A Scheme for Integrated Multi-banking Solution

Sree Rekha G
Research Assistant
CORI, PESIT
Bangalore.

V.K.Agrawal
Professor
CORI, PESIT
Bangalore

ABSTRACT

In this paper we wish to propose an integrated model which uses a combination of Biometrics, smart card, user name, single interface and single password for accessing multiple bank accounts by the user in online banking applications. A variety of biometric systems are found in the literatures which are used for authentication purpose. In general, most of the users will have multiple online bank accounts and each one of them will have separate passwords. One has to remember all the passwords if he/she wants to operate his/her account. On the other hand if the user uses same password chances for cracking would increase. We propose a system where an interface is provided to the user to enter his details along with the biometric data. These data is sent to the authentication server which in turn allows the user to operate all his bank accounts with a onetime TAN generated by the server. This is an enhanced integrated system which provides a single interface for operating multiple bank accounts, uses smart card as a database to store the templates as well as encryption, hash function etc., and two servers namely Remote Authentication Server (RAS) and Remote Control Server (RCS) along with the mobile service provider. In addition to that we propose to use artificial intelligence on the RAS side for classification and identification of genuine users and fraudulent users.

General Terms

Multifactor authentication, multiserver, multi-Banking.

Keywords

Single interface, single Password, biometrics, smart card, Remote authentication server, Remote control server, multiple bank accounts, and Transaction authentication numbers.

1. INTRODUCTION

During the last few years, the scientific community is trying to improve biometric techniques to be accepted as an alternative to other user authentication schemes. One of the sectors where user identity must be verified is the identification cards sector. In fact, if great security wants to be achieved, smart cards should be used [1]. Tamper resistant technologies have been developed with the various applications of smart cards. Therefore we assume that the user could use the tamper resistant smart card in this paper. According to smart card alliance, today’s smart card technology is extremely difficult to duplicate or forge and has built-in tamper resistant smart card chips.

Biometric and smart card technologies provide highest security because those are defined as automated methods of identifying or authenticating the identity of a living person based on unique physiological or behavioral characteristics. Biometric technologies, when used with a well designed ID system, can provide the means to ensure that an individual presenting a secure ID credential has the absolute right to use that credential. Smart cards have the unique ability to store large amounts of biometric and other data. They also carry out their own On-card functions and interact intelligently with a smart card reader. Secure ID systems that require the highest degree of security and privacy are increasingly implementing both smart card and biometric technology [2].

Combining biometrics & smart cards delivers economic and security advantages like [2]

a. Enhanced Privacy.
b. Improved Security.
c. Improved ID system Performance.
d. Improved ROI.

Once an authentication server is compromised, the attackers perform an offline dictionary attack against the user passwords. Such attacks are going to be handled in our scheme by distributing the password database as well as the authentication function to multiple servers. If an attacker wants to perform an offline dictionary attack then more servers have to be compromised [3]. In this system authentication server will interact directly with the user initially and the original bank server will act as a control server behind the screen which interacts with the user after authentication.

Lot of research works are done in the area of securing online banking transactions and many architectures as well as systems have been proposed [7,15,18]. But when it comes to security still there is no perfect method or architecture. The proposed system is going to reduce the risk of remembering more number of passwords by providing a user interface which would request the user to enter the biometric data, list of banks he want to operate, user name and password. Also a combination of both facial and fingerprint biometric is used for authentication of user. The registration and authentication server will authenticate the user by matching the biometric data as well as the password provided by him. After that a onetime six digit TAN will be generated by the authentication server and that message will be sent to the user through a mobile device.

The authentication server will notify the user as well as all the banks which the user requests at the entry level interface by selecting the check boxes provided. He has to select the bank and enter his name as well as the received TAN to operate his/her account. This system is advantageous in the sense that only if the data provided by the user is genuine then only the data will be verified with that in the bank database.

We assume that secure transmission is going to happen with the help of Secure Socket Layer (SSL) as well as firewalls on both client side and server side. A complete three factor (biometrics, authentication servers, mobile service provider) authorization can be observed in this system and if implemented properly taking all the care it would be the better secure and easier one to enable the user to operate multiple accounts. One more benefit is that the confidential data is not available to attackers as everything will be in encrypted format. This is a system proposed to enhance the security in online multi-banking along with the feature of enabling user to access multiple accounts with a single password along with enhanced security. Awareness has to be created to the banks and users in order implement this system practically. The rest of the paper is organized in the following manner. In the section2 the interfaces designed for this purpose are presented. Section3 is the modeling process of I-MBS. Section4 deals with simulation and analysis of the system proposed using Petri nets. Section5 gives a conclusion, section6 is acknowledgementand section7 is references.

