International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 6 | ISSN : 2456-3307

Study of Challenges for Cloud Computing and Cloud Security

Anand Singh*[1], Prof. (Dr.) Amod Kumar Tiwari[2]

*[1]Ph.D. Research Scholar, Department of Computer Science and Engineering, Sai Nath University, Ranchi, Jharkhand, India
[2]Director, Naraina College of Engineering and Technology, Kanpur, Uttar Pradesh, India

ABSTRACT

The objective of cloud computing is to apply customary supercomputing, or the power of high performance computing, typically used by military and research facilities to perform tens of trillions of calculations per second, application -oriented consumer, such as financial portfolios, to offer personalized information to provide data storage or feeding large immersive computer games. In this paper, we review the different security issues and challenges faced during deployment of cloud environment.

Keywords: Cloud Computing, Cloud Security, Cloud Challenges

I. INTRODUCTION

Cloud computing relies on sharing of resources to achieve coherence and economies of scale analogous to a utility (like the electricity grid) over a network. At the basis of cloud computing is the broader perception of converged infrastructure and shared services.

Cloud computing is a distributed computational model over a large pool of shared-virtualized computing resources (e.g., storage, processing power, memory, applications, services, and network bandwidth), where customers are provisioned and de-provisioned recourses, as they need. Cloud computing represents a vision of providing computing services as public utilities like water and electricity.

The architecture of cloud computing can be split in two: front-end and back-end. The front-end represents cloud customers, organizations, or applications (e.g., web browsers) that use the cloud services. The back-end is a huge network of data centres with many different applications, system programs, and data storage systems. It is metaphorically believed that, cloud service providers (CSPs) have almost infinite computation power and storage capacity.

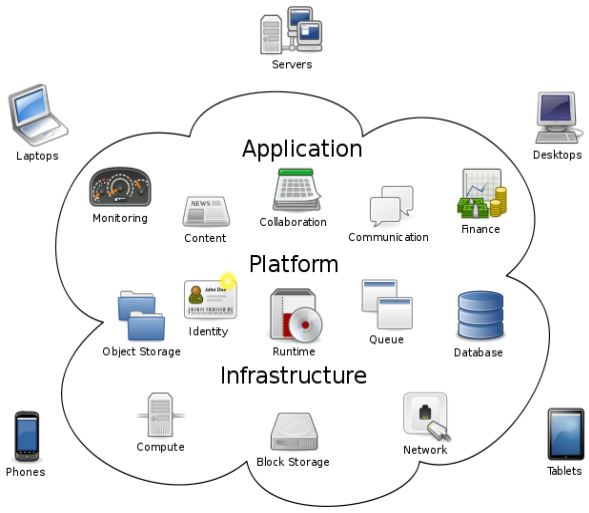

Figure 1 : Logical diagram of Cloud computing

A conceptual framework of cloud computing architecture is illustrated in Figure 2 with its two main parts.

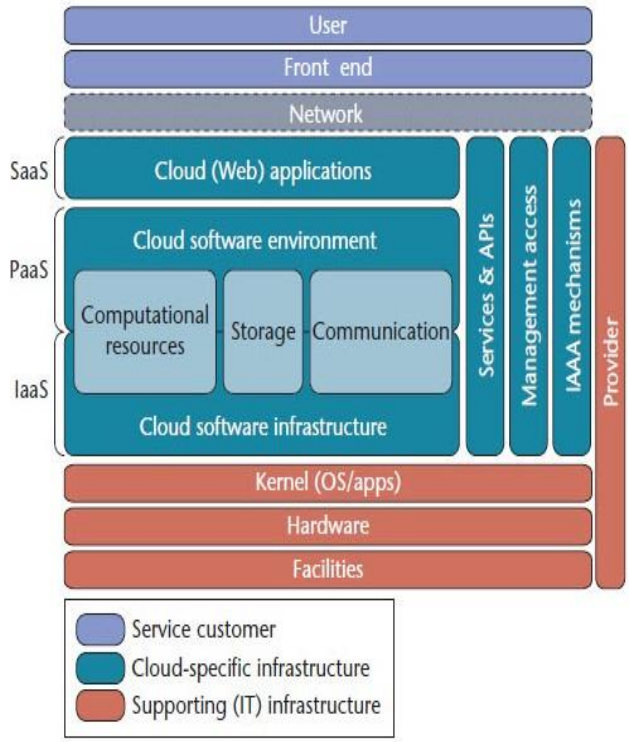

Figure 2 : Conceptual framework for Cloud Computing architecture.

