International Journal of Information Technology and Knowledge Management
July-December 2012, Volume 5, No. 2, pp. 243-246

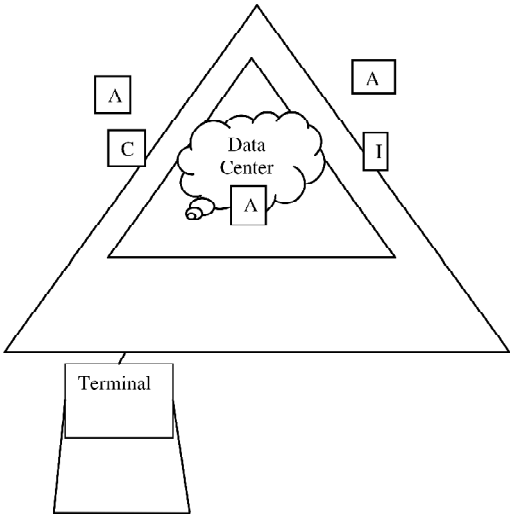
SECURITY ISSUES OF BANKING ADOPTING THE APPLICATION OF CLOUD COMPUTING

Sunita Rani[1] and Ambrish Gangal[2]

ABSTRACT: Cloud computing has become the most emerging technology now a days. It increases the flexibility scalability over internet. Every field wants to do work with the help of cloud computing because it provides promising business idea to the fastest growing areas of the information technology. One of the fields that want to merge their business or work with the cloud computing is the banking field *i.e.* Banking Appliocation. This Technology makes possible to reuse the IT resources for the banks very efficiently. According to research firm Gartner, this market for cloud services will increase from $36 billion today to $160 billion by 2015. Gartner also says 20 percent of companies will be using cloud computing for significant parts of their technology environment by 2012.[1].As cloud computing provides unlimited infrastructure to retrieve and to store data and is stored at multiple location and due to redundancy data can be modified by unauthorized users. This leads to the loss of data. So security and privacy becomes the main issue in the cloud computing for Banking application. In this paper, I explores the advantages for banking with cloud computing, problem arises when using banking with cloud computing and some solution for that.

1. INTRODUCTION

Cloud computing is a network-based environment that focuses on sharing computations or resources. Actually, clouds are Internet-based and it tries to disguise complexity for clients. [1]. During the past few years, cloud computing has grown from being a promising business idea to one of the fastest growing parts of the IT industry. IT organizations have expresses concern about critical issues (such as security) that exist with the widespread implementation of cloud computing. These types of concerns originate from the fact that data is stored remotely from the customer's location; in fact, it can be stored at any location. [1] Generally, Cloud computing has several customers such as ordinary users, academia, and enterprises who have different motivation to move to cloud. If cloud clients are academia, security effect on performance of computing and for them cloud providers have to find a way to combine security and performance. The banking sector is one section that can be assisted with adequate cloud computing models and can be managed appropriately. The cloud based services can prioritize their services after observing the customer's demand and likeliness. They can get through the customer preference through social networking interfaces and focusing on better customer relations, human relations and finance management, helping the banks to retain customers and attract new consumers. Cloud provides many services which are absolutely apt when it comes to banking. The Cloud based e- invoicing provides the exchange when the rates are most favorable. In this way, the cloud will assist the banking business model and provide frequent benefits to them.



In our research, firstly CIA i.e. confidentiality, integrity and authentication will be provides to data center and after that AAA i.e. Authorization, Acountabilty and authentication will be provided.

One research indicates that 42 percent of bankers plan to deliver just 1 percent to 9 percent of IT services over the cloud in the next 24 months. But more than a third of respondents (37 percent) expect to deliver 10 percent to 25 percent of IT services over a cloud over the next two years. Very few bankers said they expect to deliver more than a quarter of their IT over the cloud in this time period. These

[1] *E-mail*: *sheetu_sheetu20@yahoo.com*
[2] A.P. in Lovely Professional University

results fit with one of prediction that big banks will move to the cloud space in a big way in the 2012-2013 timeframe.

2. CHALLENGES

Although cloud computing models are ready to assist the banking sector in numerous ways, but the banking industry has serious concerns about their sustainability. Some of their integral and prominent concerns are security, privacy, confidentiality, data integrity, and authentication requirements, along with location of data, availability, and recoverability.

When a bank moves into cloud computing, there are two primary challenges that must be addressed:

Security : The confidentiality and security of financial and personal data and mission-critical applications is paramount. Banks cannot afford the risk of a security breach.

