A Comparison of Security Challenges in Public and Private Clouds

Adesh Kumar
Mewar University, Chittorgarh, Rajasthan – 312901, India

Abstract- Cloud computing is a set of IT services that are provided to a customer over a network on a leased basis and with the ability to scale up or down their service requirements. Usually cloud computing services are delivered by a third party provider who owns the infrastructure. Its main advantages include scalability, resilience, flexibility, efficiency and outsourcing non-core activities. Cloud computing offers an innovative business model for organizations to adopt IT services without upfront investment. Despite the potential gains achieved from the cloud computing, the organizations are slow in accepting it due to security issues and challenges associated with it. Security is one of the major issues which hamper the growth of clouds. A cloud may be private, public, community or hybrid. In this paper I briefly compare the security challenges in public clouds and private clouds.

Keywords: private cloud, public cloud, security

I. INTRODUCTION

Cloud computing is a new computing paradigm in which the computer resources (software and hardware) are delivered as a service to the users on metered basis (i.e. pay as you use) generally over the Internet [5]. For years the Internet has been represented on network diagrams by a cloud symbol until 2008 when a variety of new services started to emerge that permitted computing resources to be accessed over the Internet termed cloud computing [2]. Cloud computing encompasses activities such as the use of social networking sites and other forms of interpersonal computing; however, most of the time cloud computing is concerned with accessing online software applications, data storage and processing power. Cloud computing is a way to increase the capacity or add capabilities dynamically without investing in new infrastructure, training new personnel, or licensing new software. It extends Information Technology's (IT) existing capabilities. In the last few years, cloud computing has grown from being a promising business concept to one of the fast growing segments of the IT industry. But as more and more information on individuals and companies are placed in the cloud, concerns are beginning to grow about just how safe an environment is. Some people think cloud computing is the next big thing in the world of IT. Others believe it is just another variation of the utility computing model that has been repackaged in this decade as something new and cool [3]. Despite of all the hype surrounding the cloud, customers are still reluctant to deploy their business in the cloud. Security issues in cloud computing has played a major role in slowing down its acceptance. The cloud model is composed of five essential characteristics, three service models, and four deployment models. The five essential characteristics are as follows:

- On-demand self-service
- Ubiquitous network access
- Resource pooling
- Location independence
- Rapid elasticity
- Measured service

1.1 Cloud Deployment Models

The Cloud deployment models, which can be either internally or externally implemented, can be classified as private cloud, public cloud, community cloud and hybrid cloud as shown in fig.1 and can be described as:

1.1.1 Private Cloud

Private cloud is a new term that some vendors have recently used to describe offerings that emulate cloud computing on private networks. It is set up within an organization's internal enterprise datacenter. In the private cloud, scalable resources and virtual applications provided by the cloud vendor are pooled together and available for cloud users to share and use. It differs from the public cloud in that all the cloud resources and applications are managed by the organization itself, similar to Intranet functionality. Utilization on the private cloud can be much more secure than that of the public cloud because of its specified internal exposure. Only the organization and designated stakeholders may have access to operate on a specific Private cloud.

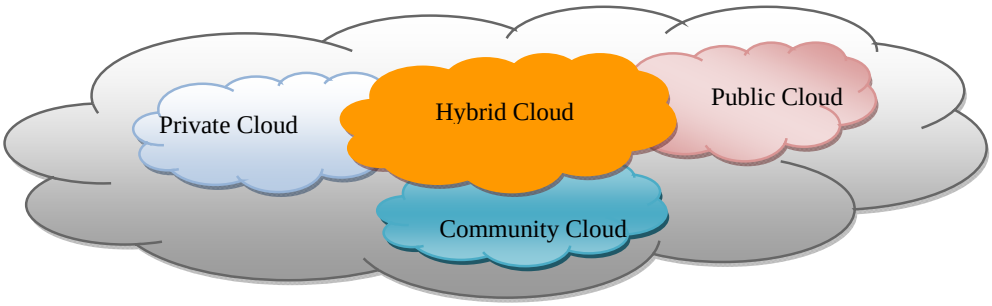

Fig.1 Cloud Deployment Models

1.1.2 Public Cloud

A public cloud is a cloud computing deployment scheme that is generally open for use by the general public [1]. The general public is defined in this case as either individual users or corporations. The public cloud infrastructure used is owned by a cloud services vendor organization; examples of public cloud deployment vendor offerings include Amazon Web Services, Google App Engine, Salesforce.com, and Microsoft Windows Azure.

