Integration of Biometric authentication procedure in customer oriented payment system in trusted mobile devices.

Vibha Kaw Raina.

Department of Computer Sciences Birla Institute of Technology, Extension Centre NOIDA.
kawvibha@yahoo.com

ABSTRACT

Mobile payments have become an important application in daily activities. The unique advantage of mobile payments over traditional payments has led to tremendous growth of mobile phones. The strong demand of mobile applications raised increased concern on the security of mobile applications as well as devices. New mobile devices are developed to serve various functions like storing sensitive information, accessing this information as well transacting this information through payment systems. In order to protect this information and mobile devices, a well defined authentication system is mandatory. Biometric authentication is much more safe and secure and very easy to use. In this paper we propose a multi modal biometric authentication procedure with respect to payment systems and integrate this model with our previous work. The aim of this paper is to integrate the proposed payment model with multi server authentication model for the purpose of maintaining security and accessing different servers (websites). The system providing resources to be accessed over the network often consists of many different servers through out the world. The distribution of the remote system hardware in different places makes the user access the resources more efficiently and conveniently.

Keywords: *M-payments, authentication, biometrics.*

1. Introduction

A mobile payment is the process of two parties exchanging financial value using mobile device in return for goods and services. It can also be defined as the transfer of money from one party to another through the exchange of information. Mobile devices may include mobile phones, PDA's, wireless tablets and any other device that can be connected to mobile telecommunications network for making payments. For any mobile payment to be widely accepted and adopted it is important to overcome the following challenges. Interoperability, Usability, Simplicity, Universality, Security, Privacy, Cost, Speed and Cross border Payments. [1] Among all these challenges security is the most crucial one. Authentication can be classified in three types. The first approach is using a PIN (Personal Identification Number) or password which is a secret knowledge based technique. This technique provides cheap and quick authentication. The second approach is the token- based technique or SIM (Subscriber Identification Module). In this approach, when users do not want to use the mobile, the mobile's SIM is removed. However, removing SIM is not recommended due to inconvenient manner. Payment systems that are developed on the basis of passwords and tokens are easily misused, due to the shortcomings (Forgotten, lost, copied, shared, distributed). The last approach is the applying of biometric technique. This technique is based on a unique characteristic of a person where identification and verification of individual is based on human characterisitics.Biometric approaches are divided into two categories: physiological and behavioural. Physiological

DOI : 10.5121/ijitcs.2011.1602

biometric is based on bodily characteristics, such as fingerprints, iris scanning and facial recognition. Behavioural biometric is based on the way people do things, such as keystroke dynamics, mouse movement and speech recognition. Biometric payment is a kind of technology that allows people to pay at shops or markets with just touch of their fingers, moving their face or laying up their hands. Biometric authentication is different than normal authentication system as they won't need any tokens or passwords for their payment other than their biometrics. With biometric payment systems the account information is automatically recognized to finish the payment procedure.

Biometric authentication is Fast, Easy, Secure. No swapping card or writing of checks is required. People can leave their wallet behind. And above all, their biometrics is unique, so only the user can access the system. [2]

The remainder of this paper is organized as follows: Related work is discussed in Section 2 Different biometric technologies and authentication process is discussed in Section 3 while Section 4 discusses the proposed model, Section 5 discusses the integration of the proposed model with our existing multiserver authentication model and Section 6 gives the Conclusion and Section 7 future work.

2. Related Work:

Uludag et al. (2004) defined biometric technique as an automated methodology for the recognition of a person based on behavioural or physiological characteristics. These characteristics include features such as hand geometry, handwriting, face, fingerprints, vein, voice, retina, and iris. The authors concluded that biometric technologies are now the key to an extensive array of highly secured identification and personal verification solutions. Welzl (2004) states that the biometric system is a pattern recognition technology that makes personal identification of an individual by determining the authenticity of a specific physiological or behavioural characteristics possessed by the user.

