ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 6, Special Issue 3, November 2017

Secured Multilevel Authentication System for Secured Financial Transactions

K.Venkatraman[1], G Maria Kalavathy[2]

Research Scholar, Anna University, Chennai, India[1]

Professor, St.Joseph's College of Engineering, Chennai, India[2]

ABSTRACT: As part of the security within distributed systems, various services and resources need protection from unauthorized use. Remote authentication is the most commonly used method to determine the identity of a remote client. This paper investigates a systematic approach for authenticating clients by three factors, namely password, smart card, and biometrics. A generic and secure framework is proposed to upgrade two-factor authentication to three-factor authentication. The conversion not only significantly improves the information assurance at low cost but also protects client privacy in distributed systems. In addition, our framework retains several practice-friendly properties of the underlying two-factor authentication, which we believe is of independent interest. The main implementation of the Project is to get the Finger Print, RFID and the PIN from the User for the Authentication. If the Finger Print is same but not so clear then the Main Server will generate the Token number to the User's Mobile number as OTP. This generated OTP would be given using Key Pad Matrix provided to the user during Account Registration. So the Server will be verifying User's Finger Print, RFID card, PIN number, OTP via Key Pad Matrix and the ID of Key Pad Matrix. This will definitely ensure proper security of the user.

I. INTRODUCTION

In a distributed system, various resources are distributed in the form of network services provided and managed by servers. The five authentication factors used are
RFID Card,PIN,Fingerprint,OTP,,Keypad with Keypad ID.Most early authentication mechanisms are solely based on password. While such protocols are relatively easy to implement, passwords (human generated passwords in particular) have many vulnerabilities. As an example, human generated and memorable passwords are usually short strings of characters and (sometimes) poorly selected. By exploiting these vulnerabilities, simple dictionary attacks can crack passwords in a short time. Due to these concerns, hardware authentication tokens are introduced to strengthen the security in user authentication. RFID card-based password authentication provides two-factor authentication, which requires the client to have a valid smart card and a correct password. While it provides stronger security guarantees than password authentication, it could also fail if both authentication factors are compromised (e.g., if an attacker has successfully obtained the password and the data in the smart card). Another existing authentication mechanism is biometric authentication where users are identified by their measurable human characteristics, such as fingerprint can be easily obtained without the awareness of the owner. In this case OTP and Keypad ID further improve the system's assurance. This motivates the five-factor authentication, which incorporates the advantages of the authentication based on, RFID card, PIN, Fingerprint, OTP and Keypad ID

1.1 PROBLEM DEFINITION

In banking system the Personal Identification Number provided by the administration can be changed by the customer. Customers usually changes the PIN number by easily remember one which can be hacked easily so, it will not be secure. Introducing the Fingerprint reader to perform transaction in banks also do not provide a completely secure way to authenticate a user although together with the ATM card and PIN it can be quite good indeed. The protection that only a fingerprint would give is not sufficient because the fingerprint of the person can be easily traced from wherever the trace is available.

II. LITERATURE REVIEW

2.1.1 Enhanced Biometrics-based Remote User Authentication Scheme Using Smart Cards

Secure and efficient authentication scheme has been a very important issue with the development of networking technologies. Li and Hwang proposed an efficient biometrics-based remote user authentication scheme using smart cards. However, recently, Li et al. pointed out that their scheme is vulnerable to the man-in-the-middle attack, and does not provide proper authentications, and Li et al. proposed an improved biometrics-based action scheme. These schemes are vulnerable to various attacks even if the schemes are based on tamper-resistant technologies. Tamper-resistant technologies have been developed with the various applications of smart cards. Therefore, we will assume that the user could use the tamper-resistant smart card in this paper. First of all, this paper shows that Li et al.'s scheme is vulnerable to the replay attack and has a weakness to the password changing scheme even if it is assumed that the scheme could use the tamper-resistant smart cards. Furthermore, we propose an enhanced authentication scheme to solve the security flaws in the two schemes.

2.1.2 A Tutorial on Fingerprint Recognition

This tutorial introduces fingerprint recognition systems and their main components: sensing, feature extraction and matching. The basic technologies are surveyed and some state-of-the-art algorithms are discussed. Due to the extent of this topic it is not possible to provide here all the details and to cover a number of interesting issues such as classification, indexing and multimodal systems. Interested readers can find in a complete and comprehensive guide to fingerprint recognition.

2.1.3 Biometric Authentication And Authorization Infrastructure

Today, with the rapid growth of internet and the introduction of Web 2.0, the rules the internet is based on are changing. The old model where the providers and the consumers of web services were two separate entities is being replaced by the new possibilities of web technology, which allow anybody who is online to be both provider and consumer. These new opportunities make the internet attractive to an increased number of companies providing services to a large number of users.

This new trend has to be put in correlation with the different security policies that companies (web providers) follow and with the influence that these policies have upon users. Seen from the side of the web providers, good security policies establish who is allowed to use a system and in which circumstances they are allowed to use it (Stein 2003). On the side of the users, the different security policies are reflected in an increased number of credentials, mostly in the form of a username / password combination. This large number of passwords leads to users tending to choose simple combinations or to use the same password for more services. Against this practice, some web service providers protect themselves by checking passwords against common dictionary entries or by implementing special rules which require that passwords should be long, with small and capitalletters, numbers and special characters. With these restrictions, passwords are often forgotten or written down, which brings other risks and security leaks.

2.1.4 Foiling the Cracker

With the rapid burgeoning of national and international networks, the question of system security has become one of growing importance. High speed inter-machine communication and even higher speed computational processors have mad the threats of system ‘‘crackers,’’ data theft, data corruption very real. This paper outlines some of the problems of current password security by demonstrating the ease by which individual accounts may be broken. Various techniques used by crackers are outlined, and finally one solution to this point of system vulnerability, a proactive password checker, is proposed.

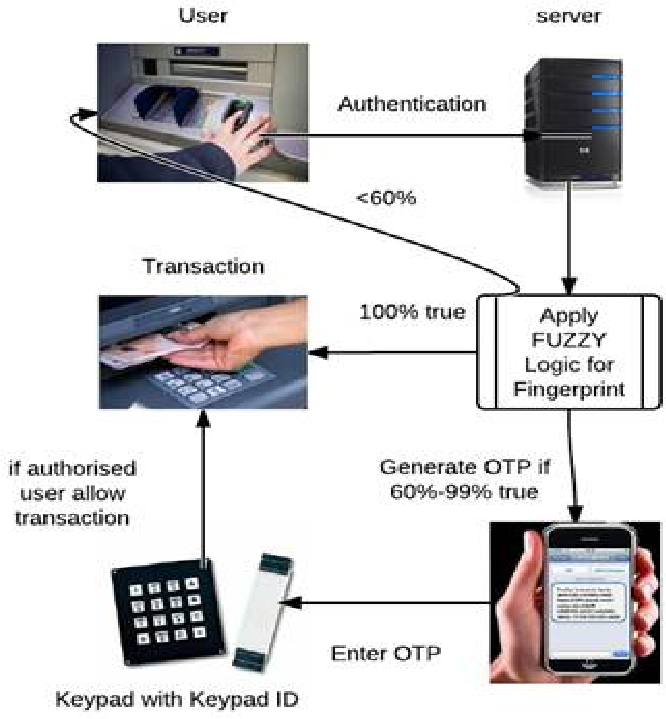
2.1.5 Fingerprint Based Remote User Authentication Scheme Using smart cards.