Typically, the cloud is operated and managed at a data center owned by a service vendor that hosts multiple clients and uses dynamic provisioning. Implementation of a scalable services platform and pay-as-you-go licensing is also an attractive element of public cloud computing, as are the advantages of shared hardware infrastructure, software infrastructure, innovation and development, and maintenance and upgrades.

Economically, using a public cloud (sometimes referred to as an external cloud) can provide almost immediate cost savings to an organization. Shared infrastructure, remote hosting, and dynamic licensing and provisioning are strong enticements for a company. Public cloud implementation can be a big help in removing the crippling infrastructure maintenance burden on IT organizations.

Depending on an organization's specific needs, such as customized configuration requirements and service-level agreements (SLAs) regarding up-time requirements, a company must carefully consider moving critical applications to a public cloud vendor. The most important of these requirements to consider is security. Of the four cloud deployment configurations discussed here, the public cloud configuration offloads the most management chores from the client, or user organization, to the third-party cloud service vendor. In addition to daily operational tasks, this third-party management includes security tasks, such as logging, monitoring, and implementation of controls. This commonly relegates the user organization to a lower degree of control of sensitive or compliant data at both the physical and logical layers of the cloud.

1.1.3 Community Cloud

A cloud deployment model that is being rapidly implemented is called a community cloud. Conceptually residing somewhere between a private cloud and a public cloud, community cloud describes a shared infrastructure that is employed by and supported by multiple companies [1]. This shared cloud resource may be utilized by groups that have overlapping considerations, such as joint compliance requirements, non-competitive business goals, or a need to pool high-level security resources.

Although the physical existence of the shared cloud may reside on any member's premises, or even on a third-party site, managing the community cloud may become complicated, due to unspecified or shifting ownership and responsibility, making it somewhat technically challenging to deal with concerns over resource management, privacy, resilience, latency, and security requirements.

1.1.4 Hybrid Cloud

A hybrid cloud is any combination of the private, public and community cloud deployment models [1]. It is defined by NIST as "a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability An example of hybrid cloud deployment may consist of an organization deploying noncritical software applications in the public cloud, while keeping critical or sensitive apps in a private cloud, on the premises. Hybrid clouds combine both public and private cloud models, and they can be particularly effective when both types of cloud are located in the same facility.

One feature of hybrid clouds that makes them distinctive from the other cloud deployment types is the engagement of the "cloudburst". A "cloudburst" generically refers to the dynamic deployment of an application that, while running predominantly on an organization's internal infrastructure, can also be deployed to the cloud

in the event of a spike in demand. Most common hybrid clouds consist of a combination of both private and public cloud computing environments, which are deployed, utilized, and functioning continuously.

II. WHY SECURITY IS IMPORTANT

Security is a principal concern when entrusting an organization's critical information to geographically dispersed cloud platforms not under the direct control of that organization [1]. In addition to the conventional IT information system security procedures, designing security into cloud software during the software development life cycle can greatly reduce the cloud attack surface.
Cloud computing security is a broad topic with hundreds of considerations—from protecting hardware and platform technologies in the data center to enabling regulatory compliance and defending cloud access through different endpoint devices [6]. One of main focus in security planning should be in strengthening data, identity, and platform protection in the data center and for client devices. The cloud security is -

- The response to a familiar set of security challenges that manifest differently in the cloud. New technologies and fuzzier boundaries surrounding the data center require a different approach.
- A set of policies, technologies, and controls designed to protect data, infrastructure, and clients from attack and enable regulatory compliance.
- Layered technologies that create a durable security net or grid. Security is more effective when layered at each level of the stack and integrated into a common management framework.
- Typically data doesn't stay in one place on your network, and this is especially true of data in the cloud. Encrypt your data wherever it is in the cloud: at rest, in process, or in motion.
- About providing protection whatever delivery model you deploy or use: private, public, or hybrid cloud environments.
- The joint responsibility of an organization and your cloud service provider(s). Depending on the cloud delivery model and services you deploy, security is the responsibility of both parties.

