Security Issues with Possible Solutions in Cloud Computing: A Review & Analysis

Dharma Raj Ojha[1] Prof. T. Srinivasa Rao[2]
[1]Student [2]Head of Department
[1,2]Department of Computer Application
[1,2]Sambhram Institute of Technology, Karnataka, India

Abstract— Cloud computing is a screen that uses an integrated concept of "software-as-a-service" and "utility processing", which provides convenient administration and demand for end users. It provides a good way to share goods and appropriate governments, which has space with many organizations. Due to the use of assets transmitted in cloud computing, it is necessary to provide security and reliability to share information to create cloud computing applications. Due to the cloud processing information and the distribution of its property on the ground, security is a major hindrance to prevent the organization of cloud situations. Strengths use the cloud to store their own information with the goal of collecting security information. There is more concern about the cloud status among the transfer of information on the cloud server. Cloud Web encourages its customers by providing virtual assets through the web. Since the distributed computing field is spread, new mechanisms have been created. This expansion in the distribution computing state extends the security challenges of cloud designers. If security is strong and stable, computing will bring the match and points in the table, which will have some credibility. Cloud providers and cloud buyers should ensure that the clouds are adequately protected from all external exposures so that the customer does not face any problem, such as harassment or theft, your important information. By optimizing approved customers, it is accessible to the cloud and affects whole cloud transit and there is a possibility to affect many consumers who share contaminated clouds. This document shows the audit of delivery of computing and cloud computing distribution of distributed computing and natural security problems. This paper is planning to show a review of computing distribution, which answers the challenges in the cloud. In addition, find out the answer to the new system or the loss of the techniques distributed by the cloud computing.
Key words: Cloud Computing, IaaS, PaaS, SaaS, Deployment Models, Service Models, Cloud Security Challenges

I. INTRODUCTION

Cloud computing is a model that enhances useful access, and management, manage, organize or configure registry properties (for example, systems, servers, archives, applications, and administrators) on demand and with minimal or cooperative collaboration Can be downloaded quickly with co-selected. Cloud is a combination of computing innovations that provide convenient and additional storage management on the Internet. Their main expectation is to provide adaptable and middle registration structures at the request of the original nature of management level.

The IT regimes distributed and distributed by various global and national organizations are creating and presenting, however, they have not considered much about reaching, preparing and collecting methods in the distributed shared state. Distribution system is well-known in the Association and academic world, because it provides versatility, compatibility and access to its customers. Similarly, cost distribution reduces the distribution of computing information distribution. The community transfers its information into the cloud, the purpose of which is to use their information for its investors. Google Apps is a matter of computing. Specifically, we are building up a safe cloud that incorporates equipment (800 Tb information stockpiling, 2400 GB memory and numerous fundamental PCs), programming (counting hadoop) and information (counting information store on mechanical plate drives, significant web). Our cloud frame will be: (a) to strengthen the effective efficiency of sensitive coded information, (b) to collect, monitor and challenge monster information measures, (c) strengthening sensitive control and (D) solid audit To strengthen This document describes our way of managing cloud anchors.

They provide three adjacent states or situations in which there are specific concerns within the configuration of distributed computing operations:

Broadcast of personal touch information on the cloud server, transmit information to client computers from the cloud server and Client's home on the client's ability to have information, such as remote servers that do not have users.

Cloud computing design incorporates several parts of the cloud, which interact with each other through different directions about different information that helps the client gain their essential information.

For the cloud, it is more committed to front and back. Front-end information is the user for which backend creates a separate data storage gadget, cloud. However, Cloud offers different functions and advantages, but there are some problems with safe access and information capabilities. Some problems are identified with cloud protection: vendor security, multiple assets, decrease in control, hindering profit, misfortune of information etc. They are part of exploration issues in distribution computing.In this document we will examine the security issues identified with the computing model distributed. The main purpose of examining various types of attacks and procedures is to present a cloud display.

