An Architecture for Integrated Multi-banking Solution

G.Sree Rekha, and V. K. Agrawal

***Abstract*—**In this paper we 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 literature which is 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 the purpose of classifying and identifying the biometric data received by the server.

***Keywords*—**Artificial intelligence, multiple servers, single password, single interface.

I. 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 need 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 and 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, and 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

Sree Rekha G is with the PES Institute of Technology, Bangalore, Karnataka, 500085, INDIA (phone: 080-26721983 e-mail: sreerekha@pes.edu).

V. K. Agrawal was with ISRO, Bangalore, INDIA. He is now with the Department of Information science and Director of R&D in PES Institute of Technology, Bangalore, Karnataka INDIA 500085 (e-mail: vk.agrawal@pes.edu).

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 paper is organized in the following manner. In the section 2, we give the architecture of the proposed system, section 3 deals with the interfaces of the system, section 4 gives details of the modeling process of I-MBS, section 5 deals with the simulation and analysis of I-MBS, section 6 is the conclusion.

A. Motivation

As per the literature, Single password Multiple Accounts is a scheme proposed by Saravana and Anupriya Mohan [5] which has motivated us 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 log in, 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 tracks due dates and allows 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.

II. The Architecture of the Proposed System

The architecture of proposed system would comprise of remote authentication server, multiple bank servers, multiple users, mobile devices, multiple databases and a mobile service provider. On one hand, before providing services, the remote server should have abilities to authenticate users, otherwise an adversary can impersonate a legal user login and get access of services. On the other hand, before accepting the services provided by the remote server, the user should have abilities to authenticate the remote server, otherwise an attacker can forge a legal server [2].

In this architecture, multiple users from various terminals would interact with the authentication server. Remote Authentication Server (RAS) plays a vital role in authenticating the user after receiving the required data. Only if the data on card and acquired data are matched, then only the server database will be accessed. For matching the information we use artificial intelligence with a combination of set of programs and algorithms.

Once authentication is perfect, then the data will be matched with that in the database. The database would be containing the biometric data, username etc., this further lead communications to happen between authentication server, user and banks. Mobile service provider will transmit the one-time number generated by the authentication server to the user. The mobile devices of the user's will receive the number. User has to make use of the number received again to gain access to the banks data.

Banks would be maintaining their own independent databases for the purpose of cross-checking.