III. SECURITY CHALLENGES IN PUBLIC CLOUD

The security issue has played the most important role in hindering Cloud computing acceptance. In public cloud putting your data, running your software on someone else's hard disk using someone else's CPU appears daunting to many. Well-known security issues such as data loss, phishing, botnet (running remotely on a collection of machines) pose serious threats to organization's data and software. Moreover, the multi-tenancy model and the pooled computing resources in cloud computing has introduced new security challenges that require novel techniques to tackle with.

3.1 Confidentiality– Confidentiality refers to the prevention of intentional or unintentional unauthorized disclosure of information. Confidentiality ensures that only those who are supposed to access data can retrieve it. Loss of confidentiality can occur through the intentional release of private company information or through a misapplication of network rights. Maintain confidentiality in public cloud is a great challenge as resources are shared by many users and due to multi tenancy nature of public cloud.

3.2 Integrity– Integrity ensures that data has not been changed due to an accident or malice. Integrity is the guarantee that the message sent is the message received and that the message is not intentionally or unintentionally altered. The concept of cloud information integrity requires that the following three principles are met:

- Modifications are not made to data by unauthorized personnel or processes.
- Unauthorized modifications are not made to data by authorized personnel or processes.
- The data is internally and externally consistent — in other words, the internal information is consistent both among all sub-entities and with the real-world, external situation.

3.3 Availability- Availability ensures the reliable and timely access to cloud data or cloud computing resources by the appropriate personnel. Availability guarantees that the systems are functioning properly when needed. In addition, this concept guarantees that the security services of the cloud system are in working order. Some of the elements that are used to ensure availability are as follows:

- Fault tolerance for data availability, such as backups and redundant disk systems
- Acceptable logins and operating process performances

- Reliable and interoperable security processes and network security mechanisms

3.4 Data Location - The location of data is not visible and fixed in public clouds. The data may be in motion from one location to another. So vendor must adopt additional security checks to ensure data security and prevent breaches due to security vulnerabilities in the application or through malicious employees. This involves the use of strong encryption techniques for data security and fine-grained authorization to control access to data [7].When information crosses borders, the governing legal, privacy, and regulatory regimes can be ambiguous and raise a variety of concerns. Consequently, constraints on the trans-border flow of sensitive data, as well as the requirements on the protection afforded the data, have become the subject of national and regional privacy and security laws and regulations. Among the concerns to be addressed are whether the laws in the jurisdiction where the data was collected permit the flow, whether those laws continue to apply to the data post transfer, and whether the laws at the destination present additional risks or benefits. Technical, physical and administrative safeguards, such as access controls, often apply.

3.5 Data Control - Due to the fact that third party providers are in charge of the data systems, many organizations feel as if they don't have enough control over their personal data with a public cloud service. A characteristic of public cloud computing services is that detailed information about the location of an organization's data is unavailable or not disclosed to the service subscriber [7]. This situation makes it difficult to ascertain whether sufficient safeguards are in place and whether legal and regulatory compliance requirements are being met.

3.6 Multi-Tenancy Risks - The shared multi-tenant nature of public clouds adds security risks such as unauthorized access of data by other tenants using the same hardware. Also, a multi-tenant environment exposes resource contention issues whenever one of the tenants using the hardware consumes a disproportionate amount of resources either due to need or due to hack attacks.

3.7 Perceived Weaker Security – Perceived weaker security sometimes is viewed as the main disadvantage in public cloud service. This is not to say that the public cloud doesn't have any security - most of them have excellent measures in place - but for customers with sensitive personal information (e.g. financial institutions), the notion of trusting this information to a third party is often intolerable and considered a liability.

