An SOA Model with Security-as-a-service in Cloud Computing Application-I banking

Shalini. G [#1], Hamsalatha. J [#2], M Shivakumar [#3]

[1]*Asst.Proffessor, Computer science and engineering, VTU*

[2]*Asst.Professor, computer science and engineering,VTU*

[3]*Professor, computer science and engineering,VTU*

Dr.TTIT, Kolar Gold Fields, India

***Abstract*— Cloud computing is an emerging technology which provides three main services namely SaaS,PaaS and IaaS where the security is addressed individually in each of these services. In this view the network traffic and computation time increases, and slows down the availability of cloud resources to the service consumers. In this paper we have proposed a new service provider namely security-as-a-service in cloud computing wherein all the security related tasks will be handled uniquely which is similar to firewall in a network topology. In our paper, we have taken i-banking application with SOA for effective, easy and secure access of cloud.**

Keywords— **Cloud, SOA, Security-as a-Service**

I. INTRODUCTION

Cloud computing represents one of the most significant shifts in information technology. Customers are both excited and nervous at the prospects of cloud computing. They are excited at the oppurtunities to reduce capital costs, on-demand computing provisioning. However,customers are also very concerned about the risks of cloud computing if not properly secured and the loss of direct control over systems for which they are nonetheless accountable.[1].A number of factors, including lower cost of connectivity, greater Internet and mobile Internet penetration, affordability of devices and the arrival of the smart phone have gone into popularizing online (Internet and mobile) banking around the world[2].Cloud computing will increasingly provide banks with new lower cost operating models thanks to virtualization, greater automation, and the ability to push more activities offshore. As these benefits are realized, banks will face decisions regarding the business case for moving legacy systems "into the cloud" or building new cloud-enabled assets that they will then integrate into the legacy environment.One of the critical issues in evaluating cloud-based services is Data security. Consumers were initially afraid that online banking would make them more vulnerable to fraud or identity theft. Now that online security technologies have improved, online banking is actually safer than getting paper statements in the mail. Likewise, using a cloud-based service supplier instead of operating your own internal system can be a major step toward becoming liberated from serious security issues.[2]

A. Advantages of cloud

1) Cost savings and usage based billing

With cloud computing, financial institutions can turn a large up-front capital expenditure into a smaller, ongoing operational cost. There is no need for heavy investments in new hardware and software. In addition, the unique nature of cloud computing allows financial institutions to pick and choose the services required on a pay-as-you-go basis.

2) Business continuity

With cloud computing, the provider is responsible for managing the technology. Financial firms can gain a higher level of data protection, fault tolerance, and disaster recovery. Cloud computing also provides a high level of redundancy and back-up at lower price than traditional managed solutions.

3)Business agility and focus

The flexibility of cloud-based operating models lets financial institutions experience shorter development cycles for new products. This supports a faster and more efficient response to the needs of banking customers. Since the cloud is available on-demand, less infrastructure investments are required, saving initial set-up time. It also allows new product development to move forward without capital investment

4)Green IT

Organizations can use cloud computing to transfer their services to a virtual environment that reduces energy consumption[3]

B.Cloud computing service models

1)Business Process-as-a-Service (BPaaS).
The cloud is used for standard business processes such as billing, payroll, or human resources. BPaaS combines all the other service models with process expertise.

2)Software-as-a-Service (SaaS).
A cloud service provider houses the business software and related data, and users access the software and data via their web browser. Types of software that can be delivered this way include accounting, customer relationship management, enterprise resource planning, invoicing, human resource management, content management, and service desk management.

3)Platform-as-a-Service (PaaS).
A cloud service provider offers a complete platform for application, interface, and database development, storage, and testing. This allows businesses to streamline the development, maintenance and support of custom applications, lowering IT costs and minimizing the need for hardware, software, and hosting environments.

4)Infrastructure-as-a-Service (IaaS).
Rather than purchasing servers, software, data center space or network equipment, this cloud model allows businesses to buy those resources as a fully outsourced service.[4]

C. Cloud computing deployment models

1)Private cloud

Private clouds are built by applying virtualization within a bank's own data centers. Because private clouds are not exposed to external "tenants,"banks tend to regard them as a more secure environment for customer data.

