Issues and Challenges in Ensuring Trust, Security, Performance and Scalability in a Common Multi-Banking Solution

Sree Rekha.G
Research Assistant,
CORI, PESIT,
Bangalore.

V.K.Agrawal,
Director,
CORI, PESIT,
Bangalore.

ABSTRACT
Internet is a network of networks and web is a network of servers. To establish connections and enable communications among them, some protocols which are common are used. Online banking system at present allows only the operations to be performed from a single bank account through a dedicated interface for that purpose. All the operations are to be done and transactions are to be performed using separate interfaces, separate usernames, separate passwords etc. It would be very convenient for any user if he/she could operate multiple bank accounts using a single login, single interface, single password. Then the question of security arises. This paper is going to discuss various issues and challenges in designing an integrated multi-banking solution for operating multiple accounts online named C-MBS. C-MBS allows users to operate multiple bank accounts through a single interface and moreover one-time login is enough for a particular session in which he/she can operate multiple accounts.

It provides all the details of the account to the customer or account holder like status of the account, balance available, any payments to be made, expiry of policy premium dates etc. Obviously one of the most important challenges of such system is security. Other issues are authentication, user acceptance, collaboration by banks, Cost effectiveness etc. This paper focuses on addressing the challenges and solutions for C-MBS.

General Terms
Single interface, single password, multi-biometrics.

Keywords
Common multi-banking solution, image based password, three factor authentication, multi-biometrics.

1. INTRODUCTION
Online business, banking and users have experienced a rapid growth in the recent past. One can easily observe the fact that there is no physical link between each other but there exists a virtual link. Since 1980s' online banking was first introduced in New York [2]. The number of users using Internet banking is increasing every year and the organizations which are in the race has to come up with the requirements of the customers and concentrate on developing the new infrastructure. While designing and developing a new system user acceptance level has to be given utmost importance because of the reason that further progress will depend on that. Currently Individual banks are offering online banking services. If a particular user is having multiple accounts in different banks then he/she need to remember all the usernames and passwords in order to operate the accounts.

2. ISSUES IN EXISTING ONLINE BANKING SYSTEM

a. Multiple interfaces:
One has to navigate through individual interfaces in the existing online banking in order to perform online transactions. For a particular bank concerned link has to open and user has to login using his username and password. If a user wants to operate multiple accounts then obviously he/she has to login to multiple sites.

b. Multiple usernames :
As stated earlier multiple usernames are required to operate more than one online banking account in the present online banking scenario.

c. Multiple passwords:
Usage of multiple passwords is a must if one has to use multiple usernames and these two are completely interrelated to each other in such a way that one can't exist without the other. But the risk of remembering more number of passwords is another issue which needs to be considered.

d. More number of steps:
Usually the numbers of steps that need to be performed for operating online bank accounts are literally more. For one bank certain procedure is to be followed and for the other the procedure will be different. To get acquainted with these procedures itself will take lot of time for a user to cope up with.

e. No integration of facilities:
There is no integration of service as such till now. Research work regarding the service integration need to be carried out in future.

f. No flexibility:

Flexibility is one of the most important features which most of the online banking customers would be looking for in any online banking application.

3. COMMON MULTI-BANKING SOLUTION ARCHITECTURE

We propose a system which employs a central authentication server as a base for authenticating a user with a single interface and a graphical image based single password for operating multiple bank accounts online [1]. In this new system the authentication is going to be done with the help of multimodal biometrics and a complete three factor authentication would be done. Authenticating a user can be done using one or all of the following

a. what you know?
b. What you have? And
c. What you are?

If all the three factors are used for authenticating a user then it is called multi-factor authentication. We propose to use dual biometrics for authenticating a user i.e. authentication will be done using facial and fingerprint images acquired from the user[5, 6].Artificial neural network based intelligent systems are employed for ensuring the better performance of classification and analysis of results on central authentication server side.

3.1 Steps to be carried out in the C-MBS

Step 1: Initially the user has to register with the authentication server. The steps to be performed by the registration server are

a. Requests user to give his details
b. Acquires the biometric data from the user.
c. Presents the user with multiple images among which he has to select one.

Step 2: Once the registration is done then the user can operated his/her accounts with the help of user name and password provided.

Step 3: while giving the password slightly different procedure will be followed

a. First the user will be given the images which he was given at registration time.
b. He/she has to select the same image that was selected at the registration time.
c. If the image is found to be the same then the user will be provided with one more image which contains some numbers on it.
d. Then the user has to click on the numbers indicated.
e. The clicks of numbers on images will be new password of that particular session.

Step 4: Then the authenticating server will request for biometric data.

