IJCSI International Journal of Computer Science Issues, Volume 13, Issue 1, January 2016
ISSN (Print): 1694-0814 | ISSN (Online): 1694-0784
www.IJCSI.org

Usage of Cloud Computing in Banking System

Nancy Awadallah

Department of Computer and Information Systems
Sadat Academy for Management Sciences Mansoura ,Egypt

Abstract
Cloud computing is known as on-demand computing and one of the latest developments in the IT industry. It provides the full scalability, reliability, high performance and relatively low cost feasible solution as compared to dedicated infrastructures. Security of Cloud computing is a sub-domain of network security, computer security and information security. This paper presents the role to improve cloud security and how cloud computing is impacting the financial services industry and what that management need to focus on when developing a strategy for their organization's adoption of cloud computing.

Keywords: *Trust, cloud computing, security issues banking system.*

1. Introduction

Virtually every business sector today is betting big on cloud computing More so, given the benefits it promises and the way it changes how technology is delivered and consumed by the end user in an enterprise. Like most other sectors, banks and financial services companies too can benefit from the fact that cloud computing helps to create a more flexible, agile business model to meet the growing business needs in a dynamic and competitive landscape. Cloud computing helps banks to transform their business processes and enhance their ability to grow in new sectors or regions without the time and cost burdens involved with establishing a physical presence. It helps to create new markets and services to differentiate from competition and improve the ways customers' access and use the bank's products and services. Banks will have a much better ability to provide consistent service to customers across branches, geographies and also integrate a plethora of disjoint customer information and analytics.

Cloud computing is based on five attributes: shared resources, massive scalability, elasticity, pay as you go and self-provisioning of resources. Unlike previous computing models, which is assumed dedicated resources, cloud computing is based on a business model in which resources are shared at network level, host level and application level [1]. Cloud computing allows the users to increase or decrease their computing resources as and when needed. Interest in the cloud computing is growing because cloud solutions helps business organizations to decrease the cost of computing resources significantly. There are three deployment models are available for cloud computing. They are public cloud, private cloud and hybrid cloud. A public cloud is hosted, operated and managed by a third-party vendor from one or more data centers. Normally in a private cloud model the day-to-day operations including the security management are handled by the implementing organization itself or by some third party contractual SLAs. A hybrid cloud environment consisting of multiple internal and/or external providers is a possible deployment for the organizations. In a hybrid cloud environment organizations might run non-core applications in a public cloud, while maintaining core applications and sensitive data using a private cloud.
The cloud computing with the proposed security model has the more stable performance when facing the attack threat, especially a variety of stacks at the same time.
Enterprises unwilling to trust their mission-critical applications or data in the public cloud look to private cloud computing as a way to introduce automation, self-service portals and further efficiencies to the company than virtualization alone can offer. Essentials enterprise IT need to build a private cloud architecture, including the latest news and tips on private cloud providers.

Cloud computing characteristics [2] include on-demand self-service, broad network access, resource pooling, rapid elasticity, measured service and multi tenacity [3], [4]. On-demand self-service characteristics means that customers or usually organizations can request as well as manage their own computing resources. Broad network access provides services to be offered over the Internet. Resource pooling characteristics means that customers draw from a pool of computing resources, usually in remote data centers. Services can be scaled larger and smaller; as well as use of a service is measured and also customers are billed accordingly. Cloud computing resource usage can be measured and controlled providing transparency for both the consumer and provider of the utilized service[5].
6th characteristics of cloud computing is multi tenacity which advocated by the Cloud Security Alliance [6]. It refers to the need for policy-driven enforcement, segmentation, service levels, as well as billing models for different consumer constituencies.

2. Security risks and guidance cloud for computing

Cloud computing represents a very dynamic area at the pre sent time, with new suppliers and new offerings arriving al l the time. There are a number of security risks associated with cloud computing that must be adequately addressed.

2.1 Security Risks

- **Loss of governance**
- **Responsibility ambiguity**
- **Isolation failure:** called guest-hopping attacks as this risk category covers the failure of separating the usage

of storage, memory, routing and even reputation between different tenants.

