ISSN 2320 - 2602
Volume 3, No.1, January 2014
International Journal of Advances in Computer Science and Technology
Available Online at http://warse.org/pdfs/2014/ijacst06312014.pdf

A SINGLE SIGN-ON BASED INTEGRATED MODEL FOR E-BANKING SERVICES THROUGH CLOUD COMPUTING

Ali Abdollahi [1], Mehdi Afzali [2]
[1] Dept. of Computer Engineering, Islamic Azad University, Zanjan Branch, Zanjan, Iran,
ali_abdollahi86@yahoo.com
[2] Dept. of Computer Engineering, Islamic Azad University, Zanjan Branch, Zanjan, Iran,
afzali@hacettepe.edu.tr

ABSTRACT

With increasing advances in technology, there's a need to learn and use new technologies. Necessity of e-banking, and mainly internet banking and their importance and role in decreasing distances and increasing service providing speed is obvious but impose many challenges to executives. Prevailing over people's distrust to the internet is one of these challenges that could be achieved with assuring security and privacy of user in internet and reducing faults. At the other hand, providing all infrastructures and tools needed in e-banking area violate cost limitations and require a great part of overall budget. Cloud computing is one of technologies that provide scalable and flexible resources via internet – that could be accessible everywhere – using *pay-for-per-use* approach, and have a great role in reducing businesses' information technology costs.

In this paper a Single Sign-On(SSO) based integrated model for e-banking services is proposed that besides assuring more security, and reducing costs using cloud computing services, provides centralized management, simplicity and reduced faults.

Key words: *E-banking, Cloud Computing, Security, Integrity, Single Sign-On (SSO), Core Banking.*

1. INTRODUCTION

Lack of secure infrastructures for electronic interchanges and dispersed behavior of banks at internet area, are problems that e-banking technology is encountering in Iran. Source of such problems is in lack of integrity in internet banking domain. Variety of debit cards and payment gateways make users memorize numerous combinations of card numbers, PIN2s, CVV2s, or usernames and passwords – that lead to confusion. Although people think this makes them secure, but issuing different identifiers for a unique identity hazards his/her security, because most people due to inability to memorize, write down their identifiers to somewhere that other people could see.

A unified authentication and authorization system that is supervised by central bank and issues unique certificates, and obligation to be authorized from this system in order to do internet and interbank transactions, rescue users from multiple authentications and multiple identifiers' issues. Users do their transactions with less apprehension and more security.

One of the other burdens of e-banking development is budget limitations, because buying all needed infrastructures impose high costs. An option is to rent needed resources from other parties. Cloud computing is a novel technology that is presented in order to reduce IT costs for businesses, and provides required resources and infrastructures everywhere and every time is needed, with nominal cost. Although using cloud computing services reduce costs, but due to use of web as base medium to deliver services, require more security [3].

At the other hand, proper communication between different banks, or between banks and businesses which use their payment services, and to get more integrity, a centralized system is needed to shorten transaction time, reduce faults while forwarding transactions, and profit more auditability.

Many unified and secure authentication mechanisms and approaches there exist [2], [4], and [8]. But considering mentioned needs and weaknesses at e-banking and cloud computing areas, we propose a model which combining advantages of cloud computing, single sign-on and core banking system, in addition to reducing costs, increasing security and integrity, provides more user-friendliness for e-banking services.

Section 2 briefly explains cloud computing, single sign-on and core banking concepts, section 3 describes proposed model, and a conclusion is presented in section 4.

2. PRIMARY CONCEPTS

2.1 Cloud Computing

Cloud computing is the delivery of computing as a service rather than a product, whereby shared resources, software, and information are provided to computers and other devices as a utility over a network. Cloud computing describes a new supplement, consumption, and delivery model for IT services based on Internet protocols, and it typically involves

provisioning of dynamically scalable and often virtualized resources. It is a byproduct and consequence of the ease-of-access to remote computing sites provided by the Internet. This may take the form of web-based tools or applications that users can access and use through a web browser, as if the programs were installed locally on their own computers. Cloud computing providers deliver applications via the internet, which are accessed from web browsers and desktop and mobile apps, while the business software and data are stored on servers at a remote location. Table 1 presents an overview of cloud systems.

