Journal of Internet Banking and Commerce

An open access Internet journal (http://www.arraydev.com/commerce/jibc/)

Journal of Internet Banking and Commerce, April 2012, vol. 17, no. 1
(*http://www.arraydev.com/commerce/jibc/*)

AN APPROACH FOR COMMON INTERFACE FOR MULTIPLE ONLINE BANKING (CIMOBM)

Sree Rekha Gurajala
Assistant Professor MCA Department and Research Associate R&D (CORI),
PES Institute of Technology, Bangalore, India
Postal Address: **100 Feet Ring Road, BSK 3rd Stage, Bangalore - 560085, India**
Author's Personal/Organizational Website: ***www.pes.edu***
Email: ***sreerekha@pes.edu***
Mrs.Sree Rekha is an Assistant Professor in PESIT, Bangalore, India. Her areas of interest are Web Banking Security, Information security in multiple online banking, Architectural and protocol design & analysis.

V.K.Agrawal
Professor ISE Department and Director R&D(CORI),
PES Institute of Technology, Bangalore, India-560085
Postal Address: **100 Feet ring Road, BSK 3rd Stage, Bangalore, 560085,India**
Author's Personal/Organizational Website: ***www.pes.edu***
Email: ***vk.agrawal@pes.edu***
Dr. Agrawal is a Professor of Information Science Engineering in the PES Institute of Technology, Bangalore, India. His current research interests are on Information security, Software and hardware architectures, Software engineering, Embedded systems and Power systems for LEO satellites. He has published many papers in various prestigious journals such as IEEE, International journal of computers and applications, International journal of embedded systems etc.,

Abstract

This research work was initiated with a main objective of providing progressively higher degree of security in online banking (web banking) for future generation Internet banking. The underlying knowledge models are represented using petrinet formalism in all the phases and systems. The plan is also represented using petrinets. Hierarchical timed petrinets (HTPN) is used for our modeling, since it captures the temporal requirements of the real time online banking operations as well as facilitates the modeling of the large-scale system with multiple levels of abstraction. The necessary primitives for the plan representation including concurrency, synchronization, temporal, activity sequencing, mutual exclusion, resource constraints and decision making actions are defined using petrinet constructs. The static and dynamic actions as well as resource modeling are illustrated using timed petrinet model, developed using HPsim tool. Planning a petrinet framework is one of the easy understandable ways of representing complex problems and various issues involved. We have presented some simulation models for representing the complex web-banking model which is common for multiple banks.

Keywords: **Multiple online banking, Petrinet based simulation, Hierarchical Timed Petrinets, Multi-server architecture.**

INTRODUCTION

Online banking operations refer to all the operations that are related to online banking activities. It can be represented as a dynamic process affected by various random factors. One of the major goals for simulations of online banking operations is to facilitate enhanced security, transaction authenticity, efficiency of the system and customer benefits. The future of internet banking will be represented in one single interface that support mobile, internet banking and electronic fund transfer transactions of multiple banks. This facility would enable to cover all the types of applications demanded at the market level.

We propose a system that uses a combination of biometrics and graphical image based passwords for the purpose of authentication along with a common interface for transacting with multiple banks online. The graphical password claims to be superior to text-based password because humans can remember pictures better than text [1].

One more aspect of consideration in our proposed system is the number of factors that are to be considered for the authentication of a user. Two-factor authentication raises some new challenges in the area of usability such as (a) Two-factor authentication is not standardized, (b) At the same time, the same authentication factor employed by different institutions is not necessarily inter-operable. As the result, usually users are expected to remember dozens of unique passwords and carry multiple physical items as the second authentication factor.
As per the content available in the literature, image based password authentication for online transactions is considered to be secure. Authentication that is based on graphical

images comes in the form of two images, one is Password image and the other is key image. Key image is a copy of password image that is always encrypted and signed by challenges and can be validated and decrypted on user's handheld device. The key image contains enough information to show the click spots to the owner of handheld. The user's password is the click points and their order [1].

Graphical password scheme appear to solve the key-logger software on the client side, which will record keystrokes for identifying and guessing the passwords, by replacing the keystrokes with clicks. However, unfortunately graphical password schemes do remain susceptible to more sophisticated attacks such as screen recording. Attackers can use the captured clicks to mount a single access attack [1].