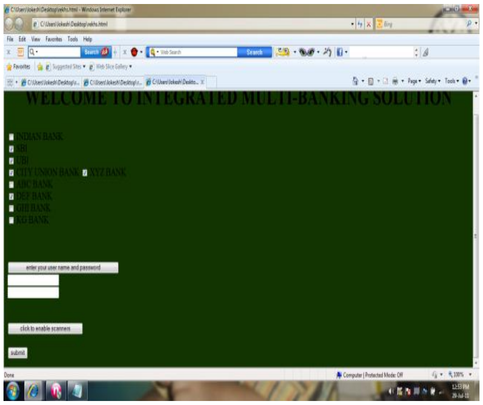
1.1 Motivation

As per the literature Single password, Multiple Accounts [5] is a scheme proposed by Mr.E.saravana kumar and Anupriya mohan which has motivated me to carry out this work. This proposed scheme allows a client to securely use a single password across multiple servers, attacks. In this system the user never reveals the password to the server at any time instead he generates a challenge as well as one time ticket and sends to the server on the basis of which the authentication will be done. Every time the database has to be updated with the new ticket because next time the user logins the server has to authenticate.

One more system is Independent Personal Financial Organizer (I-PFO) proposed by Annie Ai Bee Ng, Nasuha Lee Abdullah [18]. I-PFO is a web based application that allows users to easily organize and check their personal financial information from multiple banks using one log in. It is an integrated one stop solution for the user to pay bills or loans from multiple bank accounts. Apart from that it also track due dates and allow customization and personalization. Many challenges have been stated in designing the I-PFO. The most important is how to ensure security and others are regarding motivating the banks as well as users to subscribe to use that service.

2. INTERFACES OF THE PROPOSED SYSTEM:

Initially user registers himself/herself with the registration server. Then he would be provided with a username and password. Whenever he/she wants to login to operate his accounts, he has to select the list of banks he wants to operate in the provided list.



WELCOME TO INTEGRATED MULTI-BANKING SOLUTION

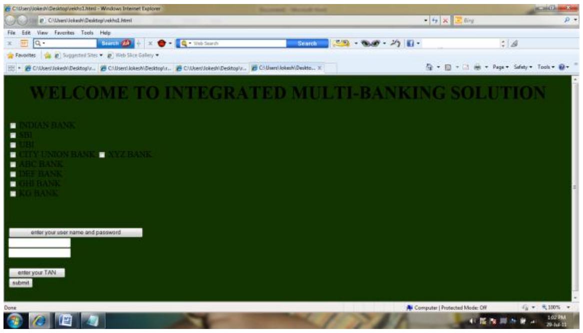
□ INDIAN BANK
☑ SBI
☑ UBI
☑ CITY UNION BANK ☑ XYZ BANK
□ ABC BANK
☑ DEF BANK
□ GHI BANK
□ KG BANK

C:\Users\lokesh\Desktop\rekhs.html - Windows Internet Explorer
File Edit View Favorites Tools Help
Search
Web Search
Favorites
Suggested Sites
Web Slice Gallery
Page Safety Tools
enter your user name and password
click to enable scanners
submit
Done
Computer | Protected Mode: Off
100%
12:53 PM
29-Jul-11

Figure 1. Initial Interface screen

After selection of banks, he/she has to provide his biometric data and also insert his/her card in a secure card reader. Once the data is submitted , it will be encrypted using the encryption function on the card and then both the data on card in encrypted format as well as currently obtained encrypted data will be sent to the Authentication server as shown in Figure 2. The server immediately performs the matching for the data received. If match is there then Transaction authentication number will be generated and will be sent to the user otherwise an error message will be sent. Along with the user the concerned banks would also receive the transaction authentication number from the authentication server.

.