III. 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.

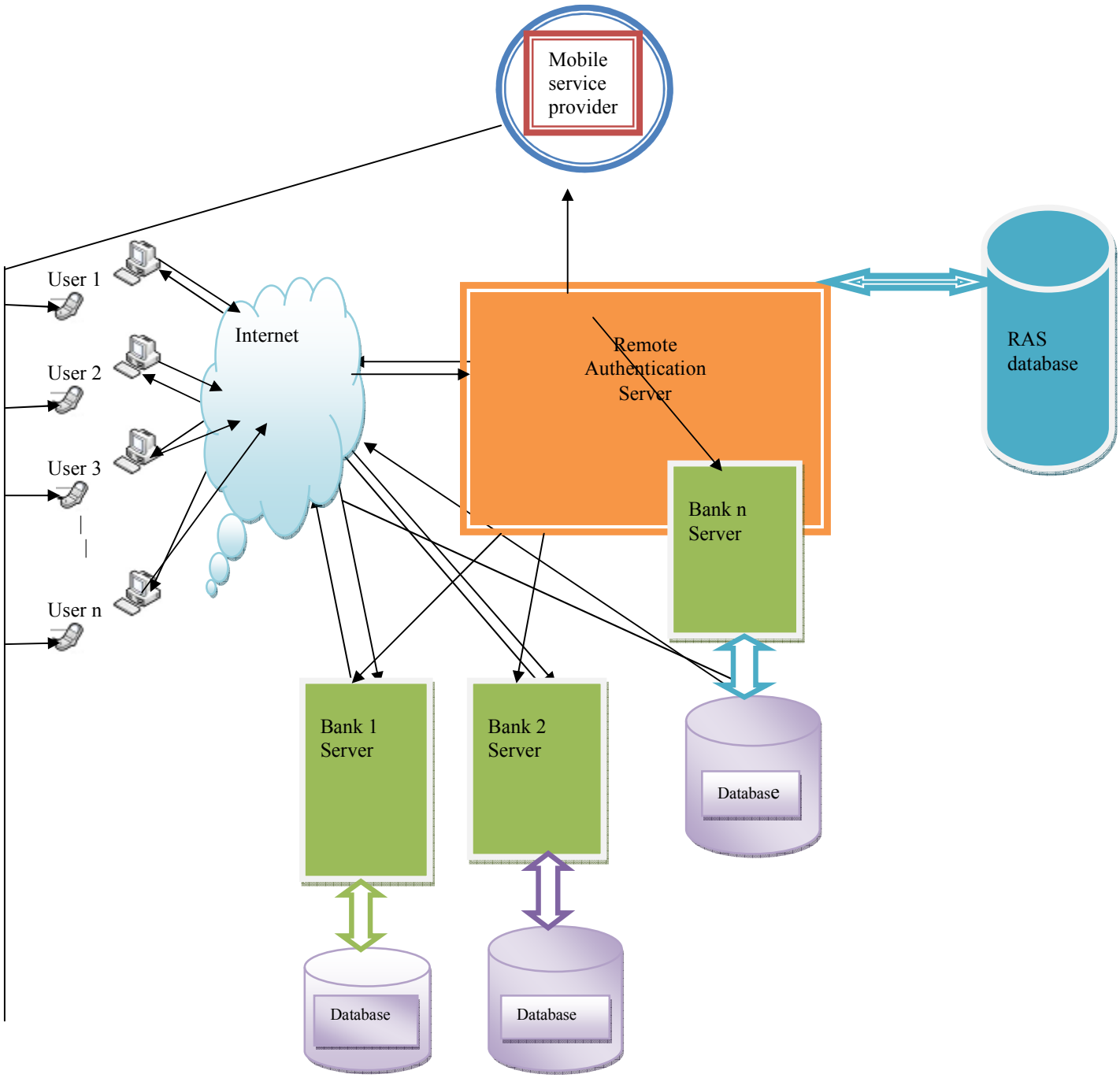

Fig. 1 Architecture for Integrated multi-banking solution

Fig. 2 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. The server immediately performs the matching for the data received. If match is accurate, then Transaction authentication number will be generated and 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.

Fig. 3 Second screen after receiving tan

Once the user receives TAN, then he/she can start using his/her accounts by entering that number in the space provided as in fig4. 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 happen the access would be denied.

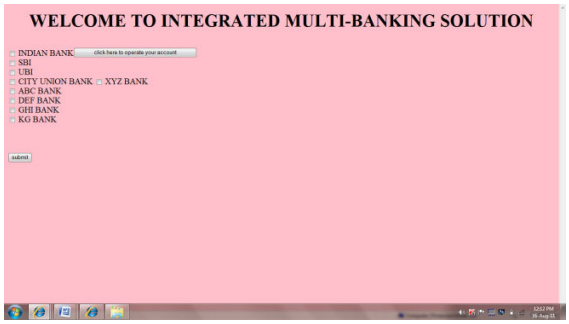

Fig. 4 Final screen before

IV. Modeling the Process of I-MBS

In Integrated Multi-Banking Solution (I-MBS) the modeling have been done in two phases: namely registration phase and login phase. 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 voter Id, 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 as shown in Fig. 4. Administrator has to do the following steps: (a) Ensure that all the documents have been submitted, (b) Create new user Id and password, (c) Ask the user to provide his biometric features by enabling the capturing devices, (d) Set the unique features such as secrets like facial features, fingerprint features etc., 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.

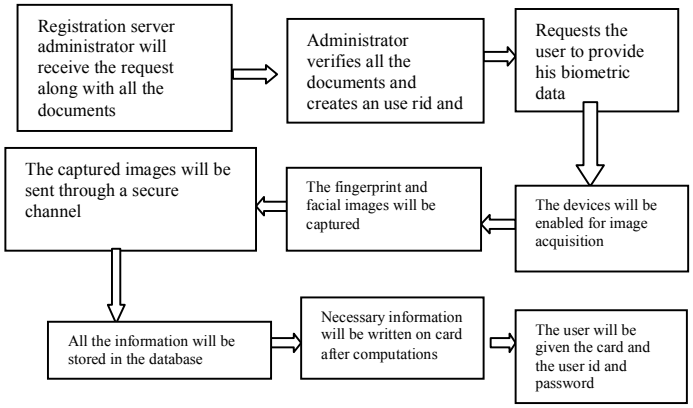

Fig. 5 Modeling of I-MBS in the registration phase

In the login phase as shown in Fig. 6, 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..

