Research Inventy: International Journal of Engineering And Science
Vol.4, Issue 9 (Sept 2014), PP 26-30
Issn (e): 2278-4721, Issn (p):2319-6483, www.researchinventy.com

Towards Securing E-Banking by an Integrated Service Model Utilizing Mobile Confirmation

[1]Ali Abdollahi, [2]Mehdi Afzali
[1]*Dept. of Computer Engineering, Zanjan Branch, Islamic Azad University, Zanjan, Iran*
[2]*Dept. of Computer Engineering, Zanjan Branch, Islamic Azad University, Zanjan, Iran*

ABSTRACT - *Increasing advances of technology improve providing of services to people. Nowadays, although e-banking technology play an important role in speeding service providing and decreasing distances and costs, but impose some challenges to executives. People are always distrusted to the internet and banking businesses are encountering challenge of security and information privacy assurance to overcome this distrust. They should also provide confirmation of transactions to prevent unauthorized transactions when sensitive authentication information is thieved. In this paper, an integrated service providing model for e-banking is proposed that combining Core Banking and Single Sign-On(SSO) systems' functionalities, provide centralized management, simplicity and reduced faults, and provide more security using transaction approval process by mobile phone.*

Keywords - *Core banking, E-banking, Integrity, Mobile Confirmation, Security, Single Sign-On*

I. INTRODUCTION

E-banking technology is encountering problems such as insecure existing infrastructures for electronic interchanges and lack of integration between different banks at net banking in Iran. Variety of debit cards and payment gateways belonging to different banks involve users with challenge of memorizing numerous credentials and risk of phishing or other problems. Unlike people's belief that think they'll have more security in this way, issuing different credentials for a unique identity hazards his/her security because some people due to inability to memorize these credentials, write down them in places that other people could access. So, there's a need to a unified authentication and authorization system that issues unique certificates under supervision of central bank, and an obligation to be authorized from a unique system to do internet transactions. Such a system saves users from multiple authentications and different credentials' problems and provides them to do their transactions with less apprehension and more security.

As banking technology goes from traditional services to e-banking form, thievery also changes to cybercrimes form. Attackers usually try to steal people's credential information for malicious purposes, and in banking, to steal their money. Phishing is the usual instance in which attackers duplicate a web page to dishonestly acquire sensitive personal information. Therefore, users need a second level confirmation for financial transactions to prevent such attacks. Furthermore, to communicate different banks and other financial parties properly and to get more integrity, a centralized system is needed to shorten transaction time, reduce faults and get more auditability. Considering all above mentioned problems, weaknesses and needs, we propose a model which combines core banking and Single Sign-On functionalities to integrate e-banking services at a general level, and uses mobile confirmation as second level of authentication process to ensure more security and user-friendliness. Remainder of this paper is organized as follows: section 2 presents background information about Single Sign-On and core banking concepts, importance of mobile confirmation, and a brief overview of related work, section 3 describes the model, and finally a conclusion of the work is presented at section 4.

II. BACKGROUND AND RELATED WORK

2.1 SINGLE SIGN-ON

SSO system (Fig. 1) provides users a centralized access to different systems using one identity and one authentication process, without need to multiple authentication and authorization for every single application system.

Using SSO has these advantages:

- Less need to various combinations of usernames and passwords
- Less need to different authentications for different application systems
- Less IT costs related to password helpdesk

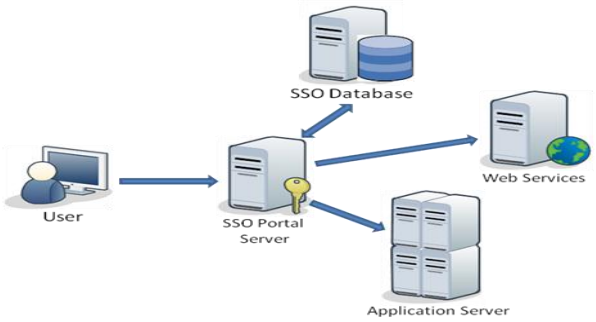

Figure 1. General Schema of SSO System

According to [1], sequence diagram of authentication and authorization process in SSO system is summarized in Fig. 2. Steps of this process are:

1) Access request to application from user
2) Sign in request or request to fill sign up form if not registered yet
3) Signing in, or filling sign up form and submitting to authentication system
4) Issuing unique ID for user and registration of this ID in system database, or search for registered user in authentication system database
5) User authorization and notification to user, or un-authorization and notification for denial of access
6) Sending user ID to application
7) Creating access link to requested service or application for this user ID
8) Sending access link to user
9) User's access to requested application