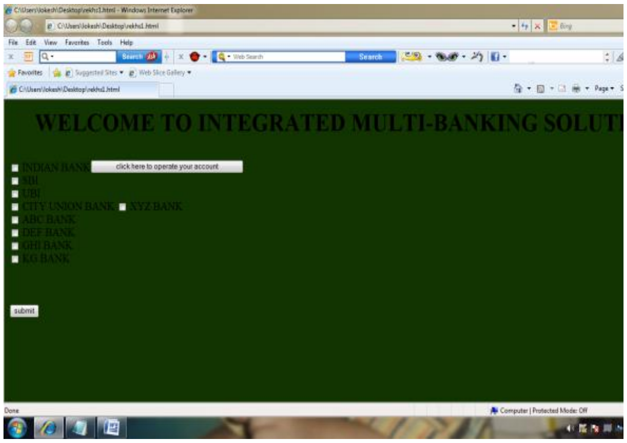
WELCOME TO INTEGRATED MULTI-BANKING SOLUTION

□ INDIAN BANK
□ SBI
□ UBI
□ CITY UNION BANK □ XYZ BANK
□ ABC BANK
□ DEF BANK
□ GHI BANK
□ KG BANK

C:\Users\lokesh\Desktop\rekhs1.html - Windows Internet Explorer
File Edit View Favorites Tools Help
Search
Web Search
Favorites
Suggested Sites
Web Slice Gallery
Page Safety Tools
enter your user name and password
enter your TAN
submit
Done
Computer | Protected Mode: Off
100%
1:02 PM
29-Jul-11

Figure 2: Second screen after receiving tan

Once the user receives TAN then he/she can start using his/her account by entering that number in the space provided as in figure 4. After that the data will be sent to the concerned bank servers, confirmation will be done by the server by once again cross checking the necessary information and then access will be allowed. If any deviation seems to be happened then the denial of access would be there.



WELCOME TO INTEGRATED MULTI-BANKING SOLUT

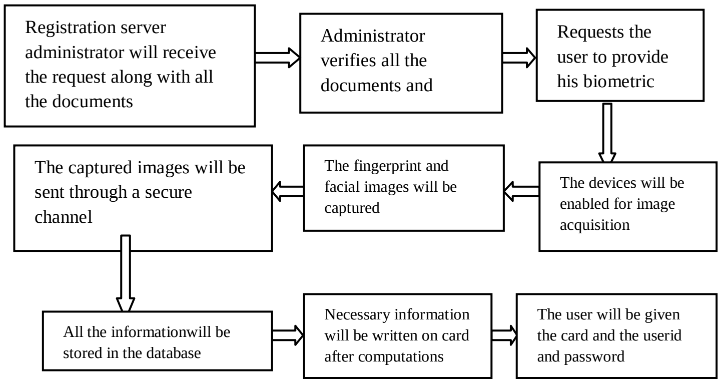
□ INDIAN BANK click here to operate your account
□ SBI
□ UBI
□ CITY UNION BANK □ XYZ BANK
□ ABC BANK
□ DEF BANK
□ GHI BANK
□ KG BANK

submit

C:\Users\lokesh\Desktop\rekhs1.html - Windows Internet Explorer
File Edit View Favorites Tools Help
Search
Web Search
Favorites
Suggested Sites
Web Slice Gallery
Page
Done
Computer | Protected Mode: Off

