ISSUES OF CLOUD SECURITY AND ITS IMPLICATIONS

Sandeep.B[1], Sachin Hebbar[2], Deepak.N.K[3], Manjunatha Hegde.Y.A[4]

[1]*Student, Computer Science and Engineering, Bangalore Institute of Technology, Karnataka, India*
[2]*Student, Computer Science and Engineering, Bangalore Institute of Technology, Karnataka, India*
[3]*Student, Computer Science and Engineering, Bangalore Institute of Technology, Karnataka, India*
[4]*Student, Computer Science and Engineering, Bangalore Institute of Technology, Karnataka, India*

Abstract

Cloud computing provides an effective computing model for institutions to access information technology and related functions with minimal investment and makes use of the resources to the maximum extent. The reduced complexity and cost of Cloud computing has attributed to it's popularity and success. The users of this phenomenon range from an individual customer to huge organizations. Though there has been major advances in cloud computing, the security concerns surrounding it cannot be ignored and remedial measures has to be taken to ensure the confidentiality and the integrity of data stored in the cloud. Hence, it is inevitable to obtain a thorough understanding of the risks and threats involved in cloud computing along with the possible remedies before it is implemented by any stake holder. In this paper the authors have provided a comprehensive understanding of the issues in cloud security, it's implications and the various remedial measures to address the same. A critical observation of the security of cloud is undertaken from the perspective of the cloud architecture, cloud stakeholder and cloud characteristics. The prime security issues that have been scrutinized in this paper include the security with respect to cloud carrier, malware injection problem, accountability problems in cloud, challenges in cloud integrity, securing data transmission in cloud, elasticity, cloud multi-tenancy, service level agreement and compromise on the integrity of the information in cloud. The possible counter measures to these issues have also been highlighted in this paper. There are number of unresolved issues that need to be dealt with respect to security and privacy in a cloud computing environment. This paper aims to elaborate and analyze the numerous threats faced and also provide solutions for most of the mentioned problems.

Key Words: *Cloud computing, Security, Privacy, Trust, Confidentiality, Integrity, Accountability, Availability, Elasticity.*

1. INTRODUCTION

Cloud computing provides a whole new dimension in distributed computing environment for stake holders to access information technology with reduced total cost of ownership. A model for delivering information, here resources are extracted from the Internet through tools rather than a server connection. It is a type of computing that relies on computing resources other than using personal mobile applications or devices. The cloud computing model has a number of issues such as:

1. Cloud security
2. Loss of control over data
3. Dependent on cloud service provider
4. Programmatic security data issues.

1.1 Cloud Architecture

A. IaaS (Infrastructure-as-a-Service): The infrastructure-as-a-service (IaaS) layer provides on-demand virtual infrastructures to third parties using physical resources such as memory, storage, and processors.

B. PaaS (Platform-as-a-Service): PaaS is a tool used for developing websites and can be executed without any administrative expertise.

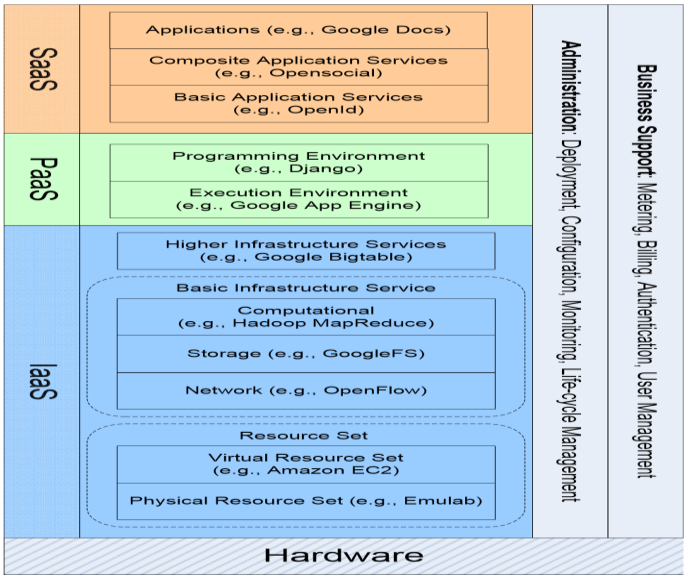

SaaS
Applications (e.g., Google Docs)
Composite Application Services (e.g., Opensocial)
Basic Application Services (e.g., OpenId)
PaaS
Programming Environment (e.g., Django)
Execution Environment (e.g., Google App Engine)
IaaS
Higher Infrastructure Services (e.g., Google Bigtable)
Basic Infrastructure Service
Computational (e.g., Hadoop MapReduce)
Storage (e.g., GoogleFS)
Network (e.g., OpenFlow)
Resource Set
Virtual Resource Set (e.g., Amazon EC2)
Physical Resource Set (e.g., Emulab)
Hardware
Administration: Deployment, Configuration, Monitoring, Life-cycle Management
Business Support: Metering, Billing, Authentication, User Management

