Comparative study of security parameters by Cloud Providers

Manish Kumar Aery[1]
Faculty of Computer Applications,
Global Infotech Institute of IT & Management (LPUDE)
aery.manish1@gmail.com,

Sumit Gupta[2]
Lecturer Computer Application,
Lovely Professional University
10.sumit@gmail.com,

ABSTRACT

Security is one of the major issues today around the world. Either it is a home user or Corporate User, a small PC or a Server System, nothing is totally secure, lots of issues have been raised regarding security. In this paper, we will be comparing the architectures of the Cloud Providers and how and what Cloud Services they are providing. Here, we will also discuss about the different Security parameters offered by different Cloud Providers and will present the comparative study of security provided at different cloud services viz. Infrastructure as a Service, Platform as a Service and Software as a Service.

Keywords: Cloud Computing, Architecture of Cloud Computing, Cloud Security.

1. INTRODUCTION

The term IT is the form of revolution, every day, every time, every minute & even every second. Day by day, number of researches and inventions are being done. Lots of researches are being carried out these days, but some of them come into existence, in other words, some of them are meaningful. But, one major topic, that is being discussed these days is the concept of cloud computing. As we all know, that cloud computing refers to the delivery of computing and storage capacity as a service to a heterogeneous community of end-recipients. But the research does not end here. It is just a beginning. Lots of views, discussions, and researches have been carried out but still there is a lot more to be done. Many of the top IT companies have started implementing the concept of cloud, but security is the root cause for any company to look-in before adopting that particular new concept/technology. So, one of the major areas to be discussed in cloud computing is security. It's a challenge for everyone, whether be it in case of business, or some other field. Security is a challenge for a new technology and cloud computing is facing the same. Still clouds provided by many of the companies are not secure. This may be due to lack of protocols, lack of trust etc. This mainly relates to the area where financial transactions are being carried out. The best example is Online Banking. The main target of each and every organization today, is to make its data secure by any means. But now, as these days, most of the top companies, act as cloud providers, the data needs to be much more secure. It becomes the responsibility of the cloud provider organization to secure the data of the customer. We can relate cloud security directly to information security, which may be a set of policies, technologies and any kind of controls to make the data secure and protected. So, two people fall into security issues/concerns – One the cloud providers, and other the customers. The main point is that the provider must take care that their infrastructure is secure which can help securing customers data and applications, and the customers must take care that their data is protected. So, the main concept that will be discussed in this paper is cloud security and the comparison between different organizations that how they provide cloud as a service.

2. Cloud Computing:

The term cloud computing is a technology that uses the internet and central remote server maintained data and application. Cloud Computing includes data, application and storage and also provides these three basic services i.e. Software as a service, platform as a service and infrastructure as a service. In software as a service model, companies provide software services to different customers by virtualized environment. In platform as a service, companies provide different software development environment to the user in which they can develop their applications by using the company's platform. In infrastructure as a service, the user of the cloud uses the physical infrastructure of the cloud providers such as servers, hard disks etc. The main advantage of cloud computing is that the customer pays for what they are using.