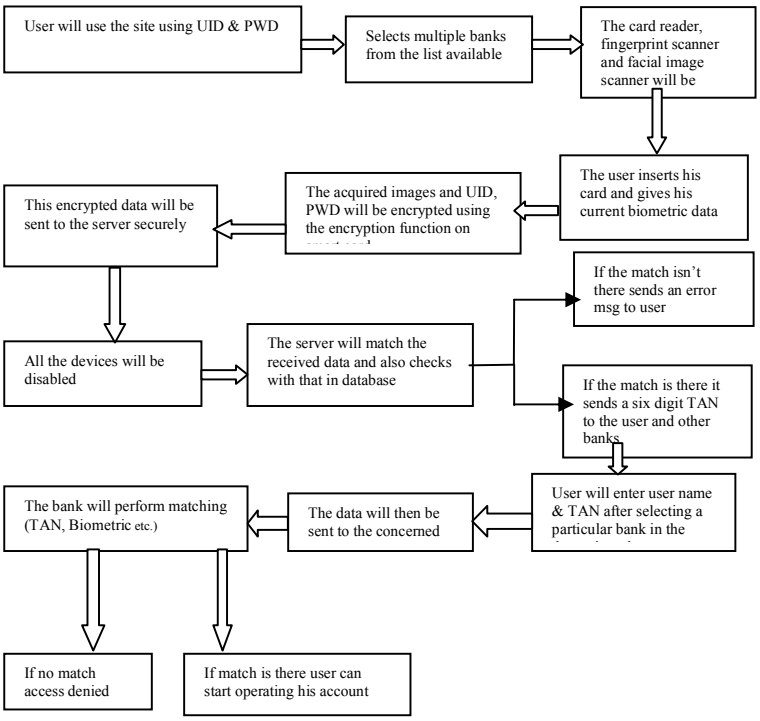

Fig. 6 modeling of I-MBS in login and transacting phase

(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

V. Simulation and Analysis of I-MBS using Petrinet Framework

The simulation of I-MBS as shown in the Fig. 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.

A. Simulation of Flow of Data on Client System

As shown in Fig. 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 to the server.

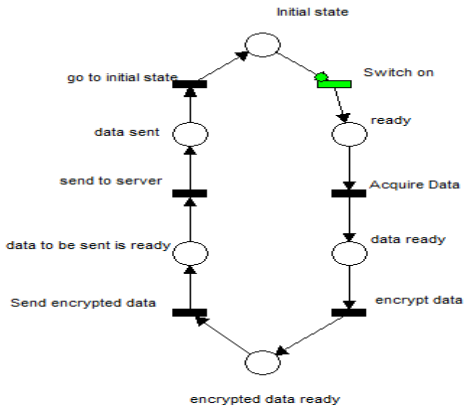

Fig. 7 Simulation of process in the client system

B. Simulation of flow of data on authentication server system

As shown in the Fig. 8, 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 split 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 stage if there is any mismatch, 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 comfortability to the user who has multiple bank accounts and at the same time not compromising the security anywhere.

C. Simulation of Process in Client System and Authentication Server System

Initially on the client side, the system assumed is in the off state which is going to be switched on in next transition. Later the devices will be enabled 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. The acquired data will be encrypted using the function that is present on the card. Then the data in encrypted format will be sent to the authentication server. See Fig. 9.

The authentication server after receiving the data will split the data accordingly as shown in Fig. 9. Then match is performed between on card data and the current provided data. If match is there then once again it will be verified with that in the database, or 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.

