PEZZOTTAITE JOURNALS

Volume 7, Number 4, October – December' 2018
ISSN (Print): 2319-9059, (Online): 2319-9067
SJIF (2016): 7.194, SJIF (2017): 7.306
H5-Index: 1, H5-Median: 1, H-Citations: 1

CLOUDE PROTECTION INTIMIDATION ANALYSIS

Dr. R. S. Mishra[1]

ABSTRACT

Cloud computing is current buzzword in the market. The popularity of clouds has driven privacy laws and data residency restrictions around the world. Cloud computing promises to serve enterprise-computing needs while providing cost savings, particularly in the area of capital H/W, data centers managements and software development.

Confidentiality, integrity, availability, authenticity and privacy are essential concerns for both cloud providers and consumers. This paper identifies threats and attacks related to the IaaS layer (Infrastructure as a service) and types of attacks and elaborated study of IaaS components security.

KEYWORDS

Cloude Protection Intimidation, Infrastructure as Services, Threats and Attacks on Cloud Security etc.

INTRODUCTION

Cloud computing involves delivering hosted services over the Internet on demand. These services include software applications, software services, network resources, platforms, computing infrastructures and virtual servers. Cloud computing is scalable and managed infrastructure. End- users simply consume these services and pay on usage basis or subscription basis. There are three famous service models of cloud computing as described below:

Software as a Service (SaaS). In this model, software application is hosted as service and end-users use the application on the web browser. SaaS applications are designed for end- users, delivered over the web.

Platform as a Service (PaaS): In this model, end-user creates, test and upload applications using tools and libraries hosted by the service provider. PaaS is the set of tools and services designed to make coding and deploying those applications quick and efficient.

Infrastructure as a Service (IaaS): This model involves hosting of hardware computing services like storage, hard-drive, servers and network components. Service provider is responsible for maintenance and managing all these resources. IaaS is the hardware and software that powers it all – servers, storage, networks, operating systems

The term "cloud" was coined from the computer network diagrams, which use it to hide the complexity of infrastructure involved.

Cloud computing provides software, platform and infrastructure as a service. Its main features include resource pooling, rapid elasticity, measured service, on-demand self-service and broad network access. Therefore, a cloud is a collection of hardware and software that runs in a data center and enables the cloud-computing model. A cloud reduces capital investment, hardware cost and software license cost.

Cloud computing also raises severe challenges especially regarding the security level required for the secure use of services provided by it. There are no publically available standards specific to cloud computing security. Therefore, in this paper, we propose the following standards for maintaining security in an unsafe cloud-computing environment.

Main characteristics include:

On-demand Self-Service. The ability for an end user to sign up and receive • services without the long delays that have characterized traditional IT.

Broad Network Access. Ability to access the service via standard platforms • (desktop, laptop, mobile etc).

Resource Pooling. Resources are pooled across multiple customers.

Rapid Elasticity. Capability can scale to cope with demand peaks.

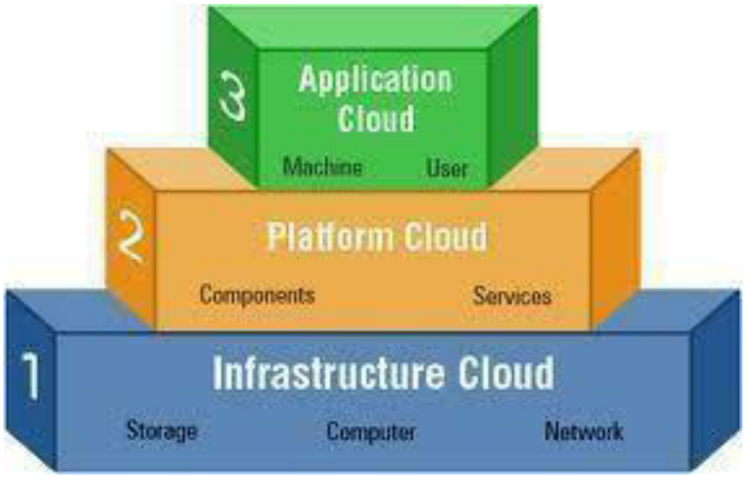
[1] Assistant Professor, Office Management & Company Secretaryship, Banaras Hindu University, Uttar Pradesh, India, ratanbhugmail.com

Measured Service. Billing is metered and delivered as a utility service.

The diagram below depicts the Cloud Computing stack - it shows three distinct categories within Cloud Computing:

I. Software as a Service,
II. Platform as a Service and
III. Infrastructure as a Service.

Figure-1



Sources: Authors Compilation

Characteristics of SaaS

Web access to commercial software.
Software is managed from a central location.
Software delivered in a "one to many" model.
Users not required handling software upgrades and patches.
Application Programming Interfaces (APIs) allow for integration between different pieces of software.

