ISSN:0975-9646

Subedari Mithila et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (5) , 2011, 1836-1840

Data Security through Confidentiality in Cloud Computing Environment

Subedari Mithila, P. Pradeep Kumar

Department of Computer Science & Engineering, Vivekananda Institute of Tech & Sciences, Karimnagar, JNTUH, Hyderabad, AP, 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 sceptical to place their data outside their own control sphere.**

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 that service can be scaled up and down based on 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 (e.g. infrastructure, storage, platform, database, software, security).The above definition is supported by five key *cloud characteristics*, three *delivery models* and four *deployment models.* These supporting properties will be explained below

1. Characteristics

Cloud computing has a variety of characteristics, with the main ones being:

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. This dynamic scaling needs to be done while maintaining high levels of reliability and security.

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 (for example, ones based on HTTP). Deployments of services in the cloud include everything from using business applications to the latest application on the newest smart phones.

Managed Metering — Uses metering for managing and optimizing the service and to 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. In short, cloud computing allows for the sharing and scalable deployment of services, as needed, from almost any location, and for which the customer can be billed based on actual usage.

2. 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 cloud provider is responsible for the management the application, operating systems and underlying infrastructure. 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. "The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations".

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, offering a wider variety of deployment possibilities for a consumer than the PaaS and SaaS models. "The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls)".

3. Deployment Models

Deploying cloud computing can differ depending on requirements, and the following four deployment models have been identified, each with specific characteristics that support the needs of the services and users of the clouds in particular way like (i) *who owns* the infrastructure; (ii) *who manages* the infrastructure; (iii) *where is* the infrastructure *located*; (iv) and *who accesses* the cloud services.

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. Public cloud users are considered to be untrusted, which means

they are not tied to the organization as employees and that the user has no contractual agreements with the provider.

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 and/or physically located in the organization's datacenters (on-premise) or that of a designated service provider (off-premise) with an extension of management and security control planes controlled by the organization or designated service provider respectively" . 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. Hybrid clouds leverage the capabilities of each cloud deployment model. 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. Where private and community clouds are managed, owned, and located on

either organization *or* third party provider side per characteristic, hybrid clouds have these characteristics on *both* organization *and* third party provider side. The users of hybrid clouds can be considered as trusted and untrusted. Untrusted users are prevented to access the resources of the private and community parts of the hybrid cloud.

4. Benefits

The following are some of the possible benefits for those who offer cloud computing-based services and applications:

Cost Savings — Companies can reduce their capital expenditures and use operational expenditures for increasing their computing capabilities. This is a lower barrier to entry and also requires fewer in-house IT resources to provide system support.

Scalability/Flexibility — Companies can start with a small deployment and grow to a large deployment fairly rapidly, and then scale back if necessary. Also, the flexibility of cloud computing allows companies to use extra resources at peak times, enabling them to satisfy consumer demands.

Reliability — Services using multiple redundant sites can support business continuity and disaster recovery.

Maintenance — Cloud service providers do the system maintenance, and access is through APIs that do not require application installations onto PCs, thus further reducing maintenance requirements.

Mobile Accessible — Mobile workers have increased productivity due to systems accessible in an infrastructure available from anywhere.

II. PROBLEM STATEMENT

Cloud computing users work with data and applications that are often located off-premise. However, many organizations are uncomfortable with the idea of having their data and applications on systems they do not control. 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 most thorough security controls needed to protect the most sensitive data may not be guaranteed in public cloud computing architectures, while they can be realized in private cloud computing architectures. As the most promising cloud computing approach, the selective cloudbursting, which acts as a hybrid cloud model with selective data transfers between public and private clouds. 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 scepticism before using cloud services which points out five areas of concern around security issues in cloud computing.

- **Privileged user access**

  Data stored and processed outside the enterprises direct control, brings with "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. Where traditional service providers are forced to comply to external audits and obtain security certifications.

- **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 how customers can retrieve their data when the needed, and at least as important; in which format the data is presented to the customer. If the data is presented in a format proprietary to the cloud provider, it may be unusable by any other provider. The use of open standards by providers to prevent data lock-in is recommended, but not always supported.

1. Our Approach

To address the security questions that raised when the organisations can use services and store data outside their own control can be addressed by identifying the security controls, its limitations in Section 3. The rest of paper followed by providing the security control solutions in Section 4 and Finally Section 5 concludes the paper.

III. SYSTEM SECURITY CONTROL SELECTION

In this section, we will describe the control selection process. We start by describing security controls classes and which security control families there 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 given the confidentiality impact level of the system. Security controls, when used correctly, can prevent, limit or deter threat-source damage to organization. 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. Next to standalone controls, technical controls also support the management and operational controls described below.

- **Management security controls**

Management security controls are implemented to manage and reduce risks for the organization and to protect an organization's mission. Management security controls can be considered of the highest level of controls, focusing on the stipulation of policies, standards and guidelines, which are carried out by operational procedures to fulfill the organization's goals and missions.

- **Operational security controls**

Operational security controls are used to correct operational deficiencies that might be exploited by potential attackers. These controls are implemented following good industry practices and a base set of requirements in the form of technical controls. Physical protection procedures and mechanisms are examples of operational security controls.

We want to focus on the technical layer of controls. Operational controls, which govern the physical protection and personnel management, will not differ much in a cloud environment with respect to the traditional computing environments. We do not include management controls in this section as they either do not differ much from the traditional environments. The technical control families we are focusing on are Access Control, Audit & Accountability, Identification & Authentication, and System and Communication Protection.

