ISSN:0975-9646

Alert Areas of Cloud Security

Shuchita Bhargava, Rahul M. Samant

Mukesh Patel School of Technology Management and Engineering,
NMIMS University, Shirpur Campus
Mumbai, INDIA

***Abstract*— Cloud Computing has created much a boom over the past few years. Cloud computing basically serves an on-demand service and stores data of the client in segregated virtual locations. Cloud computing provides a multi customer virtual environment with cost according to the consumption resources by any client. Thus it is a cost reduction approach for the business entity. All the hype of this new technology is accompanied with various issues. This paper mainly focuses on the security issues regarding the infrastructure; the data stored and secures data transfer, various legal and regulatory issues of the cloud computing which are the major concerns that are preventing people to adopt cloud.**

***Keywords*— Private, Public and Hybrid Clouds, IaaS, PaaS, SaaS**.

I. Introduction

Cloud computing is a pool of resources, applications, servers, network of remote servers, virtual servers, storage. Forrester defines cloud computing as “A pool of abstracted, highly scalable and managed compute infrastructure capable of hosting and-customer applications and build by consumption”. Cloud computing provides ‘on-demand’ services and cost according to the usage of resources by the consumer. The applications of the client are stored at different virtual locations rather than same physical area. Cloud computing provides online services and environment according to the requirements of the client.

National Institute of Standards and Technology offers up several characteristics that it sees as essential for a service to be considered “Cloud.” These characteristics include:

- On-demand self-service.
- Broad network access.
- Resource pooling.
- Rapid elasticity.
- Measured service.

The cloud computing is categorized into three types:

- *IaaS (Infrastructure-as-a-Service)*

Infrastructure as a Service (IaaS) is a way of delivering Cloud Computing infrastructure – servers, storage, network and operating systems – as an on-demand service. Rather than purchasing servers, software, datacenter space or network equipment, clients instead buy those resources as a fully outsourced service on demand

- *SaaS(Software-as-a-Service)*

Software that is deployed over the internet can be considered as software as a service.. It provides a multi customer virtual automated environment. Thereby increase usability and functionality of the application.

- *PaaS(Platform-as-a-Service)*

PaaS can be defined as a computing platform that allows the creation of web applications quickly and easily and without the complexity of buying and maintaining the software and infrastructure underneath it. Storage, security of the applications is maintained by the provider. The customer gets the platform and the libraries from the provider to create software.

In client server environments data is often stored in insecure server rooms and frequently downloaded to desktop and laptop devices which can be stolen or lost. But in cloud the data is stored in a private web cloud using cloud architecture commonly used in defence organizations and intelligence agencies

II. Security Issues

There are number of security issues as it comprise of a pool of networks, databases, operating systems, virtualization, transaction management, memory management

2. 1 INFRASTRUCTURE ISSUES

Infrastructure is a security paradigm faced by the service provider. In the cloud, your data will be distributed over these individual computers regardless of where your base repository where your data is ultimately stored. Virtualization adopted by Cloud can give benefits to hackers and attackers to leak data. The statistics that show that one-third of breaches result from stolen or lost laptops and other devices and from employees accidentally exposing data on the Internet, with nearly 16 percent due to insider theft.

On the contrary problems which the clients face in cloud computing are due to slow and poor quality connections as a result clients cannot login or maintain a connection with online email, transactions on payments have not been affected etc. Thus leading higher dependency on traditional infrastructure then clouds.

Cloud needs high quality and high speed broadband connections (in kilobyte/sec) for efficient working and utilization. The Quality of Service can be judged based on the number of times the connections are dropped, the response time, extent of delays in processing of network data and the loss of data

2.2 SECURITY OF CLIENT APPLICATIONS

Applications and Data in the cloud are open to many attacks by the hackers and authorized access. Thus the provider and the client should have an agreement to prevent future security issues. The provider should manage the infrastructure and application availability, but they should not have access to the data without client’s permission. The providers should let the external third party to check the security relating client’s data and application and undergo security auditing. The provider may let some legal authority or any internal employee access to client’s data but it should always be informed to the client before he gives the access. This hardware based protection safeguards the client against software based attacks at the infrastructure level.

