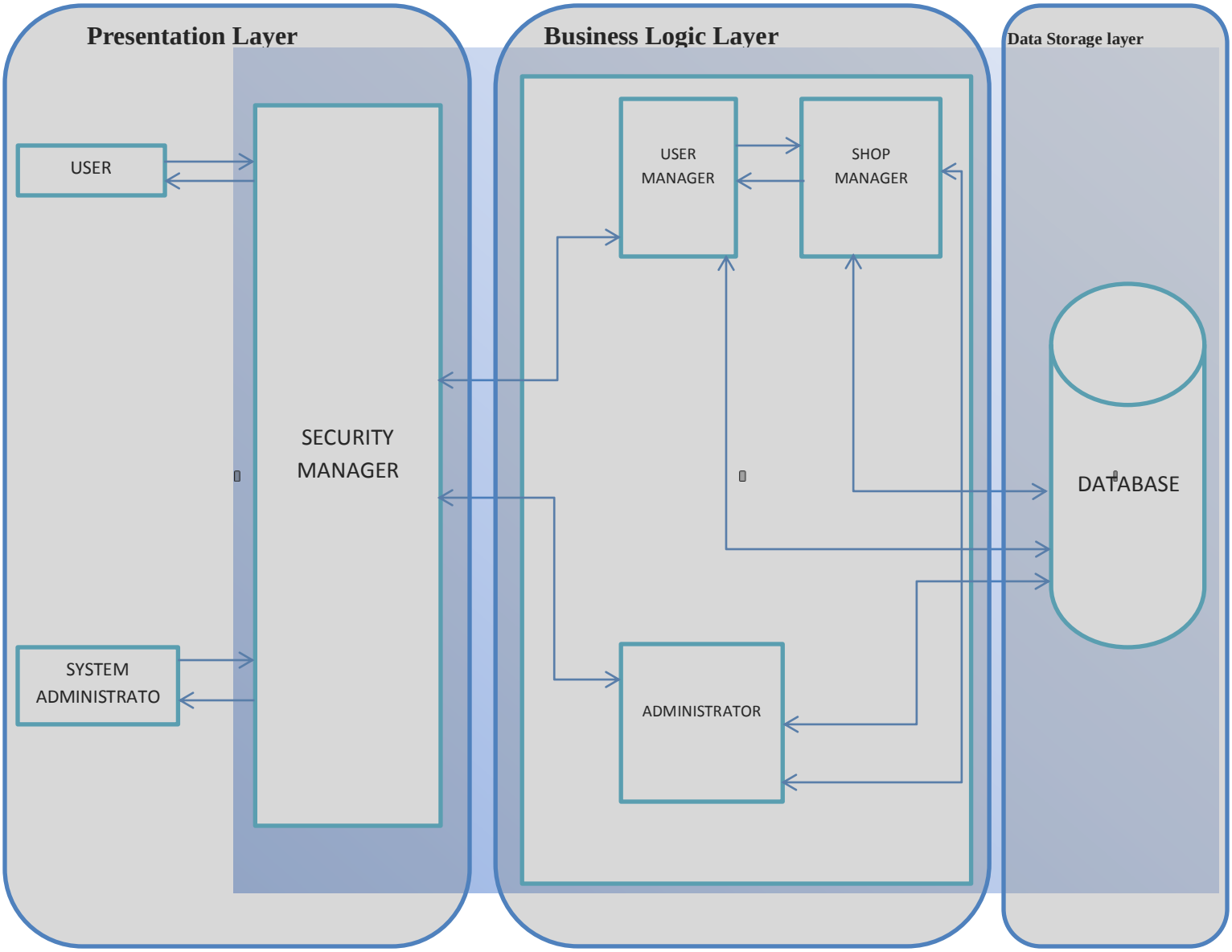

Figure 4-1: Overall architecture of Online Digital Payment System

4.4 Subsystem Decomposition

In order to simplify and minimize complexity of the system, Online Digital Payment System has been divided into four subsystems. These are Administrator subsystem, Shop Manager subsystem, User Manager subsystem, and Security Manager subsystems. The decomposition of the system is represented in Figure 4-2.

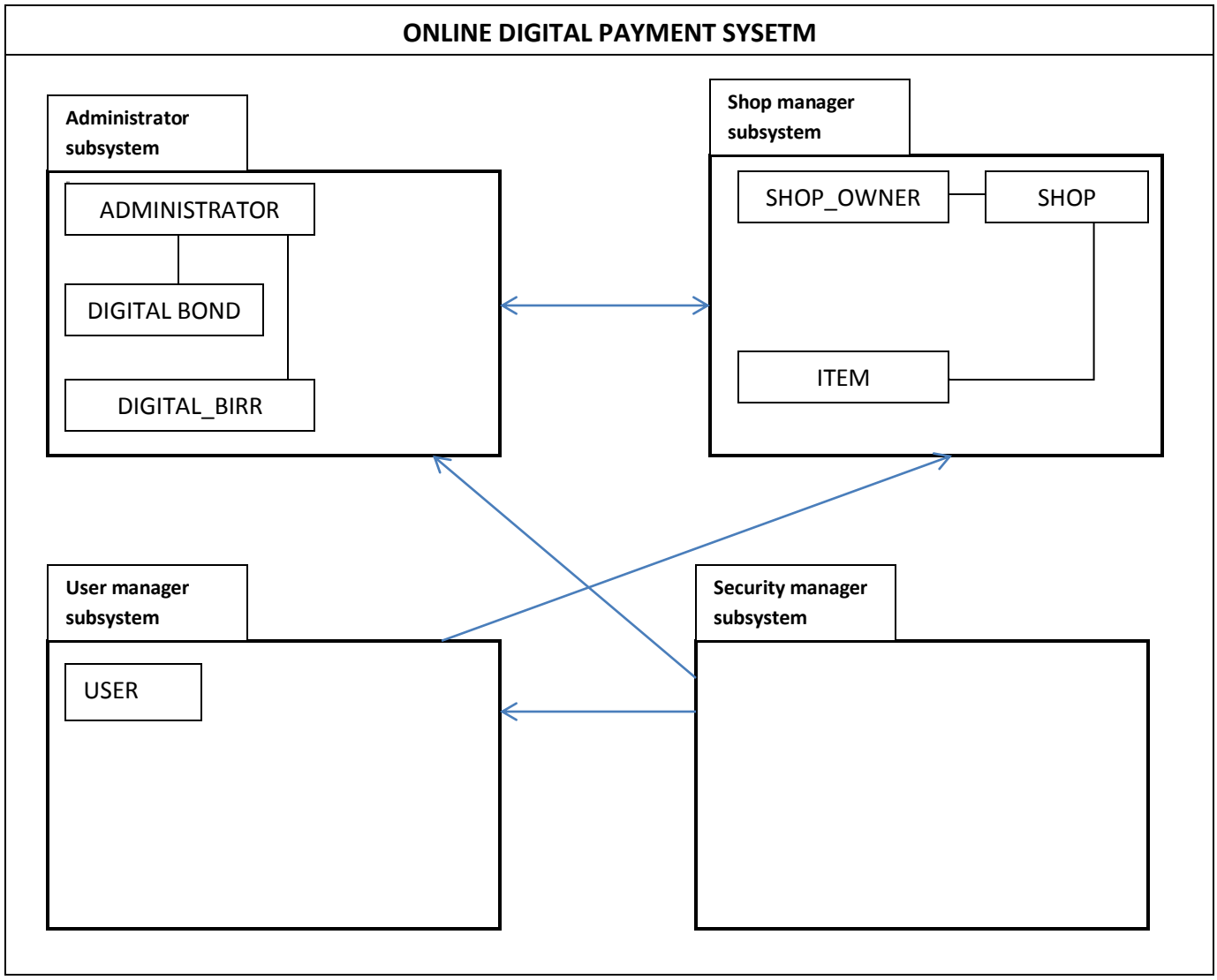

Figure 4-2: System decomposition diagram for Online Digital Payment System

4.4.1 Administration subsystem

This subsystem enables the administrator to manage issues related to security, Digital Birr generation, shop verification and report generation. The management includes generating digital birr numbers as per the request of online shop owners, verifying shop creation requests based on the criterion of the system, and generating reports containing information like amount of items sold by a particular shop, and so on.

4.4.2 Shop manager subsystem

This subsystem is mainly responsible to manage issues related to creating shops, buying Digital Birr, adding new items, selling items and even selling digital birr for a user. The activities include sending requests to create new online shops and adding items once the request is verified. Additionally, selling items to users and providing with receipt is the issue under this subsystem.

4.4.3 Security manager subsystem

The main function of security subsystem is insuring the security of the data sent and received over the network. Every transaction data needs to be secured enough so that confidentiality, availability and integrity can be achieved. In order to do that, this subsystem manages issue related to message encryption and decryption, digital signature generation, signature verification, captcha image authentication, and password hashing.

4.4.4 User manager subsystem

In this subsystem, the issues regarding all transaction related to system users are managed. These include creating user profile, editing user profile, buying items, buying digital birr and so on. Activities include creating new user account without the interaction of any other system administrators and using the account later to create online shop, buy digital birr, buy items and so on.

4.5 Payment model

In Online Digital Payment System, payment is carried out using Digital Birr. This approach will also make the system users less vulnerable to attacks as the Digital Birr and Digital Bond codes are not fixed to a specific user. Once the amount of the code is consumed by the user, it will no longer be used for payment transactions (i.e. it will expire) and that can reduce the security holes through which attackers try to penetrate into the system. A Digital Birr is a string consisting of random characters from 62 characters set (a-z|A-Z|0-9). Generally, it has the following characteristics:

- It is generated by system administrator upon a request by a Shop Owner who later on sells it for any user in the form of a receipt.
- It has some amount of money value (e.g. a 25 Birr DB)
- Its amount of money value will be reduced upon a particular purchase of goods
- It has expiry date (i.e. once its value is reduced to null it will no longer be usable)

- It is able to identify its user (i.e. the system is able to identify who bought which Digital Birr from which Shop)

Payment for Bond purchase is carried out using Digital Bond (electronic version of a tangible financial bond) which is also a string consisting of random characters from 62 characters set (a-z|A-Z|0-9) with extra properties like maturity date, interest rate and so on. It has the following characteristics:

- It is generated by system administrator upon a request by a Shop Owner who later on sells it for any user in the form of a receipt.
- It has some amount of money value (e.g. a 1000 Birr DB)
- It is able to identify its user (i.e. the system is able to identify who bought which Digital Bond from which Shop)

The Online Digital Payment System is operated by a payment system provider, in our case a bank. As shown in Figure 4-3 [35], two different banks (payer's bank and payee's bank)will be involved in the payment process. However, in our system, only one bank is involved in the payment process. This is shown in figure 4-4 and 4-5. Figure 4-3 (a) shows the process when payment modality is cash. Figure 4-3 (a) shows the process when payment modality is check. Figure 4-3 (a) shows the process when payment modality is credit card.

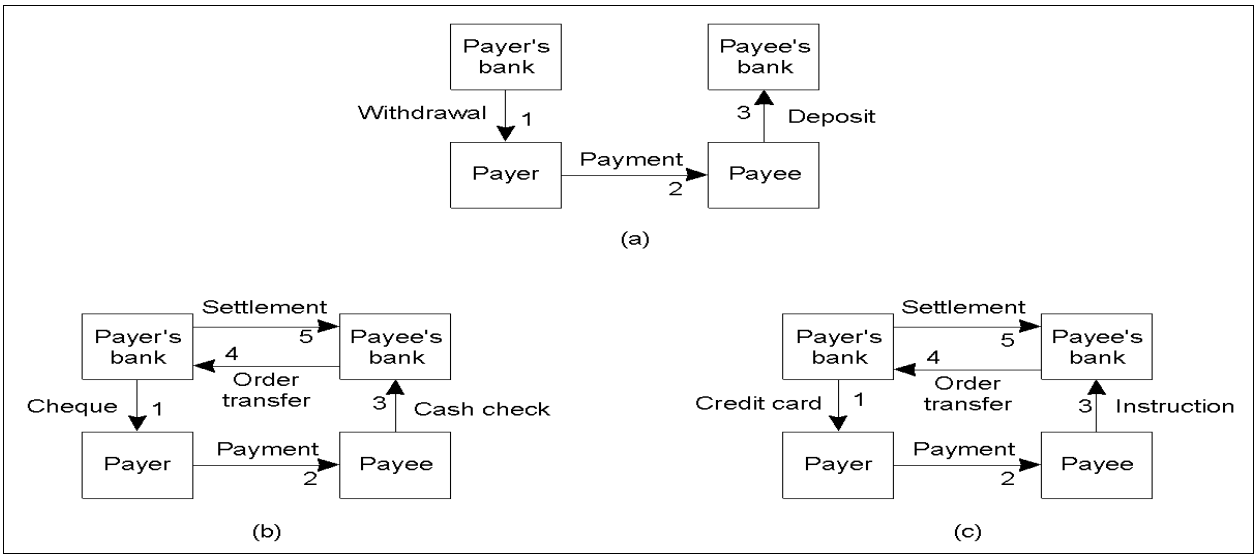

Figure 4-3: Payment systems - based on direct payment

Any user who uses Online Digital Payment System should pass through the following flow of events.

