IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

*International Advanced Research Journal in Science, Engineering and Technology*
*Vol. 2, Issue 12, December 2015*

# Security Issues and Challenges in Cloud Computing

**Dr. N. Krishna Murthy[1], Dr. R. Selvam[2]**

Assistant Professor, Department of Computer Science, Sri Subramanyaswamy Government Arts College,

Thiruvallur District, Tiruttani, Tamil Nadu, India[1,2]

**Abstract:** Cloud computing builds on established trends, where a large number of systems are connected in both public and private networks, which uses internet and one centralized server to maintain data and various applications. Due to Technology advancement, the cost of computation, application hosting, content storage and delivery is reduced significantly. Cloud Computing is a flexible, cost-effective, and proven delivery platform for providing business or consumer IT services over the Internet. Forrester defines cloud computing as: "A pool of abstracted, highly scalable, and managed compute infrastructure capable of hosting end-customer applications and billed by consumption." This paper introduces a detailed analysis of the cloud computing security issues and challenges focusing on the cloud computing types and the service delivery types.

**Keywords:** Architecture; Infrastructure; Platform; Software; Security issues; Challenges; IT.

## I. INTRODUCTION

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[1]

Cloud Computing appears as a computational paradigm as well as distribution architecture and its main objective is to provide secure, quick, convenient data storage and net computing service, with all computing resources visualized as services and delivered over the Internet.

The cloud enhances collaboration, agility, scalability, availability, ability to adapt to fluctuations according to demand, accelerate development work, and provides potential for cost reduction through optimized and efficient computing. Other Objectives of Cloud computing are Providing resources to the IT Professional ("anywhere, anytime"); To offer infinite environment over seamless and prompt elasticity; To expose supercomputer-like high performance; To lead to minimal costs.[2]

The difference that cloud computing brings compared to traditional concepts of "grid computing", "distributed computing", "utility computing", or "autonomic computing" is to broaden horizons across organizational boundaries.[3]

A simple example of cloud computing is Yahoo email, Gmail, or Hotmail etc. All you need is just an internet connection and you can start sending emails. The server and email management software is all on the cloud (internet) and is totally managed by the cloud service provider Yahoo, Google etc. [4]

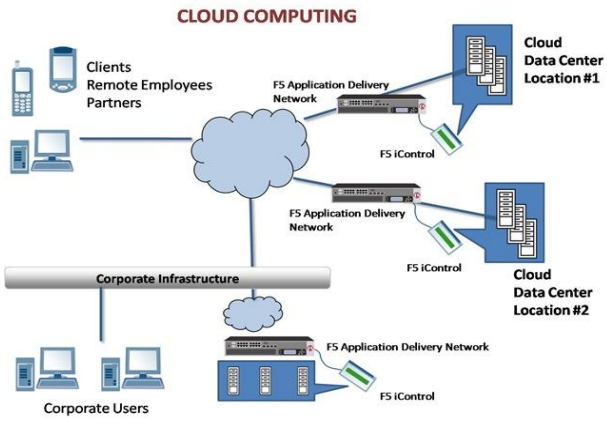


Fig. 1 Cloud Computing Architecture

## II. CLOUD SERVICE DELIVERY MODELS

The cloud model provides three types of services: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS)[5]:

**INFRASTRUCTURE AS A SERVICE (IAAS):** The effectiveness provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer has control over operating systems, storage, deployed applications, and possibly limited control of select networking components.

**PLATFORM AS A SERVICE (PAAS):** The effectiveness provided to the consumer is to deploy onto the cloud infrastructure his own applications without installing any platform or tools on their local machines. PaaS refers to providing platform layer resources, including operating system support and software development frameworks that can be used to build higher-level services.

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
*International Advanced Research Journal in Science, Engineering and Technology*
*Vol. 2, Issue 12, December 2015*

**SOFTWARE AS A SERVICE (SAAS):** The effectiveness provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email).

## III. SECURITY ISSUES ON DELIVERY MODELS ON CLOUD COMPUTING

**INFRASTRUCTURE-AS-A-SERVICE (IAAS) SECURITY ISSUE:** IaaS provides abundant resources such as servers, storage, networks, and other computing resources in the form of virtualized systems, which are accessed through the Internet. Users are entitled to run any software with full control and management on the resources allocated to them. With IaaS, cloud users have better control over the security compared to the other models as long there is no security hole in the virtual machine monitor. They control the software running in their virtual machines, and they are responsible to configure security policies correctly. IaaS providers must undertake a substantial effort to secure their systems in order to minimize these threats that result from creation, communication, monitoring, modification, and mobility. Here are some of the security issues associated to IaaS [6].

