A Security Framework on SIM Based Authentication Technique for Mobile Financial Services

Prof. Kirti B. Ahirrao
Computer Department
Ramrao Adik Institute of Technology,
Navi-Mumbai, India

Prof. Vimla Jethani
Computer Department
Ramrao Adik Institute of Technology,
Navi-Mumbai, India

Abstract* - *Various value added services on mobile phones had been widely used all across the globe and have even been able to influence the adoption of mobile phones in many countries. However, there has been a high degree of reluctance among the mobile users in adapting to mobile financial services (MFS). MFS is a broad range of financial activities that consumers engage in or access using their mobile phones Studies has shown the lack of trust about security and privacy of data to be a major roadblock for adoption of MFS. Given the fact that there are multiple entities including the bank, telecom operator, non-banking financial organization, technology platform provider and others involved in a MFS transaction, it becomes more difficult to generate trust about data security among the end users as well as among the entities involved. This paper presents a study on SIM-based tool for user authentication in financial transactions.

1. INTRODUCTION

Wide penetrations of mobile phone usage and the availability of more powerful mobile handsets and network bandwidth have made mobile devices an attractive candidate for value added services. Today mobile users can carry out basic banking and financial transactions such as transfer money, check balances or pay a bill or statement. Mobile Financial Services (MFS) will be a value added service for mobile users due to the fact that the users can carry out banking from anywhere anytime at their convenience. It also gives the opportunity for people who do not have broadband connectivity to carry out mobile banking. According to the Juniper Research, by the end of 2011 more than 150 million subscribers worldwide will have used MFS and this represents a growth of more than three fold since 2008 [1].

However, security is one of the main areas of concern, when introducing financial services in mobile devices. During the re-cent past there has been a number of mobile financial solutions emerged in the market place that are complex and hence have slowed the adoption. This paper will review the existing MFS solutions and propose a novel security framework that will provide increased security and usability features. This study was conducted by first identifying the ecosystem players of MFS and then conducting a review of literature in understanding the factors acting as drivers and inhibitors towards the adoption of MFS. Keeping these factors of adoption in view, the existing technologies for delivering mobile financial services were evaluated in order to understand the gap between the supply and the demand of the service. Based on these findings, a security framework was designed in order to address the existing issues of trust over security and privacy concerns in a multi entity environment like MFS. Further, the framework was optimized in order to suit the low memory and low processing speed constraints of a mobile device.

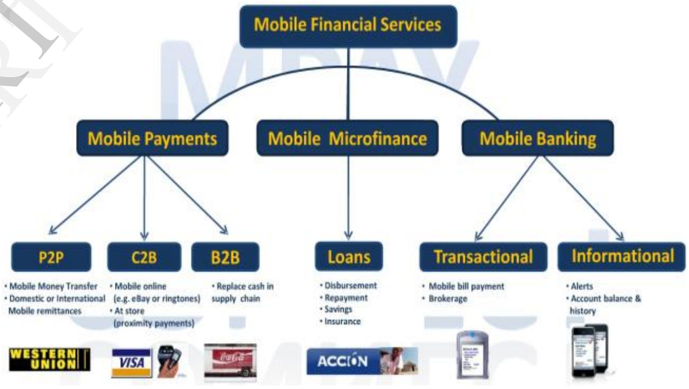

Figure 1: Mobile Financial Services Structure[2]

2. EXISTING TECHNOLOGIES FOR MFS

2.1 SMS Based Technology

The short message services in the mobile network are used to communicate between the mobile user and the bank. This is one of the most popular techniques and SMS banking offers features like check account balance, do micro payments and view mini statements. The user is registered with the bank using the mobile phone number and a password or PIN and those parameters are used to authenticate the user. The bank provides a set of SMS codes for different banking functions or user has to send messages to different destination numbers for different services. Memorizing different SMS codes for different banking functions is cumbersome to the mobile users and there is no nationally or internationally accepted standard code of practice available till-date [1].