Cloud computing services can be categorized into following:

- ✓ Application-as-a-Service (AaaS).
- ✓ Platform-as-a-Service (PaaS).
- ✓ Infrastructure-as-a-Service (IaaS).

The widely used model of cloud computing services is the AaaS model, in which the customers have access to the applications running on the cloud provider's infrastructure. Google Docs, Google Calendar, and Zoho Writer are known examples of this model. In the PaaS model, the customers can deploy their applications on the provider's infrastructure under condition that these applications are created using tools supported by the provider. The cloud service provider (CSP) hosts a set of software and development tools on its servers to be used by the developers to create their own applications. Google Apps is one of the best known PaaS models. IaaS model enables customers to rent and use the provider's resources (storage, processing, and network).Hence, the customers can deploy any applications including operating systems.

II. MODELS OF CLOUD DEPLOYMENT

The cloud computing architecture can be deployed under different models:

- ✓ Public cloud: The infrastructure of the CSP is publicly accessible by general customers and organizations in exchange for pre-specified fees according to the usage of The CSP's services.
- ✓ Private cloud: The cloud infrastructure is dedicated to an organization, which may manage the infrastructure or leave this management to a third party.
- ✓ Hybrid cloud: The cloud infrastructure is composed of two or more clouds (private or public).The organizations provide and handle some internal and external resources.

For example, an organization can use a public cloud service as Amazon Elastic Compute Cloud (AmazonEC2) to perform the general computation, while the data files are stored within the organization's local data canter in a private cloud.

III. CLOUD COMPUTING CHALLENGES

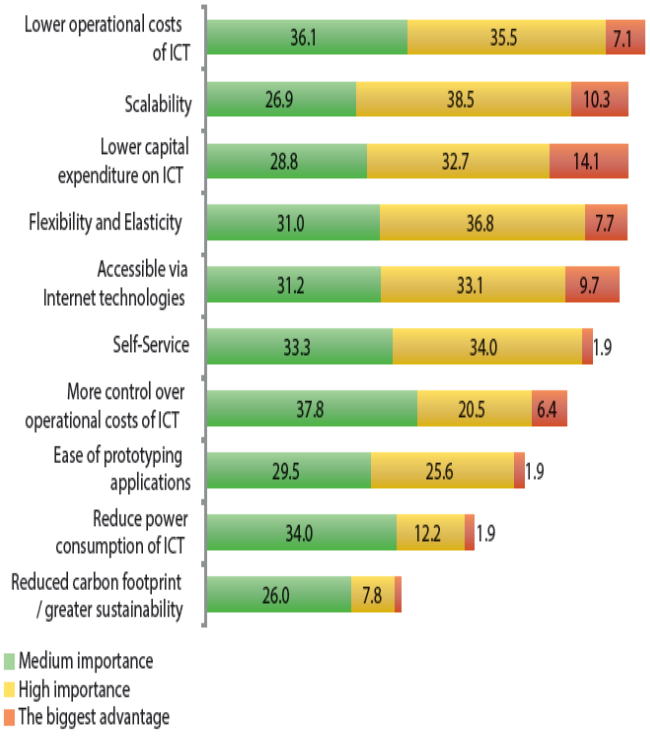

Figure 3: Benefits of Cloud Computing

Accessibility: Cloud computing model encourages single points of failure where cloud services are subject

to more attacks. Among the well-publicized incidents of cloud outages are Gmail (one-day outage) and Amazon Simple Storage Service (AmazonS3), which was down for over 7 hours. Therefore, it is of significant importance to develop new methods and techniques for sustained availability and speedy recovery from attacks.

