ISSN 2320-9984
Volume 6 Issue 4 | December 2018 ISSN: 2320-9984 (Online)
International Journal of Modern Engineering & Management Research
Website: www.ijmemr.org

A Survey of Data Protection in Cloud Computing

Raksha Nayak
M.Tech. Research Scholar
Shri Ram Group of Institutions, Jabalpur
Jabalpur, (M.P.) [INDIA]
Email: rakshanayak7may@gmail.com

Sapna Choudhary
Assistant Professor, Head of the Department
Department of Computer Science & Engineering
Shri Ram Group of Institutions, Jabalpur
Jabalpur, (M.P.) [INDIA]
Email: choudharysapnajain@gmail.com

Abstract**—***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 it is. Despite of all the hype surrounding the cloud, enterprise customers are still reluctant to deploy their business in the cloud. Security is one of the major issues which reduces the growth of cloud computing and complications with data privacy and data protection continue to plague the market. The advent of an advanced model should not negotiate with the required functionalities and capabilities present in the current model.*

The idea that computation may be organized as a public utility, like water and electricity, was formulated in the 1960s by John McCarthy, a visionary computer scientist that championed mathematical logic in artificial intelligence. Cloud computing combines the best techniques and technologies of distributed system, parallel computing and grid computing. Is a utility computing that provides a scalable standard environment for network-centric application development, testing and deployment that distributes and allocates resources via simple user, provider model pattern of pay-per-use system. This paper aims at bringing to light some of the threats and vulnerabilities to cloud computing existence, with significance of enlighten users and providers on what is at stake on moving their business or organisation whole or partially to the cloud.

Keywords:— *Cloud Computing, SaaS, IaaS, PaaS, Private Cloud, Public Cloud, Threats*

1. INTRODUCTION

Cloud Computing is an old idea whose time has come, because the technological elements were in place. It was only a matter of time before the economical advantage became apparent. It is as important "to this decade as PCs were to the 1970's. It is a technological and social leap that will change how businesses function, how cities are planned, how people carry out their work and what citizens expect from online services [9].

Cloud-Based Services technology can be considered as the key technologies to create cloud service(s). It can be defined as a set of functionalities that can be invoked by a user or a cloud application request to perform some required task(s) through the web [1].

Computing is being transformed to a model consisting of services that are commoditized and delivered in a manner

similar to traditional utilities such as water, electricity, gas and telephony. In such a model, users will access services based on their requirements without regard to where the services are hosted or how they are delivered [10].

Service-Oriented computing, Business process management and Virtualization. It has revolutionized the way computational resources are commercialized and delivered to customers. It allows customers to dynamically scale their applications, software platforms and hardware infrastructure as it is a service (cloud-based services) with the important characteristics of providing a non-functional guarantees in the form of Service Level Agreements (SLAs) [6] [12]

Due to the increase in the power demanded by data centers that was predicted to double from 2006 to 2011, and other envisioned information technology issues, the term Cloud Computing was coined in the late 2007 and currently emerges as a hot topic. Prior to this time, John McCarthy a visionary in Computer Science in the early 1960s has formulated the idea that computation may be organised as a public utility, like water and electricity. Also, in 1992, Gordon Bell delivered an invited address at a conference on Parallel Computations with the provocative title "Massively Parallel Computers:

Why not Parallel Computers for the Masses"; he argued that one of a-kind systems are not only expensive to build, but the cost of rewriting applications for them is prohibitive [2], [7].

Cloud-Based Services or Cloud Computing is seen by some analyst and vendors as an updated version of utility computing. That is virtual servers available over the Internet. It comes only when you think about what IT always needs: a way to increase capacity or add capabilities on the fly without investing in new infrastructure, training new personnel, or licensing new software. It encompasses any subscription-based or pay-per-use service that is in real time over the Internet, extends IT's existing capabilities.

