National Conference on Communication Technology & Network Security In association with
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 4 | Issue 7 | ISSN : 2456-3307

Data Security and Privacy in Cloud Computing Environment

Ganga Gudi
Department of Computer Science, KLE's S. Nijalingappa College, Bangalore, Karnataka, India

ABSTRACT

Cloud computing is an upcoming paradigm that offers tremendous advantages in economical aspects, such as reduced time to market, flexible computing capabilities, and limitless computing power. To use the full potential of cloud computing, data is transferred, processed and stored by external cloud providers. However, data owners are very skeptical to place their data outside their own control sphere. Cloud Computing is a combination of existing technologies that make a paradigm shift in building and maintaining distributed computing systems. The large improvements in processors, virtualization technology, data storage and networking have combined to make the cloud computing a more compelling paradigm.

Keywords : Cloud Computing, Security Controls

I. INTRODUCTION

Cloud Computing is a new computing paradigm in which the Internet is used to deliver reliable IT services to customers. The amount of service can be scaled up and down based on the customer needs. This flexibility, combined with the potential of a "pay-per-use" model makes the cloud attractive solution to enterprises, where the capital expenses are heavily reduced. Cloud Computing is a combination of existing technologies that make a paradigm shift in building and maintaining distributed computing systems. The large improvements in processors, virtualization technology, data storage and networking have combined to make the cloud computing a more compelling paradigm. The cloud computing service model is "X-as-a- service" where X includes IT functions. The above definition is supported by five key *cloud characteristics*, three *delivery models* and four *deployment models.*

a) Characteristics

Cloud computing has a variety of characteristics:

Shared Infrastructure: Uses a virtualized software model, enabling the sharing of physical services, storage, and networking capabilities. The cloud infrastructure, regardless of deployment model, seeks to make the most of the available infrastructure across a number of users.

Dynamic Provisioning: Allows for the provision of services based on current demand requirements. This is done automatically using software automation, enabling the expansion and contraction of service capability, as needed.

Network Access: Needs to be accessed across the internet from a broad range of devices such as PCs, laptops, and mobile devices, using standards-based APIs.

Managed Metering: It manages and optimizes the service and provide reporting and billing information. In this way, consumers are billed for services according to how much they have actually used during the billing period.

b) Service Models

Software-as-a-Service (SaaS): The SaaS service model offers the services as applications to the consumer,

using standardized interfaces. The services run on top of a cloud infrastructure, which is invisible for the consumer. The consumer can only control some of the user-specific application configuration settings.

Platform-as-a-Service (PaaS): The PaaS service model offers the services as operation and development platforms to the consumer. The consumer can use the platform to develop and run his own applications, supported by a cloud based infrastructure.

Infrastructure-as-a-Service (IaaS): The IaaS service model is the lowest service model in the technology stack, offering infrastructure resources as a service, such as raw data storage, processing power and network capacity. The consumer can use the IaaS based service offerings to deploy his own operating systems and applications.

c) Deployment Models

There are four deployment models:

Public clouds: Public cloud computing is based on massive scale offerings to the general public. The infrastructure is located on the premises of the provider, who also owns and manages the cloud infrastructure.

Private clouds: Private clouds run in service of a single organization, where resources are not shared by other entities. The physical infrastructure may be owned by organization's datacenters. Private cloud users are considered as trusted by the organization, in which they are either employees, or have contractual agreements with the organization.

Community clouds: Community clouds run in service of a community of organizations, having the same deployment characteristics as private clouds. Community users are also considered as trusted by the organizations that are part of the community.

Hybrid clouds: Hybrid clouds are a combination of public, private, and community clouds. Each part of a hybrid cloud is connected to the other by a gateway, controlling the applications and data that flow from each part to the other. The private and community clouds are managed, owned, and located on either organization or third party provider side as per characteristic.

II. PROBLEM STATEMENT

There is a lack of knowledge on how cloud computing impacts the confidentiality of data stored, processed and transmitted in cloud computing environments. In this paper we concentrate on the security controls which protect the most sensitive data in private cloud computing architectures. With cloud computing, organizations can use services and store data outside their own control. This development raises security questions and should induce a degree of skepticism before using cloud services which points out five areas of security issues in cloud computing.

- **Privileged user access**

Data stored and processed outside the enterprises direct control, brings "an inherent level of risk, because outsourced services bypass the physical, logical and personnel controls IT shops exert over in-house programs".

- **Data location**

The exact location of data in the cloud is often unknown. Data may be located in systems in other countries, which may be in conflict with regulations prohibiting data to leave a country or union.

- **Recovery**

Cloud providers should have recovery mechanisms in place in case of a disaster. "Any offering that does not replicate the data and application infrastructure across multiple sites is vulnerable to a total failure".

- **Regulatory compliance**

Data owners are responsible for the integrity and confidentiality of their data, even when the data is outside their direct control, which is the case with external service providers such as cloud providers.

- **Data Lock-in**

Availability of customer's data may be at risk if a cloud provider goes broke or is acquired by another

organization. Providers should provide procedures on how customers can retrieve their data when needed.

