International Journal of Research and Applications

ISSN (online): 2349-0020 ISSN (print): 2394-4544 http://www.ijraonline.com/

Survey Report

Cloud computing service models towards authentication in cloud

Sudheer Kumar Shriramoju

Project Manager, Wipro InfoTech, Hyderabad, India.

ARTICLE INFO

Corresponding Author:
sudheerpapers@gmail.com

DOI:
http://dx.doi.org/
10.17812/IJRA.7.25 (4)2020

Manuscript:
Received: 28th Jan, 2020
Accepted: 20th Feb, 2020
Published: 24th Mar, 2020

Publisher:
Global Science Publishing Group, USA
http://www.globalsciencepg.org/

ABSTRACT

Cloud computing is a distributed computing paradigm that focuses on providing a wide range of users with distributed access to scalable, virtualized hardware and/or software infrastructure over the internet. Despite this rather technical definition, cloud computing is in essence an economic model for a different way to acquire and manage IT resources. An organization needs to weigh the cost, benefits, and risks of cloud computing in determining whether to adopt it as an IT strategy. This paper provides cloud computing service models towards authentication in cloud.

Keywords: Service models, authentication, cloud.

1. INTRODUCTION

Recent developments in the field of could computing have immensely changed the way of computing as well as the concept of computing resources. In a cloud based computing infrastructure, the resources are normally in someone else's premise or network and accessed remotely by the cloud users (Petre, 2012; Ogigau-Neamtiu, 2012; Singh & jangwal, 2012). Processing is done remotely implying the fact that the data and other elements from a person need to be transmitted to the cloud infrastructure or server for processing; and the output is returned upon completion of required processing. In some cases, it might be required or at least possible for a person to store data on remote cloud servers.

These gives the following three sensitive states or scenarios that are of particular concern within the operational context of cloud computing:

- The transmission of personal sensitive data to the cloud server,
- The transmission of data from the cloud server to clients' computers and
- The storage of clients' personal data in cloud servers which are remote server not owned by the clients.

All the above three states of cloud computing are severely prone to security breach that makes the research and investigation within the security aspects of cloud computing practice an imperative one. There have been a number of different blends that are being used in cloud computing realm, but the core concept remain same – the infrastructure, or roughly speaking, the resources remain somewhere else with someone else's ownership and the users 'rent' it for the time they use the infrastructure (Bisong & Rahman, 2011; Rashmi, Sahoo & Mehfuz, 2013; Qaisar & Khawaja, 2012).

In some cases, stored sensitive data at remote cloud servers are also to be counted. Security has been at the core of safe computing practices. When it is possible for any unwanted party to 'sneak' on any private computers by means of different ways of 'hacking'; the provision of widening the scope to access someone's personal data by means of cloud computing eventually raises further security concerns. Cloud computing cannot eliminate this widened scope due to its nature and approach. As a result, security has always been an issue with cloud computing practices. Robustness of security and a secured computing infrastructure is not a one-off effort, it is rather ongoing – this makes it essential to analyses and realize the state-of-the-art of the cloud computing security as a mandatory practice.

Cloud is mainly categorized as private cloud, community cloud, public cloud and hybrid cloud - the discussion in this paper assumes only one category of cloud exists which is public cloud; as this assumption will well satisfy all the characteristics of any other type of cloud. Due to its diversified potentiality, the approach to cloud computing is being thought to be as the 5th utility to join the league of existing utilities water, electricity, gas and telephony rather than being just another service.

The study presented in this paper is organized with a view to discuss and identify the approach to cloud computing as well as the security issues and concerns that must be taken into account in the deployment towards a cloud based computing infrastructure. Discussion on the technological concepts and approaches to cloud computing including the architectural illustration has been taken into consideration within the context of discussion in this paper. Security issues inherent in cloud computing approach have been discussed afterwards.

The exploration in the technological and security concerns of cloud computing has led to the concluding realization on the overall aspects of cloud computing. The approaches to counter security issues inherent in cloud computing are numerous with diversified facets and applications which has been kept out of scope. A discussion on the authentication of cloud computing has been addressed as it forms the holistic basis to embed integrity in the context of cloud computing security.

2. AUTHENTICATION IN CLOUD

Security is the most prioritized aspect for any form of computing, making it an obvious expectation that security issues are crucial for cloud environment as well. As the cloud computing approach could be associated with having users' sensitive data stored both at clients' end as well as in cloud servers, identity management and authentication are very crucial in cloud computing (Kim & Hong, 2012; Emam, 2013; Han, Susilo & Mu, 2013; Yassin, Jin, Ibrahim, Qiang & Zou, 2012). Verification of eligible users' credentials and protecting such credentials are part of main security issues in the cloud - violation in these areas could lead to undetected security breach (Kumar, 2012) at least to some extent for some period. A possible authentication scenario for a cloud infrastructure is illustrated in figure 1.