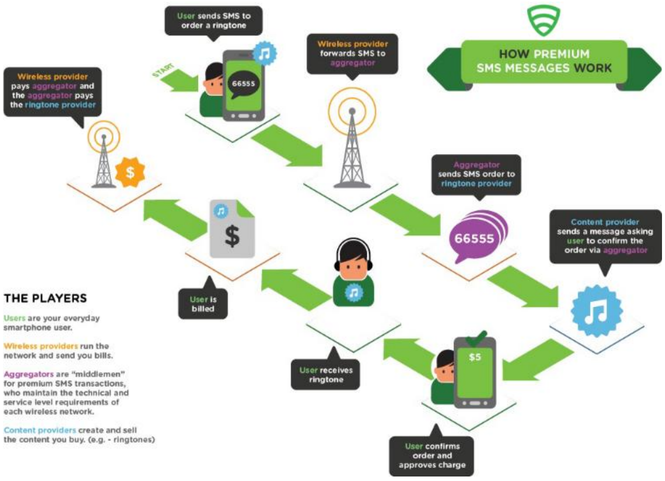
User sends SMS to order a ringtone
HOW PREMIUM SMS MESSAGES WORK
START
66555
Wireless provider forwards SMS to aggregator
Wireless provider pays aggregator and the aggregator pays the ringtone provider
Aggregator sends SMS order to ringtone provider
66555
Content provider sends a message asking user to confirm the order via aggregator
$
User is billed
THE PLAYERS
Users are your everyday smartphone user.
Wireless providers run the network and send you bills.
Aggregators are "middlemen" for premium SMS transactions, who maintain the technical and service level requirements of each wireless network.
Content providers create and sell the content you buy. (e.g. - ringtones)
User receives ringtone
$5
User confirms order and approves charge

Figure 2.1: VAS via SMS

2.2 WAP-GPRS Technology

Wireless application protocol (WAP) browser provides all the basic services of a web browser but simplied for a mobile phone.WAP banking in other terms is mobile Internet banking such as mobile user's access banking websites designed to be accessed from mobile phones. This MFS would require all or a part of the authentication credentials used in Internet banking. Mostly, the users have to enter the username, password and account number. The extra security is added by some banks with introducing a One Time Password service. The bank issues a password that is valid for just single login or single transaction. So ever time when user makes a new transaction the One Time Password is sent through SMS to the mobile phone. The user has to enter the password in the WAP site to authenticate.

However, entering all the security parameters using a mobile phone with restricted key pad (e.g. most of the mobile phones represent 4 letters by a single key in the key pad.) is not a user-friendly authentication method in MFS[1].

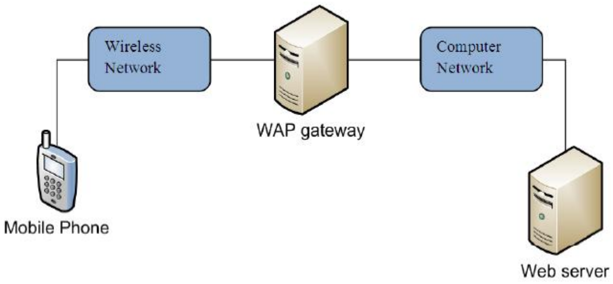

Figure 2.2: WAP Process

2.3. MOBILE-Browser Technology

Most banks are in the process of adopting this technology. The MFS application is downloaded to the mobile device and then user is authenticated using username and password technique and the mobile number is used for the user identification in some of the existing applications. However, still the user entered password is required by the bank for the user authentication. This password is recommended to be strong characters to prevent security attacks. Meanwhile, Interactive Voice Response(IVR) calls are implemented in the MFS platform by some of the banks to improve the security features. Most of the MFS inherit user authentication using one or more combinations of username, password, PIN, phone number and IVR calls. Meanwhile, an extra PIN or password based authentication is required to authorize money transactions in MFS[1].

However, according to the article [3], the number of user inputs to the mobile application using the mobile key pad should be minimized since it should be convenient for users to operate while on the move. Clarke and Furnell [4] presented security weaknesses in PIN and other user intrusive authentication systems in mobile devices. They highlighted the importance of nonuser intrusive authentication methods for sensitive service access at mobile devices.