Characteristics of PaaS

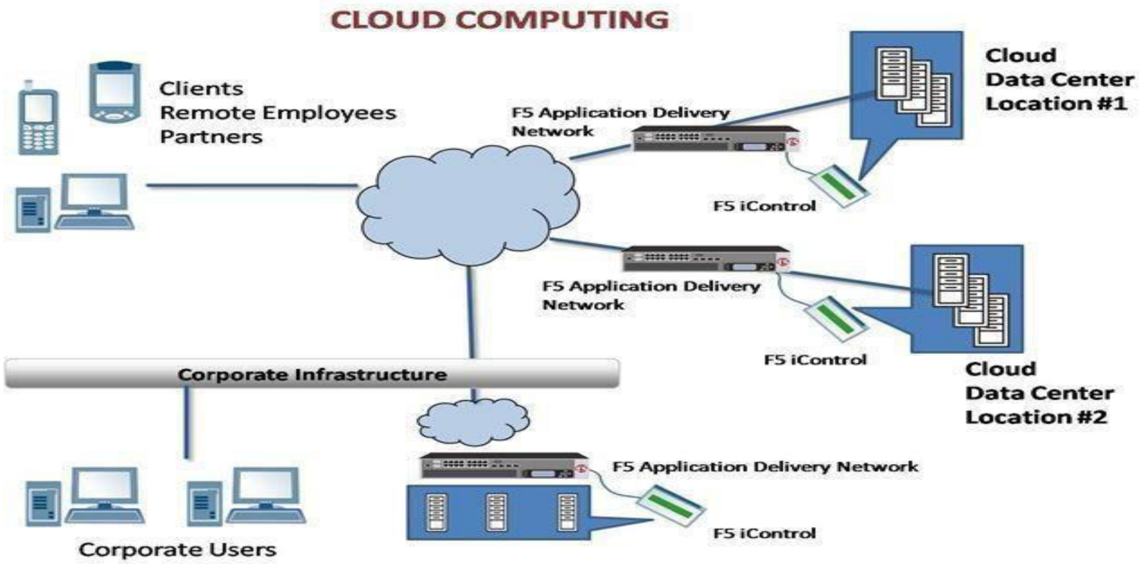
Services to develop, test, deploy, host and maintain applications in the same integrated development environment. All the varying services needed to fulfill the application development process
Web based user interface creation tools help to create, modify, test and deploy different UI scenarios.
Multi-tenant architecture where multiple concurrent users utilize the same development application.
Built in scalability of deployed software including load balancing and failover.
Integration with web services and databases via common standards.
Support for development team collaboration – some PaaS solutions include project planning and communication tools
Tools to handle billing and subscription management.

Characteristics of IaaS

Resources are distributed as a service.
Allows for dynamic scaling.
Has a variable cost, utility pricing model.
Generally includes multiple users on a single piece of hardware.
Desktop virtualization
Policy based services
Internet connectivity
Automation of administrative tasks.

CLOUD COMPUTING ARCHITECTURE

Figure-2


CLOUD COMPUTING
Clients
Remote Employees
Partners
F5 Application Delivery Network
F5 iControl
Cloud Data Center Location #1
F5 Application Delivery Network
F5 iControl
Cloud Data Center Location #2
Corporate Infrastructure
F5 Application Delivery Network
F5 iControl
Corporate Users

Sources: Authors Compilation

VARIOUS TYPES OF CLOUDS

Clouds are broadly classified as:

Personal Clouds: Such clouds are especially operated by single organization.

General Clouds: These clouds are used for providing services to common people.

Domain-Specific Clouds: These clouds are maintained for specific requirements by a group of organizations.

Mixed Clouds: These clouds are mixtures of above said three clouds, which can share data to achieve, fulfill a specific requirement.

CURRENT SECURITY PROBLEM AND SOLUTION

The main problems cloud computing faces are preserving confidentiality and integrity of data in aiding data security. The primary solution for these problems is encryption of data stored in the cloud. However, encryption of data also brings up new problems. Here is an overview of some of the main problems faced by cloud systems and some solutions.

Trust

Trust between the Service provider and the customer is one of the main issues cloud computing faces today. There is no way for the customer to be sure, whether the management of the Service is trustworthy, and whether there is any risk of insider attacks. This is a major issue and has received strong attention by companies.

The only legal document between the customer and service provider is the Service Level Agreement (SLA). This document contains all the agreements between the customer and the service provider; it contains what the service provider is doing and is willing to do (Weis & Alves-Foss, 2011). However, there is currently no clear format for the SLA, and as such, there may be services not documented in the SLA that the customer may be unaware that it will need these services at some later time.