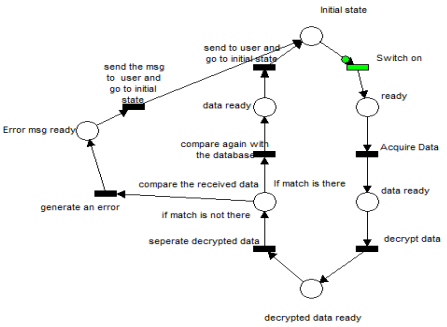

Fig. 8 Simulation of process in the server

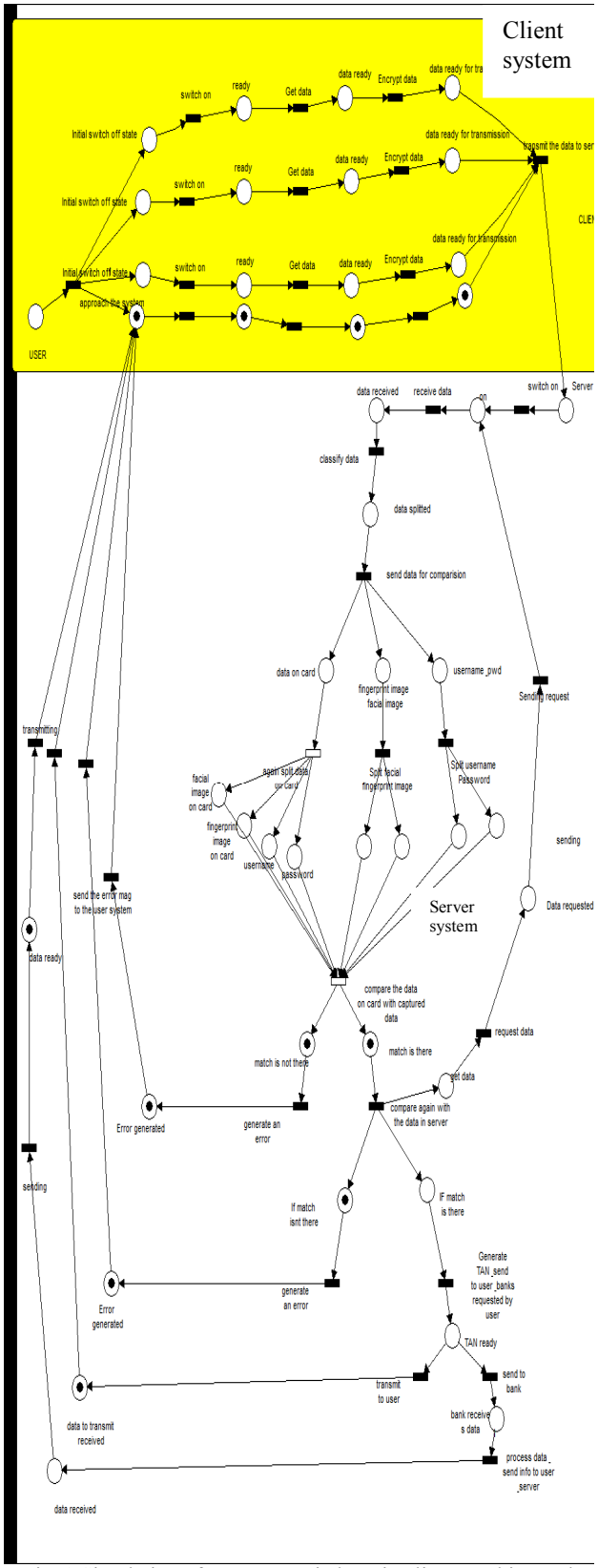

Fig. 9 Simulation of process carried out in client machine and authentication server

D. Simulation of Process in Bank Server System

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 sends it to user. Finally user will be allowed to perform required operations on his/her account. The entire process can be seen in Fig. 10.

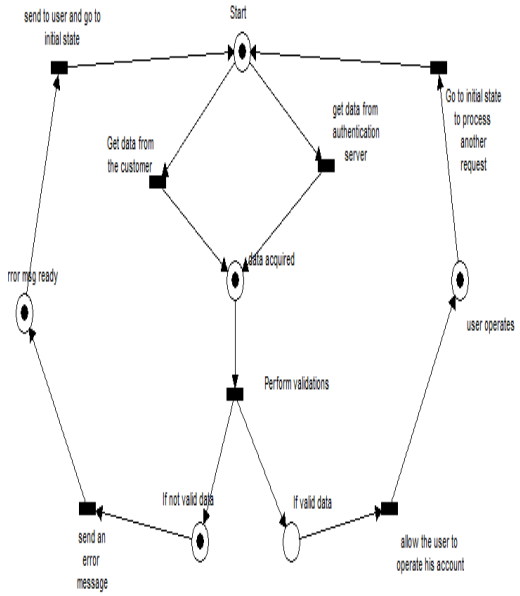

Fig. 10 Process on bank server side

VI. 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 petrinets, timed petrinets, Colored petrinets etc.

Acknowledgment

We would like to thank our college management and staff for extending their continuous support for us to carry out this part of work successfully.

References

[1] R. Sanchez-Reillo, L. Mengihar-Pozo C. Sanchez-Avila, Microprocessor Smart Cards with Fingerprint User Authentication, Aerospace and electronic systems magwzine, IEEE, vol. 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. Benet, 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] 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.

[11] 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.

[12] 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.

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

[14] 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.

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

[16] 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.

[17] 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.

[18] 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.

[19] 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.

Sree Rekha G is working as an asst. prof. in PES Institute of Technology, Bangalore. She has 3 years of teaching experience and 1 year of research in that. She graduated from S. V. University, Tirupathi in 2005 and obtained her masters in 2008, Master of computer applications from the S.V. University, Tirupathi. Her area of interests are biometric based online banking security, Web banking service integration and web banking security enhancement.

Prof.V.K.Agrawal worked in ISRO, Bangalore for more than 30 years and he recently joined as the Director, R&D department of PESIT and also Professor in ISE Dept. He has obtained his PhD from IISC Bangalore in 1983. His area of interests is embedded systems and information security.