2)Public cloud
Public clouds extend the data center's capabilities by enabling the provisioning of IT services from third-party providers over a network.The data and processing may be located anywhere in the world on infrastructure that is shared with the cloud provider's other customers,or "tenants".

3)Hybrid cloud
Hybrid clouds blend public and private clouds depending on the sensitivity of the data and applications in each process, and the degree of business criticality and differentiation. Most banks will follow a "hybrid" cloud strategy which can also be a cloud owned by and located within the bank,but operated by a third-party.[5]

D. Security challenges pertaining to each of the three cloud service models—Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

SaaS deploys the provider's applications running on a cloud infrastructure; it offers anywhere access, but also increases security risk. Security risks are data security,network security,data locality,data integrity,data access, authorization and authentications. For example, with Salesforce.com, only certain salespeople may be authorized to access and download confidential customer sales information.
PaaS is a shared development environment, such as Microsoft™ Windows Azure, where the consumer controls deployed applications but does not manage the underlying cloud infrastructure. This cloud service model requires strong authentication to identify users, an audit trail, and the ability to support compliance regulations and privacy mandates.
IaaS lets the consumer provision processing, storage, networks, and other fundamental computing resources and controls operating systems, storage, and deployed applications.public cloud poses major risk whereas private cloud security have lesser impact. As with Amazon Elastic Compute Cloud (EC2), the consumer does not manage or control the underlying cloud infrastructure. Data security is typically a shared responsibility between the cloud service provider and the cloud consumer. Data encryption without the need to modify applications is a key requirement in this environment to remove the custodial risk of IaaS infrastructure personnel accessing sensitive data
A single security system would be too costly for certain applications and also if the cloud has a common security methodology in place,it will be a high value asset for hackers because it makes entire cloud vulnerable to attack[6].

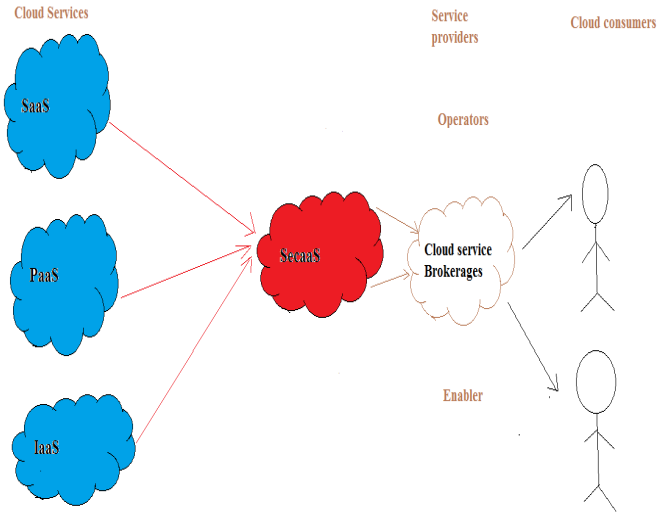

Fig. 1 The three cloud services ans SecaaS which acts as a firewall

Secaas is a service oriented approach to IT security architecture and thus a consequent evolution of traditional security landscapes. It is defined as a model for the delivery of standardized and comprehensive security, functionality in accordance with Saas model. It thus follows the cloud computing complying with related principals. In the figure we can see that a new cloud service Secaas is included which

acts as a firewall. The end users when accessing the cloud services has to cross this firewall which protects the cloud. The security enablers include technologies ,such as cryptography, directories and key stores that are utilized to perform the tasks.

II.SERVICE ORIENTED CLOUD BASED ARCHITECTURE

SOA, a flexible, modular approach to delivering IT services, is an essential foundation for emerging technologies like cloud. Plus, SOA provides significant advantages over current IT architectures. While it lowers costs, its primary benefit is the improvement in agility that it provides to organizations, enabling them to respond to the increasing rate of change occurring in nearly every business around the world.[7]

A. *Five key reasons to utilize SOA on the way to cloud:*

1)Accessibility: the cloud is accessible through a SOA interface

2)Visibility: SOA tools and techniques can help an organization find services that meet its needs.

3)Extensibility: Cloud services can be modified and customized using SOA techniques.

4)Matching Expectations: Cloud services require clear SLA'S, deploy these using SOA contract management techniques.

5)Adherence to standard: SOA policy management techniques validate that an organization follow appropriate cloud standards.