**PLATFORM-AS-A-SERVICE (PAAS) SECURITY ISSUES:** PaaS facilitates deployment of cloud-based applications without the cost of buying and maintaining the underlying hardware and software layers. As with SaaS and IaaS, PaaS depends on a secure and reliable network and secure web browser. PaaS application security comprises two software layers: Security of the PaaS platform itself (i.e., runtime engine), and Security of customer applications deployed on a PaaS platform. PaaS providers are responsible for securing the platform software stack that includes the runtime engine that runs the customer applications[11].

**SOFTWARE-AS-A-SERVICE (SAAS) SECURITY ISSUES:** SaaS provides application services on demand such as email, conferencing software, and business applications such as ERP, CRM, and SCM. SaaS users have less control over security among the three fundamental delivery models in the cloud. The adoption of SaaS applications may raise some security concerns.

## IV. SECURITY ISSUES IN CLOUD COMPUTING:

Security issues over cloud computing is definitely one of the major concerns that many companies are trying to recognize. With the development in technology market, experts are also worried about the increased security needs for cloud computing [7].

Security concerns relate to risk areas such as external data storage, dependency on the "public" internet, lack of control, multi-tenancy and integration with internal security. Compared to traditional technologies, the cloud has many specific features, such as its large scale and the fact that resources belonging to cloud providers are completely distributed, heterogeneous and totally virtualized. Traditional security mechanisms such as identity, authentication, and authorization are no longer enough for clouds in their current form. Security controls in Cloud Computing are, for the most part, no different than security controls in any IT environment [12].

***Three deployment models identified for cloud architecture***

In the cloud deployment model, networking, platform, storage, and software infrastructure are provided as services that scale up or down depending on the demand. The Cloud Computing model has three main deployment models which are Private, Public & Hybrid [8].

**PRIVATE CLOUDS:** The cloud infrastructure is operated for a private organization. It may be managed by the organization or a third party, and may exist on premise or off premise. 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.

**PUBLIC CLOUDS:** The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services. Public Clouds describes cloud computing in the traditional mainstream sense, whereby resources are dynamically provisioned on a fine-grained, self-service basis over the Internet, via web applications/web services, from an off-site third-party provider who shares resources and bills on a fine-grained utility computing basis. It is typically based on a pay-per-use model, similar to a prepaid electricity metering system which is flexible enough to cater for spikes in demand for cloud optimization.

**HYBRID CLOUDS:** The cloud infrastructure is a composition of two or more clouds (private or public) that remain unique entities, but are bound together by standardized or proprietary technology, that enables data and application portability (e.g., cloud bursting for load-balancing between clouds). Hybrid cloud is a private cloud linked to one or more external cloud services, centrally managed, provisioned as a single unit, and circumscribed by a secure network. It provides virtual IT solutions through a mix of both public and private clouds.

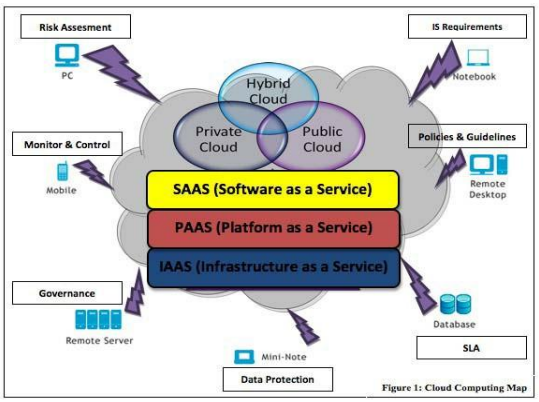


Fig. 2 Cloud Computing Models

## V. CHARACTERISTICS OF CLOUD COMPUTING

These are the six essential characteristics that cloud computing offers business[9].

**SCALABILITY OF INFRASTRUCTURE:** new devices can be added or dropped from the network as can physical servers, with restricted modifications to infrastructure set up and software. Cloud architecture can scale horizontally or vertically, according to demand.

**RELIABILITY:** improves through the use of multiple redundant sites, which makes cloud computing suitable for business continuity and disaster recovery.

**FLEXIBILITY/ELASTICITY:** users can rapidly provision computing resources, as needed, without human interaction. Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out or up.