2.1.1 Service models

It is generally supposed that there are three basic types of cloud computing services:

Infrastructure as a Service (IaaS): In IaaS, CPU, grids or clusters, virtualized servers, memory, networks, storage and systems software are delivered as a service.

Platform as a Service (PaaS): PaaS provides virtualized servers on which users can run applications, or develop new ones, without having to worry about maintaining the operating systems, server hardware, load balancing or computing capacity.

Software as a Service (SaaS): SaaS is software that is developed and hosted by the SaaS vendor and which the end user accesses over the Internet. Unlike traditional applications that users install on their computers or servers, SaaS software is owned by the vendor and runs on computers in the vendor's data center (or a co-location facility). Broadly speaking, all customers of a SaaS vendor use the same software: these are one-size-fits-all solutions.

2.1.2 Deployment models

There are generally four types of Cloud deployment models:

Private cloud: Private cloud is infrastructure operated solely for a single organization, whether managed internally or by a third-party and hosted internally or externally.

Table 1: *Cloud Systems Overview [10]*

Features	Elasticity, Reliability, Virtualization, …
Benefits	Cost reduction, ease of use, time consumption, …
Service Models	IaaS, PaaS, SaaS
Deployment Models	Private, Community, Public, Hybrid
Stakeholders	Users, Adopters, Resellers, Providers, …
Locality	Local, Remote, Distributed
Compares to	Grid, Service-Oriented Architecture, Internet of Services, …

Community cloud: Community cloud shares infrastructure between several organizations from a specific community with common concerns (security, compliance, jurisdiction, etc.), whether managed internally or by a third-party and hosted internally or externally. The costs are spread over fewer users than a public cloud (but more than a private cloud), so only some of the benefits of cloud computing are realized.

Public cloud: A public cloud is one based on the standard cloud computing model, in which a service provider makes resources, such as applications and storage, available to the general public over the Internet. Public cloud services may be free or offered on a pay-per-usage model.

Hybrid cloud: Hybrid cloud is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together, offering the benefits of multiple deployment models. It can also be defined as multiple cloud systems that are connected in a way that allows programs and data to be moved easily from one deployment system to another.

Compared to other distributed systems such as grids or clusters, cloud computing solutions give enterprises significantly more flexibility. They can dispense with IT infrastructures of their own and only have to pay for the resources and services they actually use. These can be dynamically adapted to changed business requirements and processes with the help of virtualization technologies and service oriented, distributed software systems.

At the same time, the use of cloud computing systems also involves a number of security risks – most of them linked to the insufficient use of, and support for, security technologies. Yet-to-be-developed or immature technologies can likewise lead to security deficiencies in cloud computing systems. As a result, the use of cloud computing systems is still restricted, and a detailed assessment of the potential security risks is essential because users expect secure cloud services to comply with the same high security standards as the systems used in the past. These risks can have a significant influence on the end user's business model – for instance, if confidential information is stolen [9].

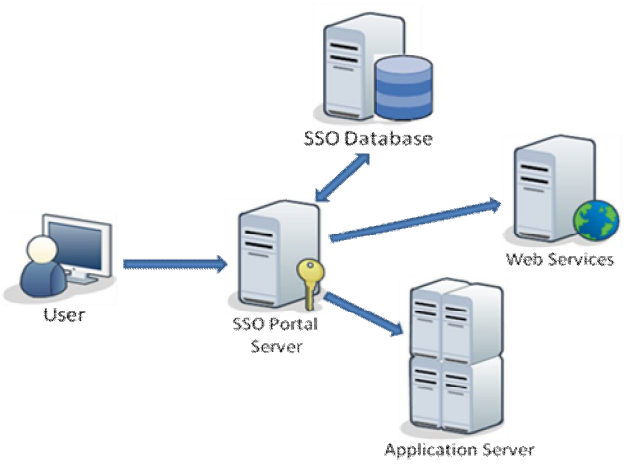
2.2 Single Sign-on

SSO system (Figure 1) provides users a centralized access to different systems using one identity and one authentication process, without need to multiple authentications and authorizations 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 Figure 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 unauthorization 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 access to requested application