As with every new paradigm, there is always some threats to their being accepted by individuals and the public at large. Cloud-Based services/Cloud Computing is not an exception as there are emerging threats to its existence, such as availability, security, performance, data confidentiality & audit-ability, reliability & Quality of Service (QoS), Data/Vendor lock-in, standardization, etc. Among these, security is the most talked about.

In terms, of Security, a typical cloud environment expects the cloud user to be responsible for his/her application-level security, while the cloud provider is responsible for physical and virtual machine security. Malicious cloud provider may gain access to private user information which poses threats to security. At present the concern is to find ways of protecting the cloud user from such malicious cloud user or cloud provider [4].

In summary the purpose of this paper is to bring to light the threats and vulnerabilities of cloud computing and why security consideration is vital. Also, it enlightens users and providers on the stake of moving businesses and organisations partially or wholly to the cloud environment.

1.1 Cloud-Based Services/Cloud Computing

Cloud computing is the convergence of three major terms Virtualization, Utility Computing and Software as a Service.

Virtualization: were applications are separated from infrastructure.

Utility Computing*:* were server capacity are accessed across the grid at a very shared-price/point service.

Software as a Service: were applications are available on-demand on a subscription basis.

The first step to any Cloud computing is to adapt applications to run as virtualized images, it is not scrapping the Internet but is a means of using the Internet for our computer needs. Instead, it is a new paradigm based on a pay-per-use model to flexibly access hardware and software resources through Internet, allowing companies to reduce costs and increase performance. Below is the evolution of Cloud Computing;

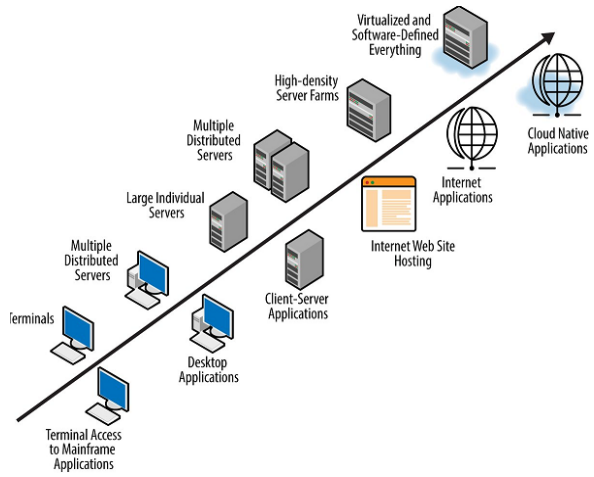

Figure 1: The Evolution of Cloud Computing (adapted from IBM 2009)

As seen in the table above, it all started with Grid Computing which solves large problems with parallel computing in the late 1980s, then Utility and software as a Service which are two complementary trends; as Utility computing can only be successful on the market if a critical mass of applications is able to run on it and SaaS needs a flexible, scalable and easily accessible infrastructure on which it can run. So to meet market demand, the next in evolution by nature is the integration of the two trends into a new holistic approach which offers the following functionality;

Scalable, flexible, robust and reliably physical infrastructure. A Platform services that enables programming access to physical infrastructure through abstract interfaces.

SaaS developed, deployed and running on a flexible and scalable physical infrastructure.

This functionality gives rise to the emerging clouds and cloud computing/cloud-based services. So cloud computing is resulting from the convergence of Grid computing, Utility computing and SaaS, and thus essentially represents the increasing trend towards the external deployment of IT resources, such as computational power, storage or business application and obtaining them as services [5].

The estimated cost advantage of cloud computing is said to be three to five times for business applications and more than five times for consumer applications.