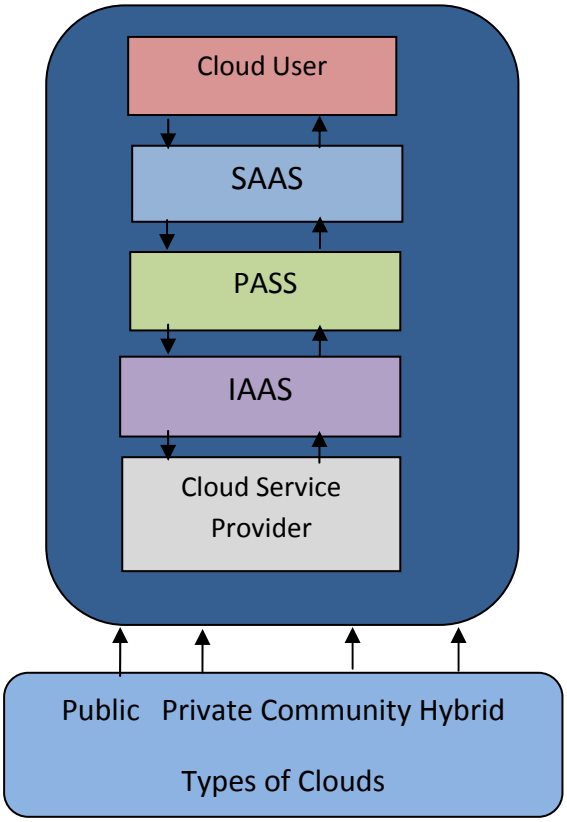

FIGURE 1

3. Cloud Computing Security

The security of cloud is one of the major challenges for cloud providers. All cloud providers provide best security solutions but still clouds are not secure. The cloud security is all about making cloud more secure. It is basically a control required for organization to accept financial as well as legal responsibilities by using set of policies, technologies and controls organized to shield the data, privacy, storage, applications, operations etc. of cloud computing.

3.1 Security Challenges

An environment where all the major services of any computing environment i.e. Infrastructure, software& platform has been provided at same place by some of the major organization will increase the risk of affecting large amount of data and applications and also been highly targeted zone for the attackers. Providing the cloud services is one of the major addition and interests of companies but it increase more risk too.