Jain et al. (2003) describe the significant differences between the physiological and behavioural biometrics. The physiological biometrics consists of measurements and data congregated from direct measurement of a part of the human body. Samples of these include but not limited to hand geometry, facial recognition, fingerprint, iris-scan etc. On the other hand, the behavioural characteristics originate from the actions of an individual, and it indirectly measures unique characteristics of the human body. Samples of these include but not limited to signature-scan, keystroke-scan, voice recognition, etc. Time can act as a metric for behavioural biometrics, because it measures behaviour by considering the timeline of a given process (Shoniregun, 2003; Ratha et al., 2001; Putte and Keuning, 2000).

Jain and Uludag (2003), and Soutar (2002), among others noted that an ideal biometrics system should be universal, unique, permanent and collectable. It must be universal that every person possesses the characteristics and uniqueness; where no two persons share the characteristic and permanency; where the characteristic should neither be changed nor be alterable; and finally the characteristics must be collectable and be readily presentable to a sensor and is easily quantifiable (Uludag, et al., 2004). Some other studies found that characteristics that satisfy all the above mentioned requirements may not be practical or feasible for a useful biometric system (Linnartz and Tuylus, 2003).

Schneier (1999) and Timmers (2000) in their studies indicate that the integration of biometric technologies into applications was achieved using proprietary software developers' kits (SDK's). However more recent studies summarized that a standardized biometric application programming interface, BioAPI, Version 1.1 of the specification released in 2001 was instituted to enhance the portability of unrelated biometric technology within applications (Soutar, 2002; Jain and Uludag, 2003; Adler, 2004).

Also, it was determined that developers and vendors of a practical biometric system should consider other issues such as performance, acceptability and circumvention (Ross et al., 2005).

Performance in this sense means systems accuracy, speed, robustness, as well as its resource requirements and operational or environmental factors that affect its accuracy and speed. Acceptability means the extent people are willing to accept a given biometric sample identifier in their daily lives. Circumvention means how easy it is to fool the system through fraudulent methods (Uludag et al., 2005).
Biometrics based authentication applications that is critical to the growth of the global economy comprises of many features. These include but not limited to single sign-on, Web security, transaction security, application logon, data protections, workstations, remote access to resources, and etc. (Maltoni, 2003).

3. Different Types of Biometric Technologies:

Following are the types of biometric technologies which can be used for mobile payments.

- Facial Recognition: This technology is used to identify people from still or video photograph image of their faces.[3]
- Fingerprint Identification: The technology that make authentication through fingerprint. A fingerprint is the pattern of ridges and furrows on the surface of fingertip. No two persons have exactly the same arrangement of patterns, and the patterns of any individual remains same through out life.[4]
- Retinal Pattern Recognition: The technology to authenticate people through scanning their eyes. The retina is the innermost layer of the eye. The pattern formed by veins beneath the surface of the retina is unique to each individual. [5]
- Iris Based Identification: This technology authenticates with iris scanning. The coloured part of the eye is iris. It lies at the front of the eye surrounding the pupil.[5]
- Voice Recognition or speaker recognition is a technology through which voice of a person is recorded. The biometric technology uses the acoustic features of speech that have been found to differ between individuals. These acoustic patterns reflect both anatomy (i.e. shape and size of throat and mouth) and learned behavioural patterns (i.e. voice pitch, speaking style).[6,7]
- Signature Recognition: This technology is used to verify the signature of the individual. Signatures of people vary substantially. It is based on measuring dynamic signature features such as speed, pressure and angle used when a person signs a standard, recorded pattern (e.g. autograph). [6,7]

3.1. Biometric Authentication Process:

There are two processes in biometric authentication. Enrollement process and verification process.