Regulatory compliance : Customers are ultimately responsible for the security and integrity of their own data, even when it is held by a service provider. Traditional service providers are subjected to external audits and security certifications. Cloud computing providers who refuse to undergo this scrutiny are "signaling that customers can only use them for the most trivial functions", according to Gartner. [4]. Many banking regulators require that financial data for banking customers stay in their home country. Certain compliance regulations require that data not be intermixed with other data, such as on shared servers or databases. As a result, banks must have a clear understanding of where their data resides in the cloud.

Financial institutions must select the right service, deployment, and operating models to address security and compliance concerns. In the initial phases of cloud computing adoption, it is expected that banks will own and operate the cloud themselves with service providers taking increasing ownership and control of the cloud infrastructure as cloud computing matures and more rigorous controls become available.

There should be a clear strategic policy for cloud computing and management, prioritizing data that can be entrusted to the cloud operator, with clearly defined service level agreements (SLA) with milestones and a set time-frame, backed by a comprehensive governance structure. While choosing the cloud service provider, it is important to look into the firm's financial stability, ability to improve functionality and service levels and integrate data across different technology platforms and cloud services. The policy-based key management, with industry-standard encryption, is emerging as the cryptography model for better control on data in the cloud as the common encryption key management techniques are susceptible to vulnerability. Cloud security services are emerging to address data security, privacy and compliance risks, as well as prevention of data theft, ensuring disaster management, and detecting compliance violations with robust server security for virtualized data centers.

3. SECURITY RISKS

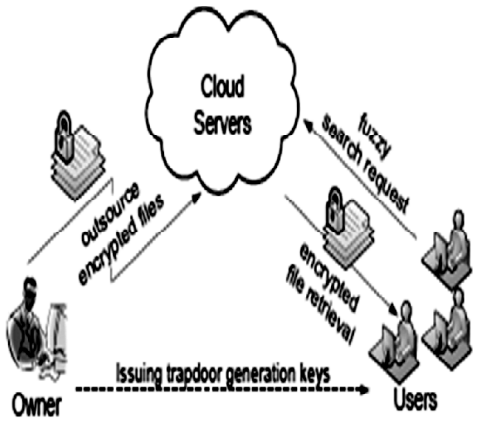
Well-known Gartner's seven security issues which cloud clients should advert as mentioned below [5]:

Privileged user access: There resides sensitive data that is processed outside the organization inherent risk of security of data because outsourced services bypass the "physical and logical IT controls".

- **Regulatory compliance** : Customers are responsible for the security of their data. Traditional service providers are subjected to external audits and security certifications.
- **Data location**: When users use the cloud, they have no knowledge about the hosted data.. Distributed data storage is a main reason of cloud providers that can cause lack of control and that is risky for customers.
- **Data segregation**: As cloud is typically in a shared environment in that data can be shared.so there is the risk for data loss. Is encryption available at all stages, and were these encryption schemes designed and tested by experienced professionals?
- **Recovery**: It is very essential to recover the data when some problem occurs and creates failure.so the main question arises here is that can cloud provider restore data completely or not? This issue can cause an stalemate in security.

o **Investigative support**: Cloud services are especially difficult to investigate, because logging and data for multiple customers may be co-located and may also be spread across an ever-changing set of hosts and data centers.

- **Long-term viability**: Ideally, cloud computing provider will never go broke or get acquired by a larger company with maybe new policies. But clients must be sure their data will remain available even after such an event.

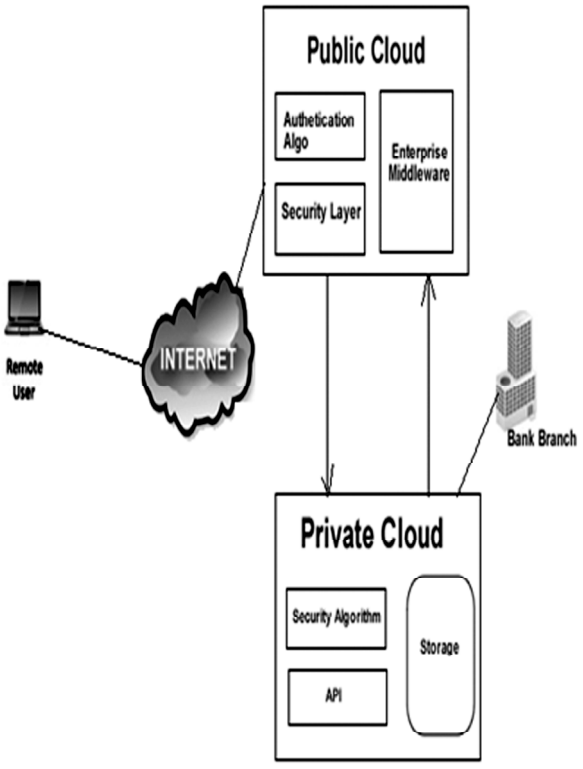


[8] Architecture of cloud data utilization service

Other risks are given below:

(*a*) **Leakage of Data**: as the data is not residing at the customer's local machine and also used for multi-tenant environment. This will lead to the data leakage problem. For this purpose we have to prevent this problem.

