# REVIEW OF SOLUTIONS FOR CLOUD COMPUTING SECURITY AGAINST MANY ISSUES

*[1]A. Padmaja, Assistant Professor, Mail ID:gspgsp26@gmail.com*
*[2]E Muralidhar Reddy, Assistant Professor, Mail ID:krishna81.reddy@gmail.com*
*[3]B Pannalal, Assistant Professor, Mail ID:bpannalal@gmail.com*
*[4]Dr.M.Chandra Naik, Associate Professor, Mail ID:venkatesh.kgs@gmail.com*
*Department of CSE Engineering,*
*Pallavi Engineering College Hyderabad, Telangana 501505*

***Abstract: - The interest of the entire planet has been aroused by cloud storage, a quickly evolving digital technology. Cloud computing is Internet-based computing, whereby machines and devices on demand, such as the power grid, are supplied with common services, applications and knowledge. The convergence of conventional computer technologies and network technology, such as grid computing, distributed parallel computing, etc., is the result of cloud computing. More interest has been drawn to cloud storage. Cloud infrastructure has begun to be pursued by more and more businesses and government departments. Security challenges have, though, arisen on an increasing scale with the widespread usage of cloud storage. To encourage the broader uses of cloud computing, it is important to address these protection problems. The purpose of this research is to recognise the most susceptible security risks in cloud computing, allowing both end-users and suppliers to learn about the core security threats associated with cloud computing. This would encourage researchers and security experts to learn about the needs of consumers and suppliers and to critically examine the numerous proposed security models and tools.***

***Keywords: Grid computing, middleware, replication, risks, virtualization, cryptography.***

## I. INTRODUCTION

The Internet has become a guiding influence in the advancement of diverse technology. Cloud Infrastructure is arguably one of the most debated amongst all of these. For nearly all companies seeking to make their entrance into it, cloud infrastructure is seen as a development in the modern scenario. As the new direction to address alternate distribution models with IT capabilities, the cloud is evolving. In the form of apps, networks and more, it is a means of providing IT-enabled services.

"Cloud computing can be described as "A computing cloud is a collection of network-enabled resources that include scalable, Quos-assured, typically customizable, inexpensive on-demand computing platforms that can be accessed in an easy and omnipresent manner"[1]. Cloud infrastructure is the synthesis of a technology, a network that offers Internet hosting and storage facilities, in plain terms. Request device infrastructures with decent service efficiency. In order to access high quality software across the Internet, Cloud Infrastructure is the introduction of engineering concepts. The key purpose of cloud computing is to offer high-quality service levels with flexible and affordable on-demand computing infrastructures. The internet-based, extremely flexible distributed computer frameworks in which intellectual services are delivered as a commodity is supported by cloud computing. The benefits of allowing use of cloud infrastructure are:

(i) lowered expenses for hardware and repairs,

(ii) Connectivity in the world, and

Flexibility and a fully automated process in which the user does not have to think about updating apps, which appears to be an everyday thing. It is important to split cloud computing into two parts, the consumer and the cloud. The consumer is linked via the internet to the cloud in most scenarios. It is also possible to provide a private cloud within an enterprise where a person is linked with an intranet. The customer sends requests to the server and the service is delivered by the computer. Two main aspects of the cloud paradigm are multi-tenancy and elasticity. Multi-Tenancy allows the same example of operation to be exchanged by multiple tenants. Elasticity requires capital dedicated to a service to be adjusted up and down depending on the existing service specifications. Both features concentrate on optimising the use of energy, expense and affordability of facilities.

## II. ARCHITECTURE OF CLOUD COMPUTING

It's useful to break it into two parts when learning about a cloud storage system: the front end and the back end. Via a network, normally the Internet, they link to one another. The front end is the hand used by the owner of the machine, or client. The back end is the part of the system's "cloud"