3.1.1 Enrollement Process:

In this process the biometric template of the customer is captured and stored in biometric database. The typical steps in enrolment process are:
i) The customer is asked to enter a customer identity number (this could be a bank related number, a national ID or any other unique identity number).
ii) The customer is then asked to present their biometric template on a scanner that then captures the images.
iii) The enrolment system may ask the customer to present their biometric multiple times to ensure that the quality of image captured is good for verification.
iv) An ISO 19794-2 template is derived from the captured images.
v) The template along with the raw image is stored in the biometric server against the customer identity number for later retrieval and verification.

3.1.2 Verification Process:

In this process customer biometric template is verified to authenticate the payment. In verification process the customer enters their customer identity number into the verification system. The system then prompts the customer to present their live biometric on the scanner. The live biometric is then compared with the biometric template stored against the customer identity number in the biometric server. In case the verification is successful the payment transaction is considered authenticated and the transaction sent to the bank for processing. In case of a failure the customer may be asked to present the biometric template again up to a certain maximum number of tries.
Implementing a biometric authenticated payment system requires three primary system elements to be put in place by a bank or acquirer. These are:

a) **Enrolment System**:

Used for enrolling customers on to the program and recording their biometric identity. In enrolment stage the biometric images of the different individuals to be verified are first processed by feature extraction module; the extracted features are stored as template in a database for later use.

b) **Verification System**:

Used at retail locations for verifying the live biometric template with the stored fingerprints for authenticating payments. The biometric image of the individual to be verified first processed by feature extraction modules; the extracted features are then fed to a matching module with his/her identity ID, which matches them against his/her templates in the database.

c) **Biometric Server**:

Used for storing the biometric template, extracting and verifying biometric template during a payment process and providing an interface to banks and acquirers for managing the customer data and reports. [8]

4. Proposed Model:

The proposed model gives the flexibility to perform any payment or transaction, where no external entity is involved other than bank. This model is based on customer centric and bank centric approach which is useful for both the bank as well as the user. The model has the three levels of security to authenticate the user. The first level asks for the account number and password for the respective account. The second level of security asks for the biometric template, where user after entering his biometric will be able to access his account and the third level of security asks for barcode scanning of the mobile device. Since, this model is also used for P2P transactions and it uses mobile wallet it becomes necessary to ask for the security of mobile device. After entering the security credentials the model gets activated and the user can perform any kind of payment or transaction. The proposed model is to be implemented in J2ME and J2EE.
The first step in the proposed model is to check the first level of security i.e. in the form of account number and password. After entering the account number and password the system checks the validity of the user credentials. If the user enters the right account number and password the system enters into second level of security otherwise again asks for the account number and password. After authenticating the first level the system asks for the second level of security which is the biometric template of the user. The system verifies the biometric template of the user with the stored biometric template in the database. If the user enters the valid biometric template then the system enters the third level of security i.e. barcode. The system asks for the scanning of the barcode of the phone. Otherwise the system again asks for the

biometric template. After the scanning of the barcode of the phone the system checks for its validation. If the validation is right then the system proceeds and enters in to the mode of transactions/payments otherwise it will continue asking the valid set of credentials till the loop ends (three times).