While the cloud undoubtedly presents enormous benefits to the business, moving away from a centralized IT architecture can open up a business to new risks. Utilizing specific techniques within SOA can improve security, such as using an intermediary for communication and run-time policy enforcement to ensure that communications are secure. In a cloud environment, it is important to always investigate who is responsible for securing the cloud and whether their security matches the organization's expectations. If not, the organization should work with a partner to ensure that all areas of security across the architecture are sufficient. Planning how to measure and test security means SOA contracts can be proposed while SOA services are still relatively small in number. The figure2 given shows how we can implement the three security services in a single place as secaas .

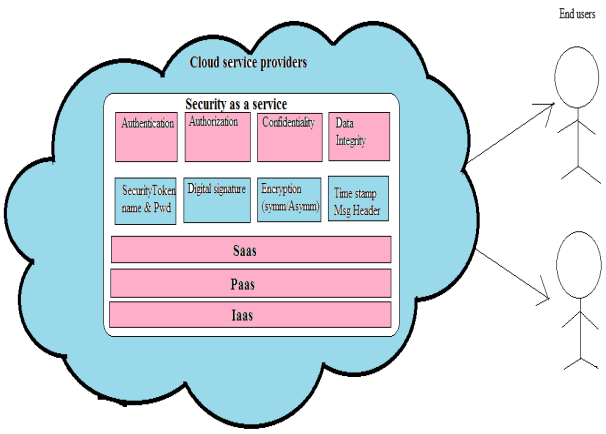

Fig. 2 Secaas using SOA model

In the figure, we can see three main cloud services i.e Iaas, Saas, Paas .above these we have Secaas which makes use of SOA model to address security issues.
The SOA Security Pattern addresses security along four dimensions:

1)Authentication – It must be possible for the service provider to ascertain the identity of the service requester.

2)Authorization – The service provider must be able to determine whether the requester has the appropriate rights to invoke the service.

3)Message Confidentiality – Message contents must only be visible to the intended recipient.

4)Message Integrity – It must be possible to guarantee that a message has not been altered or tampered with in transport between the service consumer and the service provider.

The security information related to the message payload is typically contained in the message header as shown in the figure. The security header for the message contains a security token, a digital signature when necessary, and information related to the encryption of the message if the message has been encrypted. Authentication is supported through the use of client-side x.509 certificates, username and password, and Security Assertion Markup Language (SAML) certificates. Message confidentiality can be guaranteed at the transport layer via Secure Sockets Layer (SSL) or within individual messages. Encryption at the message level ensures confidentiality across multiple "hops" in the integration infrastructure. Message integrity can be guaranteed through signing using digital certificates. Time stamps are used to prevent replay attacks[8].

III.BANKING IN THE CLOUD

Cloud computing is much more than simply renting servers and storage on-demand to reduce infrastructure costs-as many believe. In fact, a bank may have many reasons for moving to the cloud, but the primary reason will likely be applications. A key stumbling block for major investments in new technologies has always been the capital expenditure needed for new infrastructure. With cloud computing, financial institutions only have to budget for operational expenses and pay for the services they use. This makes it easier and more cost effective to test new applications on the cloud versus current traditional infrastructure [3]. No single cloud computing services model is expected to meet all the technology requirements for every financial institution. Instead, banks should develop and maintain an application portfolio consisting of both cloud and on-premise applications. While investments in legacy systems are expected to continue, cloud based services are ideal for newer business areas. Cloud-based services are expected to provide the advantage of both lower investments in implementing business strategies and faster turnaround time for product and service offerings, especially those delivered over mobile devices and the Internet.A good example is Singapore, where all major banks provide internet banking platforms. Using cloud reduces software licencing costs by centralizing across enterprise, efficient use of hardware and network assets, better absorb explosions of data without increasing network investments. But still there are security issues in moving core data to the public cloud but with smarter privacy like 3 factor authentication(smartcard, password, bio-metric identification like voice signature) would become smarter reducing disruption and increasing satisfaction.