An authentication system, which does not require a password tale to authenticate its users, is proposed. By removing a password table, and introducing smart card and fingerprint verification, the scheme can be more secure and reliable. In addition, the scheme can withstand message replaying attack and impersonation. This paper is based on the ElGamal public key cryptosystem, also does not require a system to maintain a password table, but to keep only two secret keys secret. By adding one more secret key than Hwang and Li, our scheme can withstand impersonation. In addition, to enhance and strengthen our system, we store public elements used in our scheme on a smart card and each user can gain access to his own smart card by verifying himself using his fingerprint. Accordingly each user can participate in our scheme using only his own smart card and fingerprint.

The fingerprint verification method is based on minutia extraction and matching. Whenever a fingerprint is input, a different map of minutia is made, so we can generate a one-time random number for the ElGamal public key cryptosystem using that map. As described, our scheme requires a system to authenticate each user by each user's knowledge, possession and biometrics, and this feature makes our scheme more reliable.

III. PROPOSED SYSTEM

Every User is provided with RFID Card for the initial Authentication Scheme, and then the user will have to give the PIN number that is provided during the Registration. Then the user will be allowed to give his / her Finger Print to the main server. If the Finger Print is exactly matched, then the user is allowed for the transaction. If the Finger Print does not match exactly with the registered Finger Print then the Server sends One Time Password as SMS Alert to the User's Mobile Number. This One Time Password which is generated as SMS is given by the User to the main server for authentication using the Keypad provided to the user after registration. If the OTP matches exactly with the OTP generated in the server then the user will be allowed for transaction.


User
server
Authentication
<60%
Transaction
100% true
Apply FUZZY Logic for Fingerprint
if authorised user allow transaction
Generate OTP if 60%-99% true
Enter OTP
Keypad with Keypad ID

.

Fig: 3.3.1.1 System Architecture

3.4 IMPLEMENTATION

MODULE DESCRIPTION

- Registration.
- Login and Authentication.
- One Time Password (OTP) generation.
- Transaction.

3.4.1.1 Registration

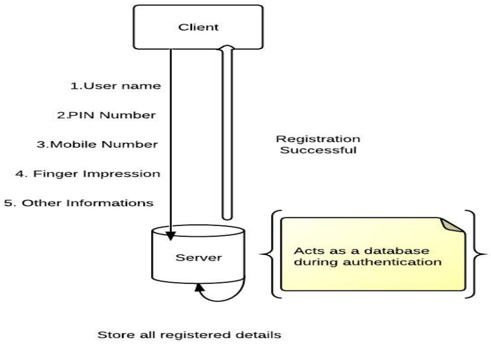


Fig 3.4.1.1 User Registration

Every user must have to register the Server by providing the basic information about them so that they will be allowed to perform the transaction in bank,

- Name
- Phone Numbers
- E mail ID
- Address
- Finger impression & other particulars

required to complete the registration process.

Once the user completes his/her Registration then the user will be provided with

- RFID card
- PIN number
- Keypad along with Keypad ID

3.4.1.2 Login and Authentication

The client first inserts the RFID card into a card reader which will extract the data. After that, the client enters the PIN and his/her fingerprint data.

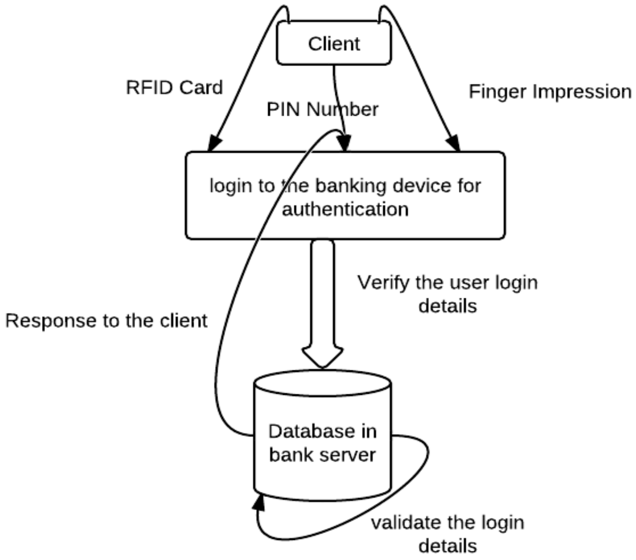

Client
RFID Card
PIN Number
Finger Impression
login to the banking device for authentication
Verify the user login details
Response to the client
Database in bank server
validate the login details

Fig 3.4.1.2 Login and Authentication

A fingerprint scanner is used for extraction at this phase. The login procedure is as follows

- The PIN that the user enter should match with already existing one in the database otherwise the user cannot proceed further.
- Once the PIN matches perfectly the user has to give his/her fingerprint on the fingerprint scanner. Fuzzy logic is applied as soon as the fingerprint is obtained on the fingerprint scanner. If the fingerprint matches exactly (100%) with existing fingerprint in the database then the user will be allowed for transaction.
- If the obtained fingerprint matches less than 60% with the existing fingerprint in the database, transaction cannot be performed.

3.4.1.3 One Time Password (OTP) generation

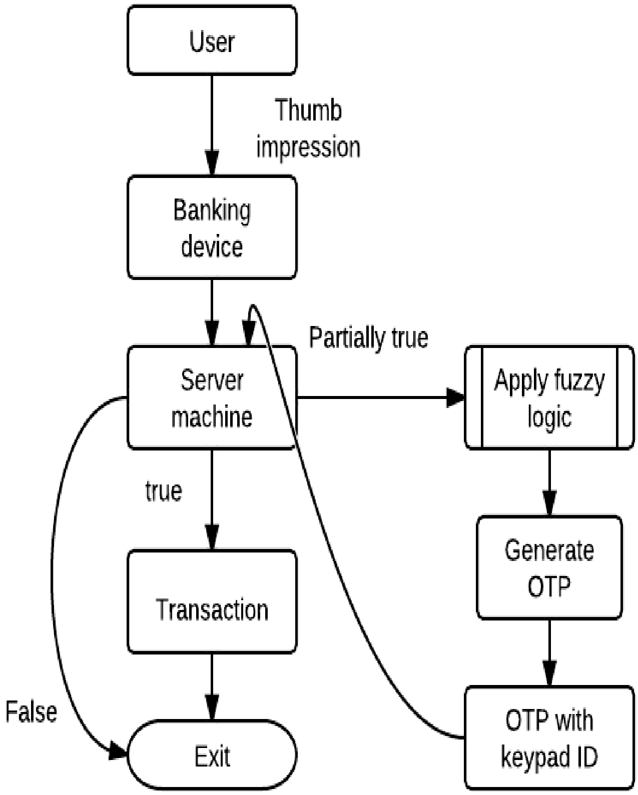


Fig 3.4.1.3 One Time Password process flow

If the fuzzy logic says fingerprint of the user is partially true (60%-99%) then OTP will be generated automatically and sent to the real user’s mobile using “RSA” algorithm. The user must be an authenticated person to receive OTP via mobile. The generated OTP must be entered using the keypad which is already updated with the keypad ID. The user is allowed for transaction if the OTP matches perfectly.

