“Secured banking transaction using virtual Password”

A PROJECT REPORT

submitted by

Utkarsh Sharma -16BCE0226

in partial fulfillment for the award

of the

B. Tech.

degree in

Computer Science and Engineering

School of Computer Science and Engineering

School of Computer Science and Engineering

School of Computer Science and Engineering

DECLARATION

I hereby declare that the project entitled **"Secured Banking Transaction using virtual password"** submitted by us to the School of Computer Science and Engineering, VIT University, Vellore in partial fulfillment of the requirements for the award of the degree of **Bachelor of Technology in Computer Science and Engineering** is a record of bonafide work carried out by us under the supervision of **Prof. Ramanathan L, Assistant Professor (Selection Grade)**. I further declare that the work reported in this project has not been submitted and will not be submitted, either in part or in full, for the award of any other degree or diploma of this institute or of any other institute or university.

Utkarsh Sharma -16BCE0226

School of Computer Science and Engineering

CERTIFICATE

The project report entitled "**Secured Banking Transaction using virtual Pasword**" is prepared and submitted by **Utkarsh Sharma (Register No: 16BCE0226).**

It has been found satisfactory in terms of scope, quality and presentation as partial fulfillment of the requirements for the award of the degree of **Bachelor of Technology in Computer Science and Engineering** in VIT University, India.

Internal Examiner

Prof. Ramanathan L

ACKNOWLEDGEMENT

I would like to express my gratitude to all those who have helped me in the successful completion of this project. Without their support, I would not have been able to achieve the goal of the project successfully.

I would like to take this opportunity to thank our guide, Prof. Ramanathan L, for his constant support, guidance and mentorship without whom it would have been really difficult to complete the project on time.

Furthermore, I would also like to acknowledge with much appreciation, the important role of Dr. R Senthil Kumar, Head of the Department, Department of Software Systems, SCOPE, whose contribution in encouragement helped me plan better.

I would like to thank our Dean, Dr. Arunkumar T., who provided me with the facilities required and conducive conditions for the project.

Finally, I would like to express my sincere gratitude to VIT University, which provided me with a platform to hone my skills.

ABSTRACT

One time password (OTP) is the authentication method used in online banking system today. Hackers are getting better each day at cracking sensitive information. Once this happened, they can gain access to our private network and steal our sensitive business information. A common technology used for the delivery of OTPs is text messaging.OTP over SMS might not be encrypted by any service provider. In addition, the cell phones which are used to receive the SMS also play an important role, in which more than one phone comes into account. The vulnerable parts of the cell phone network can be mount to man-in-the-middle attack. To overcome the difficulties the virtual password concept is introduced. The virtual pssword concept involves a small amount of human computing to secure user's passwords in online environments. To provide high security, we enhance the existing system with virtualization concept. Hacker may guess our password but he cannot access our account because he cannot access virtual password. The major hacking threats like phishing, key-logger, shoulder-surfing attacks, and multiple attacks cannot affect our schema. In user-specified functions, we adopted secret little functions in which security is enhanced. Virtual password is a password that is valid for only one login session or transaction and after that it becomes obsolete. The calculation of the virtual password is done at the client side which reduces the delay of time in receiving OTP via SMS. To make the client more convenient in calculating the virtual password an application is used which reduces the work of the client. This method is more instant than the traditional OTP system used today.

CONTENTS

INTRODUCTION

Today, The Internet has indulged into day -to-day activities of common man which expects the security system and authentication system to be of greater strength. Besides normal browsing we are more involved in sensitive transaction such as online payment, online booking, online banking, etc., more and more services have been moved online. One of the main sectors that are gaining more and more attention and importance is banking system, where once the sensitive information of an individual is stolen, the consequences are very dangerous. Hence the Research and Development (R&D) department is working hard to make the banking process more secured. The OTP received via email is unsecured because of end-to-end security provided by the mobile network. There may be fluctuation or delay in time due to network facility available; using multiple mobiles for receiving OTP makes the password unsecured. In Virtual Password schema, the calculation of the OTP is done by client side using an application in the mobile; it becomes independent of mobile network which increases the performance of the system . The user is provided with permanent PIN number and a random number on the login page, which makes the hacking difficult. Even if the hacker hacks the account information of an individual, the intruder cannot access our mobile application, since it uses random number generation concept. The developer cannot guess the random number that is generated for the particular transaction at a time.

LITERATURE SURVEY

AUTHORS	PURPOSE
Krishnammal A, Sindhiya S, Dhivya P,Janaki K	**A common technology used for the delivery of OTPs is text messaging.OTP over SMS might not be encrypted by any service provider. In addition, the cell phones which is used to receive the SMS also play an important role, in which more than one phone comes into account.**
R.Anbuvizhi, V.Balakumar,V.Gokulakrishnan	**Nowadays fraud transactions in real time are increasing, so identifying large-scale patterns across many transactions or detecting anomalous behavior from an individual user can change the fraudulent in online transaction. Thus banks are turning to analytics to predict and prevent fraud in real times. In this project, proposed system deals with Credit / Debit card management to improve its scalability and efficiency in big data environment, it is implemented on (HDFS) Hadoop distributed file system. On the other hand, nowadays fraudulent and web attacker are increased to steel the password.**

Mohammed Hamid Khan	**In today's world, money can be required at anytime or anywhere such as shopping, travelling or health emergencies etc. The need of money can only be satisfied when you are carrying money with you. That also increases the risk of getting robed. Bank is a safest place to keep money. Bank provides Automated teller machine (ATM) which can provide money any where you want. ATM is an easy way to get money, you just need to insert card and password and you just got the money.**

OVERVIEW OF THE PROPOSED SYSTEM

Though there are many online systems available on internet but this can compete with them with some advancement in its functionality and can be used by any bank organization to maintain their customers' account and online transaction process. The basic functionalities of the system are:

1) **Sign Up**
2) **Login**
3) **Password Recovery**
4) **View Profile**
5) **Contact Form**
6) **Amount Transaction**
7) **Amount Deposit**
8) **Amount Withdrawal using virtual password(OTP)**
9) **Delete account**

System requirement:

To view your accounts in Online Banking you will need internet access using one of thefollowing supported browsers:

1) **Microsoft Internet Explorer 6 or higher**

2) **Firefox 3**

3) **Safari 3**

Also, we used the following tools in the development of this project:

1) **Java NetBeans IDE**

2) **Java Development Kit**

3) **Oracle Database application**

Some features of the proposed model include:

1) **MENU DRIVEN:**

The project uses menu throughout which we can choose required options. Menus are self-explanatory, as they are very easy to use and user can go to any other web page using the menu.

2) **USER CONFIRMATION:**

Whenever the user tries to delete or edit the data, the system asks for the confirmation. This is used to avoid the accidental changes to the database. A confirmation is also provided for the exit of the application.

3) GRAPHICAL USER INTERFACE:

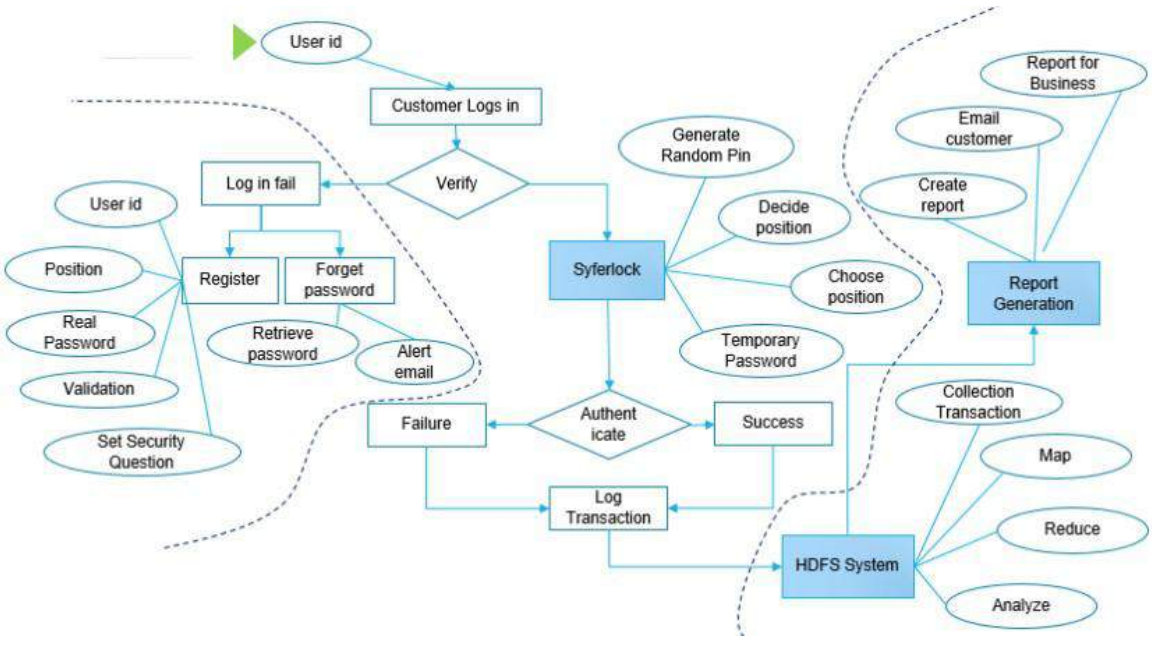
User is provided with a graphical interface in which user can select from various options and can perform desired operations with perfect understanding of the menu selected.

4) SECURITY AND ACCESS:

A password form has been provided at the beginning of the package. Entering the correct password will take user to the main user page

ER DIAGRAM

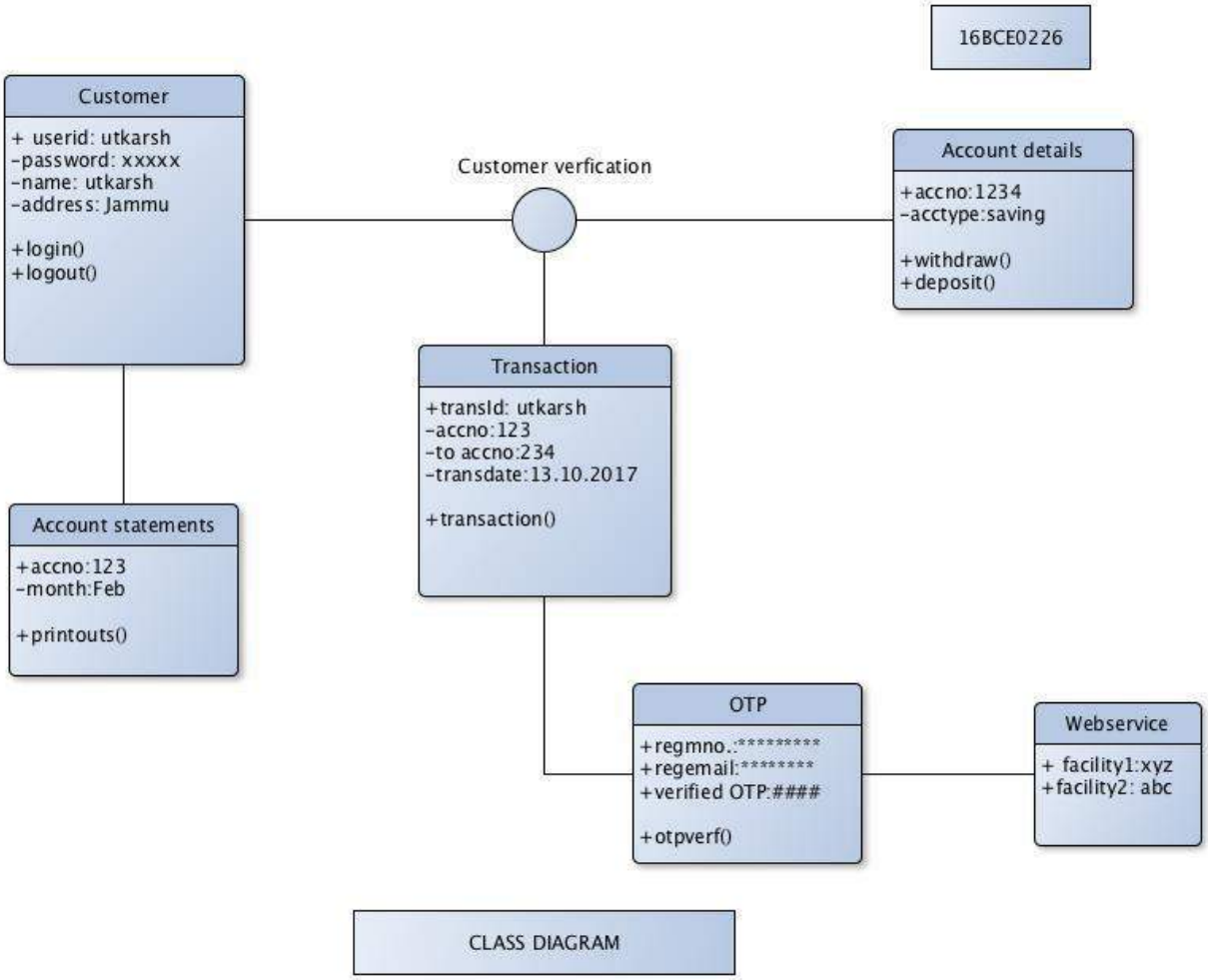
1) **Entitles,**
2) **Relationship between entities,**
3) **structural constraints**