2.3 DATA PRIVACY-SECURING STORED DATA AND DATA TRANSFER

Data protection and privacy are often presented as being key risks where personal information. Fact is that employee irresponsibility and negligence (*e.g.* lost laptop, smart phone, etc.) cause many data security breaches, and hacks by cybercriminals are also on the rise. Moving data to the cloud can be a bad thing for data security if the vendor is weak on security and careless..

Concerns also arise by the owning organization that multitenancy clouds often pose risks to sensitive data.

"*Cloud is purchased at lower price and provides faster deployment of applications. 52% cloud application target business application. By 2013, 80% companies will spend 7 to 30% of their IT budget in cloud.*"

There have been cases where there has been a complete blackout of entire cloud services and washed out for hours and even days due to bugs.

- Google's Gmail-went down for 2 hours
- Citrix's GoToMeeting and GoToWebinar-were temporarily unavailable.
- Amazon.com's simple storage service-out of the commission for excruciating 8 hours.

2.4 GARTNER'S RESEARCH

Gartner Inc., World's leading information technology research and advisory company has identified security concerns that a cloud user must address with cloud computing providers before adopting:

- User Access:
- Regulatory compliance
- Data Location
- Data Segregation
- Disaster recovery verification
- Disaster Recovery
- Long term viability

2.5 LEGAL AND REGULATORE ISSUES

Legal issues in cloud computing as mentioned in one of the article 'Don't Overlook Legal Issues in the Cloud' by William B. Baker in May 2009-

A vastly important legal issue in "cloud computing" is jurisdiction. Bits and bytes stored in the cloud do actually physically reside on a server somewhere.

Cloud clients of US, Canada or the European Union, they are subject to Control Objectives for Information and related technology and safe harbor. Failure to adequately protect your data can have many consequences.

For US agencies Clinger-Cohen Act of 1996, the office of Management and Budget (OMB) Circular No. A-130, The Privacy act of 1974, E-Government Act of 2002.

- Clinger-Cohen Act assigns responsibilities for the efficiency, security and privacy of computer systems within the federal government and focusing information resource planning and reconstructing the strategies of work before investing in information systems.
- Privacy Act governs the collection, maintenance, use and dissemination of information about individuals that is maintained in system of record by federal agencies and can be retrieved by personal identifier.
- The E-Government Act of 2002 is a United States statute enacted on December 17, 2002. Its stated purpose is to improve the management and promotion of electronic government services and processes by establishing a Federal Chief Information Officer within the Office of Management and Budget.

III. ISSUES REGARDING PUBLIC CLOUD

As public cloud is an open infrastructure base many issues can rise regarding the security. Access can be a major problem. A person putting data in a public cloud cannot fully restrict its access. Being on a public cloud access restriction is far less as compared to private cloud. It is a big question as to how, when and what access rights should be given of some data.

Security policies in public cloud are common for all the members. Changes in those policies are not due to any particular user. These changes affect the data security even if you do not require that change individually.

Public clouds are more susceptible to attacks and breach. As infrastructure of the public cloud is shared segregation and protecting the confidentiality of data of different data is a major concern.

Encryption and key management can overcome these attacks to secure data from unauthorized access of data in public cloud.

IV. ISSUES REGARDING PRIVATE CLOUD

Private clouds are like your private virtual network (VPN) but still you should not have blind trust on these private clouds in regard to the security.

Private clouds are for a single organization where its employees have the access to its data and resources. Inside attacks can be a security concern in private clouds. More attention is given to security in private clouds than public clouds to maintain its confidentiality and integrity. To protect data from inside attack configuration of access controls is necessary according to the sensitivity of the data.

Private clouds mainly work on virtual machines. Security of private cloud can be enhanced by allowing communication between virtual machine and virtual machine only. Communication between virtual machine and physical Ethernet should be avoided.

Further private cloud virtual network should not entertain guest virtual network from other unsecure zone and deny any host.

V. MAJOR CHALLENGES PREVENTING CLOUD ADOPTION

Based on the survey conducted by IDC in 2008, the major challenges that prevent cloud computing from being adopted are-

- **Security**: Data and client application security is the major concern among all. Prevention against data losses, phishing.
- **Costing Model**: Migrating to cloud can significantly reduce the infrastructure cost. It does reuse the cost of data communication i.e cost of transferring an organization's data to and from the public and community cloud and the cost per unit of computing resource used is likely to increase.
- **Charging Model**: Is this the cost is calculated based on consumption of static computing.