We propose a combination of graphical image based password and the biometric authentication to enhance the security and effectively use the image based passwords in online banking applications.

OVERVIEW OF COMMON INTERFACE FOR MULTIPLE ONLINE BANKING (CIMOBM)

The proposed common interface for multiple online banking model consists of a novel architecture which encompasses the single interface for transacting with multiple banks online. This is basically a graphical image based password authentication system which uses biometrics for the purpose of identifying the genuine user. This work is an extension to the work done in " An Architecture for integrated multi-banking solution".

In this Common multi-banking system, the complete three-factor authentication is proposed to be done to ensure the security aspect. Some of the general objectives of online security can be as follows:

- Confidentiality
- Availability
- Accountability
- Integrity

In order to ensure all the above-mentioned security objectives one has to design a system in such a way that it employs all the advanced mechanisms for authentication as well as authorization. Our proposed model is a sophisticated one that withstands most of the attacks like man in the middle attack, key-logger software attack, screen recording attack etc.

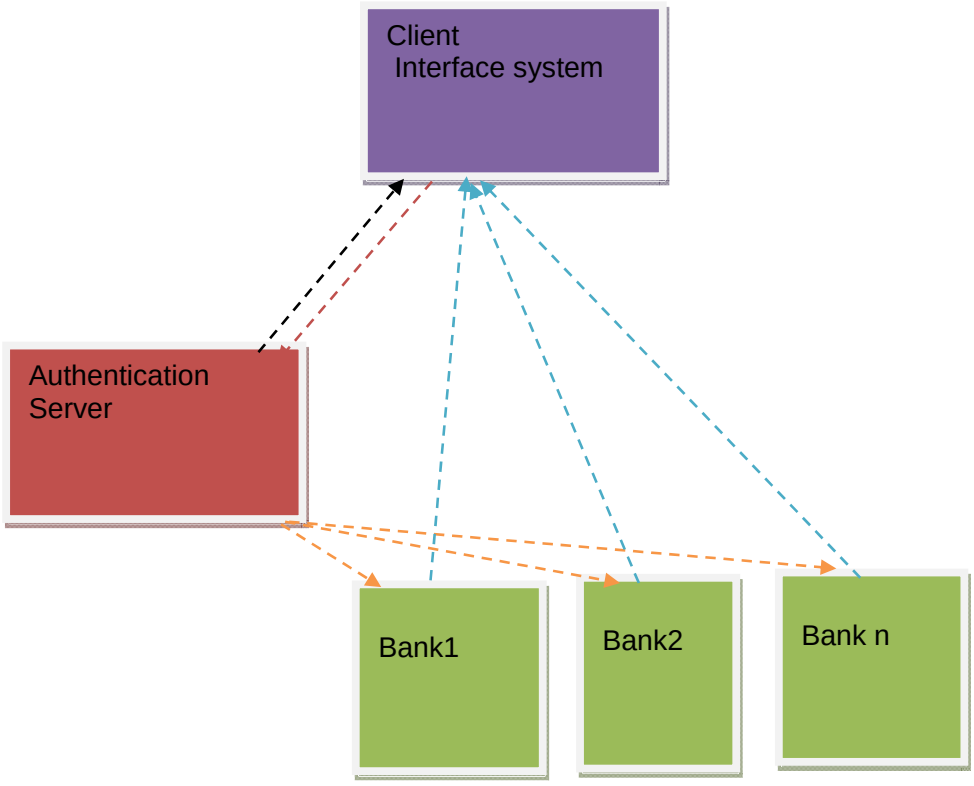

Figure 1: Formal Model of Common multi-banking solution

COMPONENTS OF CIMOBM

The major components in the proposed system are as follows:

Facial image scanner:
Facial image scanner is one of the components of the proposed model. The purpose of this is to take the image of the face which is present in front of the screen.

Fingerprint scanner:
This is a small USB device which is used for the purpose of obtaining the fingerprint image from the user. The fingerprints are most widely used means of authenticating a user and therefore we propose to use fingerprint scanner for getting the fingerprints from the user.