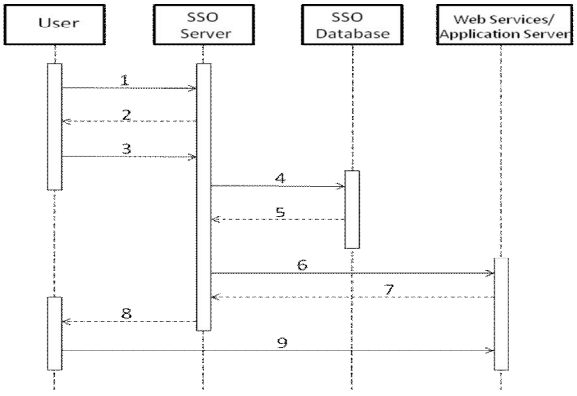


Figure 2: *Sequence Diagram of SSO System*

2.3 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.

3. PROPOSED MODEL

In our proposed model, relying on functionalities and advantages of core banking and SSO systems, and aggregating these systems, we combined their functionalities and presented an integrated system with centralized management. Core banking system is used for integration of payment methods in e-banking. SSO is used in order to integrate authentication process for this system. And cloud computing is used as a fundamental technology in order to reduce system development costs and time. Since cloud computing provides services in infrastructure, platform and software layers, everywhere cost is a limitation for system development, we could profit its services.

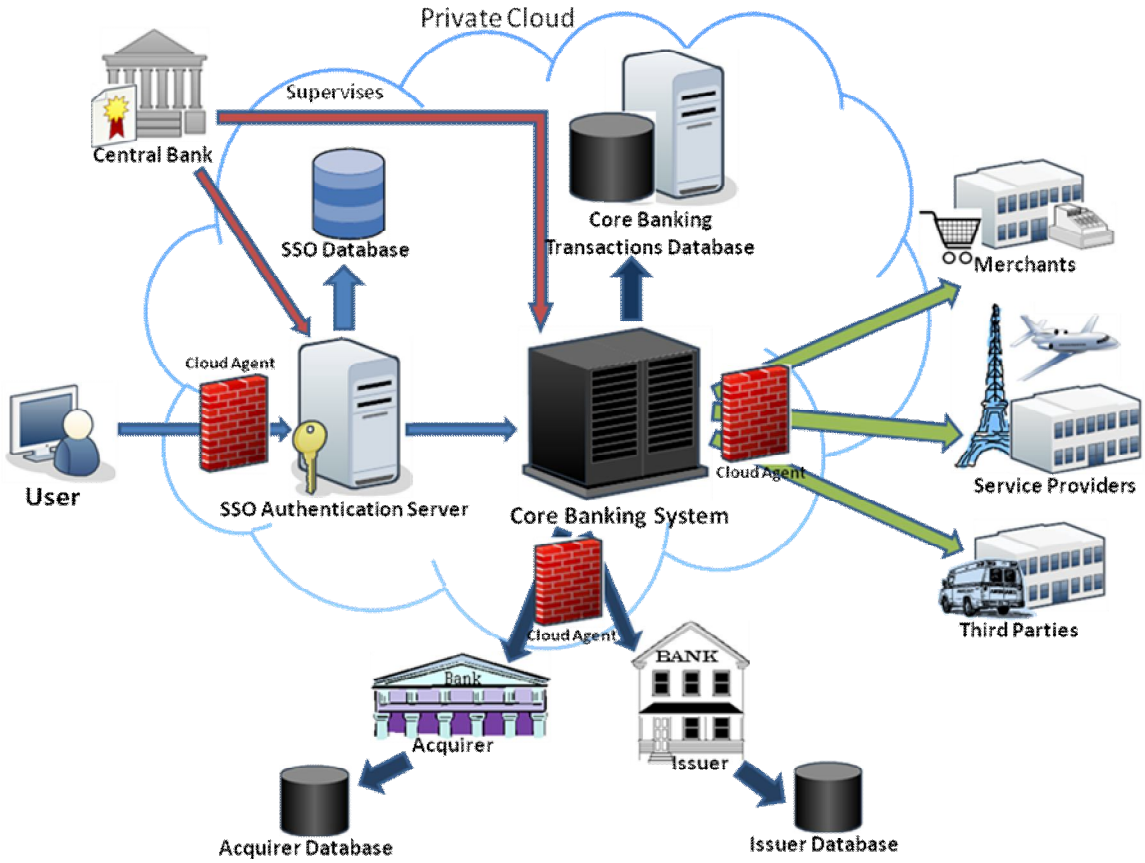


Figure 3: *Proposed Model*

In order to assure more security for banking system, private cloud deployment model is used to profit SSO-as-a-Service and Core Banking-as-a-Service. Of course access to the cloud is done via cloud agent that takes care of cloud security.