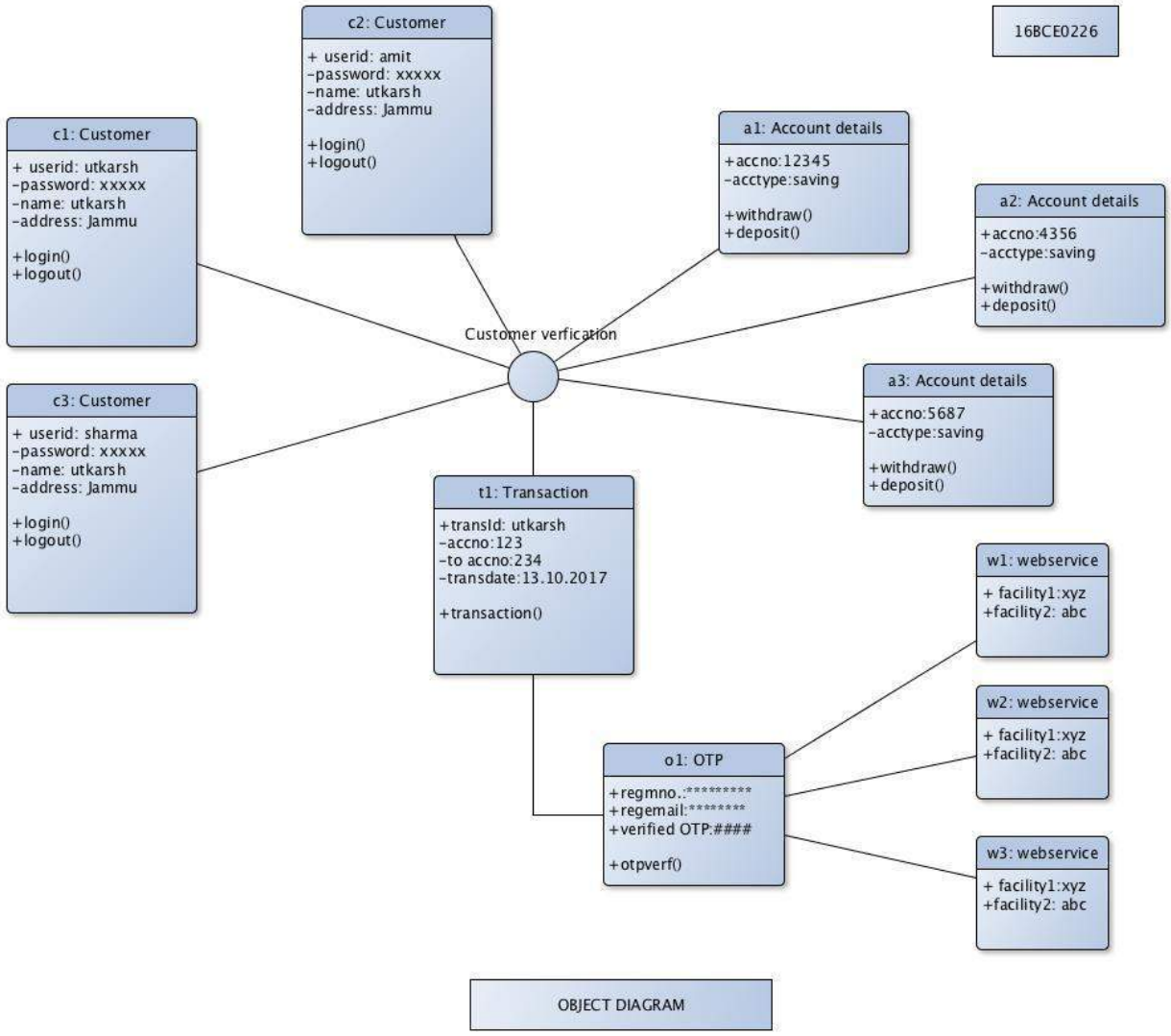
PROPOSED SYSTEM MODEL

1) Structural Diagrams

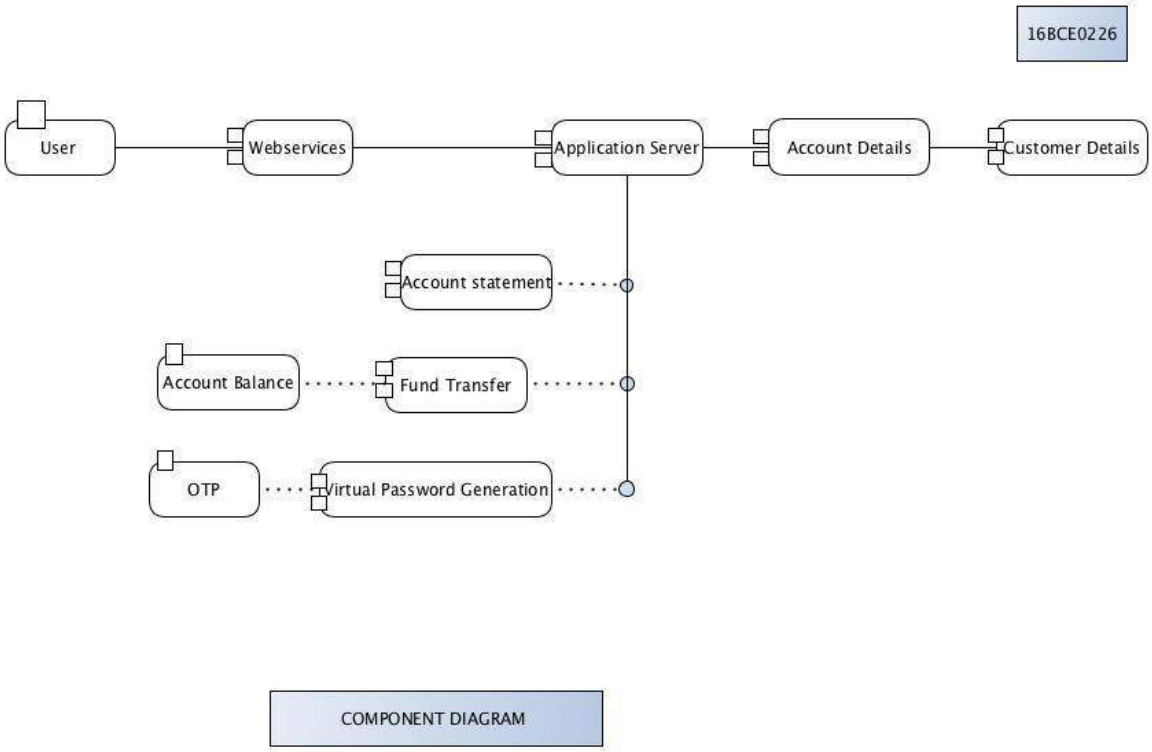
Class diagram



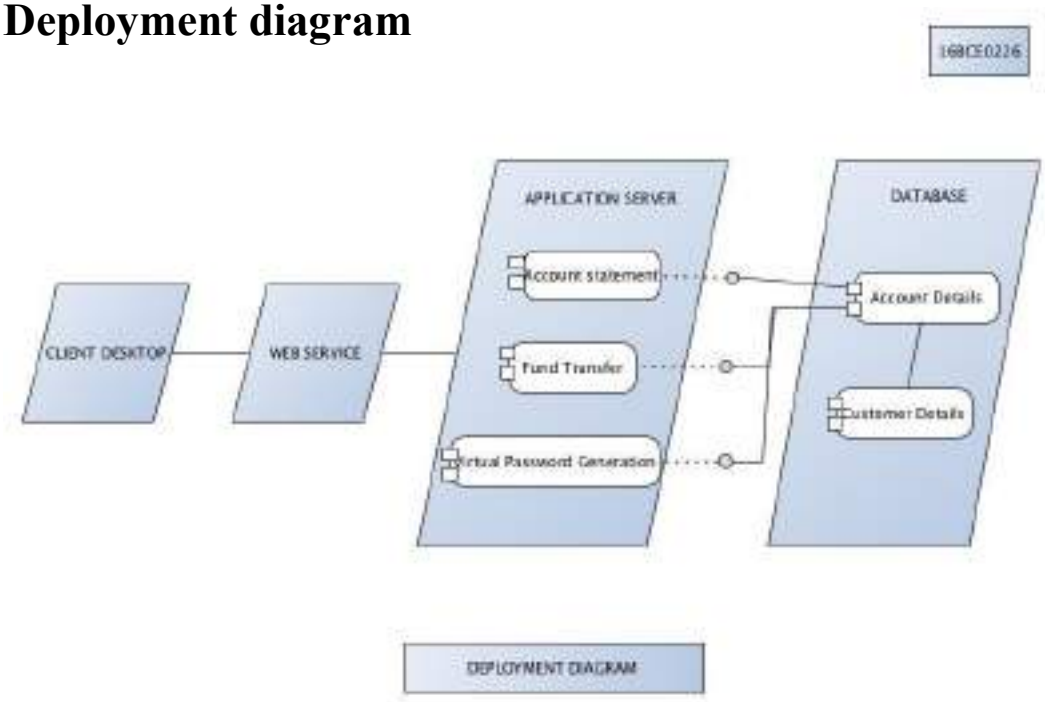
Object diagram



Component diagram

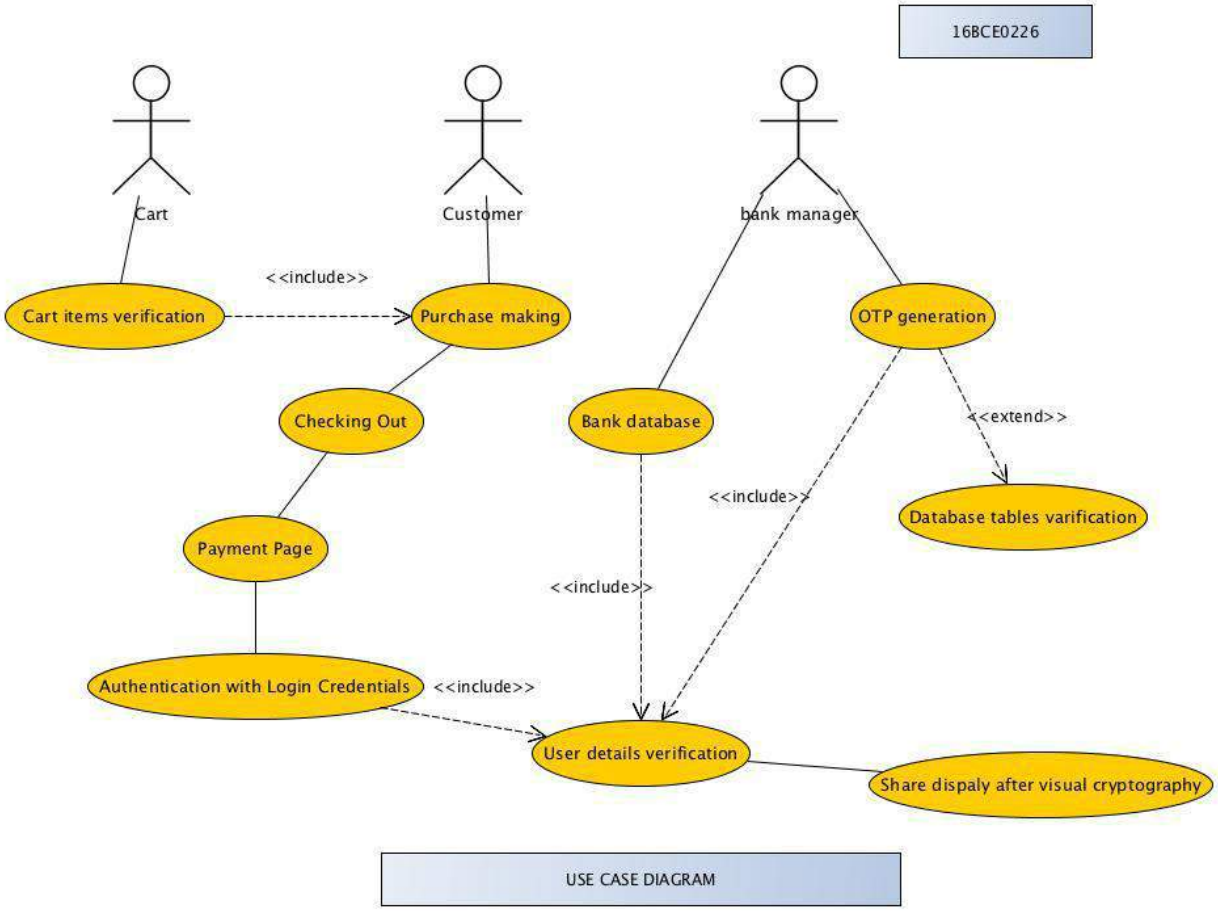


Deployment diagram

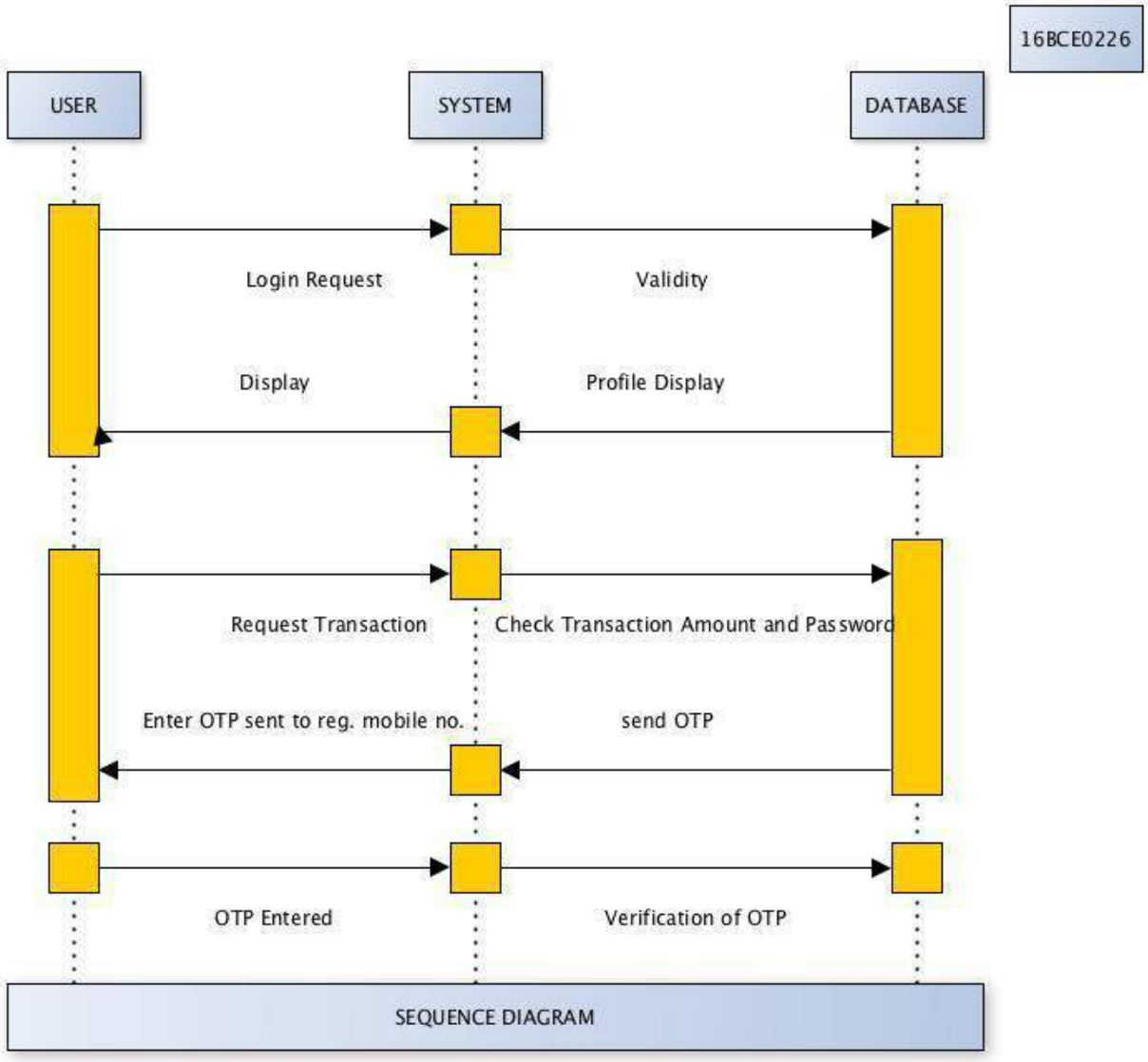


2) Behavioral Diagrams

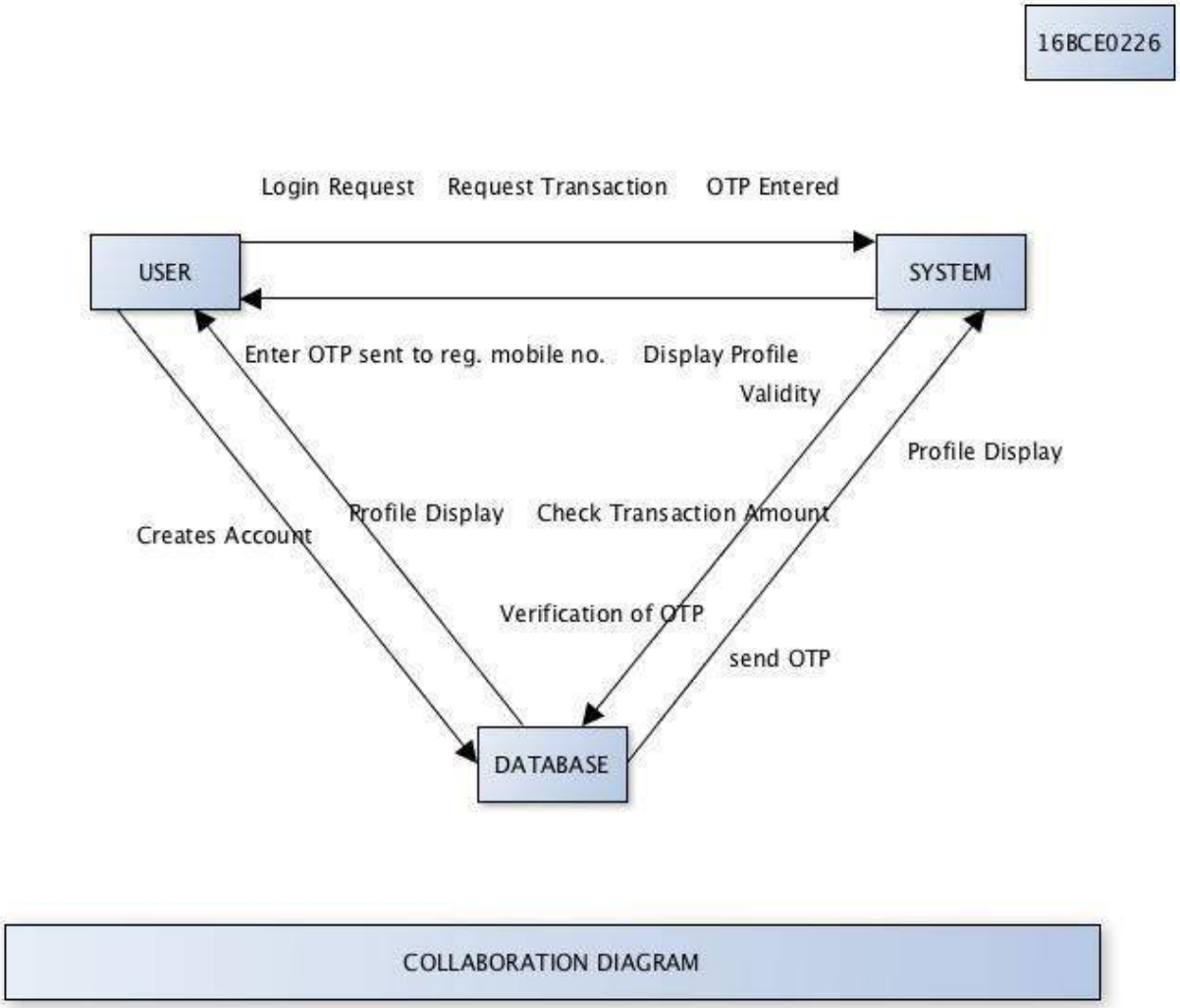
Use case diagram



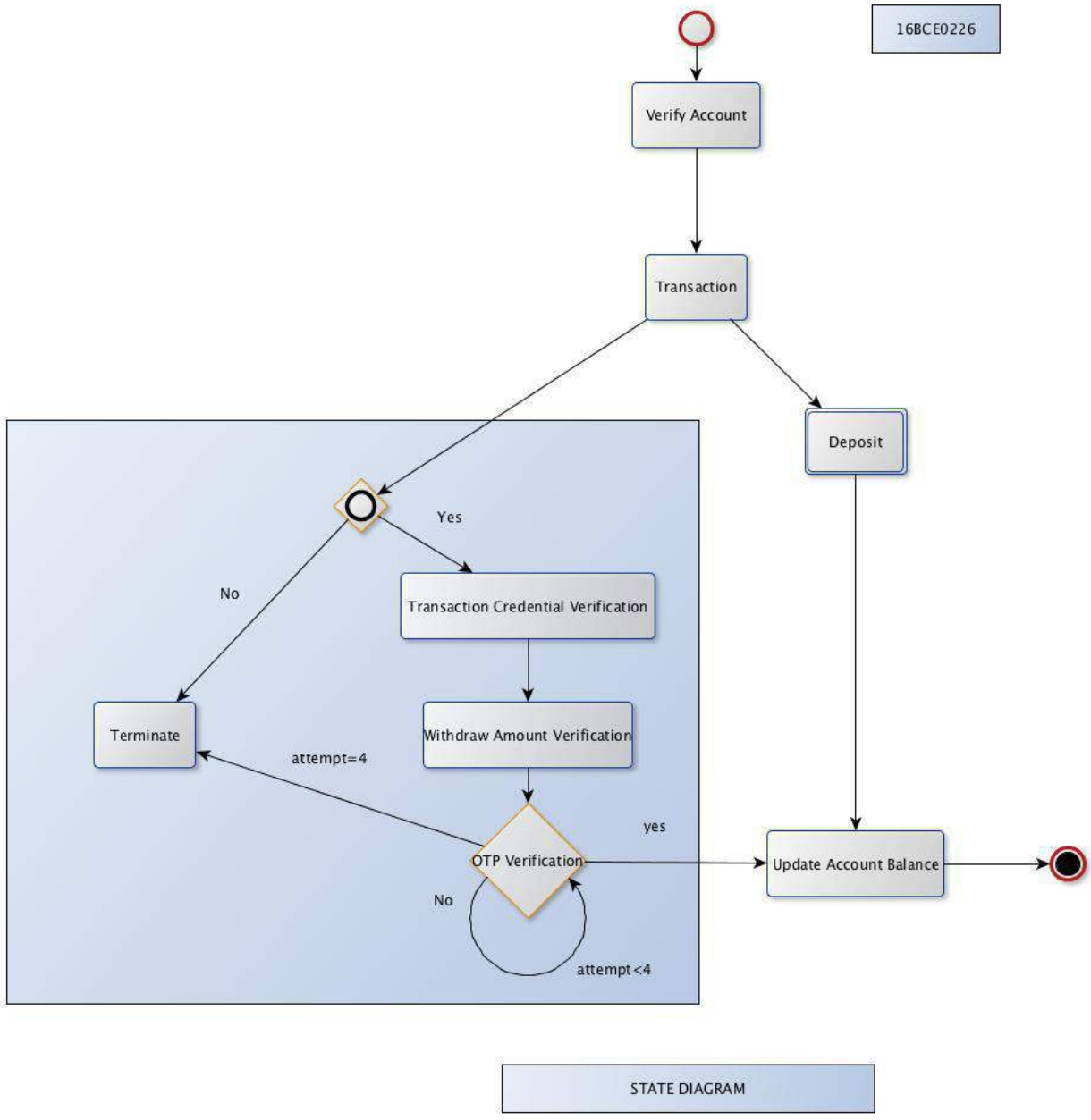