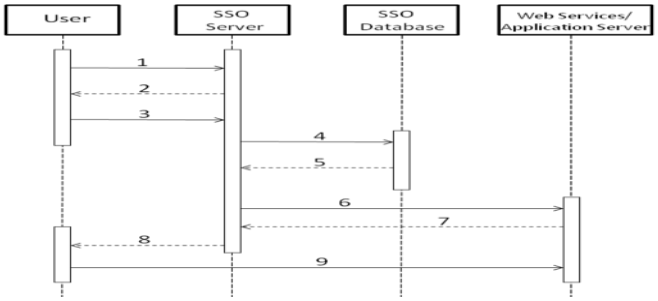

Figure 2. Sequence Diagram of SSO System

2.2 CORE BANKING

Core banking system is a kind of banking system in which all financial information and transactions of banking network are saved and recorded at a central information unit. Such a system is used to satisfy strategic financial policies in order to improve operations, reduce costs, and make opportunities for banking businesses to mature. Core banking system presents all banking products and services, and their steering and management operations, using shared databases centralized as a whole. Flexibility and customer-orientation are key characteristics of this system. Without creating a centralized and integrated database, e-banking services will be at a dispersed manner. In a centralized modular banking system based on new technologies, component-based software makes it possible to integrate with traditional banking technologies.

Development of core banking system has these advantages:

- Customer satisfaction due to variety of products and services
- Higher operational output
- Higher efficiency and output of human resources
- Management of operation and maintenance costs
- Centralized product management
- Centralized Customer Relationship Management (CRM)
- Centralized accounting
- Centralized monitoring
- Centralized marketing management

Propagation of electronic services based on core banking, results in high Return on Investment (ROI) and facilitates resource planning, because buying branches for banks and attendance of customers in bank branches is expensive. [2]

2.3 MOBILE CONFIRMATION

Most people have their cell phone along with them all day long; most of them do many works with their mobile phone and even do their financial transactions by network operators' mobile payment facilities all over the world. Cell phones are so propagated and easily purchasable that we could say everyone has a mobile phone or at least the people who use e-banking services have one. So, the user who requests for a financial transaction could be easily accessible via his/her mobile phone to confirm requested transaction. When a user receives a notification for a financial transaction to confirm while not actually requested it, he/she finds out that his/her credential information is stolen and rejects the transaction by replying the message, and reports the attack. With increasing attacks like phishing and pharming that aim to get people's sensitive information, probability of leakage increases and banking enterprises should guarantee security of users' financial assets in such situations. Mobile approval is an efficient mechanism to prevent such illegal transactions.

2.4 RELATED WORK

Many secure models and authentication mechanisms there exist in e-banking area. In [3] traditional and unified identity management models are discussed, and Federated Identity framework along with the other methods, and a comparison between them are presented that could have useful information about single sign-on. In [4] a model for securing e-banking applications with emphasis on phishing attack is presented that include server authentication process and could guarantee secure operation of an internet banking environment even in presence of malware at server side. In [5] a threat modeling process for e-banking applications using Microsoft's Software Development Life Cycle is proposed that could be useful for banking software developers. In [6] an evaluation framework for e-banking with emphasis on interaction between security and usability is proposed that could be a guide for security assurance systems of e-banking. In [7] a model named Notified Credit Card Payment System (NCCPS) is proposed to increase security of online credit card payments. Idea of mobile confirmation in our work is taken from this work. Also, other mechanisms and approaches with emphasis on encryption there exist [8], [9].

Of course all mentioned systems have significant advantages and each of them could be useful at proposed area, but this paper propose a framework for e-banking services with security point of view and include a part of our past work [10] that mobile confirmation is added to it to ensure more security for users' transactions.

III. PROPOSED MODEL

Information systems of an organization could be effective if they have correlation between them. Today, integration is one of orientations and objectives of organizations' IT managers and is used greatly in system and information technology literature. Integration between information systems is not solely about data bytes transferring. Performance of business processes is dependant to a variety of software and information systems that each of them is developed at specific time and with specific technology. So, automation of such processes is depended on interoperability between different systems. In this way, creation of a well defined bed between different banks, in order to integration of banking processes and services, and unification of information assets is a fundamental necessity. In our proposed model core banking system is used in order to integration of payment systems in e-banking, single sign-on system is used in order to integration of authentication process of this centralized system, and finally, mobile confirmation system is used in order to ensure more security for users.