-**Vendor lock in:** Services that do not support portability of applications and data to other providers increase the risk of data and service unavailability.

- **Compliance and legal risks:**by migration to use cloud c omputing if the cloud provider cannot provide evidence of their own compliance with the relevant requirements or if the cloud provider does not permit audit by the cloud consumer.

- **Handling of security incidents**

- **Management interface vulnerability**

– **Data protection**

– **Malicious behavior of insiders**

- Business failure of the provider: data and applications to the consumer's business unavailable.

- **Service unavailability:** software failures in the provider's data center ,through failures of the communications between the consumer systems and the provider services.

– **Insecure or incomplete data deletion:** Requests to dele te cloud resources.

While the above security risks need to be addressed, use of cloud computing provides opportunities for innovation in provisioning security services that hold the prospect of improving the overall security of many organizations .

Cloud service providers should be able to offer advanced f acilities for supporting security and privacy due to their economies of scale and automation capabilities potentially a boon to all consumer organizations, especially those who have limited numbers of personnel with advanced security skills.

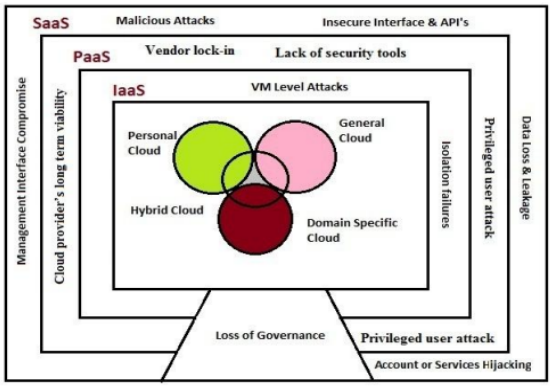

Figure 1 Cloud computing security risks categories [7]

2.2 Guidance for cloud computing

Consideration must be given to the different models of ser vice delivery: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) as each model brings different security requirements and responsibilities.
The prescriptive series of steps that should be taken by cloud consumers to evaluate and manage the security of their cloud environment with the goal of mitigating risk and delivering an appropriate level of support [8].

-Ensure effective governance, risk and compliance processes exist [9].
- Audit operational and business processes
- Manage people, roles and identities
- Ensure proper protection of data and information
- Enforce privacy policies
- Assess the security provisions for cloud applications
- Ensure cloud networks and connections are secure
-Evaluate security controls on physical infrastructure and facilities .
-Manage security terms in the cloud service level argument (SLA) .
- Understand the security requirements of the exit process

3. Banking in the cloud

The rapid emergence of cloud computing is transforming the way financial institutions think about how they consume their IT resources. Until now, technology has typically been a costly hurdle for financial institutions, particularly those in emerging markets where developing customized solutions or investing in advanced banking platforms has either been unfeasible or the result has been too many failures, too many resources used and too much time wasted. Cloud computing, which in the most basic of terms offers unlimited computing resource as a service on a pay-per-use basis, is proven to directly translate to less upfront, capital expense and reduced IT overheads, offering a cost-effective, simple alternative to accessing enterprise-level IT without the associated costs.

Cloud computing has the ability to make enterprise-level banking systems and associated technologies available in the cloud on a pay-per-use basis, now there is no barriers associated with this technology as anyone, anywhere can have access to banking systems without the cost and other.

Cloud computing offers compelling advantages, when it comes to financial services companies, the most important benefit is quite clear: the ability to scale on demand without procuring intensive, expensive infrastructure.

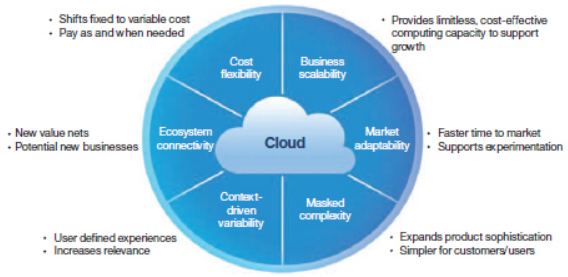

Figure 2 Banking in the Cloud

4. Implementation of cloud computing technology under banking system

As many banks' branches run under one central bank with same financial transactions, withdraw and deposit etc,. even if with same transaction we run individual banking system. So there will be central cloud server where all the computing (s/w and h/w) resources will be there where each end user can communicate through API and perform the appropriate operation.