Figure 2.3 : Mobile browser

3.SIM AUTHENTICATION TECHNIQUE

The security framework in this paper uses the SIM based authentication at the mobile operator to authenticate the mobile users to the MFS. Then identity and attribute (parameter) based key generation functionality is proposed to authorize more sensitive financial services at the mobile device. The combination of SIM authentication and parameter based authorization generates a simple security framework for MFS. The mobile service environment has various stakeholders like the customer, telecom operator and the financial institute (like bank, for example). The customer's mobile device has a SIM card connected to a mobile network.

The proposed security framework allows mobile users to use the SIM based authentication mechanisms at the bank to access MFS. The authentication functionality is based on Federated Identity Management (FIM) technologies with the standard 3G authentication techniques at the mobile operator. The FIM is an extended version of the Single-Sign-On (SSO) technique and it enables a single authentication system to be shared across multiple trust domains. The mobile operator and the bank are in two trust domains but the user authentication is linked using the FIM technology. The mobile users and the bank are connected to the mobile operator to access the outsourced SIM based credentials for authentication in the proposed model [1].

4. LITERATURE SURVEY

4.1. Enhancing E-commerce Security Using GSM Authentication

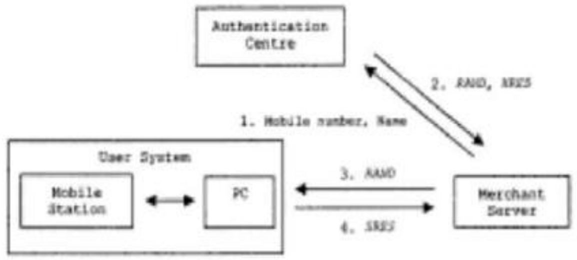

Figure 4.1: Enhancing e-commerce Security Using GSM Authentication [7]

Process

Merchant server send a RAND to the User System and SIM. Upon the receipt of the RAND, the SIM generates the SRES and send sit to the merchant server via user PC. The merchant serve subsequently sends the cardholder's name, his/her mobile number, the RAND, and the SRES to the AuC to verify. In message 3,Merchant server supplies the cardholder name as well as the mobile number. The AuC is then required to perform the matching between the name supplied in message 1 with the name it has associated with the GSM number, If they do not match the protocol should not be proceed. If they do match, in message 4the AuC simply provides a (RAND,XRES) pair.[7]

Advantages:

- The protocol provides user authentication based on GSM based user authentication.
- Since stolen debit card or credit card details cannot be used to launch a successful e commerce transaction.
- The protocol support us user mobility. The user authentication process requires only the correct software to be landed on the PC, and for there to exist a means to connect the MS to PC.
- From Merchant point of view, the protocol will lessen fraudulent transactions and hence reduce the cost of 'card not present' charge backs.

Disadvantage:

- Prior agreement is required between merchant and mobile phone service provider to support the portocol between AuC and merchant server.
- Merchants may be charged for the AuC services.

- If U-SIM Toolkit is to be used, the proposed protocol may require an ME and a SIM that support the functionality.

4.2. A Conceptual Framework for a SIM-based Electronic Transaction Authentication System

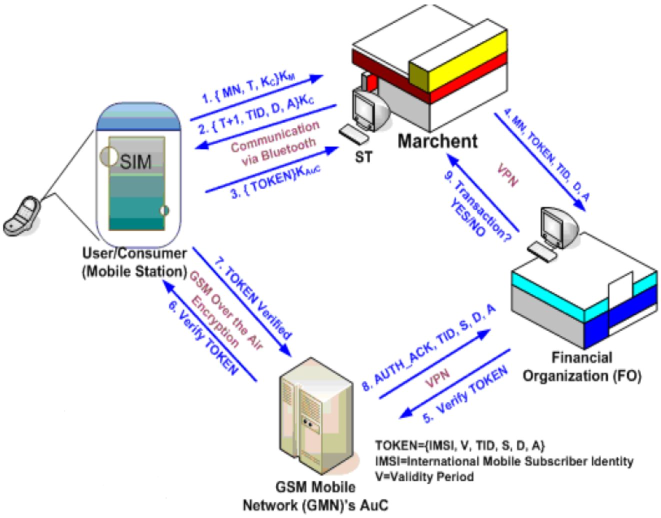
SIM
User/Consumer (Mobile Station)
1. { MN, T, Kc}KM
2. { T+1, TID, D, A}Kc
Communication via Bluetooth
3. { TOKEN}KAuC
ST
Marchent
4. MN, TOKEN, TID, D, A
VPN
9. Transaction? YES/NO
Financial Organization (FO)
5. Verify TOKEN
VPN
8. AUTH_ACK, TID, S, D, A
7. TOKEN Verified
GSM Over the Air Encryption
6. Verify TOKEN
GSM Mobile Network (GMN)'s AuC
TOKEN={IMSI, V, TID, S, D, A}
IMSI=International Mobile Subscriber Identity
V=Validity Period