Fig -1: Architecture of cloud computing [1]

C. SaaS (Software-as-a-Service): SaaS is run by a cloud service provider and available to the users through internet.

Fig. 1 depicts the general architecture of a cloud platform It is usually supported by modern data centers and offers services and various forms from the bottom layer to top layer. In this platform each layer represents one service model. Infrastructure-as-a-Service (IaaS) is offered in the bottom layer, where resources are aggregated and managed physically or virtually and services are delivered in forms of storage. . The middle layer delivers Platform-as a-Service (PaaS), in which services are provided as an environment for programming the top layer being software as-a- service in which services are offered by a vendor and user can avail it over the internet

1.2 Types of Cloud Computing [2]

A. Public Cloud: A Public cloud is a set of computers based on the main cloud model. Here a service provider provides a set of resources for general public for their usage on the internet. They may be pay-per use or for free.

B. Private Cloud: A Private cloud is implemented within a corporate firewall and under the control of the IT department of the organization.

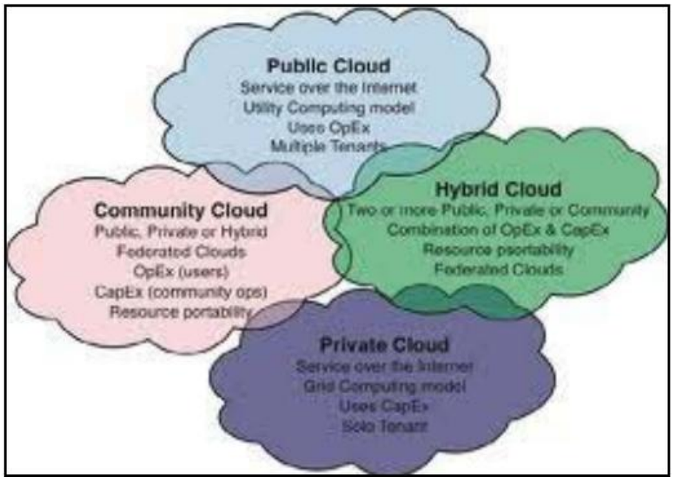


Fig -2: Types of Cloud Computing

C. Community Cloud: This cloud is a mixture of one or more public, private or hybrid clouds, and is shared by many organizations to ensure security of data .It is managed by a third party. The price of a community cloud is lesser than a public cloud but greater than private cloud.

D. Hybrid Cloud: It is a combination of public, private and community clouds .Hence it serves as a breeding ground for internal or external suppliers of cloud services and is used by most of the organizations.

2. ISSUES IN CLOUD SECURITY

Security is a primary concern of cloud computing as the cloud gives access to data but does not ensure the integrity of data. cloud computing offers amazing benefits in communication such as a number of applications, high processing speed and unlimited storage , but the compromise on the integrity and confidentiality of the data stored on cloud is an important shortcoming of cloud computing and can’t be ignored.

2.1 Cloud Carrier Security

Normally the cloud users do not have control over the cloud carrier which is present between the cloud user and cloud provider. It forms a intermediate layer between the two .The data being transferred between these two is seldom safe as its security depends on availability of a secure carrier. Other than the firewall of present there is no other mechanism to protect the transfer of data .This results in the compromising of the integrity and security of the network. This results in breach of the uses privacy and leaves the user dissatisfied. To overcome this a service level agreement (SLA) can be agreed between the cloud provider and cloud user.