3.4.1.4 Transaction

Once all the authentication process gets completed the system displays main menu to the user to proceed with transaction. The user can then perform the normal transaction.

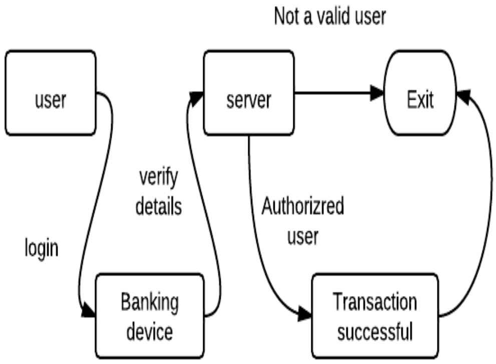
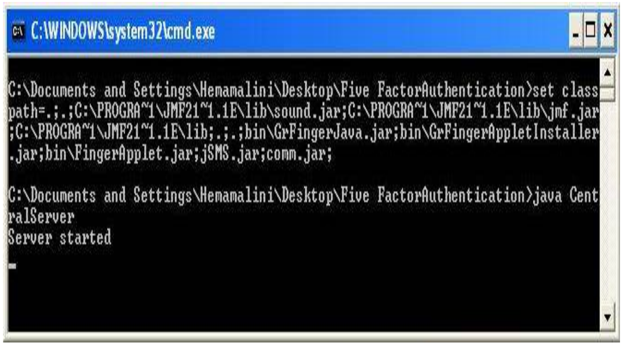


Fig 3.4.1.4 Transaction

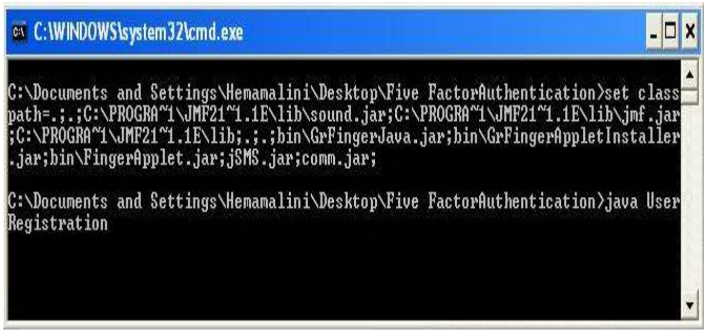
4. RESULTS AND DISCUSSION



```
C:\Documents and Settings\Hemamalini\Desktop\Five FactorAuthentication>set class
path=.;.;C:\PROGRA~1\JMF21~1.1E\lib\sound.jar;C:\PROGRA~1\JMF21~1.1E\lib\jmf.jar
;C:\PROGRA~1\JMF21~1.1E\lib;.;.;bin\GrFingerJava.jar;bin\GrFingerAppletInstaller
.jar;bin\FingerApplet.jar;jSMS.jar;comm.jar;

C:\Documents and Settings\Hemamalini\Desktop\Five FactorAuthentication>java Cent
ralServer
Server started
_
```

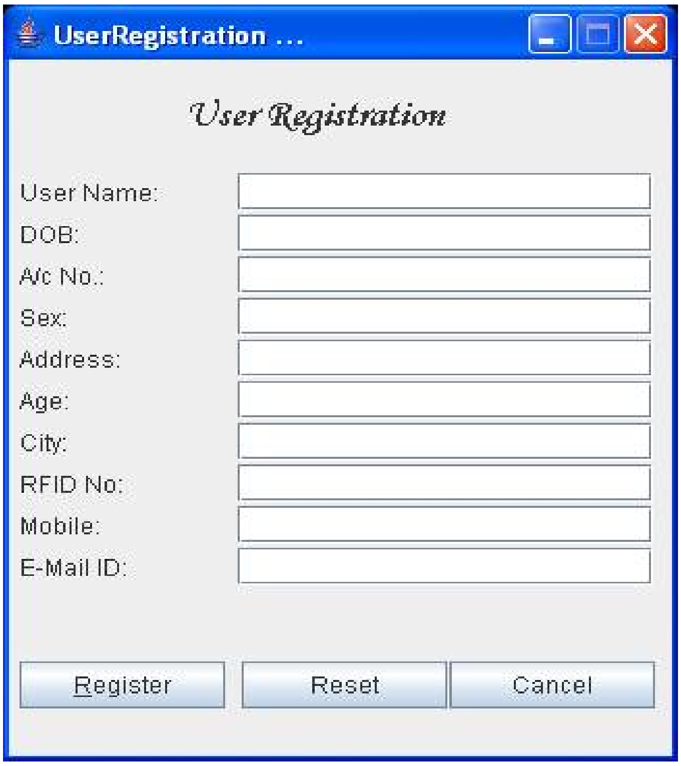
4.2.1 Server started



```
C:\Documents and Settings\Hemamalini\Desktop\Five FactorAuthentication>set class
path=.;.;C:\PROGRA~1\JMF21~1.1E\lib\sound.jar;C:\PROGRA~1\JMF21~1.1E\lib\jmf.jar
;C:\PROGRA~1\JMF21~1.1E\lib;.;.;bin\GrFingerJava.jar;bin\GrFingerAppletInstaller
.jar;bin\FingerApplet.jar;jSMS.jar;comm.jar;

C:\Documents and Settings\Hemamalini\Desktop\Five FactorAuthentication>java User
Registration
```

4.2.2 User Registration

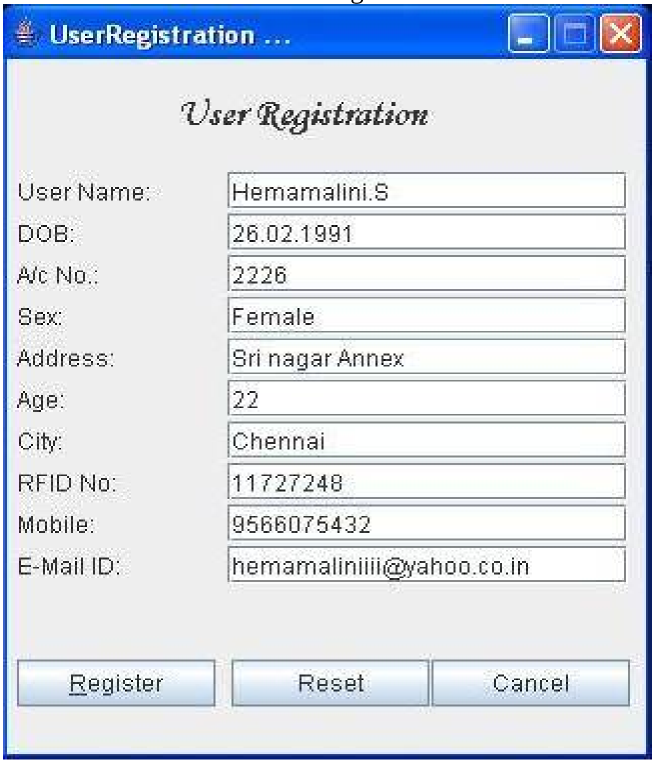


UserRegistration ...

