

Implementing a Software Switch and a Mobile Application to Prevent Frauds and Control the Usage of Electronic Transactions

G T C Liyanage

149218J

Dissertation submitted to the Faculty of Information Technology, University of Moratuwa, Sri Lanka for the partial fulfillment of the requirements of the Degree of Master of Science in Information Technology

May 2017

Declaration

I confirm that this thesis is a presentation of my original research work for the degree of M.Sc. in Information Technology. Wherever contributions of others are involved, every effort is made to indicate this clearly, with due reference to the literature, and acknowledgement of collaborative research and discussions.

The work was done under the guidance of Mr. B. H. Sudantha, at the Faculty of Information Technology, University of Moratuwa, Sri Lanka.

G. T. C. Liyanage

Date:

...

In my capacity as supervisor of the candidate's thesis, I certify that the above statements are true to the best of my knowledge.

Mr. B. H. Sudantha

Date:

Acknowledgement

First of all I would like to express my sincere gratitude to Mr. B. H. Sudantha (Senior Lecturer at Faculty of IT, University of Moratuwa and Course Coordinator) for giving me the opportunity to work under him and to be the supervisor for this research project without second thoughts. His patience and guidance have helped me a lot towards the successful project selection, continuation and completion.

Further I would like to thank especially Prof. A. S. Karunanda (Dean of Kothalawala Defense University) for guiding towards how to do research and how to write thesis. Additionally I would like to thank Mr. S. Premarathne (Senior Lecturer) and all the lecturers who have helped throughout the course by giving unlimited support.

I would also like to thank my superior Mr. Kanishka Weeramunda of PayMedia for helping and guiding in selecting a suitable research area, Mr. Nuwan Wickramanayake and Dilan Ekanayake from InfoTech Department of Sampath Bank for their insights on this project.

Last, but not least I would like to thank my wife for enormous support and patience she have been holding throughout my work. And also I wish to thank my parents, brother and all the colleagues for encouraging me in all aspects of life apart from this.

G T C Liyanage

Dedicated

To Mr. B. H. Sudantha

&

To My Wife and Parents

&

To those who lost their valuable money
Because of they had no control over their plastic card

Table of Contents

Declaration	I
Acknowledgement.....	II
Dedication	III
Glossary of Terms	XII
Abstract	xiii
1 Introduction.....	1
1.1 Prolegomena	1
1.2 Background and Motivation	1
1.3 Types of Credit Card Frauds	3
1.3.1 Card Related Frauds	3
1.3.2 Merchant Related Frauds	5
1.3.3 Internet Related Frauds	5
1.4 Problem Statement	5
1.5 Hypothesis	6
1.6 Aims and Objectives	6
1.7 Software Switch and Mobile Application Based Approach.....	7
1.8 Structure of Thesis.....	7
1.9 Summary	7
2 Study on Electronic Transaction Frauds and Control of Transactions	8
2.1 Introduction	8
2.2 Related Work on Credit Card Fraud Detection	8
2.2.1 Bayesian Networks.....	9
2.2.2 Hidden Markov model	10
2.2.3 Genetic Algorithm.....	10

2.2.4	Decision Tree	10
2.2.5	Neural Networks	11
2.3	Related work on Credit Card Fraud Prevention and Control	11
2.3.1	Manual Review	11
2.3.2	Address Verification System.....	12
2.3.3	Card Verification Methods.....	12
2.3.4	Negative and Positive Lists.....	12
2.3.5	Payer Authentication.....	12
2.4	Problem Definition	13
2.5	Summary	13
3	Technology of Banking in Electronic Environment.....	14
3.1	Introduction	14
3.2	Standard Banking Systems	14
3.2.1	ISO8583 Protocol.....	14
3.3	APIs for Public Access.....	16
3.3.1	Usage of Identity servers and API managers	16
3.4	Personal Banking.....	17
3.4.1	Web Presence	17
3.4.2	Mobile Presence	17
3.5	Encryption Functions	17
3.6	Technologies used in Novel Solution.....	18
3.7	Summary	19
4	An Approach to Prevent Card Fraud and Misuse	20
4.1	Introduction	20
4.2	ePaySwitch	20
4.3	Inputs to the system.....	20
4.3.1	User Inputs	20