The T24 on Windows Azure offering is based on a software-as a-service model (SaaS). This model allows financial institutions of all sizes and locations to quickly take full advantage of the rich functionality of T24, without having to manage and invest upfront capital in a complex on-premise deployment. And because T24 is offered as a pre-configured model bank, the solution can not only be rolled out quickly, but it requires very little customization.

4.1 Private cloud benefits

The private cloud is the first step towards cloud computing, and it is here that the most critical applications of the enterprise will be hosted for quite some time. The private cloud emerges stronger than the public cloud because it grants banks control over their IT while providing reduced complexity, increased flexibility, and all other benefits associated with cloud computing. Private clouds have emerged as the hot favorite of the banking industry also because in a financial environment where applications are critical and governed by stringent user industry compliance, they can provide high security. They ensure that no data is lost or misplaced and also provide the flexibility of control in order to modify resource configuration according to demand. Private clouds allow more systems to operate at high transaction volumes without loading the network or slowing the process, ensuring better customer experience. Since resources are rented instead of purchased, it helps convert CAPEX to OPEX, reducing the total cost of ownership. Private clouds come with the advantages of affordability and safety and enable a transition in banking. To guarantee long-term success, banks need to properly understand the technology and develop new applications that would benefit the customer. When an organization changes its infrastructure to a cloud configuration, it should be done in real-time to curb the wastage of unused resources. Technologies such as Cisco's Unified Computing Systems (UCS) help to monitor the server, storage, memory and network capacity. They can calculate, with reasonably high levels of accuracy, which servers require more resources and automatically prioritize them. A well designed private cloud computing platform also costs less than a dedicated server on a per server basis. Cloud based collaboration technologies can also provide a platform for application development, cost reduction and help banks to reach out to their customers more effectively. Beyond cost, they can create significant opportunities for banks to develop new business models that are customer-centric, thereby increasing growth and profitability.

There are six big benefits of the banking cloud:

1. Cut costs: cloud computing means banks will not have to invest heavily in dedicated hardware, software and related manpower. It is much easier for them to update their IT infrastructure and the cloud's modular, pay-on-demand model means they pay only for the hardware and software they need.

2. Improve flexibility and scalability: the cloud gives banks the ability to respond quickly to changing market, customer and technological needs. They can scale up and scale down technology according to requirement. The ability to respond quickly will be an important competitive edge.

3. Increase efficiency: banks will enjoy improved efficiency ratios and operating leverage. The standardisation inherent in the cloud could makes it easier to integrate new technologies and applications in the future. Because technology and business operations can be much more closely aligned, the cloud gives banks a golden opportunity to drive out complexity.

4. Serve clients faster: cloud computing makes new and bundled products and services easier to develop and launch, either on a stand-alone basis or in partnership. It eliminates procurement delays for hardware and software. Banks will be able to boost computing power to meet demand peaks and provide the latest treasury solutions without needing to worry about whether the technology is up to date. Corporates will be able to access bank systems using web browsers from anywhere at anytime.

5. Forge stronger client relationships: The combination of big data and potentially unlimited computing power will allow banks to develop systems capable of providing better insight into clients and make better decisions on their behalf. Services could become more customised.

6. Bring clients closer to their clients: transaction banking eases payments between buyers and sellers. At the moment the activities needed to process payments are inherently inefficient because they use different technology. But buyers and sellers could be brought together on shared applications in the cloud.

4.2 Challenges to cloud

Although cloud computing is not a new concept for banks, this sector has been slow in adopting the technology. The key concerns are that such deployment models could lead to an environment sprawl and a lack of control in terms of change management. This can further lead to security risks, reliability issues and a lack of effective business continuity planning. A lack of core application solutions has delayed the process further. From the public cloud standpoint, the issues are around regulation, location, liability and recoverability in the cloud. These are some of the reasons that have slowed down the adoption and deployment of cloud computing and rather led most banks to start building mini 'private' infrastructure clouds.
To reduce this risk, the management of the infrastructure that underpins these computing environments needs to move away from complex IT provisioning requests to the presentation of a series of standardized services. Through

the use of standardized processes and workflows, implementation risk is minimized, while established change management practices are supported. Reaching this state is the beginning of the journey to the cloud. Concerns about the external cloud and rebuttals to them not with standing, banks have evolved technologies, which virtualized the IT infrastructure within an enterprise, to deliver IT as a service to internal users, calling it the internal or private cloud.