User Registration

User Name:	
DOB:	
A/c No.:	
Sex:	
Address:	
Age:	
City:	
RFID No:	
Mobile:	
E-Mail ID:	

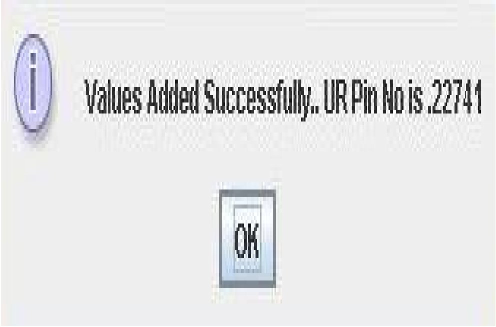
4.2.3 User Registration



UserRegistration ...

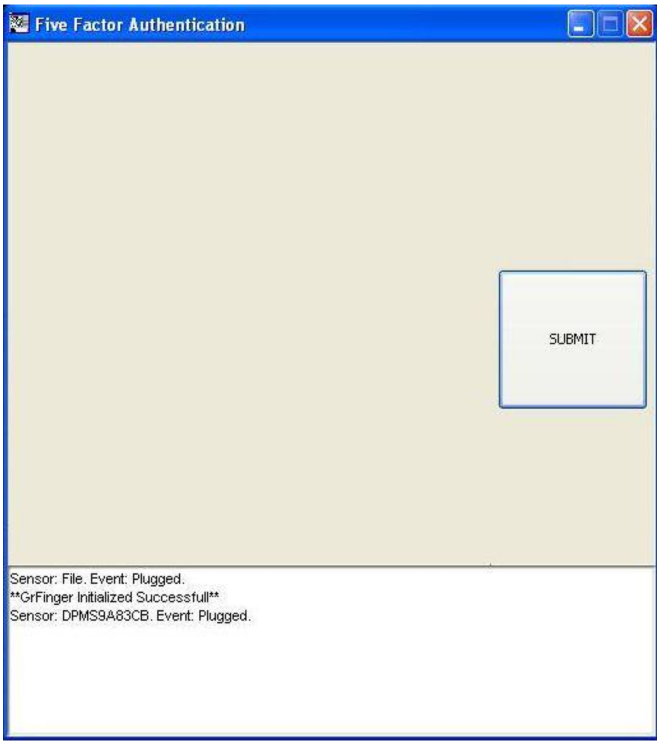
User Registration

User Name:	Hemamalini.S
DOB:	26.02.1991
A/c No.:	2226
Sex:	Female
Address:	Sri nagar Annex
Age:	22
City:	Chennai
RFID No:	11727248
Mobile:	9566075432
E-Mail ID:	hemamaliniiii@yahoo.co.in



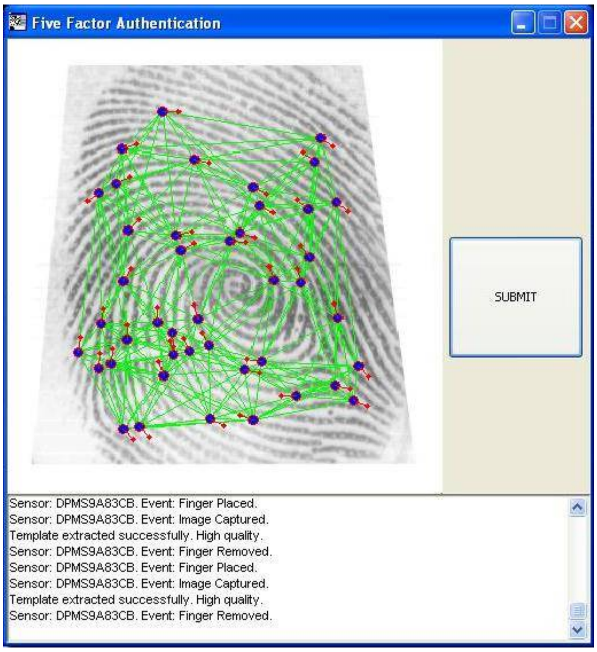
Values Added Successfully.. UR Pin No is 22741

4.2.4 Storing User details in Database and PIN Number Generation



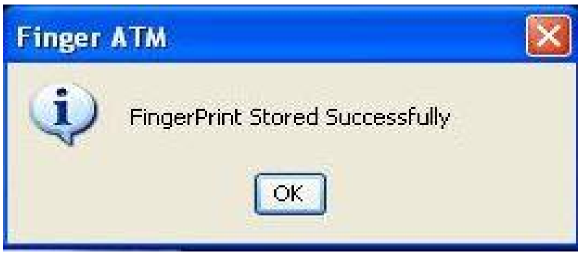
```
Sensor: File. Event: Plugged.
**GrFinger Initialized Successfull**
Sensor: DPMS9A83CB. Event: Plugged.
```

4.2.5 Fingerprint Initialization



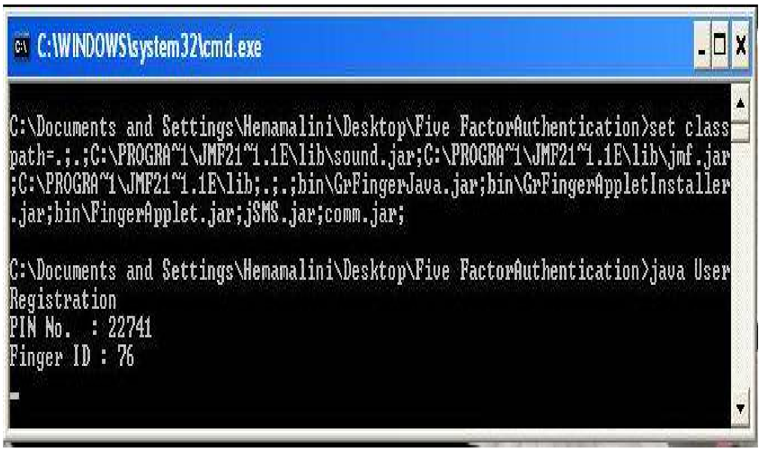
```
Sensor: DPMS9A83CB. Event: Finger Placed.
Sensor: DPMS9A83CB. Event: Image Captured.
Template extracted successfully. High quality.
Sensor: DPMS9A83CB. Event: Finger Removed.
Sensor: DPMS9A83CB. Event: Finger Placed.
Sensor: DPMS9A83CB. Event: Image Captured.
Template extracted successfully. High quality.
Sensor: DPMS9A83CB. Event: Finger Removed.
```