3.8 Identity Management – Organizations manage dozens to thousands of employees and users who access their public cloud applications and services, each with varying roles and entitlements [8]. Cloud providers must allow the cloud consumer to assign and manage the roles and associated levels of authorization for each of their users in accordance with their security policies. These roles and authorization rights are applied on a per resource, service or application basis. The cloud provider must have a secure system for provisioning and managing unique identities for their users and services. This Identity Management functionality must support simple resource accesses and robust consumer application and service workflows. A key requirement for moving a consumer application to the cloud is assessing the provider's ability to allow the consumer to assign their user identities into access groups and roles that reflect their operational and business security policies

3.9 Denial of Service (DoS) - A denial of service attack involves saturating the target with bogus requests to prevent it from responding to legitimate requests in a timely manner [7]. An attacker typically uses multiple computers or a botnet to launch an assault. Even an unsuccessful distributed denial of service attack can quickly consume large amounts of resources to defend against and cause charges to soar. The dynamic provisioning of a cloud in some ways simplifies the work of an attacker to cause harm. While the resources of a cloud are significant, with enough attacking computers they can become saturated.

3.10 Data Loss or Leakage – Protecting data can be a headache because of the number of ways it can be compromised. For example, customer data, employee data, or financial data should be protected from unauthorized users. But data can also be maliciously deleted, altered, or unlinked from its larger context [6]. Loss of data can damage your company's brand and reputation, affect customer and employee trust, and have regulatory compliance or competitive consequences.

3.11 Account or Service Hijacking – Attacks using methods such as phishing and fraud continue to be an ongoing threat. With stolen credentials, hackers can access critical areas of your cloud and potentially eavesdrop on transactions, manipulate or falsify data, and redirect your clients to illegitimate sites [6]. IT organizations can fight back with strong identity and access management, including two-factor authentication where possible, strong password requirements, and proactive monitoring for unauthorized activity.

3.12 Abuse And Nefarious Use Of Cloud Services – Many infrastructure-as-a-service (IaaS) providers make it easy to take advantage of their services [6]. With a valid credit card, users can register and start using cloud services right away. Cybercriminals actively target cloud services providers, partially because of this relatively weak registration system that helps obscure identities, and because many providers have limited fraud-detection capabilities. Stringent initial registration and validation processes, credit card fraud monitoring, and subsequent authentication are ways to remediate this type of threat.

3.13 Unknown Risk – Releasing control of your data to a cloud service provider has important security ramifications [6]. Without clearly understanding the service provider's security practices, your company may be open to hidden vulnerabilities and risks. Also, the complexity of cloud environments may make it tempting for IT managers to cobble together security measures. Unfortunately, that same complexity and the relatively new concept of cloud computing and related technologies make it difficult to consider the full ramifications of any change, and you may be leaving your cloud open to new or still undiscovered vulnerabilities.

IV. SECURITY CHALLENGES IN PRIVATE CLOUD

Due primarily to the security concerns associated with the public cloud, many firms have elected to favour private cloud deployments over public clouds. While security pros are on their guard when it comes on private cloud. Private cloud gives more control to in house staff, but increased control cannot ignore the security. On the other hand, there are some security risks associated with all cloud models, private included. Because of security pros are less sensitive to risks and the control is high in the private model.

4.1 Data Location **–** In Private clouds, the sensitive data of each enterprise continues to reside within the enterprise boundary and is subject to its physical, logical and personnel security and access control policies. One of the most common compliance issues facing an organization is data location. Use of an in-house computing center allows an organization to structure its computing environment and to know in detail where data is stored and what safeguards are used to protect the data.

4.2 Greater control - Due to the fact that the hardware is on-site, organizations have more control over their data. The organization is in charge of monitoring and maintaining the data giving them complete oversight of their data.

4.3 More security – Because private cloud services are dedicated to a single organization, the hardware, data storage, and network can be designed to assure high levels of security that cannot be accessed by other clients in the same data center [10]. To be clear, this is not say that public cloud service is not secure. It's just that certain companies will feel the data is more secure by having it reside in-house. Another reason that a private cloud would be desirable has to do with country regulatory issues. In certain countries, the data center hosting a public cloud service must reside within the local country where its users reside as well. When there is no public cloud option that can be provided from the local country, a private cloud is the only option that can be used.