- User (Payer) creates an account
- Shop Owner creates a Shop
- Bank (System Provider) verifies the Shop created by Shop Owner
- Shop Owner requests for Digital Birr and/or Digital Bond
- Bank (System provider) approves the request and generates new Digital Birr and/or Digital Bond codes for the requesting Shop
- Shop Owner sells Digital Birr and/or Digital Bond to the user

If the code is Digital Birr

- User browses for a Shop selling items (payee). (Note: Payee Shop could be owned by the Shop Owner from which a User has bought Digital Birr or some other shop owned by some other owner. But all are part of the system)
- User buys an item using Digital Birr
- Payee Shop sends deposit information to the Bank (System Provider)

Else if the code is Digital Bond

- User buys Digital Bond using the Digital Bond code
- User sends notification to the Bank

Payment models for buying goods and a bond are shown in Figure 4-4 and Figure 4-5 respectively.

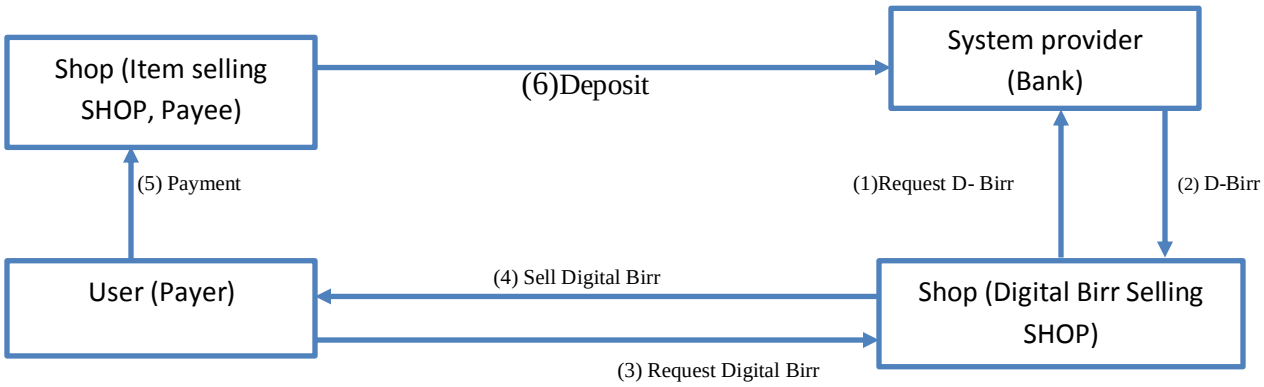

Figure 4-4: Payment model for buying an item

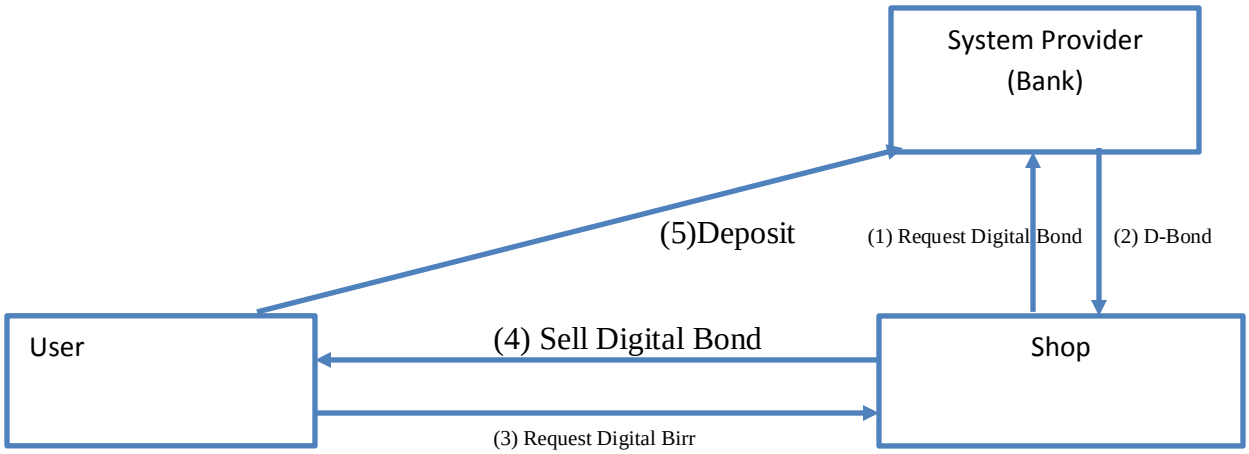

Figure 4-5: Payment model for buying bond

4.6 Hardware/Software Mapping

Hardware/software mapping is one of the major tasks in system design which deals with which components would be part in which hardware and so on. Online Digital Payment System consists of web based system used by administrators, shop owners and users. All of the above users of the system simply need to start their browsers and enter the URL of the application Web site. The server hosting the Web site is responsible for allocating all the resources the Web application requires. All components of the entire system run on different hardware but work as if they reside on one machine. The deployment diagram describes the relationship of components with that of hardware nodes. It gives a high-level view of each component. Figure 4-6 shows the deployment.

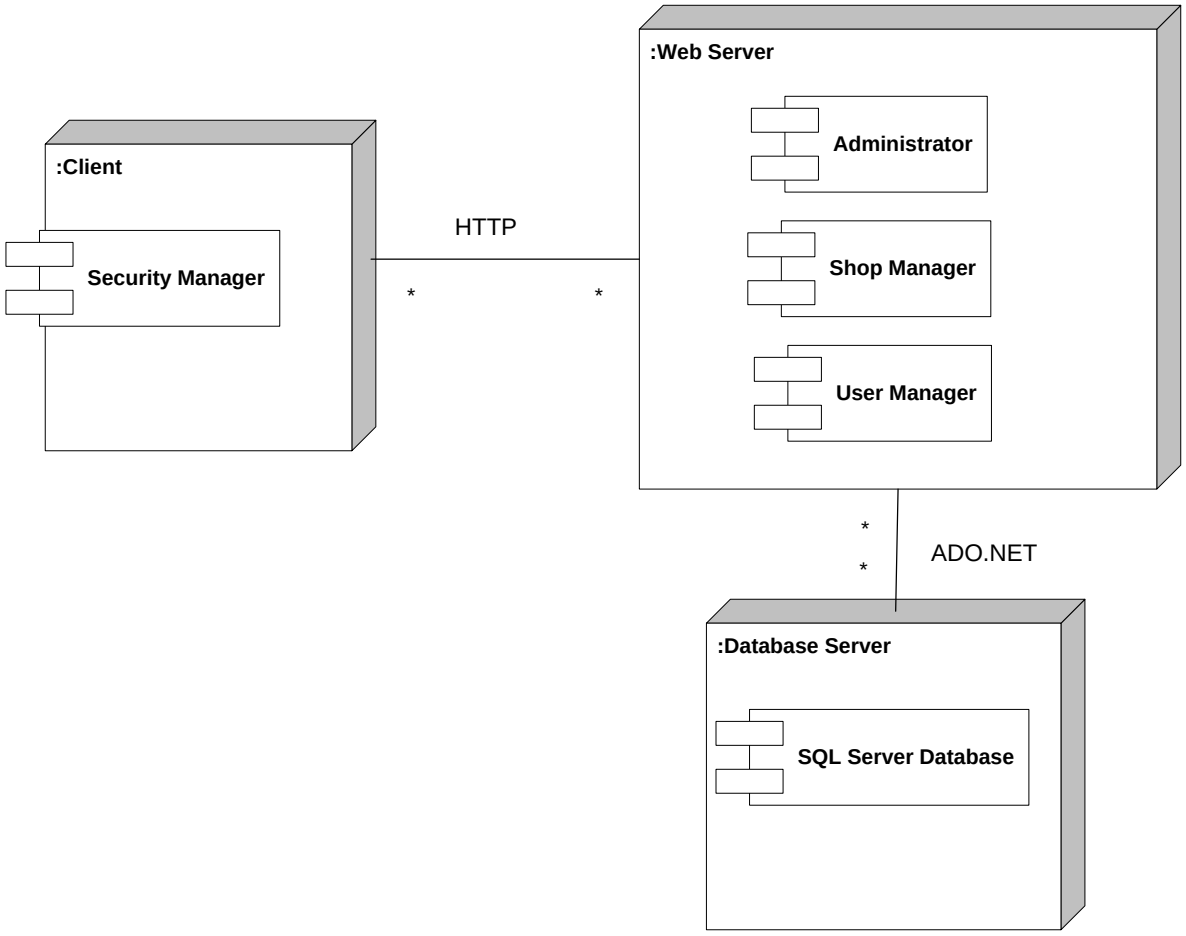

Figure 4-6: Deployment diagram for Online Digital Payment System

4.7 Persistent Data Management

Persistent data management deals with how the persistent data are stored and managed. The user's profile, Digital Birr values, shop profile, shop item data, have to be persistently kept in the database; otherwise it is not possible for the system to operate correctly and data duplication may occur which may lead to the entire system failure.

4.7.1 Relationships among Tables

This part is to describe and show the necessary relationships among the tables, which are selected to store the data persistently in the system. Generally there are three types of relationships in a relational database system. These are one-to-one, one-to-many and many-to-many relationships. The relationship among tables is shown in Figure 4-7.

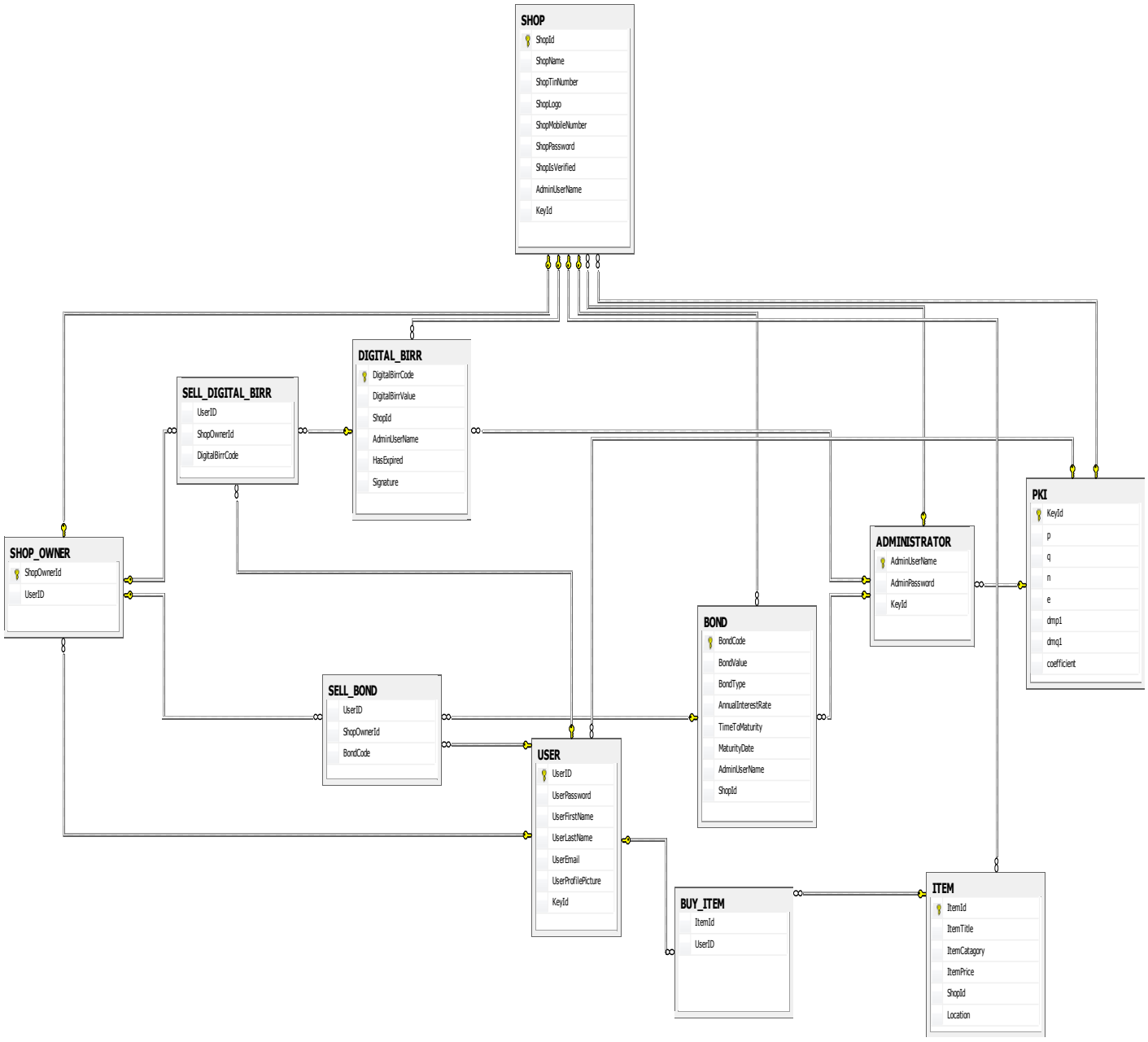

Figure 4-7: Relationship among tables

CHAPTER FIVE

IMPLEMENTATION

In this Chapter, the development tools used in the implementation of the Online Digital Payment System prototype are presented and the prototype itself is discussed by taking its sample snapshots from web browsers.