4.2.6 Fingerprint Image Capturing



FingerPrint Stored Successfully

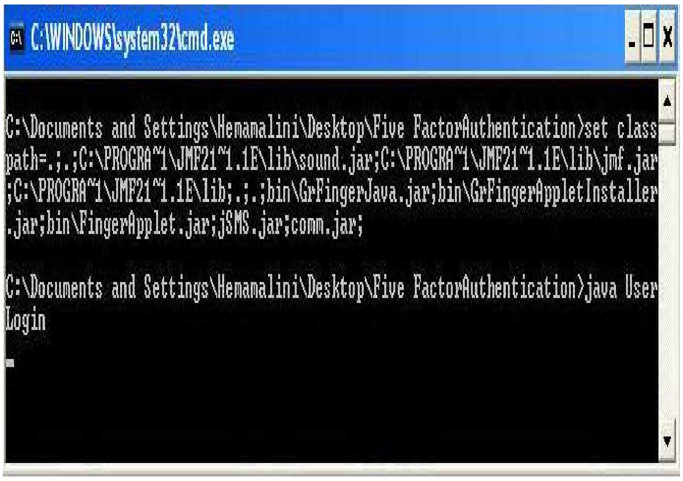
4.2.7 Updating Database with User Fingerprint



```
C:\Documents and Settings\Hemamalini\Desktop\Five FactorAuthentication>set class
path=.;.;C:\PROGRA~1\JMF21~1.1E\lib\sound.jar;C:\PROGRA~1\JMF21~1.1E\lib\jmf.jar
;C:\PROGRA~1\JMF21~1.1E\lib;.;.;bin\GrFingerJava.jar;bin\GrFingerAppletInstaller
.jar;bin\FingerApplet.jar;jSMS.jar;comm.jar;

C:\Documents and Settings\Hemamalini\Desktop\Five FactorAuthentication>java User
Registration
PIN No.  : 22741
Finger ID : 76
```

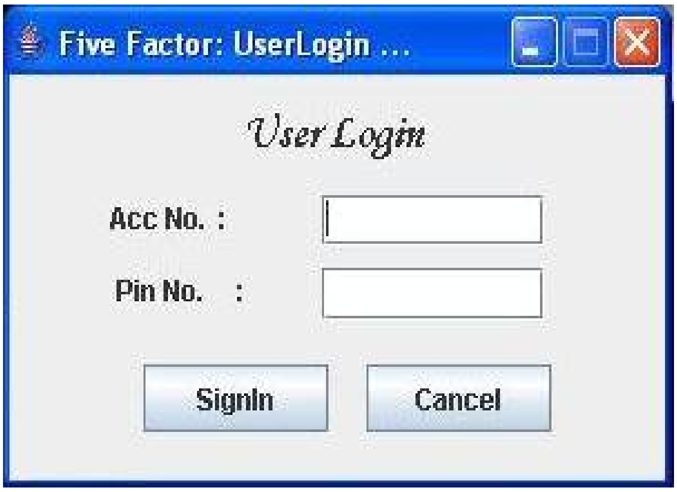
4.2.8 Registration information in server



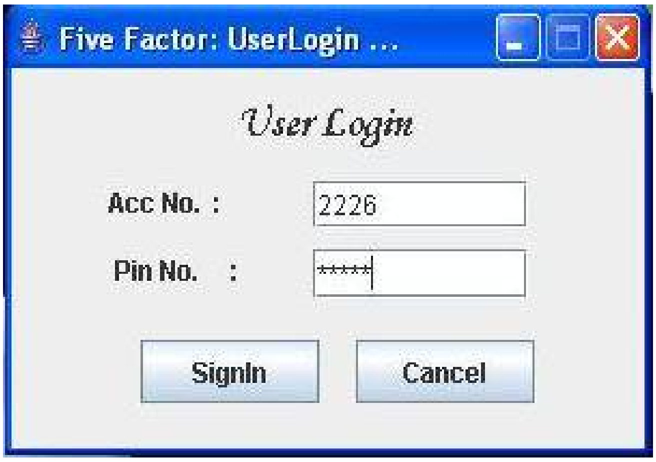
```
C:\Documents and Settings\Hemamalini\Desktop\Five FactorAuthentication>set class
path=.;.;C:\PROGRA~1\JMF21~1.1E\lib\sound.jar;C:\PROGRA~1\JMF21~1.1E\lib\jmf.jar
;C:\PROGRA~1\JMF21~1.1E\lib;.;.;bin\GrFingerJava.jar;bin\GrFingerAppletInstaller
.jar;bin\FingerApplet.jar;jSMS.jar;comm.jar;

C:\Documents and Settings\Hemamalini\Desktop\Five FactorAuthentication>java User
Login
```

4.2.9 User Login



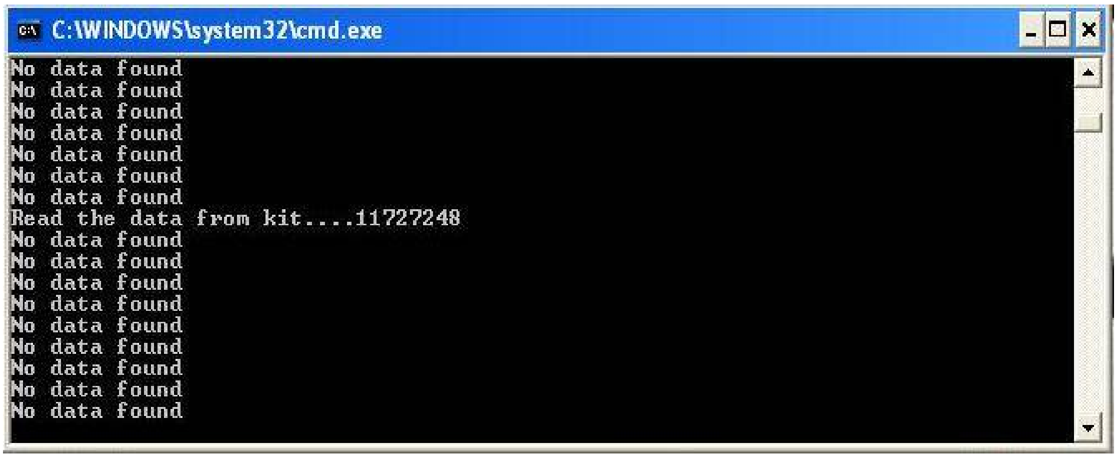
4.2.10 User Login Form



Acc No. : 2226

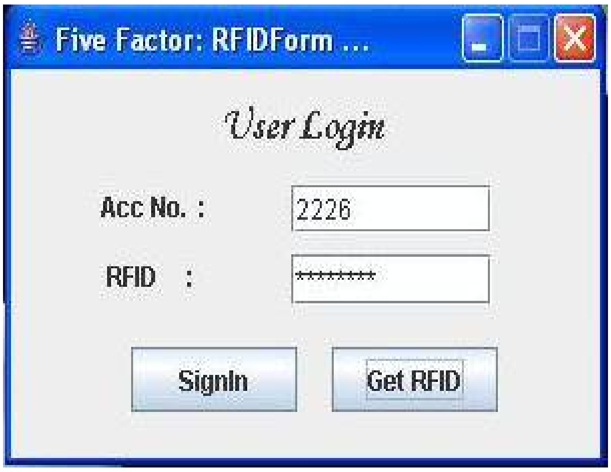
Pin No. : *****

4.2.11 Read the PIN number



```
No data found
No data found
No data found
No data found
No data found
No data found
No data found
Read the data from kit....11727248
No data found
No data found
No data found
No data found
No data found
No data found
No data found
No data found
No data found
```