4.3.2	Input from Banking Officer	21
4.3.3	Core System Inputs	21
4.4	Outputs of the system	21
4.4.1	Output from ePaySwitch	21
4.4.2	Outputs from ePaySwitch Mobile Application	22
4.5	Processes	22
4.5.1	User Registration and Authentication	22
4.5.2	Card Registration	22
4.5.3	Card Control.....	23
4.5.4	Mobile Application to ePaySwitch Communication	23
4.5.5	Communication with ePaySwitch and the Core System.....	23
4.6	Users of system	23
4.6.1	Financial Institutes	23
4.6.2	End Users	23
4.7	Features of ePaySwitch	24
4.8	Summary	24
5	Design of ePaySwitch.....	25
5.1	Introduction	25
5.2	Architecture of ePaySwitch.....	25
5.2.1	Block Diagram	25
5.2.2	Server Architecture	26
5.2.3	Use Case Diagram.....	26
5.2.4	Activity Diagram.....	27
5.2.5	High Level Network Diagram.....	28
5.3	Hierarchy of ePaySwitch.....	29
5.3.1	Mobile application	29
5.3.2	APIs for Mobile Access	32

5.3.3	Payments Processor.....	32
5.3.4	Customers and Cards Manager	33
5.3.5	Data Storage of ePaySwitch.....	33
5.4	The Actual Transaction	34
5.5	Summary	36
6	Implementation of ePaySwitch.....	37
6.1	Introduction	37
6.2	Building Blocks of ePaySwitch.....	37
6.2.1	Mobile Application	37
6.2.2	APIs for Mobile Access	38
6.2.3	Payments Processor.....	39
6.2.4	Cards & Customers Manager	39
6.2.5	ePaySwitch Database	39
6.3	Implementation of ePaySwitch	40
6.3.1	User Registration.....	40
6.3.2	Sign In	42
6.3.3	Card Registration	42
6.3.4	Adding Rules and Card Controls (Update Card)	44
6.3.5	Payments Processor.....	48
6.3.6	Card Availability and Active/Inactive State	52
6.3.7	Card On/Off	54
6.3.8	Online Transactions	56
6.3.9	Offline Transactions.....	57
6.3.10	Withdrawals	59
6.4	Overall Implementation.....	60
6.5	Summary	61
7	ePaySwitch Testing & Evaluation	62

7.1	Introduction	62
7.2	Software Simulation	62
7.2.1	Simulation Test Cases	63
7.2.2	Simulation Test Output	64
7.3	Questionnaire.....	66
7.4	Results	67
7.4.1	Simulation	67
7.4.2	Software Simulation Conclusion	68
7.4.3	Questionnaire	68
7.4.4	Questionnaire Conclusion	70
7.5	Summary	70
8	Conclusion	71
8.1	Introduction	71
8.2	ePaySwitch Achievements	71
8.3	Problems and Limitations.....	71
8.4	Improvements and Further Work	71
8.5	Summary	72
	References.....	73
	Appendix A – ISO8583 Message Sample.....	76
	Appendix B – Important Code Segments.....	80
	Appendix C – User Interfaces	92
	Appendix D – Questionnaire and Responses	96