- **Service Level Agreement (SLA)**: Although cloud users do not have control over the underlying computing resources, they do need to ensure the quality, availability, reliability and performance of these resources.
- **What to migrate**: According to the survey the seven IT systems/application being migrated to the cloud are: IT Management Applications (26.2%), Collaborative Application (25.4%), Personal Application (25%), Business Application (23.4%), Application Development and deployment (16.8%), Server capacity (15.6%) and Storage Capacity (15,5%). This research reveals that organizations still have security/privacy concerns in moving their data on to the cloud.
- **Cloud Interoperability issue**: The primary aim of interoperability is to realize the seamless fluid data across clouds and between cloud and local applications. Standardization appears to be good solution to address the interoperability issue.

VI. SOA And Cloud

Service Oriented Architecture (SOA) provides the architecture needed by any cloud. Service Oriented based architecture provide appropriate platform for efficient implementation of cloud services. SOA can provide the cloud service providers both front application logic and abstracted business logic. SOA in cloud provides cost optimization reusability and load balancing. SOA and cloud are complementary to each other.

- Agiliance's Cloud Risk Management Services provide security to enterprise, cloud providers. Customers can have broad set of options to select and are offered wider range of implemented services. Customers can access Cloud on Demand for beta versions, feedback.
- Athenahealth is a cloud based service in health care information technology which keeps continuous monitoring on medical patient's performance, treatments and patient's documents.
- Citrix provides secure-by-design cloud to protect data from attack. Data and services are managed and secured centrally wherever they are—public clouds, private clouds or enterprise datacenters—and delivered securely anywhere, over any kind of connection to any device.

VII. Securing Cloud Channels

The Unisys Secure Private Cloud solution is the second product Unisys has made available under its software channel initiative. The Unisys Stealth Solution Suite provides automated services providing time utilization resource optimization and easy for installations.

IBM with AT&T Inc. offer to provide secure channels for data transmission and access to the resources. It aims at providing high speed and security of AT&T's global network.

McAfee Cloud Security Framework applies its own security services to protect the data transmission and making cloud more secure. Data should be segregated on the basis of its sensitivity and then appropriate policies should be applied to keep it safe during its transfer.

VIII. Securing Cloud Storage

Control access for where the cloud store its data is important for enhancing data security. Cloud allows online data storage and makes it readily available wherever and whenever needed. Thus security of the data is required.

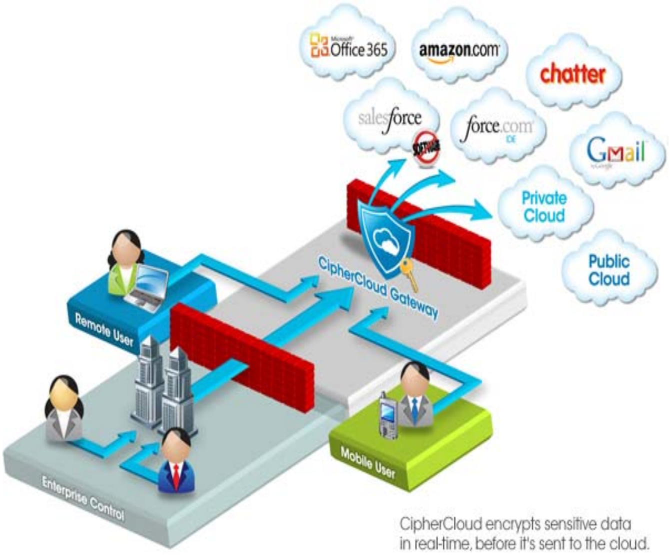
Safe Guard Encryption protects the data stored in cloud. Rightful people with correct encryption keys can access the data. Data should get industry-certified encryption.

The Cloud Storage Network's high-performance storage complements the key transaction processing systems at banks, asset managers, insurance companies, and other financial institutions.

IX. Cipher Cloud

CipherCloud eliminates concerns relating to data privacy, residency, security and compliance. CipherCloud provide data protection for public and private clouds.