In SSO based system, user is identified by a unique identity and uses a unique gateway to facilitate payment services of all banks. Certificate Authority (CA) that issues unique certificate or identity for every party or person, works under supervision of central bank but can use different authentication mechanisms. But, in order to satisfy non-repudiation – that is one of the fundamental security requirements of a secure internet payment system [5] – authentication mechanism should include digital signatures. The unique identity depending on authentication mechanism could be at forms of username and password pairs, signature cards [6], etc.

Structure of an online banking system is commonly composed of five elements: user, internet, bank's server, authentication, and transactions [7]. In another view, this system is composed of three elements: customer network, internet, and bank server and private network [4]. In our model that is shown in Figure 3, after successful authentication and authorization, user signs in core banking system and requests for transactions. Depending on his/her certificate, these transactions could be performed or rejected. After searching core banking transactions database, system performs transactions if performable, and saves them in transactions database. Finally, these changes will be saved in banks' database.

All banks, merchants, service providers, and third party enterprises which need payment system, are connected to core banking system and recognize user's unique identity, and user has no need to be authenticated by every system again.

Tracking and auditing of transactions require just searching for one identifier per identity in SSO database, and checking transactions related to this identity in centralized transactions database. Such an auditing is simpler and faster than existing systems.

4. CONCLUSION

In this paper, a secure integrated model based on SSO and core banking system for providing e-banking services through cloud computing presented that speeds up and simplifies transactions by centralizing and aggregating e-payment rules.

Furthermore, using cloud computing services, this model profits key advantage of this technology that is IT cost saving.

Our proposed system releases users from memorizing different combinations of usernames and passwords and numbers and digits and letters, for different banks and payment gateways due to use of unique identity. Also simplifies management and auditing processes.

It is worth mentioning that, because of using unique identity, and possibility to access all systems using this identity, its importance and tendency to theft it will be higher and require more effort to keep it secure and private.

REFERENCES

1. Zh. Liang, and Y. Chen. **The Design and Implementation of Single Sign-on Based on Hybrid Architecture**, *Journal of Networks*, Vol. 7, No.1, pp. 165-172, January 2012.
2. F. Pimenta, C. Teixeira, and J. S. Pinto. **GlobaliD: Privacy Concerns on a Federated Identity Provider Associated with the Users' National Citizen's Card**, in *Proc. 3rd IEEE Conf. Advances in Human-Oriented And Personalized Mechanisms, Technologies and Services*, 2010, pp. 16-21.
3. J. P. Choi, Ch. Fershtman, and N. Gandal. **Network Security: Vulnerabilities and Disclosure Policy**, *Journal of Industrial Economics*, July 2009.
4. A. San Martino, and X. Perramon. **A Model for Securing E-Banking Authentication Process: Antiphishing Approach**, in *Proc. IEEE Congress on Services*, Part I, 2008, pp. 251-254.
5. Zoran Djuric. **IPS – Secure Internet Payment System**, in *Proc. IEEE Conf. Information Technology: Coding and Computing (ITCC'05)*, 2005.
6. Marvin A. Sirbu. **Credits and Debits on the Internet**, *IEEE Spectrum*, pp. 23-29, February 1997.
7. C. Mockel, and A. E. Abdallah. **Threat Modeling Approaches and Tools for Securing Architectural Designs of An E-Banking Application**, in *Proc. 6th IEEE Conf. Information Assurance and Security*, 2010, pp. 149-154.
8. 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, in *Proc. 6th Conf. Machine Learning and Cybernetics*, Hong Kong, August 2007, pp. 3831-3837.
9. W. Streitberger, and A. Ruppel. **Cloud Computing Security: Protection Goals, Taxonomy, Market Review**, Fraunhofer AISEC, 2010.
10. Lutz Schubert. **The Future of Cloud Computing: Opportunities for European Cloud Computing Beyond 2010**, Expert Group Report, ver. 1.0.