Sequence diagram



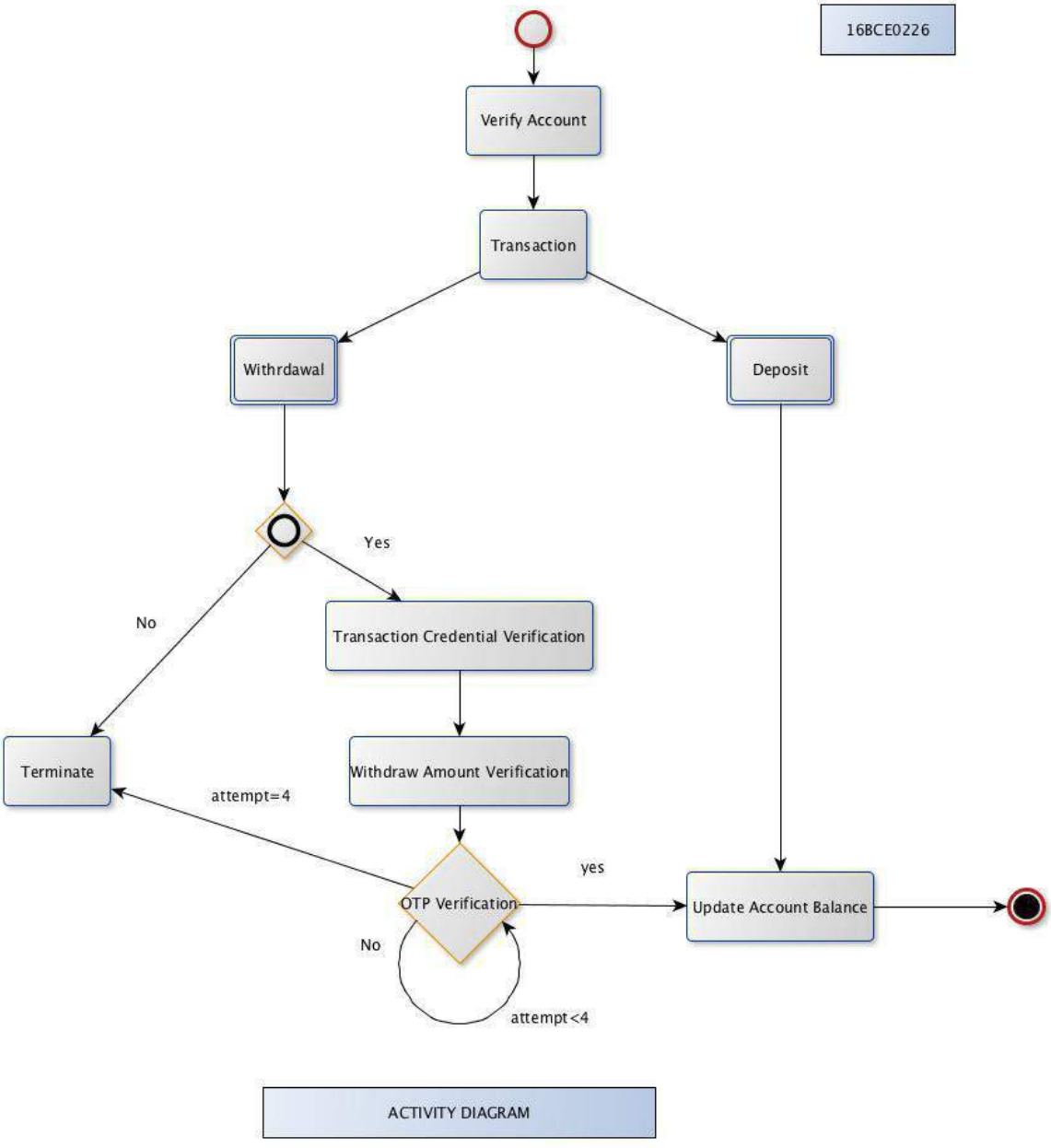
Collaboration diagram



Statechart diagram

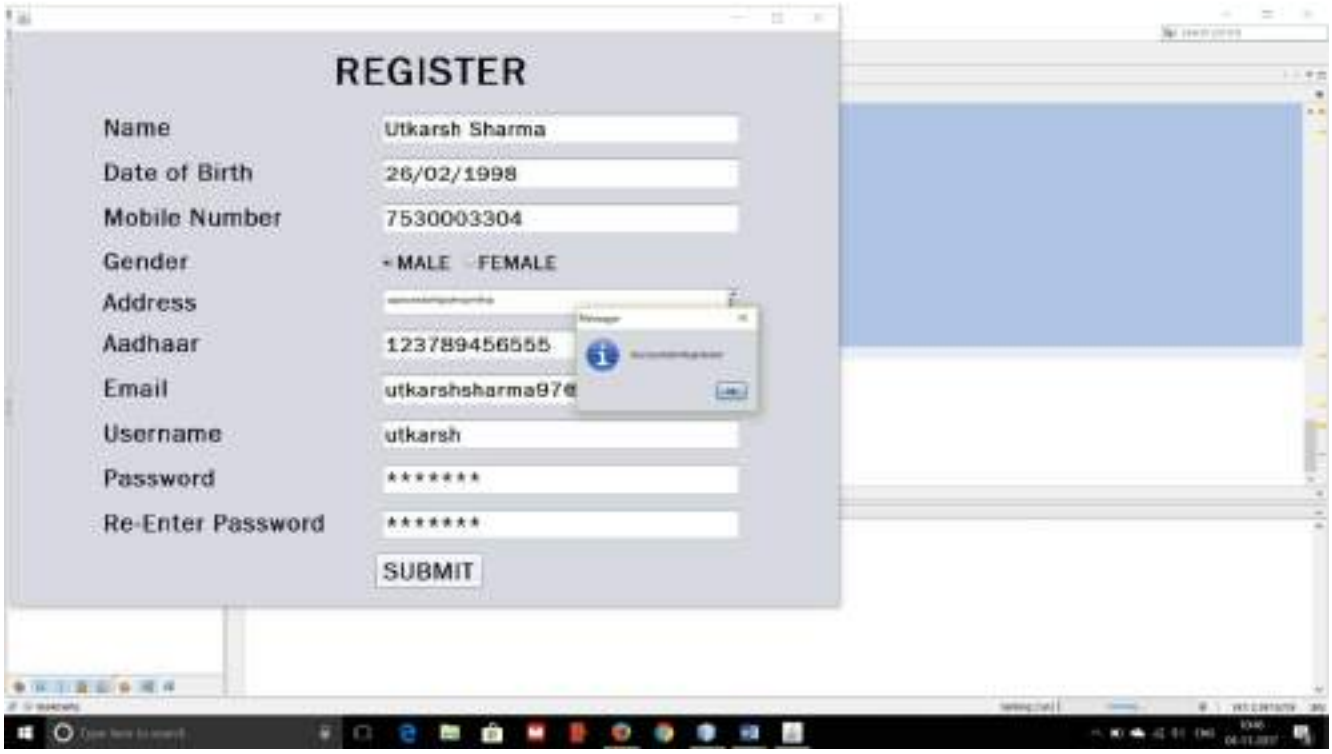


Activity diagram

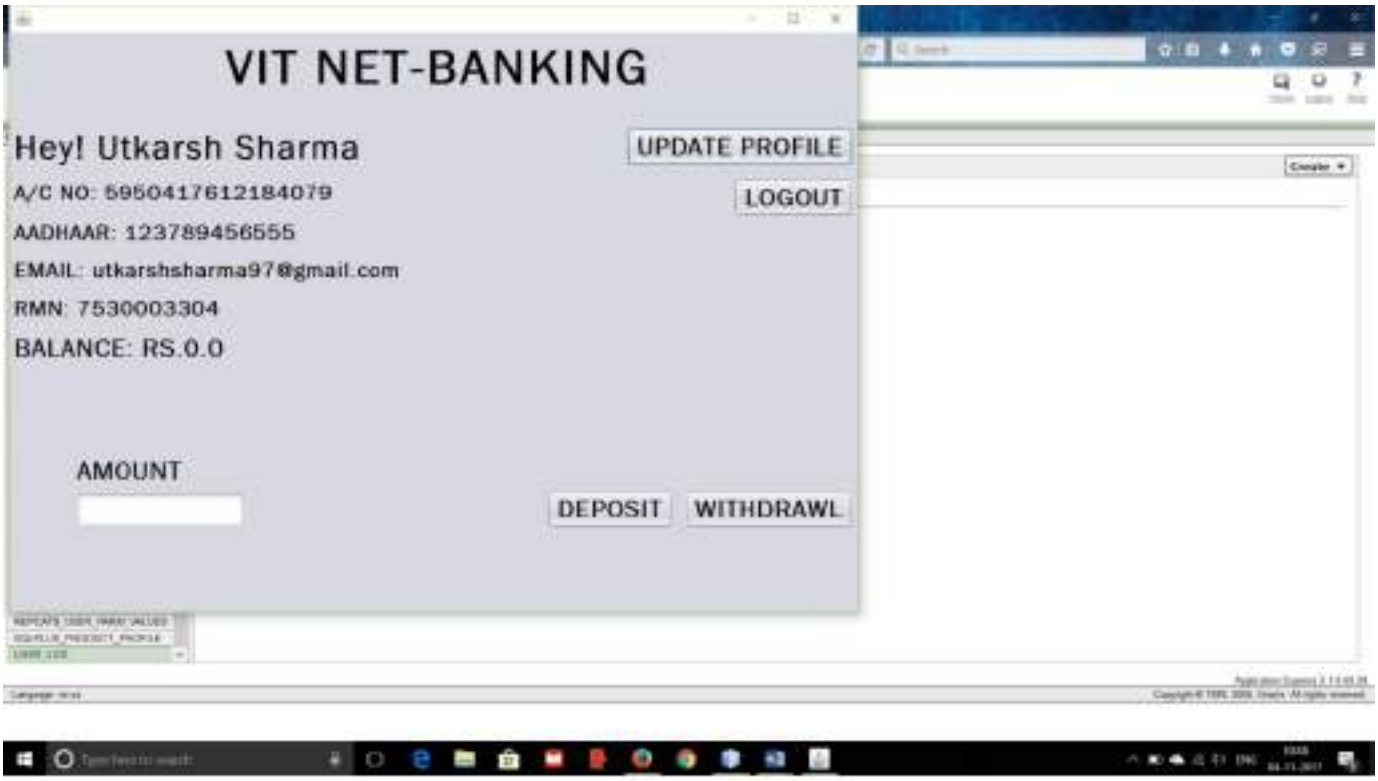


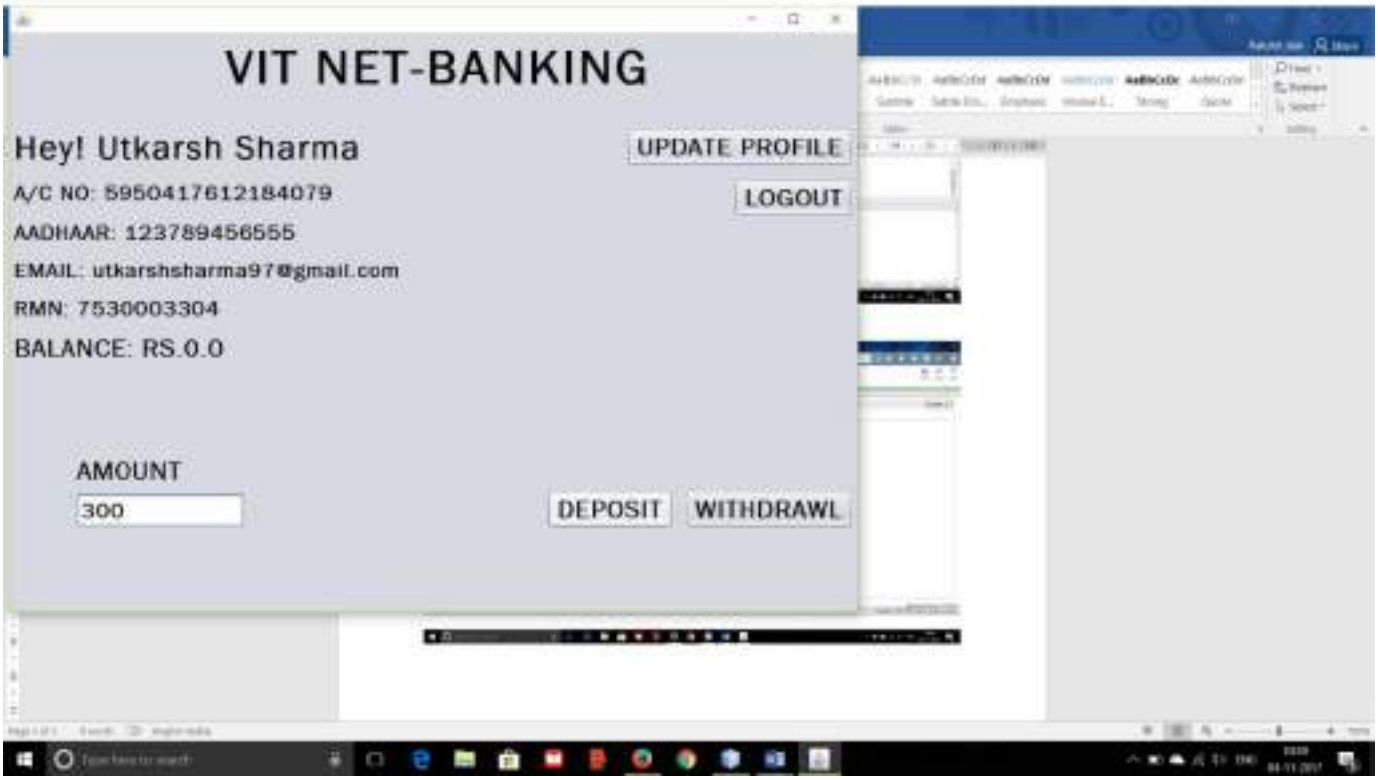
DEMOMSTRATION

STEPS: 1)Online Registration and Signup:

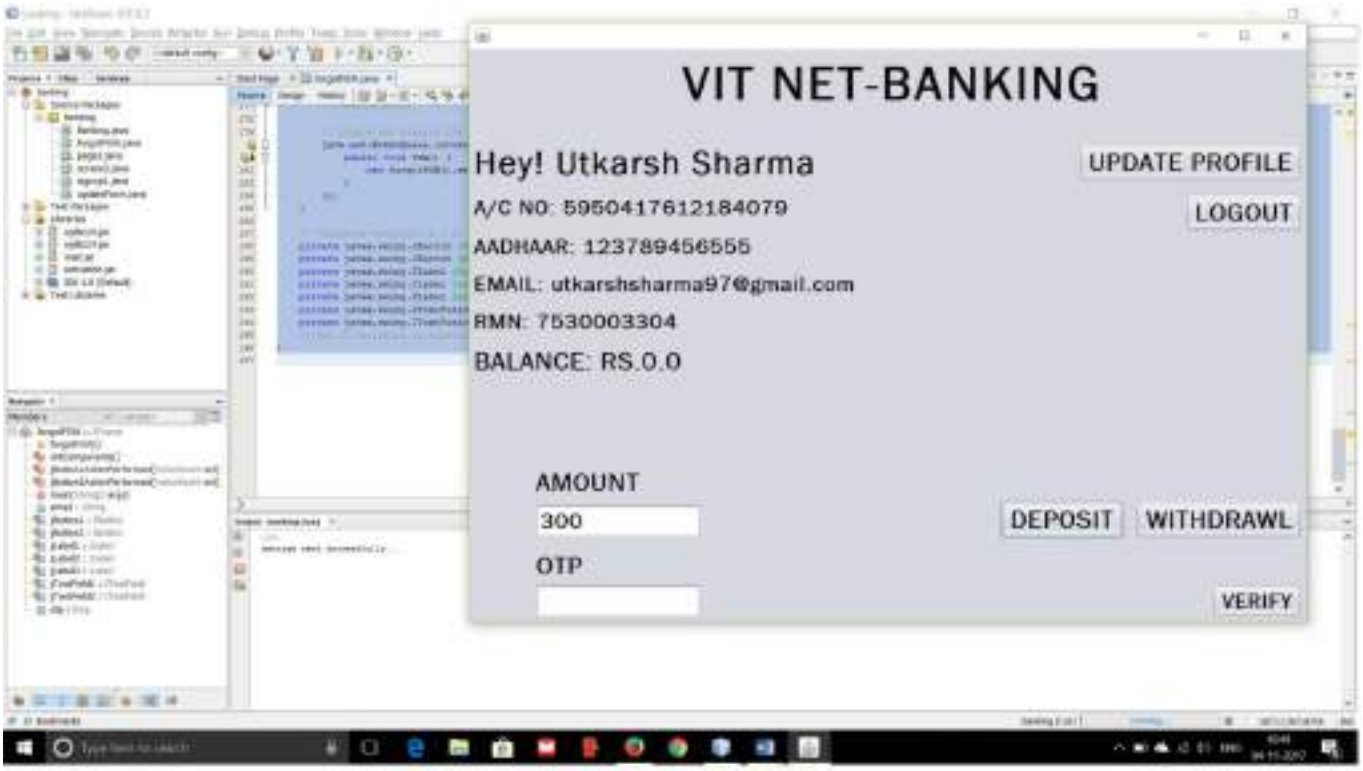


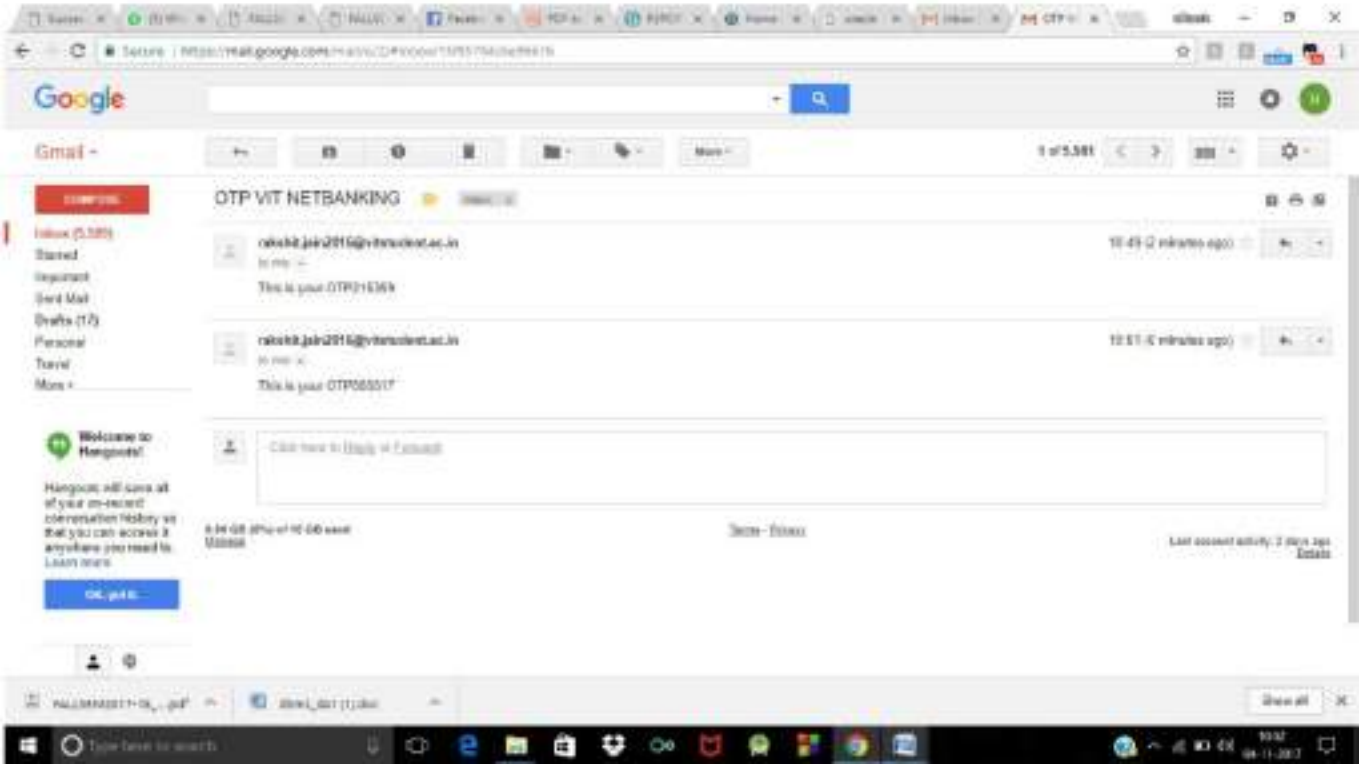
2) Depositing amount (Transaction)

