Volume 8, No. 4, May 2017 (Special Issue)
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
REVIEW ARTICLE
Available Online at www.ijarcs.info

Cloud Computing Risks and Benefits

Er. Gurpinder Singh[1]
Ph.D Scholar
Sant Baba Bhag Singh University[1]
Jalandhar, Punjab, India[1]
Sirhind007@gmail.com[1]

Parminderpal[2]
M.Tech. Scholar
Sant Baba Bhag Singh University[2]
Jalandhar, Punjab, India[2]
parminder_mahey@yahoo.com[2]

***Abstract:*-The cloud is a next generation platform that provides dynamic resource pools, virtualization and high Availability. The service oriented, loose coupling, strong fault tolerant, business model and ease use are main characteristics of cloud computing. However there are some risks also.Cloud computing provides captivating benefits and cost-effective options for IT hosting and expansion, new risks and opportunities for security exploits are introduced**

Key Terms: Cloud computing, Service model, Risks.

I. INTRODUTION

Cloud Computing is one of the newest and most promising efforts to bring computing to the user as a service rather than a product. Cloud computing is essentially the management and provision of applications, information and data as a service. These services are provided over the internet, often on a pay-as-you-go based model. Cloud computing provides a convenient way of accessing computing services, independent of the hardware you use or your physical location. It relieves the need to store information on your PC, mobile device or gadget with the assumption that the information can be quickly and easily accessed via the net. Cloud computing also negates the need to download or install dedicated software on your own computer, freeing up on board memory and reducing energy costs. Economically, the main appeal of cloud computing is that customers only use what they need, and only pay for what they actually use. Resources are available to be accessed from the cloud at any time, and from any location via the internet. There's no need to worry about how things are being maintained behind the scenes – you simply purchase the IT service you require as you would any other utility. Because of this, cloud computing has also been called utility computing, or 'IT on demand [1]

The NIST definition is one of the clearest and most comprehensive definitions of cloud computing and is widely referenced in USgovernment documents and projects. This definition describes cloud computing as having five essential characteristics, three service models, and four deployment models. The essential characteristics are:

a) *On-demand self-service:* computing resources can be acquired and used at any time without the need for human interaction with cloud service providers. Computing resources include processing power, storage, virtual machines etc.

b) *Broad network access:* the previously mentioned resources can be accessed over a network using heterogeneous devices such as laptops or mobiles phones.

c) *Resource pooling:* cloud service providers pool their resources that are then shared by multiple users. This is referred to as multi-tenancy where for example a physical server may host several virtual machines belonging to different users.

d) *Rapid elasticity*: a user can quickly acquire more resources from the cloud by scaling out. They can scale back in by releasing those resources once they are no longer required.

e) *Measured service:*resource usage is metered using appropriate metrics such monitoring storage usage, CPU hours, bandwidth usage etc. [2]

II. SERVICE MODELS

The three most common service models are:

A. *Software as a Service (SaaS):* This is where users simply make use of a web-browser to access software that others have developed and offer as a service over the web. At the SaaS level, users do not have control or access to the underlying infrastructure being used to host the software. Sales force's Customer Relationship Management software3 and Google Docs4 are popular examples that use the SaaS model of cloud computing.

B. *Platform as a Service (PaaS):* This is where applications are developed using a set of programming languages and tools that are supported by the PaaS provider. PaaS provides users with a high level of abstraction that allows them to focus on developing their applications and not worry about the underlying infrastructure. Just like the SaaS model, users do not have control or access to the underlying infrastructure being used to host their applications at the PaaS level. Google App Engine5[4] and Microsoft Azure6 are popular PaaS examples.

C. *Infrastructure as a Service (IaaS):* This is where users acquire computing resources such as processing power, memory and storage from an IaaS provider and use the resources to deploy and run their applications. In contrast to the PaaS model, the IaaS model is a low level of abstraction that allows users

CONFERENCE PAPERS
National Conference on Emerging Trends on Engineering & Technology (ETET-2017)
On 21st April 2017
University Inst. of Engg. & Tech. & University Inst. of Computer, SBBS University, Punjab (India)

to access the underlying infrastructure through the use of virtual machines. IaaS gives users more flexibility than PaaS as it allows the user to deploy any software stack on top of the operating system. However, flexibility comes with a cost and users are responsible for updating and patching the operating system at the IaaS level. Amazon Web Services' EC2 and S37[3] are popular IaaS examples.

III. DEPLOYMENT MODELS

The NIST[6] definition defines four deployment models:

A. *Public Cloud:* In simple terms, public cloud services are characterized asbeing available to clients from a third party service provider via the Internet. The term "public" does not always mean free, even though it can be free or fairly inexpensive to use. A public cloud does not mean that a user's data is publically visible; public cloud vendors typically provide an access control mechanism for their users. Public clouds provide an elastic, cost effective means to deploy solutions.