II. TYPES OF CLOUD COMPUTING

1) Service module
2) Development module

A. Cloud Computing Services Module

1) SaaS – Software as a Service

This administration or unit allows each product to be used administratively and provides programming feedback for the final customer. This part is the best layer of cloud computing,

and the customer can afford this administration. For example, limiting applications when using Google Docs, Administration, and Email, ERP and CRM applications will be used.

2) PaaS – Platform as a Service

This module allows the production of their own applications in the cloud using the cloud and unique tools and lingo. It has built-in administration for databases, web applications and nearby organizations.

3) IaaS – Infrastructure as a Service

Framework provides virtualized servers and programming as a rule. This will be provided on cloud data centers. When you need to use those virtualized hardware or servers, we have to pay the merchants in the cloud. The main advantage is that we do not have to buy all the hardware and programming for a long time. We pay for the systems used in the Virtual Environment (Cloud).

Client vendor monitor and manage data centers. You can basically focus on your business. IAS provides full infrastructure level such as virtual server, storage, network, security and system administration.

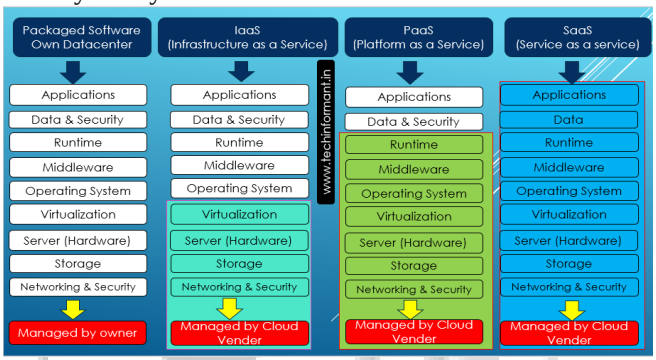

Fig. 1:

B. Cloud Computing Development Module

1) Private Clouds

A private cloud claims a lonely collaboration. Private Mist distributes distribution computing innovation to an organization that uses different parts, areas or categories of organization as a means of access to IT assets.

When there is a private cloud that is a controlled domain, then the problems in the Risks and Challenges section do not apply. Using a private cloud can change the range of power and limitations in a way that can be corrected and connected. The right organization of the private cloud status is accomplished by the internal or subcontinent staff.

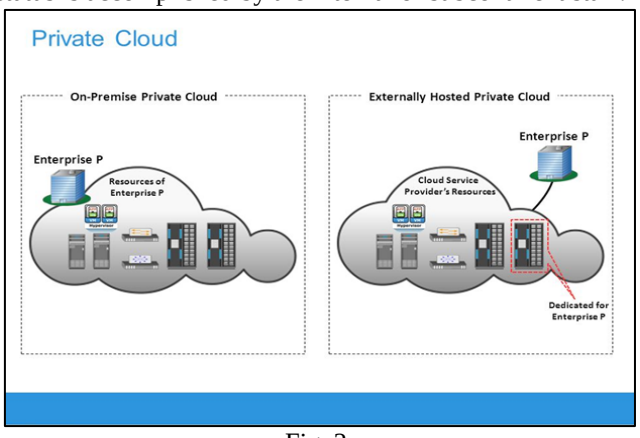

Fig. 2:

2) Public Clouds

Open Cloud is claimed by a cloud-state cloud external suppliers. In open snow, IT properties are usually provided by the already described cloud transit model, and often sell to cloud buyers via cost or through various roads (eg promotions). The cloud provider is responsible for the construction and current management of people's cloud and their IT assets. Many cases and designs examined in the following sections include open ice sheets and links between suppliers and IT property buyers.