5.1 The System Development

5.1.1 Development Editor

For the implementation of the Online Digital Payment System prototype a web development editor is used to write the code in XHTML, ASP.NET, JavaScript and CSS. Particularly, Microsoft Visual Studio 2008 is used in the development process. Microsoft Visual Studio is an integrated development environment (IDE) from Microsoft. It is used to develop console and graphical user interface applications along with web sites, web applications, and web services [29].

5.1.2 Markup and Scripting Languages

XHTML (Extensible Hypertext Markup Language) is used as a markup language to present the contents of the Online Digital Payment System [30]. It is a family of XML markup languages that extends versions of the widely used Hypertext Markup Language (HTML), the language in which web pages are written.

While HTML was defined as an application of Standard Generalized Markup Language (SGML), XHTML is an application of XML, a more restrictive subset of SGML. Because XHTML documents need to be well-formed, they can be parsed using standard XML parsers—unlike HTML, which requires a lenient HTML-specific parser.

The dynamic part of the implementation has been done using JavaScript, client-side scripting langue and ASP.NET (C-Sharp) [31], server-side scripting languages. JavaScript is used to execute client-side functionalities like, message digest (message hashing), digital signature generation, message encryption, signature verification, message decryption and printing relevant data (e.g. Digital Birr). Generally, JavaScript is used for implementing functionalities in the presentation layer of the Online Digital Payment System.

ASP.NET (C-Sharp) is used in order to handle server-side functionalities such as item uploading and downloading, session management, data source communication and report generation. Crystal Reports, a business intelligence application used to design and generate reports from a wide range of data sources, is used as a report generator. Main functionalities of the system are implemented using this language. As it runs on the business logic layer of the system it is used as a means to communicate with both the presentation and data source (Microsoft SQL Server 2005) layers of Online Digital Payment System. IIS is used as a web server software application to run ASP.NET source codes [32].

5.1.3 jsrsasign 3.0.2 JavaScript API

It is an open source and free API for implementing RSA cryptography algorithm [33]. In our system, 256-bit-sized RSA keys are used for digitally signing a message and also for encryption and decryption of sensitive data. Additionally, based on the recommendations of NIST 800-107 [34], SHA-1 is used as a hashing algorithm for the purpose of digesting sensitive data. For example, passwords are hashed before getting stored on the database. SHA-1 has also been used along with RSA while generating digital signatures.

5.2 The Prototype

Here, the implemented Online Digital Payment System prototype is described. Interactions between the user and the system, the results of the interactions, and outputs from the system are described.

In order to use the services delivered by the system, a user should first be registered on the system to be a member. To do that, a user browses the Online Digital Payment System site. As a result, the login page is displayed as shown in Figure 5-1. The user can fill in the required fields and presses the ‘Register’ button to get registered. As shown in Figure 5-2, the ‘Key Manager’ page is displayed to provide the user with new RSA private key which is later used for digital signature, signature verification, and data encryption and decryption.

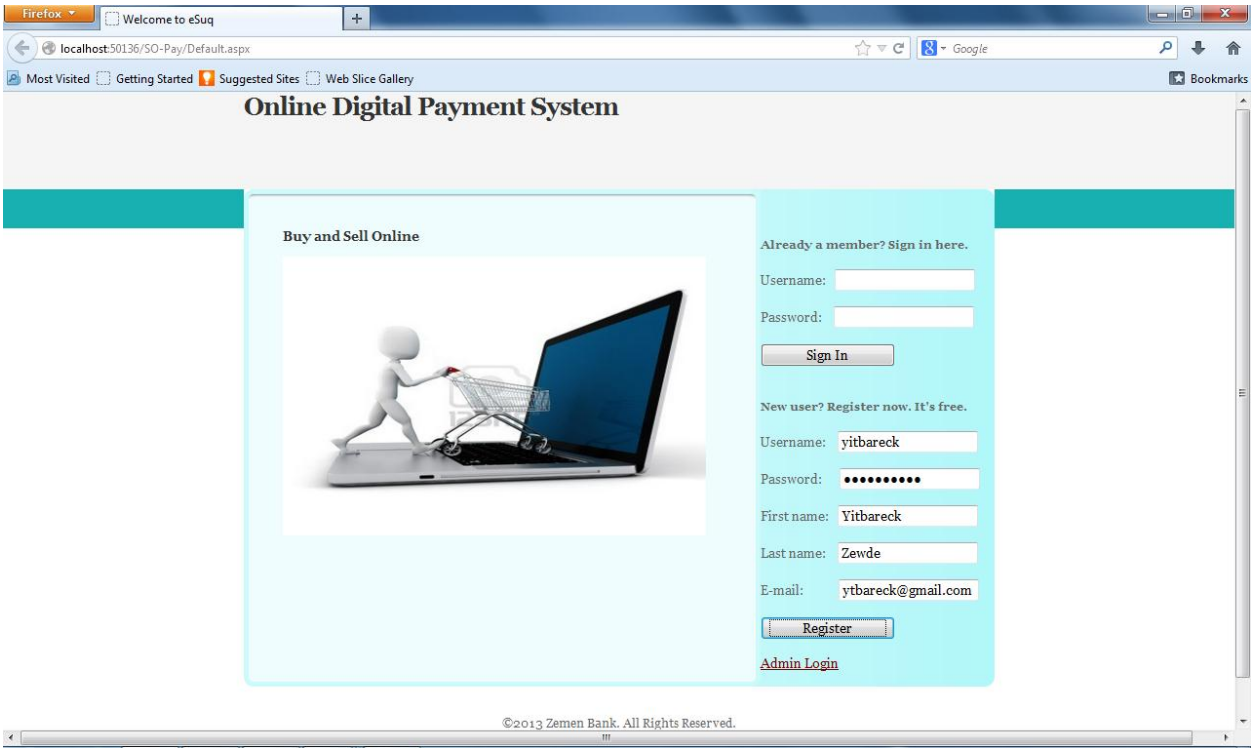

Figure 5-1: Login and registration page

Figure 5-2: Key management page

Once the user stores his private key, he/she can hit the 'Continue' button to go to the main page of the prototype. On this page, a user can do different things based on his/her status. If the user is a shop owner, he/she can create a shop as shown in Figure 5-3.

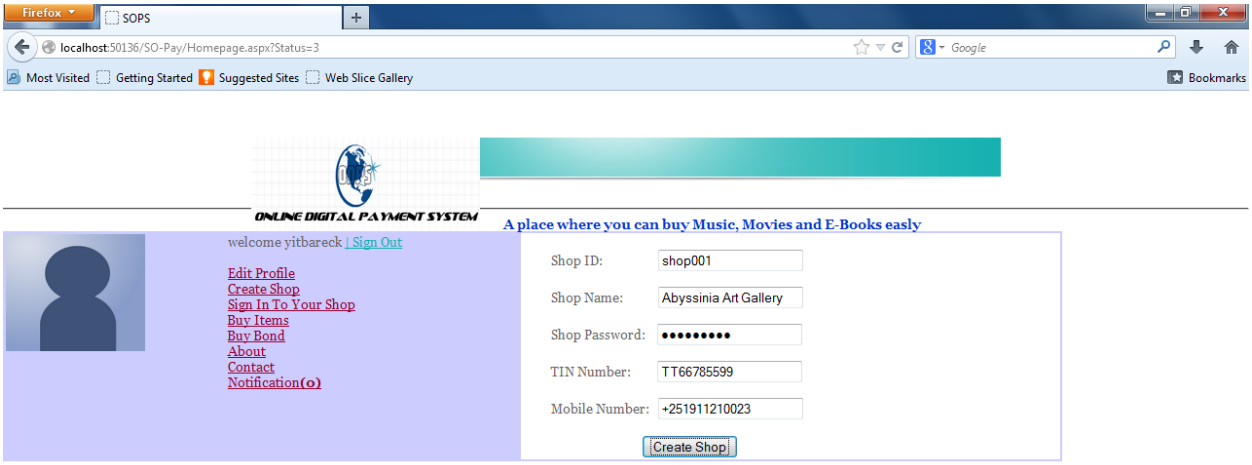

Figure 5-3: Shop creation page

Once the user submits the completed form data, a request is sent to be approved by the system administrator as shown in Figure 5-4.

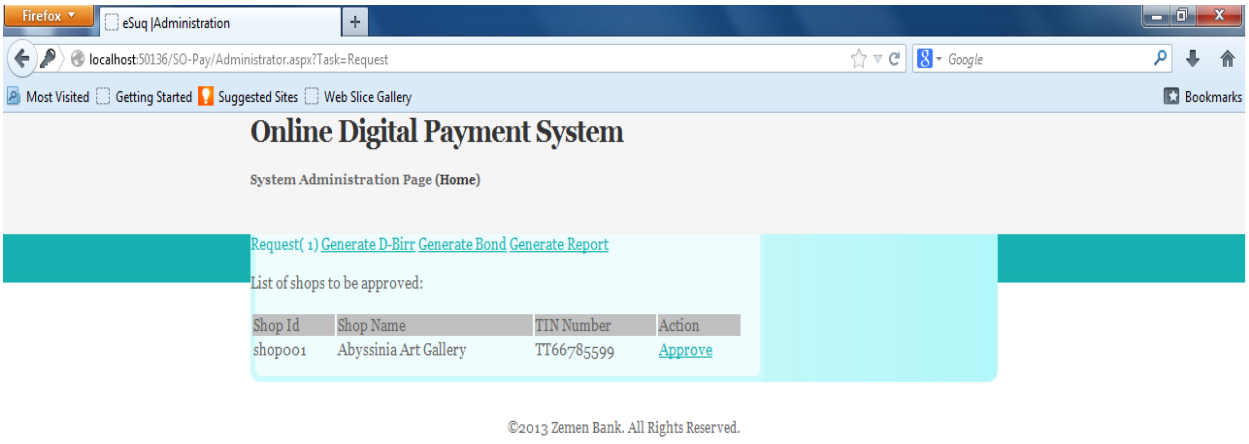

Figure 5-4: Request approval page

Upon the approval of the creation of the shop, a notification is sent back to the shop owner. The shop owner now can go to his shop and upload different items as shown in Figure 5-5.

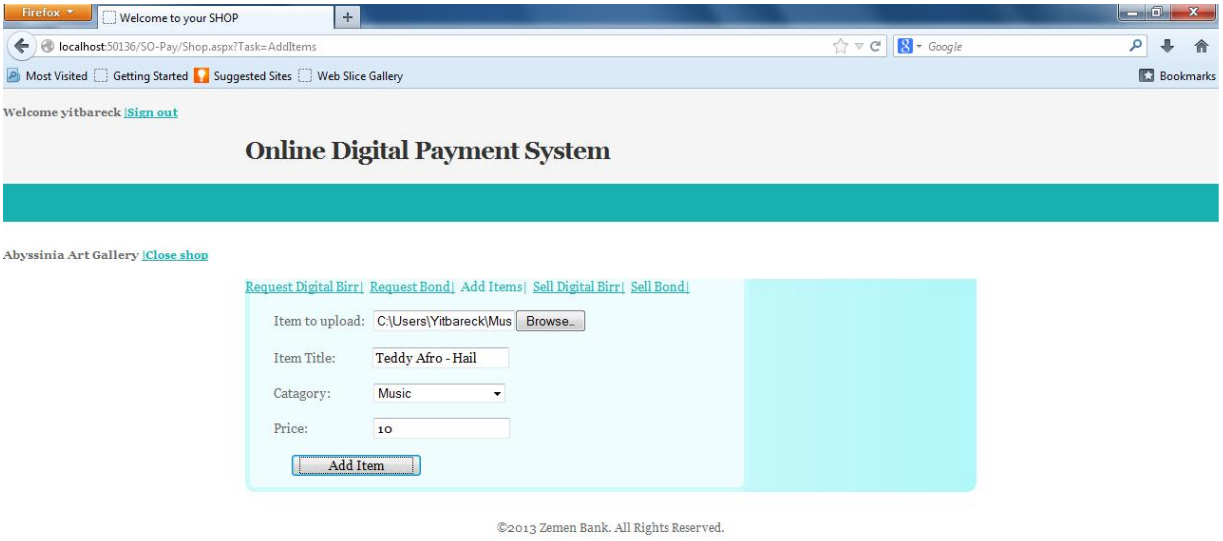

Figure 5-5: Page to add items to the shop

Additionally, the shop owner can request for Digital Birr as shown in Figure 5-6 so that it will be sold to the customers who register as normal users of the system. Once the request is received by the system administrator new Digital Birr number will be generated and signed as shown in Figure 5.7.

