International Journal of Recent Trends in Engineering & Research
ISSN(ONLINE) : 2455-1457
IMPACT FACTOR : 3.344

Cloud Computing Security

Sanchita Agarwal [1], Ankit Pandey [2], Sandhya Pati [3]
[1,2,3] Computer Science, FCRIT

Abstract—Cloud computing is a way to run one's business. It is an epitome in which the resources can be used whenever required thus reducing the cost and complexity of service providers. It has the capacity to add and subtract the resources as per the requirement. This helps in providing elasticity. Cloud computing promises to cut operational and capital costs and more importantly let IT departments focus on strategic projects instead of keeping datacenters running. We just pay for what we actually use. We can get the capacity on demand. It is highly flexible. It allows the user to access applications that do not reside at user's location. Confidentiality, Integrity, Availability, Authenticity, and Privacy are essential concerns for both Cloud providers and consumers as well. In this paper, we discuss the need for valuation of Cloud Computing, structure the key components in a framework, and identify security issues related to Cloud Computing.

Keywords— Computing, Cloud Computing Security, Infrastructure-as-a-Service, Software-as-a-Service, Platform-as-a-Service

I. INTRODUCTION

A Cloud Computing is big and it is becoming bigger every day. It has been a major objective of the industries which ensures on-demand provisioning of scalable and reliable compute services. Cloud Computing allows consumers to be able to rent infrastructure according to their needs and charges them based on the usage of the service they do. It not only deploys applications but also stores data, and access them via Web protocols.

The acceptance of Cloud Computing depends on the ability to implement a model. The framework assists decision makers in estimating Cloud Computing costs and to compare these costs to traditional IT solutions. Whenever the situation arises that a company requires hardware and components to meet the requirements it is Cloud Computing that provides network, server, storage, application, service and so on and they can be deployed with much quick and easy manner and least management.

Cloud computing thus improves the availability of the resources and owns many advantages over other computing techniques. Users can use the IT infrastructure with Pay-per-Use-On-Demand mode [4]. As a result this would provide advantage and save the cost to buy the physical resources that may be vacant.

II. ARCHITECTURAL COMPONENTS

Cloud Computing Architecture is commonly divided into three layers SaaS, PaaS, and IaaS. It's helpful to add more structure to the service model stacks: Fig. 1 shows a cloud reference architecture [3] that makes the most important security-relevant cloud components explicit and provides an abstract overview of cloud computing for security issue analysis.

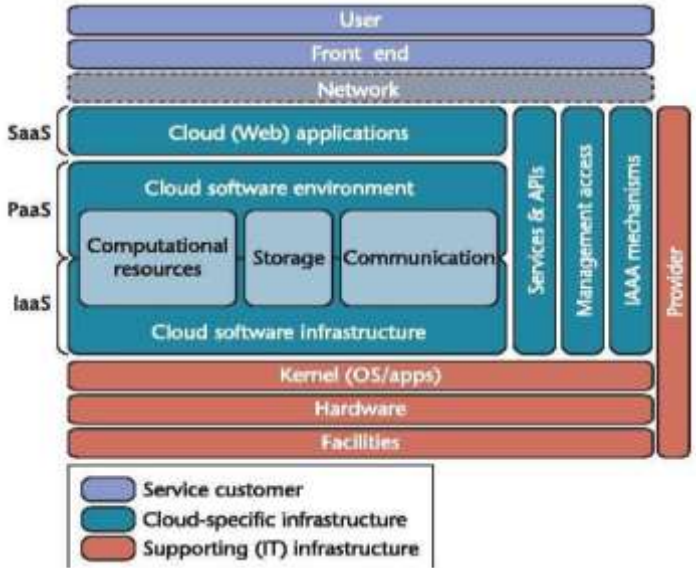

Fig. 1. The cloud reference architecture.

2.1. Software as a Service (SaaS)

Software as a Service (**SaaS**) is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet [6]. It is the easiest way to cloud compute. The applications in a hosting environment are released by cloud consumers, which can be accessed through networks from various clients. In SaaS cloud the cloud consumers do not have control over the cloud infrastructure, so different cloud consumers' applications are organised in a single logical environment. Examples of SaaS include SalesForce.com, Google Mail, Google Docs, and so forth [3].