4. Architecture of different Cloud Providers

4.1 IBM Cloud Architecture

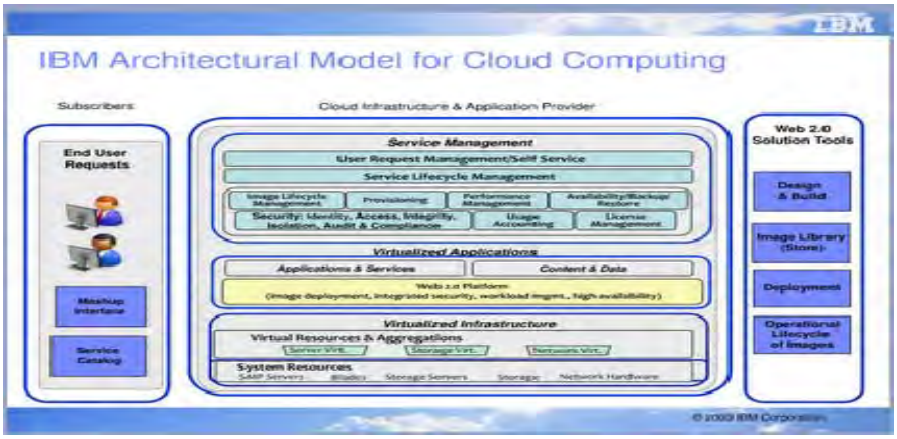

Fig-2 Cloud Architecture Provider by IBM

4.2 Bluelock Cloud Architecture

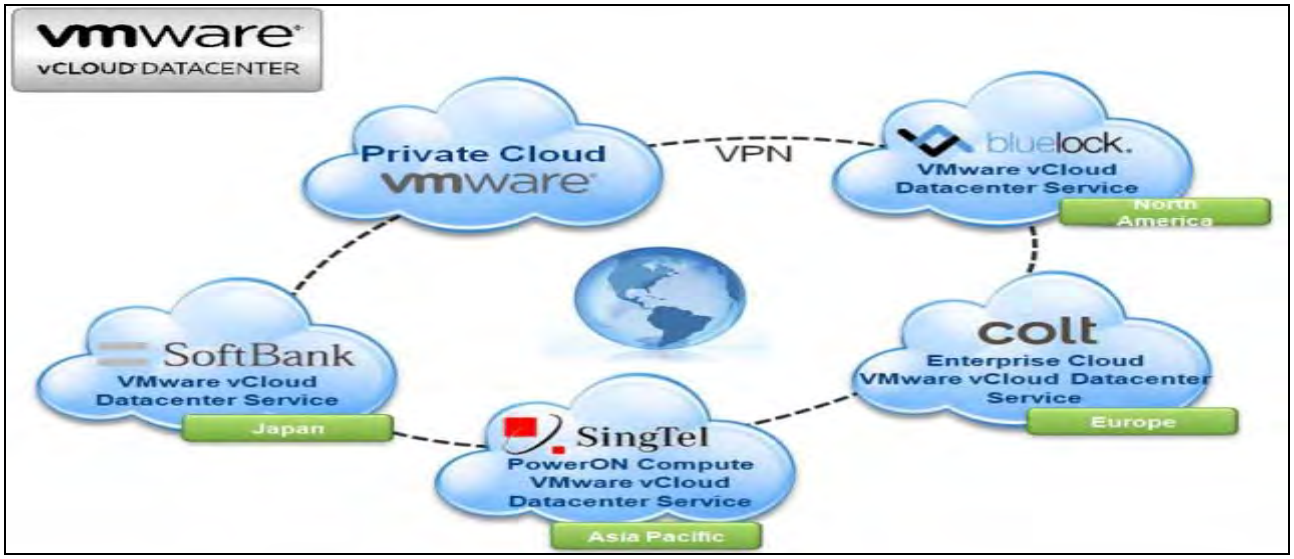

Fig-3 Cloud Architecture Provided by Bluelock

4.3 Rackspace Cloud Architecture

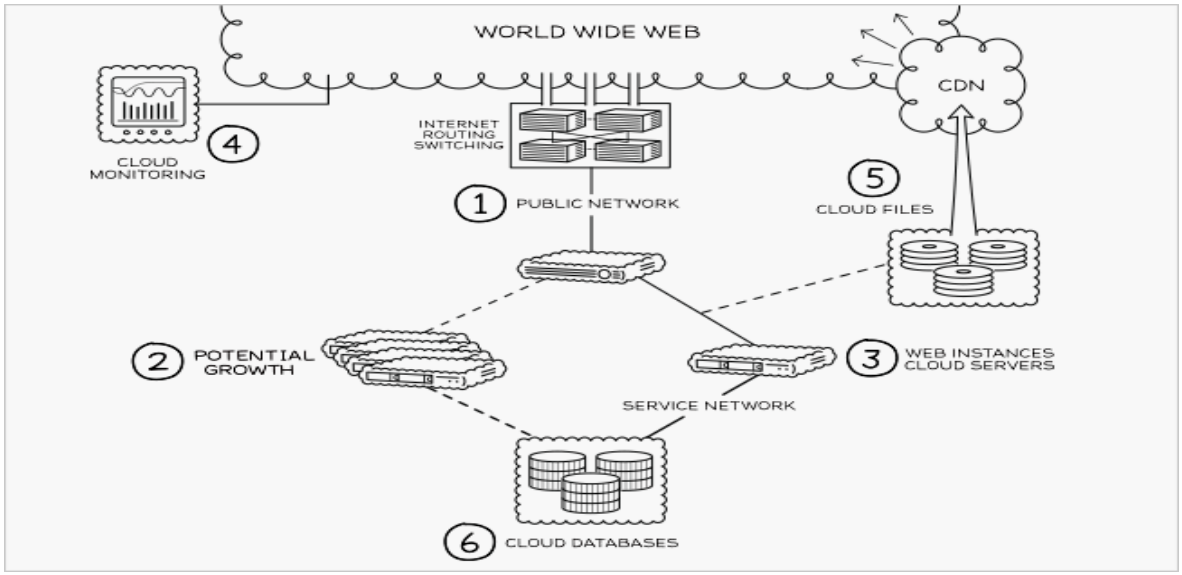

Fig-4 Basic Cloud Solution of Rackspace

5 CHOOSING A CLOUD PROVIDER

As we know and discuss above that the cloud providers provide the services on infrastructure, software and platform. Different users has different requirements, some want infrastructure, some want software, some want platform and some want all the services. So it is very important for user prospective what kind of services they want and who will best provide them choosing the cloud provider is one exercise that has been done by cloud user. Every organization has their own set of billing, pricing, support and other parameters. Now its completely depend on the enterprise/user that which of cloud services they need to adopt and from which organization

Fig-5.1 Different Cloud Providers

6 CLOUD PROVIDERS-A COMPARISON TABLE

The table below shows the comparison between different cloud providers over the various security parameters