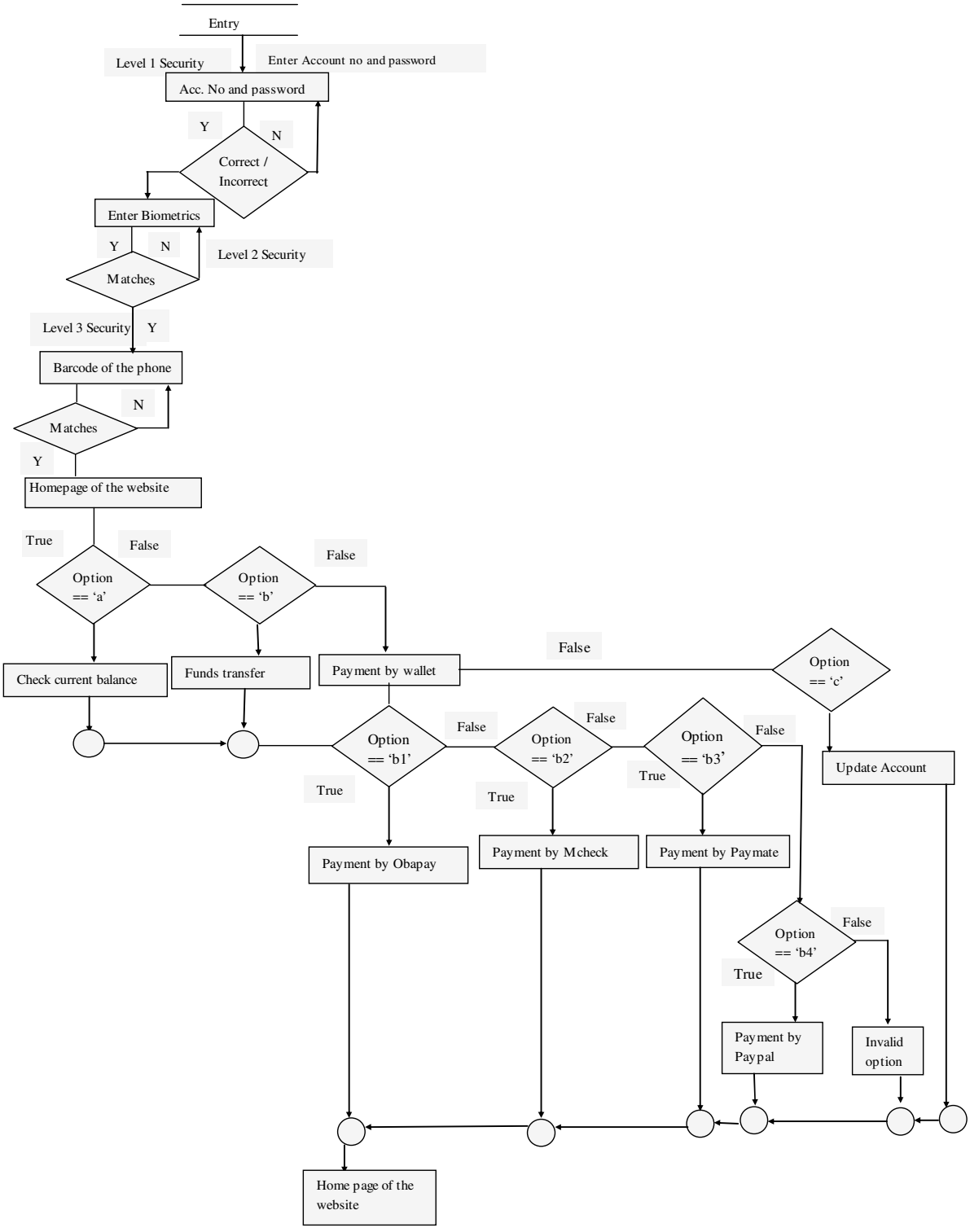
a) The first option provided in the model is to check the current balance of the account holder. By this option the user is able to check the details of the balance in the account.