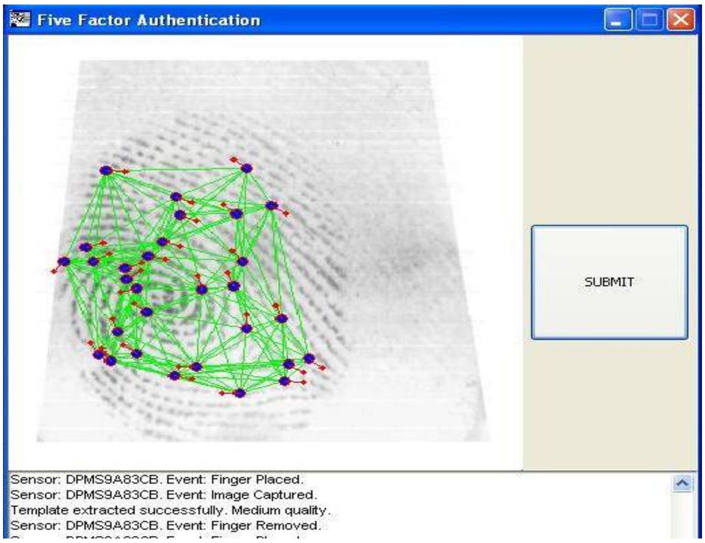
4.2.12 Read the RFID number using kit



Acc No. : 2226

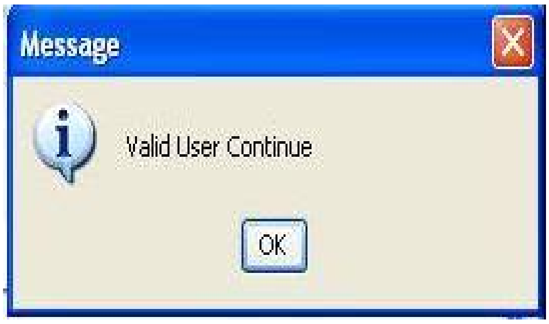
RFID : ********

4.2.13 Get the RFID number



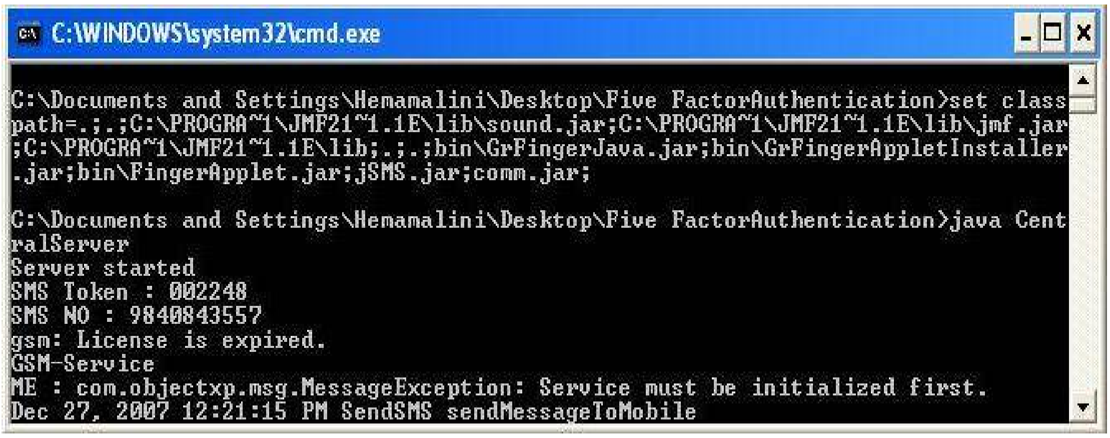
```
Sensor: DPMS9A83CB. Event: Finger Placed.
Sensor: DPMS9A83CB. Event: Image Captured.
Template extracted successfully. Medium quality.
Sensor: DPMS9A83CB. Event: Finger Removed.
```

4.2.14 Fingerprint submission



Valid User Continue

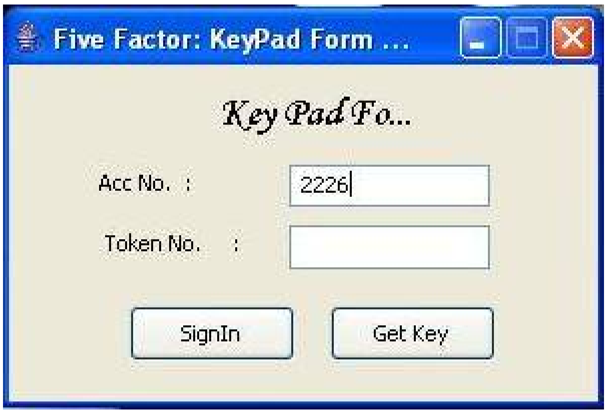
4.2.15 Authentication for Transaction



```
C:\Documents and Settings\Hemamalini\Desktop\Five FactorAuthentication>set class
path=.;.;C:\PROGRA~1\JMF21~1.1E\lib\sound.jar;C:\PROGRA~1\JMF21~1.1E\lib\jmf.jar
;C:\PROGRA~1\JMF21~1.1E\lib;.;.;bin\GrFingerJava.jar;bin\GrFingerAppletInstaller
.jar;bin\FingerApplet.jar;jSMS.jar;comm.jar;

C:\Documents and Settings\Hemamalini\Desktop\Five FactorAuthentication>java Cent
ralServer
Server started
SMS Token : 002248
SMS NO : 9840843557
gsm: License is expired.
GSM-Service
ME : com.objectxp.msg.MessageException: Service must be initialized first.
Dec 27, 2007 12:21:15 PM SendSMS sendMessageToMobile
```