Table 6.1-Comparision table

Parameters	IBM	Blue Lock	RackSpace
Data Security	It pretends the way data is stored and accessed Encrypting and managing encryption keys of data in transit to the cloud or at rest in the service provider's data center are critical to protect data privacy and comply with compliance mandates. The encryption of mobile media and the ability to securely share those encryption keys between the cloud service provider and the customer is an important and often overlooked need	In blue lock they use NETAPP virtual storage console which provide both operating system and application consistent backup with both VMware snapshoot and NETAPP array biased snapshoot at both VMDK and file level driven by end user defined policy	Anti-virus protection security. Firewall services are being used. Encryption technology of SSL is being used to secure data. Special techniques are applied to guard the data against worms and Trojans
Physical Security	All the components of cloud infrastructure should be physically secure, weather it is router, or any storage device, security must be ensured for each and every component of a cloud. Physical access using biometric access control measures and close circuit television (CCTV) monitoring acts like a safeguard.	They provide physical security by internal and external high definition video recorders that can record thousand hours video footage. Provide three factor biometric authentications for access control. Daily physical audit trails has been done on each and every end point. Card key and coded entry for each individual	Data center access limited to RackSpace data center technicians. Biometric Scanning for controlled data center access Security camera monitoring at all data centers 24*7 onsite staff provides additi-onal protection against Unauthorized entry.
Storage security	IBM provides intercloud storage by: ➢ Confidentiality through encryption ➢ Integrity with crypto-graphic hashing and		It provides support for direct attached storage. Shared Storage Area Network. Dedicated Storage Area Network. Dedicated Network Attached Storage

	signatures resilience with replication		
Application Security	To ensure that the data is not exposed, suspension and demolition of images must be performed carefully	Bluelock provides all of its cloud clients with dedicated VALNs which ensure isolation from all other clients. At the environment level security includes enter-prise-class firewalls. These fully managed devices are also virtual availability mode for maximum fault tolerance. Within the virtual cloud Enterprise environment all clients are provided a dedicated checkpoints virtual machine appliance which provides services and can optionally support. Intrusion prev-ention and detection capabilities as well as web Application firewalls	RackSpace has certified expert database admini-strators to manage the critical database and get the best and optimal performance from your system it can provide ➢ Flexible database licensing ➢ Installation services ➢ Monitoring and troubleshooting ➢ Emergency response services
Operational Security		In bluelock the client firewalls maintain a authorization log of remote access methods such as SSL or IPsec VPN as well as log of what firewall rules are configured and when they are changed for both win server 2008 and Linux virtual servers. Bluelock uses industry leading patch management and security policy auditing software to ensure that managed operating systems remain compliant. Operating system venders patches are applied on regular schedule and reports are provided to show what patches are applied to manage virtual servers	Systems access logged and tracked for auditing purposes. Secure document-destruction policies for all sensitive information. Best practices used in the random generation of initial passwords. All passwords are encrypted during the transmission and while in storage at RackSpace. Help available from RackSpace in configuring system logging to create a system audit trail.
Privacy	IBM offers InfoSphere Optim and InfoSphere Gurdium solutions for data security and privacy which protects diverse data types across different locations throughout the enterprise, including the protection of structured and unstructured data in both production and non production	The bluelock use following privacy factors: Registration, e-newsletter, service related Announcements, Client Service, Children Privacy, cookies, Choice/Opt-out, Business Transactions.	All employees trained an documented information security and privacy RackSpace offers a portfolio of private cloud solutions, Each backed by the exceptional service branded as financial support

	environment		

7 CONCLUSION

The above discussion on various security parameters shows that how the security has been needed by user and should provide by cloud providers. We also show the importance of security and its challenge. As we see that all the organizations provide different type of security at different levels. Security refers to confidentiality. Meaningful transparency and disclosure is a necessity from security point of view, Cloud providers already provide algorithms for generating hashes, whenever a file is stored in cloud, which bypasses the need for encryption. Our future work will be providing the some solutions to security challenges.

8 References

[1] IBM-Thoughts on cloud openness
[2] Bluelock-Announcing support for global connect
[3] www.rackspace.co.uk/solutions-configurator
[4] On-demand security architecture for cloud computing
[5] A Cloud-Oriented Cross-Domain Security Architecture
[6] Dependability in the cloud: Challenges & opportunities
[7] www.mhprofessional.com/downloads/products/0071626948/0071626948_chap01.pdf