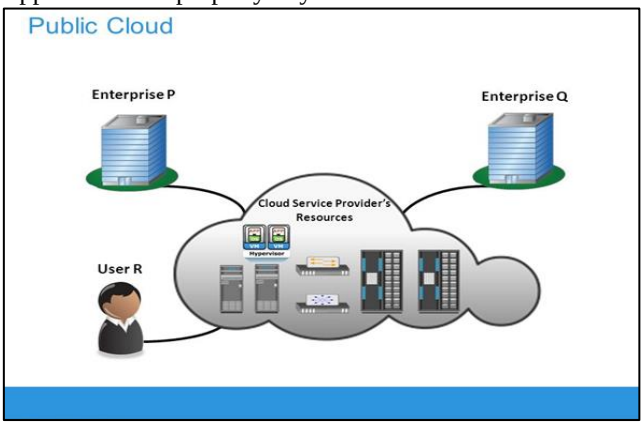

Fig. 3:

3) Community Clouds

The clouds of a group of people are like an open cloud, which reaches the client's specific network accessibility. Group clouds can be claimed in the network or by external cloud suppliers, which cures open clouds with restricted access. Cloud buyers share a network share of network cloud representation and development. Nomination in the network does not really guarantee the access or control of all IT assets in the cloud. Meetings outside the network are not generally accepted, except that the network allows it.

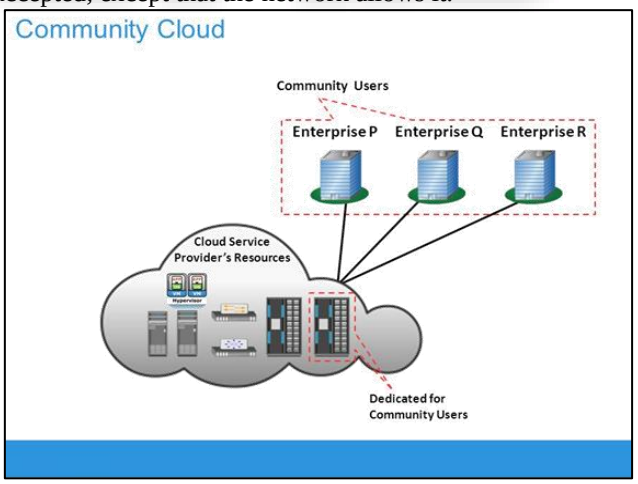

Fig. 4:

4) Hybrid Clouds

The mid-cloud cloud is a clouded situation that includes at least two separate cloud-sending models. For example, the cloud buyer could transmit cloud administration to a private cloud to provide cloud-sensitive information and other less sensitive cloud governments to open the cloud. This mixture effect is a show of half-reproduction system Cross-submission design complexity and potential in cloud conditions. Potential identification and performance functions are usually performed by the private cloud provider

association Cloud provider and maintain the test. General population cloud.

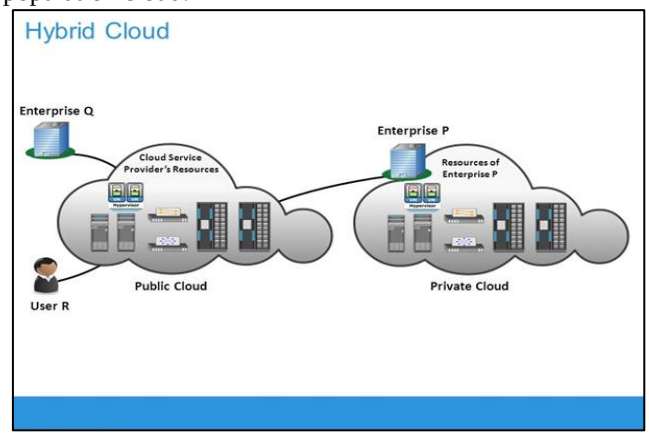

Fig. 5:

III. Common Cloud Computing Security Issues

A. Security

While various organizations share assets, information is threatened with misuse. Therefore, information about staying away from danger based on information repository and additional form, storage, travel or process. Information security is the most difficult problem in distribution computing. To improve security in distribution computing, it is necessary to verify, accept and control access to information stored on the cloud. Three basic areas of information security secrecy: - Top vulnerabilities are to be checked to guarantee that information is shielded from any assaults. So security test must be done to shield information from pernicious client, for example, Cross-site Scripting, Access Control components etc.,. Honesty: - To provide protection to consumer information, only some thin customers are used to access certain properties. Customers should not collect their information to ensure respect, for example, password.