1.2 Definitions:

There are various definitions of Cloud Based Service/Cloud Computing, but the most accepted is the one by NIST (National Institute of Standards & Technology) which states that "Cloud Computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications & services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." [3]

Other definitions which see cloud computing from the end-users perspective include;

Garner (2008b): "A style of computing in which massively IT-related capabilities are provided 'as a service' using Internet technologies to multiple external customers"

IDC (Gens 2008): "An emerging IT development, deployment and delivery model, enabling real-time delivery of products, services and solutions over the Internet (i.e., enabling cloud services)"

The 451 Group: "A service model that combines a general organising principle for IT delivery, infrastructure components, an architectural approach and an economic model-basically, a confluence of grid computing, virtualization, utility computing, hosting and software as a service

(SaaS)" (Fellow 2008)

Merrill Lynch 2008: "the idea of delivering personnal (e.g. email, word processing, presentations) business productivity applications (e.g. sale force automation, customer service, accounting) from centralized servers."

2.0 CLASSIFICATION / CHARACTERISTICS / FEATURES / ELEMENTS & COMPONENTS OF CLOUD COMPUTING

Cloud computing/Cloud-Based services is based on a paradigm shift with profound implications on computing ethnics. The main elements of this shifts are;

- A The control is relinquished to third party services.
- The data is stored on multiple sites administered by several organisations.
- Multiple services interoperate across the network.
- From the definitions in section 1.2, the following Features of Cloud computing was deduced. The figure below illustrates;
- A Cloud computing is a new computing paradigm.

A Infrastructure resources (hardware, storage and system software) and applications are provided in a X-as-a-Service manner. When these services are offered by an independent provider or to external customers, cloud computing is based on pay-per-use business models.

A Main features of clouds are virtualization and dynamic scalability on demand.

A Utility computing and SaaS are provided in an integrated manner, even though utility computing might be consumed separately.

A Cloud services are consumed either via web browser or via a defined API (Application Programming Interface).

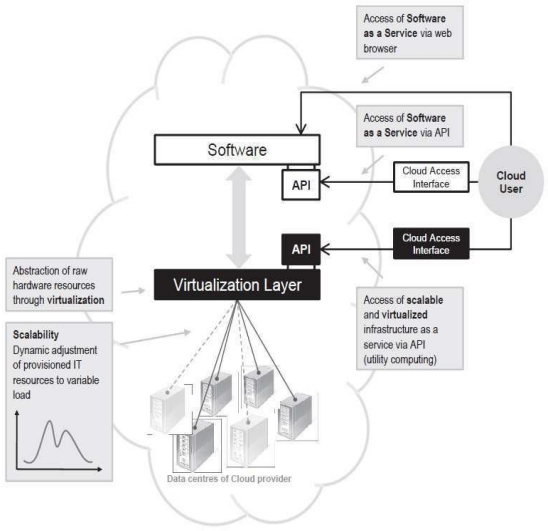

Figure 2: Defining Features of Cloud Computing/ Cloud-Based Services

There are seven (7) major components of Cloud Computing/Cloud-Based Services. They are; Application, Client, Infrastructure, Platform, Service, Storage and Processing Power. [5]

2.1 Classification/Types of Cloud-Based Services (Cloud Deployment Models)

Cloud Computing is classified into three or four forms. They include;

A Public Cloud: this is a style of computing where scalable and elastic IT-enabled capabilities are delivered as a service to external customers using Internet technologies. Is a data centre of hardware and software run by third parties such as Google & Amazon, which expose their services to companies and consumers via the Internet. It is not restricted to a limited user base and it is made available in a pay- as-you-go manner to the general public.

A Private Clouds: is a style of computing where scalable and elastic IT-enabled capabilities are delivered as a service to internal customers using Internet technologies. It is also seen as an internal data centre of a company or other organisation and

is fully owned by a single company who has total control over the applications run on the infrastructure, the place where they run and people or organizations using it.

A Hybrid Cloud: this is the combination of Public & Private clouds and allows an organization to both run some applications on an internal cloud infrastructure and others in a public cloud. This helps companies to benefit from scalable IT resources offered by external cloud provider while keeping specific applications or data inside the firewall.

A Federated Clouds/Federation of clouds: it is the collaboration or sharing of services/infrastructure among mainly public clouds even though private clouds may be involved. It is a collection of single clouds that can interoperate that is exchange data and computing resources through defined interfaces.