In single sign-on based system, user is identified by a unique identity and uses a unique payment gateway to enjoy payment services. In this system, issuing identities and credentials is in responsibility of Certificate Authority (CA) that works under supervision of central bank. Depending on authentication mechanism, the unique identity could be at forms of username and password pairs, signature cards [11], etc.

In this model that is shown in Fig. 3, user after successful authentication and authorization logs in core banking system, could request for different transactions, and depending on his/her certificate these transactions could be done or rejected. User's cell phone number – that is given to authentication system firstly while registration – is used to send a notification message by mobile network operator to him/her. This message contains date, time, amount and type of transaction and could be at form of Short Message Service (SMS) or Unstructured Supplementary Service Data (USSD) push. After confirmation of transaction by user, this transaction will be performed if performable and then will be saved in transactions database.

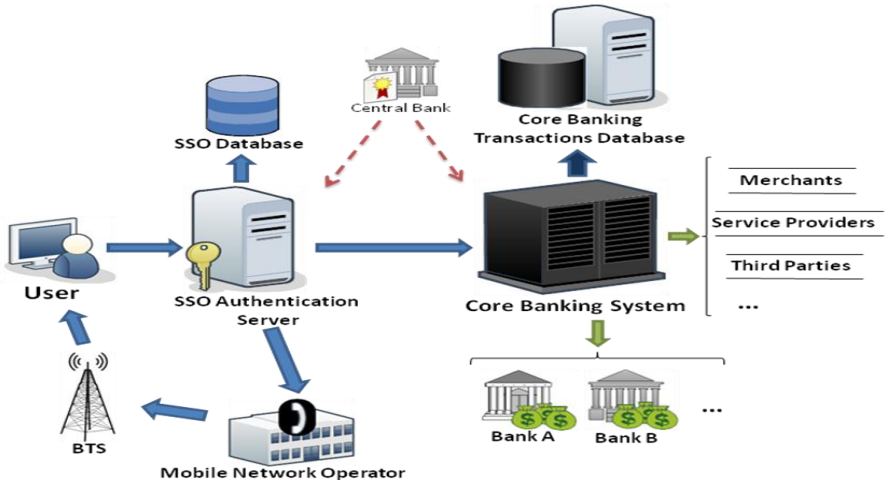

Figure 3. Proposed Model

All of banks, merchants, service providers and other third parties are connected to core banking system and recognize user's unique identity, and user has no need to re-authentication for every system. Furthermore, tracking and auditing for transactions is more easier and faster than existing non-centralized systems because require seeking for one identifier per user in single sign-on database, and checking transactions related to this user in transactions database.

Thanks to the mobile confirmation process, even if user's credential be stolen, there will be no possibility for attacker to do illegal transaction unless he/she would access user's mobile phone, too. This is the end of misery, but could be preventable by message signature mechanism. In this way, user signs sent messages by another password or other signature that he/she memorizes and knows himself/herself and nobody has access to it.

Sequence diagram of a sample online shopping process is given in Fig. 4. Other banking transactions would have similar sequence diagram with few differences.

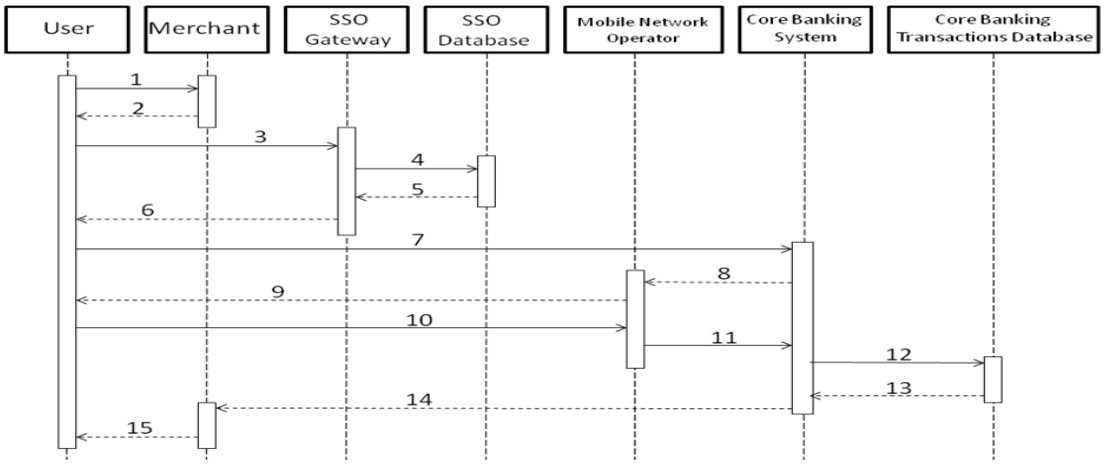

Figure 4. Sequence diagram of an online shopping process

Steps of the sequence diagram related to a shopping process are:

