Cloud Computing Risks and Benefits

I. INTRODUCTION

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 mobile 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
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 as being 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 cloud computing 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 group of 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 targeting shared-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 different software 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 in another 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 particular target VM is likely to reside, and then instantiates 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 same servers hosting targeted websites. By identifying the target VMs, attackers can potentially monitor the cache(a small allotment of high-speed memory used to store frequently-used information) in order to steal data hosted on the same physical machine. Such an attack is also known as a side-channel attack. The findings from this research may only be a proof-of-concept at this stage, but it raises concerns about the possibility of cloud computing servers being a central point of vulnerability that can be criminally exploited. The Cloud Security Alliance, for example, listed this as one of the top threats to cloud computing. Attacks have surfaced in recent years that target the shared technology inside cloud computing environments. Disk partitions, CPU caches, GPUs, and other shared elements were never designed for strong compartmentalization. As a result, attackers focus on how to impact the operations of other cloud customers, and how to gain unauthorized access to data. (Cloud Security Alliance 2010: 11)

B. VM-based malware:

Vulnerabilities in VMs can be exploited by malicious code (malware) such as VM-based rootkits designed to infect both client and server machines in cloud services. Rootkits are cloaking technologies usually employed by other malware programs to abuse compromised systems by hiding files, registry keys and other operating system objects from diagnostic, antivirus and security programs. For example, in April 2009, a security researcher pointed out how a critical vulnerability in VMware’s VMdisplay function could be exploited to run malware, which allows an attacker to read and write memory on the "host" operating system [OS]'VM-based root kits, as pointed out by Price (2008: 27), could be used by attackers to gain complete control of the underlying OS without the compromised OS being aware of its existence...[and] are especially dangerous because they also control all hardware interfaces. Once the VM-based rootkits are installed on the machine, they can “view keystrokes, network packets, disk state, and memory state, while the compromised OS remains oblivious”.

C. Botnet hosting:

Bot malware typically takes advantage of system vulnerabilities and software bugs or hacker-installed backdoors that allow malicious code to be installed on machines without the owners’ consent or knowledge. They then load themselves into computers often for nefarious purposes. Machines infected with bot malware are then
turned into ‘zombies’ and can be used as remote attack tools or to form part of a Botnet under the control of the Botnet controller. Zombies are compromised machines waiting to be activated by their command and control (C&C) servers. The C&C servers are often machines that have been compromised and arranged in a distributed structure to limit traceability. Cybercriminals could potentially abuse cloud services to operate C&C servers to carry out distributed denial-of-service (DDoS) attacks, which are attacks from multiple sources targeting specific websites by flooding an web server with repeated messages, tying up the system and denying access to legitimate users, as well as other cybercriminal activities. In December 2009, for example, a ‘new wave of a Zeus bot (Zbot) variant was spotted taking advantage of Amazon EC2’s cloud-based services for its C&C… functionalities’.

D. Launch pad for brute force and other attacks:
There have also been suggestions that the virtualised infrastructure can be used as a launching pad for new attacks. A security consultant recently suggested that it might be possible to abuse cloud computing services to launch a brute force attack (a strategy used to break encrypted data by trying all possible decryption key or password combinations) on various types of passwords.

E. Data availability (Business continuity):
A major risk to business continuity in the cloud computing environment is loss of internet connectivity (that could occur in a range of circumstances such as natural disasters) as businesses are dependent on the internet access to their corporate information. In addition, if a vulnerability is identified in a particular service provide by the cloud service provider, the business may have to terminate all access to the cloud service provider until they could be assured that the vulnerability has been rectified. There are also concerns that the seizure of a data-hosting server by law enforcement agencies may result in the unnecessary interruption or cessation of unrelated services whose data is stored on the same physical machine.

F. Rogue clouds:
Just like entrepreneurs, cybercriminals and organised crime groups are always on the lookout for new markets and with the rise of cloud computing, a new sector for exploitation now exists. Rogue cloud service providers based in jurisdictions with lax cybercrime legislation can provide confidential hosting and data storage services for a usually steep fee. Such services could potentially be abused by organised crime groups to store and distribute criminal data (eg child abusematerials for commercial purposes) to avoid the scrutiny of law enforcement agencies. Hosting confidential business data with cloud service providers involves the transfer of a considerable amount of management control to cloud service providers that usually results in diminished control over security arrangements. There is the risk of rogue providers mining the data for secondary uses such as marketing and reselling the mined data to other businesses. Unfortunately, clients (especially SMEs) are often less aware of the risks and may have an easy way of determining whether a particular cloud service provider is trustworthy. Tim Watson, head of the computer forensics and security group at De Montfort University remarked that ‘one provider may offer a wonderfully secure service and another may not, if the latter charges half the price, the majority of organisations will opt for it as they haveno real way of telling the difference’

G. Regulation and governance:
The privacy and confidentiality risks faced by businesses that use cloud services also depend to a large extent on the terms of service and privacy policy established by the cloud service providers. Failure to comply with data protection legislation may lead to administrative, civil and criminal sanctions. Data confidentiality and privacy risks may be magnified when the cloud provider has reserved the right to change its terms 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 meet 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