Client system:
Client system is one which is used by the user for the purpose of performing the online banking transaction with the bank. It can be a PC, a laptop.

Server system:
Server system here means the bank servers which will be containing all the information regarding their customers and also the transactions that are being done by them.

Central authentication system:
Central authentication system is one which performs the process of authenticating a user and notifying the banks for the provision of the services to a particular customer.

Image matching algorithm:
The success factor of any pattern recognition or facial recognition would depend upon the algorithm which we are going to use. So an effective image matching algorithm is a must.

Internet:
Internet and online banking are becoming synonyms these days and one cannot exist without the other. A secure internet connection is a must for secure online banking transaction.

Common interface:
The specialty of the proposed system is the commonality in interacting with multiple banks. So a common interface through which a user can interact with his/her multiple banks accounts and perform transactions is needed which is developed for the purpose.

The above mentioned components are all essential for our proposed model. The level of importance that is proposed to be given is represented graphically as an approximation. Client side system would be consisting of scanners which will capture the images and then send to the central authentication system for further processing. Once the authentication is done successfully, then the information will be communicated to the server which would enable the user to proceed further in carrying out his/her transactions.

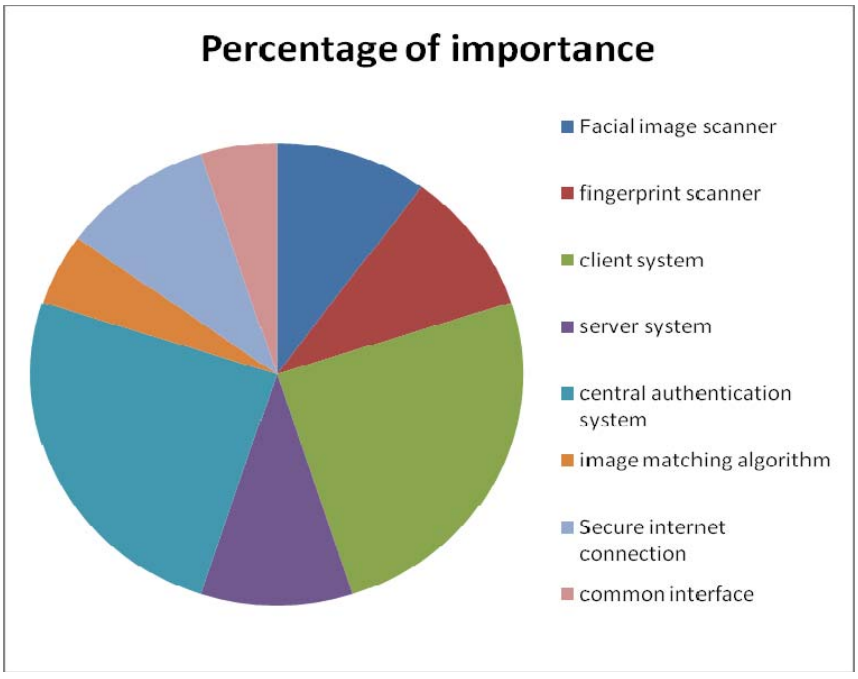

Figure 2: Percentage of importance of each component

WORKING MECHANISM OF CIMOBM

The working mechanism of the common interface for multiple online banking during registration phase is as follows:
Initially the user has to register with the registration server.
He/she has to submit the required biometric data i.e., facial image and fingerprint.
Once the data is submitted, the registration server will give the list of images from which user has to select one.
All these data provided by the user will be stored in the authentication server's database for future verification
User will be given username with which he can start using the system from the next session.

After registering successfully to the server user can follow the below mentioned steps for transacting online:

User has to enter his/her username, by entering into the site.
Once the username is valid, he/she will be asked to provide his/her biometric data.
The authentication server will validate the data received.
Once if it is found to be matching, then authentication server will send the list of images which were given at the time of registration to the user. User has to select the one which he/she selected earlier at the time of registering.
Again the information provided will be evaluated. If it is found to be genuine then the user will be given an encrypted image which consists of numbers placed on it. He/she has to click on those numbers and that will be the password for that particular session. If data is not found to be correct then the user will be given an intimation that incorrect data will be sent to the user.
After successful completion of authentication formalities by the user, he/she will be directed to use his/her multiple bank accounts and transact online.