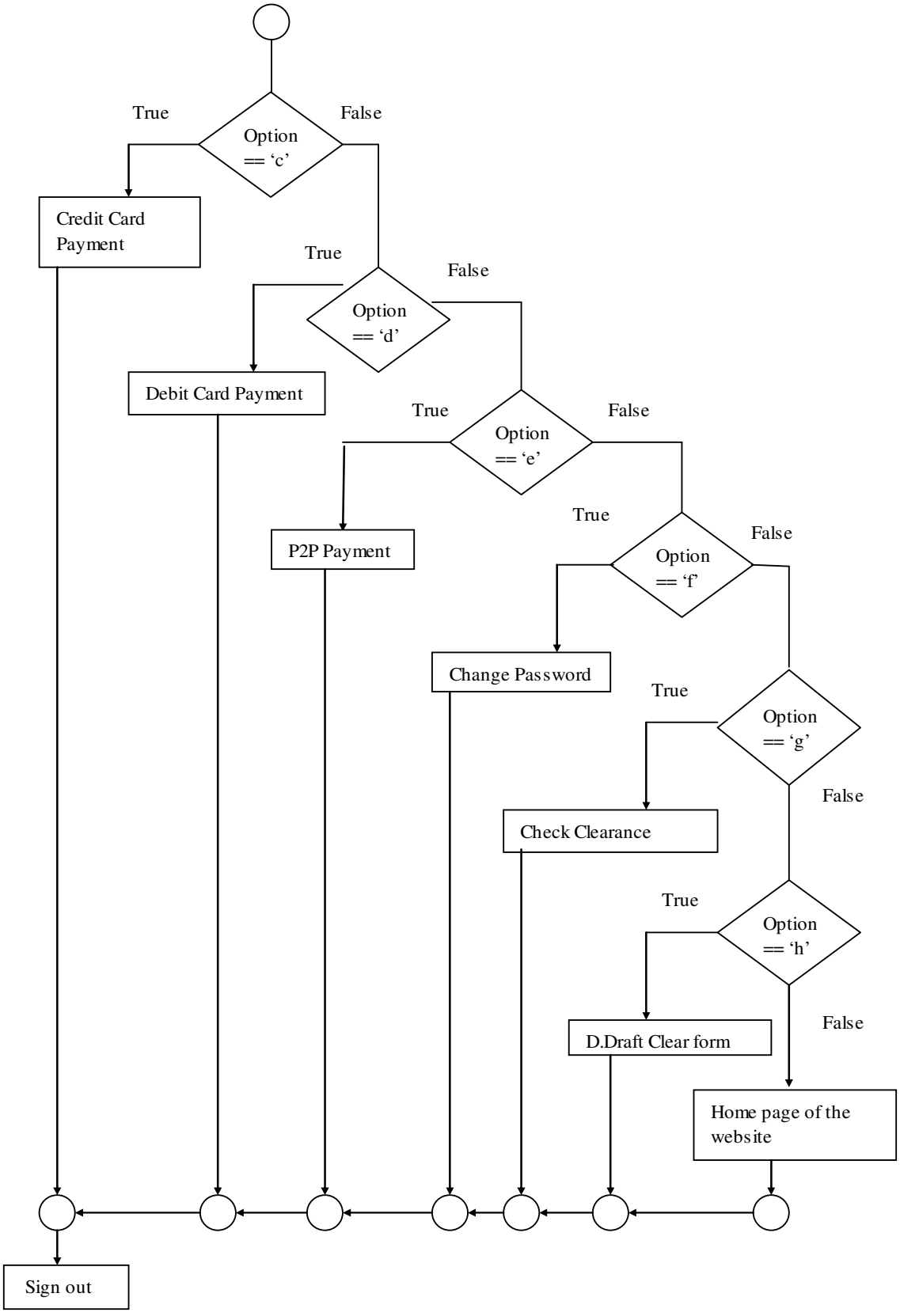
b) The second option is for transferring the funds from existing account to another account in any of the banks (money transfer).

c) The third option is the payments with the help of mobile wallets. This option is further having different choices that include payment with Pay Pal, M-check, Obapay, Pay mate. These payment options are useful for P2P transactions providing the facility to do transactions with electronic money.

d) The fourth option will be updating of the account.

The flow chart of the proposed model is given below using if then else statement.


Entry
Level 1 Security
Enter Account no and password
Acc. No and password
Y
N
Correct / Incorrect
Enter Biometrics
Y
N
Level 2 Security
Matches
Level 3 Security
Y
Barcode of the phone
N
Matches
Y
Homepage of the website
True
False
Option == 'a'
Option == 'b'
False
Check current balance
Funds transfer
Payment by wallet
False
Option == 'c'
Option == 'b1'
False
Option == 'b2'
False
Option == 'b3'
False
Update Account
True
True
True
Payment by Obapay
Payment by Mcheck
Payment by Paymate
Option == 'b4'
False
True
Payment by Paypal
Invalid option
Home page of the website


True
Option
== 'c'
False
Credit Card
Payment
True
Option
== 'd'
False
Debit Card Payment
True
Option
== 'e'
False
P2P Payment
True
Option
== 'f'
False
Change Password
True
Option
== 'g'
False
Check Clearance
True
Option
== 'h'
False
D.Draft Clear form
Home page of the
website
Sign out

Multi model Biometric authentication of the proposed model: The authentication models for authenticating are to authenticate the customer who has registration in the service of the multimodal biometric payment system.