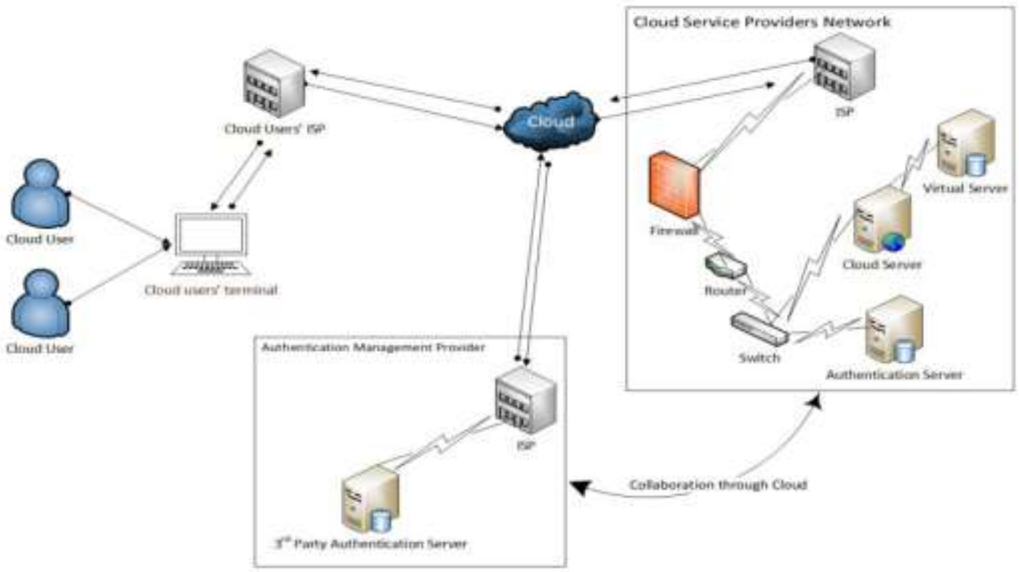

Figure 1: Authentication in the Cloud

The illustration presented in figure 1 conveys that the authentication for the cloud users can be done either by the cloud service provider or the service provider can outsource the identity management and authentication service to third party specialists (Gonzalez, Miers, Redigolo, Simplicio, Carvalho, Naslund & Pourzandi, 2012; Sharma & Mittal, 2013). In the latter case, the cloud service provider is required to have collaboration with the third party authentication specialist – the collaboration between the cloud service provider and the third party authentication specialist during the authentication process of cloud users is done essentially through cloud. This feature adds performance overheads and security issues to the cloud context as the message passing between third party authentication management authority and the cloud service provider as part of collaboration might essentially be done through cloud infrastructure. As discussed earlier, the total authentication process and how they are carried out - regardless of the involvement of third party authentication specialists – is transparent to the cloud users. The illustration on the authentication scenario presented above is a fairly simple one – if geographically dispersed servers are deployed by the cloud service providers then the total authentication process might be far more complex in terms of security, underlying algorithm as well as performance level. Whatever is the level of complexity, the introduction of third party authentication and identity management specialist into any cloud architecture should have only one goal; and the goal is to strengthen the robustness of security in the concerned area which the cloud service provider itself is not capable of to deploy or offer.

3. CLOUD COMPUTING MODELS

Cloud hosting deployment models are classified by the proprietorship, size and access. It tells about the nature of the cloud. Most of the organizations are willing to implement cloud since it reduces the expenditure and controls cost of operation

Cloud computing deployment models

Public Cloud

It is a type of cloud hosting in which the cloud services are delivered over a network that is open for public usage. This model is actually true representation of cloud hosting. In this the cloud model service provider provides services and infrastructure to various clients. Customers do not have any control over the location of the infrastructure. There may be very little or no difference between public and private clouds structural design except the level of security that are offered for various services given to the public cloud subscribers by the cloud hosting providers. Public cloud is suited for business which require managing load. Due to the decreasing capital overheads and operational cost the public cloud model is economical. Dealers may provide the free service or license policy like pay per user. The cost is shared by all the users in public cloud. It profits the customers by achieving economies of scale. Public cloud facilities may be available for free an e.g. of a public cloud is Google.