PETRINET BASED WORLD MODELING

Planning a petrinet framework is a problem of finding the sequence of transition firing from the initial state to the goal state, which is essentially, is the sub-marking reach ability problem.
The CIMOBM model pertaining to the independent system is grouped into four categories and each category has to be clearly understood for the purpose of modeling the overall system successfully. Planning knowledge is considered to be the primary and the authentication and authorization knowledge is the key for ensuring the performance of the proposed system.

1. Planning knowledge
2. Control knowledge
3. Authentication & Authorization knowledge
4. Diagnostic knowledge

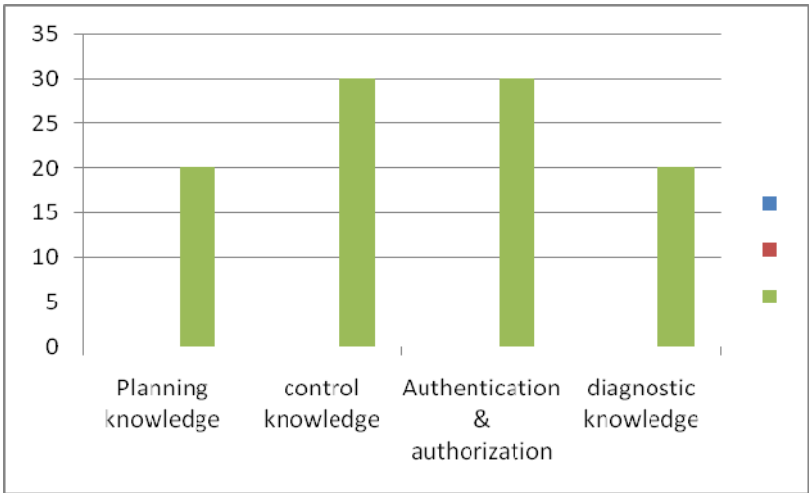

Figure 3: Level of knowledge required

1. Planning knowledge:

This planning knowledge describes the high-level goals and the method of achieving the goals. The knowledge regarding the long-term goals and information regarding how they are decomposed into sub-goals is required by the planning agent who is going to operate in a long-term horizon. The required task structure has to be determined in order to achieve the goals. One more information that is being included in this planning task knowledge is the various methods available, when alternate methods are available and also how to select from the alternatives.

2. Control knowledge:

This would encompass both static and dynamic knowledge. The architecture of the system including various subsystem and components, their function, constraints and relationships will be covered in static knowledge. The various modes of operations, the dynamic behavior over time, the resources available, the state and their transitions would be represented by the dynamic knowledge.

3. Authentication & Authorization knowledge:

The basic knowledge required for authentication is the strong database information. Authentication mechanisms which are widely used would be studied and the selection of the best methods for authenticating will be investigated. Authorization is required for allowing only the genuine user to use or interact with the system.

4. Diagnostic knowledge:

Fault diagnosis is nothing but the set of failures and the relationship between the observations and failures. The cause-effect relationship is described by this.

The online banking models are represented hierarchically across the different layers. Hierarchical modeling aspects and the hierarchical planning process using petrinets are discussed in the following section.

The diagnostic knowledge is required for analyzing the root cause of any failures/deviations. The uniqueness of require a separate knowledge representation for performing diagnosis.