Figure 3: final screen before starting transactions

3. MODELING THE PROCESS OF I-MBS:

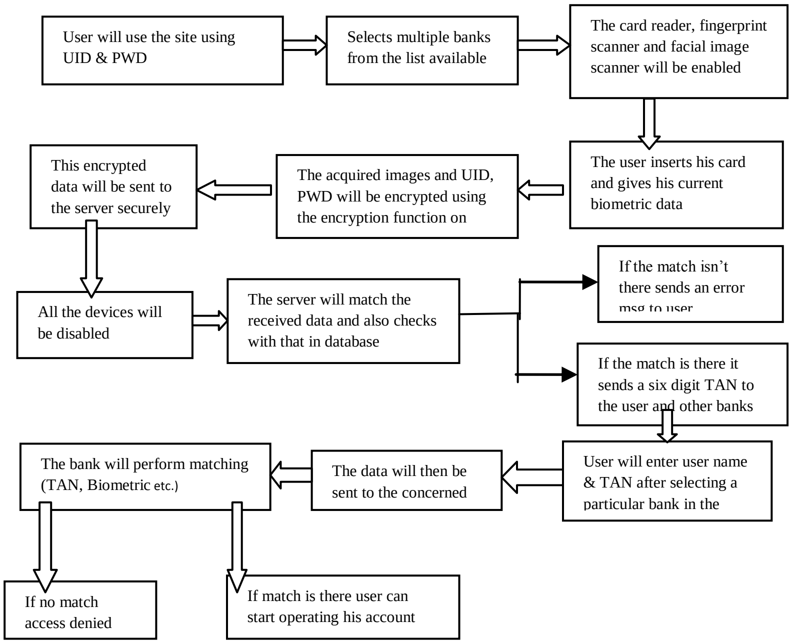


Registration server administrator will receive the request along with all the documents
Administrator verifies all the documents and
Requests the user to provide his biometric
The devices will be enabled for image acquisition
The fingerprint and facial images will be captured
The captured images will be sent through a secure channel
All the informationwill be stored in the database
Necessary information will be written on card after computations
The user will be given the card and the userid and password

Figure 4 modeling of I-MBS in the registration phase

In Integrated Multi-Banking Solution (I-MBS) the modeling have been done in two phases namely registration phase and login phase. As shown in the Fig4, in the registration phase a new user requests the administrator of the registration server by completing all the formalities required to be completed. User has to provide the biometric data along with the other details through a secure channel. Initially the administrator asks for all the documents like voterid, passport etc. Once user satisfies the criteria, the administrator will do computations as mentioned in the system description and write the necessary data on the card and sends that to the user through a secure means. In addition to that he will create a new user name and password for the user using which he can start using the services. The first operation will be carried at the registration time for the services. Administrator has to do the following steps:(a) ensure that all the documents have been submitted, (b) create new userid and password, (c) ask the user to provide his biometric features by enabling the capturing devices, (d) set the unique features as secrets like facial features, fingerprint featuresetc., for uniquely identifying the user in the database, (e) perform the various operations on the available data and write the necessary information on the card and issue it to the user.

In the login phase as shown in Figure 5 the following steps would be taking place: (1) user will provide his id & password along with selecting the list of banks to the RAS.(2) the scanners will be enabled through which user will give his biometric data (3) he inserts his card in a secure card reader (4) the captured data will be encrypted using the smart card and the data on the card as well as the captured data will be sent to the server (5) the server will receive the data and performs necessary matching (6) if the match is found to be correct then it will compute a six digit TAN and then send it to the user as well as to other banks which user has requested to operate (7) upon receiving the number the user can interact with all the banks he requested using his username and TAN (8) the bank will confirm the authenticity of the user by cross checking the information available(9)if the user is found to be genuine then he would be allowed to perform required operations on his account with the concerned bank.



User will use the site using UID & PWD
Selects multiple banks from the list available
The card reader, fingerprint scanner and facial image scanner will be enabled
The user inserts his card and gives his current biometric data
The acquired images and UID, PWD will be encrypted using the encryption function on
This encrypted data will be sent to the server securely
All the devices will be disabled
The server will match the received data and also checks with that in database
If the match isn't there sends an error msg to user
If the match is there it sends a six digit TAN to the user and other banks
User will enter user name & TAN after selecting a particular bank in the
The data will then be sent to the concerned
The bank will perform matching (TAN, Biometric etc.)
If no match access denied
If match is there user can start operating his account

Figure 5 modeling of I-MBS in login & transacting phase

4. SIMULATION AND ANALYSIS OF I-MBS USING PETRI NETS:

The simulation of I-MBS as shown in the figure 8 is done using the Petri nets. Petri nets were created in the 1960s by Carl Adam Petri (1962) to study complex, dynamic systems of communications among automatons. Here we are giving some information regarding Petri nets before using in our system. Their application has been expanded to various domains such as computer science, operational research, biology, and organizational management, including human–machine information system modeling (Meldman, 1977), supply chain performance modeling (Viswanadham & Srinivasa Raghavan, 2000), and online order processing modeling (Weitz, 1998). A complete overview of Petri net modeling of workflow systems has been done by Salimifard & Wright (2001). A Petri net is a graphically oriented language for system design, specification, simulation, verification and optimization. We use the petri net model for simulation of the I-MBS.

A Petri net is a triple N = {P, T, F}, where P is a set of places, T is a set of transitions, and F is a set of directed arcs. Places describe the states of the system and are graphically represented by circles. Transitions, represented as rectangles, describe the events that occur in the system. Finally, arcs describe how the Petri net changes when a transition occurs. A marking assigns token counts to the various places of the net; each place contains a positive (or 0) number of tokens.