Most models are based on network authentication system and are composed of client terminal, server side, which is used to collect the multimodal biometric data and to provide the services respectively. The multimodal biometrics template storage place and the verification place may be held at client side, server side and trusted third party (TTP) that may be a smart card to perform complex calculations. The different components required for the biometric payment systems are:

1) Secure Online Banking Server (SBS): It has access to customer's data; establishes connection with the Online Banking Software (BSW); conducts capital transactions and is able to identify a Biometric Trusted Device (BTD) as a communication partner to establish a secure connection.
2) Online Banking Software (OBS): It is stored on the client and communicates with SBS in order to process different transactions.
3) Secure Biometric Trusted Device (BTD): A trusted piece of hardware with predefined security criteria to provide secure functionality; cannot be manipulated by malware; has a biometric capture device as a fake resistant sensor which is qualified for unsupervised operation.

5. Integration of Proposed Payment System with Existing Multi Server Authentication Model:

This section introduces the multi-server authentication based on one way hash function and this model is our previous work. The aim of this scheme is to get integrated with the proposed payment model for the purpose of maintaining security and accessing different servers (websites) with mutual authentication and session keys generated. The system providing resources to be accessed over the network often consists of many different servers through out the world. The distribution of the remote system hardware in different places makes the user access the resources more efficiently and conveniently. [9]

The scheme is composed of three phases which are the server registration phase, user registration phase and authentication phase. The notations used in this paper are as follows:

- Si : The Server;
- Ui : The User;
- RC : The Registration Centre;
- ID, Pwd : Ui's identity and password, respectively;
- Bi : Biometric template of Ui;
- SIDi : Si's identity;
- x : Ui 's secret key maintained by the registration centre;
- y : Si's secret key maintained by the registration centre;
- K,N : Random nonce;
- h(.) : Secure one way hash function;
- $\oplus$: Exclusive – or (XOR) operation;
- || : Concatenation operation;
- A $\longrightarrow$ B:M : A sends a message M to B;

5.1 Server Registration Phase:

Step 1: When the server Si wants to register and becomes a new legal server, Si freely chooses his identity SIDi and submits it to the registration centre through a secure channel.

Si $\longrightarrow$ RC: SIDi

Step 2: RC computes h (SIDi ||y) and sends back to Si through secure channel.

RC ⟶ Si: h (SIDi||y)

5.2 User Registration Phase:

Step 1: When User wants to register and become a new legal user, Ui freely chooses his identity ID, password pwd, biometric template Bi of user Ui and a random nonce K and submits ID, pwd, Bi $\oplus$ K to RC through a secure channel.

Ui ⟶ RC: ID, pwd, Bi $\oplus$K

Step 2: RC computes user authentication key M=h (ID||x) and C=M $\oplus$ Pwd$\oplus$Bi$\oplus$K.
Then, RC stores C and h (.) into smart card and issues it to user Ui through a secure channel.

RC⟶ Smart card: Ui

Step 3: Upon receiving the smart card, Ui enters K into his/her smart card.

5.3 Authentication Phase:

After server registration phase of the proposed scheme, the following steps are then performed during the authentication phase:

Step1: When user Ui wants to login to a server Si, Ui inserts smart card into a card reader and enters his personal biometrics Bi, along with ID and Pwd . The card reader extracts M by computing C $\oplus$ Pwd $\oplus$Bi $\oplus$ K generating a random nonce NU and computes L1=h(M||NU)=h(h(ID||x)||NU). Then, Ui sends ID, NU and L1 to Si.