Private Cloud

It is also known as internal cloud. This platform for cloud computing is implemented on cloud-based secure environment and it is safeguarded by a firewall which is governed by the IT department that belongs to a particular corporate. Private cloud permits only the authorized users and gives the organization greater control over their data. The physical computers may be hosted internally or externally they provide the resources from a distinct pool to the private cloud services. Businesses having unanticipated or dynamic needs, assignments which are critical management demands and uptime requirements are better suited to adopt private cloud. In private cloud there is no need for additional security regulations and bandwidth limitations that can be present in a public cloud environment. Clients and Cloud providers have control of the infrastructure and improved security, since user's access and the networks used are restricted. One of the best examples is Eucalyptus Systems [4].

Hybrid Cloud

It is a type of cloud computing, which is integrated. It could constitute an arrangement of two or more cloud servers, i.e. either of the combination of private, public or community cloud that is bound together but remain individual entities. Hybrid clouds are capable of crossing isolation and overcoming boundaries by the provider; therefore, it cannot be simply categorized into public, private or community cloud. It allows the user to increase the capacity as well as the capability by assimilation, aggregation and customization with another cloud package / service. In a hybrid cloud, the resources are managed either in-house or by external providers. It is an adaptation between two platforms in which the workload exchanges between the private cloud and the public cloud as per the needs and demand of organization. Resources which are non-critical like development and test workloads can be housed in the public cloud that belongs to a third- party provider. While the workloads that are critical or sensitive should be housed internally. Organizations may use the hybrid cloud model for processing big data. Hybrid cloud hosting has features like scalability, flexibility and security.

Community Cloud

It is a type of cloud hosting in which the setup is mutually shared between a lot of organizations which belong to a particular community like banks and trading firms. It is a multi-tenant setup that is shared among many organizations that belong to a group which has similar computing apprehensions. Theses community members usually share similar performance and security concerns. The main intention of the communities is to achieve business related objectives. Community cloud can be managed internally or can be managed by third party providers and hosted externally or internally. The cost is shared by specific organizations within the community, therefore, community cloud has cost saving capacity. Organizations have realized that cloud hosting has a lot of potential. To be the best one must select the right type of cloud hosting Therefore, one need to know the business and analyze his/her demands. Once the appropriate type of cloud hosting is selected, one can achieve business related goals easily.

4. CLOUD COMPUTING SERVICE MODELS

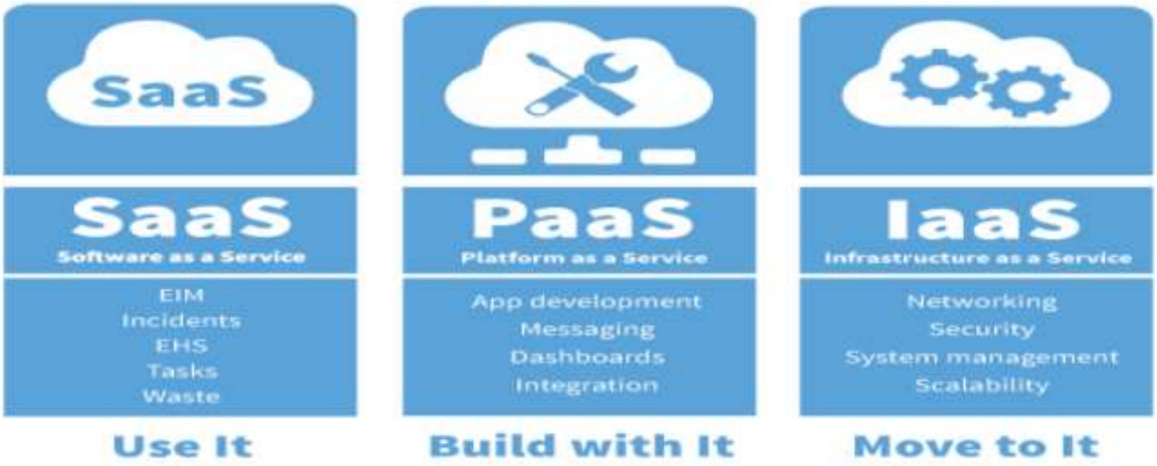

Figure 2: Cloud computing service models

Software as a Service (SaaS)

Software as a Service (SaaS) is growing rapidly. SaaS makes uses the web to provide applications which are managed by a third-party vendor and whose interface is accessed on the client side. SaaS applications can be run from a web browser without the need to download or installation, but these require plugins. The cloud provider provides the consumer with the ability to deploy an application on a cloud infrastructure [5].Because of this web delivery model SaaS removes the need to install and run applications on individual computers. In this model it is easy for enterprises to improve their maintenance and support, because everything can be managed by vendors: applications, runtime, data, middleware, OS, virtualization, servers, storage and networking. Popular SaaS services include email and collaboration, healthcare-related application. SaaS providers usually offer browser-based interfaces. APIs are also normally made available for developers. The key benefit of SaaS is that it requires no advance investment in servers or licensing of software. The application developer, have to maintain one application for multiple clients.