**BROAD NETWORK ACCESS.** Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous platforms (e.g., mobile phones, laptops, and PDAs).

**LOCATION INDEPENDENCE.** 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 datacenter).

**ECONOMIES OF SCALE AND COST EFFECTIVENESS.** Cloud implementations, regardless of the deployment model, tend to be as large as possible in order to take advantage of economies of scale. Large cloud deployments can often be located close to cheap power stations and in low-priced real estate, to lower costs.

**Challenges of Cloud Computing:**

*An adoption of new technology of cloud computing is associated with numerous challenges because users are still skeptical about its authenticity*[10][13]*:*

**SECURITY:** It is clear that the security issue has played the most important role in hindering Cloud computing acceptance. Without doubt, 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.

**COSTING:** Cloud consumers must consider the tradeoffs amongst computation, communication, and integration. While migrating to the Cloud can significantly reduce the infrastructure cost, it does raise the cost of data communication, i.e. the cost of transferring an organization's data to and from the public and community Cloud and the cost per unit of computing resource used is likely to be higher.

**CHARGING:** The elastic resource pool has made the cost analysis a lot more complicated than regular data centers, which often calculates their cost based on consumptions of static computing.

## VI. SCOPE OF CLOUD COMPUTING

In Future, we are likely to see how low-power processors crunching many workloads in the cloud, housed in highly automated datacenters and supporting massively federated, scalable software architecture.

## VII. CONCLUSION

Cloud computing has received a lot of popularity in the last few years, however, it also raises some security problems which may slow down its use. Cloud Computing is an emerging trend of provisioning scalable and reliable services over the Internet as computing utilities. Even though, cloud computing too has its pros and cons. While the technology can prove to be a great asset to any business / individuals, it could also cause harm if not understood and used properly. As described in this paper, storage, virtualization, and networks are the biggest security concerns in Cloud Computing. Virtualization which allows multiple users to share a physical server is one of the major concerns for cloud users. Also, another challenge is that there are different types of virtualization technologies, and each type may approach security mechanisms in different ways. Virtual networks are also target for some attacks especially when communicating with remote virtual machines.

## REFERENCES

[1] S. Subashini, and V. Kavitha. (2010) "A survey on security issues in service delivery models of cloud computing." *J Network Comput Appl* doi:10.1016 / j.jnca.2010.07.006. Jul., 2010.
[2] A Platform Computing Whitepaper. "Enterprise Cloud Computing: Transforming IT." *Platform Computing*, pp6, 2010.
[3] Torry Harris – "Cloud Computing – Overview"
[4] Zhang S, Zhang S, Chen X, Huo X (2010) Cloud Computing Research and Development Trend. In: Second International Conference on Future Networks (ICFN'10), Sanya, Hainan, China. Washington, DC, USA: IEEE Computer Society. pp 93-97
[5] Nazia Majadi - "Cloud Computing: Security Issues and Challenges " - International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013
[6] S. Ramgovind, M. M. Eloff, E. Smith. "The Management of Security in Cloud Computing" In PROC 2010 IEEE International Conference on Cloud Computing 2010.
[7] R. K. Balachandra, P. V. Ramakrishna and A. Rakshit. "Cloud Security Issues." In PROC '09 IEEE International Conference on Services Computing, 2009, pp 517-520.
[8] Venkatesh. P - "Cloud Computing Security Issues and Challenges " - International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online) Vol. 2, Issue 3, pp: (122-128)
[9] "Addressing cloud computing security issues" - Future Generation Computer Systems - Volume 28, Issue 3, March 2012, Pages 583–592
[10] Kuyoro S. O., Ibikunle F. & Awodele O; Cloud Computing Security Issues and Challenges; International Journal of Computer Networks (IJCN), Volume (3) : Issue (5) : 2011; pp 247-257.
[11] N. Gruschka, L. L. Iancono, M. Jensen and J. Schwenk. "On Technical Security Issues in Cloud Computing" In PROC 09 IEEE International Conference on Cloud Computing, 2009 pp 110-112.
[12] R. K. Balachandra, P. V. Ramakrishna and A. Rakshit. "Cloud Security Issues." In PROC '09 IEEE International Conference on Services Computing, 2009, pp 517-520.
[13] P. Kresimir and H. Zeljko "Cloud computing security issues and challenges." In PROC Third International Conference on Advances in Human-oriented and Personalized Mechanisms, Technologies, and Services, 2010, pp. 344-349.