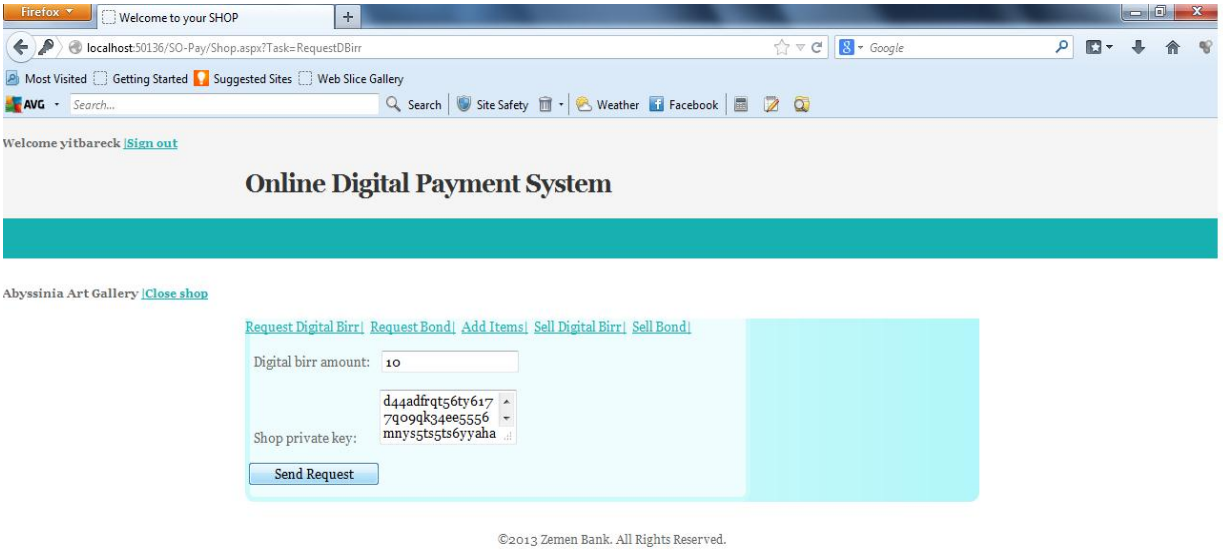

Figure 5-6: Digital Birr request page

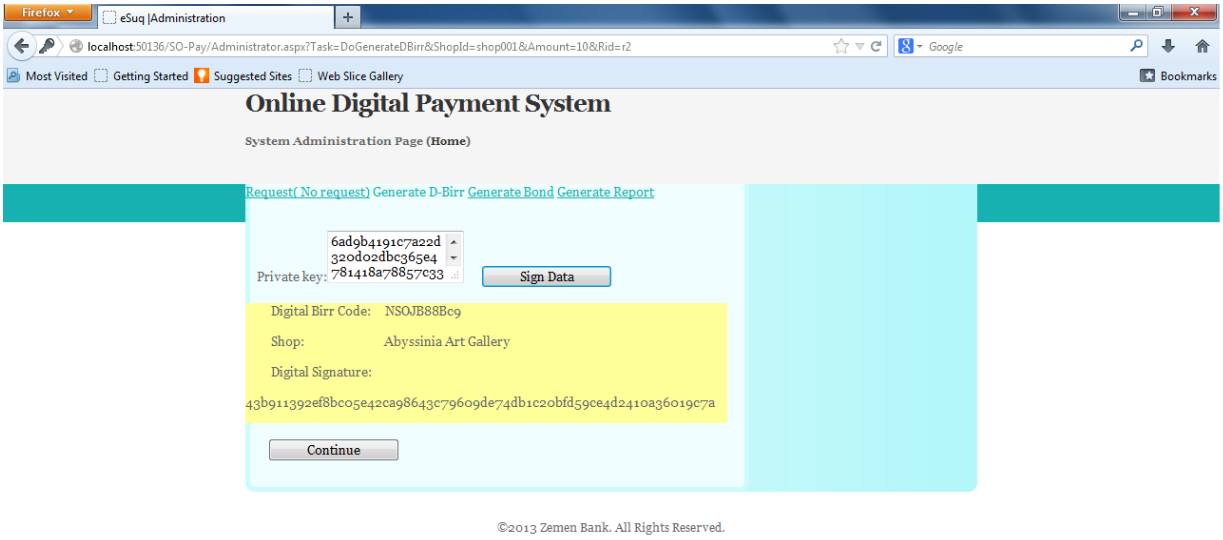

Figure 5-7: Digital Birr generation page

Then, as it is shown in Figure 5-8, the shop owner can sell the Digital Birr to any normal user of the system, who later uses the code to buy items as shown in Figure 5-9.

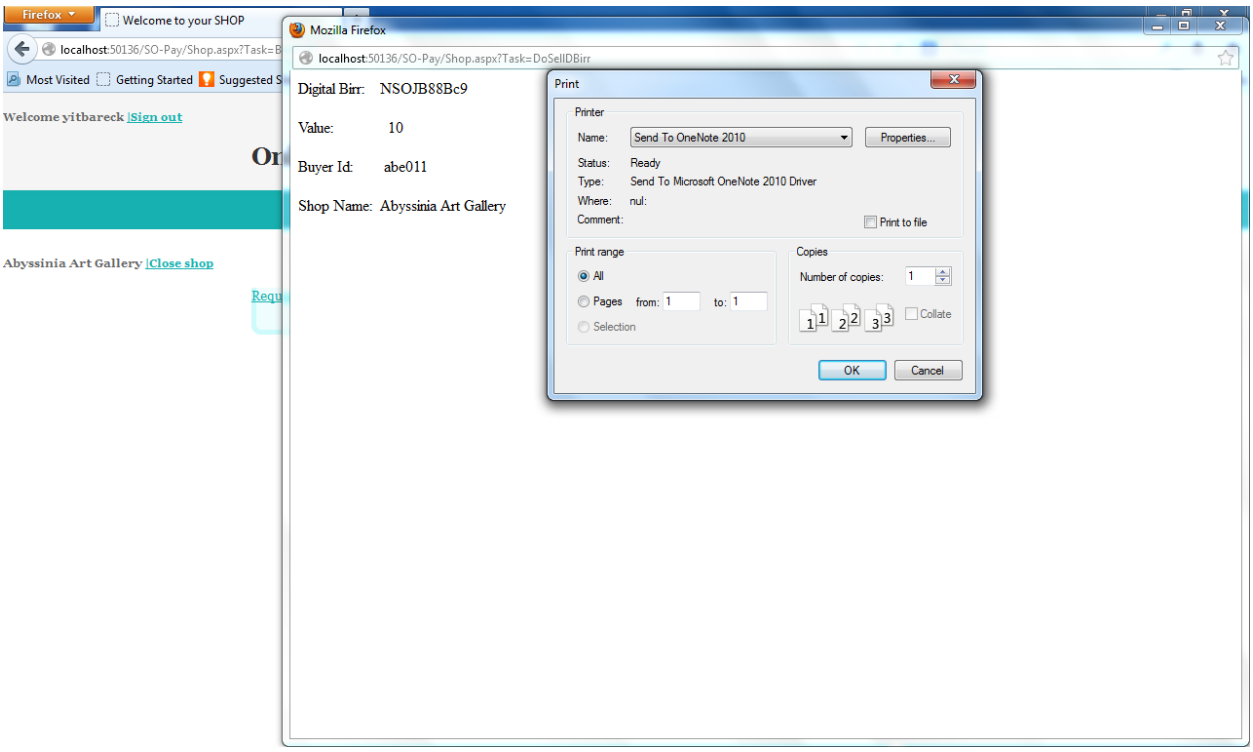

Figure 5-8: Digital Birr selling page

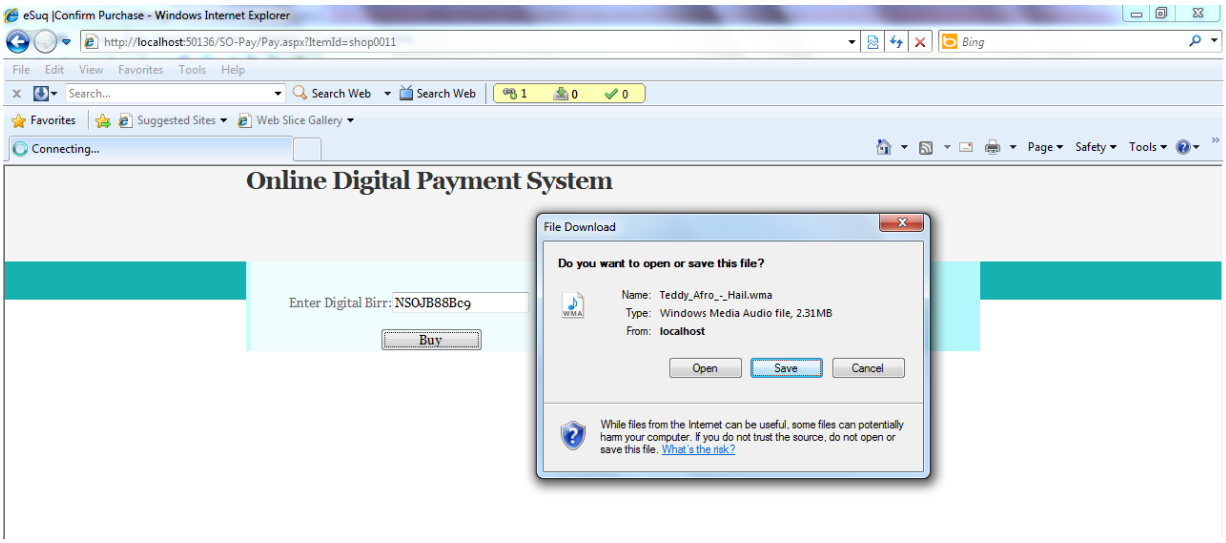

Figure 5-9: Payment page

CHAPTER SIX

EVALUATION

6.1 Overview

Evaluation of the Online Digital Payment System was performed based on the ISO 9241-11 usability testing attributes, such as efficiency (refers to how fast users can accomplish a task while using an application), effectiveness (refers to completeness and accuracy with which users achieve certain goals**)** and user satisfaction.

6.2 Evaluation

In the prototype evaluation, 5 different banks were involved. We have used random sampling technique to select representative number of participants. The participants were chosen considering their knowledge of the basics of computer. 5 employees (one from each bank supposed to be IT professionals) and 20 different customers (4 from each bank with basic computer knowledge) have participated. Before conducting the evaluation process, detailed description about the prototype has been given to the participants as it helps them in having an insight to the system. Two different questionnaires have been prepared (see APPENDIX B and C), one to be filled in by bank employees and the other to be filled in by bank customers. This is helpful in identifying the experience of the users in online payment systems as an employee of a bank and as a customer of a bank. The participants then got engaged on the demonstration of the system acting as customer, shop owner and system administrator depending on their respective user privileges. After the demonstration of the prototype, participants were provided with respective questionnaires. A five level likert scale (strongly agree (5), agree (4), neutral (3), disagree (2) and strictly disagree (1)) is used for the responses of the questions.

Table 6.1 summarizes the responses of bank's employees (One employee from each bank) and Table 6.2 summarizes the responses of bank's customers (Five customers from each bank).