B. *Private Cloud:* A private cloud offers many of the benefits of a public cloudcomputing environment, such as being elastic and service based. The difference between a private cloud and a public cloud is that in a private cloud-based service, data and processes are managed within the organization without the restrictions of network bandwidth, security exposures and legal requirements that using public cloud services might entail. In addition, private cloud services offer the provider and the user greater control of the cloud infrastructure, improving security and resiliency because user access and the networks used are restricted and designated.

C. *Community Cloud:* A community cloud is controlled and used by a groupof organizations that have shared interests, such as specific security requirements or a common mission. The members of the community share access to the data and applications in the cloud.

D. *Hybrid Cloud:* A hybrid cloud is a combination of a public and private cloud That interoperates. In this model users typically outsource non-business critical information and processing to the public cloud, while keeping business-critical services and data in their control.

IV. CLOUD COMPUTING RISKS

A. *Attacks targetingshared-tenancy environment:-*

A virtual machine (VM) is the software implementation of a computer that runs its own operating system and application as if it was a physical machine (VMware 2009). Multiple VMs can concurrently run differentsoftware applications on different operating system environments on a single physical machine. This reduces hardware costs and space requirements. In a shared-tenancy cloud computing environment, data from different clients can be hosted on separate VMs but reside on a single physical machine. This provides maximum flexibility. Software applications running in one VM should not be able to impact or influence software running inanother VM. An individual VM should be unaware of the other VMs running in the environment as all actions are confined to its own address space. In a recent study, a team of computer scientists from the University of California, San Diego and Massachusetts Institute of Technology examined the widely-used Amazon EC2 services. They found that 'it is possible to map the internal cloud infrastructure, identify where a particulartarget VM is likely to reside, and then instantiate new VMs until one is placed co-resident with the target'. This demonstrated that the research team were able to load their eavesdropping software onto the sameservers hosting targeted websites. By identifying the target VMs,attackers can potentially monitor the cache(a small allotment of high-speed memoryused to store frequently-used information)in order to steal data hosted on the samephysical machine . Suchan attack is also known as a *side-channelattack*.The findings from this research may onlybe a proof-of-concept at this stage, butit raises concerns about the possibility ofcloud computing servers being a centralpoint of vulnerability that can be criminallyexploited. The Cloud Security Alliance, forexample, listed this as one of the top threatsto cloud computing.Attacks have surfaced in recent yearsthat target the shared technology insideCloud Computing environments. Diskpartitions, CPU caches, GPUs, and othershared elements were never designedfor strong compartmentalization. As aresult, attackers focus on how to impactthe operations of other cloud customers,and how to gain unauthorized access todata. (Cloud Security Alliance 2010: 11)

B. *VM-based malware:*

Vulnerabilities in VMs can be exploitedby malicious code (malware) such asVM-based rootkits designed to infect bothclient and server machines in cloud services.Rootkits are cloaking technologies usuallyemployed by other malware programs toabuse compromised systems by hiding files,registry keys and other operating systemobjects from diagnostic, antivirus andsecurity programs. For example, in April2009, a security researcher pointed outhow a critical vulnerability in VMware's VMdisplay function could be exploited to runmalware, which allows an attacker 'to readand write memory on the "host" operatingsystem [OS]'.VM-based root kits, as pointed out by Price(2008: 27), could be used by attackers to'gain complete control of the underlying OSwithout the compromised OS being awareof their existence…[and] are especiallydangerous because they also control allhardware interfaces. Once the VM-based rootkits are installed on the machine, theycan "view keystrokes, network packets,disk state, and memory state, while thecompromised OS remains oblivious"'.

C. *Botnet hosting***:**

Bot malware typically takes advantage ofsystem vulnerabilities and software bugsor hacker-installed backdoors that allowmalicious code to be installed on machineswithout the owners' consent or knowledge.They then load themselves into computersoften for nefarious purposes. Machinesinfected with bot malware are then turnedinto ‘zombies’ and can be used as remoteattack tools or to form part of a Botnetunder the control of the Botnet controller.Zombies are compromised machineswaiting to be activated by their commandand control (C&C) servers. The C&C serversare often machines that have beencompromised and arranged in a distributedstructure to limit traceability.Cybercriminals could potentially abuse cloudservices to operate C&C servers to carry outdistributed denial-of-service (DDoS) attacks,which are attacks from multiple sourcestargeting specific websites by flooding aweb server with repeated messages, tyingup the system and denying access tolegitimate users, as well as other cybercriminal activities. In December 2009, forexample, a ‘new wave of a Zeus bot (Zbot)variant was spotted taking advantage ofAmazon EC2’s cloud-based services for itsC&C…functionalities’ .

D. Launch pad for bruteforce and other attacks:

There have also been suggestions that thevirtualised infrastructure can be used as alaunching pad for new attacks. A securityconsultant recently suggested that it maybe possible to abuse cloud computingservices to launch a brute force attack(a strategy used to break encrypted databy trying all possible decryption key orpassword combinations) on various typesof passwords.