1) User chooses desired goods from merchants website and orders the purchase
2) Merchant gives order number to the user and forwards user to the payment system
3) User's request for authentication is sent to authentication system
4) SSO seeks for user's identity in SSO database
5) SSO database replies to request of SSO server
6) User is authorized/or system denies access of user to the system if his/her identity there not exist in SSO database or even not mach
7) User's transaction request is sent to core banking system
8) Core banking system requests for confirmation message from network operator

9) Mobile network operator sends notification for user's cell phone
10) User replies the message and confirms the transaction
11) Transaction confirmation report is sent to core banking system
12) User's credit inquiry is sent to core banking database for payment and transaction will be done if performable
13) Result is sent to core banking system
14) Result is sent to merchant (and the user)
15) Merchant reports completion of payment process to user and provides requested services to him/her

IV. CONCLUSION

Broadly speaking, e-banking is a set of systems that correlate with each other and if we consider it from the weakness point of view, the chain of e-banking is as weak as its weakest ring. So, the least faults of rings of this chain the strongest the whole system. Internet banking is one form of e-banking that reduces total number of rings of e-banking chain. Proposed system, utilizing core banking and single sign-on systems, tries to reduce total number of these rings so far as possible. Using proposed system has some advantages like centralization of electronic payment system, reducing IT management costs for banks, reducing workload for IT section of banks, while it has disadvantages like difficulties of coordination between different banks, reducing competition due to singularity, and high implementation costs. Although implementation of such system requires high investments but long-term use of it will result in high return on investment.

REFERENCES

[1] Zh. Liang, and Y. Chen, The Design and Implementation of Single Sign-on Based on Hybrid Architecture, *Journal of Networks, 7(1)*, 2012, 165-172.

[2] Wikipedia Website, Core Banking, http://en.wikipedia.org/wiki/Core_banking.

[3] F. Pimenta, C. Teixeira, and J. S. Pinto, GlobaliD: Privacy Concerns on a Federated Identity Provider Associated with the Users' National Citizen's Card, *Proc. 3rd IEEE International Conf. on Advances in Human-Oriented And Personalized Mechanisms, Technologies and Services*, 2010, 16-21.

[4] A. San Martino, and X. Perramon, A Model for Securing E-Banking Authentication Process: Antiphishing Approach, *Proc. IEEE Cong. on Services, Part I*, 2008, 251-254.

[5] C. Mockel, and A. E. Abdallah, Threat Modeling Approaches and Tools for Securing Architectural Designs of An E-Banking Application, *Proc. 6th IEEE International Conf. on Information Assurance and Security*, 2010, 149-154.

[6] C. Möckel, Usability and Security in EU E-Banking Systems: Towards an Integrated Evaluation Framework, *Proc. IEEE/IPSJ International Symposium on Applications and the Internet*, 2011.

[7] W. N. Y. Yan, and D. K. W. Chiu, Enhancing E-Commerce Processes with Alerts and Web Services: A Case Study on Online Credit Card Payment Notification, *Proc. 6th International Conf. on Machine Learning and Cybernetics*, Hong Kong, 2007, 3831-3837.

[8] G. Nacira, and A. Abdelaziz, Secured Net-Banking by θ-Vigenere in Syverson's Protocol, *IEEE*, 2005.

[9] Z. Djuric, IPS – Secure Internet Payment System, *Proc. IEEE International Conf. on Information Technology: Coding and Computing (ITCC'05)*, 2005.

[10] A. Abdollahi, and M. Afzali, A Single Sign-on based Integrated Model for E-banking Services through Cloud Computing, *International Journal of Advances in Computer Science and Technology (IJACST), 3(1)*, 2014, 34-38.

[11] M. A. Sirbu, Credits and Debits on the Internet, *IEEE Spectrum*, 1997, 23-29.