4.4 Identity Management - Identity management and access control are fundamental functions required to secure private cloud computing. The simplest form of identity management is logging on to a computer system with a user ID and password. However, true identity management, such as is required for cloud computing, requires more robust authentication, authorization, and access control. It should determine what resources are authorized to be accessed by a user or process by using technology such as biometrics or smart cards, and determine when a resource has been accessed by unauthorized entities.

4.5 Comingled regulatory environments – Security cannot be fitted in every situation of IT environment [4]. For example, that an entity regulated under PCI (Payment Card Industry) would find a non PCI certified environment is unacceptable for systems which are in cardholder data environment. This is true for both the public and private cloud. An infrastructure is dedicated to be used alone does not mean everything can go with equal ease. Because private cloud grants greater control over regulatory compliance and security, the security should always be given the forefront of planning, particularly when multiple types of regulated data are in play, such as a customer data, comingled mix of payment card data and sensitive business intelligence.

4.6 Data expansion – Cloud is a fantastic enabler of resource centralization. For example, a virtualized environment can allow far-flung resources to come together under an environment [4]. However, if resources are centralized, data becomes denser. While this is a boon for management, it is challenging from security standpoint, particularly when considering tools are being used that operate across the data in aggregate.

Antimalware scanning, bulk encryption and data discovery tools required that when we have a harder time dealing very large amounts of data. Existing tools should be examined to determine what impact they have on data volumes increase and new tools are considered when operation would be impacted severely and old tools are ineffective.

4.7 Future proofing – Private cloud does not means "on-premise," but some may think that way [4]. The defining aspect of private cloud is about which are users that use the infrastructure, not who maintains the infrastructure. So it is not necessarily many private cloud deployments will use on-premise infrastructure. And even if a deployment uses on-premise or dedicated resources today, that cannot prevent it from migrating off-premises to use a service provider or onto shared infrastructure. Organizations that put into a private environment today can easily migrate tomorrow. So, private cloud deployments have many security advantages. A private cloud deployment is every bit as serious as a move to public cloud and needs to be planned for accordingly

4.8 Isolation – In the IaaS, PaaS, and SaaS service delivery models, you may not know which tenant services are co-hosted on the same physical devices at any particular time. In consequence, a problem in one tenant service could affect the performance, network connectivity, or network availability of other tenant services on the same physical hardware. Your design must ensure isolation between tenants in both the physical and virtual environments that make up the private cloud. If your private cloud is partially or wholly hosted by a third party, then you must be assured that the cloud infrastructure used by the third party also guarantees isolation, both between your services and between your services and any other organization's services that the third party also hosts. Private Cloud isolation should separate access to all cloud services including:

- Service Catalog – contains VMs, application templates, service offerings and automation scripts
- Service Catalog Library – the physical location of source files, software library and virtual disks
- Tenant compute – access to compute resources controlled by capacity, type or location controlled using templates
- Tenant Storage – access to storage resources controlled by capacity, data type, or location controlled using templates
- Tenant networking – access to networks controlled by network purpose, and classification
- Backup and recovery – access to backed up resources and data controlled through automation

4.9 All Data Locations are Accessible - In private cloud architectures, many data locations are exposed as services. For example, virtual machines may mount virtual hard disks from a storage resource, or they may use virtual queues, virtual tables, or virtual binary large object (BLOB) storage. A tenant may provision these resources through an automated self-service portal as part of the infrastructure or platform services provisioning process. If an attacker can gain access to a tenant's virtual environment, you must assume that they may also gain access to the tenant's data locations. Because of this, you should consider when and how to encrypt data and how to store and manage the encryption keys that enable access to the data stored in the cloud. The exposure of multiple data location make creating and protecting data classification zones an important design consideration.