Some authors refer to Federated clouds as Community clouds. It is said to imply that the infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g. Mission, security requirements, policy and compliance consideration). It may be managed by the organizations or a third party and may exist on premises or off premises. [2], [5]

2. GENERIC STRUCTURE/ ARCHITECTURAL LAYERS OF CLOUD COMPUTING

The generic structure/architectural layers of cloud computing/cloud-based services are;

A Infrastructure as a Service (IaaS): this is the use of fundamental computing resources, e.g. storage, networks, servers, to provide services to end-users. The end-users can deploy and run arbitrary software including both applications and operating systems.

Example is Amazon EC2. Here the consumer does not control the underlying infrastructure, but can typically launch virtual machines with chosen operating systems which in turn are managed by the consumer.

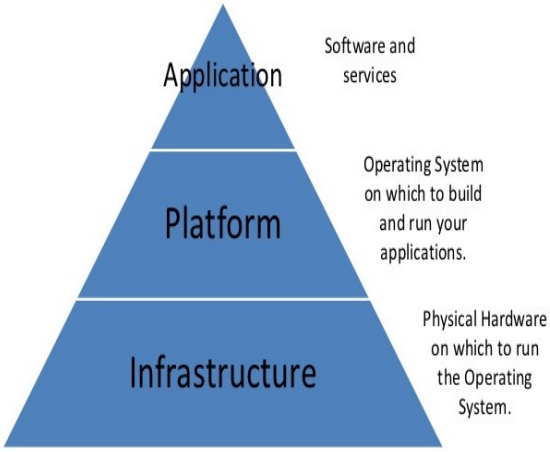

Figure 3: The 3 Layers of Cloud Computing (SaaS, PaaS & IaaS)

A Platform as a Service (PaaS): this is the use of tools and resources running on a cloud infrastructure to provide services to end-users. The applications are developed and/or acquired by end-users on top of the tools provided. Microsoft Windows Azure and Google App Engine are examples of cloud PaaS. The consumer does not control the underlying infrastructure or operating systems, but does control deployment of individual applications.

A Software as a Service (SaaS): this is the use of applications running on a cloud infrastructure to provide services to end-users. SaaS can deliver business applications such as customer relationship management (CRM), enterprise resource planning (ERP), and accounting. Examples of cloud SaaS are Google Apps and Salesforce CRM. The consumer does not control underlying infrastructure [13]

3.1 Benefits/Opportunities of Cloud-Based Services

Companies, organizations and individuals switch to cloud-based services for various reasons such as data storage, pervasive computing, etc or implement their own solution. For this reason a compromising attack often leads to devastating impact on the structure as a whole and time of recovery is

not quite known.

In terms of benefits and successes of cloud computing, it can be grouped as par technological advancement, a realistic system model, user convenience and financial advantages. They include but not limited to;

A Cloud computing is in a better position to exploit recent advances in software, networking, storage and processor technologies. It is promoted by large IT companies where these new technological developments take place and these companies have a vested interest to promote the new technologies.

A cloud consists of a homogeneous set of hardware and software resources in a single administrative domain. In this setup; security, resource management, fault- tolerance, and quality of service (QoS) are less challenging than in a heterogeneous environment with resources in multiple administrative domains.

A It is focused on enterprise computing; its adoption by industrial organisations, financial institutions, healthcare organizations and so on has a potentially huge impact on the economy.

A It provides the illusion of infinite computing resources; its elasticity frees the applications designers from the confinement of a single system.

A It eliminates the need for up-front financial commitment and it is based on a pay -as- you-go approach; this has the potential to attract new applications and new users for existing applications formatting a new era of industry-wide technological advancements. [2].

A From users perspective, the utility-based payment model is considered one of the main benefit of cloud computing, as you pay for the IT resources used. No need for up-front infrastructure investment such as software licenses and no risk of unused but paid software license, as well as investment in hardware infrastructure and related maintenance and staff. So, capital expenditure is turned into operational expenditure.