Step 5: Artificial intelligence based system will classify and identify data.

Step 6: Once all the above steps are performed then the central authentication server will send the notification to the banks regarding provision of services.

Step 6: Then the user can start operating his/her multiple bank accounts.

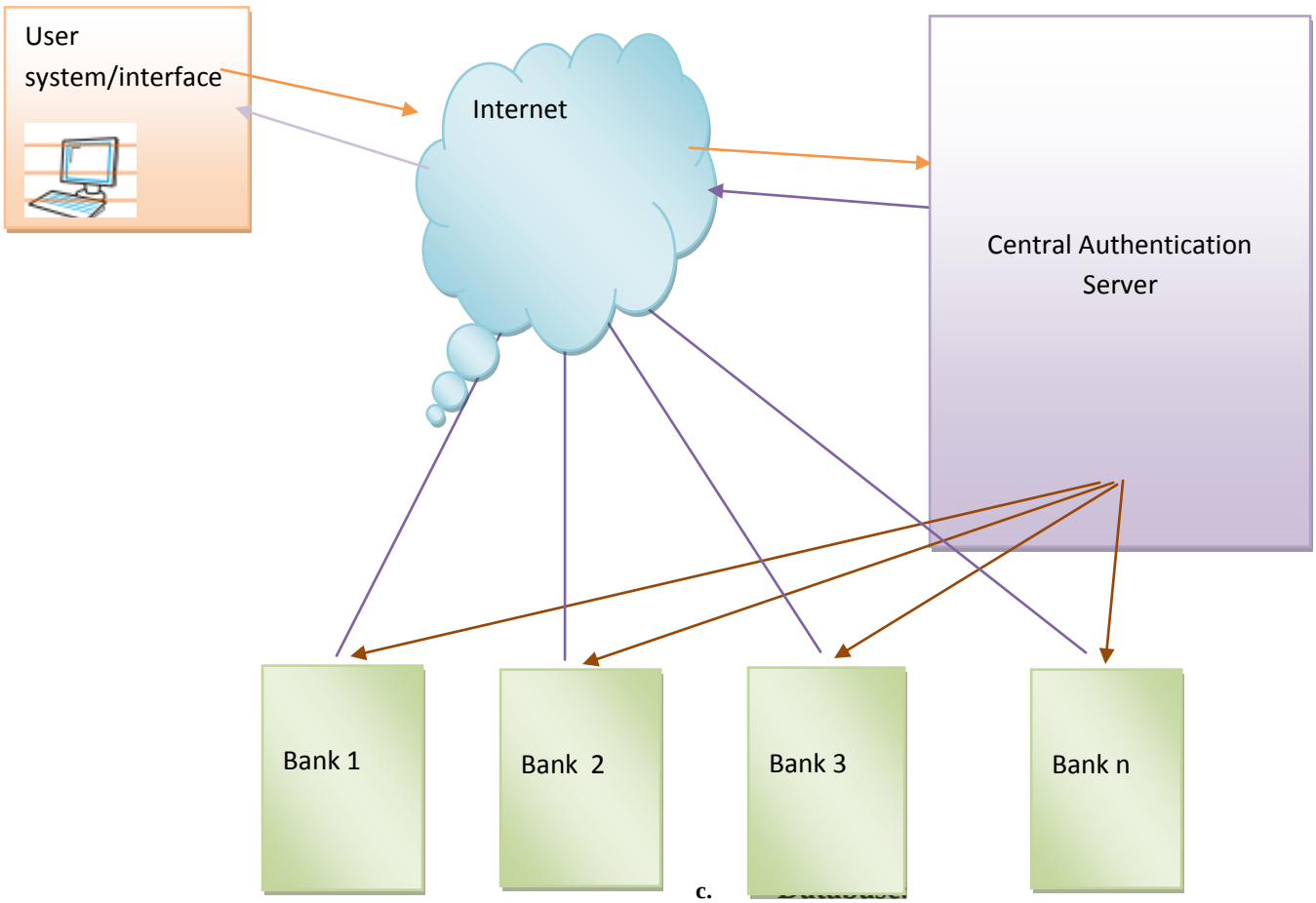

Figure: 1 Architecture of proposed system

4. CHALLENGES IN C-MBS DESIGN

a. Collaboration of banks:

One of the biggest challenges while integrating any services is the collaboration by the various organizations. It is a well known fact that a group can achieve better performance compared with the individual's performance. If at least some of the banks could collaborate together to provide better and enhanced services to their customers then the proposed system could be very attractive and beneficial to both the customers and users.

b. User acceptance:

User acceptance is another aspect which has to be given due consideration while designing and developing any new system. If more number of services are provided within a single interface then obviously users will show interest towards that and the chance for attacks will also be more. So we should be in a position to ensure the security of the system in order to attract more number of users.

c.