4.1 Simulation of flow of data on client system

As shown in figure 6 initially user will start using the system and available devices. First the transitions used to represent the switch off state and then the tokens are indicated for the system interface, camera, fingerprint scanner and card reader which will go through a transition called switching on. Once everything is ready then the data will be captured and then transmitted to the server.

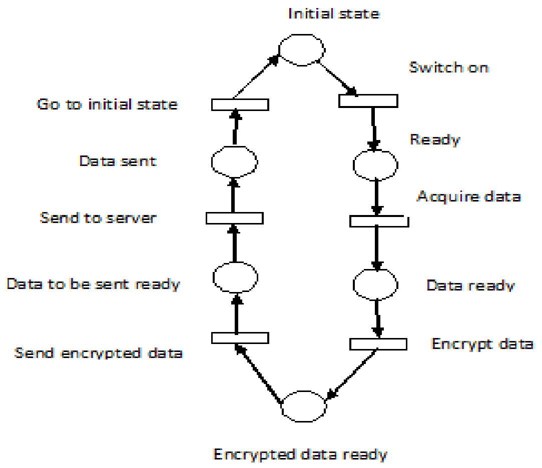


Figure 6 Simulation of process in the client system

4.2 Simulation of flow of data on authentication server system

As shown in the Figure7 the server will receive the information after ensuring that it is ready to receive information. The data which is received by the server will be splitted into different parts for the purpose of comparing the acquired data with the data on the card. Once the match is successful the next step is to verify the matched data with that in the server. Again if the match is successful then the TAN will be generated and will be sent to the user as well as the other banks which the user has requested to operate. The user can access and operate his desired account of any bank using that TAN and username from the next level onwards. At every failure stage if any mismatch is there the server will send an error message to the user so that again he can produce new data. Once if the user finishes resending the data for more than three times then his login will be disabled for the particular entire day. The requested banks will be notified with the TAN. So that immediately after receiving the data from the user requesting the services it will also cross check the information to ensure the authenticity. As per our analysis this system will give more comfort ability to the user who has multiple bank accounts along with not compromising the security anywhere.

4.3 Simulation of process in client system and authentication server system:

The system is assumed to be in the off state initially which is going to be switched on in next transition. The devices will be enabled later and customer provides his username, password, and biometric data through appropriate interfaces. The smart card is inserted into the card reader, and the data will be read. Encryption of the acquired data will be done using the function that is present on the card. Then the data in encrypted format will be sent to the authentication server. See Figure 8

After receiving the data the authentication server will split the data accordingly as shown in Figure 8. Match is performed between on card data and the current provided data. Verification will be done with the data that is there in the database if the match is found to be there, else an error message will be sent to the user. Again if match is there authentication will generate TAN and intimate the same to the user and banks, or else error message will be sent. Finally after receiving TAN user will start requesting the bank to provide services. Bank server in turn will cross check the information with that existing in their database and based on that user will be allowed to transact.

After the authentication server verifies the customer data and provides him TAN, the process will take place in between the customer and the bank. Initially bank will receive data from the customer and the authentication server. Once the required data is acquired then it verifies for the correctness of information received from both the parties. Then if the data is found to be correct it will be cross checked with that in their database, else it generates an error message and send it to user. Finally user will be allowed to perform required operations on his/her account. The entire process can be seen in Fig9

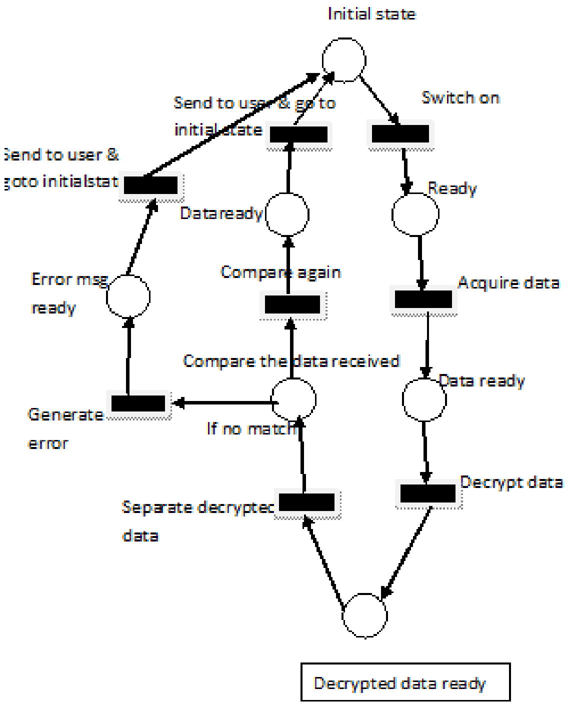


Figure.7 Simulation of process in the server

4.3.1 Places and Transitions used in Figure 8:

Places:

