CLOUD COMPUTING: SECURITY ISSUES AND CHALLENGES

Sachin Kumar Singh[1], Devendra Kumar Singh[2]
[1]Department of Computer Science & Engineering, REC Sonbhadra, Churk(U.P),India.
[2]Lecturer, REC Sonbhadra, Churk (U.P), India.

ABSTRACT

Cloud storage is defined as "the storage of data online in the cloud," wherein a company's data is stored in and accessible from multiple distributed and connected resources that comprise a cloud. Although cloud service providers implement the best security standards and industry certifications, storing data and important files on external service providers always opens up risks. Using cloud-powered technologies means you need to provide your service provider with access to important business data. Meanwhile, being a public service opens up cloud service providers to security challenges on a routine basis. The ease in procuring and accessing cloud services can also give nefarious users the ability to scan, identify and exploit loopholes and vulnerabilities within a system. For instance, in a multi-tenant cloud architecture where multiple users are hosted on the same server, a hacker might try to break into the data of other users hosted and stored on the same server. The following paper deals with the service models of cloud computing along with types of cloud computing & characteristics of cloud. Further challenges and security issues in cloud computing is also discussed and at last conclusion and future demand for research in the field of cloud computing.

KEYWORDS: *Cloud computing, Cloud platforms, Data Security, Security Challenges.*

I. INTRODUCTION

Cloud computing is a general term for the delivery of hosted services over the internet. Often referred to as simply “the cloud”, is the delivery of on-demand computing resources- everything from application to data centres- over the internet on a pay-for-use basic. Cloud service providers (CSP’s) offer cloud platforms for their customers to use and create their web services.

Cloud computing appear as a necessity for business nowadays. Initially this was only in academics area but now it got industrial exposure due to the companies like Microsoft, Amazon, Google etc. There are various reasons because of which organizations are moving to IT solutions that include cloud computing as they have to pay for the resources on consumption basis. This makes it possible for the new start-ups to enter the market easily, since the cost is diminished. This allows the start up to concentrate to business value rather on the starting budget.

One of the most appealing factors of cloud computing is its pay-as-you-go model of computing as a resource. This revolutionary model of computing has allowed businesses and organizations in need of computing power to purchase as many resources as they need without having to put forth a large capital investment in the IT infrastructure. Other advantages of cloud computing are massive scalability and increased flexibility for a relatively constant price. For example, a cloud user can provision 1000 hours of computational power on a single cloud instance for the same price as 1 hour of computational power on 1000 cloud instances [1].

Clouds are the new trend in the evolution of the distributed systems, the predecessor of cloud being the grid. The user does not require knowledge or expertise to control the infrastructure of clouds; it provides only abstraction. It can be utilized as a service of an Internet with high scalability, higher throughput, quality of service and high computing power. Cloud computing providers deliver common online business applications which are accessed from servers through web browser [2].

II. SERVICE MODEL OF CLOUD COMPUTING

There are various broad ways a cloud-based service is consumed and utilized. In the world of cloud computing, there are three different approaches to cloud-based services:

- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Software as a Service (SaaS)

Microsoft offers impressive Cloud services based on its widely used on-premises software products.

Office 365 is SaaS, which provides an online version of MS Office Suite (Office Web Apps) along with SharePoint Server, Exchange Server and Lync Server.

Windows Azure is both IaaS and PaaS, which makes the Windows Server operating system and other features available as services.

2.1. Infrastructure as a Service (IaaS)

With the IaaS model, you can outsource the elements of infrastructure like Virtualization, Storage, Networking, Load Balancers and so on, to a Cloud Provider like Microsoft.

To deploy your applications to the Cloud, you have to install OS images and related application software on the cloud infrastructure. In this model, it's your responsibility to patch/update/maintain the OS and any application software you install. The Cloud provider will typically bill you on computing power by the hour and the amount of resources allocated and consumed (as per its service level agreement (SLA).

For example, using Microsoft Windows Azure, you can set up new Windows Server and Linux virtual machines and adjust your usage as your requirements change. You only have to pay for the service that you use.

One of the biggest benefits of IaaS is that it provides granular control, where you can choose the core components for your infrastructure. By pooling your computing and storage resources you can scale with ease and speed to meet the infrastructure needs of your entire organization or individual departments, globally or locally.

2.2. Platform as a Service (PaaS)

With the PaaS model, you get a core hosting operating system and optional building block services that allow you to run your own applications or third-party applications. You need not be concerned about lower level elements of Infrastructure, Network Topology, Security and Load Balancers -- all this is done for you by the Cloud Service Provider. The Provider gives you a fully functional OS with major platform software.