As stated by Pravin Kothari Founder and CEO of CipherCloud," CipherCloud applies encryption, before sensitive data leaves the enterprise. CipherCloud is deployed as an in-line security gateway within the enterprise network that sits between the users and cloud applications. Enterprises can identify which data they consider sensitive (such as proprietary information, personally-identifiable information or other regulated data). When that data is posted or updated into the cloud, we apply the selected encryption or tokenization method, on the fly, to protect that data before it leaves the enterprise network. We reverse the process when employees access the cloud application through the gateway, decrypting data in real time so the users see the actual data rather than the encrypted version that resides within the cloud. CipherCloud's highly securing encryption and tokenization preserves both the format and operations of the data, so that the cloud application remains operational but its real content remains locked within the enterprise".



CipherCloud encrypts sensitive data in real-time, before it's sent to the cloud.

X. CONCLUSION

Cloud services are an ideal way to manage all your digital content without limitations. Still there is much confusion regarding the security of cloud computing to keep the integrity and confidentiality of data and applications of the client protected hence many today also hesitate to shift their businesses from the traditional infrastructure to entrusted third party clouds.

Much of the work is in process to make cloud more secure and make it for usable and acceptable. Gartner's strategic planning assumption expects at least 25% of enterprises will use a single platform to secure all their clouds. Instead of relying on disparate systems, enterprises will save 30%. This is already a reality today for CipherCloud customers. Enterprises are using encryption, tokenization, and integrated security services like malware detection to secure data in Sales force, Force.com, Gmail, Office 365,Amazon AWS, and more clouds. CipherCloud is joined by Cisco, Intel, McAfee, and Symantec in Gartner's representative set of vendors in the Cloud Access Security Brokers category.

Some of the world's largest tech companies have launched cloud services, including Apple, Amazon and Google. It is stating that the health care cloud computing market will grow from $1.7 billion in 2011 to $5.4 billion by 2017, an encouraging 20.5% compounded annual growth rate. The National Science Foundation announced it had awarded $5 million in grants to fourteen universities as part of its Cluster Exploratory (CLuE) program.

From the above mentioned facts it may be concluded that Cloud Computing is mushrooming rapidly but by adopting more secure strategies including encryption, access control on data, securing the channel transmission the technology may flourish much more without having consumers to comment on the security issues.

REFERENCES

[1] "Making the leap to the cloud: IS my data private and secure?"- CS.ThomsonReuters.com

[2] "Security Issues for cloud computing" International Journal of Information Security and Privacy, 4(2), 39-51, April-June 2010 39 Copyright © 2010, IGI Global.

[3] "Security and privacy issues of cloud computing; Solutions and secure framework" Prof: Asha Matthew* International Journal of Multidisciplinary Research Vol.2 Issue 4, April 2012, ISSN 2231 5780

[4] "Understanding the cloud computing stack- IaaS, SaaS, PaaS" Diversity ltd

[5] Sophos Data Sheet 1.12v1.dNA, SOPHOS LTD.

[6] "Healthcare Industry Finds that Hybrid Cloud Solutions Offer Enhanced Cloud Protection & Data Security" David Canellos PerspecSys President and CEO

[7] "Oracle Enterprise Gateway: Integration with Oracle Service Bus and Oracle Web Services Manager" *by William Markito Oliveira and Fabio Mazanatti*

[8] "Emerging issues: Cloud programming" Southern African Internet Governance Forum Issue Paper no: 1 of 5

[9] "Client computing in the cloud" Intel IT Center

[10] "Data security in cloud computing" Vic (J.R.) Winkler7/11/2011 11:54 AM EDT

[11] "Logica and RightScale deliver hybrid cloud solution for enterprise customers with Windows Azure"- Toronto, Canada July 11, 2012, Logica and RightScale

[12] "Cloud computing security issues and challenges" International Journal of computer networks, volume 3 issue 5, 2011L

[13] "Cloud computing: Legal and regulatory issue" Vic (J.R.) Winkler

[14] eweek.com

[15] "McAfee Cloud Security Platform Building a secure bridge between the enterprise and the cloud"-Solution brief, McAfee Intel Company.

[16] The Cloud: Understanding the Security, Privacy and Trust Challenges- Neil Robinson, Lorenzo Valeri, Jonathan Cave & Tony Starkey (RAND Europe) Hans Graux (time.lex) Sadie Creese & Paul Hopkins (University of Warwick)

.