P1:user, P2, P3, P4, P5: Initial switch off state, P6, P7, P8, P9: Ready, P10, P11, P12, P13: Dataready, P14, P15, P16, P17: Data ready for transmission, P18: Server initial state, P19: On state, P20: Data received, P21: Data splitted, P22: Data on card, P23: Fringerprint & facial image, P24: Username & password, P25: Facial image on card, P26: fingerprint image on card, P27: Username on card, P28: Password on card, P29:Facial image acquired, P30: Fingerprint image acquired, P31: Username acquired, P32: Password acquired, P33: Match is not there, P34: If match is there, P35: Error generated, P36: Get data, P37: Data Requested, P38: If match is not there, P39: Error generated, P40: If match is there, P41: TAN ready, P42: Data to transmit received, P43: Data received, P44: data ready to be transmitted.

Transitions:

T1: Approach the system, T2, T3, T4, T5: Switch on the system, T6, T7, T8, T9: Get data, T10, T11, T12, T13: Encrypt data, T14: Transmit the data to server, T15: Switch on, T16: Receive data, T17: Classify, T18: Send data for comparison, T19: Again split data on card, T20: Split facial and fingerprint images, T21: Split username and password, T22: Compare data on card with captured data, T23: If match is not there, T24: Send the error message to the user system, T25: If match is there again with data in server, T26: Request data, T27: Sending request, T28: Generate error, T29: Send message to user,T30: Generate TAN and send to banks requested by user, T31: Transmit to user, T32: Transmit to banks, T33: Transmitting, T34: Process data send information to user server, T35: Sending, T36: Transmitting.