Maintaining and updating the databases is one of the most important things which play a vital role especially in online banking applications. Because every time the customer operates his account, the same has to be updated in the database. The work is even more when more number of services is going to be provided through a single interface and much more updates have to be done to multiple databases.

d. Mutibiometrics:

Use of multimodal biometrics is not that easy when it comes to practical implementation of its usage. One should be in a position to convince the users that they can afford for that instead of compromising for security. This is how challenge may arise while making use of Mutibiometrics in authenticating a user.

5. LIMITATIONS AND SECURITY IMPLICATIONS

There are many things to be considered

a. First the expiry of tokens has to be ensured once they are used.

b. Second, In order to prevent some authentication spam some kind of self-destruct feature has to be assured.

c. When one account is compromised immediate notification has to be made.

Today if one of our accounts is compromised, then we can reset password by following the link. By this we can

detect that something wrong is going on due to the fact that you can't login normally anymore. However, this only have implications in the long term.

To implement very strong authentication system generally Public Key Infrastructure (PKI) comes to mind in general. But at present scenario further more levels of authentication seem to be required. Let's consider an example, when the application authenticates with you, you receive the message encrypted with your public key. The only way to read it is to have your private key at hand and this is much better way of authentication than using simplistic and prone to failure username/password-based authentication mechanisms. We propose furthermore secure and easy to use authentication method which depends on multi biometrics, one time graphical image based password and a single interface.

6. SECURITY SOLUTION FOR C-MBS

Obviously many challenges will arise during the process of developing an integrated system for users. The developed system must ensure that it is convenient to use and also it is very secure. Often both convenience and security are to be maintained in developing an efficient system.

C-MBS plans to use the following list of solutions for the problems listed in section 4.

- C-MBS employs three factor authentication with the help of multiple servers and also multi-biometrics.
- Secure Socket layer authentication will be done for the site which ensures the security of the site.
- Biometric based authentication helps the system to identify any fraudulent user as and when they attempt to do any fraud.
- Awareness has to be created for both the users and banks in order to make them understand most common threats in online banking, and then only they can easily identify any misbehavior of the system while working.
- Firewalls are to be strong on both server sides as well as on the user side in order to avoid unforeseen circumstances.
- Data provided by the user is checked for its authenticity and then only Transaction authentication number will be generated and sent to the user.

7. FLOW OF DATA IN PROPOSED SYSTEM

As shown in the Figure 2 we analyzed the flow of data using a Petri-net based simulation tool **HPSIM.** Initially user and user system will be ready to perform the task. Once the equipments required are ready the data will be captured and sent to the authentication server. The authentication server then separates the data accordingly and performs matching with that in the database. If an error occurs at this stage user will be sent a message. If match is there then images will be sent to the user among which he/she has to select for further authentication. In the final image sent to the user the password will be in encrypted format. User has to just click the numbers present in the image and then provide the biometric data as well to the central authentication server. After proper authentication the server will send the messages to the concerned banks requesting for providing the services. Then the user can start operating his/her multiple bank accounts simultaneously without any trouble. This is how the data will be propagated in the proposed system.

7.1 Places used:

P1: User ready

P2: Data ready

P3: data sent

P4: Separate data

P5: If match is there

P6: If match is not there

P7: error message to be sent

P8: Images ready

P9: Transmitting

P10: clicks ready

P11: Received by server

P12: Information ready

P13: Bank 1 received info

P14: Bank2 received info

P15: Bank3 received info

P16: communicating to user

P17: data ready to be transmitted.

7.2 Transitions used

T1: Get data from the user

T2: Send to Authentication server

T3: Data received

T4: Match the data with the database

T5: Send error message to user

T6: Transmit the message to the user

T7: Send the images to the user

T8: Sending images

T9: Transmitting images

T10: ensuring transmission securely

T11: user clicks the images

T12: Send the info to the authentication server

T13: Processing the information to be sent to the banks

T14: Send notification to the banks

T15: communicate with the user

T16: sending the message

T17: Starter communicating and transacting.