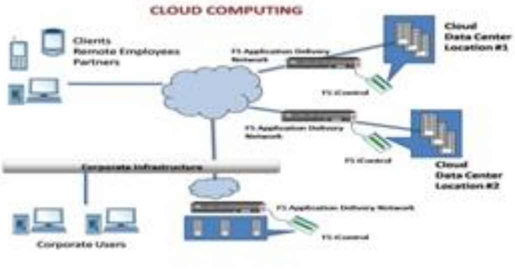


***Fig 1: -The architecture of cloud data storage service***

The front end contains the machine of the customer and the programme used to enter the cloud storage infrastructure. Not all applications for cloud storage have the same user experience. Current Online browsers such as Internet Explorer or Firefox are leveraged for utilities like Web-based e-mail programmes. Other networks provide special programmes and provide clients with network connectivity. The numerous machines, servers and data storage facilities that build the "cloud" of computing resources are on the back end of the device. To ensure it operates properly, a central server controls the device, tracking traffic and client demands. It follows a series of guidelines called protocols and uses middleware, a specific type of programme. Middleware helps machines that are networked to connect with each other. Servers don't run at maximum speed much of the time. A cloud storage system would generate a backup of the knowledge of all its users and archive it on other computers. Copies enable the central server to reach backup computers to restore data that would be unavailable otherwise. Making data copies as a reference is known as replication. Providers of cloud platforms aim to offer services that can be categorised into three categories: software as a service, network as a service, and service infrastructure.

**i) Software as a Service (SaaS):**

To offer on-demand tech facilities. Cloud applications with various end customers or client entities are used to access a single instance of the programme. Salesforce.com is the most well recognised representation of Seas, but several other examples have come to market, including the provision of simple business resources by Google Applications, including email and word processing. Though salesforce.com followed the cloud computing concept by a few years, it now works by using its counterpart force.com, which can be defined as a service portal.

**(ii) Application as a Service (Peas):**

Framework as a utility encapsulates a software layer and provides it as a service that can be used to construct applications at a higher level. Depending on the viewpoint of the manufacturer or user of the services, there are at least two viewpoints on Peas:

Through combining an OS, middleware, application software, and even a production environment that is then given to a consumer as a service, anyone who produces Peas might create a network.

An encapsulated service that is delivered to them by an API will be used by those utilising Peas. Via the API, the user communicates with the application, and the platform performs what is needed to handle and scale it and deliver a certain quality of service. You may identify virtual appliances as Peas instances. The Google Apps Engine, which supports Google infrastructure programmes, provides commercial examples of Peas. Pea's platforms like this may provide a powerful basis for delivering apps, but the features that the cloud provider decides to deliver can constrain them.

**(iii) As-a-service technology (Iasi):**

Infrastructure as a service offers essential storage and computational resources across the network as structured networks. In order to manage workloads varying from device modules to high-performance computer devices, computers, disc devices, switches, routers and other systems are combined and made usable. Commercial instances of Iasi include Joint, whose primary commodity is a line of virtualized servers that offer an infrastructure that is extremely usable on requests.

## I. In cloud Infrastructure, risks

Cloud storage has developed from being a promising market model in the last few years to one of the IT industry's fastest rising markets. Recession-hit enterprises are now rapidly finding that they can obtain easy access to best-of-breed business apps or dramatically expand their infrastructure capacity simply by tapping into the cloud, both at a marginal expense. But as more and more data on individuals and enterprises were put in the cloud, questions over how reliable an environment it is are starting to emerge.

- Safety of the Network:

Network communications problems and configurations relevant to cloud storage infrastructures. The perfect approach for network security is to have cloud providers as an extension of the current internal networks of customers [2], implementing the same safety mechanisms and security precautions that are applied locally. And to enable local techniques to be applied to every distant resource or operation.

- Safety of transfer:

Distributed systems, large resource sharing and replication of virtual machine (VM) instances mean more cloud data in transit, thereby requiring VPN mechanisms to defend the device from sniffing, spoofing, and assaults by man-in-the-middle and side-channel.

- Firewalling:

Firewalls defend the internal cloud resources of the vendor from insiders and external users [3]. They often allow VM separation, fine-grained filtering for addresses and ports, Denial-of-Service (Does) prevention, and external security evaluation procedures to be identified. Efforts to adapt

The desire to adjust current technologies to this modern software model shows a consistent firewall and related protection mechanisms unique to cloud environments.

- Safety settings:

Configuring protocols, frameworks and technology to have the protection and privacy standards needed without sacrificing performance or efficiency [4].

## III. Security Issues

The vendor of cloud storage software must guarantee that confidential knowledge regarding the client is well shielded from all vendors, clients and consumers. As most servers are external, the cloud service company can make sure who accesses the data and who manages the system in order to allow the provider to secure the sensitive details of the user.