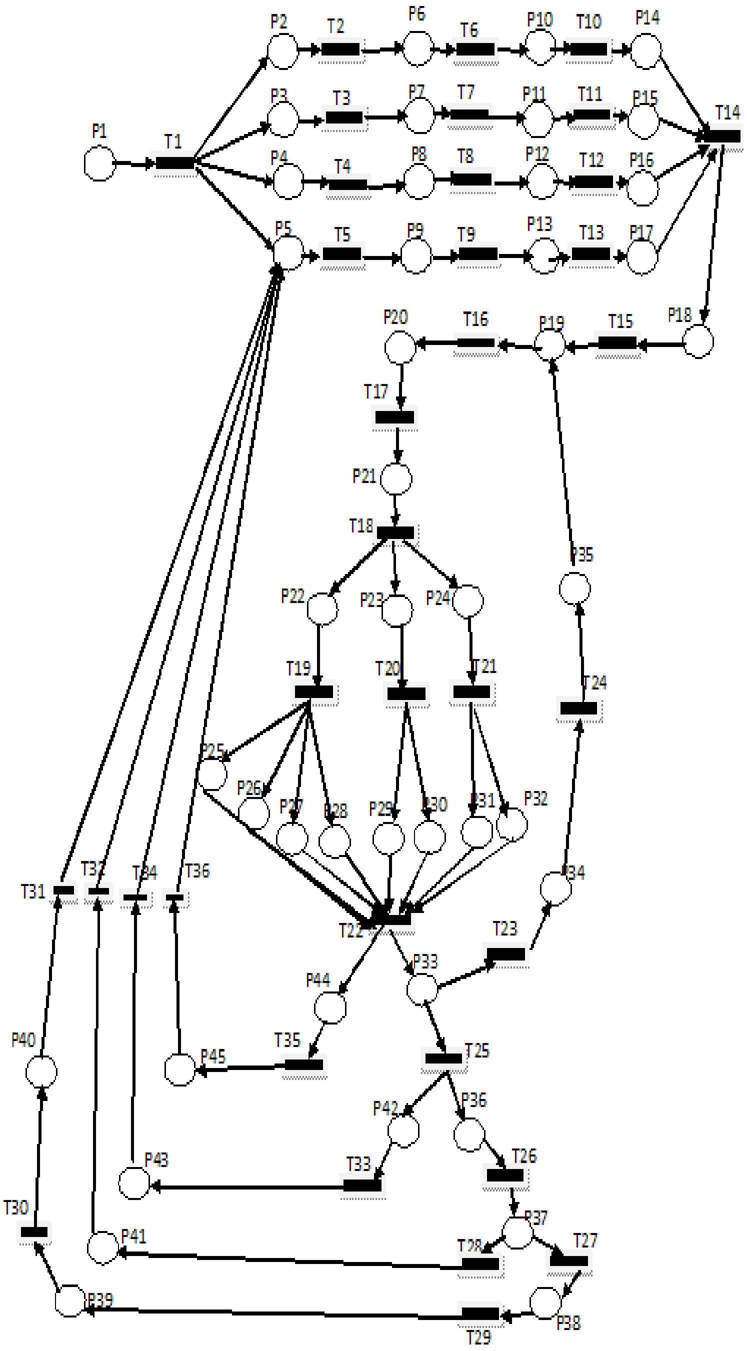


Figure 8: simulation of process carried out in client machine and authentication server

4.4 Simulation of process in Bank server system:

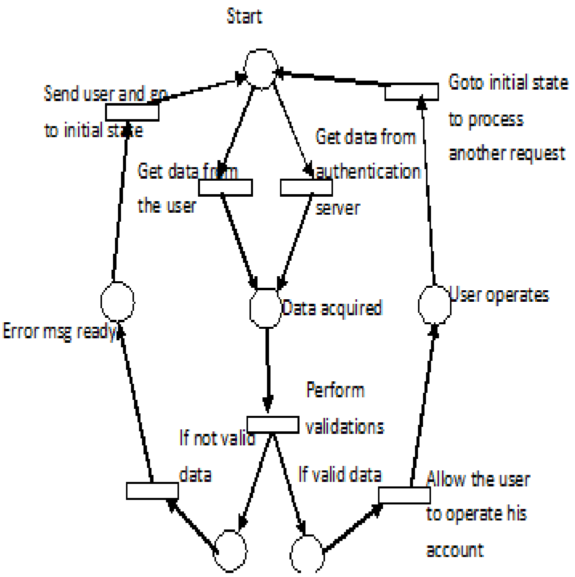


Figure 9: Process on bank server side

5. Graphical representation of proposed system compared to existing system:

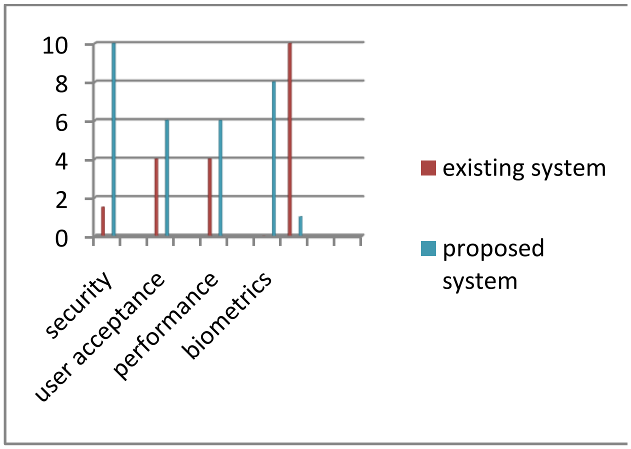


Figure 10:graphical representation of existing system compared with new system

In this graph we have indicated the various aspects related to existing system compared with the new system. The level of security is much better in new system comparitively. User acceptance is ralatively high in new system because more secure transaction is the one which everyone prefers. The performance will also be improved in new system. Whereas use of biometrics in existing system is almost nil, but in new system dual biometrics are proposed to be used. Finally last but not least the number of interfaces for transacting with ten banks for example will be ten in existing system. It will be one and the same interface in case of new system.