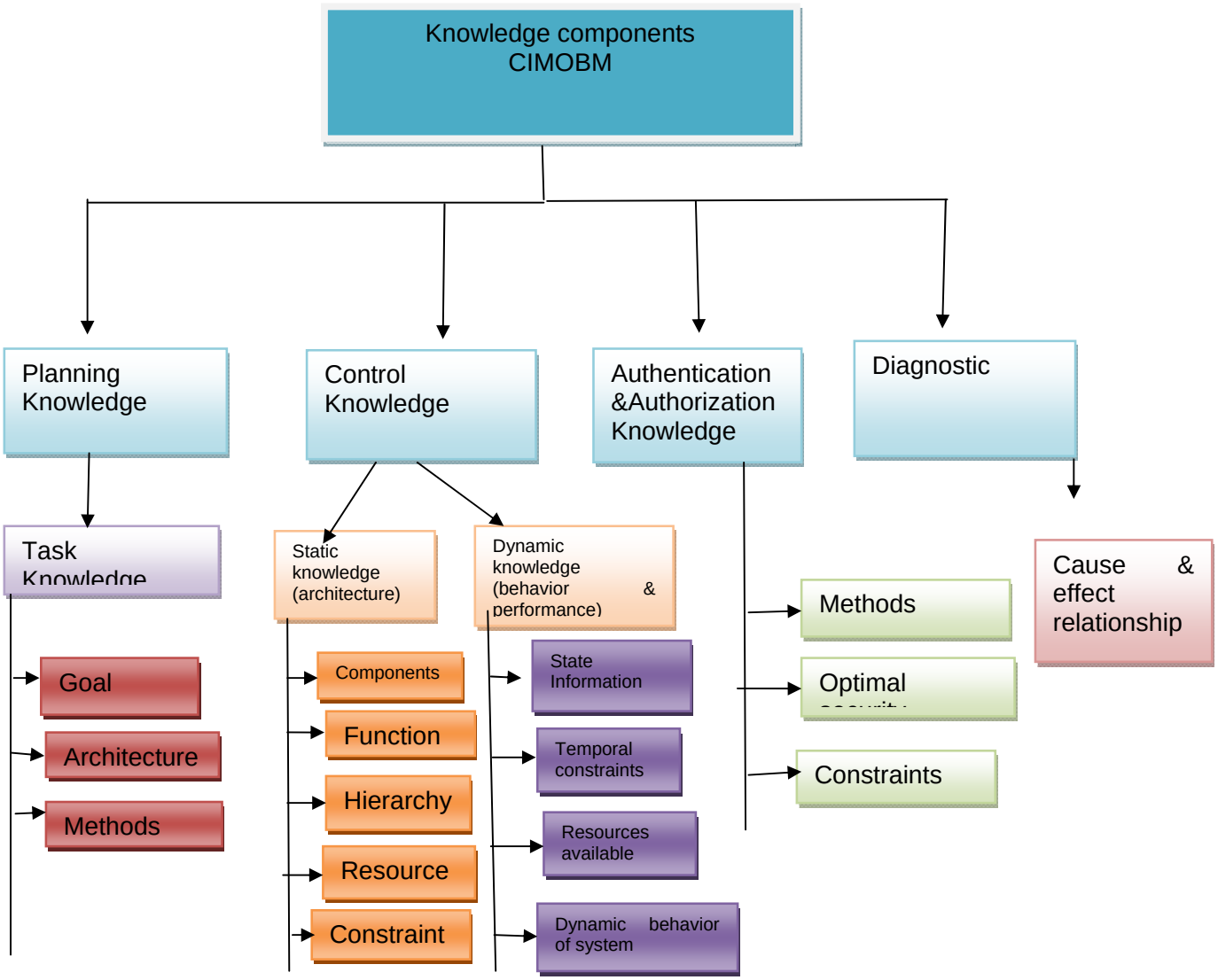

Figure 4: Various knowledge components analysis

SIMULATION OF THE PROPOSED SYSTEM

We simulate the process in order to ensure that uninterrupted flow of data is going to be there and wherever the authentication is needed, it is going to be done properly. It also emphasizes what happens if in a particular place the required action is not taking place, i.e., the alternative path would be taken for further flow.

The assumed process during the registration as shown in figure 5 would be as follows: Initially the user has to send a request to the server requesting username. The server after receiving the request, again ask for the further information like other details, biometric data etc. Once the user provides the information, the server sends a list of images to the user. The user has to select one among the list and send back to the server. The server then stores all the information in its database.