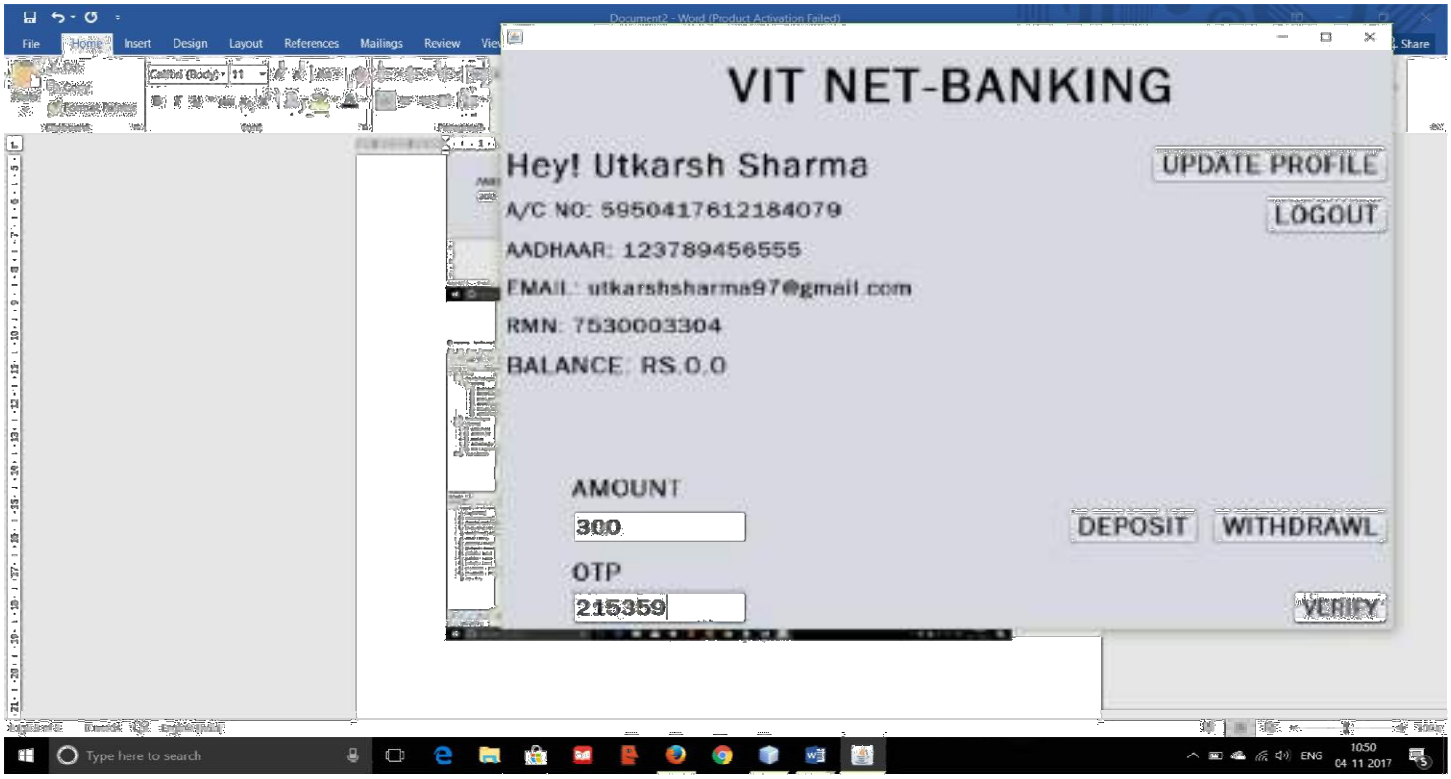


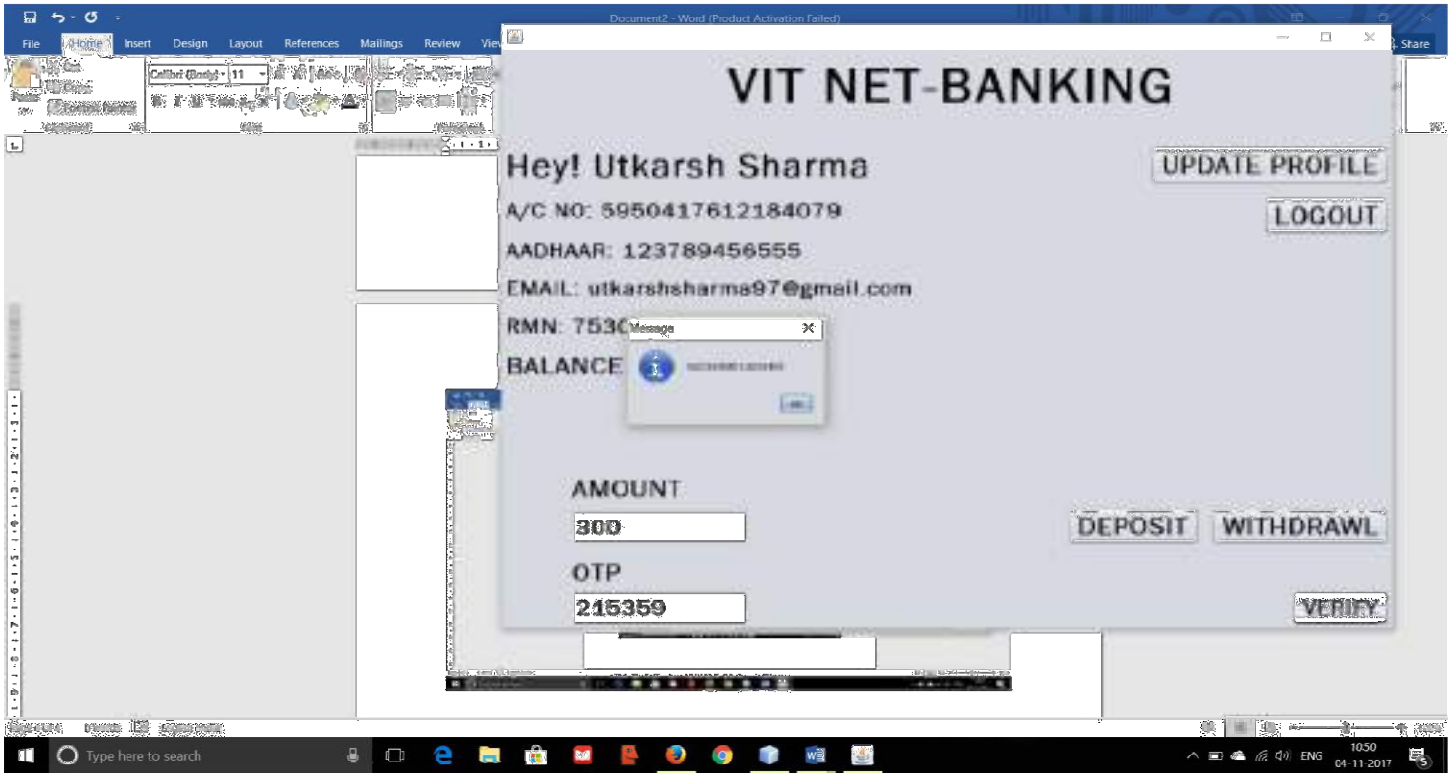


3) OTP Generation and Verification

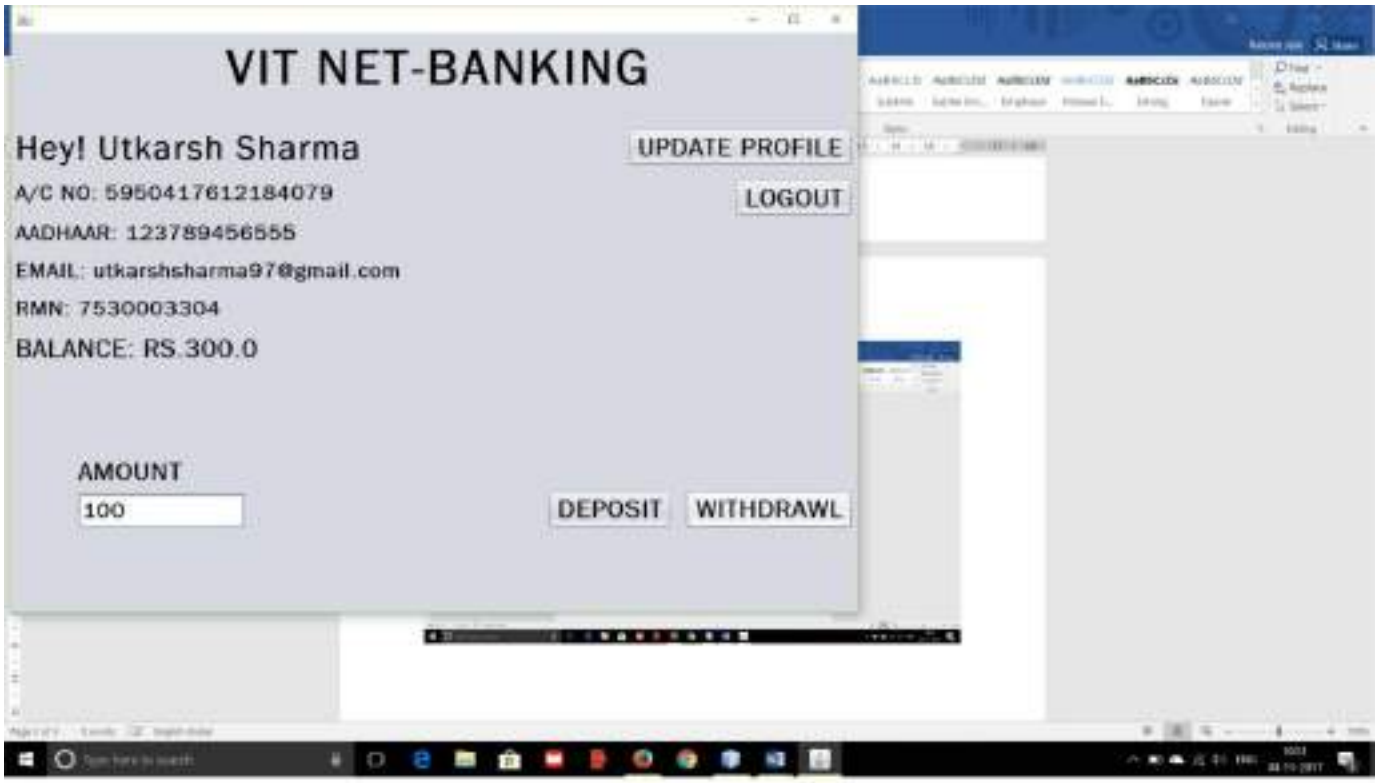


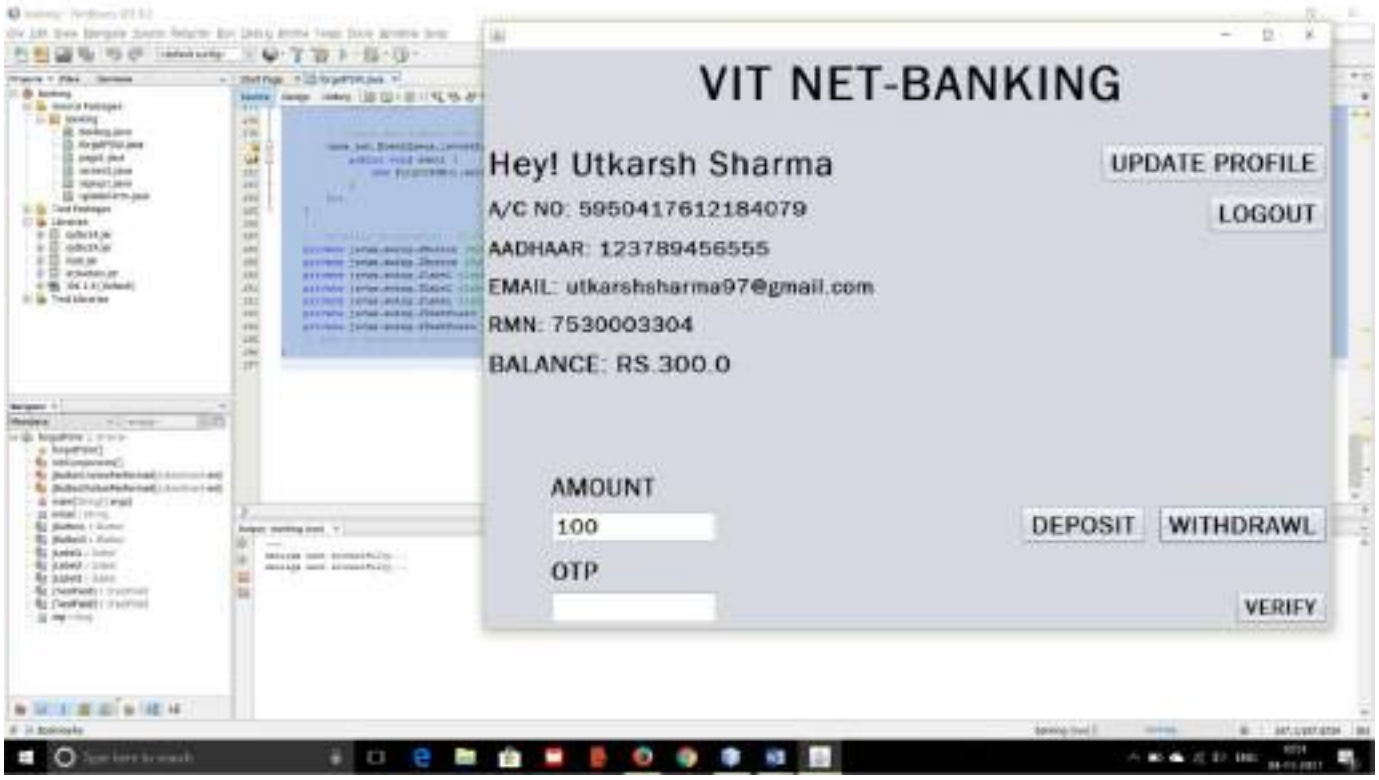



VIT NET-BANKING
Hey! Utkarsh Sharma
A/C NO: 5950417612184079
AADHAAR: 123789456555
EMAIL: utkarshsharma97@gmail.com
RMN: 7530003304
BALANCE: RS.0.0
UPDATE PROFILE
LOGOUT
AMOUNT
300
DEPOSIT
WITHDRAWL
OTP
215359
VERIFY

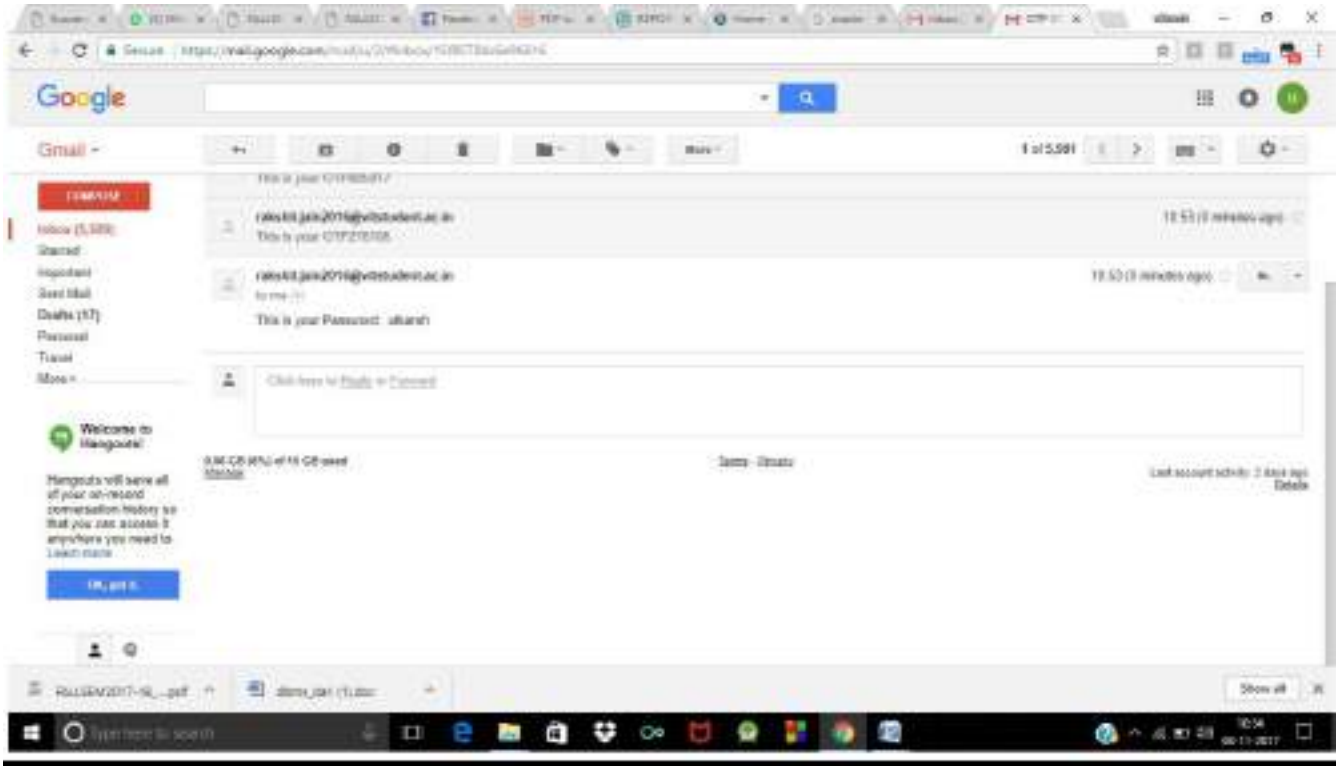

VIT NET-BANKING
Hey! Utkarsh Sharma
A/C NO: 5950417612184079
AADHAAR: 123789456555
EMAIL: utkarshsharma97@gmail.com
UPDATE PROFILE
LOGOUT
AMOUNT
300
DEPOSIT
WITHDRAWL
OTP
215359
VERIFY

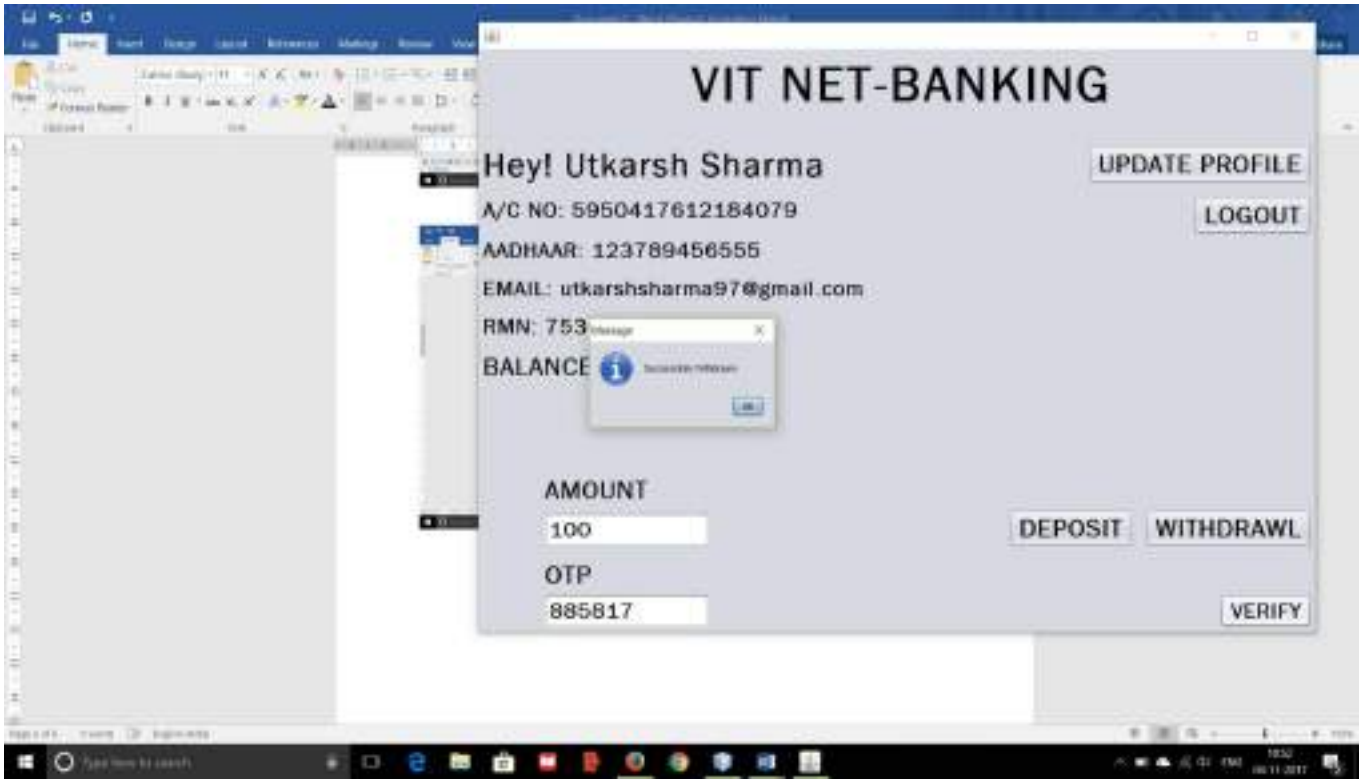
4) Withdrawing amount(Transaction)