Table 6-1: Detailed summary of questionnaire result (bank employees)

Question No.	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree	Mean Value
1	3	1	1	0	0	4.4
2	4	0	1	0	0	4.6
3	3	1	0	1	0	4.2
4	4	1	0	0	0	4.8
5	2	1	1	1	0	3.8
6	3	0	1	1	0	4
7	5	0	0	0	0	5
8	4	1	0	0	0	4.8
9	2	1	0	2	0	3.6
10	5	0	0	0	0	5
11	4	1	0	0	0	4.8
12	3	1	1	0	0	4.4
13	2	0	1	2	0	3.4
Number of participants with online payment experience						0

Number of participants familiar with credit cards	4
Number of participants whose company allows use of credit cards for online payment	1
Overall usability (%)	87.38

The result of Table 6.1 clearly shows that the participants are not familiar with payment using credit cards. The banks they are working in do not allow use of credit cards for online payment. 100% of respondents agreed that the system is a low-cost system compared to credit card based systems.

Table 6-2: Detailed summary of questionnaire result (Bank customers)

Question No.	Strongly agree	Agree	Neutral	Disagree	Strongly disagree	Mean value
1	10	3	3	4	0	3.95
2	10	4	6	0	0	4.2
3	11	1	3	5	0	3.9
4	12	3	5	0	0	4.1
5	8	2	3	7	0	3.55
6	10	3	3	4	0	3.95
7	18	1	1	0	0	4.85
8	10	6	0	4	0	4.1
9	10	3	7	0	0	4.15
10	10	5	0	5	0	4

11	14	6	0	0	0	4.7
12	12	3	5	0	0	4.35
13	4	2	5	9	0	3.05
Number of participants with online payment experience						0
Number of participants familiar with credit cards						0
Number of participants who have used credit cards for online payment						0
Overall system usability (%)	81.3					

According to Table 6.2 all of the respondents:

- have never used credit cards for online payment
- have no online payment experience
- are not even familiar with credit cards

The result of the evaluation has shown that the Online Digital Payment System is easy to use, secure, and can save time resource and cost imposed by traditional paper based payment systems.

CHAPTER SEVEN

CONCLUSION AND FUTURE WORK

7.1 Conclusion

Nowadays, due to the availability of the Internet, everything is becoming online. Mail systems (Postal services), cinemas, shops, and so on, can be accessed from anywhere through computers and mobile devices using web pages. Particularly, payment for goods can easily be carried out online through the Internet. This has brought an opportunity to design and implement a web based payment systems. In Ethiopia, there is no a low-cost and convenient way of buying and selling goods online.

Thus, this project work, an online payment without the use of credit cards is designed and implemented. Instead Digital Birr, a payment code, is used as a means of paying for goods. In order to design the architecture of the system, the functional and non-functional requirements are identified and analyzed using the use case diagram, sequence diagram and class diagram, which can show the static and dynamic behaviors of the system developed, Online Digital Payment System.

The system contains four major components: security manager, user manager, shop manager and administration manager. When the user registers or logs on to the system, the security manager component will take care of issues related to hashing private data, authentication and authorization. Based on the authorization status the user will be redirected to authorized pages. A user with administration capability will be redirected to administration manager component. Here, the user can manage issues like, approving different requests, generating Digital Birr and/or Digital Bond codes and generating reports. A default user will be redirected to user manager component. The redirected user can edit profile, buy items, buy Digital Birr, buy Digital Bond and send request to create shop. Up on successful approval of the request, the user manager component communicates the user to the shop manager component where issues like adding items, requesting Digital Birr and/or Digital Bond, selling Digital Birr and selling Digital Bond are managed. All components run on the business logic layer of the system except security manager which runs on the presentation layer.

For implementation purpose XHTML is used to present the contents on the client web browser. The dynamic parts are implemented using JavaScript, for client-side scripting and ASP.NET (C-Sharp), for server-side scripting.

The Online Digital Payment System prototype is evaluated through a questionnaire about the prototype which is prepared by considering the ISO 9241-11 usability test standard attributes. In the prototype evaluation, 5 different banks were involved. 5 employees (one from each bank) and 20 different customers (4 from each bank) have participated using random sampling. Generally, 25 different users were participated in the evaluation process. The respondents participated (by acting as real users) on the demonstration of the system using a personal computer. The results of the evaluation have shown that the Online Digital Payment System is easy to use and secure; it can save time and resources. It is also seen that the system is a low-budget system compared to other credit card based online payment systems.

7.2 Future Work

In this project work only non-tangible items such as music files, movie files, electronic books, Digital Bond and application software are considered as goods to sell and buy online using Digital Birr. Buying and selling tangible items, items such as clothes, car, mobile devices and even pizza from any restaurant, can possibly be integrated to the system so that the application area of the system can be widespread. Thus, as a future work, tangible items can be considered as good that can be bought online to boost the applicability area of the system.

It is known that the Online Digital Payment System is a web based system and that means there are many possible ways to access it. One way of accessing a web based system is a mobile phone. Nowadays, accessing web information and services at anytime from anywhere is becoming realistic using WAP enabled mobile devices. The content of information (can be described as size, format and so on) displayed on mobile phone browsers should not be the same as that of desktop browsers. The Online Digital Payment System prototype is designed and implemented considering desktop browsers which is a limitation as the content of the pages are not as clear as those in desktop browsers. Thus, as a future work, interface abstraction for different user platforms can be considered as a means to enhance user satisfaction.

References

[1] Organisation for Economic Co-operation and Development, Online Payment Systems For E-Commerce, April 18, 2006

[2] Bond (finance), Available on http://en.wikipedia.org/wiki/Bond_(finance), Accessed on February 27, 2012.

[3] Mandana Jahanian Farsi, Master's Thesis, Digital Cash, Department of Mathematics and Computing Science, Göteborg University,1997

[4] Jithendara Dara, Llexman Gundemoni, Master's Thesis, Credit Card Cecurity and e-Payment, Department of Business Administration and Social Sciences, Division of Information Systems Sciences, Lulea University of Thechnology,2006

[5] Behzad Pouralinazar, Master's Thesis in Information and Communication System Security, The System for Secure Mobile Payment Transactions, KTH Royal Institute of Technology, Sweden, 2013

[6] Ajeet Singh, Karan Singh, Shahazad, M.H Khan, Manik Chandra, A Review: Secure Payment System for Electronic Transaction, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 3, March 2012

[7] Supakorn Kungpisdan, Master's Thesis, Modeling, Design and Analysis of Secure Mobile Payment Systems, Faculty of Information Technology, Monash University, 2005

[8] Online and electronic payment solutions, Available on http://www.electronic-payments.co.uk/benefits_index.jsp, Accessed on February 27, 2013

[9] Mahil Carr, Mobile Payment Systems and Services: An Introduction, 2007

[10] Stan Sienkiewicz, Credit Cards and Payment Efficiency, Federal Reserve Bank of Philadelphia Payment Cards Center Discussion Paper No. 01-02, 2001

[11] Credit card costs, available at https://en.wikipedia.org/wiki/Credit_card#Costs, last accessed on February 27, 2013

[12] Credit cards, available at https://en.wikipedia.org/wiki/Credit_card#Costs, last accessed on February 27, 2013

[13] Etienne Gerts, Master's Thesis, Towards an Improved EMV Credit Card Certification, 2007

[14] Yang Jing, On-line Payment and Security of E-commerce, School of KeXin, Hebei University of Engineering, Handan, China, in Proceedings of the 2009 International Symposium on Web Information Systems and Applications (WISA'09), 2009

[15] Zoran Đurić, Ognjen Marić, Dragan Gašević, Internet Payment System: A New Payment System for Internet transactions, Journal of Universal Computer Science, vol. 13, no. 4 (2007), 479-503

[16] Jan L. Camenisch, Jean-Marc Piveteau, Markus A. Stadler, Security in Electronic Payment Systems, Institute for Theoretical Computer Science, ETH Zurich, CH-8092 Zurich, UBILAB, Union Bank of Switzerland, Bahnhofstrasse 45, CH-8021 Zurich,

[17] Master card, Credit Card basic for first time users, 2009

[18] Buy Now, Pay Later: a history of the Credit Card, available at, http://www.randomhistory.com/1-50/008credit.html, last accessed on February 27,2013

[19] Cryptography, available at, http://en.wikipedia.org/wiki/Cryptography, last accesed on February 27, 2013

[20] Anoop MS, Public key cryptography: Applications Algorithms and Mathematical Explanations, Tata Elxsi Ltd, 2007,

[21] CGI Group Inc., Public Key Encryption and Digital Signature: How do they work?, 2004

[22] Federal Information Processing Standards Publications (FIPS PUBS) , SECURE HASH STANDARD, 2002

[23] R.L. Rivest, A. Shamir, and L. Adleman, A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, National Science Foundation grant MCS76-14294, 2004

[24] Glenn Durfee , CRYPTANALYSIS OF RSA USING ALGEBRAIC AND LATTICE METHODS, June 2002

[25] Tomi Dahlberg , Niina Mallat , Jan Ondrus b, Agnieszka Zmijewska c Past, present and future of mobile payments research: A literature review, Electronic Commerce Research and Applications (2007),

[26] EBay, Available on http://en.wikipedia.org/wiki/EBay, Accessed on April 18, 2013.

[27] Amazon.com, Available on http://en.wikipedia.org/wiki/Amazon.com, Accessed on April 18, 2013.

[28] An Information Systems Security Risk Assessment Model under Dempster-Shafer Theory of Belief Functions, Lili Sun Rutgers, The State University of New Jersey Rajendra P. Srivastava The University of Kansas and Theodore J. Mock University of Southern California, Journal of Management Information Systems, Vol. 22, No. 4, Spring 2006: 109-142.

[29] What is new in Visual studio 2008, product guide, available at download.microsoft.com/.../3/B/D/.../VS2008ProductGuideEMEA.doc, Accessed on May 21, 2013

[30] XHTML, Available at http://en.wikipedia.org/wiki/XHTML, Accessed on May 21, 2013

[31] ASP.NET, Available at http://www.w3schools.com/aspnet/, Accessed on May 21, 2013

[32] Internet Information Services, Available at, http://en.wikipedia.org/wiki/Internet_Information_Services, Accessed on May 21, 2013

[33] RSA JavaScript API, Available at, http://kjur.github.io/jsrsasign/api/symbols/RSAKey.html, Accessed on May 21, 2013

[34] Quynh Dang, Recommendation for Applications Using Approved Hash Algorithms, NIST Special Publication 800-107, August 2012

[35] Electronic Payment System, Available at, http://www.docslide.com/electronic-payment-systems-1/, Accessed on May 21, 2013