6. CONCLUSION

In recent years various sectors like e-banking, e-shopping etc., are facing the security threats regarding their transactional sensitivity and database sensitivity. We introduce an Integrated Multi-Banking Solution in order to enable the user's to operate multiple bank accounts at a time simultaneously with a single password i.e., TAN, without compromising the security at any stage. Moreover instead of storing all the information in one single server we propose to distribute among two servers namely Authentication server and Master server. In case if any of the server is compromised, then also an attacker cannot extract the data by dictionary attacks. And also our system can withstand other possible attacks because of the firewall protection on both client side as well as server side. Our system is very easy to implement and convenient to use. Enhancements can be done using stochastic petri nets, timed petrinets, colored petrinets etc.,

7. ACKNOWLEDGMENTS

Our thanks to the management and staff of PESIT who have encouraged us to carry out this work.

8. REFERENCES

[1] R. Sanchez-Reillo, L. Mengihar-Pozo C. Sanchez-Avila, Microprocessor Smart Cards with Fingerprint User Authentication, Aerospace and electronic systems magwzine, IEEE, volume 18, issue 3, p 22-24.

[2] Dexin Yang, Bo Yang , A New Password Authentication Scheme Using Fuzzy Extractor with Smart Card, Proc of International conference on computational intelligence and security, 2009.

[3] D. Bennet, Dr. S. Arumugaperumal, Fingerprint based multiserver authentication system, proc of 3rd International conference on electronics computer technology, 2011.

[4] Shirley GAW, Edward W. Felten, Password Management Strategies for Online Accounts, Symposium On Usable Privacy and Security (SOUPS) 2006, July 12-14, 2006, Pittsburgh, PA, USA.

[5] Mr. E. Saravanakumar, Anupriya Mohan, Single Password Multiple Accounts, Proceedings of the 2008 International Conference on Computing, Communication and Networking (ICCCN 2008)

[6] Art Conklin, Glenn Dietrich, Diane Walz, Password-Based Authentication: A System Perspective, Proc of the 37th annual hawaai international conference on system sciences, 2004.

[7] Dexin Yang, Bo Yang ,A Biometric Password-based Multi-server Authentication Scheme with Smart Card, proc of International conference on computer design and applications,2010.

[8] Yanjiang Yang, Feng Bao, Password Protected Credentials, Proc of International conference on multimedia information networking and security, 2010.

[9] Qiang Wang, Zhiguang Qin, Stronger User Authentication for Web Browser, Proc of 3rd International conference on advanced computer theory and engineering, 2010.

[10] D. Bennet, Dr. S. Arumugaperumal, Fingerprint Based Multi-Server Authentication System, Proc of 3rd International conference on electronics computer technology, 2011.

[11] Jennifer R. Kwapisz, Gary M. Weiss, and Samuel A. Moore, Cell Phone-Based Biometric Identification, Proc of 4th IEEE conference on Biometrics: Theory, systems and applications (BTAS), 2010.

[12] Dexin Yang,South, Bo Yang, Woei-Jiunn Tsaur , Chia-Chun Wu , Novel Two-Server Password Authentication Scheme with Provable security, Proc of 10th International conference on computer and information technology, 2010.

[14] Yanjiong Wang 1, Qiaoyan Wen, Hua Zhang, A Single Sign-On Scheme For Cross Domain Web Applications Using Identity-Based Cryptography, 2nd International conference on network security wireless communications and trusted computing, 2010.

[15] Sahana K. Bhosale, Architecture of a Single Sign on (SSO) for Internet Banking , proc of International conference on wireless mobile and multimedia networks, 2008.

[16] Jianhong Zhang, XueLiu, On the Security of An Identity-based Single-sign-on Scheme, Proc of 3rd IEEE international conference on computer science and information technology, 2010.

[17] Eun-Jun Yoon, Kee-Young Yoo, Robust Multi-Server Authentication Scheme, 6th IFIP International conference on network and parallel computing, 2009.

[18] Annie Ai Bee Ng, Nasuha Lee Abdullah, Security Challenges in Designing an Integrated Web Application for Multiple Online Banking, International symposium in information technology, 2010.

[19] V C Subbarayudu and Munaga, V N K Prasad, Multimodal Biometric System, Proc of first international conference on emerging trends in engineering and technology, 2008.

[20] Sebastian Rieger, Gesellschaft für, Using Federated Identities to access IP-protected Web Resources in Multi-Customer Environments, 5th International conference on internet and web applications and services, 2010.

[21] Yanjiang Yang, Feng Bao, Enabling Use of Single Password Over Multiple Servers in Two-Server Model, Proc of 10th International conference on computer and information technology, 2010.