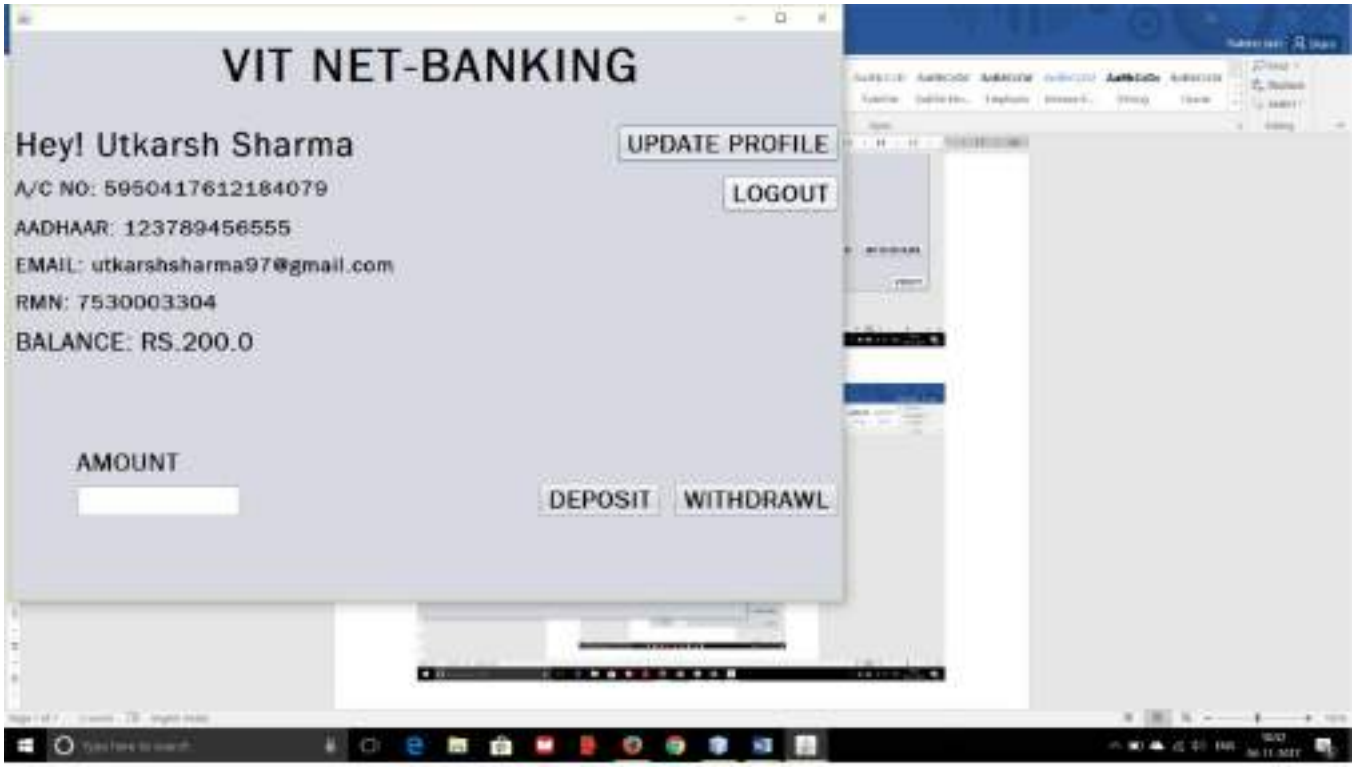


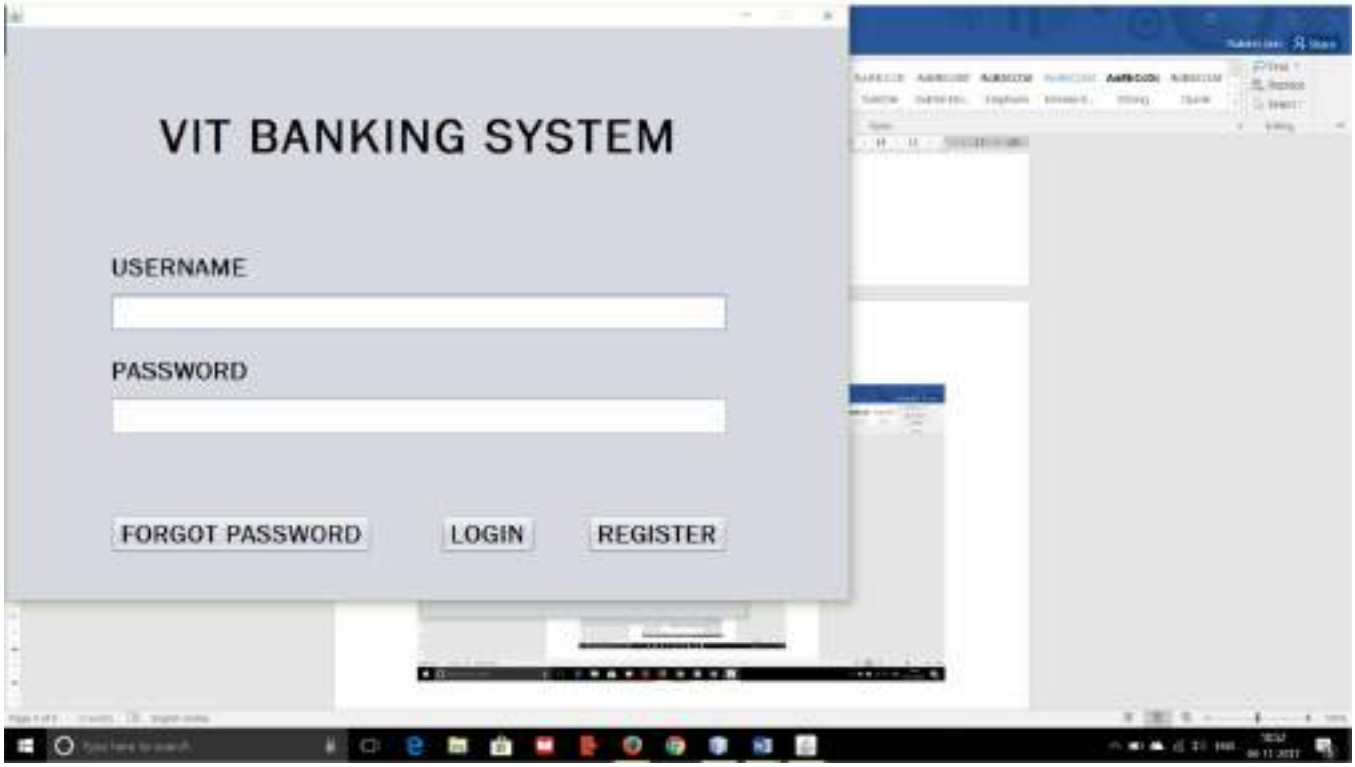
5) OTP Generation and Verification

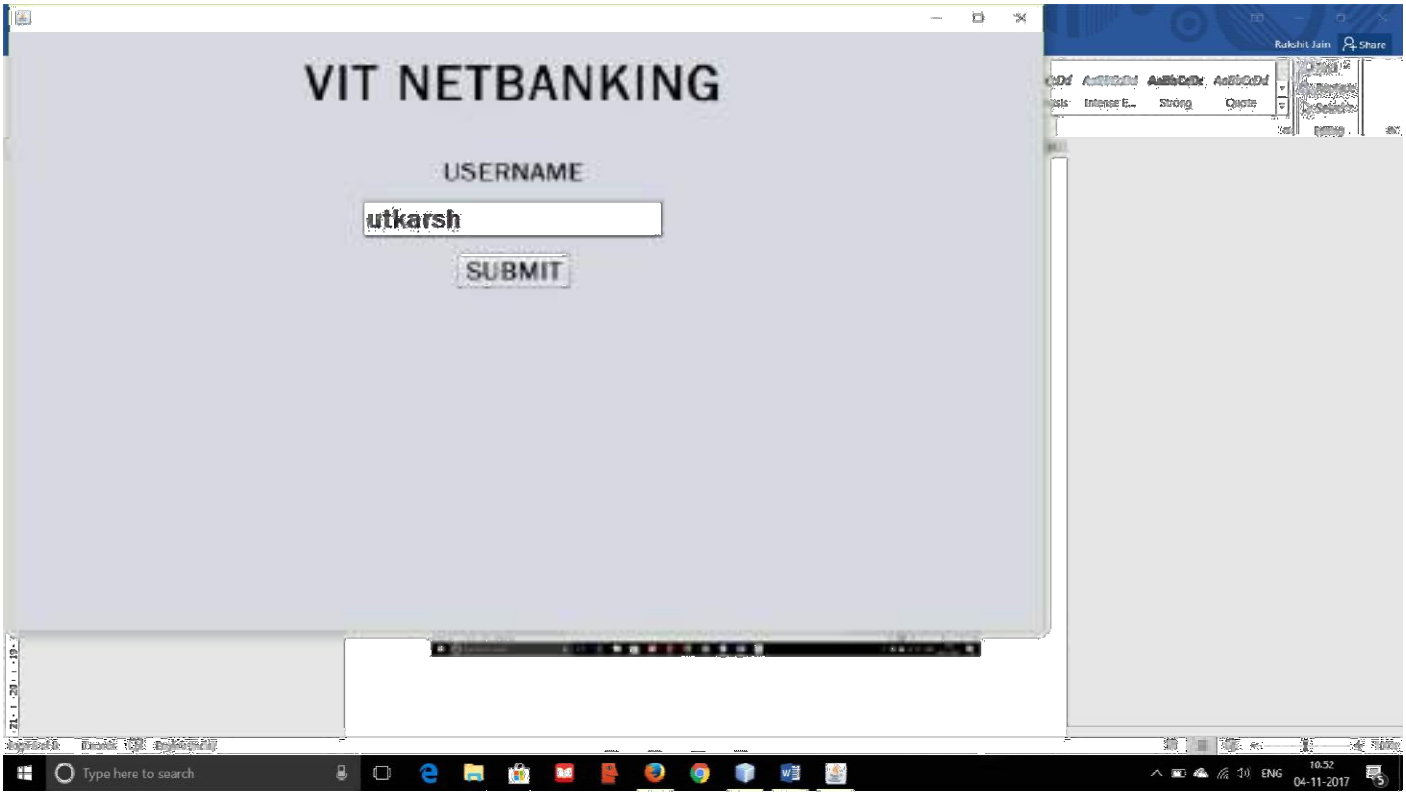


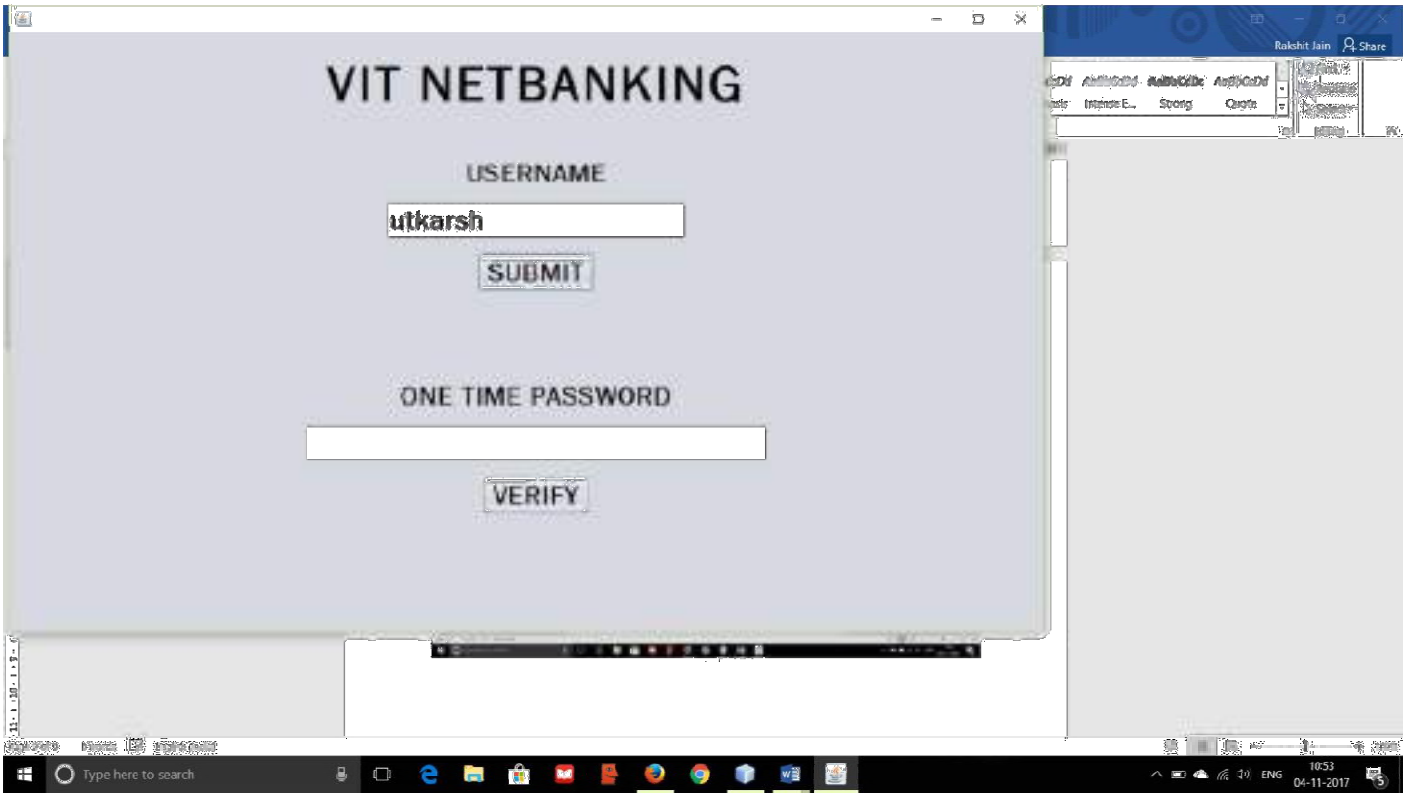


6) Changing Password

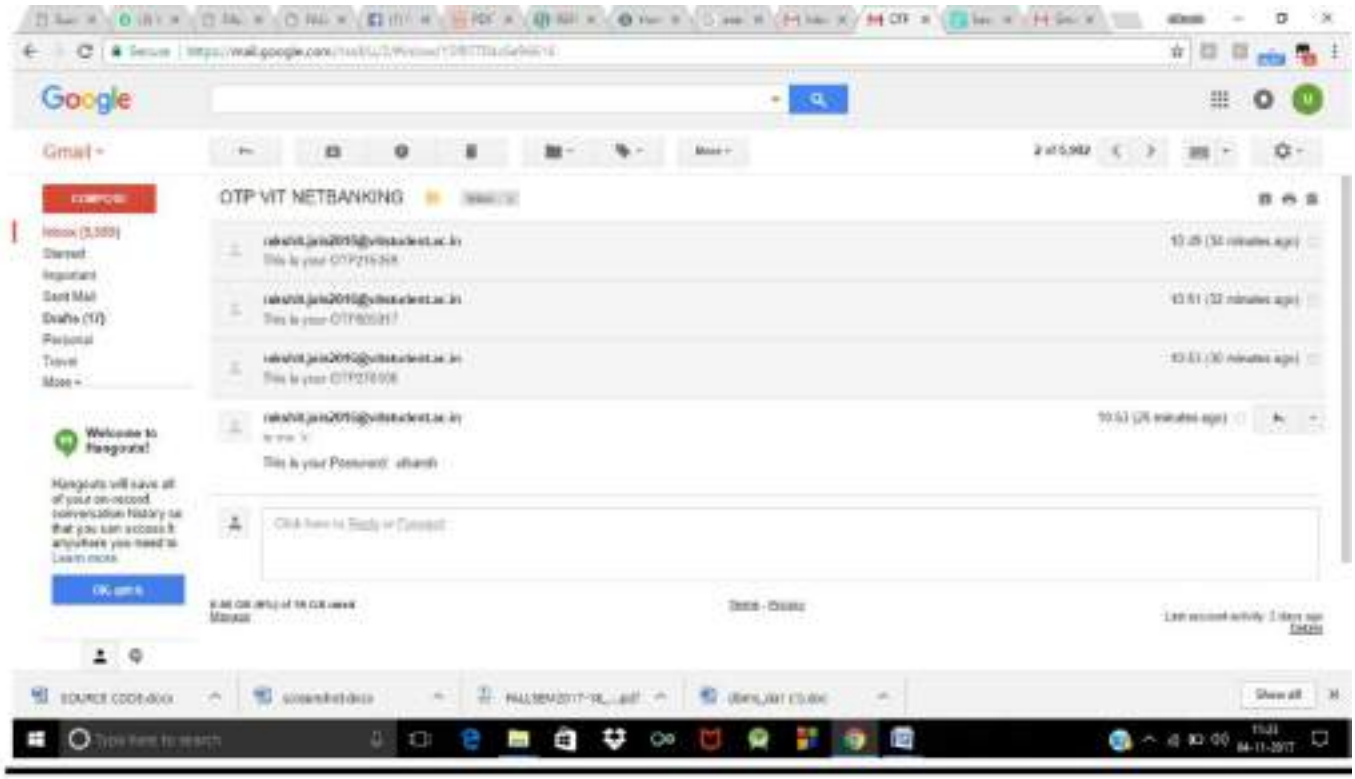


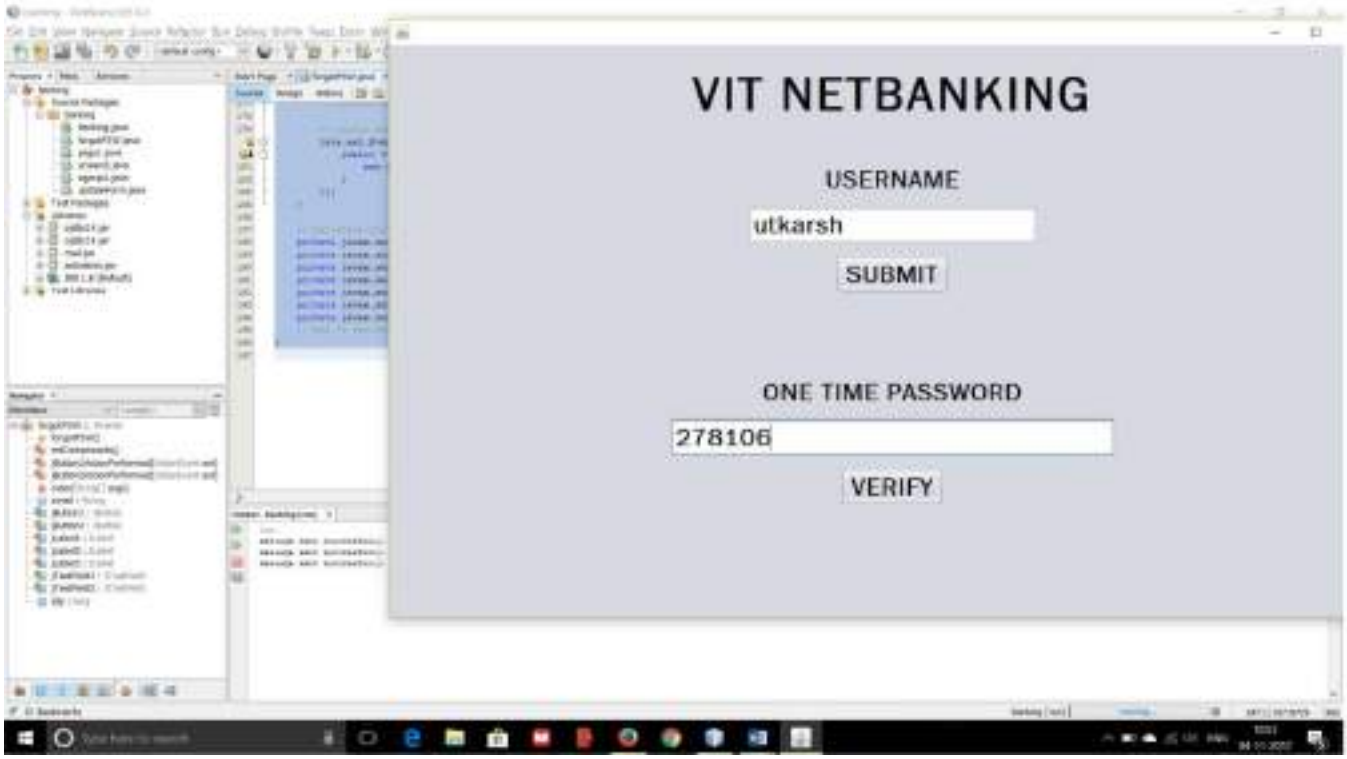


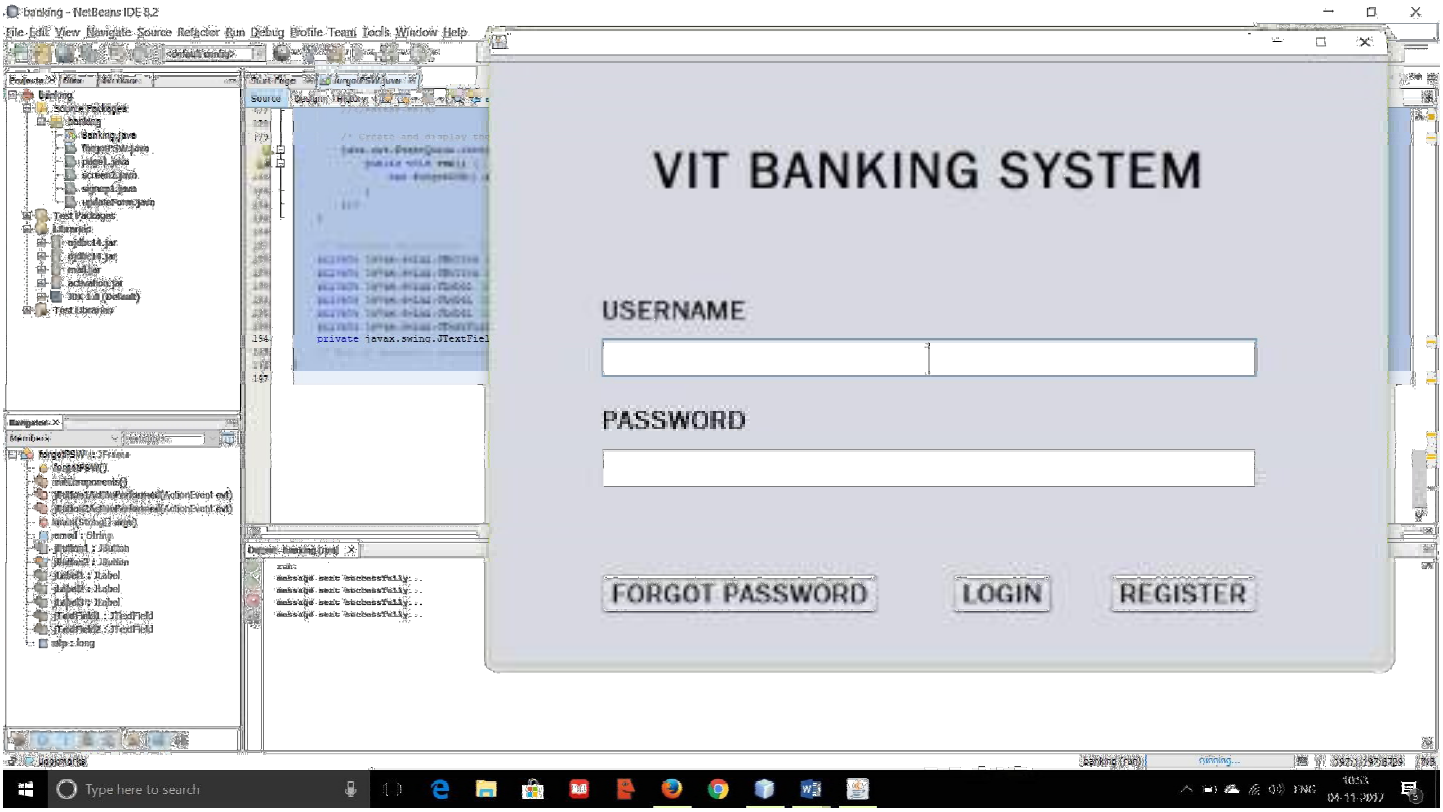

VIT NETBANKING
USERNAME
utkarsh
SUBMIT


VIT NETBANKING
USERNAME
utkarsh
SUBMIT
ONE TIME PASSWORD
VERIFY

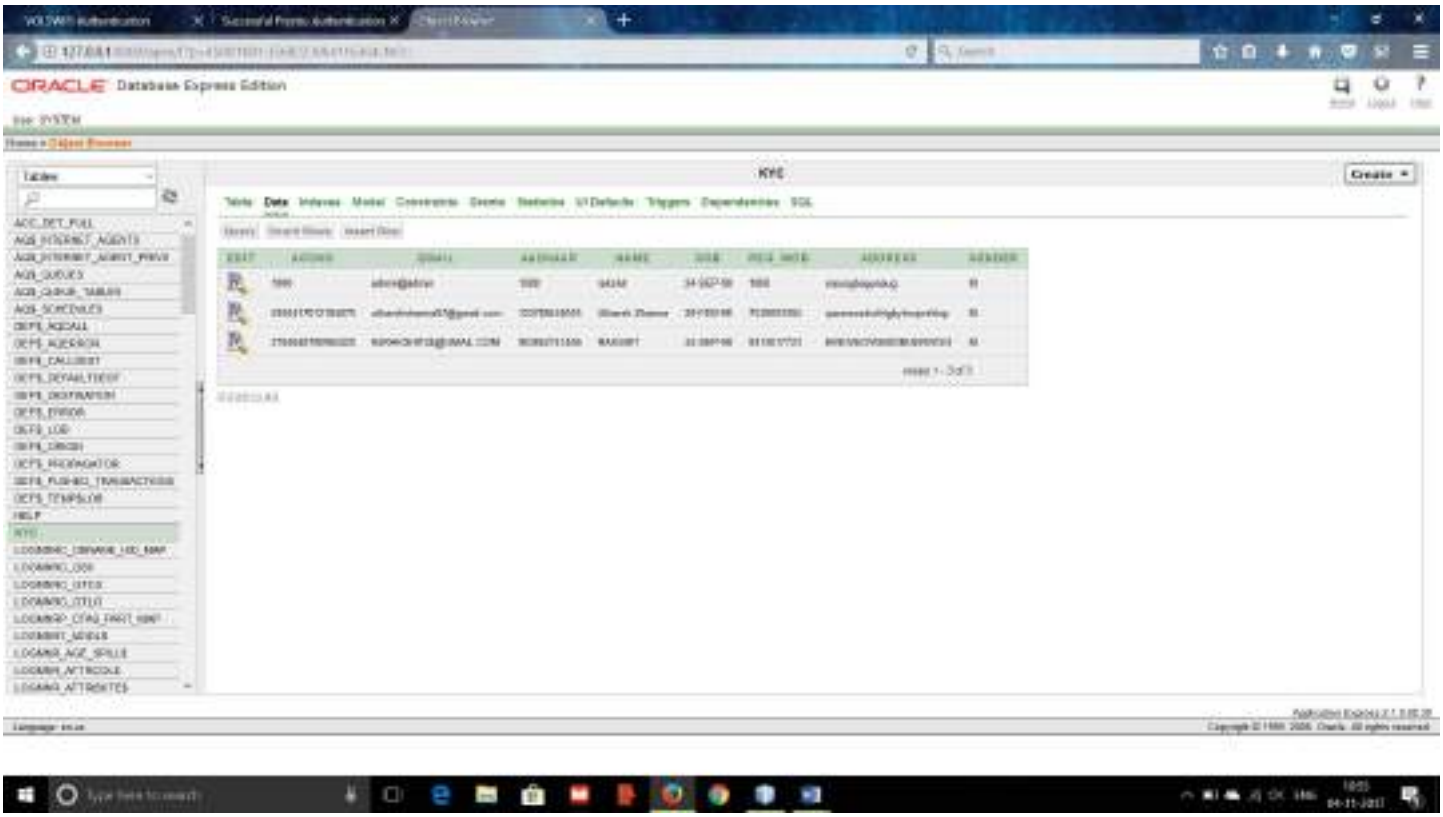
7) OTP Generation and Verification

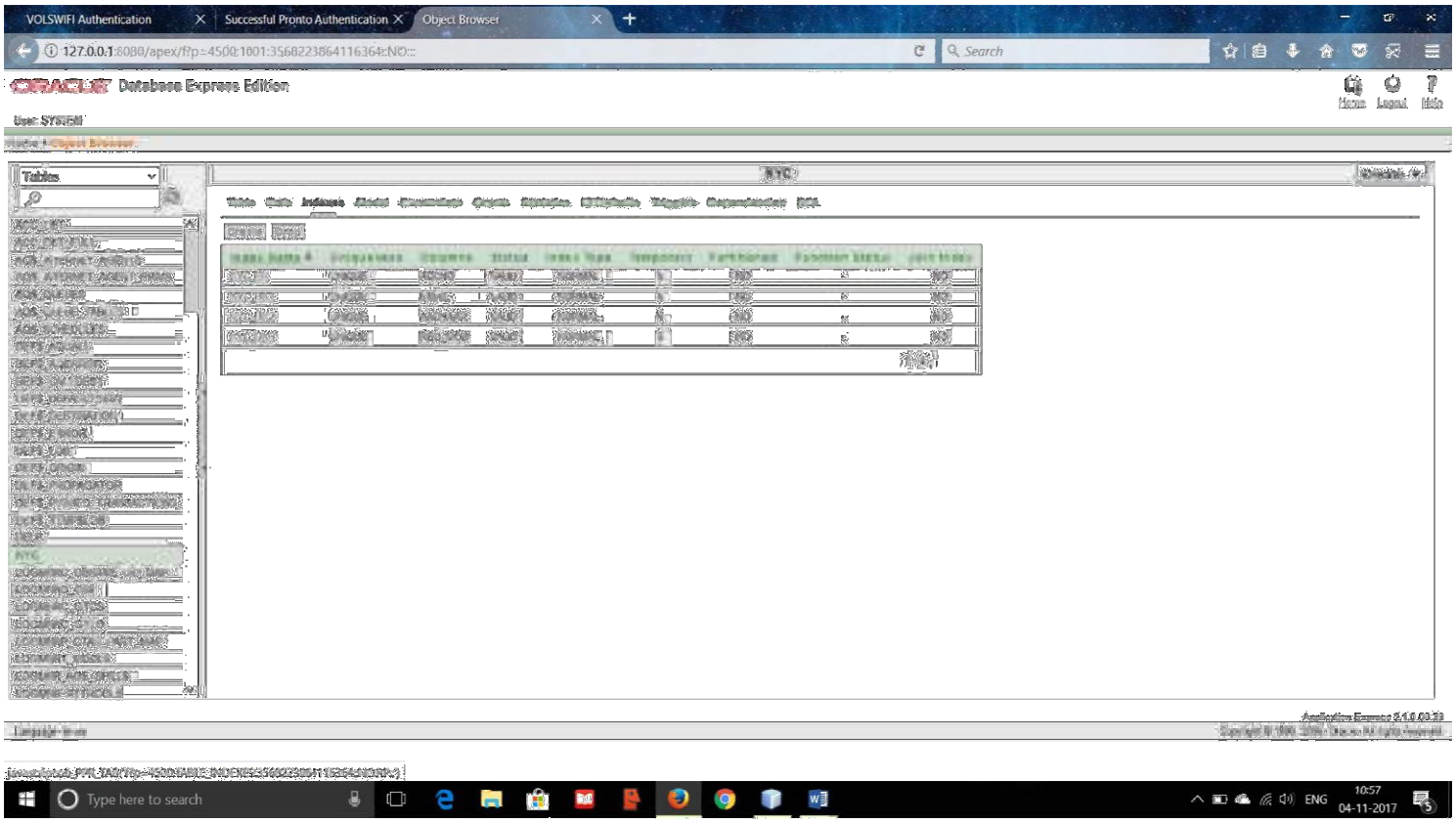


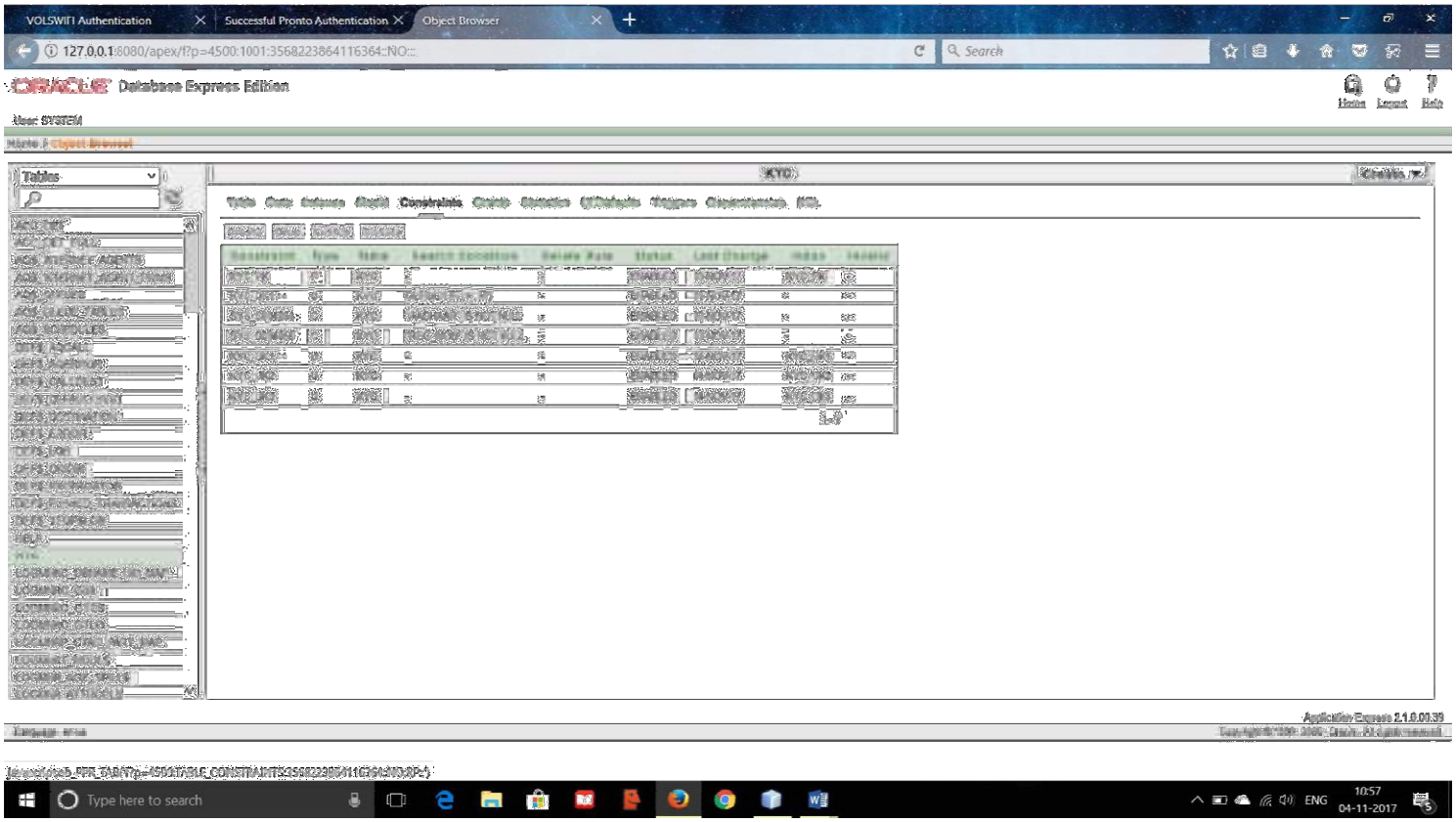


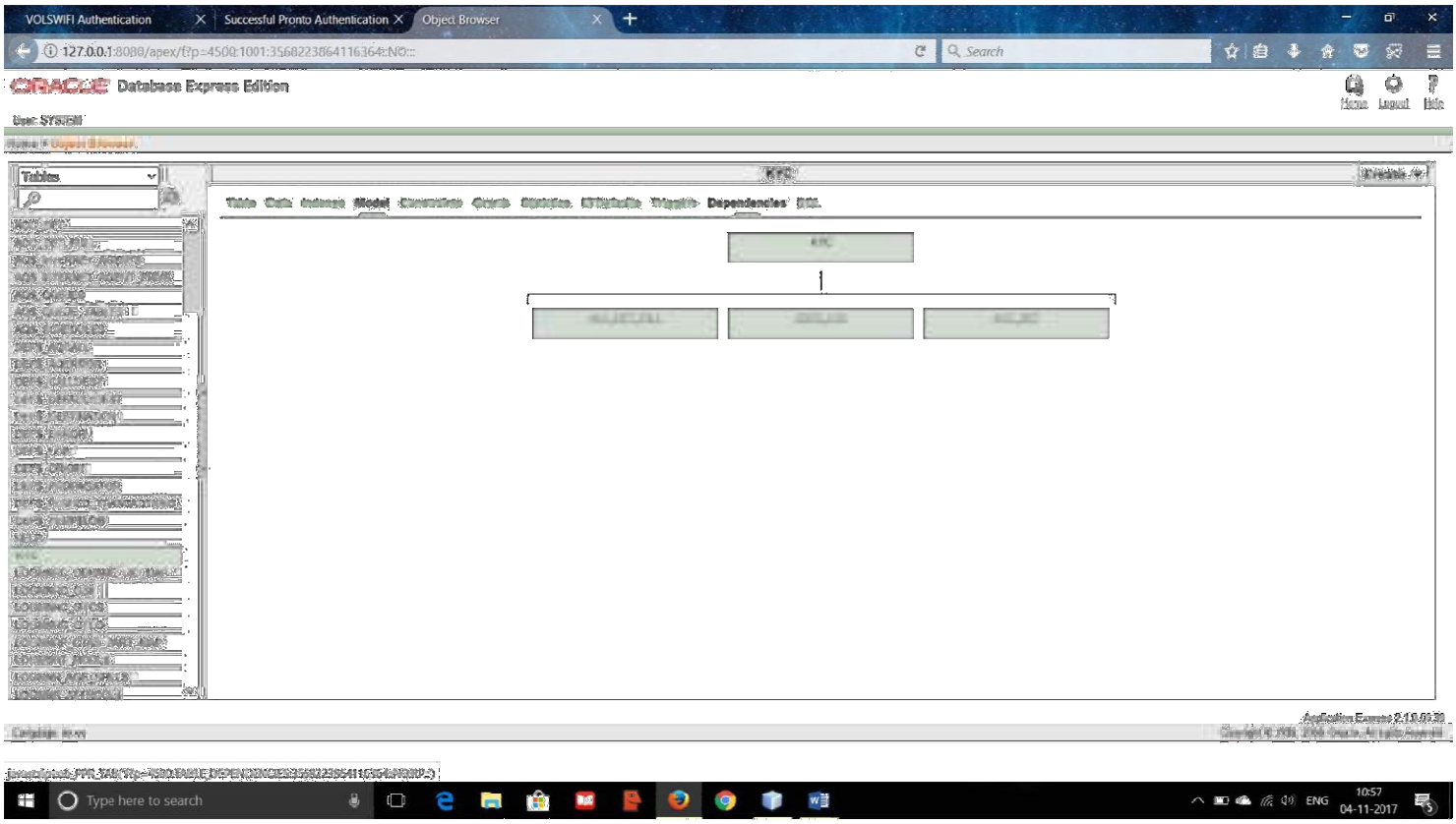


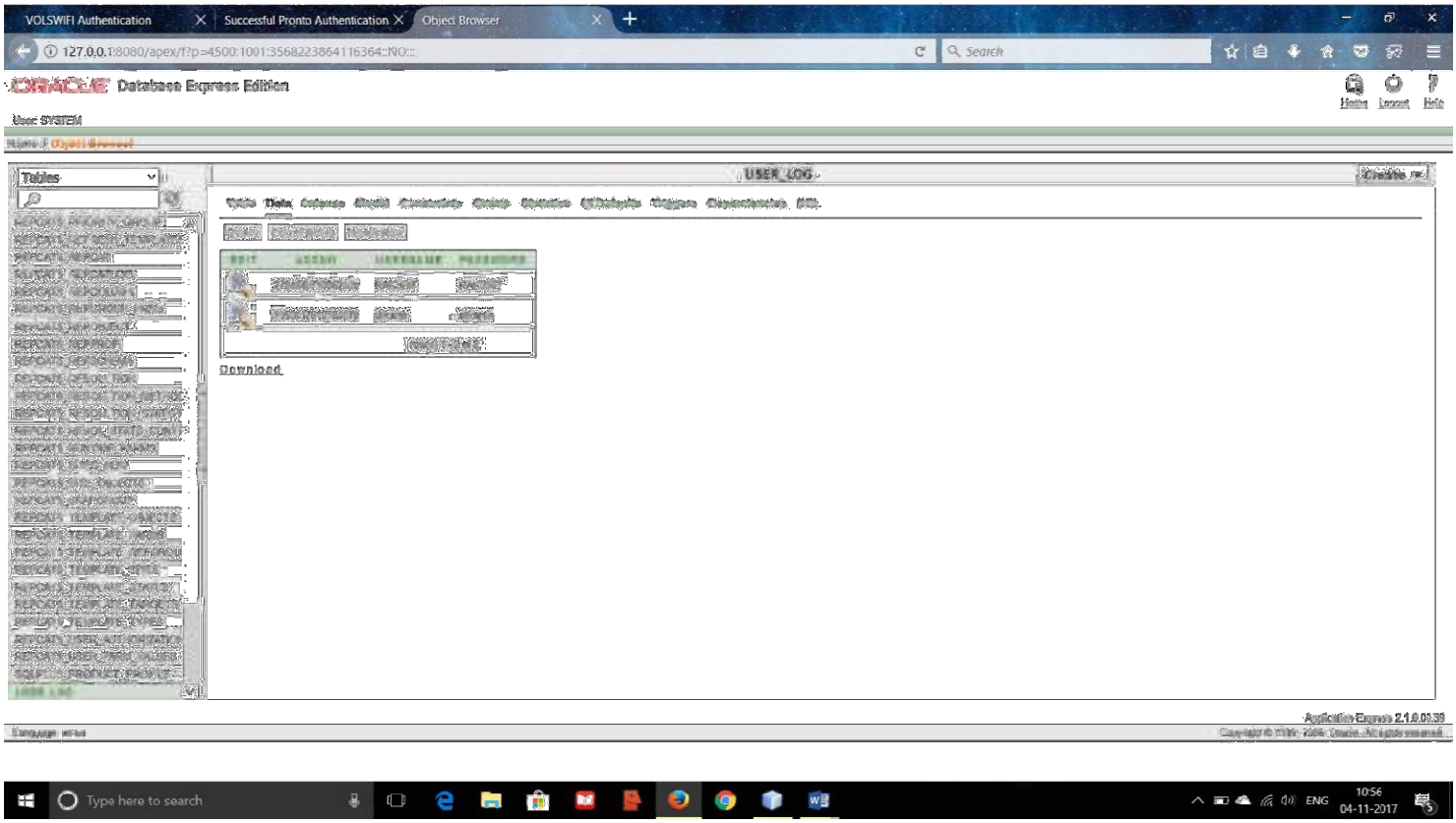
ORACLE DATABASE APPLICATION