Ui ⟶ Si: ID, NU, L1

Step 2: Upon receiving the message in Step 1, Si generates a random nonce NS and computes L2 = h (h (SIDi||y) ||NS). Then, Si sends ID, NU, L1, SIDi, NS, and L2 to RC.

Si⟶ RC: ID, NU, L1, SIDi, NS, and L2.

Step 3: Upon receiving the message in step 2, RC computes L1'=h (h (ID||x) ||NU) and L2' = h(h(SIDi||y)||NS) and then checks whether L1=L1' and L2=L2' respectively. If they are equal Si computes session key V=h (h(SIDi||y)||NS||NU) the ephemeral secret key W=h(h(ID||x)||NU||NS)) for Ui and Si, L3=V $\oplus$ W and L4 =h(V||W) . Then, RC sends L3 and L4 to Si.

RC⟶ Si: L3, L4.

Step 4: Upon receiving the message in Step 3, Si computes V'=h (h (SIDi) ||y) ||NS||NU) and extracts the ephemeral secret key W by computing L3 $\oplus$ V'. Then, Si computes L4'=h (V'||W) and checks whether L4=L4'. If they are equal, Si computes the shared session key.
SK= (ID||SIDi||W||NU||NS) and L5=h(W||SK). Finally Si sends NS and L5 to user.

Si ⟶ Ui: NS, C5

Step 5: After receiving the message in Step 4, Ui computes the secret key W=h(h(ID||x)||NU||NS) and the shared session key, SK=h(ID||SIDi||W||NU||NS). Then, user computes L5'=h (W||SK) and checks whether L5=L5'.If they are equal Ui computes L6=h (W||SK||NS) and sends it to Si .

Ui ⟶ Si: L6

Step 6: Upon receiving the message in step 5, Si computes L6'=h (W||Sk||NS) and checks whether L6=L6'. If they are same then Si confirms the legality of user. As a results, Ui and Si can use shared secret session key, SK= h(ID||SIDi||W||NU||NS) in private communication.

6. Conclusion:

In this paper multimodal biometric payment model is integrated with the biometric multiserver authentication model. This paper has been developed from the broader perspectives of payments and transactions along with the security concerns. The proposed biometric payment model gives the user friendly approach to the customers from transaction and payment perspective. And the multiserver authentication model allows the user to get connected to the different servers across the world for different services and accesses satisfying the different security measures like resist guessing attacks, resists replay attacks, resists stolen - verifier attacks, resists insiders attacks, resists server spoofing attacks, resists registration center spoofing attacks, resists impersonation attacks, provides security of session key, provides the security of ephemeral secret key, provides the mutual authentication. The multiserver biometric authentication model is our previous work which has been presented in a national conference held in India.

7. Future work:

The future work can be diversified in the area of mobile payments and additional features can be added to it. (NFC, Barcodes).Based on the experiences drawn from researching risk and threat analysis on mobile payment systems, this is an area that needs to be further investigated. There is also a lack transaction protocols and databases used to compare the security of similar concepts which would be useful in order to evaluate different technologies. This might however depend on the difficulty of quantifying security which is highly subjective and can only be used as a pointer towards a correct value.

References:

[1] Praveen Chandrahas, Deepti Kumar, Ramya Karthik, Timothy Gonsalvis, Ashok Jhunjhunwala and Gaurav Raina **"** Mobile Payment Architectures for India", National Conference on Communications,2010.

[2] JuCheng Yang "Biometric Verification Techniques Combing with Digital Signature for Multimodal Biometrics Payment Systems". IEEE International Conference on Management of e-Commerce and e-Government 2010.

[3] Yadan Li, Xu Xu. "Revolutionary Information System Application in Biometrics". IEEE International Conference on Networking and Digital Society 2009.