A Users of a cloud service only use the volume of IT resources they actually need, and only pay for the volume of IT resources they actually use. The scalability and flexibility of the cloud is utilized by the user as cloud computing enables easy and fast scaling of required computing resources on demand. [5]

4. THREATS/VULNERABILITIES/ OBSTACLES TO CLOUD-BASED SERVICES

Threat means something that is a source of danger. While vulnerabilities implies being susceptible to attack and obstacles means an obstruction that stands in the way and must be removed or surmounted or circumvented.

Table 1: Summarized Threats with Opportunities for Growth of Cloud Computing [8]

S. No.	Obstacles	Opportunity
1.	Availability of Service	Use multiple cloud providers Use elasticity to prevent DDOS.
2.	Data/ Vendor Lock-In	Standardize APIs; compatible software (SW) to enable surge computing.
3.	Data Confidentiality & Auditability	Deploy Encryption, VLANs, Firewalls; Geographical Data storage.

Cloud-based service/cloud computing threats include the following;

- A Ensuring Security and compliance
- A Improving manageability
- A Deeper integration with on-premise applications
- Providing mobile access
- Performance monitoring/ management
- Improving data quality

- Improving application governance
- Reporting and analytics
- Driving user adoption/productivity

In conclusion, these threats can be summarized into three broad categories;

A Attacks against virtualization: Weakness in this technology of virtualization which cloud computing uses a lot, may allow attacks against the hypervisor or against co-hosted virtual machines ranging from leakages of coarse-grained load information to full compromise.

A API-level attacks against cloud services: Along with general-purpose computing cloud like Amazon AWS, we are also seeing the growth of specialized cloud that provide services such as file hosting, device synchronization and music streaming. Each of these services typically exposes its own complex API, that may suffer from vulnerabilities that lead it to compromise user's privacy or worse.

A Old attacks with new implications: When a cloud-computing provider suffers any kind of compromise to its infrastructure, this has additional implications compared to when the same compromise occurs within an ordinary company's network infrastructure. This has been recently demonstrated by the compromise of Sony's PSN network. In this case, the compromise caused a month-long down-time of the PSN service that is used by millions of users, & led to the theft of user's personal information (including credit card details) on a massive scale. If a general purpose cloud computing platform were compromised, the consequences could be even more severe, and the ramifications uncertain. For individual customers it might be difficult to even find out if their virtual machines had been compromised making it very difficult to select remediation actions. (www.syssec- project.eu, 2011)

4.1 Some Cloud-Based Service Roviders/ Users

A Amazon Elastic Compute Cloud (EC2)/Simple Storage Service (S3) is an IaaS cloud and is the most well known cloud. Through the use of virtual machines EC2 clients create as many (virtual) machines they require and then host all their required services within the machines. They charge client per CPU hour. It is even possible to create a cluster within EC2 by requesting EC2 to create multiple instances of a base virtual machine and then installing the required cluster software into each machine.

A Google App Engine is a PaaS cloud that provides a complete Web service hosting environment to clients. Unlike EC2, App Engine clients do not need to address hardware configurations or software installations. With App Engine, clients create their own services and the services are run on Google's servers.

A Microsoft Azure cloud is also a PaaS cloud that allows clients to easily create services and then host them within Azure without having to know about hardware and software configurations, compared to the clouds above, Azure has an in-built discovery mechanic for services in its underlying, .NET Services Bus. When a service is hosted in Azure, it is able to register a URI to the Bus so that clients can discover the service without needing to know its location. As the Bus does the location resolution, clients are able to use the service no matter where the service is moved.

A Salesforce cloud is a SaaS provider, it offers access to customer relations management (CRM) software. It offers the highest level of abstraction where all maintenance from hardware to configuration to software updates is managed by Salesforce without involvement from its clients.

Amazon's EC2/S3, Google Apps and force.com of Salesforce are commercial solution clouds, while Amazon, IBM,

Microsoft and Google are Public Cloud providers.