4.10 Distrust Client Information - You cannot make any assumptions about the security of any of the client applications that access the tenant services hosted in the private cloud. This proviso is especially important when the tenant wants to enable broad network access to the tenant service from multiple device types and from multiple locations. Poorly designed client applications could accidently reveal credentials or keys, and may perform limited validation on the data that they send to the services hosted in the cloud. Therefore, cloud management services and tenant services must perform their own validation of data sent from all client applications.

4.11 Personnel Security – One important question in private cloud is that how to trust on the employs of organization. What policies and procedures do you have in place when hiring your IT administrators or others with system access? These should include pre-employment checks (identity, nationality or status, employment history and references, criminal convictions, and vetting (for senior personnel in high privilege roles)).

4.12 Maintenance - Since the private cloud is hosted at the company's site, the organization needs to provide adequate power, cooling, and general maintenance. The host organization also runs the risk of data loss due to physical damage of the unit (i.e. fire, power surge, water damage). Also, if a company has multiple data centers with each data center having a private cloud, the onsite maintenance and the associated costs go up significantly.

V. CONCLUSION

The debate between public clouds and private clouds shows no signs of relenting. Conventional wisdom suggests that a private cloud may be more secure due to a higher level of control and visibility. However, the problem is that an apples-to-apples comparison is virtually impossible. Public cloud providers will rarely disclose their specific security practices and architectures, which may be viewed as proprietary and thus a source of competitive advantage. Public cloud providers also typically won't shed any light on how well their security measures are implemented. In contrast, during the course of negotiations, private providers may be more likely to not reveal their practices but also to negotiate in certain protective provisions. Private cloud service makes a lot of sense to bigger companies because it is based on a model where they run their own servers and infrastructure. The idea of controlling your own infrastructure and only allow workers within the same firewall to access all the content from the private cloud makes it comfortable to use for larger companies.

REFERENCES

[1] R. L. Krutz and R. D. Vines, "Cloud Security: A Comprehensive Guide to Secure Cloud Computing", Wiley Publishing, pp.62-85, 2010

[2] S. O. Kuyoro, F. Ibikunle, and O. Awodele,"Cloud Computing Security Issues and Challenges" International Journal of Computer Networks (IJCN), Volume (3), Issue (5), pp.247-254, 2011

[3] J. W. Rittinghouse, and J. F. Ransome," Cloud Computing: Implementation, management and Security", CRC Press, pp.26-37, 2010

[4] S. Singh and T. Jangwal, "Cost breakdown of Public Cloud Computing and Private Cloud Computing and Security Issues" International Journal of Computer Science & Information Technology (IJCSIT) Vol 4, No 2, pp.17-31, April 2012

[5] F. Douglis, "Staring at Clouds", IEEE Internet Computing, pp.4-6, June 2009

[6] Intel IT Center, "Planning Guide: Cloud Security", pp.3-5, May 2012

[7] W. Jansen,And T. Grance, DRAFT: Guidelines on Security and Privacy in Public Cloud Computing, NIST, U.S. Department of Commerce, Special Edition 800-144, pp.9-15,January 2011

[8] R. Kean, et al., the Security for Cloud Computing: 10 Steps to Ensure Success, White Paper, Cloud Standards Customer Council, pp.6-7, August 2012

[9] B. R. Kandukuri, et al., "Cloud Security Issues": IEEE International Conference on Services computing, pp.517-520, 2009

[10] Aerohive Networks,Public or Private Cloud: The Choice is Yours, White Paper, pp 3-5,2013

[11] J. Chen, Y. Wang and X. Wang, "On Demand Security Architecture for Cloud Computing", Research Feature, Computer, IEEE Computer Society, pp. 73-78, July 2012

[12] W. Juang and Y. Shue. "A Secure and Privacy Protection Digital Goods Trading Scheme in Cloud Computing", p.288, 2010

[13] Cloud Computing Security. A Trend Micro White Paper, pp.2-10, May 2010

[14] G. Lin, D. Fu, J. Zhu, and G. Dasmalchi, "Cloud computing: It as aservice," IT Professional, vol. 11, no. 2, pp.10-13, 2009.

[15] DRAFT: Cloud Computing Synopsis and Recommendations. NIST, U.S. Department of Commerce, Special Edition 800-146, pp.9-10