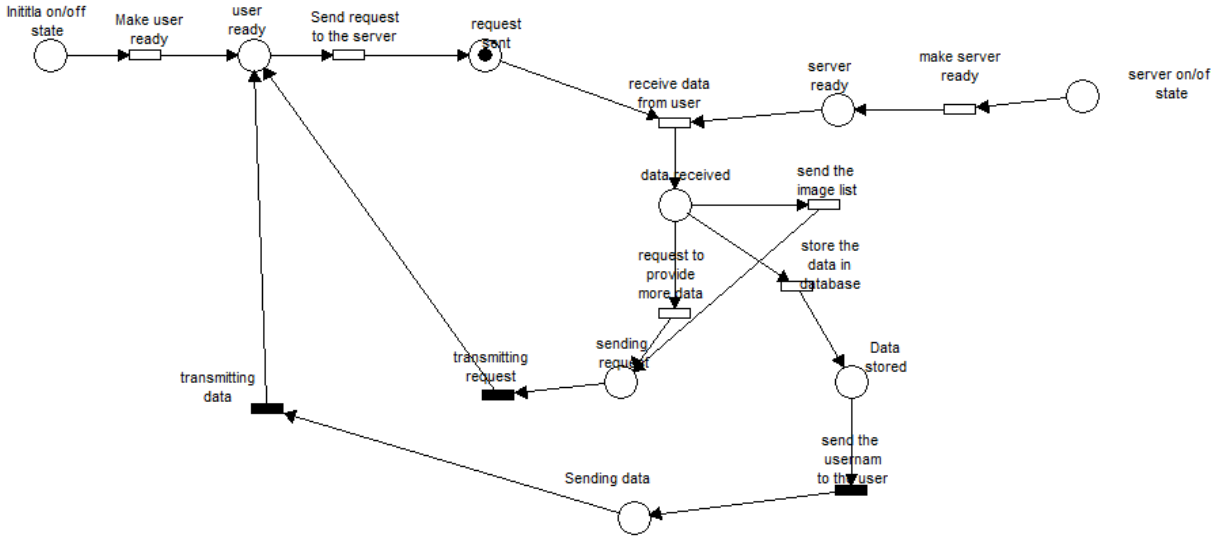

Figure 5: Simulation of process during registration phase

After running the simulations for a particular period of time we have observed that the flow of data from one state to another is as expected. As we have set time for each and every transition, particular event was happening only when the corresponding one is finished. Thus we can ensure the successful registration phase.

Once the registration is successfully completed then the user can start operating his/her account online anytime. The process that is to be followed while operating online as shown in figure 6 would be as follows: Initially the user starts operating the system by entering this username. The authentication server will ask for the additional information. After being provided information by the user, the authentication server ensures that it is genuine information by comparing it with those in the database. If a match is found to be there, then the server generates a list of images corresponding to that user which is stored in the database. Again user has to select the same image which he/she has selected at the time of registration.

If the image is found to be correct, then the server generates an image which consists of encrypted password.
The image will be sent to the user, and he has to click on the points present on the image, the sequence of which will be the password for that particular session.
Simultaneously, the authentication server will also send the intimation to all the banks requested by the user to provide their services to particular customer as he/she is an authorized person to operate his/her account online.