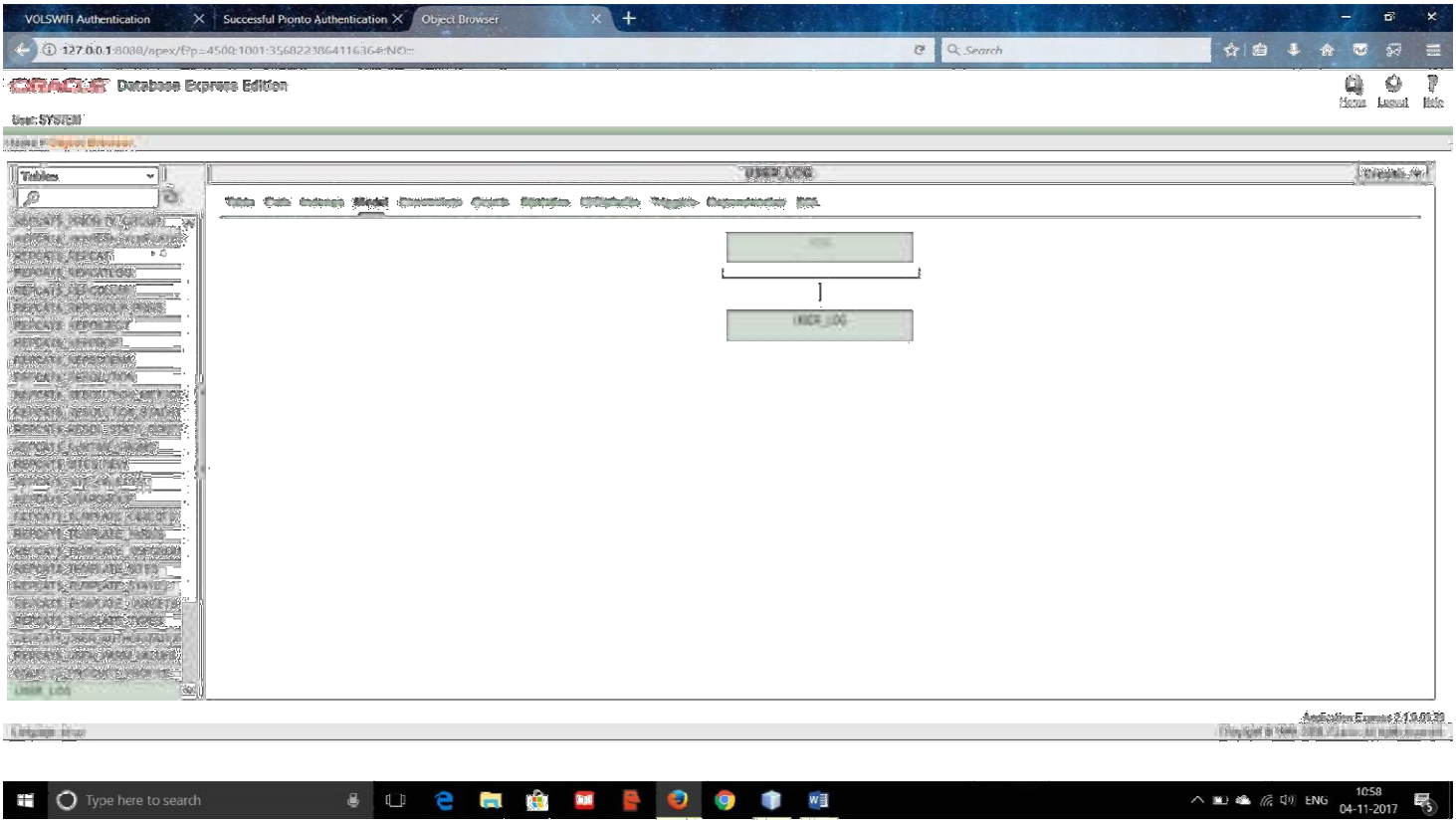


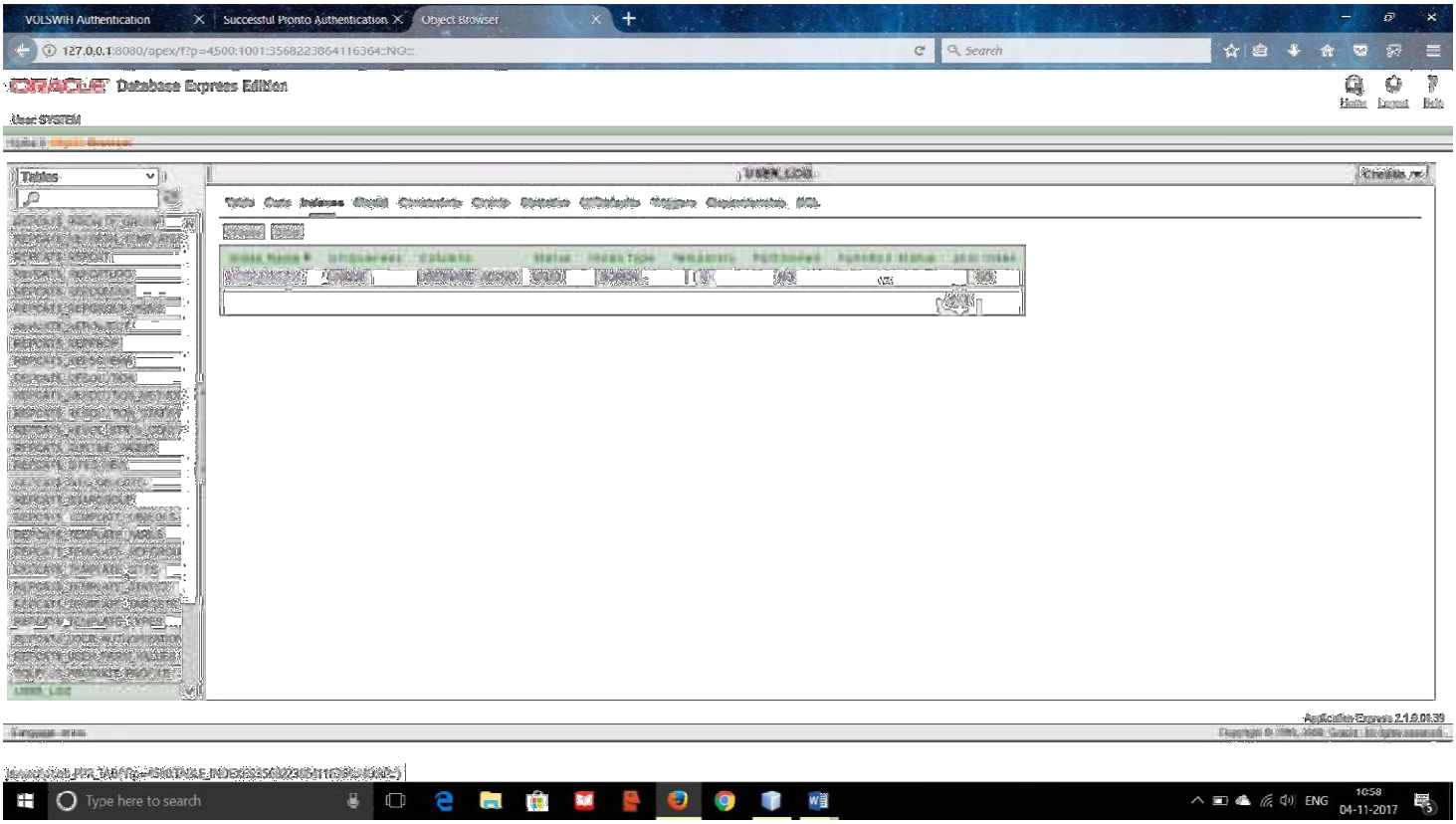

VOLSWIFI Authentication
Successful Pronto Authentication
Object Browser
127.0.0.1:8080/apex/f?p=4500:1001:3568223864116364::NO:::
Search
ORACLE Database Express Edition
Home
Logout
Help
Tables
XYC
Type here to search
ENG
10:57
04-11-2017

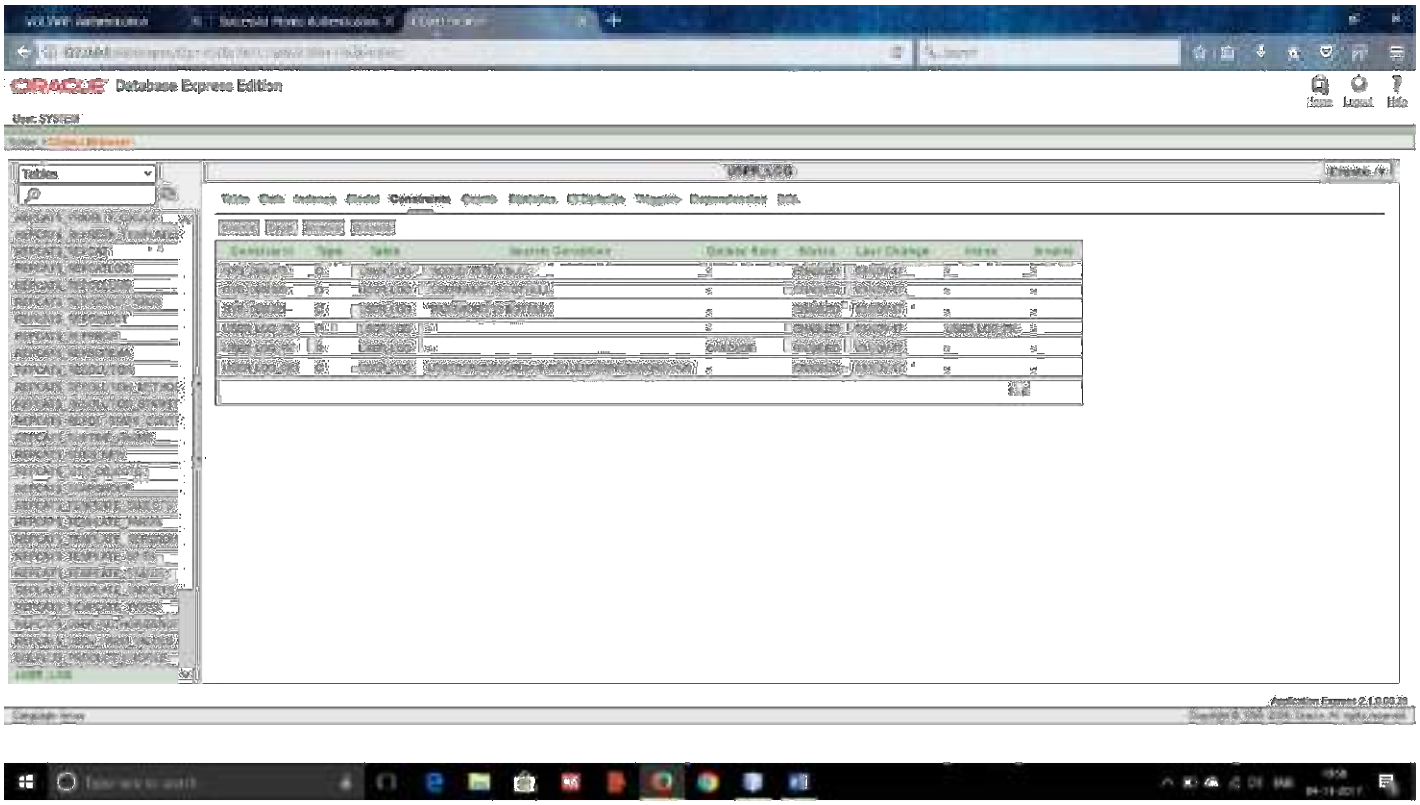

VOLSWIFI Authentication
Successful Pronto Authentication
Object Browser
127.0.0.1:8080/apex/f?p=4500:1001:3568223864116364::NO:::
Search
ORACLE Database Express Edition
Home
Logout
Help
Tables
XYC
Type here to search
ENG
10:57
04-11-2017

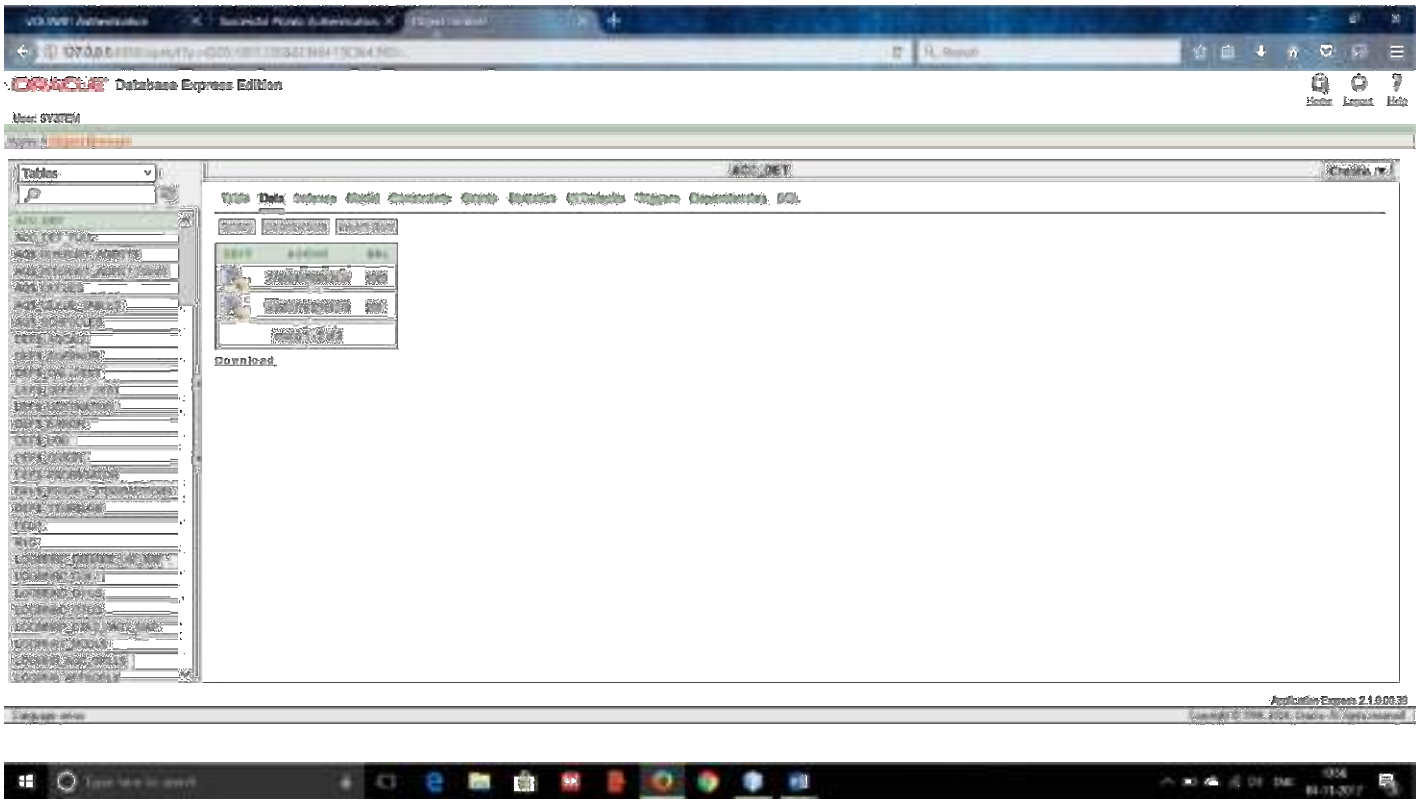

VOLSWIFI Authentication
Successful Pronto Authentication
Object Browser