B. Integrity

Framework security should be maintained with the final purpose to adjust the information from the person who has accepted it. In a cloud-based state, the respect for information should be managed effectively to maintain strategic distance from the loss of information. On all say, in every distributed computing, each exchange should take ACID properties to maintain respect for the information. Most web administrations take more time as part of exchange management issues because it uses HTTP administration. The benefit of the HTTP does not change or changes in insurance transfer. This can be solved by updating the administration of changes in APIs.

C. Access

Information mainly comes in the context of information security systems. In an organization, workers are given access to the information section of the security methods of their organization. The same information cannot be obtained by the same representation of the same structure. Different encryption methods and key management systems are used to ensure that information is distributed to legitimate customers only. The key is only broadcast in approved meetings using various major transport units. To be based on the information of the rejected customers, the information security process should be taken completely. All clients in the cloud can be accessed by the privileged customers, to be accessible through the web. Customer information encryption and security systems can be used to avoid security risks.

D. Confidentiality

Cloud consumer cloud contains information about remote servers and objects, such as information, recordings, with unique or multiple suppliers. At the time of collecting information on a remote server, the classification of information is one of the major requirements. In order to maintain privacy information and order knowledge, customers should know what information is stored in the cloud and its availability.

E. Distributed-Denial-of-Service Attacks

When delivery computing was initially known, the attack on the Cloud Stage (DoS) service delivery was largely unfamiliar; High rate of IT regime distributed by assets disrupted the Diodes attack. Since the same number of gadgets, cell phones and other structures is available with the Internet, DOS is expanding extraordinarily in attack exercises. When many movements start for the distributed computing structure, then it can be full or experienced experience.

F. Shared Cloud Computing Services

Not all Cloud Infrastructure and Distributed Computing Administration are the same. Many cloud solutions do not provide essential security to consumers, which cause properties, applications, and frames to be shared. In this situation, risks may start with the administration of delivery computing in different customers and the risk of focusing on the customer can also affect the different consumers.

G. Employee Negligence

For workers and monitoring representatives, there are the biggest security problems in all frames, however, risks with cloud fixes are especially vulnerable. Current representatives can sign up for cloud contracts from their cell phones, home tablets, and home-based area PCs, possibly without the protection of many external risks without frame protection.

H. Data Loss and Inadequate Data Backups

Due to the lack of information strengthening and degrading information, many organizations have security without Torrent Sent Wire, risk of cloud risk. Ransom ware "restricts" the organization's information on encrypted documents, which gives access to information after payment of payment. With proper arrangements for data consolidation, organizations will not be back on these risks

1) Phishing & Social Engineering Attacks

Due to the transparency of the distributed computing framework, phishing attacks and social design have proven to be particularly common. After obtaining login data or other classified data, a bad customer can easily break into the framework because the frame can be accessed from anywhere. In order to avoid such attacks it is necessary for workers to know about phishing and social design.

I. System Vulnerabilities

In any case, there may be frame errors in the distribution computing framework, especially on systems with complex foundations and many external steps. When vulnerability is known with a major outer frame, then this inability can be used without contradicting the association. Regardless of system monitoring systems to fight this risk, legitimate stabilization and updated traditions are fundamental. Distributed computer security issues are not impossible; In fact, you can put a large number of risks against using dedicated data insurance benefits. Information security agreements in the cloud protect information against malicious and risky digital security, allowing the firm to use the cloud effect without the risk associated with it.