E. Data availability(Business continuity):

A major risk to business continuity in thecloud computing environment is loss ofinternet connectivity (that could occur ina range of circumstances such as naturaldisasters) as businesses are dependenton the internet access to their corporateinformation. In addition, if vulnerability isidentified in a particular service provide bythe cloud service provider, the business mayhave to terminate all access to the cloudservice provider until they could be assured that the vulnerability has been rectified.There are also concerns that the seizureof a data-hosting server by law enforcementagencies may result in the unnecessaryinterruption or cessation of unrelatedservices whose data is stored on the samephysical machine.

F. Rogue clouds:

Just like entrepreneurs, cybercriminals andorganised crime groups are always on thelookout for new markets and with the riseof cloud computing, a new sector forexploitation now exists. Rogue cloud serviceproviders based in jurisdictions with laxcybercrime legislation can provideconfidential hosting and data storageservices for a usually steep fee. Suchservices could potentially be abused byorganised crime groups to store anddistribute criminal data (eg child abusematerials for commercial purposes) to avoidthe scrutiny of law enforcement agencies.Hosting confidential business data withcloud service providers involves the transferof a considerable amount of managementcontrol to cloud service providers thatusually results in diminished control oversecurity arrangements. There is the riskof rogue providers mining the data forsecondary uses such as marketingand reselling the mined data to otherbusinesses. Unfortunately, clients (especially SMEs) areoften less aware of the risks and may nothave an easy way of determining whethera particular cloud service provider istrustworthy. Tim Watson, head of thecomputer forensics and security group atDe Montfort University remarked that ‘oneprovider may offer a wonderfully secureservice and another may not, if the lattercharges half the price, the majority oforganisations will opt for it as they haveno real way of telling the difference’

G. Regulation and governance:

The privacy and confidentiality risks facedby businesses that use cloud services alsodepend to a large extent on the terms ofservice and privacy policy established bythe cloud service providers. Failure tocomply with data protection legislationmay lead to administrative, civil and criminalsanctions. Data confidentiality and privacy‘risks may be magnified when the cloudprovider has reserved the right to change itsterms and policies at will’.

V. BENEFITS

The following are some of the possible benefits for those who offer cloud computing-based services and applications:

a) *Cost Savings:* - Companies can reduce their capital expenditures and use operational expenditures for increasing their computing capabilities. This is a lower barrier to entry and also requires fewer in-house IT resources to provide system support.
b) *Scalability/Flexibility:*- Companies can start with a small deployment and grow to a large deployment fairly rapidly, and then scale back if necessary. Also, the flexibility of cloud computing allows companies to use extra resources at peak times, enabling them to satisfy consumer demands.
c) *Reliability:*-Services using multiple redundant sites can support business continuity and disaster recovery.
d) *Maintenance:*-Cloud service providers do the system maintenance, and access is through APIs that do not require application installations onto PCs, thus further reducing maintenance requirements.
e) *Mobile Accessible:*- Mobile workers have increased productivity due to systems accessible in an infrastructure available from anywhere

VI. CONCLUSION

Vulnerabilities in a particular cloud service or cloud computing environment can potentially be exploited by criminals and actors with malicious intent. However, no single public or private sector entity ‘owns’ the issue of cyber security. There is, arguably, a need to take a broader view and promote transparency and confidence building between cloud service providers, businesses and government agencies using cloud services as well as between government and law enforcement agencies In addition, an effective cyber-security policy should be comprehensive and encompass all (public and private sector) entities.

REFERENCE

[1] Ian Foster. What is the Grid? A Three Point ChecklistJuly 2002. Argonne National Laboratory & University of Chicago http://dlib.cs.odu.edu/ WhatIsTheGrid.pdf

[2] Software as a service,Wikipedia, ttp://en.wikipedia.org/wiki/Software_as_a_service>

[3] Amazon, “Amazon Web Services,” http://aws.amazon.com/.

[4] Google, “Google app Engine, “http://code.google.com/appengine/.

[5] Sales force, “CRM”, http://www.salesforce.com/

[6] “What is cloud computing?” http://searchcloudcomputing.techtarget.com/s Definition

[7] /0sid201gci1287881, 00.htmlNIST, http://csrc.nist.gov/groups/SNS/cloudcomputing/..

[8] Foster, Y. Zhao, I. Raicu and S. Lu, “Cloud Computing and Grid Computing 360-Degree Compared”, Proceedings of the IEEE Grid Computing Environments Workshop, pp. 1-10, 2008

[9] Kaufman LM 2009. Data security in the world of cloud computing. IEEE Security & Privacy July/ August: 61–64

[10] Keizer G 2009. VMware bug allows Windows hack to attack Macs. Computerworld 16 April. http://www.networkworld.com/news/2009/041509-vmware-bug-allowswindows-hack.html