2.2. Platform as a Service (PaaS)

Platform as a service (**PaaS**) is a development platform which allows cloud consumers to develop cloud services and applications (e.g. SaaS) directly on the PaaS cloud. It supports the full "Software Lifecycle". Hence, the major difference between SaaS and PaaS is that SaaS only hosts completed cloud applications whereas PaaS offers a development platform that hosts Cloud Computing [3].PaaS ensures that the cloud vendor provides not only the virtualization layer but also manage it. It allows users to create and maintain their own applications. The applications can be provided publically or privately. An example of PaaS is Google App Engine. Fig 2 clearly describes PaaS.

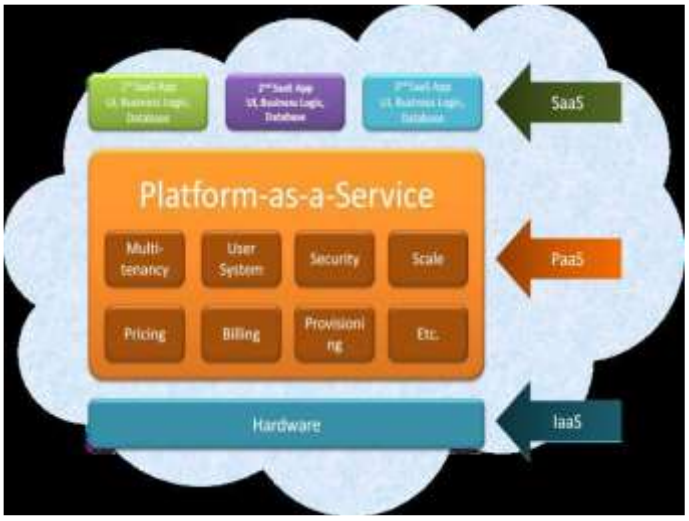

Fig 2. Platform-as-a-service (PaaS)

2.3. Infrastructure as a Service (IaaS)

In the Infrastructure as a Service (**IaaS**), cloud consumers directly use IT infrastructures. Virtualization is extensively used in IaaS cloud in order to integrate or decompose physical resources in order to meet growing or shrinking resource demand from cloud consumers [3]. The concept of virtualization allows many users to share a single physical server. The basic strategy of virtualization is to set up independent virtual machines (VM) that are isolated from both the underlying hardware and other VMs. An example of IaaS is Amazon's EC2.

III. CLOUD COMPUTNG MODELS

The major cloud computing models are explained and are depicted in Fig 3.

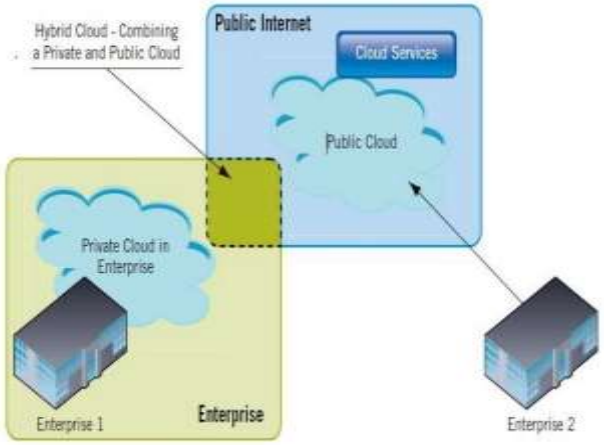

Fig 3. Cloud Computing Models

3.1. Public cloud

In a public cloud, a service provider makes resources like applications and storage which in turn is available publically over the Internet. A public cloud is based on the standard cloud computing model. Public cloud services may be free or offered on a pay-per-usage model [2]. The main benefits of using a public cloud service are:

1. Easy and inexpensive set-up because hardware, application and bandwidth costs are covered by the provider. Scalability to meet needs.
2. Resources are not wasted because you pay for what you use.
3. The term "public cloud" arose to differentiate between the standard model and the private cloud and it uses cloud computing technologies such as virtualization.

Examples of public clouds include Amazon Elastic Compute Cloud (EC2), IBM's Blue Cloud, Sun Cloud, Google App Engine and Windows Azure Services Platform.

3.2. Community cloud

A community cloud may be established where several organizations have similar requirements and seek to share infrastructure so as to realize some of the benefits of cloud computing.