Using this SecaaS makes availability efficient because we are not providing security in individual cloud services (Iaas, Paas,Saas) rather addressed in a single SOA model Secaas . It addresses authentication, authorization, message integrity and confidentiality by applying various authentication and authorization techniques(username, passwords, smart cards, biometrics), encryption and decryption algorithms are used, digital signatures are used and also acts like a firewall in network topology but again security concern should be taken care because the entire security feature is available in a single place for hackers

Example: BBVA banks on Google cloud operates in 26 countries and the applications used are gmail, chat, calendar, docs and video conferencing to achieve a cultural change[5].

TABLE 1

CHALLENGES IN CLOUD

Challenge	Description	Possible approach
Identification and authentication	identification is the process whereby a network element recognizes a valid users identity and authentication is a process of verifying claimed identity of user	User id's and passwords, smartcards, cryptography,bio-metric identification
Authorization	Determine whether the requester has the appropriate rights to invoke the service.	Digital signature
Confidentiality	Limiting information access and disclosure to authorized users	Physical isolation, cryptography
Integrity and reliability	Refers to the trustworthiness of information resources	Digital signature
Non-repudation	To ensure that transferred message has been sent and received by the parties claiming to have sent and received the message	Digital signature
Availability	Availability of information resources	Load balancing techniques

Security threats in cloud are: malicious insider attack, denial-of-service, man-in-the–middle attack, message alteration, replay attack, false repudation, insecure interfaces and APIs, shared technology issues, data loss or leakage, account or service hijacking and unknown risk profile.

The areas of Cloud Security as a Service that most likely will interest consumers and security professionals are:

Identity Services and Access Management Services
Data Loss Prevention (DLP)
Web Security
Email Security
Security Assessments
Intrusion Management, Detection, and Prevention (IDS/IPS)
Security Information and Event Management (SIEM)
Encryption
Business Continuity and Disaster Recovery
Network Security [8]

IV Conclusion

Cloud computing is a Kind of network where user can use services provided by Service provider on pay per use bases. It is a research area which provides a wide range of applications under different topologies where every topology computing that is expected to be adopted by government, manufacturers and academicians in the near future. Banks appreciate the relevance of cloud and SOA solutions. At the moment, however many are reluctant to entrust their sensitive customer and financial data to public cloud services run by third parties. Data privacy and security regulation in many countries prohibit the storage and processing of customer data outside national borders. Banks are also worried about disastrous impact of a serious breach of security or privacy. This paper gives an overview of how we can provide a separate Security as a cloud service using SOA model, which addresses security issues like Authentication, Authorization , Message confidentiality and message integrity. In this approach load balancing is easy but the entire cloud will be affected if the hacker attacks the single security service. Hence extensive work has to be done towards securing the single SOA integrated cloud security as a service.

REFERENCES

[1] Cloud security alliance*," top threats to cloud computing v1.0*", prepared by CSA march 2010

[2] TC Dinesh, Senior principal, Infosys limited*, "what the future of online banking authentication",* finacle from Infosys

[3] Sudhir sriram *,"cloud computing in Banking*", "www.Capgemini.com/financialservices "

[4] Santosh Nikam1, Chandrabhan Ghuge2, Harish Bhabad 3, Ajeet Patel4, Pankaj Kulkarni *" I-BANKING AN APPLICATION OF CLOUD COMPUTING,"*www.ijater.com" ISSN No: 2250-3536 Volume 2, Issue 6, Nov. 2012

[5] Emmanuel viale*, a new era in banking*, www.accenture.com

[6]s.subhashini, v.kavitha*," A survey on security issues in service delivery models of cloud computing*", www.elseier.com/locate/jnca, 2010

[7] Andy Mulholland, Ruse Daniele,tim hall,mary Johnson,pite chargin,www.hp.com/wp_cloudcomputing_soa

[8]Soa security Design and implementation,IBM,www.redbooks.com, isbn: 0738486655

Authors Profile

Shalini G, Currently Working has Assistant Professor in the Department of Computer science and engineering at Dr.TTIT, KGF has profound knowledge in research and area of interest is Network Security, cloud Computing, operating System Etc.,

Hamsalatha.J, Currently Working has Assistant Professor in the Department of Computer science and engineering at Dr.TTIT, KGF has profound knowledge in research and area of interest is storage area network , cloud computing, Data Security Etc.,

Dr.M.ShivaKumar , Head of the Department of Computer science and engineering Dr.TTIT, KGF has profound knowledge in research and area of interest is Network Security, cloud computing, operating System Etc. and guided for this paper,