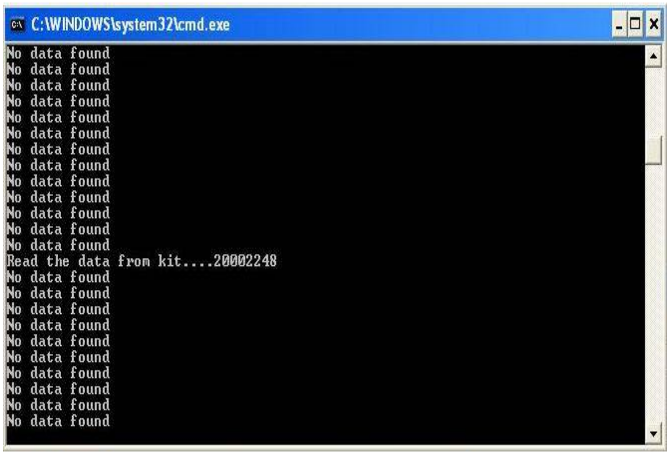
4.2.16 Token number generated from server



Acc No. : 2226

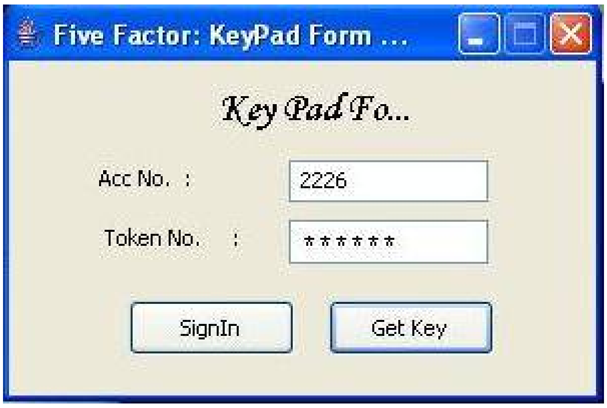
Token No. :

4.2.17 Keypad Form



```
No data found
No data found
No data found
No data found
No data found
No data found
No data found
No data found
No data found
No data found
No data found
No data found
No data found
Read the data from kit....20002248
No data found
No data found
No data found
No data found
No data found
No data found
No data found
No data found
No data found
No data found
```

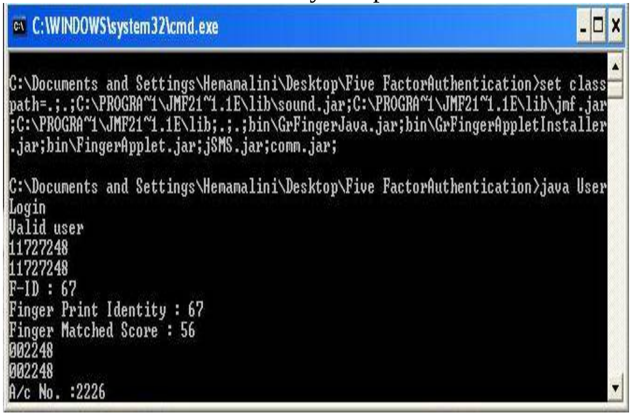
4.2.18 Token number reading



Acc No. : 2226

Token No. : ******

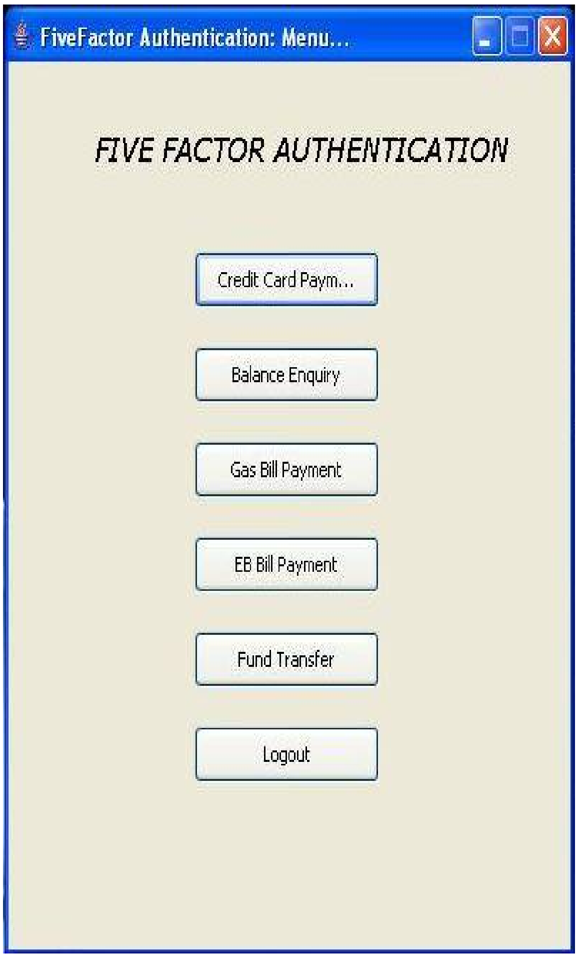
4.2.19 Key reception



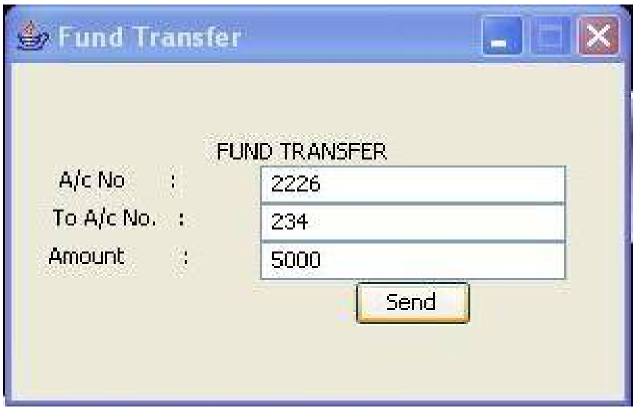
```
C:\Documents and Settings\Hemamalini\Desktop\Five FactorAuthentication>set class
path=.;.;C:\PROGRA~1\JMF21~1.1E\lib\sound.jar;C:\PROGRA~1\JMF21~1.1E\lib\jmf.jar
;C:\PROGRA~1\JMF21~1.1E\lib;.;.;bin\GrFingerJava.jar;bin\GrFingerAppletInstaller
.jar;bin\FingerApplet.jar;jSMS.jar;comm.jar;

C:\Documents and Settings\Hemamalini\Desktop\Five FactorAuthentication>java User
Login
Valid user
11727248
11727248
F-ID : 67
Finger Print Identity : 67
Finger Matched Score : 56
002248
002248
A/c No. :2226
```