3.3. Hybrid cloud

A hybrid cloud is a Cloud Computing environment in which an organization provides and manages some resources in-house and has others provided externally. For example, an organization might use a public cloud service, such as Amazon Simple Storage Service (Amazon S3) for archived data but continue to maintain in-house storage for operational customer data [3]. Ideally, the hybrid approach

not only ensures scalability but also cost-effectiveness that a public cloud computing environment offers without exposing data to third-party vulnerabilities.

3.4. Private cloud

Private cloud is also termed as internal cloud or corporate cloud. It is a term coined for a computing architecture which provides hosted services to a limited number of people. Corporate network and datacenter administrators to effectively become service providers due to the advances in virtualization and distributed computing that in turn has allowed them to meet the needs of their "customers" within the corporation. "Private cloud" appeals an organization that needs control over their data such as Amazon's Elastic Compute Cloud (EC2) or Simple Storage Service (S3).

IV. CHALLENGES

The following are some of the notable challenges associated with cloud computing, and although some of these may cause a slowdown when delivering more services in the cloud, most also can provide opportunities, if resolved with due care and attention in the planning stages [1].

4.1. Security and privacy

Security and Privacy are perhaps two of the more important issues surrounding cloud computing that relate to storing and securing data. They are generally regarded to slow the deployment of cloud services. These challenges can be addressed, for example, by storing the information internal to the organization, but allowing it to be used in the cloud. For handling such challenges the security mechanisms between the organization and the cloud need to be robust.

4.2. Lack of standards

Clouds have documented interfaces. But there are no standards associated with these as a result of which it is unlikely that most clouds will be interoperable. The Open Grid Forum is developing an Open Cloud Computing Interface to resolve this issue and the Open Cloud Consortium is working on cloud computing standards and practices [2]. So it is essential that the findings of these groups need to mature, but it is not known whether they will address the needs of the people deploying the services and the specific interfaces these services need. However, keeping up to date on the latest standards as they evolve will allow them to be leveraged, if applicable.

4.3. Continuously evolving

The user requirement is continuously evolving along with the requirements for interfaces, networking, and storage. This implies that the cloud continuously evolves and thus not remain static.

4.4. Compliance concerns

Data Protection directives in the EU (Europe) are just two among many compliance issues affecting cloud computing, based on the type of data and application for which the cloud is being used. The EU has a legislative backing for data protection across all member states, but in the US data protection is different and can vary from state to state. These typically result in Hybrid cloud deployment with one cloud storing the data internal to the organization [2].

V. SECURITY ISSUES

Cloud computing security is an evolving sub-domain of computer security, network security, and 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 [2]. There are a number of security issues/concerns associated with cloud computing but these issues fall into two broad categories: security issues faced by cloud providers and security issues faced by their customers. The benefactor must however ensure that their infrastructure is secure and that their client

data and applications are threatened while the user must take measures to strengthen their application and use robust passwords and authentication actions.

When an association selects to store data or host applications on the public cloud, it drops its ability to have physical access to the servers hosting its data. As a result, potentially business sensitive and confidential data is at risk from insider attacks and the insider attacks are the third biggest threat in cloud computing. Therefore, Cloud Service providers must ensure that thorough background checks are conducted for employees who have physical access to the servers in the data center.

Additionally, data centers must be frequently monitored for suspicious activity. In order to conserve resources, cut costs, and maintain efficiency, Cloud Service Providers often store more than one customer's data on the same server. As a result, there is a chance that one user's private data can be viewed by other users. To handle such sensitive situations, cloud service providers should ensure proper data isolation and logical storage segregation.

5.1. Security and privacy

5.1.1. Identity management

Every enterprise will have its own identity management system to control access to information and computing resources [4]. Cloud providers either assimilate the customer's identity management system into their own infrastructure, using alliance, or a biometric-based identification system, or provide an identity management solution of their own. Cloud ID, for instance, provides a privacy-preserving cloud-based and cross-enterprise biometric identification solutions for this problem

5.1.2. Physical security

Cloud service providers physically secure the IT hardware (servers, routers, cables etc.) against unauthorized access, interference, theft, fires, floods etc. and ensure that essential supplies (such as electricity) are sufficiently robust to minimize the possibility of disruption.