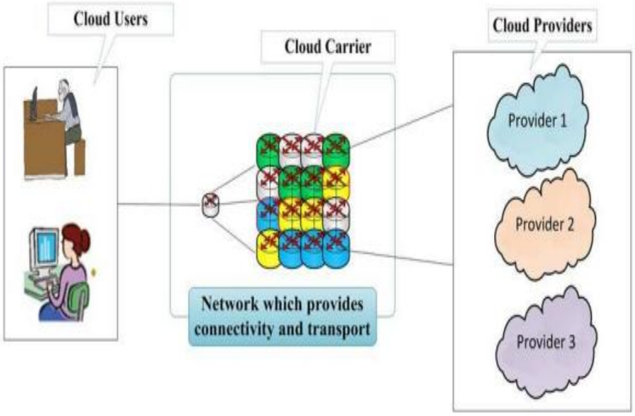


Fig -3: Cloud Carrier

2.2 Malware Injection Problem

The main idea of this problem is to create a new copy of the state instance of the user and allow the services of the user to run in this malicious instance. Using any of the attacks like Denial-Of-Service the hacker gains access of the victim's data in the cloud. Here a new malicious adversary of the SaaS or PaaS or IaaS is created and introduced into the cloud. Now this is used to trick the cloud that the malicious instance is a valid instance of the cloud state If the hacker succeeds in gaining access, the cloud redirects all user requests to this malicious service implementation. An appropriate counter measure would be for the cloud to perform service integrity checks before servicing any user requests.

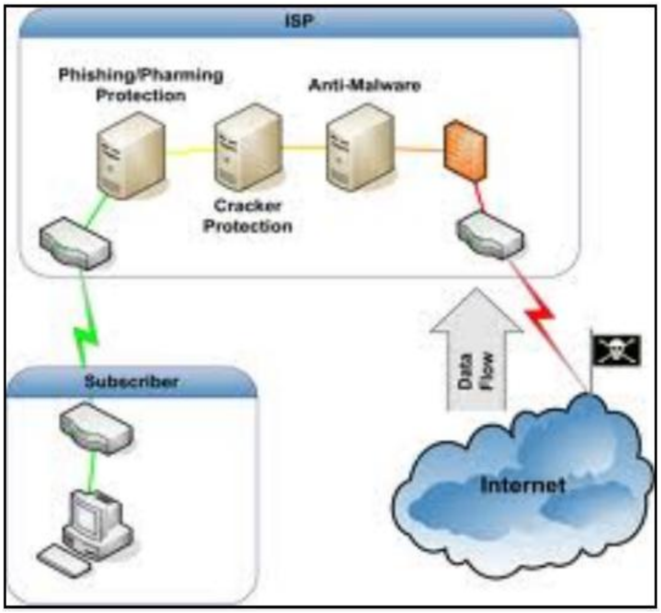


Fig -4: Malware Protection

2.3 Problems in Accountability

The method of payment in a cloud computing system is based on the user's amount of data transfer in the network and the number of CPU cycles. When an attacker successfully intrudes the cloud by running a malicious code which consumes lot of storage from the cloud, the user is charged illegitimately. This results in a dispute and hence an important challenge to the cloud security. A solution to such kind of disputes would be to place effective authentication mechanism.

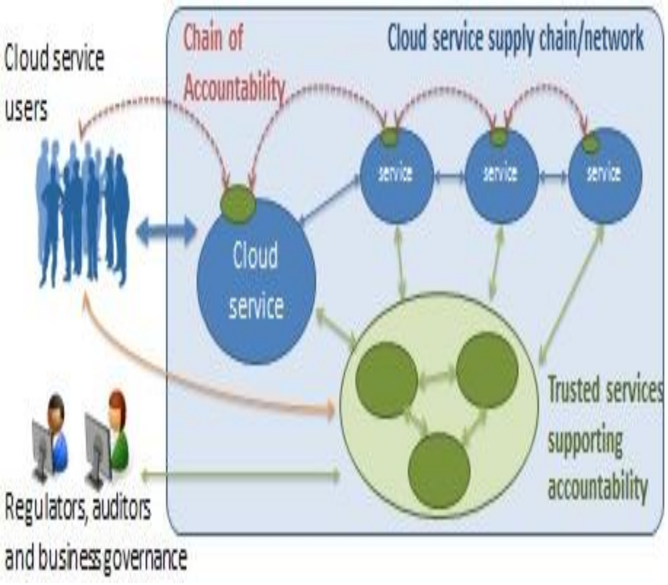

Cloud service users
Chain of Accountability
Cloud service supply chain/network
service
service
service
Cloud service
Trusted services supporting accountability
Regulators, auditors and business governance

Fig -5: Accountability in cloud

2.4 Challenges in cloud integrity

A. Data loss/manipulation: In cloud computing servers store large amounts of data and these servers may not be secure or reliable which may result in the data being attacked on purpose or lost accidentally [5]. Data loss or manipulation can also occur due to the errors on the part of the administrator during data migration and changing memberships.

B. Dishonest computation in remote servers: The computational details in cloud are not directly available to cloud customers and also the cloud server may not behave properly and not return the expected output.