III. SYSTEM SECURITY CONTROL SELECTION

It describes the security controls classes and to which families they are. Then we will describe the control selection process, presenting a recommended baseline of controls for each impact level of an information system. We will also show how this baseline can be refined to match the specific requirements of an organization. The result will be a list of required technical controls to match the security requirements of an information system. Security controls can be placed into three classes:

- **Technical security controls**

Technical controls can be used to protect against specific types of threats. These controls can range from simple to complex measures and consist of a mix of software, hardware and firmware.

- **Management security controls**

Management security controls are implemented to manage and reduce risks for the organization. Management security controls can be considered as the highest level, which focuses on the stipulation of policies, standards and guidelines.

- **Operational security controls**

It is used to correct operational deficiencies that might be exploited by potential attackers. Physical protection procedures and mechanisms are examples of operational security controls.

a) Procedure for selection process

When organizations start the selection process, there are three steps to be executed:

Selecting the initial security control baseline

The selection process begins with a baseline of controls, which are later on tailored and supplemented when the need arises.

Tailoring the security control baseline

After selecting the initial security control set, the organization continues the selection process by tailoring this baseline to their specific business conditions. Tailoring a baseline consists of two steps.

- Policy & regulatory related considerations
- Public access related considerations

Supplementing the tailored security controls

The tailored security control baseline acts as the starting point for determining whether or not this selection of controls provides enough security for the information system. This is done by comparing the organizations assessment of risk and what is required to sufficiently mitigate the risks to the organization. Two approaches can be taken to identify which additional controls and control enhancements must be included in the final agreed-upon set of controls:

- **Requirements definition approach**: In this approach the organization investigates possible threats and acquire specific information about what adversaries may be capable of, and what damage human errors may inflict. With this assessment of possible threats, additional security can be obtained by adding control enhancements.
- **Gap analysis approach:** It begins with an assessment of the current security capabilities, followed by a determination of what threats can be expected. This approach identifies the gap between the current security capabilities and selects additional controls enhancements.

b) Cloud Control limitations

In this, five properties influence the applicability of a security control, depending on the deployment of the information system and inherently, the deployment of the control itself.

IV. CLOUD SECURITY SOLUTIONS

The goal of this section is to describe the solutions and choices available to either counter these limitations,

or accept the limitations. When an organization considers a cloud service offering as operational environment for the information system in question, both parties can perform a gap analysis to determine which security controls are required for the information system, and which security controls the cloud service provider supports. The difference between the required controls and the supported controls is called the security gap. To reduce the organizational risk that the security gap imposes, the NIST recommends the following three options:

1. Use the existing contractual vehicle to require the external provider to meet the additional security control requirements established by the organization.
2. Negotiate with the provider for additional security controls if the existing contractual vehicle does not provide for such added requirements.
3. Employ alternative risk mitigation measures within the organizational information system when a contract either does not exist or the contract does not provide the necessary leverage for the organization to obtain needed security controls.

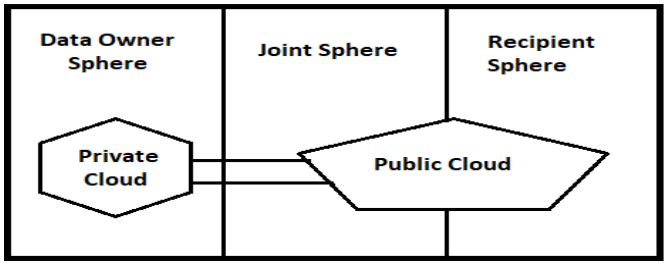

Fig 1. Hybrid cloud computing; the combination of clouds in multiple control spheres

V. CONCLUSION

The usage of cloud computing as a computing environment for information systems and data can place data outside the data owner's control. The amount of protection needed to secure data is directly proportional to the value of the data. When the value of data increases, the number and extensiveness of needed security controls also increase. It could be a problem if these security controls are not supported by the cloud provider. The uncertainty of how security can be guaranteed in external computing environments raises several security questions concerning the availability, integrity, and confidentiality of data in these cloud computing environments. We have focused on the confidentiality issues in cloud computing environments and proposed hybrid cloud computing is a very promising cloud deployment model that can cope with the security limitations occurring in a public cloud environment, while still being able to support many of the economical advantages of public cloud computing. Hybrid clouds depend heavily on the gateway between the private part of the hybrid cloud and the public part of the hybrid cloud. The gateway between the private and public parts of a hybrid cloud is an interesting point for research.

VI. REFERENCES

[1]. http://www.infoworld.com.
[2]. http://www.thestandard.com/article/0,1902,5466,00.html.
[3]. An example of a 'Cloud Platform' for building applications.
[4]. Klein, D. A. Data security for digital data storage
[5]. Mell, P., Grance, T. The nist definition of cloud computing National Institute of Standards and Technology 2009
[6]. Cloud Security Alliance. http://www.cloudsecurityalliance.org.

Cite this article as : Ganga Gudi, "Data Security and Privacy in Cloud Computing Environment", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 4 Issue 7, pp. 155-158, September-October 2019. Journal URL : http://ijsrcseit.com/CSEIT194728