Microsoft Windows Azure as PaaS can be used as a development, service hosting and service management environment. SQL Azure can provide data services, including a relational database, reporting and data synchronization. Both Windows Azure and SQL Azure are the key components of the Azure Cloud Platform. With this platform, you can focus on deploying your custom applications and can easily configure your applications to scale up or down as demands change.

Microsoft Azure platform as a PaaS can support different roles, such as Worker and Web. For example, you can run web applications with the Web Role, as well as host middle tier applications, such as Workflow, in the Worker Role. Similarly, SQL Azure provides Microsoft’s core relational database engine as a platform service.

One of the key benefits of PaaS is that you need not be concerned about the running OS or updates (service packs) and hardware upgrades. The Provider regularly patches your OS, updates platform features (such as the core .NET platform or SQL database engine) and updates hardware on demand to meet your demand.

2.3. Software as a Service (SaaS)

With the SaaS model, you consume as a service only the Applications that you need for your business. These applications run on the provider’s cloud infrastructure, making them accessible from various devices like browser or mobile.The SaaS provider manages everything -- that includes Infrastructure, Load balancers and firewalls, Operating Systems and runtime environments like .NET and Java, the line of business applications and services such as email or a CRM.

You need not be concerned about managing the underlying cloud infrastructure, which includes network, servers, operating systems or storage (except some user-specific application configuration settings).With SaaS, you get fully provisioned services with a well-defined feature set, which are customizable to a certain degree. SaaS providers usually offer browser-based interfaces so users can easily access and customize these services. APIs are also usually made available for developers.

Each organization or user served by the SaaS provider is called a Tenant, and this type of arrangement is called a Multitenant architecture. The Provider's servers are virtually partitioned so that each organization or user works with a customized virtual application instance.The key benefit of SaaS is that it requires no upfront investment in servers or software licensing. For the application developer, there is only one application to maintain for multiple clients.

Microsoft Office 365 is a SaaS that provides these types of services, which include SharePoint Online, Exchange Online, Lync Online and Office Professional Plus. Most of these online services have a subset of the features available on their on-premises counterparts. Microsoft Online Services are subscription-based, on-demand applications and hosted services, providing your organization with a consistent experience across multiple devices.

III. TYPES OF CLOUD COMPUTING

Cloud computing comes in three forms: public clouds, private clouds, and hybrids clouds. Depending on the type of data you're working with, you'll want to compare public, private, and hybrid clouds in terms of the different levels of security and management required.

3.1. Public Clouds

A public cloud is basically the internet. Service providers use the internet to make resources, such as applications (also known as Software-as-a-service) and storage, available to the general public, or on a 'public cloud. Examples of public clouds include Amazon Elastic Compute Cloud (EC2), IBM's Blue Cloud, Sun Cloud, Google AppEngine and Windows Azure Services Platform.

For users, these types of clouds will provide the best economies of scale, are inexpensive to set-up because hardware, application and bandwidth costs are covered by the provider. It's a pay-per-usage model and the only costs incurred are based on the capacity that is used.

There are some limitations, however; the public cloud may not be the right fit for every organization. The model can limit configuration, security, and SLA specificity, making it less-than-ideal for services using sensitive data that is subject to compliancy regulations.

3.2. Private Clouds

Private clouds are data centre architectures owned by a single company that provides flexibility, scalability, provisioning, automation and monitoring. The goal of a private cloud is not sell "as-a-service" offerings to external customers but instead to gain the benefits of cloud architecture without giving up the control of maintaining your own data centre. Private clouds can be expensive with typically modest economies of scale. This is usually not an option for the average Small-to-Medium sized business and is most typically put to use by large enterprises. Private clouds are driven by concerns around security and compliance, and keeping assets within the firewall. One of the best examples of a private cloud is Eucalyptus Systems [7].

3.3. Hybrid Clouds

By using a Hybrid approach, companies can maintain control of an internally managed private cloud while relying on the public cloud as needed. For instance during peak periods individual applications, or portions of applications can be migrated to the Public Cloud. This will also be beneficial during predictable outages: hurricane warnings, scheduled maintenance windows, rolling brown/blackouts.

The ability to maintain an off-premise disaster recovery site for most organizations is impossible due to cost. While there are lower cost solutions and alternatives the lower down the spectrum an organization gets, the capability to recover data quickly reduces. Cloud based Disaster Recovery (DR)/Business Continuity (BC) services allow organizations to contract failover out to a Managed Services Provider that maintains multi-tenant infrastructure for DR/BC, and specializes in getting business back online quickly.