APPENDIX A: Sequence Diagrams

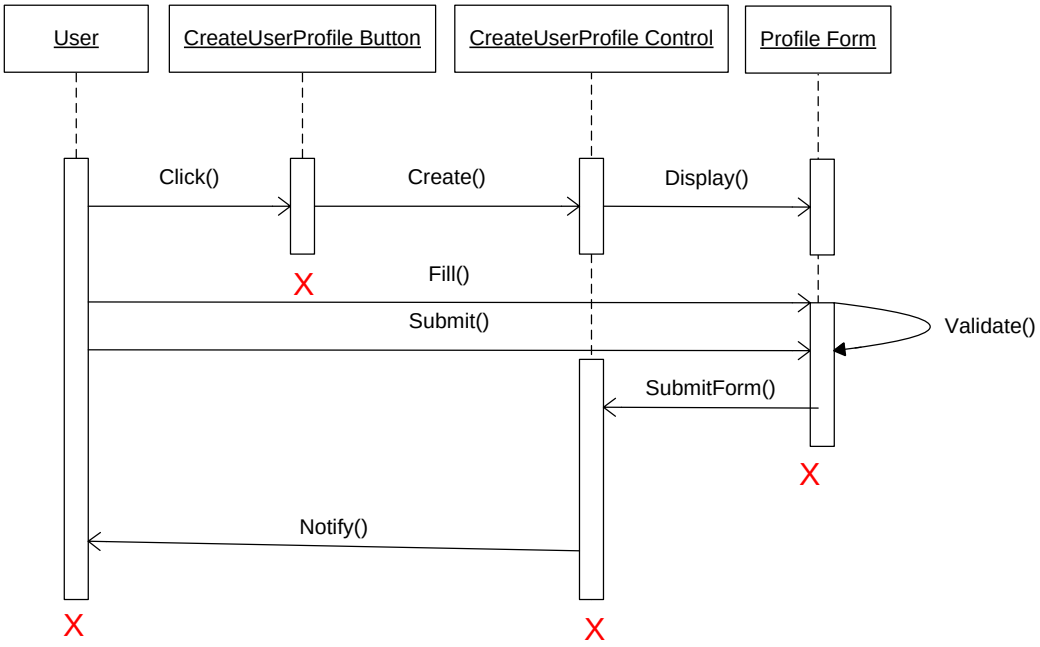

Figure 3-1: Sequence diagram for CreateUserProfile use case

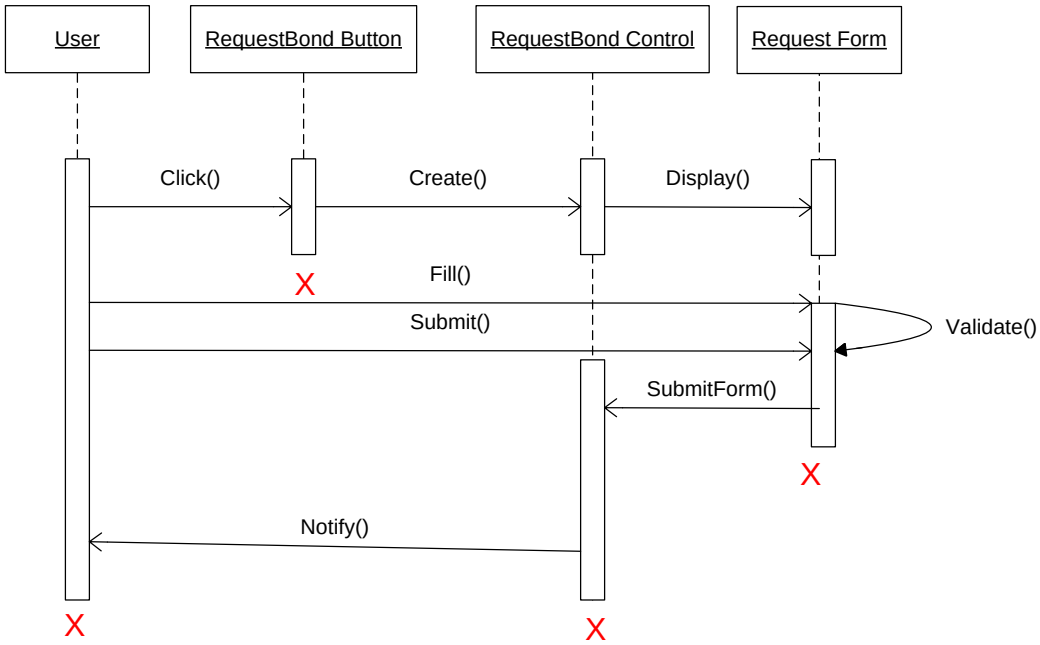

Figure 3-2: Sequence diagram for RequestBond use case

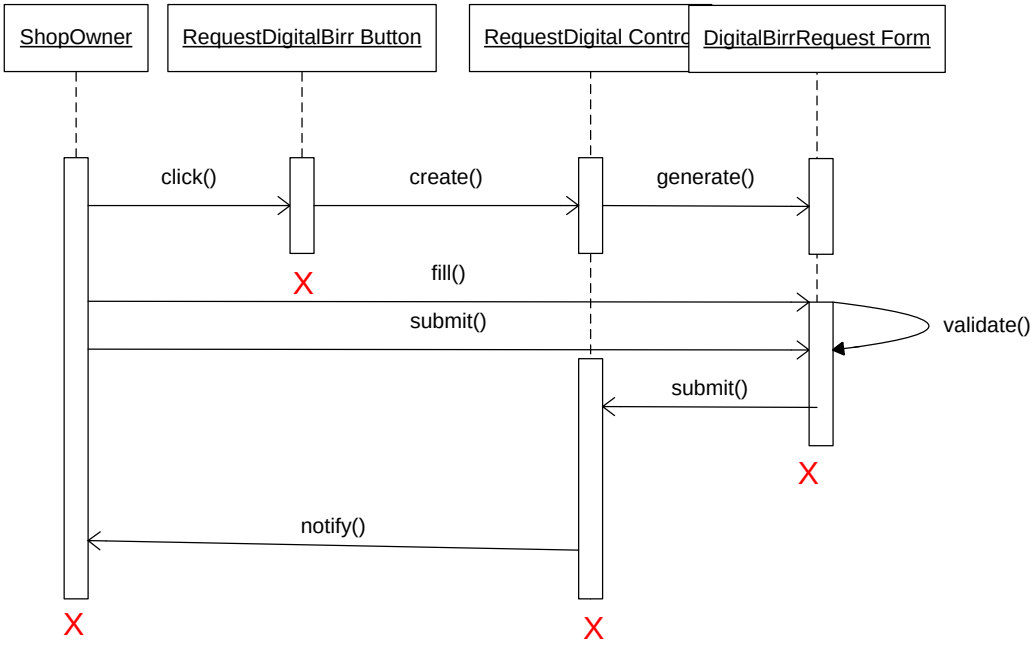

Figure 3-3: Sequence diagram for RequestDigitalBirr use case

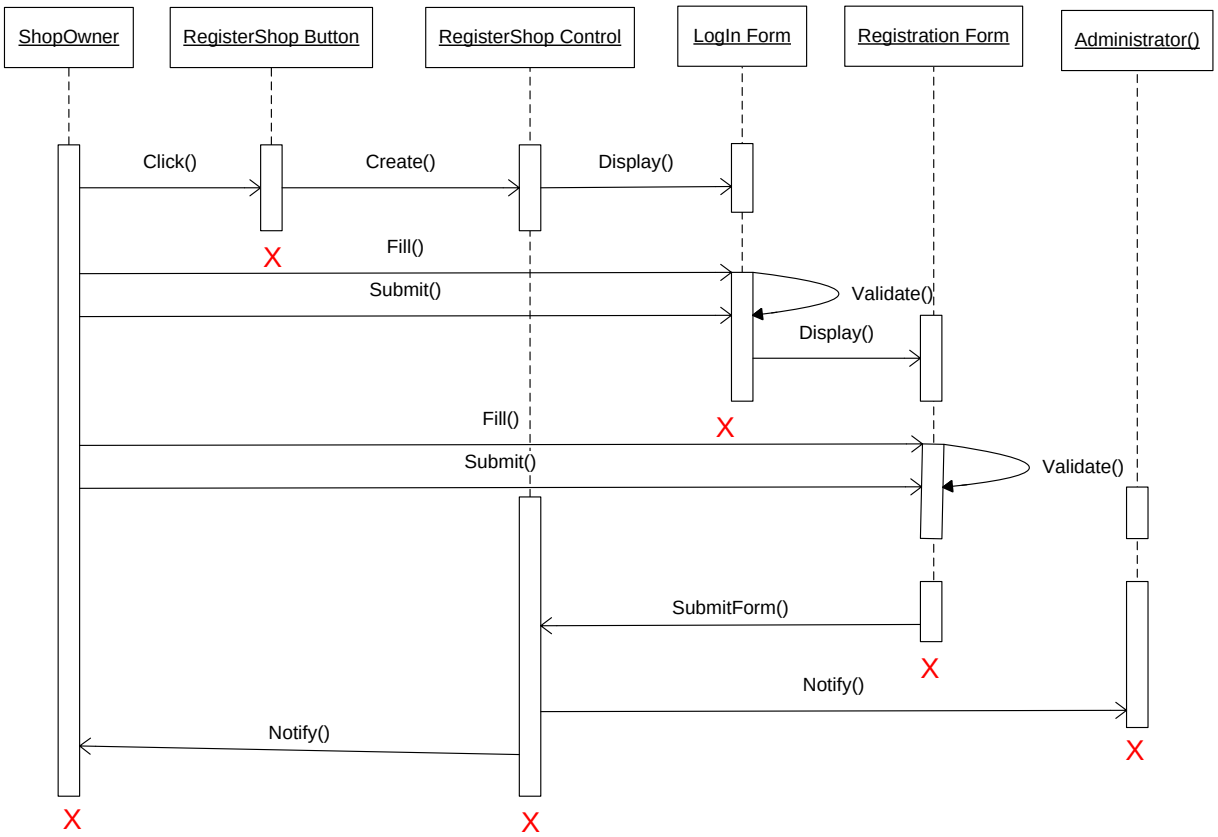

Figure 3-4: Sequence diagram for RegisterShop use case

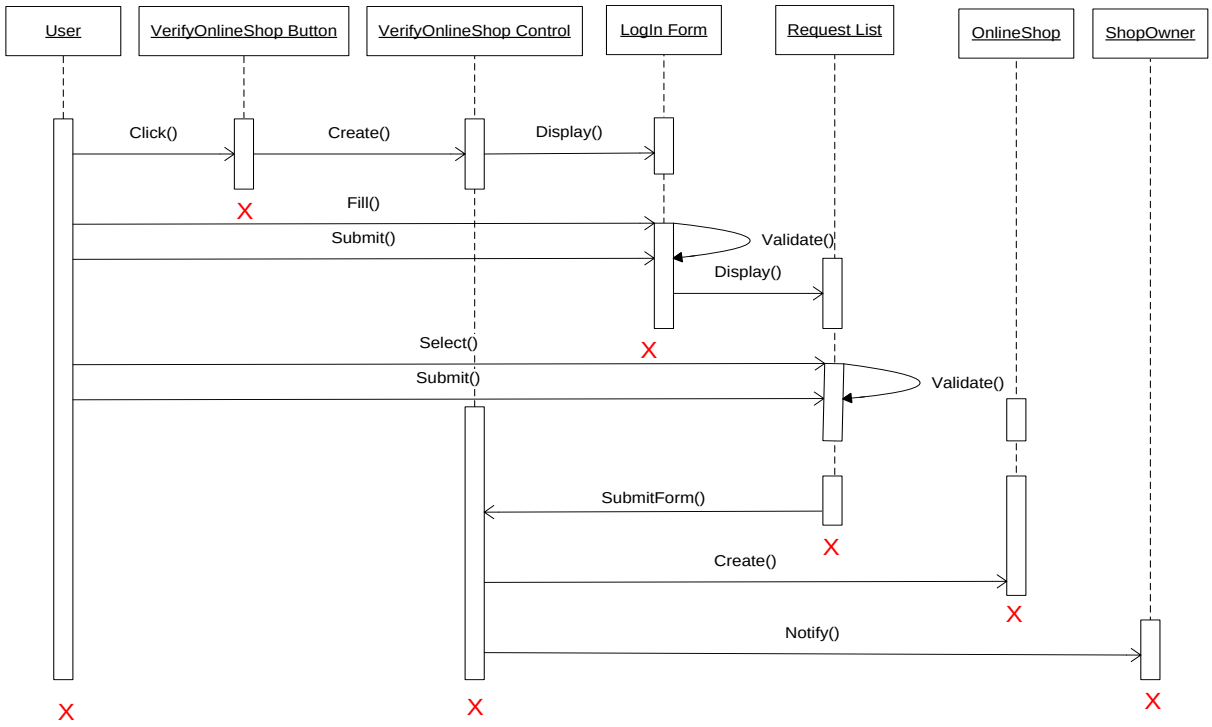

Figure 3-5: Sequence diagram for VerifyOnlineShop use case

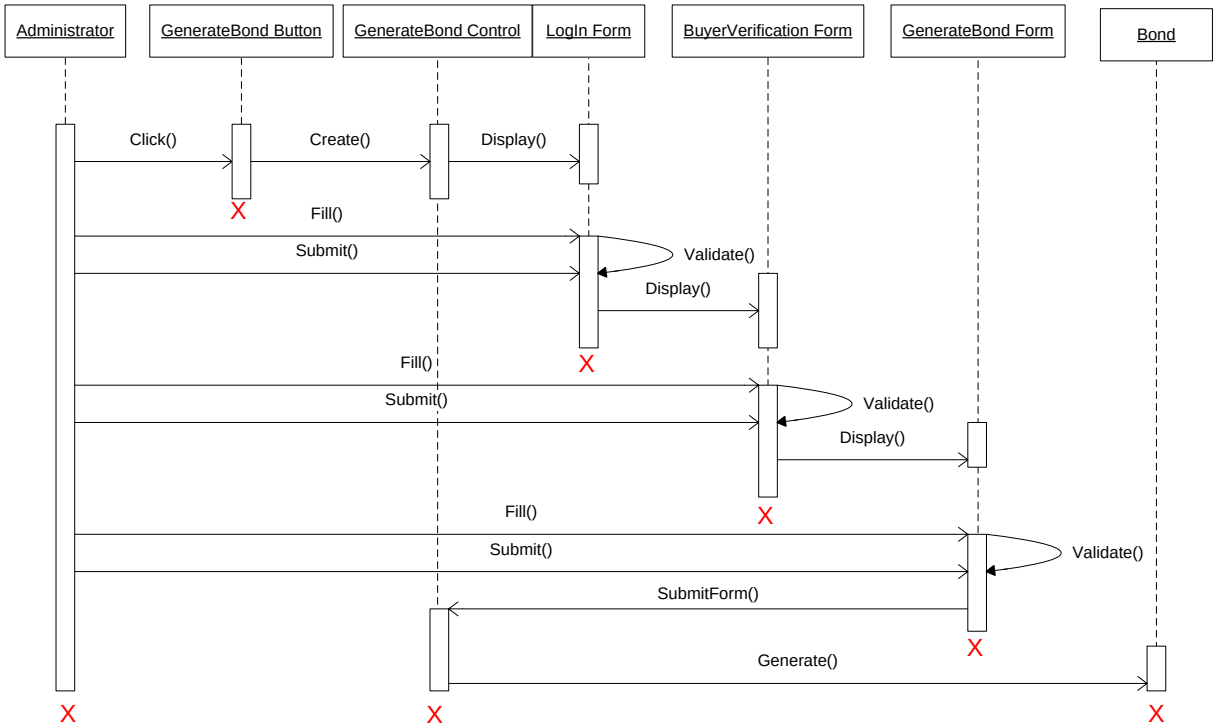

Figure 3-6: Sequence diagram for GenerateBond use case

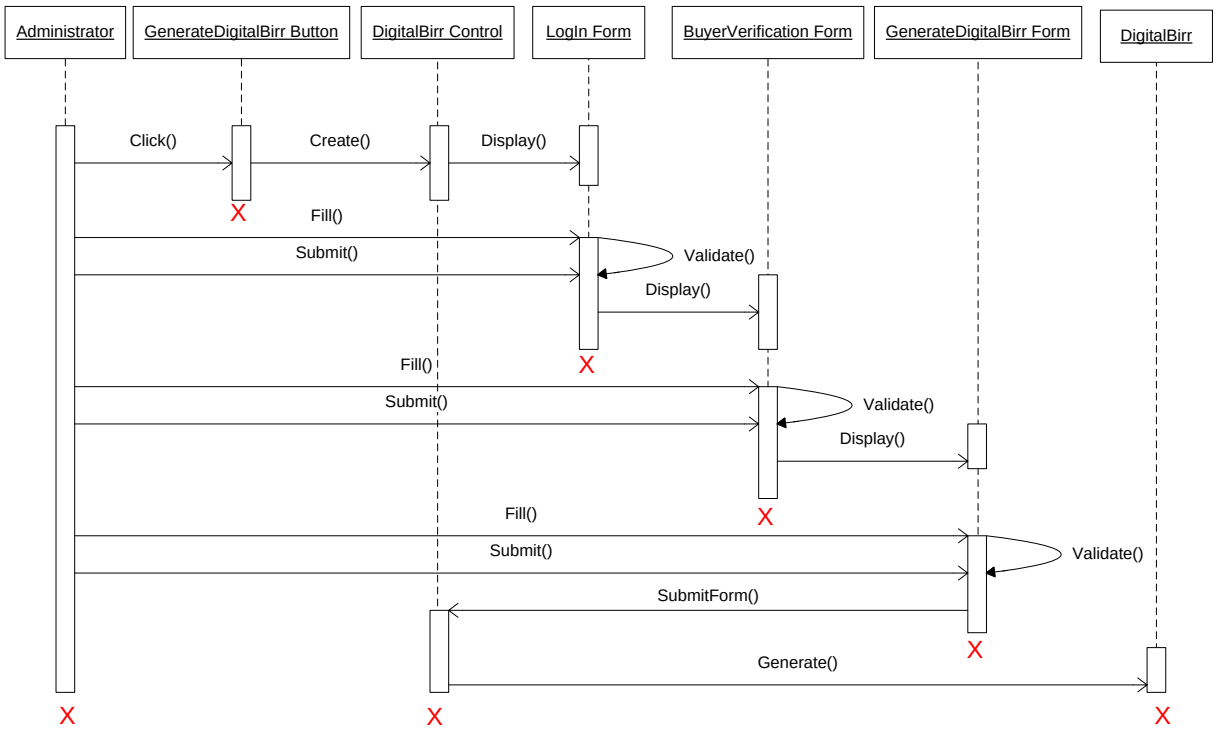

Figure 3-7: Sequence diagram for GenerateDigital Birr use case

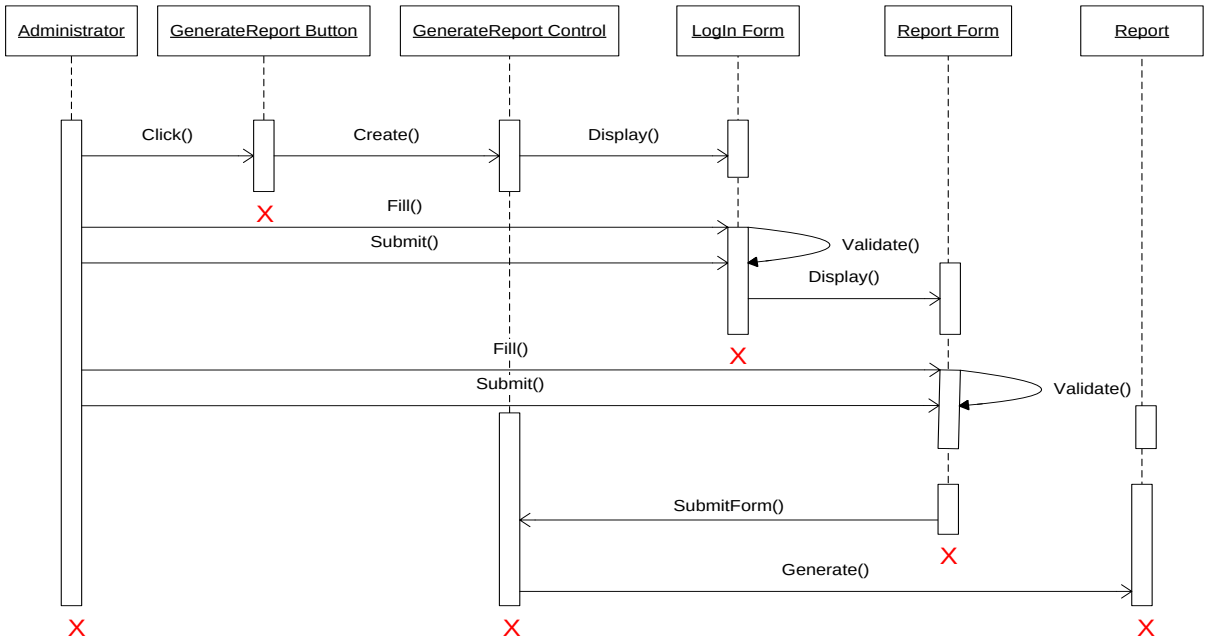

Figure 3-8: Sequence diagram for GenerateReport use case

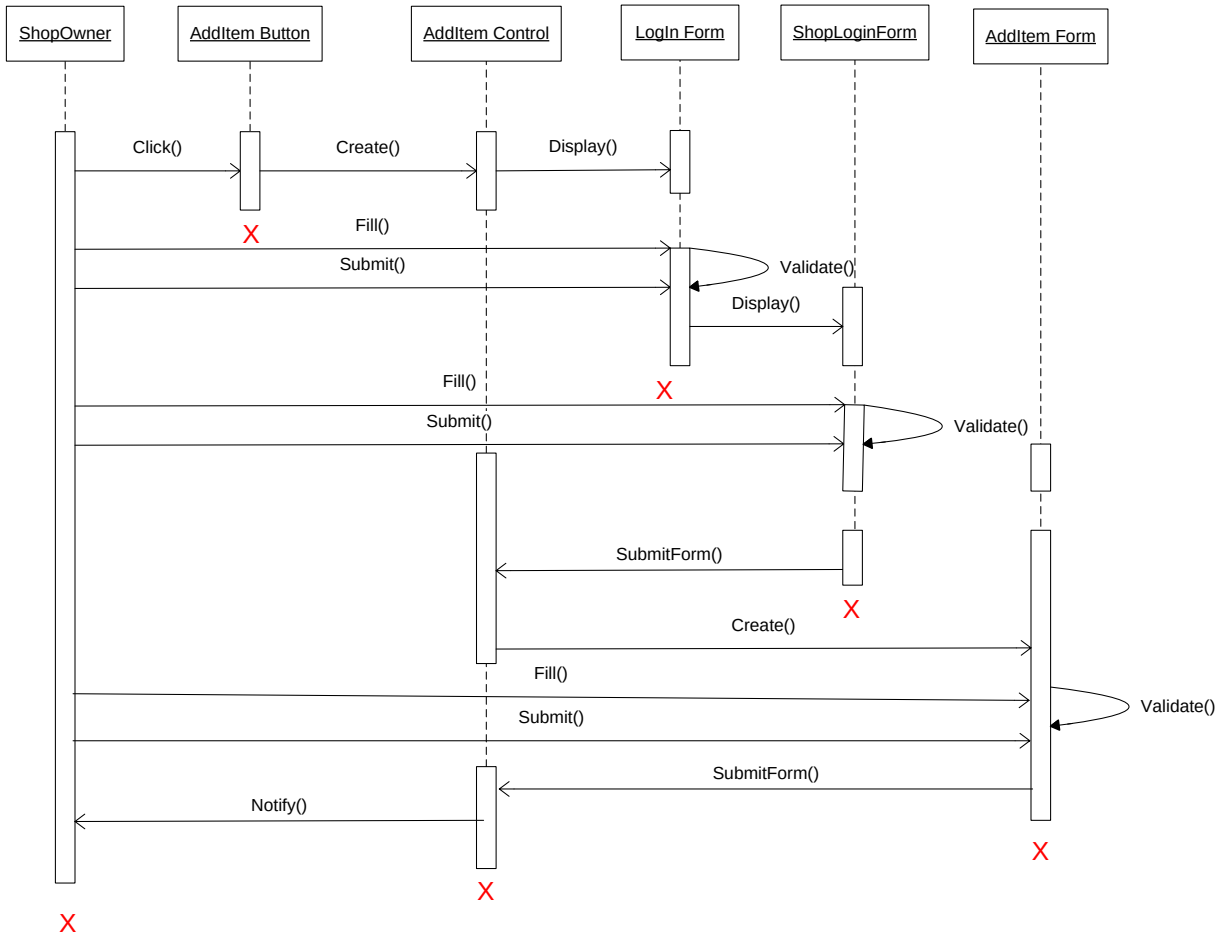

Figure 3-9: Sequence diagram for AddItem use case

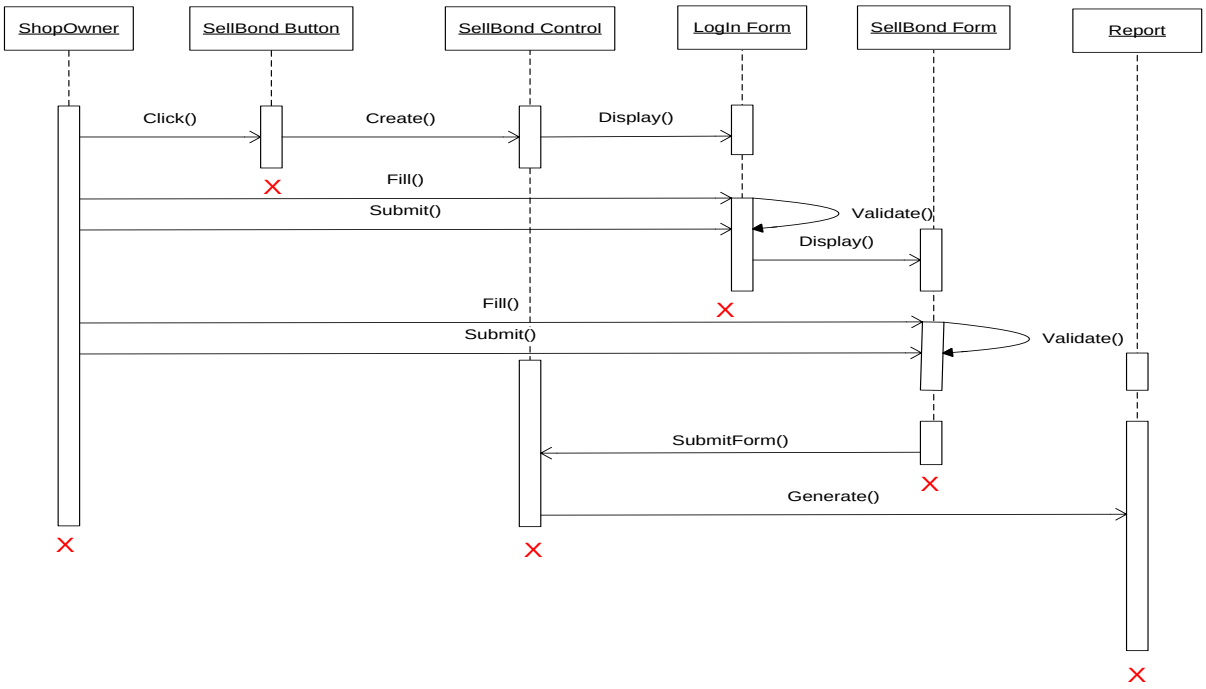

Figure 3-10: Sequence diagram for SellBond use case

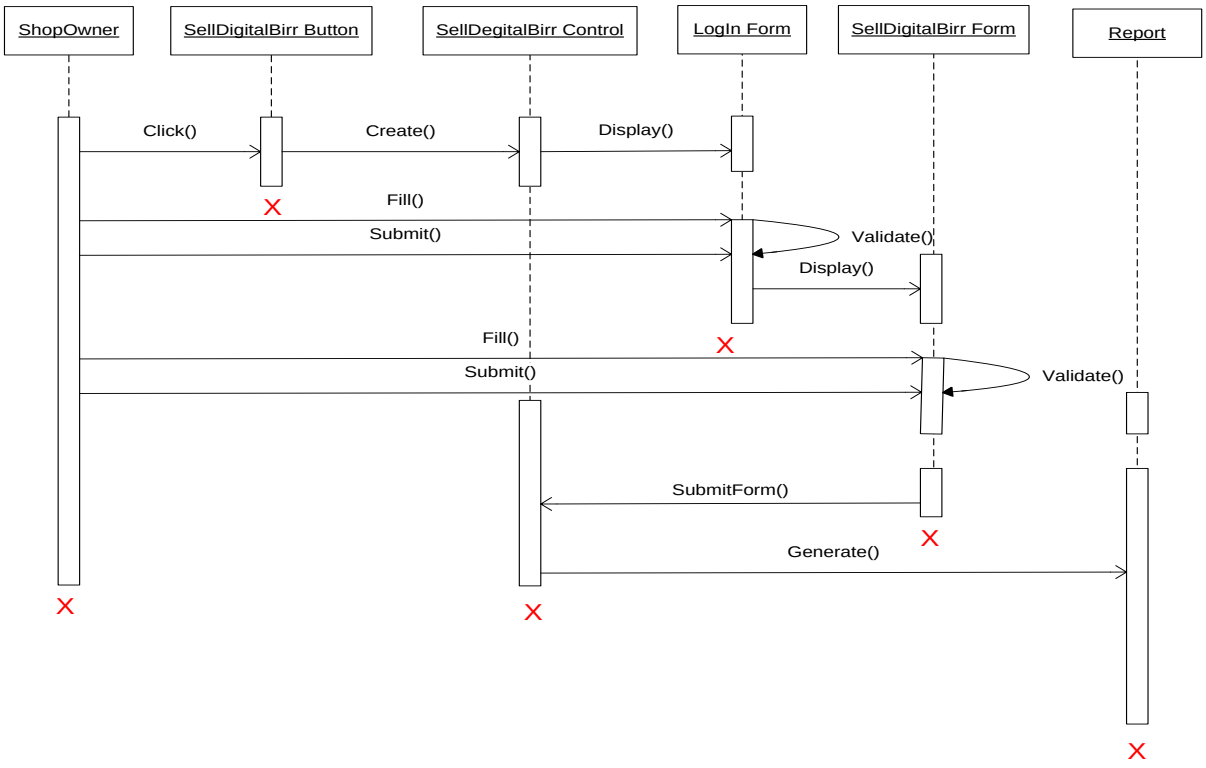

Figure 3-11: Sequence diagram for SellDigitalBirr use case

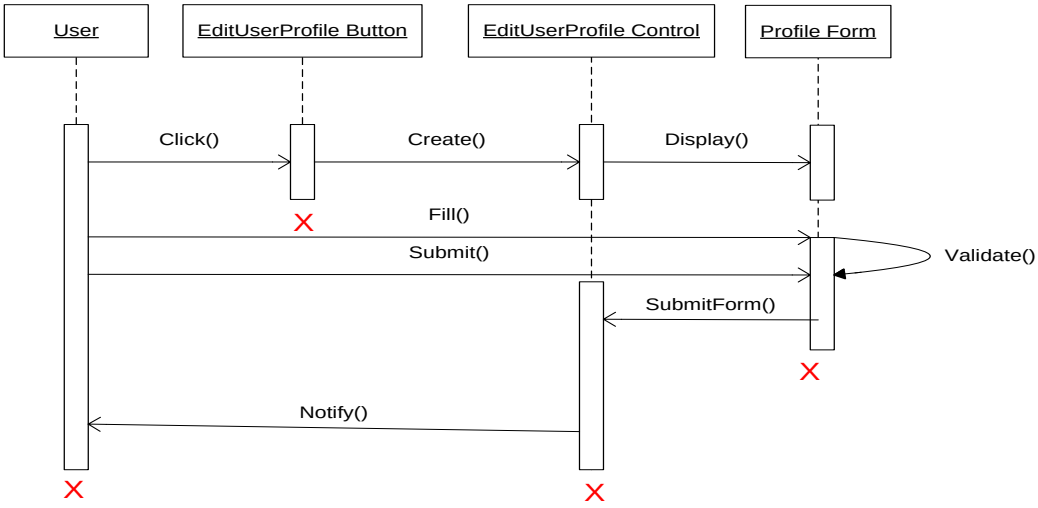

Figure 3-12: Sequence diagram for EditUserProfile use case

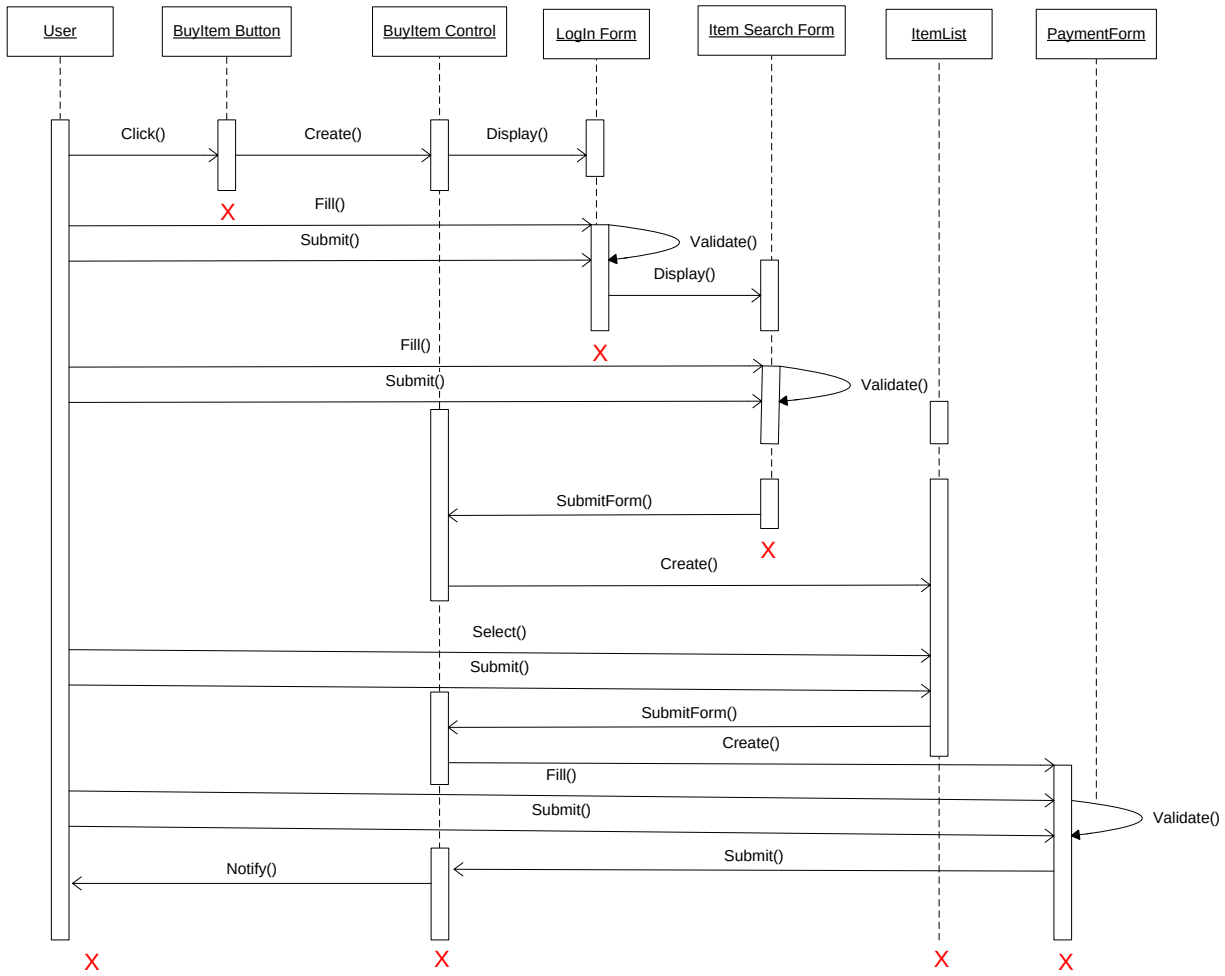

Figure 3-13: Sequence diagram for BuyItem use case

APPENDIX B

ONLINE DIGITAL PAYMENT SYSTEM

Usability Testing Questionnaire (User1- Bank)

This questionnaire is intended to know user satisfaction related to the service provided.

I Background Information about the company and the user

1. Name of the company _____
2. Your position _____
3. Do you have online payment experience? ☐ Yes ☐ No
4. Are you familiar with credit cards? ☐ Yes ☐ No
5. Does your company allow use of credit cards for online payment? ☐Yes ☐ No
6. If your answer for question number 5 is Yes, please describe how much successful it is_____