Legal Issues

There are several regulatory requirements, privacy laws and data security laws that cloud systems need to adhere to. One of the major problems with adhering to the laws is that laws vary from country to country, and users have no control over where their data is physically located.

Confidentiality

Confidentiality is preventing the improper disclosure of information. Preserving confidentiality is one of the major issues faced by cloud systems since the information is stored at a remote location that the Service Provider has full access. Therefore, there has been some method of preserving the confidentiality of data stored in the cloud. The main method used to preserve data confidentiality is data encryption; however, encryption brings about its own issues, some of which are discussed later.

Authenticity (Integrity and Completeness)

Integrity is preventing the improper modification of information. Preserving Integrity, as if confidentiality is another major issue faced by cloud systems that needs to be handled, and is mainly done by the use of data encryption.

In a common database setup, there would be many users with varying amount of rights. A user with a limited set of rights might need to access a subset of data, and might also want to verify that the delivered results are valid and complete (that is, not poisoned, altered or missing anything) (Weis & Alves-Foss, 2011).

A common approach to such a problem is to use digital signatures; however, the problem with digital signatures is that not all users have access to the data superset, therefore they cannot verify any subset of the data even if they're provided with the digital signature of the superset; and too many possible subsets of data exist to create digital signatures for each.

Recently, researchers have tried to find solutions to this problem. The primary proposal is to provide customers with the superset's signature and some metadata along with the query results. This metadata (called verification objects) lets customers fill in the blanks of the data, which they don't have access to, and be able to validate the signature. There are two primary variations of this idea, one based on Merkle trees and the other based on signature aggregation (Weis & Alves- Foss, 2011).

Encryption

The main method used for ensuring data security in the cloud is by encryption. Encryption seems like the perfect solution for ensuring data security; however, it is not without its drawbacks. Encryption takes considerably more computational power, and this is multiplied by several factors in the case of databases (Weis & Alves-Foss, 2011).

Cryptography greatly affects database performance because each time a query is run, a large amount of data must be decrypted; and since the main operation on a database is running queries, the amount of decryption operations quickly become excessive. There are several approaches developed to handle data encryption; each having its own compromises and downsides, some provide better security mechanisms, and some focus on facilitating more operations to the customers. Some of these methods are mentioned below:

Early Approaches

Early approaches have used extensions to the query language that simply applied encryption before writing to the database and apply decryption before reading from the database.

Querying Encrypted Data

There are several methods that were proposed to handle Querying of Encrypted Data, one such method was proposed by Purushothama B.R. and B.B. Amberker in (Purushothama & Amberker, 2013).

In the proposed scheme, several cryptographic methods were used to encrypt the data in each cell of each table to be stored in the cloud. When a user needs to query this data, the query parameters are encrypted and checked against the stored data. No data decryption is done in the cloud, thus protecting the Authenticity and integrity of the information. When the results of the query is returned (in encrypted form) to the user, the user then decrypts the data and uses it.

This scheme also has significant improvements for select queries over previous related schemes.

Key Management

Since encryption is the main method used to ensure data security, naturally we would be faced with the problem of key management. The encryption keys cannot be stored on the cloud, therefore the customer must manage and control a key management system for any cryptographic method used (Weis & Alves-Foss, 2011). For simple encryption schemas such as the “Early Approaches” described above, there might not be a problem since a single encryption and decryption key can be used for the entire system. However, almost any real database requires a more complex system (Weis & Alves-Foss, 2011). This simple system to manage keys might even have to take the form of a small database, which would have to be a secure local database; which again, may defeat the purpose of moving the original database to the cloud.

Clearly, Key Management is a real problem for cloud systems using encryption, and recent research has been done on using two-level encryption, which allows the Key Management system to be stored in the cloud. This scheme is efficient, and may be the solution to the Key Management problems cloud systems faces; however, it has not yet been applied specifically to database encryption.

Data Splitting

Some methods have been developed that serve as alternatives to encryption. These methods are generally faster than encryption but have their own drawbacks.

Divyakant Agrawal and his colleagues initially developed data splitting. The idea is to split the data over multiple hosts that cannot communicate with each other; only the owner who can access both hosts can collect and combine the separate datasets to recreate the original. This method is extremely fast compared to encryption but it requires at least two separate, but homogeneous service providers.

Multi-clouds Database Model (MCDB)
(AlZain, Soh, & Pardede, 2012)

This is a method of Data Splitting, which uses multiple clouds and several other techniques to ensure data is split in across clouds in a manner that preserves the data Confidentiality, Integrity and ensures Availability.

MCDB provides cloud with database storage in multi-clouds. MCDB model does not preserve security in a single cloud; rather security and privacy of data will be preserved by applying multi- shares technique on multi-clouds. By doing so, it avoids the negative effects of single cloud, reduces the security risks from malicious insiders in cloud computing environment and reduces the negative impact of encryption techniques (AlZain, Soh, & Pardede, 2012).