4.2.20 Database in the server

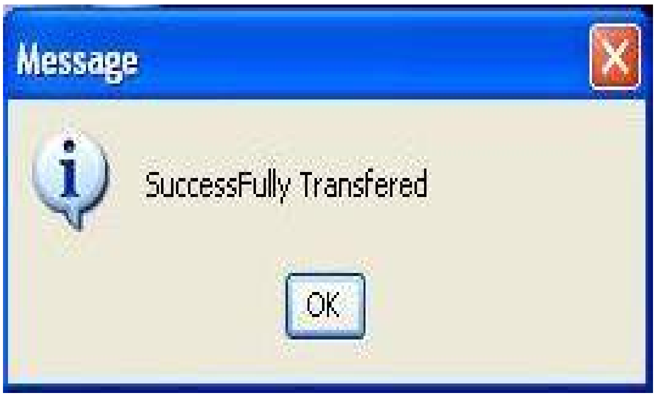


4.2.21 ATM Menu



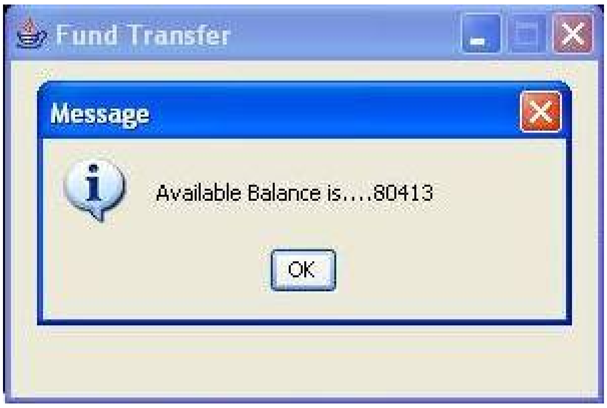
A/c No : 2226
To A/c No. : 234
Amount : 5000

4.2.22 Fund Transfer



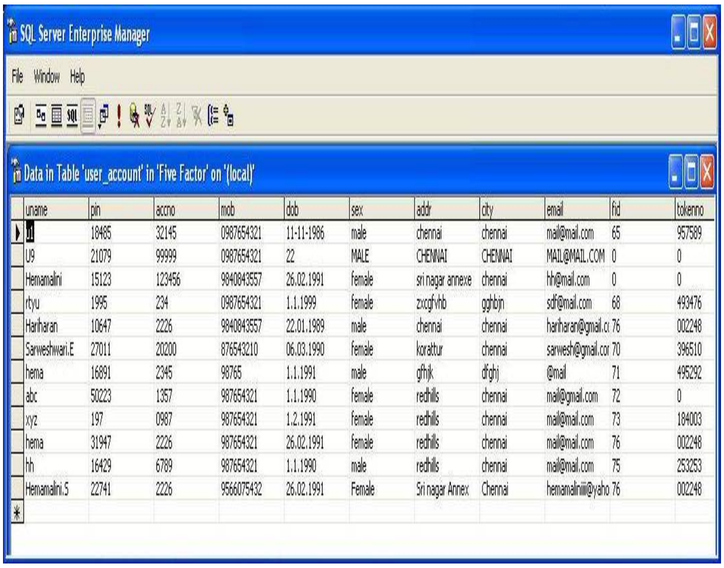
SuccessFully Transfered

42.2.23 Successful amount Transaction



Available Balance is....80413

4.2.24 Balance Check



Data in Table 'user_account' in 'Five Factor' on '(local)'

uname	pin	accno	mob	dob	sex	addr	city	email	fid	tokenno
u1	18485	32145	0987654321	11-11-1986	male	chennai	chennai	mail@mail.com	65	957589
U9	21079	99999	0987654321	22	MALE	CHENNAI	CHENNAI	MAIL@MAIL.COM	0	0
Hemamalini	15123	123456	9840843557	26.02.1991	female	sri nagar annexe	chennai	hh@mail.com	0	0
rtyu	1995	234	0987654321	1.1.1999	female	zxcgfvhb	gghbjn	sdf@mail.com	68	493476
Hariharan	10647	2226	9840843557	22.01.1989	male	chennai	chennai	hariharan@gmail.c	76	002248
Sarweshwari.E	27011	20200	876543210	06.03.1990	female	korattur	chennai	sarwesh@gmail.cor	70	396510
hema	16891	2345	98765	1.1.1991	male	gfhjk	dfghj	@mail	71	495292
abc	50223	1357	987654321	1.1.1990	female	redhills	chennai	mail@gmail.com	72	0
xyz	197	0987	987654321	1.2.1991	female	redhills	chennai	mail@mail.com	73	184003
hema	31947	2226	987654321	26.02.1991	female	redhills	chennai	mail@mail.com	76	002248
hh	16429	6789	987654321	1.1.1990	male	redhills	chennai	mail@mail.com	75	253253
Hemamalini.S	22741	2226	9566075432	26.02.1991	Female	Sri nagar Annex	Chennai	hemamaliniiii@yaho	76	002248

4.2.25 Five Factor Authentication Database

V. CONCLUSION

Preserving security and privacy is a challenging issue in distributed systems. This project makes a step forward in solving this issue by proposing a fuzzy implementation of biometrics with five-factor authentication to protect services and resources from unauthorized use. The authentication is based on password, RFID card, OTP, fingerprint and keypad ID. Our work not only demonstrates how to obtain secure five-factor authentication from three-factor authentication, but also addresses issues of biometric authentication in distributed systems (e.g., client privacy). The analysis shows that the work satisfies all security requirements on five-factor authentication and has several other practice-friendly features

REFERENCES

[1] Argav-Spantzel.A, Squicciarini.A.C, Bertino.E, Modi.S, Young.M, and Elliott.S.J, “Privacy Preserving Multi-Factor Authentication with Biometrics,” J. Computer Security, vol. 15, no. 5, pp. 529-560, 2007.

[2] Davide Maltoni “A Tutorial on Fingerprint Recognition,” Lecture notes in Computer Science,2005,Volume 3161/2005

[3] Dawson.E, Lopez.J, Montenegro and Okamoto.E “Biometric Authentication And Authorization Infrastructures” ITRE- 2003

[4] Dodis.Y, Reyzin.L, and Smith.A, “Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data,” Proc. Int’l Conf. Theory and Applications of Cryptographic Techniques (Eurocrypt), pp. 523-540, 2004.

[5] Fan C.-I. and Lin Y.-H., “Provably Secure Remote Truly Three- Factor Authentication scheme with Privacy Protection on Bio- metrics,” IEEE Trans. Information Forensics and Security, vol. 4, no. 4, pp. 933-945, Dec. 2009.

[6] Klein.D.V “Foiling the Cracker” Computer Standards Interfaces, vol. 29, no. 1, pp. 82-85, Jan. 2007.

[7] Lee.J.K, Ryu.S.R and Yoo K.Y, “Fingerprint Based Remote User Authentication Scheme Using Smart Cards” Electronics Letters, vol. 38, no. 12, pp. 554-555, June 2002.

[8] Lee.Y and Kwon.T, “An improved Fingerprint-Based Remote User Authentication Scheme Using Smart Cards,” Proc. Int’l Conf. Computational Science and Its Applications (ICCSA), 2006.

[9] Ll-soo jeon, Hyun-Sung Kim and Myung-Sik Kim “Enhanced Biometrics-based Remote User Authentication Scheme Using Smart Cards,” Scholarpedia, vol. 5, no. 1, p. 9201,2010

[10] Xinyi Huang, Yang Xiang, Jianying Zhou and Robert Deng.H, “A Generic framework for three factor authentication: Preserving security and privacy in distributed systems” IEEE Trans. Parallel and distributed system Vol. 22, no. 8, pp. 1390-1397, August 2011.