Figure 4.2: Conceptual Framework for Sim Authentication[6]

Steps Authentication protocol in following steps.

Step 1: The Consumer will initiate the process by sending the Mobile Number (MN), Time Stamp (T), and Consumer's Public Key (*K*c) by encrypting with the Merchant's Public Key (*K*M) to the Service Terminal (ST) at the Merchant Side.
Step 2: The Merchant sends a TOKEN request with timestamp T+1, Transaction ID (TID) and Amount (A) by encrypting with *K*c to the TGS of MS. T+1 ensures that the TOKEN request is from the actual merchant from whom the consumer is intending to purchase items.
Step 3: If the Consumer agrees with the received information, TGS sends a TOKEN encrypting it with GMN's Public Key (*K*AuC), to the ST of the Merchant. The TOKEN contains International Mobile Subscriber Identity (IMSI), Validity Period (V), Transaction ID (TID), Source Account Information (S), Destination Account Information (D) and Amount to Transfer (A).

IMSI is used to identify the Consumer's SIM, V for protection against replay attack. If the actual request arrives within V, the request is valid to the Consumer for the first entry only.
Step 4: The Merchant sends the TOKEN along with the Consumer's Mobile Number (MN), Transaction ID (TID), Destination Account Information (D) and Amount to Transfer (A) to the Consumer's Financial Organization (such as a bank) for transaction.
Step 5: The financial organization will send the TOKEN received from the Merchant to GMN's AuC to authenticate the request. AuC decrypts the TOKEN with its Private Key (K^{-1}_{AuC}).

Step 6: GMN's AuC sends a verification request to the Consumer's MS.
Step 7: Consumer's MS sends verification acknowledgement to the AuC.
Step 8: Then GMN's AuC sends Authentication Acknowledgement (AUTH ACK), TID, S, D, and A to Financial Organization (FO).
Step 9: If successful (i.e., TID, D and A matches with those sent by the Merchant), then FO will complete the transaction with the Merchant against the TID.

Dialogue Summary
1. Consumer Merchant: MN, T, KCKM;
2. Merchant Consumer: T+1, TID, D, AKC
3. Consumer Merchant: TOKENK AuC
4. Merchant FO: MN, TOKEN, TID, D, A
5. FO GMNfs AuC: Verify TOKEN Req.
6. GMNfs AuC Consumer: Verify TOKEN Req.
7. Consumer GMNfs AuC: TOKEN Verified Ack.
8. GMNfs AuC FO: AUTH ACK, TID, S, D, A
9. FO Merchant: Transaction? YES/NO

5. Technique 1: SIM Authentication Via GSM Network

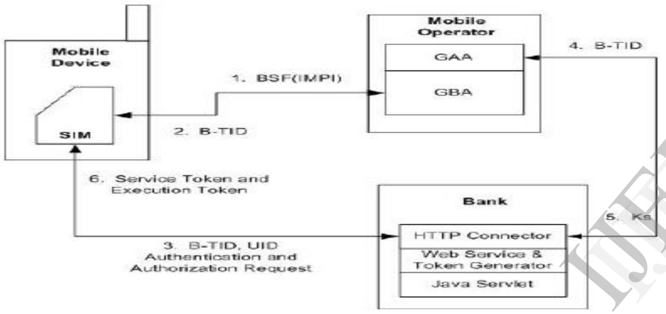
Mobile Device
SIM
1. BSF(IMPI)
2. B-TID
Mobile Operator
GAA
GBA
4. B-TID
5. Ks
6. Service Token and Execution Token
3. B-TID, UID Authentication and Authorization Request
Bank
HTTP Connector
Web Service & Token Generator
Java Servlet