127.0.0.1:8080/apex/f?p=4500:1001:35682238641163 64::NO::
Search
ORACLE Database Express Edition
Home
Logout
Help
User: SYSTEM
Tables
Table
Data
Columns
Model
Constraints
Grants
Statistics
UI Defaults
Triggers
Dependencies
DDL
Application Express 2.1.0.00.39
Type here to search
ENG
10:57
04-11-2017

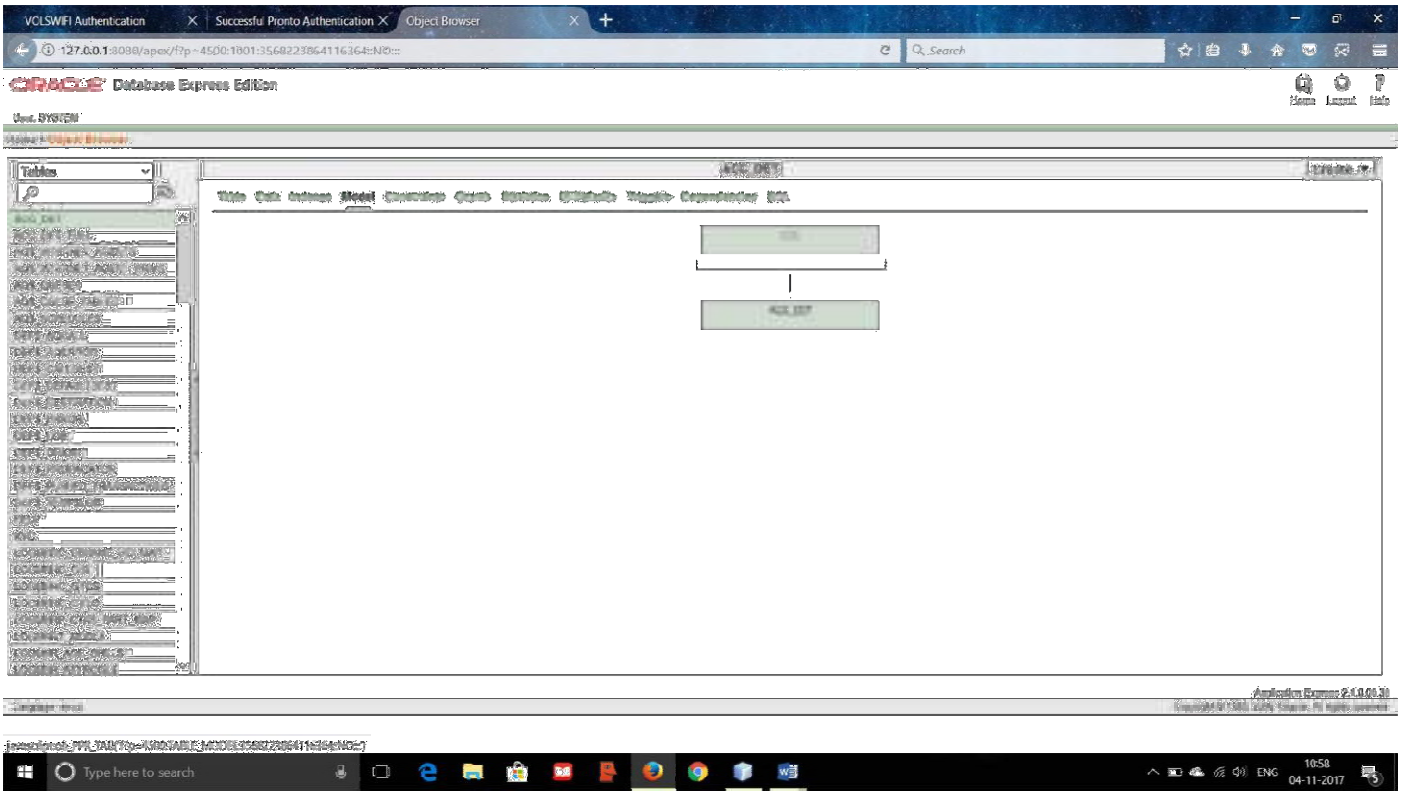

VOLSWIFI Authentication
Successful Pronto Authentication
Object Browser
127.0.0.1:8080/apex/f?p=4500:1001:35682238641163 64::NO::
Search
ORACLE Database Express Edition
Home
Logout
Help
User: SYSTEM
Tables
USER_LOG
Table
Data
Columns
Model
Constraints
Grants
Statistics
UI Defaults
Triggers
Dependencies
DDL
Download
Application Express 2.1.0.00.39
Type here to search
ENG
10:56
04-11-2017