5. CONCLUSION

In conclusion, despite the threats and vulnerabilities mentioned in the paper, it is of note that they are being addressed currently as research are on-going in finding ways to reduce and subsequently overcome the threats and vulnerabilities enlisted. So in all cloud adoption and existence has come to stay and it provides a path to the next generation enterprise.

REFERENCES:

[1] Atif F.M & Hamid M. (2011) "Cloud Services Testing: An Understanding" Elsevier Ltd, Procedia Computer Science 5(2011) pg. 513-520. Retrieved from www.sciencedirect.com on Dec. 4, 2012

[2] Dan C. Marinescu (2012) "Cloud Computing: Theory & Practice" pg. 19-28 &109-111. Retrieved from www.lectureNotes.pdf on Dec. 6, 2012

[3] Eumir P. Reyes (2010) "A System thinking Approach of Business Intelligence Solution Based on Cloud Computing" M.Sc Thesis in Engineering & Management pg. 10-12. Retrieved from www.mscthesis667715636.pdf on Dec. 5, 2012

[4] Hanunah Othman, Habibah H., Jamalul-lail Al. M., (2011) "PE-TLBs:Secure Location Based Services Environment with Emphasis on Direct Anonymous Attestation Protocol" International Journal Multimedia & Image Processing (IJMIP), vol.1, Issue1, March 2011. Retrieved from www.salam.uitm.edu.my on Sept. 6, 2011

[5] Katarina S.S., Thomas W., Santi R., (2010) "Grid & Cloud Computing; A Business Perspective on Technology & Applications" Springer Heidelberg Dordrecht London New York pg. 23-60. Retrieved from www.springer.com/...pdf on Dec. 5, 2012

[6] Kertesz A., Kecskemeti G., Brandic I., (2012) "An Interoperable & Self-adaptive approach for SLA- based service virtualization in heterogeneous cloud environments". Retrieved from www.elsevier.com/ locate/fgcs on Dec. 6, 2012

[7] Lizhe W., Marcel K., Jie T., Gregor Von L., (2012) "Towards building a cloud for scientific application" Elsevier Ltd. Retrieved from www.doi.1-s2.0...main.pdf on Nov. 9, 2012

[8] Michael Armbrust, Armando F., Rean G., et al (2009) "Above the clouds: A Berkeley View of cloud computing". Retrieved from http:// www.eecs.berkeley.edu/pubs/ techrpts/ 2009/eecs-2009-28.html on Dec. 5, 2012

[9] Nancy J.K., & Raja V.T., (2012) "Protecting the Privacy & Security of Sensitive Customer data in the cloud". Retrieved from www.compseconline.com/ publications/prod claw.htm/ on Dec. 5, 2012

[10] Rajkumar B., Chee S, .Y., Srikumar V., James B., Ivona B., (2008) "Cloud Computing & emerging IT platforms: Vision, Hype & reality for delivering computing as the 5th utility". Retrieved from www.elsevier.com/locate/fgcs on Dec. 5, 2012

[11] Rodrigo N.C., Adel N.T., Christian V., Rajkumar B., (2012) "A

coordinator for scaling elastic applications across multiple clouds". Retrieved from www.elsevier.com/ locate/fgcs/ on Dec. 5, 2012

[12] Rong Chunming, Son .T.N., Martin G.J., (2012) "Beyond lighting: A survey on security challenges in cloud computing" Elsevier Ltd. Retrieved from ttp://dx.doi.org/10.1016/ j.compeleceng.201 2.04.015/ on Dec. 4, 2012

[13] Seventh Frame work programme Syssec, (2011 & 2012) "A European Network of Excellence in managing threats & vulnerabilities in the future Internet: Europe for the world". Retrieved from www.syssec-project.eu on Dec. 6, 2012

[14] Xappirio "State of the public cloud: The cloud adopters' perspective". Retrieved from www.state-thepublic cloud.results_final_102910.pdf/ on Dec. 9, 2012.