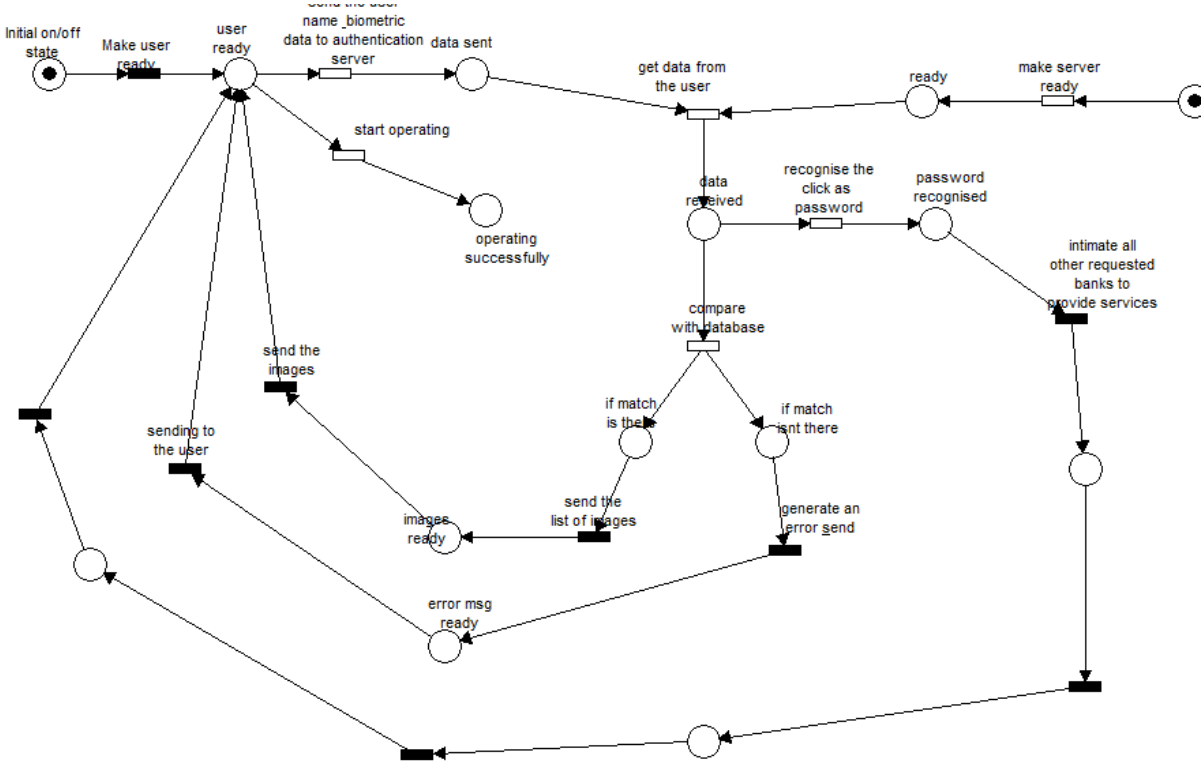

Figure 6: simulation of process carried out during operating online

We have set the time for each and every transition to ensure that no transaction could happen before the completion of the previous one. After running the simulation designed for the login and transaction phase, the flow of data and the performance of the system was as expected. Until the entire authentication process is finished neither bank nor the user can get any information or notification from the side of central authentication server.

CONCLUSION

In this paper we proposed an extended common interface for multiple online banking which uses a combination of biometrics along with the graphical image based password for enhancing the security in online banking applications and ensuring the minimum number of details to be remembered by the user in order to operate his/her account online. The major contributions of this work include definition of a general framework for secure online web banking, design of a generic architecture for web banking, simulation

and demonstration of the system components by developing examples from web banking domain. The concepts and the design of the integrated web banking are demonstrated using the petrinet tools available in public domain. From the simulations, we could see that all the requirements are fulfilled and the results are found to be satisfactory. No single tool, available in public domain supports all the required features for implementing online secure web banking and fault diagnosis capabilities of the web banking system. The most important issue is ensuring the collaboration of the banks for successful implementation.

ACKNOWLEDGEMENT

We would like to thank our college management and principal for encouraging us to carry out this Research work successfully. In addition, we are thankful to our colleagues for their continuous support.

REFERENCES

Alireza Pirayesh Sabzevar, Angelos Stavrou, Universal Multi-Factor Authentication Using Graphical Passwords, Proceedings of IEEE International Conference on Signal Image Technology and Internet Based Systems, 2008.

Tarek E Abdelzaher and Chenyang Lu, Modeling and Performance Control of Internet Servers, Proceedings of the 39th IEEE Conference on Decision and Control , Sydney, Australia December, 2000

Antonio San Martino, Xavier Perramon, A Model for Securing E-Banking Authentication Process:Antiphishing Approach , Proceedings of 2008 IEEE Congress on Services 2008 - Part I.

Marin Šili_, Jakov Krolo, and Goran Dela, Security Vulnerabilities in Modern Web Browser Architecture, Proceedings of MIPRO 2010, May 24-28, 2010, Opatija, Croatia

Richard S. Cox, Jacob Gorm Hansen, Steven D. Gribble and Henry M. Levy, A Safety-Oriented Platform for Web Applications, Proceedings of the 2006 IEEE Symposium on Security and Privacy (S&P'06)

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.

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

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.

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.

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

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.

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.

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

Sree rekha G and V.K.Agrawal, Issues and challenges in ensuring trust, security, performance and scalability in a common multi-banking solution, International conference on web services computing, ICWSC-2011, Cochin, Kerala.