MCDB preserves security and privacy of user’s data by replicating data among several clouds, using a secret sharing approach that uses Shamir’s secret sharing algorithm, and using a triple modular redundancy (TMR) technique with the sequential method. It deals with the cloud manager to manage and control operations between the clients and the multi-clouds inside super cloud service provider (AlZain, Soh, & Pardede, 2012).

Multi-Tenancy

Cloud systems share computational resources, storage, services between multiple customer applications (tenants) in order to achieve efficient utilization of resources while decreasing cost, this is referred to as multi-tenancy. However, this sharing of resources violates the confidentiality of tenants’ IT Assets. This implies that unless there is a degree of isolation between these tenants, it is very difficult to keep an eye on the data flowing between different realms which make the multi-tenancy model insecure for adoption (Behl & Behl, 2012). Some multi-tenancy issues are:

Virtual Machine Attacks

Typically, in a cloud, business data and applications are stored and ran within virtual machines. These virtual machines are usually running on a server with other virtual machines, some of which can be malicious. Research has shown that attacks against, with and between virtual machines are possible.

If one of the virtual machines on a server hosts a malicious application that breaches legal or operational barriers; this may lead legal authorities, the service provider or other authorities to shutting down and blocking access the entire server. This would greatly affect the users of the other Virtual Machines on the server.

Shared Resources

Assuming the cloud system is not running on a virtual machine, the hardware is now an issue. Research has shown that it is possible for information to flow between processor cores, meaning that an application running on one core of a processor can get access to information of another application running on another core. Applications can also pass data between cores.

Multicore processors often have complex and large caches. With these hardware resources, if data is decrypted in the cloud, if even for a moment for comparison, it would then exist unencrypted in the memory of some one of the cloud machines. The problem is that we do not know what other application is running on these machines. Other malicious cloud users or the service provider can me monitoring the machine memory and be able to read our data. However, the likelihood of these hardware attacks is very small (Weis & Alves-Foss, 2011).

If one of the applications on a server hosts is malicious, this may lead to the service provider or some other authority shutting down and blocking access the entire server in order to investigate and determine the malicious application. This would greatly affect the users of the other applications on the server.

CONCLUSION

Security concerns are an active area of research and experimentation. Lots of research is going on to address the issues like network security, data protection, virtualization and isolation of resources. Addressing these issues requires getting confidence from user for cloud applications and services. Obtaining user confidence can be achieved by creating trust for cloud resource and applications, which is a crucial issue in cloud computing.

Trust management is attracting much attention. Providing secure access to cloud by trusted cloud computing and by using service level agreements, made between the cloud provider and user; requires lots of trust and reputation management. We will be focusing on the analysis of solution in the cloud-computing environment. Also lots of our survey based in the field of trust and trust management. In this article we gave a telling overview of security threats of cloud computing. We have also provided the reader with some effective countermeasures, besides introducing main elements of security in cloud computing.

Cloud computing offers real benefits to companies seeking a competitive edge in today's economy. Many more providers are moving into this area, and the competition is driving prices even lower. Attractive pricing, the ability to free up staff for other duties, and the ability to pay for "as needed" services will continue to drive more businesses to consider cloud computing.

The decision to move to cloud-based services should fit into the organization's overall corporate objectives. Before any services are moved to the cloud, the organization's senior management should ensure such actions are consistent with their strategic plans and meet acceptance criteria that address the ten items discussed in this article. Just as there are advantages to cloud computing, there are also several key security issues to keep in mind. One such concern is that cloud computing blurs the natural perimeter between the protected inside the hostile outside. Security of any cloud-based services must be closely reviewed to understand what protections your information has. There is also the issue of availability. This availability could be jeopardized by a denial of service or by the service provider suffering a failure or going out of business.

REFERENCES

Behl, A., and Behl, K. (2012). An Analysis of Cloud Computing Security Issues. *IEEE*, 109-114.

Wikimedia. (2013, January 16). *Data as a Service*. Retrieved from Wikipedia: http://en.wikipedia.org/wiki/DaaS

Tripathi, A., and Mishra, A. (2011). *Cloud Computing Security Considerations", Signal Processing, Communications and Computing (ICSPCC)*, IEEE International Conference.

(2011). Understanding the Cloud Computing Stack SaaS, Paas, IaaS, © Diversity Limited.

Kumar, K. G., and Chaudhari, Minubahi. (2012). *To Achieve Trust in the Cloud.* In 2nd International Conference on Advanced Computing & Communication Technologies.

Purushothama. B., & Amberker, B. (2013). *Efficient Query Processing on Outsourced Encrypted Data in Cloud with Privacy Preservation.*

*****