7. If your answer for question number 5 is No, please describe possible reasons _____

II Prototype

The following items are related to the main functionalities of the Online Digital Payment System. Please indicate your agreement by making "✓" in the boxes.

No.	Question	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
1	Do you think the terminology used in the prototype is consistent?					
2	Are you satisfied with the user interface of the system?					
3	Do you think the Online Digital Payment System prototype can be used easily?					
4	Do you think the system is good enough to buy and/or sell goods online?					

5	Do you think the system is secure enough (in terms of privacy, data integrity)?					
6	Do you think the response time for most operations is fast enough?					
7	Do you think the cost of using Digital Birr and/or Digital Bond is lower than that of the cost of using credit cards?					
8	Does the system give enough description when an error occurs?					
9	Do you think the system can be used by any user with basic knowledge of using computers?					
10	Do you think the text which appears on the pages is clearly readable throughout operating on the system?					
11	Do you think the interaction to accomplish tasks is simple and complete with a few commands?					
12	Do you think the menu items (or navigation buttons and links) are consistently located and work without failure?					
13	Are Digital Birr and Bond codes easy to use (easy to read and write)?					

Please write any other comment about the Online Digital Payment System:

_____

_____

_____

_____

APPENDIX C

ONLINE DIGITAL PAYMENT SYSTEM

Usability Testing Questionnaire (User2- Customer)

This questionnaire is intended to know user satisfaction related to the service provided.

I Background Information about the company and the user

1. Do you have online payment experience? ☐ Yes ☐ No
2. Are you familiar with credit cards? ☐ Yes ☐ No
3. Have you ever used credit cards for online payment? ☐ Yes ☐ No