Figure 5.1: Authentication based on gsm technique[1]

A. Architecture

The mobile device has an over-the-air installed application that uses the SIM card as one of its security elements. This application is named as the Security Capsule. The MFS content is provided by the services provider in accordance with the Web services standard over the Simple Object Access Protocol (SOAP) messaging. The mobile operator provides the authentication service using the Generic Bootstrapping Architecture (GBA)architecture of Generic Authentication Architecture (GAA). The Security Capsule uses the physical and logical identities and key credentials at the mobile device as inputs.

The following are the necessary credentials: 1)IMPI (IP Multimedia Private Identity).2)IMEI (International Mobile Equipment Identity)3)UID: The identity provider issued unique identity for the security capsule. The UID is inserted into the source code of the Security Capsule and it cant be retrieved by external parties.4)Token Key: This cryptographic key is issued by the bank as a result of successful mobile user authentication and authorization.

B. Security Protocol Design
1) Registration: A mobile user registers with the bank for MFS. The mobile user downloads the security capsule and then shares some secret credential information with the bank for the authentication. The mobile user registers for the MFS by downloading the Security Capsule from the bank. The Security Capsule is downloaded and installed to the mobile device using over the air technique of the mobile network. It contains a unique identification number (UID) and it is used to identify the mobile user at the identity provider. The security capsule sends a registration acknowledgement to the bank after the successful installation. The registration acknowledgement consists of the UID and identification parameters at the mobile handset.

2) Authentication: The mobile user authenticates with the bank to access services on the bank account. The secret credentials are exchanged and parties are mutually authenticated with each other. The mobile device uses the Bootstrapping Server Function at the mobile operator to create the application layer credentials. The generation of the application layer credentials is presented by the messages 1 and 2 in Figure2. The B-TID is a mobile operator generated reference to the application layer credentials. These credentials are then shared with the bank according to the GBA of GAA. The messages 3and 4 in Figure 2 are referred to the GAA function between the mobile operator and the bank. The knowledge of the shared secret mutually authenticates the mobile user and the bank to the MFS framework as shown in messages 5 and 6 in Figure2. The bank uses its public key certificate to authenticate with the mobile user and Security Capsule generated shared key is used for secured communication post authentication.

3)Authorization: This is an extended security feature in MFS and bank would use the authorization before any financially valuable transactions. For example, activities such as money transfer from account, setting up direct debit, change personal information, etc. These activities have to be authorized with special credentials compared to the authentication C. Security Tokens and Data Key Generation The protocol is optimized for minimum number of communication messages in registration, authentication and authorization processes. The size and the complexity of the tokens are reduced to suit the constraints related to the processing power of the mobile devices as well as the bandwidth constraints of mobile networks.

1) SecurityToken Design: The Service Token is encrypted by the public key of the bank and it is signed by the secret key of the bank. There are two public key pairs that are maintained for the signature and encryption operations at the bank. This token is a property of the bank and the bank uses the token to identify the authenticated mobile devices. Therefore, the bank is the only entity that can decrypt the token. However, the mobile user validates the token signature to verify the banks authentication to the communication channel.

2) Data Key Generation: The Data Key is generated at the Security Capsule to present the mobile legitimacy and authorization to access the requested sensitive services from the bank. This key is generated using some of the shared attributes and key credentials between the mobile device and the bank. The bank generates a random number and it is named as Execution Challenge. The bank generates the Execution Challenge Response, sends the Execution Challenge to the Security Capsule and requests the Security Capsule to generate the Execution Challenge Response. Finally, the bank compares both Execution Challenge Response outputs before authoring mobile users to execute services[1].