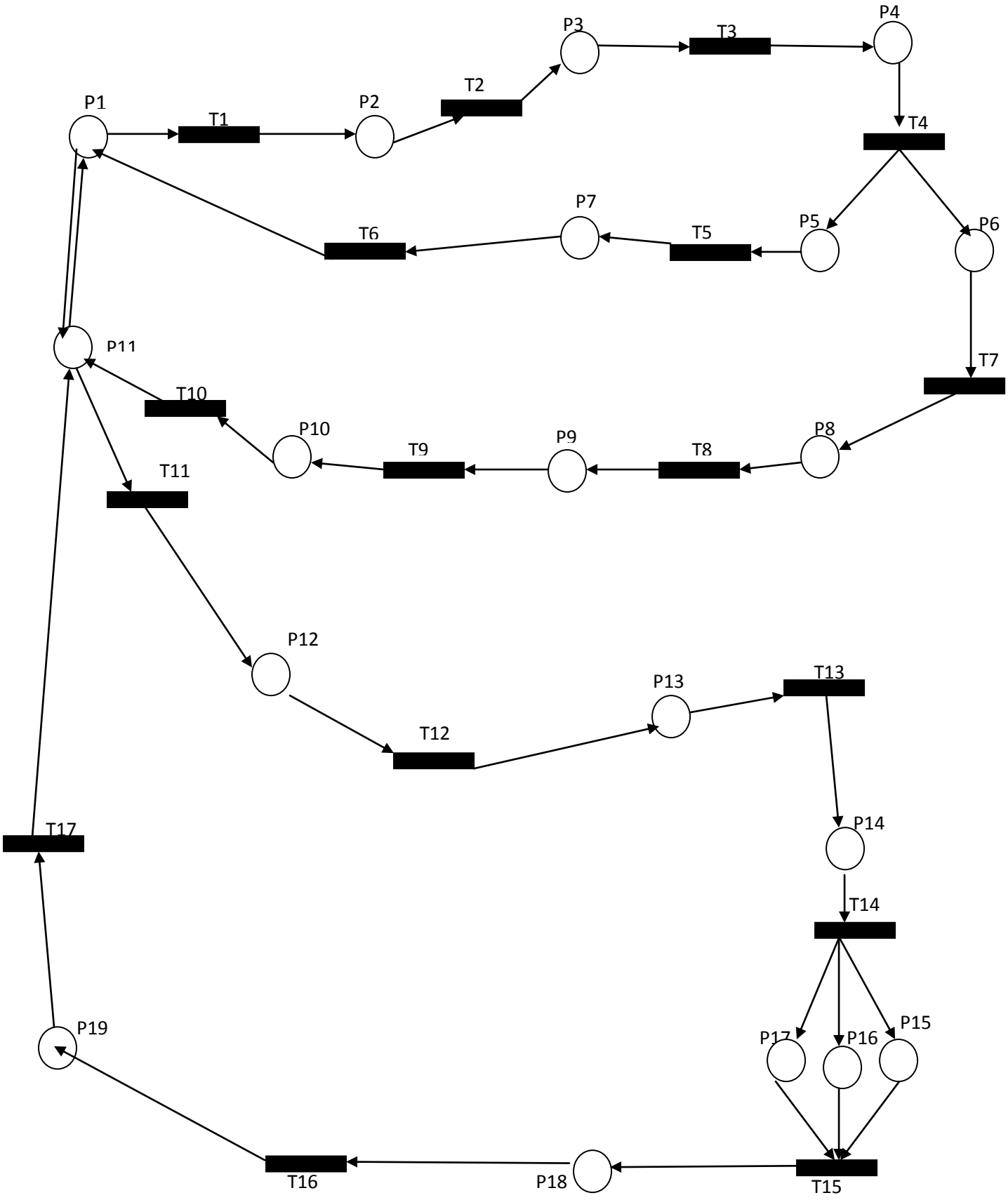

Figure: 2 Flow of Data in the proposed system

8. CONCLUSION

Various issues and challenges in ensuring security, reliability, performance, and trust and scalability in Common multi-banking solution have been discussed in this paper. We propose a novel mechanism of having a central authentication for all the banks and who ever registers and get authenticated can make use of the services. Authentication procedure will be based on the acquisition of biometric data and image based passwords which are more secure way of ensuring security. Finally, proper implementation of the proposed system could improve the performance of online banking applications along with the enhanced security and could be able to provide a common interface for multiple online banking.

9. ACKNOWLEDGEMENT

We would like to thank the management and faculty of PESIT for extending their co-operation for carrying out this work.

10. REFERENCES

[1] Universal Multi-Factor Authentication Using graphical passwords, Alireza Pirayesh Sabzevar, Angelos Stav, 2008 IEEE International Conference on Signal Image Technology and Internet Based Systems.

[2] Mary J Cronin, Banking and Finance on the Internet, New York Van Nostrand Reinhold, 1997.

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

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

[5] 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.

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

[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.