2.5 Securing Data Transmission

Securing data is a main concern because the users are anxious about their data being lost on the cloud. Many encryption protocols are used. SSL(Secure Socket Layer) is the widely used protocol. Here it creates a channel between two systems connected over the internet.SSL ensures secure connection to the web server.SSL is a good experience for end users. We know that many applications use cloud. Here are a few examples of SSL being employed:

- To secure online credit card transactions.
- To secure system logins and any sensitive information exchanged online.

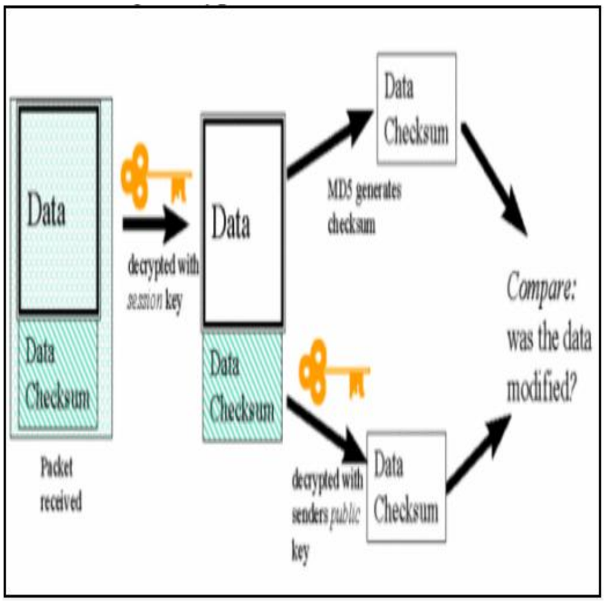


Fig-6: Encryption Technique [3]

2.6 Elasticity

This refers to the fact that the consumers can expand the network or downsize the network based on the demand. So when the users expand the network it provides a chance for other users .to join the network this results in the compromising of the integrity of the network. To remediate the above threats, resources must be placed with in the boundary of the network. There can also be a inclusion of a migration policy which to make use the resources of the other cloud providers which helps to meet the demand of the expanding network.

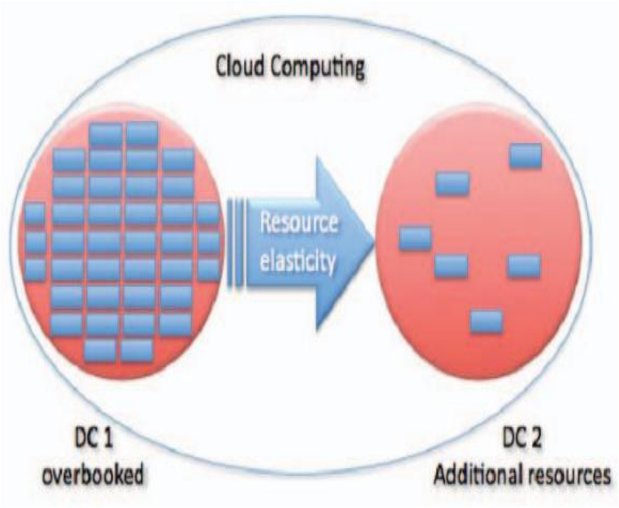
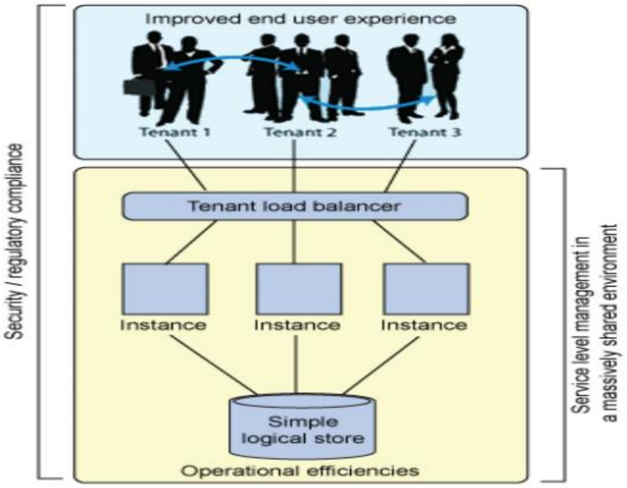


Fig-7: Cloud Resource Elasticity

2.7 Cloud Multi-tenancy

Multi tenancy is a main feature in cloud computing. Basically a single architecture caters to various users. This results in proper use of resources provided with cloud. Consumers need to use most resources which multi tenancy fulfils. But this compromises the cloud security[4]. Also using multi tenancy will lead to inflexibility. Multi tenancy is very costly to implement. This will lead to problems in budget since putting up the cloud also takes lot of budget.