[4] Ashbourn, J., Biometric Methodologies in Biometrics Advanced Identity Verification The Complete Guide, 2002, pp.45-63, Springer, London.

[5] Jain, A., Biometrics, WA: Microsoft Corporation, 2005.

[6] Fernando L. Podio: "Personal Authentication through Biometric technologies".

[7] Anil K. Jain, Arun Ross and Salil Prabhakar: "An Introduction to biometric Recognition" IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image and Video-Based Biometrics, Vol. 14, No. 1, January 2004.

[8] Innoviti Simplifying Communications "Online Biometric Authenticated Payment Systems. 2008

[9] Vibha Kaw Raina and U.S Pandey "Biometric and ID based user authentication mechanism using smart cards for multi-server environment" Proceedings of National Conference on Communications INDIA Com 2011.

[10] Adler, A. (2004), Images can be regenerated from quantized biometric match score data, Proc. Canadian Conf. Electrical Computer Eng., pp. 469-472, (Niagara Falls, Canada).

[11] BioAPI (2001), BioAPI Specification, American National Standards Institute, ANSI/INCITS 358, Version 1.1. Retrieved December 20, 2005 from http://www.bioapi.org/BIOAPI1.1.pdf

[12] Jain, A. K. and Uludag, U. (2003), Hiding biometric data, IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 25, no. 11, pp. 1494-1498.

[13] Kohler, E., Handley, M. and Floyd, S. (2004), RFC4340: Datagram Congestion Control Protocol (DCCP), Retrieved January 30, 2006from http://www.read.cs.ucla.edu/dccp/.

[14] Linnartz J. P. and Tuylus, P. (2003), New shielding functions to enhance privacy and prevent misuse of biometric templates, Proc. AVBPA 2003, Fourth International Conference on Audio- and Video-Based Biometric Person Authentication, pp. 393-402, Guildford, UK.

[15] Putte, T and Keuning, J. (2000), Biometrical fingerprint recognition: don't get your fingers burned, Retrieved November 20, 2005 from http://cryptome.quintessenz.org/mirror/fake-prints.htm.

[16] Ratha, N. K., Connell, J. H. and Bolle, R. M. (2001), An analysis of minuntiae matching strength, Proc. AVBPA 2001, Third International Conference on Audio – and Video-Based Biometric Person Authentication, pp. 223-228.

[17] Ross, A., Shah, J. and Jain, A. K. (2005), towards reconstructing fingerprints form minutiae points, Proc. SPIE, Biometric Technology for Human Identification II, Vol. 5779, pp. 68-80, (Orlando, FL).

[18] Schneier, B. (1999), Inside Risk: The uses and abuses of biometrics, Comm. ACM, vol. 42, no. 8, p. 136.

[19] Shoniregun, C.A., (2003), Are existing Internet security measures guaranteed to protect user identity in the financial services industry? Int. J. Services Technology and Management, vol. 4, no. 2, pp.194-216.

[20] Soutar, C. (2002), Biometric System Performance and Security. Retrieved October 10, 2005 from http://www.bioscrypt.com/assets/bio_paper.pdf

[21] Timmers, P. (2000) Electronic Commerce (Strategies and Models for Business-to Business Trading), John Wiley Publications, New York.

[22] Uludag, U., Pankanti, S. and Jain, A. K. (2005), Fuzzy vault for fingerprints, Proc. Audio- and Video- based Biometric Person Authentication (AVBPA), (Rye Brook, NY), July.

[23] Uludag, U., Pankanti, S., Prabhakar, S, and A.K. Jain (2004),Biometric cryptosystems: issues and challenges, Proceedings of the IEEE, vol. 92, no. 6, pp. 948-960.

[24] Welzl, M. (2004), TCP Corruption Notification options, Internet-draft (work in progress) draft-welzl-tcp-corruption-00.txt, June 2004. Retrieved February 12, 2011 from http://www.ietf.org or http://www.welzl.at/research/publications.