Infrastructure as a Service (IaaS)

Infrastructure as a Service, are used for monitoring, and managing remote datacenter infrastructures, such as compute (virtualized or bare metal), storage, Users can purchase IaaS based on consumption, similar to other utility billing. IaaS users have the responsibility to be in charge applications, data, runtime and middleware.. Providers can still manage virtualization, servers, storage, and networking. IaaS providers offer databases, messaging queues, and other services above the virtualization layer as well.

Platform as a Service (PaaS)

Platform as a service (PaaS) is a kind of cloud computing services that provides a platform that allows customers to develop, run, and manage applications without the problem of building and maintaining the infrastructure. One need not be bothered about lower level elements of Infrastructure, Network Topology, Security all this is done for you by the Cloud Service Provider. With this technology, third-party providers can manage OS, virtualization, and the PaaS software itself. Developers manage the applications. Applications using PaaS inherit cloud characteristic such as scalability, multi-tenancy, SaaS enablement, high- availability and more. Enterprises benefit from this model because it reduces the amount of coding, automates business policy, and help in migrating applications to hybrid model.

5. CONCLUSION

The evolution of cloud computing might significantly affect the collection and retention of digital evidence. The vastness and potentiality of cloud computing cannot be overlooked, subsequently robust security models for cloud computing scenarios is the most prioritized factor for a successful cloud based infrastructure development and deployment. With the goal of secured exploitation of a Service Oriented Architecture, the security aspects and issues of cloud computing are inherent not only with the elements that from the cloud infrastructure but also with all associated services as well as the ways computing is done both at the users' and the cloud service providers' ends. This paper provided the cloud computing service models towards authentication in cloud.

REFERENCES

1) Foster, I., Zhau, Y., Ioan, R., & Lu, S. "Cloud Computing and Grid Computing 360-Degree Compared." Grid Computing Environments Workshop, 2008.2. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4738445.
2) Grossman, R. "The Case for Cloud Computing." IT Pro 11, 2 (March/April 2009): 23-27.
3) Hayes, B. "Cloud Computing." Communications of the ACM 51, 7 (July 2008): 9-11.
4) Lin, G., David, F., Jinzy, Z., & Glenn, D. "Cloud Computing: IT as a Service." IT Pro 11, 2 (March/April 2009): 10-13.
5) McEvoy, G. & Schulze, B. "Using Clouds to address Grid Limitations," 1-6. Proceedings of the 6th International Workshop on Middleware for Grid Computing (MGC). Leuven, Belgium, December 2008. ACM, 2008. ISBN: 978-1-60558-365-5.
6) Sudheer Kumar Shriramoju, Surya Teja N, "Security in Different Networks and Issues in Security Management", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 8, Issue 2, February 2020.
7) Sudheer Kumar Shriramoju, "Access Control and Density Based Notion of Clusters", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN: 2395-602X, Print ISSN: 2395-6011, Volume 1 Issue 3, pp. 215-220, July-August 2015.
8) Sudheer Kumar Shriramoju, "Review on NoSQL Databases and Key Advantages of Sharepoint", International Journal of Innovative Research in Science, Engineering and Technology, ISSN (Online): 2319-8753, ISSN (Print): 2347-6710, Vol. 7, Issue 11, and November 2018.
9) Sudheer Kumar Shriramoju, "Capabilities and Impact of SharePoint on Business", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN: 2456-3307, Volume 2, Issue 6, November-December-2017.
10) Sudheer Kumar Shriramoju, "Security Level Access Error Leading to Inference and Mining Sequential Patterns", International Journal of Scientific Research in Science, Engineering and Technology, Volume 2, Issue 4, July-August 2016.
11) Sudheer Kumar Shriramoju, "An Overview on Database Vulnerability and Mining Changes from Data Streams", International Journal of Information Technology and Management, Vol. VII, Issue No. IX, August-2014.
12) Sudheer Kumar Shriramoju, "A Comprehensive Review on Database Security Threats and Visualization Tool for Safety Analyst", International Journal of Physical Education and Sports Sciences, Vol. 14, Issue No. 3, June-2019.
13) Sudheer Kumar Shriramoju, "Integrating Information from Heterogeneous Data Sources and Row Level Security", Journal of Advances and Scholarly Researches in Allied Education, Vol. IV, Issue No. VIII, October-201.
14) Sudheer Kumar Shriramoju, "A Review on Database Security and Advantages of Database Management System", Journal of Advances in Science and Technology, Vol. V, Issue No. X, August-201.