Computational Veracity: Outsourcing computation is a growing trend for resource- constrained clients to benefit from powerful cloud servers. The ability to verify out-sourced computations and validate the returned results is a key requirement of cloud customers. Another imperative point is that the amount of work performed by the clients to verify the outsourced computations must be substantially cheaper than performing the actual computations on the client side.

Substantiation: The development of cloud computing encourages the use of resource- constrained devices (e.g., PDA and cell phones) on the client side. Rather than data storage and software installation on local devices, users will authenticate in order to be able to access the data and use cloud applications. This computing model makes software piracy more difficult and enables centralized monitoring. Although cloud computing architecture stimulates mobility of users, it increases the need of secure authentication. User authentication based on passwords in not an efficient approach for sensitive data/applications on the cloud. The use of passwords is a major point of vulnerability in computer security, as passwords are often easy to guess by auto- mated programs running dictionary attacks. Moreover, users cannot remember very long passwords, and usually they use some meaningful passwords making them subject to dictionary attacks.

Auditing: The internal operations of the CSP are opaque, and thus the auditing process is a major challenge. Customers with constrained computing resources and capabilities resort to external audit party to check the integrity of their outsourced data. They need to assure that there is no information leakage even by this third party. Third party auditing process should bring in no new vulnerabilities towards the privacy of client's data.

IV. CLOUD SECURITY

Cloud computing security is an evolving sub-domain of computer security, network security, and more broadly, information security. It refers to a broad set of policies, technologies and controls deployed to protect data, applications and the associated infrastructure of cloud computing. Cloud security is not to be confused with security software offerings that are "cloud- based". The scope of the cloud security spans across all the three service delivery models deployed in any of the four cloud deployment models (private, public, hybrid and community cloud) and exhibiting the five essential characteristics of the cloud. It is this span of the scope of security in the cloud that makes it very important and at the same time much complicated. The wide scope of the security thus has multiple facets including but not limited to security related to application, data transmission, data storage, authentication and authorization, network, virtualization and physical hardware. This raises multiple questions with respect to each of these facets.

V. CONCLUSION

Cloud computing entails the sharing or storage by users of their own information on remote servers owned or operated by others and accesses through the Internet or other connections. Cloud computing services subsist in numerous variations, comprising video sites, tax preparation sites, data storage sites, personal health record websites etc. In this paper, we studied the different challenges such as substantiation, computational veracity, auditing etc. We conclude that cloud security has multiple facets including but not limited to security related to application, data transmission, data storage, authentication and authorization, network, virtualization and physical hardware.

VI. REFERENCES

[1]. Kaufman, L.M. "Data Security in the world of cloud computing", Security and Privacy, IEEE Vol. 7, No. 4, pp. 61-64, 2009.

[2]. Puthal, D., Sahoo, B. P. S., Mishra, S., & Swain, S., Cloud computing features, issues, and challenges: a big picture. IEEE International Conference on Computational Intelligence and Networks (CINE), pp. 116-123, 2015

[3]. Hendre, Amit, and Karuna Pande Joshi. "A semantic approach to cloud security and compliance." IEEE 8th International Conference on Cloud Computing. pp. 1081-1084, 2015.
[4]. Youngmin, J. and Mokdong, C. "Adaptive security management model in cloud computing environment", In the 12th International Conference on Advanced Communication Technology (ICACT), pp 1664-1669, 2010.
[5]. Bret, M. "In Clouds Shall we Trust?," Security and Privacy, IEEE, Vol7, No.5, p 3, 2009.
[6]. Stanojevi, R. and Shorten, R. "Fully decentralized emulation of best- effort and processor sharing queues", In ACM SIGMETRICS international conference on Measurement and modeling of computer systems, ACM Press, New York 2008, pp. 383-394, 2008.
[7]. Hashizume, Keiko, et al. "An analysis of security issues for cloud computing." Journal of Internet Services and Applications 4.1, pp. 5, 2013.
[8]. Ahmed, Monjur, and Mohammad Ashraf Hossain. "Cloud computing and security issues in the cloud." International Journal of Network Security & Its Applications 6.1, pp 25, 2014.