II Prototype

The following items are related to the main functionalities of Online Digital Payment System. Please indicate your agreement by making "✓" in the boxes.

No.	Question	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
1	Do you think the terminology used in the prototype is consistent?					
2	Are you satisfied with the user interface of the system?					
3	Do you think the Online Digital Payment System prototype can be used easily?					
4	Do you think the system is good enough to buy and/or sell goods online?					
5	Do you think the system is secure enough in keeping your privacy?					
6	Do you think the response time for most operations is fast enough?					
7	Do you think the cost of using the system is lower than that of the cost of using credit cards?					
8	Does the system give enough description when an error occurs?					

9	Do you think the system can be used by any user with basic knowledge of using computers?					
10	Do you think the text which appears on the pages is clearly readable throughout operating on the system?					
11	Do you think the interaction to accomplish tasks is simple and complete with a few commands?					
12	Do you think the menu items (or navigation buttons and links) consistently be located and work without failure?					
13	Are Digital Birr and Bond codes easy to use (easy to read and write)?					
14	Do you think the system can bring job (work) opportunity?					

Please write any other comment about the Online Digital Payment System:

_____

_____

_____

_____

Declaration

This thesis is my original work and has not been presented for a degree in any other university, and that all sources of material used for the project have been duly acknowledged.

Name: **Yitbarek Zewde**

Signature: _____

Date: _____

Advisor Confirmation:

Name: **Dida Midekso (PhD)**

Signature: _____

Date: _____

November, 2013

Addis Ababa, Ethiopia