IV. SOLUTIONS TO DATA SECURITY CHALLENGES

Encryption is recommended as a good response to secure data. Before saving information on the cloud server, it is quick to add this information. Owners of information can give a specific part of the meeting, which is the ultimate goal of obtaining information without effort. It is important to use various security-driven information so that information can be obtained. Display of information security should be done with the purpose of certifying information, collecting information, retrieving information, retrieving information and improving customer insurers through the cloud. Information insurance can be used administratively to ensure information security and security. An encryption app is used to confuse information access to different customers, misleading information and confuse common encryption access. Before transferring information to the cloud, the customer ensures that the information is stored in the reinforcement units and the key phrases in the record are unchanged. This ensures that the hash information of the document will not be modified before the cloud server is moved. This hash calculation can be used for the integrity of information; however, it is difficult to take care of it. Trustworthiness can be confirmed by RSA based information by adding personality based cryptography and RSA signature. The mother-in-law guarantees that there should be clear limitations in the app level to separate the physical level and information from many customers. Dispaminated control engineering can be used to reach management in distributed computing. To distinguish approved customers, it is best to use a qualified or attribution based system. The administration can be used to tell the client what part of the information can be obtained. The Granular Access Control Tool allows you to assign focusing accounts to the cloud server, regardless of the owner's information.

Data-driven structure can be used to secure information and exchange between cloud clients. The structure of the counter function is gradually used to identify the risks based on system hurdles. RSA-based efficiency protection technology can be used to represent important documents with different sizes and to inform the safety of remote data.

V. CONCLUSIONS & FUTURE WORK

Cloud computing is a new development innovation that shows the appropriate benefits for customers to face security challenges. In these documents, problems and diagnostic systems that address the risks associated with the cloud computing account for these problems. In the future, you can build strong standards for distributed IT security. To access protected information in the cloud, the suspended crypto system can be used to store and retrieve information from the cloud. In addition, the proper key management mechanism can be used to transmit the cloud client path, and the ultimate goal is that canonical and alone people can access the information. The firm specializing in delivery computing and the buyer should ensure that their cloud is fully protected from all external risks or attacks, so that concrete and general explanations can be provided by the consumer suppliers. The biggest whole test among cloud security applications and research theory is to solve some essential resistance between the real security of cloud of speculation and the protection of the virtual machine. The investigation should focus on these holes and contradictions and their evacuation. The method to make cloud computing programming can be one of the system bits, and there may be pre-production preparation for other specific consumer applications. Buyer's behavior can be controlled and controlled, for example, if the buyer allows computerized programming to run or update antivirus definitions, or does the general population understand the way to strengthen their virtual machines in the cloud.

REFERENCES

[1] Prince Jain -Security Issues and their Solution in Cloud Computing Prince Jain-2012
[2] Pradeep Kumar Tiwari -Cloud Computing Security Issues, Challenges and Solution-Aug, 2012
[3] Manpreet Kaur-A REVIEW OF CLOUD COMPUTING SECURITY ISSUES –Jun, 2015
[4] Monjur Ahmed -CLOUD COMPUTING AND SECURITY ISSUES IN THE CLOUD –Jan, 2014
[5] Abhinay B.Angadi-Security Issues with Possible Solutions in Cloud Computing-A Survey –Feb, 2013
[6] Jahangeer Qadiree -Solutions of Cloud Computing Security Issues –Apr, 2016
[7] Kevin Hamlen -Security Issues for Cloud Computing – Jun, 2010
[8] Amit Wadhwa -Study of Security Issues in Cloud Computing-Jun, 2015
[9] Gary Utley-Most Common Cloud Computing Security Issues- April 12, 2018
[10] R. Velumadhava Raoa -Data Security Challenges and Its Solutions in Cloud Computing, 2015
[11] Jahangeer Qadiree -Solutions of Cloud Computing Security Issues- mar-apr 2016