6. TECHNIQUE 2: SIM AUTHENTICATION TECHNIQUE VIA BLUETOOTH

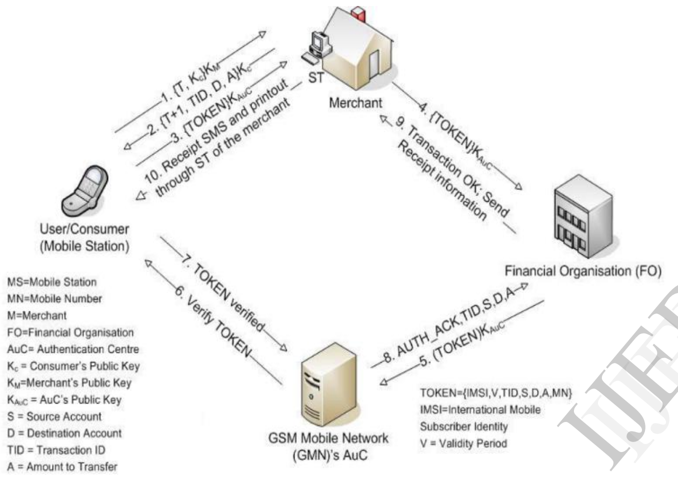
Merchant
ST
$1. \{T, K_c\}K_M$
$2. \{T+1, TID, D, A\}K_c$
$3. \{TOKEN\}K_{AuC}$
10. Receipt SMS and printout through ST of the merchant
$4. \{TOKEN\}K_{AuC}$
9. Transaction OK; Send Receipt information
User/Consumer (Mobile Station)
Financial Organisation (FO)
7. TOKEN verified
6. Verify TOKEN
8. AUTH_ACK,TID,S,D,A
$5. (TOKEN)K_{AuC}$
GSM Mobile Network (GMN)'s AuC
MS=Mobile Station
MN=Mobile Number
M=Merchant
FO=Financial Organisation
AuC= Authentication Centre
K_c = Consumer's Public Key
K_M=Merchant's Public Key
K_{AuC} = AuC's Public Key
S = Source Account
D = Destination Account
TID = Transaction ID
A = Amount to Transfer
TOKEN={IMSI,V,TID,S,D,A,MN}
IMSI=International Mobile Subscriber Identity
V = Validity Period

Figure 6.1: Authentication Bluetooth Technique[5]

The authentication protocol technique is described in the following steps[5].

Step 1: The Consumer will initiate the process by sending the Time Stamp (T) and Consumer's Public Key (KC) by encrypting it with the Merchant's Public Key (KM) to the Service Terminal (ST) at the Merchant side.

Step 2: The Merchant sends a TOKEN request with times-tamp T+1, Transaction ID (TID) and Amount (A) by encrypting them with KC to the TGS of MS. T+1 ensures that the TOKEN request is from the actual Merchant from whom the consumer is intending to purchase items.

Step 3: If the Consumer agrees with the received information then the TGS sends a TOKEN encrypting it with GMNs Public Key (KAuC) to the ST of the Merchant. The TOKEN contains International Mobile Subscriber Identity (IMSI), Validity Period (V), Transaction ID (TID), Source Account Information (S), Destination Account Information (D), Mobile Number (MN) and Amount to Transfer (A). IMSI is used to identify the Consumers SIM and V for protection against replay attack. If the actual request arrives within V then the request is valid to the Consumer for the first entry only.

Step 4: The Merchant sends the TOKEN along with the Consumers Mobile Number (MN), Transaction ID (TID), Destination Account Information (D) and Amount to Transfer (A) to the Consumers Financial Organization (such as a bank) for transaction.

Step 5: The financial organization will send the TOKEN received from the Merchant to GMNs AuC to authenticate the request. AuC decrypts the TOKEN with its Private Key (K1AuC).

Step6: GMNs AuC sends a verification request to the Consumers MS.

Step 7: Consumers MS sends verification acknowledgement to the AuC.

Step 8: GMNs AuC sends Authentication Acknowledgement (AUTH ACK), TID, S, D and A to the Financial Organization (FO).

Step 9: If successful (i.e., TID, D and A matches with those sent by the Merchant) then the FO will complete the transaction with the Merchant against the TID. The FO sends the purchase information, e.g. partial information of the sender card (for security), purchase date, amount etc. to the Merchant.