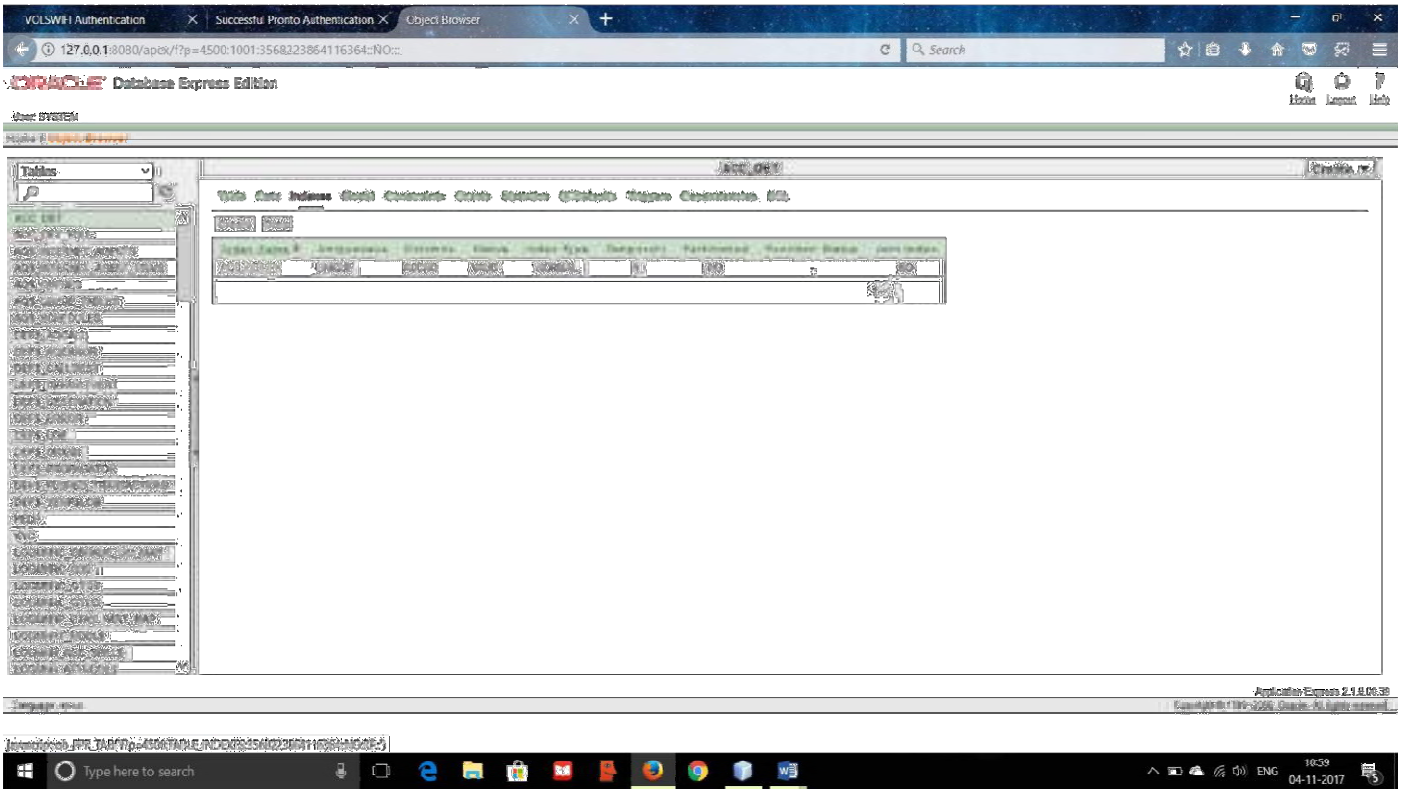

VOLSWIFI Authentication
Successful Pronto Authentication
Object Browser
Search
ORACLE Database Express Edition
Home
Logout
Help
Tables
Type here to search
ENG
10:58
04-11-2017

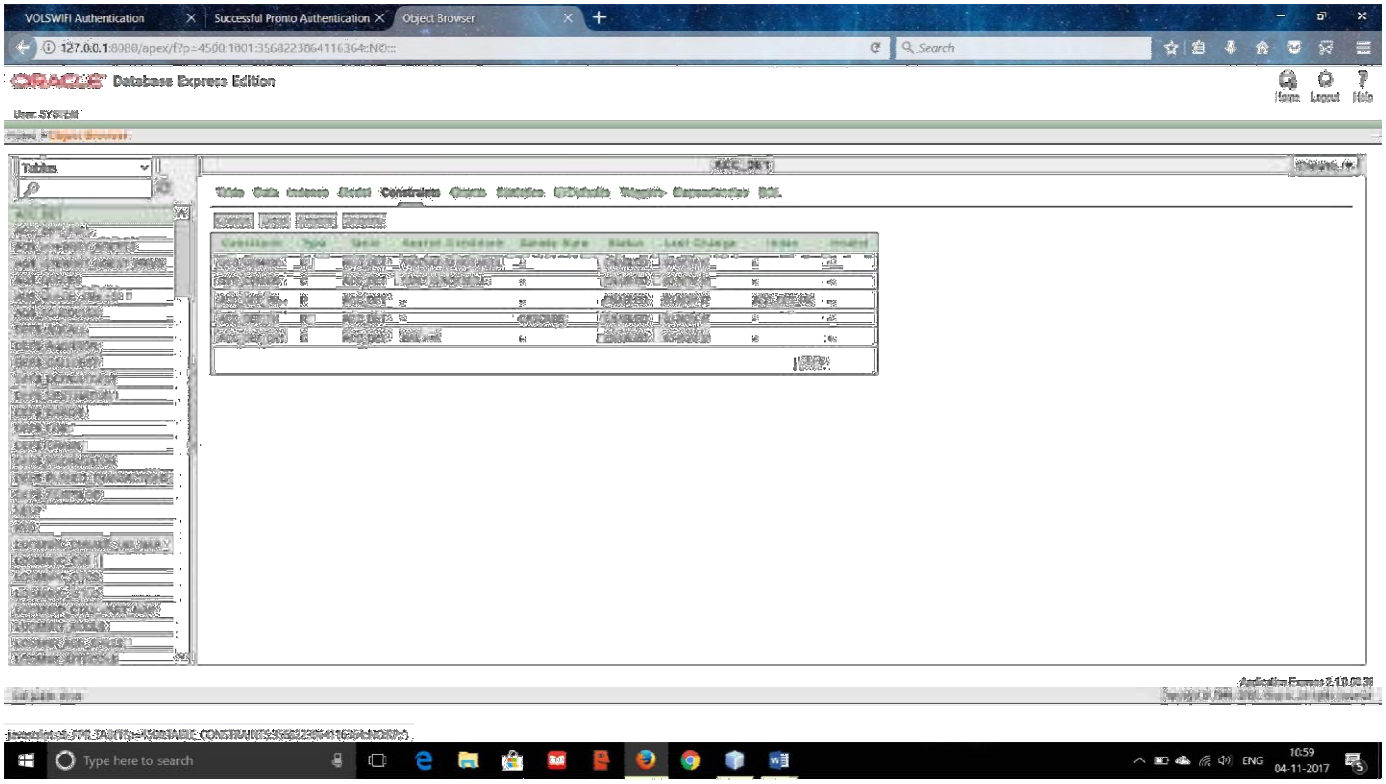

VOLSWIH Authentication
Successful Pronto Authentication
Object Browser
Search
ORACLE Database Express Edition
Home
Logout
Help
Tables
Type here to search
ENG
10:58
04-11-2017

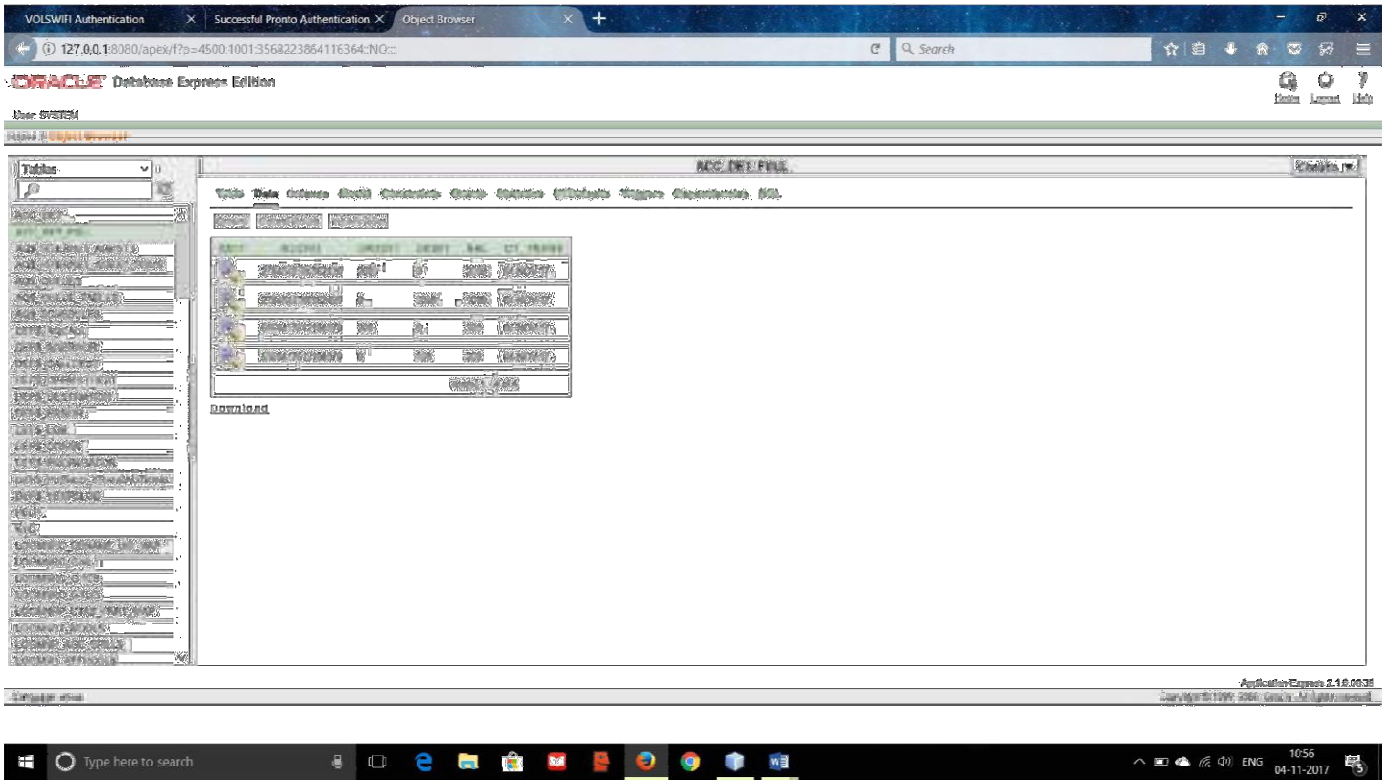

ORACLE Database Express Edition
Tables

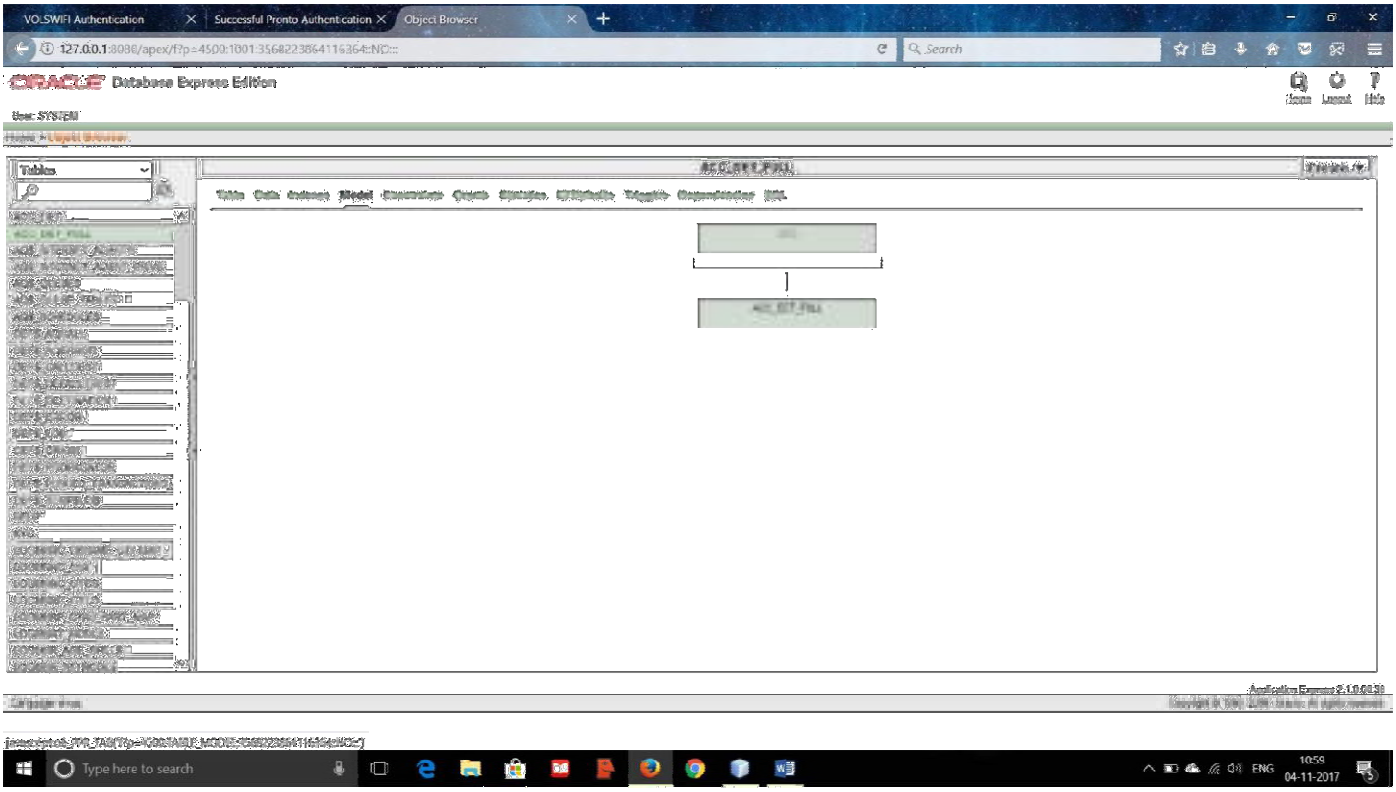

ORACLE Database Express Edition
Tables
Download

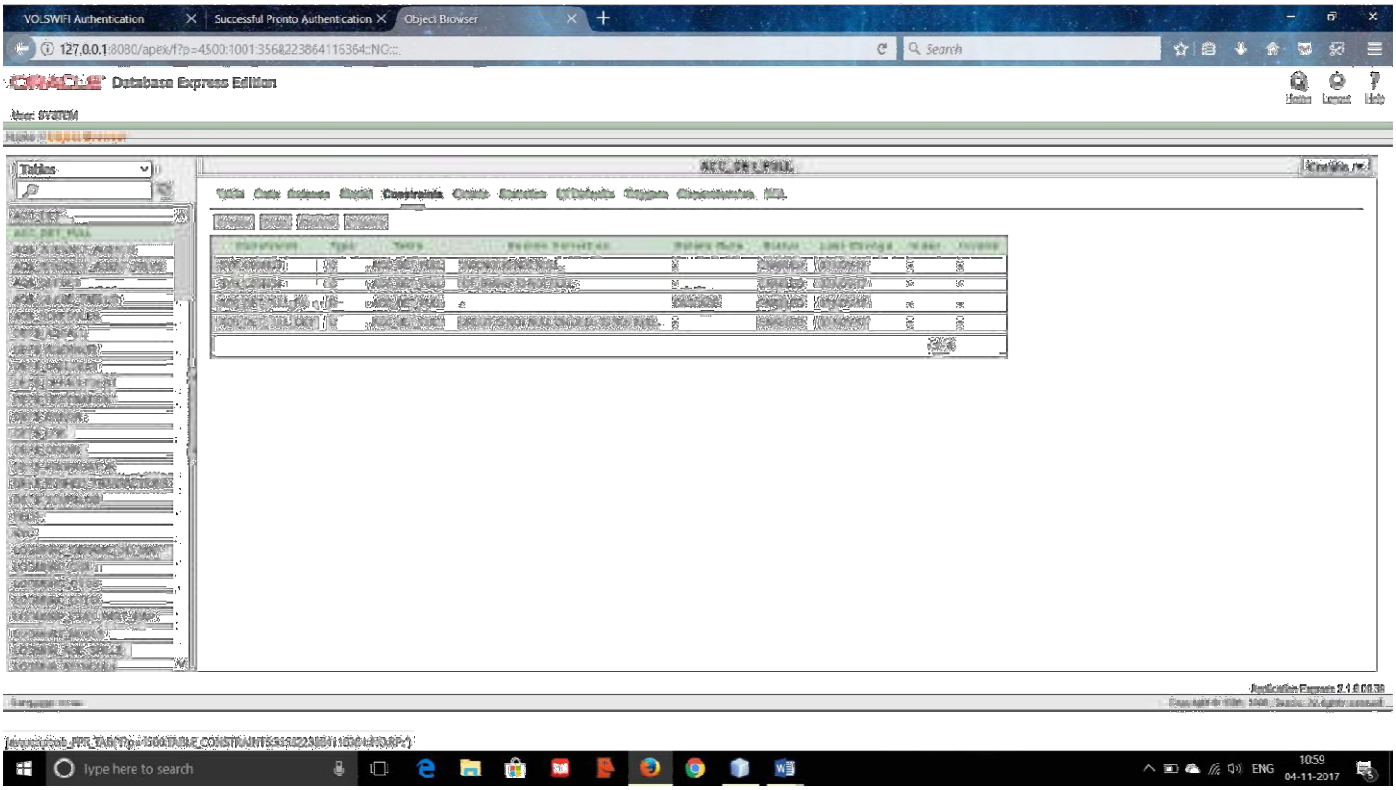

VCLSWIFI Authentication
Successful Pronto Authentication
Object Browser
Database Express Edition
Tables
Type here to search
ENG
10:58
04-11-2017


VCLSWIFI Authentication
Successful Pronto Authentication
Object Browser
Database Express Edition
Tables
Type here to search
ENG
10:59
04-11-2017


VOLSWIFI Authentication
Successful Pronto Authentication
Object Browser
127.0.0.1:8080/apex/f?p=4500:1001:35682238641163 64:NO:::
Search
ORACLE Database Express Edition
Home
Logout
Help
User: SYSTEM
Tables
Type here to search
ENG
10:59
04-11-2017


VOLSWIFI Authentication
Successful Pronto Authentication
Object Browser
127.0.0.1:8080/apex/f?p=4500:1001:35682238641163 64:NO:::
Search
ORACLE Database Express Edition
Home
Logout
Help
User: SYSTEM
Tables
Download
Type here to search
ENG
10:56
04-11-2017


VO:SWIFI Authentication
Successful Pronto Authentication
Object Browser
Database Express Edition
Tables
Type here to search
ENG
10:59
04-11-2017


VO:SWIFI Authentication
Successful Pronto Authentication
Object Browser
Database Express Edition
Tables
Type here to search
ENG
10:59
04-11-2017

CONCLUSION

The Internet of today has become an integral part of our everyday life and the proportion of users expecting to be able to manage their bank accounts anywhere anytime is constantly growing. As such, Internet banking has come to age as a crucial component of any financial institution's multi-channel strategy.
Traditionally, information about financial institutions, their customers, and financial transactions are considered most sensitive. Doing such business via a public network consequently introduces new challenges for security and trustworthiness. Basically, any Internet banking system must solve the issues of authentication, confidentiality, integrity, and non-repudiation. This means it must ensure that only qualified people can access an Internet banking account, that the information viewed remains private and cannot be modified by third parties, and that any transactions made are traceable and verifiable.

Internet banking systems must authenticate users before granting access to particular services. More precisely, the banking system must determine whether a user is, in fact, who he claims to be by asking the user to directly or indirectly prove knowledge of some sort of secret or credential. Based on the assumption that only an authentic user is able to do so, successful authentication eventually enables an authorized user to access his private information.

The proposed model can be employed in order to successfully validate the users during online transactions and also acts as a tool for withdrawing, depositing amounts and to change the login credentials.

REFERENCES

[1] Anti-Phishing Working Group. http://www.antiphishing.org

[2] JavaCard Platform Specification. Sun Microsystems. http://java.sun.com/products.javacard

[3] PKCS#15: Cryptographic Token Information Format Standard. RSA Laboratories.

[4] FINREAD Specification. FINREAD Consortium. (accepted as work item 1.17.34 for ISO/IEC JTCS1/SC17). http://www.finread.com

[5] PKCS#11: Cryptographic Token Interface Standard. RSA Laboratories.

[6] PC/SC Specification Version 2.0. http://www.pcscworkgroup.com/specifications/specdownload.php

[7] Secure user authentication over a communication network. UBS Patent, Europe: EP-87 458; US: 10/237,080

[8] Secure user and data authentication over a communication network. UBS Patent, Europe: EP-87 903; US: 10/235,936

[9] Richard E. Smith. Authentication: From Passwords to Public Keys. Addison Wesley, 2001.

[10] RSA SecureID Token. RSA Laboratories.

[11] M-Card smart. Migrosbank Switzerland. http://www.migrosbank.ch/de/Private/KartenZahlungsverkehr/MCardMCardSmart.htm.

[12] FinTS – Financial Transaction Services. http://www.hbci-zka.de/english/index.html

[13] http://www.pcworld.com/news/article/0,aid,118757,00.asp

[14] http://www.microdasys.com/

[15] Bruce Schneier. Two-Factor Authentication: Too Little, Too Late. Communications of the ACM vol 48, no.4, April 2005.