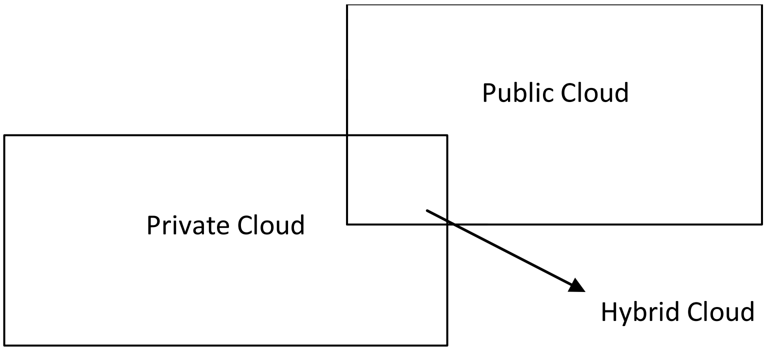

Figure1. Hybrid Cloud

IV. CHARACTERISTIC OF CLOUD COMPUTING

1.) On-demand self-service: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

2.) Broad network access: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops and workstations).

3.) Resource pooling: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state or datacentre). Examples of resources include storage, processing, memory and network bandwidth.

4.) Rapid elasticity: Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

5.) Measured service: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth and active user accounts). Resource usage can be monitored, controlled and reported, providing transparency for the provider and consumer.

V. CHALLENGES AND SECURITY ISSUES IN CLOUD COMPUTING

1.) **Data Security -** As soon as data is created, it can be tampered with. It could be improperly classified or have access rights changed by intruders, resulting in loss of control over the data.[3]Because CSPs are third-parties, the complete security of CSP systems is unknown, so data must be protected from unauthorized access, tampering by network intruders, and leakage [3]. Due to the multi-tenant nature of cloud computing, controls must be put in place to compensate for the additional security risks inherent to the commingling of data. During the use phase, which includes transmission between CSP and consumer and data processing, the confidentiality of sensitive data must be protected from mixing with network traffic with other cloud consumers. If the data is shared between multiple users or organizations, the CSP must ensure data integrity and consistency. The CSP must also protect all of its cloud service consumers from malicious activities from its other consumers [3].Data persistence is the biggest challenges present in the destroy phase. For data to be completely destroyed, it must be erased, rendered unrecoverable, and as appropriate, physically discarded [4].

2.) **Access control -** Access management is one of the toughest issues facing cloud computing security. An organization can utilize cloud services across multiple CSPs, and can use these services as an extension of its internal, potentially non-cloud services. It is possible for different cloud services to use different identity and credential providers, which are likely different from the providers used by the organization for its internal applications. The credential management system used by the organization must be consolidated or integrated with those used by the cloud services [4].Requirements for user profile and access control policy vary depending on whether the cloud user is a member of an organization, such as an enterprise, or as an individual. Access control requirements include establishing trusted user profile and policy information, using it to control access within the cloud service, and doing this in an auditable way [4].A federation is a group of two or more organizations that have agreed upon standards for operation [5]. Federations allow multiple, disparate entities to be treated in the same way. In cloud computing, federated sign-on plays a vital role in enabling organizations to authenticate their users of cloud services using their chosen identity provider .The federated identity system would have a trusted authority common to multiple CSPs, and provide single or reduced sign-on through the common authority [6].

3.) **Data Storages location Data Locations -** When users use, they probably won't know exactly where their data will hosted and which location it will stored in. In fact, they might not even know what country it will be stored in. Service providers need to be asked whether they will accomplish to storing and alter data in particular arbitration, and on the basis of their customers will they make a fair accomplishment to follow local privacy requirement [8].

4.) **Compliance with laws and regulations -** Regulations written for IT security require that an organization using IT solutions provide certain audit functionality. However, with cloud computing, organizations use services provided by a third-party. Existing regulations do not take into account the audit responsibility of a third-party service provider [4].In order to comply with audit regulations, an organization defines security policies and implements them using an appropriate infrastructure. The policies defined by an organization may impose more stringent requirements than those imposed by regulations. It falls on the customer of the cloud services to bridge any gap between the audit functionality provided by the CSP and the audit mechanisms required for compliance [4]

VI. FUTURE WORK

The cloud has been widely hailed as the most disruptive force in modern business. Indeed, the world is in the midst of fundamentally profound transformations, enabled by the cloud, in the ways in which we access and interact with data and applications.

Unfortunately, the security industry has not kept pace with these transformational trends, necessitating an equally profound change in the way we secure modern businesses against cyber-attack. The coming wave of disruption will change the entire way in which we think about enterprise security.