1. Procedure for selection process

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

1.1 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.

1.2 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**

Security controls related to information and information systems that are governed by laws, directives, policies and regulations are required to be implemented only if the implementation of the control is consistent with the information and information systems covered by the laws, directives, policies and regulations.

- **Public access related considerations**

When public access is allowed to an information system, security controls related to personal identification and authentication are only applicable in a limited manner. For example, while these controls offer identification and authentication of personnel that maintain a publicly available website, those controls are not needed for access to public available information.

1.3 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. In many cases, additional controls and control enhancements must be selected to supplement the tailored security control baseline. Two approaches can be taken to identify which additional controls and control enhancements must be included in the final agreed-upon set of controls; the r*equirements definition* approach and the *gap analysis* approach.

- **Requirements definition approach**

In this approach the organization investigates possible threats and acquires credible and specific information about what adversaries may be capable of, as well as what damage human errors may inflict. With this assessment of possible threats, additional security can be obtained by adding controls and control enhancements

- **Gap analysis approach**

In gap analysis approach 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 and control enhancements.

2. Cloud Control limitations

In this, we discuss that the application of these security controls in cloud environments can have limitations.

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.

- Who owns the information system?
- Who manages the information system?
- Where is the information system located?
- Who has access to the information system?
- How is the information system accessed?

The first three questions should be answered from the perspective of the data owner, where the information system in question processes, transfers or stores the data.

The last two questions should be answered from the perspective of the information system user.

- The *ownership* of the information system and the underlying infrastructure of the information system, lies with either the owner of the data inside the system, or lies with a 3rd party.
- The *management* of the information system and the underlying infrastructure is either done by the data owner, by a party managing the information on behalf of the data owner, or by another party who has no official relation with the data owner.
- The *location* of the information system and the underlying infrastructure, is either within the organizational boundaries of the entity owning the data, or is located external to the data owner's location.
- *Who accesses* the information system and the data within the information system can be divided into three groups; 1) Public users, who do not have to be identified or authenticated as they access only public information, 2) Non-organizational users, who do not belong to the organization, but access information not deemed as public and as such, require identification and authentication. For example, a website owner needs to log in before he can change the content of his website,
  3) Organizational users, who are either employees of the organization, or users deemed to have equal status as employees (e.g. contractors, guest researchers). The reason we make this difference between user groups, is that each group require different controls to access an information system.
- *How* the information system is *accessed*, is described by the type of connection a user has to the information system and data. The type of connection has a strong relation to the traditional organizational boundary of an organization. The connection to an information system can be divided in local and network based access. Network based access can be further divided in access via internal networks (e.g. LAN, WAN and VPN connections), and access via external networks (e.g. Internet, Dial-in, Wireless, Broadband). How an information system is accessed, is an important factor in the matter how much the access can be trusted to be secure

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 to close the gap between what security is needed and what security is offered by external service providers:

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 (including compensating 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"

The following setup is very useful as a workaround for the control problems that occur in both the joint and recipient sphere. Also the three general problems like. Access related limitations, Security assurance limitations, System separation limitation can be handled by this setup.

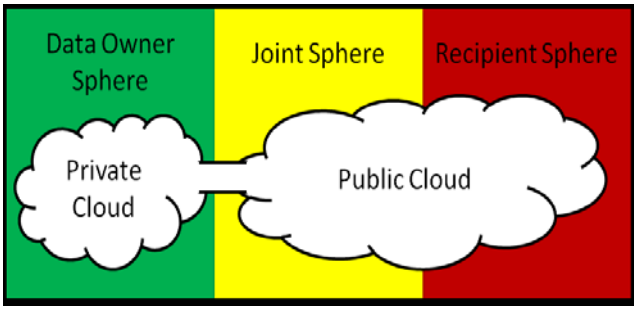

Fig 1: Hybrid cloud computing; the combination of clouds in multiple control spheres

For example, when the public cloud providers do not support physical separation of systems that are classified as Moderate and High systems, these systems should be hosted in the private part of the hybrid cloud, where these limitations do not occur.

Likewise, if the encryption requirements are not properly supported by the public cloud providers, the Moderate and High systems should operate in the data owner sphere, while Low systems and data could operate in both parts of the Hybrid cloud.

It is important to magnify on the connection between the private and public cloud. This gateway between the two control spheres is of critical importance to the usability of the hybrid deployment model. This gateway is responsible for the following functions and security objectives;

1.Allow information systems and data flow between the public and private cloud parts, in order to support the independent resource pooling and rapid elasticity characteristics of cloud computing.

2. Prevent information systems and data to flow from the private part to the public part, if the
Security for those systems and data cannot be guaranteed by the public cloud provider.

This gateway has the responsibility for the trade-off between usability of the public cloud, and security of the private cloud

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.

REFERENCES

[1] http://www.infoworld.com/d/cloud-computing/what-cloud-computin g -really-means-031.

[2] http://www.thestandard.com/article/0,1902,5466,00.html.

[3] Building GrepTheWeb in the Cloud, Part 1: Cloud Architectures.Developer.amazonwebservices .com

[4] http://developer.amazonwebservices.com/connect /entry. jspa? external ID=1632&categoryID=100. Retrieved 2010-08-22.

[5] An example of a 'Cloud Platform' for building applications.