Improved end user experience
Tenant 1
Tenant 2
Tenant 3
Tenant load balancer
Instance
Instance
Instance
Simple logical store
Operational efficiencies
Security / regulatory compliance
Service level management in a massively shared environment

Database recovery by tenant source: IBM

Fig-8: Cloud Multi-tenancy Model

2.8 Service Level Agreement

When a service provider ports its services to cloud, risk is taken in terms of non-availability of critical information in when needed the most due to a number of factors which range from provider's resources going offline to attacks on provider's storage. These issues should not be neglected and compromised.

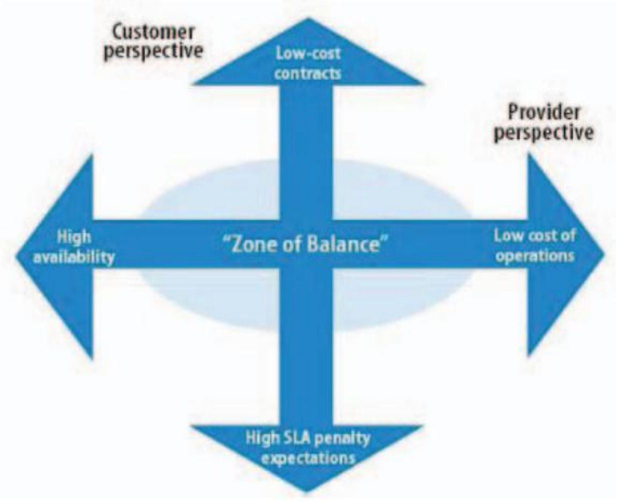


Fig-9: Cloud Service Level Agreement (SLA)

There is a two-fold remedy to this attack as described below in the following:
A. Service Level Agreement which is a trust between the cloud provider and consumer and defines the time limit for which the resources can be used by the user.
B. A back up plan to cover an outage event as well as resources for the critical information. This enables the user to avail the critical data off-hand whenever needed, even when the resources of the provider are not available. The provider also makes use of a notification system to notify the user of the imminent down time.

2.9. Information Integrity and Privacy [6]

When data is uploaded onto the cloud it is obvious that the data will be visible to hackers and invalid users alike. To avoid any loss of data a simple trust between the service provider and consumer has to be established. The provider has to make sure that the data the consumer provides should go through various stages of authorization and authentication and only then it has to be uploaded onto the cloud. RSA and SSH can be used for this purposes. The many levels of authorization make sure that only legal users gain access to "their" data. Also encryption and encryption can be used for providing integrity and privacy of information. The keys will have to be handled by the service provider. The protocols that may be used to access the user's resources like VPN, SOAP, RTC, CML and so on. Since there is no authentication and poor infrastructure of cloud the integrity is compromised hence the above methods are used.

3. CONCLUSIONS

From this paper we can conclude that cloud is a vibrant tool which has many faces and uses. But along with advantages there come disadvantages. The main concern is of security of data uploaded on the cloud. The most serious issues are illustrated in this paper. At Least integrity and confidentiality has to be maintained for the data on the cloud.

Also many newer technologies are coming up which will result in making our lives easier ,however this will result in more security challenges like achieving end-to-end security. Also providers have to make sure they are adaptive in nature to cope up with the environmental changes. Sufficient amount of API's have to be provided by the cloud to ensure security.
All types of cloud computing have threats and have to be kept in check. Remedial actions for most of the issues have been highlighted.

REFERENCES

[1]. A. Lenk, M. Klems, J. Nimis, S. Tai, and T. Sandholm, "What's inside the Cloud? An architectural map of the Cloud landscape," Software Engineering Challenges of Cloud Computing, 2009. CLOUD'09. ICSE Workshop on, 2009, pp. 23-31.
[2]. Cloud Computing- A Practical Approach by Velte Tata McGraw-Hill Edition
[3]. Meiko Jenson, Jorg Schwenk, Nils Gruschka, Luigi Lo Iacono. On Technical Security Issues in Cloud Computing. IEEE International Conference on Cloud Computing 2009.
[4]. Users Demand More From Cloud Providers.
http://meship.com/Blog/2011/01/18/users-demand-more-from-cloud-providers
[5]. G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession,"
[6]. D. Kormann and A. Rubin, ―Risks of the passport single sign on protocol, no. 1–6, pp. 51–58, 2000.
[7]. Cloud Computing Bible-by Barrie Soinsky,Wiley Publishing Inc.