In the near Future, Enterprises will favour integrated cloud services vs. on premise point products. Endpoint and network security technologies will become inextricably intertwined. We will move from a world of alert-driven to intelligence-driven security. Cloud security will enable a secure foundation for the internet of things (IoT).

VII. CONCLUSIONS

Cloud computing is built for the world of tomorrow, where we each use many different kinds of computing devices: desktop, laptop, cellphone, or tablet. The intention is to make the functionality and data we need always accessible no matter where we are in the world, and no matter what we're using to access the Internet.

In addition, cloud computing is cheaper for businesses. If an online storage service is used, there's no need to buy server hardware, for example, or to pay for staff to maintain hardware. Of course, there are some downsides. Putting data into the cloud involves a lot of trust that the cloud provider will not let it leak out. Cloud providers are a little coy when discussing issues such as this. Additionally, cloud services tend still at a primitive stage compared to equivalents on a desktop computer Google Docs is only a fraction as powerful as Microsoft Office, for example.

REFERENCES

[1] Armbrust, M. et. al., (2009), “Above the clouds: A Berkeley view of Cloud Computing”, UC Berkeley EECS, Feb 2010.

[2] Lizhe Wang, Jie Tao, Kunze M., Castellanos A.C., Kramer D., Karl W., “Scientific Cloud Computing: Early Definition and Experience,” 10th IEEE Int. Conference on High Performance Computing and Communications, pp. 825-830, Dalian, China, Sep. 2008, ISBN: 978-0-7695-3352-0.

[3] Xiaojun Yu; Qiaoyan Wen, "A View about Cloud Data Security from Data Life Cycle," Computational Intelligence and Software Engineering (CiSE), 2010 International Conference on , vol., no., pp.1-4, 10-12 Dec. 2010.

[4] Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, 2009.

[5] “Federated identity management.” Internet http://en.wikipedia.org/wiki/Federated_identity_ http://en.wikipedia.org/wiki/Federated_identity_management, [Dec. 16, 2011].

[6] Cloud Computing Use Case Discussion Group, Cloud Computing Use Cases Whitepaper v4.0, July 2010.

[7] B. R. Kandukuri, R. Paturi V, A. Rakshit, “Cloud Security Issues”, In Proceedings of IEEE International Conference on Services Computing, pp. 517-520, 2009.

[8]. Feng-Tse Lin, Teng-San Shih, “Cloud Computing: The Emerging Computing Technology,” ICIC Express Letters Part B: Applications (ISSN: 2185-2766), v1, September 2010, pp. 33-38.

[9] Shigang Chen, Meongchul Song, Sartaj Sahni, Two Techniques for Fast Computation of Constrained Shortest Paths, IEEE/ACM Transactions on Networking, vol. 16, no. 1, pp. 105-115, February 2008.

[10] King-Shan Lui, Klara Nahrstedt, Shigang Chen, Hierarchical QoS Routing in Delay-Bandwidth Sensitive Networks, in Proc. of IEEE Conference on Local Area Networks (LCN’2000), pp. 579-588, Tampa, FL, November 2000.

[11] Shigang Chen, Yi Deng, Attie Paul, Wei Sun, Optimal Deadlock Detection in Distributed Systems Based on Locally Constructed Wait-for Graphs, in Proc. of 16th IEEE International Conference on Distributed Computing Systems (ICDCS’96), Hong Kong, May 1996.

[12] L.J. Zhang and Qun Zhou, “CCOA: Cloud Computing Open Architecture,” ICWS 2009: IEEE International Conference on Web Services, pp. 607-616. July 2009.

[13] Tim Mather, Subra Kumaraswamy, Shahed Latif, Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance, O’ Reilly Media, USA, 2009.

[14] Ronald L. Krutz, Russell Dean Vines “Cloud Security A Comprehensive Guide to Secure Cloud Computing”, Wiley Publishing, Inc.,2010

[15] K. Vieira, A. Schulter, C. B. Westphall, and C. M. Westphall, “Intrusion detection techniques for Grid and Cloud Computing Environment,” IT Professional, IEEE Computer Society, vol. 12, issue 4, pp. 38-43, 2010.

AUTHORS

Sachin Kumar Singh is pursuing Bachelors in Computer Science and Engineering at Rajkiya Engineering College, Sonbhadra (UP), India. His research interests include Cloud Computing, Complexity theory and algorithm design.

Devendra Kumar Singh is currently working as Lecturer at Rajkiya Engg. College Sonbhadra (UP), India. He teaches mechanics, material science and computer integrated manufacturing. He is M.Tech from Mechanical Engg. Department at Madan Mohan Malaviya University of Technology Gorakhpur, India in CIM Specialization.