The five main challenges of the banking cloud:

1. Security and compliance: maintain at all times the security of data. Banks need to demand stringent safety measures from suppliers and ensure new applications meet the latest and most rigorous security standards. Service Level Agreements (SLAs) are a must.

2. Reliability: ensure that applications and data are always available in the event of a natural disaster or an unpredictable event. Banks need to have stringent SLAs in place, complete with guarantees, end-game scenarios and remedies if a provider fails to meet service levels.

3. Cloud management: achieving visibility and measuring performance are harder to do, especially if, as seems likely, large banks will source cloud services from several providers and to use them for both internal – or private – and external, or public, services. This could result in a bank having to handle multiple security systems, and the need to ensure all parts of their business can communicate with each other and where necessary with clients. I

Increased use of various technology infrastructures and a mix of different cloud environments internally and externally mean banks will need to develop fully-fledged cloud management platforms. They will be a necessity to ensure banks can fully realise the cost savings and flexibility benefits of cloud computing.

4. Interoperability: banks will need to ensure data and applications can be moved across cloud environments from a number of providers. They should look to develop a single interface and management layer that can work across different platforms internally and externally.

5. Regulation: the rules governing the cloud vary from country to country. Many countries' data protection laws impose constraints on where data is kept, limiting take-up. This is why the EC's move to regulate the cloud is welcome.

Conclusion

Trust and security have prevented businesses from fully accepting cloud platforms. To protect clouds, providers must first secure virtualized datacenter resources, uphold user privacy, and preserve data integrity. Financial services organizations are starting to use cloud computing technologies in a number of areas, in particular for mobile applications, innovation testing and micro-banking. The banks need to know that this is all about 'business model transformation' and to achieve business agility for the next level of growth. The key is to ensure that each bank starts working on a cloud reference architecture, which will define its winning strategy.

References

[1] K. Hashizume, D. G Rosado, E. Fernz-Medina and E. B Fernandez "An analysis of security issues for cloud computing"; Hashizume et al. Journal of Internet Services and Applications 2013, 4:5; http://www.jisajournal.com/content/4/1/5.

[2] Wayne Jansen, Timothy Grance, "Guidelines on Security and Privacy in Public Cloud Computing", Draft Special Publication 800-144, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD 20899-8930.

[3] S. Jain , R. Kumar, S. Kumawat , S. K. Jangir " An analysis of security and privacy issues, Challenges with possible solution in cloud computing " , National Conference on Computational and Mathematical Sciences (COMPUTATIA-IV) – 2014 .

[4] Peter Mell, Timothy Grance, "The NIST Definition of Cloud Computing", Recommendations of the National Institute of Standards and Technology, Special Publication 800-145 .

[5] Viswa prakash babu, Banda Sreenivas, Thota Praveen Kumar, R.Jawahar Lal, "Cracking Bluetooth security" Int. Journal of Applied Sciences and Engineering Research, Vol. 3, No. 2, 2014, www.ijaser.com , ISSN 2277 – 8442

[6] Robert Gellman, "Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing", February 23, 2009 .

[7] M. Sharma, H. Bansal, A. K. Sharma ," Cloud Computing: Different Approach & Security Challenge"International Journal of Soft Computing and Engineering (IJSCE) , Volume-2, Issue-1, March 2012 .

[8] Tripathi, A., Mishra, A., IT Div., "Cloud Computing Security Considerations", Signal Processing, Communications and Computing (ICSPCC), IEEE International Conference,2011.

[9] K. Hwang, D. Li ,"Trusted Cloud Computing with Secure Resources and Data Coloring ",IEEE Computer Society , 2010 .