Step 10: The Merchant sends a SMS receipt to the MS. Optionally a printout of the receipt is generated through the Service Terminal (ST) of the Merchant.

7. COMPARATIVE STUDY

The parameters are the one on which comparative study done of two Sim Authentication Techniques. Hence, Table shown state the technique which is better for mobile financial services. Mobilenumber (Mobnum) should be kept anonymous for user security; another element is account number(Accnum) of an user which contain essential details of user identity. Bank account number have name, address and phone number. It can reveal user's whole identity to unknown vendor. In the protocol, the mobile number (which is registered at the relevant Financial Organization beforehand) is used in conjunction with the encryption methods used in etransactions.

The protocol uses an asymmetric authentication from the mobile terminals to the authentication server, which indirectly reduces the threat posed by the storage of unencrypted card numbers in a Merchant server. It therefore makes sense to use any GSM based authentication in conjunction with GPRS to provide network services. In short, the protocol makes use of the mobile station portability and the GSM authentication mechanism to provide user authentication in a way that also supports user mobility.

Sr.No	Parameters	Sim Based by GSM	Sim Based by Bluetooth
1	Anonymity	Mobnum	No Accnum, Mobnum
2	Model Structure	Peer-to-peer	Client-Server
3	Deadlock	Occur	Handle
4	Authentication	Mobile user	Mobile operator
5	Memory Power	Less power	Gain more power
6	Message Transactions	Small	Large
7	Correctness	Sequence not considered	Sequence considered

Table 7.1: Comparative Study of sim authentication techniques

8. CONCLUSION

Sim based authentication (i.e. Technique 2) provide more secure structure and transactions.Token which is used in encrypted by public key so that can't be interrupted. The connectivity of FO and AuC is also through the optimal link. All the AuCs must synchronously update the central database. While connecting the User to its nearest AuC the token verification process will use the mutual authenticities of all the AuCs with the corresponding central database. The TOKEN generated by the users mobile station (MS) is verified by the AuC using direct encrypted communication with the users MS.

Hence, this paper satisfies all parameters that need to follow for mobile financial services. The Merchant is not concerned about the Consumers account. It keeps the Consumers account anonymous. The user information is sent using an asymmetric authentication procedure via the Merchant server to the FO. Furthermore, FO to Merchant connectivity is done using a VPN, where the authenticity and security risks are handled predominantly from the FO side. They assume that the communication links between the MS and Merchant server is secured using the latest Bluetooth security [8].

8. BIBLIOGRAPHY

[1] *"Security Framework for addressing the issues of Trust on Mobile Financial Services"*, RajanishDass, Rajarajan Muttu krishan, 2011

[2] "*Mobile Financial Service: A competitive (and fragmented) land scape"*, Francesco Burelli, Roger Clarke ,Edward Cliaord and Mark Weston, Dec 2012.

[3] *"Secure Web Authentication with Mobile Phones"*,in DIMACS Workshop on Usable Privacy and Security Software, M. Wu, S. Garfinkel, and R. Miller, 2004.

[4] *"Authentication of users on mobile telephones"*, Computersand Security,N. Clarke and S. Furnell, vol. 24, no. 7, pp.519-527, 2005.

[5] *"A SIM-based electronic transaction authentication system"*, Comput Syst Sci and Eng 4: 1320, Manzur Ashrafand Syed Mahfuzul Aziz, M. Lutful Kabir and Biswajit K.Dey,2009.

[6]"*A Conceptual Framework for a SIM-based Electronic Transaction Authentication System"*, IFIP International Conference on Network and Parallel Computing, Manzur Ashraf, Syed Mahfuzul Aziz, M. Lutful Kabir, Biswajit k.Dey,2007.

[7]"*Enhancing E-commerce Security Using GSM Authentication"*, Springer Berlin/Heidelberg, V. Khu-smith and C. Mitchell, 2003.

[8] *Wireless network security 802.11,bluetooth and handheld devices*, T. Karygiannis and L.Owens, TechRep, NIST, 2002.