**A. Security of data**:
Cloud data is housed in various physical repositories, spread in different areas of the World, and data security is challenging to achieve safety in the absence of corresponding technological and regulatory restrictions. First of all, various areas, some ahead and some behind, have different levels of technology. Somewhere, data is secure, but in another position, there could be some danger. Secondly, in different areas, there are numerous laws.

**B. The Interfaces:**

Concentrate on both users, technical and programming interface problems with cloud usage and control.

API: In order to avoid malicious usage, programming interfaces (essential to Iasi and Peas) for accessing virtualized services and systems must be protected [5].

- Administrative interface:

Allows remote control of Iasi (VM management) services, Peas (coding, deployment and testing) development and Seas framework tools (user access control, configurations).

- User interface:

The end-user guy for the exploration of the supplied materials and tools (the service itself) suggests the need to take environmental conservation steps.

- Verification: Authentication

Mechanisms that are needed to allow cloud access. As a result, most providers depend on standard accounts that are vulnerable to a multitude of assaults, the effects of which are boosted by multi-tenancy and resource sharing.

**C. Virtualization: Isolation between VMs, hypervisor bugs and other virtualization technology utilisation issues [6].**

- Isolation:

While technically isolated, all VMs share the same hardware and consequently the same infrastructure, facilitating the exploitation of data leaks and cross-VM attacks by malicious entities [7]. It is also necessary to extend the principle of separation to more fine-grained properties, such as computing capital, storage and memory.

- Vulnerabilities in hypervisors:

The key software feature of virtualization is the hypervisor. While hypervisors have known security weaknesses, solutions are still rare and mostly proprietary, needing more studies to harden these elements of security.

- Leakage of data:

In order to leak data from virtualized infrastructures, obtain sensitive consumer data and harm security and honesty, circumvent hypervisor bugs and lack of isolation controls.

### *A. **Governance: Governance***

Issues linked to cloud storage solutions (losing) administrative and protection measures. [8, 9] Uh,

**(i) monitoring details**

Transfer information to the cloud involves losing power of redundancy, venue, file systems and other settings that are important.

**ii) Management of security:**

Loss of protection frameworks and policies governance as terms of use prevent customer-side vulnerability evaluation and penetration testing although poor Service Level Agreements (SLA) contribute to security holes

**iii) Safe transmission of data:**

The Internet would be traversed with all the traffic from your network and any service you reach in the cloud. Make sure that your information still passes on a protected channel; only link your browser to the provider with a URL that starts with "https." Your details should also always be secured and authenticated utilising industry-standard protocols, such as IPSec (Internet Protocol Security), explicitly configured to protect Internet traffic.

**B. Service loss:**

Due to the interconnections between systems (e.g., a Seas uses virtualized infrastructures offered by an Iasi), service outages are not unique to cloud environments but are more severe in this case, as seen in several instances [10-12]. These points to the need for effective disaster management plans and service guidance to, where necessary, enforce customer-side redundancy.

## IV. CRITICAL EVALUATION

From the early years to the present status of cloud computing:

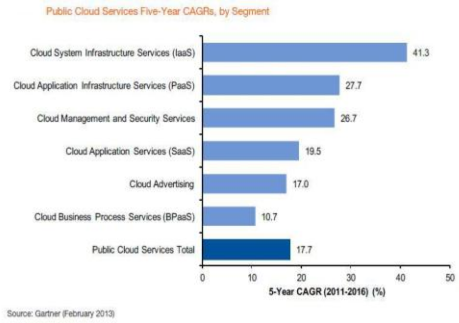
Cloud computing forerunners appeared decades earlier, first as time and computing sharing on mainframes, then as utility computing through private network providers. Application service providers (ASPs) and grid computing began to get some momentum when the Internet was developed in the late 1990s. Both of them, though, had to contend with restrictions, the key one being inadequate network capacity to render them workable for vast quantities of consumers. Today, cloud infrastructure has the resources and pipelines it wants and has branched into public, private and hybrid cloud systems due to internet, fibber-optic cable, enhanced applications and several other developments. Yet it's also early in the past of clouds.

**I. Lead the Charge with SMBs**

While the majority of organisations, both big and small, have somehow embraced cloud infrastructure, when it comes to the percentage of resources they rely on from the cloud, small and medium-sized businesses (SMBs) lead the group. A latest Spice works study found that more than 60% of SMBs reacting to the survey are utilising cloud-based services today; according to IDC, expenditure on these services is expected to rise by almost 20% in the next five years [13].