(*b*) **Database and server security for the System**: As the database and server security is must on front end while using cloud computing. If there exits security only then the banks can use variety of services of the cloud computing .By this the data for the banks will be remotely stored and they have no need to worry about hardware implementations. But the important concern is that there must be exist confidentiality, Authorization and integrity.



(*c*) **User authentication**: [3] For all of the enterprises, the management of user's account and their corresponding authorized access privilege is very important and must be strictly defined. A lot of enterprises usually confront the problem of user account such as the adoption of single sign on (SSO) or each employee will be dispatched some different accounts to access different systems.Thus, multi-authentication for each employee might be very often to be confronted in an enterprise.

Those accounts that come along with each individuals might be the same or different. Therefore, how could the administrator well manage those user's identification accounts and the corresponding passwords or achieve the state of SSO is another important issue. Nevertheless, the application of SSO for identification and authentication does have serious information security risk. In addition, the management of authorized access privilege is also a critical key point. How can the administrator define the appropriately access privilege for each employee to utilize the resources very satisfy and to achieve the goal maintaining information security without any leakage or the loss of confidential sensitive information through misuse in the meanwhile is kind of achieving the state of art.[3]

4. SOLUTION TECHNIQUE

Bank would use Hybrid Cloud for transactions It would have a private cloud for highly secure transactions. And it would use a public cloud for upper layer of it's application. For Authenticatation purpose kerboes will be used. Kerboes is

Architecture for secure cloud for banking application authentication protocol that works on ticket basis and provide identity for secure authentication by which identity is proved by this protocol. Kerberos uses symmetric key cryptography and requires a trusted third party during certain phases of authentication.[9].. Dynamic Firewall is used to protect the outsider attacks. Honey Pot is used to detect unauthorized use of data. These honey pots do not add direct value to a particular organization; instead, they are used to research the attacks for the organizations and used to protect against those attacks.[10]. IDS i.e. intrusion detection system is used to monitor the network or policy violations and provide reports to management station.[11]. Some systems may attempt to stop an intrusion attempt but this is not required for monitoring a system.[11]

REFERENCE

[1] "Banking on Cloud", Daniel Benton and Walid Negm, 2010.

[2] Farzad Sabahi, "Cloud Computing Security Threats and Responses", Faculty of Computer Engineering Azad University, 2001 IEEE.

[3] Chang-Lung Tsai Uei-Chin Lin et, "Information Security Issue of Enterprises Adopting the Application of Cloud Computing", Chinese Culture University, 2011 IEEE.

[4] Farzad Sabahi, "Cloud Computing Reliability, Availability and Serviceability (RAS): Issues and Challenges", *International Journal on Advances in ICT for Emerging Regions*, September, 2011.

[5] J. Brodkin. (2008). "Gartner Seven Cloud-computing Security Risks". Resideat: http://www.networkworld.com/news/200S!07020Scloud.html

[6] Gartner Incorporation, http://www.gartner.com/.

[7] Ramgovind S., Eloff M.M., Smith E., "The Management of Security in Cloud Computing", 978-1-4244-5495-2/10/ $26.00 ©2010 IEEE.

[8] Cong Wang, Qian Wang, and Kui Ren, "Towards Secure and Effective Utilization over Encrypted Cloud Data", 2011 31st *International Conference on Distributed Computing Systems Workshops*, 2011 IEEE.

[9] L. Zhu "Microsoft Corporation", B. Tung "Aerospace Corporation", "Public Key Cryptography for Initial Authentication in Kerberos (PKINIT)" June 2006.

[10] Lance Spitzner (2002). "Honeypots Tracking Hackers". Addison-Wesley. pp. 68-70. ISBN 0321108957.

[11] Scarfone, Karen; Mell, Peter (February 2007). "Guide to Intrusion Detection and Prevention Systems (IDPS)". Computer Security Resource Center <marque> (National Institute of Standards and Technology) (800-94</marque>). Retrieved 1 January 2010.