Table of Figures

Figure 1-1: U. S. Card Fraud by Type	2
Figure 1-2: ID Fraud Victims and their Loses	3
Figure 5-1: High Level Architecture	25
Figure 5-2: ePaySwitch Server Block Diagram	26
Figure 5-3: High Level Use Case Diagram	27
Figure 5-4: Activity Diagram	28
Figure 5-5: High Level Data Network Diagram	29
Figure 5-6: Wireframes of the Mobile Interface	30
Figure 5-7: Login Flow Chart	31
Figure 5-8: Customer and Card Registration Sequence Diagram	32
Figure 5-9: Payments Processor	33
Figure 5-10: High Level Database Diagram	34
Figure 5-11: Conventional Card Transaction (Offline)	35
Figure 5-12: Conventional Message Flow	35
Figure 5-13: ePaySwitch Intermediator	36
Figure 6-1: Database Table Implementations of ePaySwitch	40
Figure 6-2: User Registration Form	41
Figure 6-3: Customer Activation Portal	41
Figure 6-4: User Sign-In Form	42
Figure 6-5: card Registration Form	43
Figure 6-6: Inactive Cards List	44
Figure 6-7: Card Remove Form	44
Figure 6-8: Card On/Off and Adding Rules	45
Figure 6-9: Payment Processor Flow	49
Figure 6-10: Card Availability and Active/Inactive State	53
Figure 6-11: card On/Off Flow	54
Figure 6-12: Card Status Off	55
Figure 6-13: Card Status On	55
Figure 6-14: Online Transaction Rules Flow	56
Figure 6-15: Online Transactions Off	56
Figure 6-16: Online Transaction On and Rules Apply	57

Figure 6-17: Offline Transactions Flow58

Figure 6-18: Withdrawal Flow59

Figure 6-19: Overall Implementation.....60

Figure 7-1: People who need to try ePaySwitch68

Figure 7-2: People who commented on ePaySwitch.....69

Figure 7-3: People's reaction for transaction amounts69

List of Tables

Table 3-1: ISO8583 Common Response Codes.....	16
Table 3-2: MD5 and SHA Comparison	18
Table 6-1: Database Stored Procedures	40
Table 6-2: Card Availability and Active/Inactive State Response Codes.....	54
Table 6-3: Card On/Off Status	55
Table 6-4: Online Transactions Response Codes.....	57
Table 6-5: Offline Transactions Response Codes	58
Table 6-6: Withdrawals Response Codes	60
Table 7-1: Simulation Results.....	67

Glossary of Terms

API	Application Programming Interface
ASCII	American Standard Code for Information Interchange
ATM	Automated Teller Machine
CRUD	Create, Read, Update, Delete
DDC	DieBold® Direct Connect
DSS	Data Security Standard
FOS	Free and Open Source
GPL	General Public License
ISO	International Standards Organization
MD5	Message digests - 5
NDC	NCR® Direct Connect
PCI	Payment Cards Industry
POS	Point of Sales
SHA	Secure Hash Algorithm
SOAP	Simple Object Access Protocol
SQL	Structured Query Language
WCF	Windows Communication Foundation
XFS	eXtensions for Financial Services

Abstract

The growth of the electronic payment methods have rapidly increased in past decades. This has been resulted in growth in electronic transactions fraud. The main source of electronic transactions is card payments. People are reluctant to do card payments online because they think twice about the security. On the other hand if a person loses his card or identity of any electronic payment system, he/she has a higher chance of losing their money. ePaySwitch is less complicated but reliable method of preventing a card fraud which gives the control of the card to the user.

ePaySwitch gives the control of the card to the end customer through the mobile application. ePaySwitch server is installed on premises of the bank or financial institute. Server has two main sub modules as ‘Payments Processor’ and the ‘Customer and Cards Manager’ which implemented on two separate servers. These two modules are connected to the database which runs on a separate server. Combination above two modules with database and mobile application together, we call the ePaySwitch.

Customer can keep their cards turned on or off using the mobile application. They even can set whether can perform transactions Online, Offline or for Withdrawal. Additionally they have the facility to set maximum transaction values for each of the above transaction types. This feature enables the customers to protect their money even their cards have lost or stolen.

Mobile application communicates with the server via APIs bind to the mobile application. These APIs are written Java and hosted on an Apache Tomcat server. Payments Processor and the Customers and Cards Manager have written in PHP and hosted on an Apache web server. Database is a MySql GPL version for the current version of ePaySwitch.

Simulation shows how the system will work on real environment. Answers to the questionnaire we prepared shows that some customers’ biggest paint point is fear of losing their money because of cards. Some have showed that they have no idea on their spending when using the cards. But somehow they are willing to user a solution like ePaySwitch if they had a chance.

Finally it is shown that ePaySwitch is a practical solution for prevent frauds and control transactions in the electronic environment.