5.1.3. Personnel security

Various information security concerns relating to the IT and other professionals associated with cloud services are typically handled through pre-, para- and post-employment activities such as security screening potential recruits, security awareness and training programs, proactive security monitoring and supervision, disciplinary procedures and contractual obligations embedded in employment contracts, service level agreements, codes of conduct, policies etc.

5.1.4. Availability

Cloud providers help ensure that customers can rely on access to their data and applications, at least in part (failures at any point - not just within the cloud service providers' domains - may disrupt the communications chains between users and applications).

5.1.5. Application security

Cloud providers ensure that applications available as a service via the cloud (SaaS) are secure by specifying, designing, implementing, testing and maintaining appropriate application security measures in the production environment.

5.1.6. Privacy

Providers ensure that all critical data (credit card numbers, for example) are masked or encrypted and that only authorized users have access to data in its entirety. Moreover, digital identities and credentials must be protected as should any data that the provider collects or produces about customer activity in the cloud.

5.2. Cloud Security Control [4]

These controls are put in place to safeguard any weaknesses in the system and reduce the effect of an attack. While there are many types of controls behind a cloud security architecture, they can usually be found in one of the following categories.

5.2.1. Deterrent controls

These controls are intended to reduce attacks on a cloud system. Some consider them a subset of preventive controls.

5.2.2. Preventive controls

Preventive controls strengthen the system against incidents, generally by reducing if not actually eliminating vulnerabilities. Strong authentication of cloud users, for instance, makes it less likely that unauthorized users can access cloud systems, and more likely that cloud users are positively identified.

5.2.3. Detective controls

Detective controls are intended to detect and react appropriately to any incidents that occur. In the event of an attack, a detective control will signal the preventative or corrective controls to address the issue.

5.2.4. Corrective controls

Corrective controls reduce the consequences of an incident, normally by limiting the damage. They come into effect during or after an incident. Restoring system backups in order to rebuild a compromised system is an example of a corrective control.

5.3. Effective Encryption

5.3.1. Attribute-Based Encryption Algorithm

a) Cipher text -policy ABE (CP-ABE)

In the CP-ABE, the encrypt or controls access strategy, as the strategy gets more complex, the design of system public key becomes more complex, and the security of the system is proved to be more difficult

b) Key-policy ABE (KP-ABE)

In the KP-ABE, attribute sets are used to explain the encrypted texts and the private keys with the specified encrypted texts that users will have the left to decrypt.

5.3.2. Fully homomorphic encryption (FHE)

Fully Homomorphic encryption allows straightforward computations on encrypted information, and also allows computing sum and product for the encrypted data without decryption.

VI. SECURITY APPROACHES

6.1. Authentication and Identity Management

User-centric Identity Management (IDM) handles private and critical identity attributes. In this approach, identifiers or attributes help identify and define a user [7]. It lets users control their digital identities. Users must be able to export their digital identities and securely transfer them to various computers as they can access the cloud from various places such as home, office, school, or other public places.

6.2. Secure-Service Provisioning and Composition

To optimize resource utilization, cloud service providers often use virtualization technologies that separate application services from infrastructure. To provide newly composed services to customers it is essential to provide automatic service provisioning that allow cloud service providers and service integrators to describe services with unified standards. The challenges of such collaboration

systems include dynamic access control to resources shared by agents and controlling collaborative actions that are geared towards a collaboration goal.

6.3. Secure Interoperation

Researchers have addressed secure interoperation and policy engineering mechanisms to integrate access policies of different domains. A dynamic environment makes the conventional centralized approaches inappropriate and demands decentralized approaches as the domains are ephemeral and might need to interact for a specific purpose. Security Assertion Markup Language (SAML), Extensible Access Control Markup Language (XACML), and Web services standards are viable solutions toward this [7].

REFERENCES

1. Thomas Erl ,Cloud Computing: Concepts, Technology & Architecture , May 2013
2. John Rhoton ,Cloud Computing Protected: Security Assessment Handbook , January 2013.
3. Michael J. Kavis ,Architecting the Cloud: Design Decisions for Cloud Computing Service Model , January 2014
4. Prasanta Pattnaik (Author), Manas Kabat (Author), Souvik Pal (Author), Fundamentals of Cloud Computing
5. http://searchcloudcomputing.techtarget.com/definition/Software-as-a-Service
6. http://csis.pace.edu/~marchese/SE765/Paper/security2.pdf