**II. Having increasingly dynamic clouds to handle**

Growing customer demand, shorter timelines, the rise of mobile devices and the bring-your-own-device (BYOD) era for several big corporations have culminated in a dynamic combination of large enterprises' data centre networks and public, private and hybrid cloud providers. Furthermore, in terms of both storage and processing power, the rise of big data poses a massive challenge. In addition to these factors, the advantages of agile scalability and pay-as-you-go in cloud infrastructure fuel cloud growth in large organisations to better meet these obstacles.



Source: Gartner (February 2013)

*Fig 2: -Evaluation of cloud computing:*

**Security Still the Main Source of Distrust**

Given these developments and the advantages of the cloud paradigm, many main corporate programmes are nevertheless discouraged from switching to cloud services by a strong degree of concern over frameworks and data protection. Mission-critical apps have stayed in-house and under the oversight of IT for several major companies. Cloud-based platforms would soon allow a mere 30 to 40 percent of company functionality, according to management consultancy and technology services company Trains, whilst the remaining 70 to 60 percent of functionality would depend on technologies offered by home-grown IT.

**I. More Gathering Clouds Inside the Firewall**

Surveys reveal that internal and virtual clouds are widely utilised when IT continues to transform internal networks into more versatile and cost-effective private cloud providers.

### II. More Cloud-based core market applications will be

Mission-critical applications will become more cloud-based with the advent of emerging technology and platforms that will enable the provisioning of full physical servers while allowing them to maintain the simplicity and automation that cloud services offer.

### III. Automation, quick configurability: keys to the success of the Cloud

Cloud services must provide the following to facilitate potential adoption: the ability to provide hybrid platforms that provide private and public cloud computing resources seamlessly; the ability to provide virtual and physical infrastructure to help a broad variety of applications, including performance-intensive mission-critical apps; robust features that provide user self-service with a high degree of user self-service

## Safety Measures for Cloud Computing:

Taking into consideration Cloud Computing main security concerns, this paper summarised some appropriate response measures:

### a. Strengthen the potential to deter attacks:

Anti-attack hardware, anti-virus applications, and firewalls can be implemented in the clouds. "Cloud security" and "cloud antivirus" and other applications have been introduced by several security vendors.

### b. Information-security-centric:

We recommend moving from shielding data from the outside (systems and apps that utilise the data) to protecting data from the inside in order for organisations to expand leverage of data in the cloud. This approach to data and knowledge that preserves itself is called information-centric [14]. This self-protection means bringing intelligence into the data itself. Info, regardless of its setting, needs to be self-described and defended. Data has to be encrypted with a usage policy and bundled. Data should consult its policies when accessed and aim to re-create a protected environment utilising virtualization and expose itself only if the environment is checked as trustworthy (using Trusted Computing). A logical continuation of the movement toward faster, stronger, and more accessible data privacy is information-centric security.

### c. Encryption of Information:

A different solution to ensuring data access is to enable protection of all cloud data. The issue is that data access is restricted by encryption. The quest and indexing of the data are especially troublesome. For egg, if data is stored in clear-text, by defining a keyword, you can search for a record effectively. For standard, randomised encryption methods, this is difficult to achieve. To solve these problems, state-of-the-art cryptography can give new tools. Recently, cryptographers have invented flexible encryption schemes that facilitate cipher text activity and computation.

The cloud service provider has some capacity to scan for encrypted data, cloud data proliferation can theoretically allow better insider vulnerability monitoring (e.g., by identifying user behaviours beyond the norm) and better avoidance of data loss (DLP) (e.g., through detecting anomalous content).

Applied cryptography can often provide resources to resolve other protection concerns relevant to cloud storage, in addition to maintaining anonymity. For egg, the storage server should show compact evidence that it holds all the data of the client correctly in proof of irretrievability.

### d. Remote Server High-Assurance Attestation:

Customers currently need to be happy with cloud services using manual auditing methods such as SAS-70.

Trusted Computing is the foundation for a promising solution to solving this problem. Imagine a trusted cloud server-installed controller that can monitor or inspect the cloud server's activities. The trustworthy monitor can provide the data owner with "proof of compliance," specifying that such access policies have not been broken. Trusted Computing often enables safe bootstrapping of this monitor to operate next to (and safely disconnected from) the operating system and software in order to maintain monitor integrity. The supervisor will implement rules for access management and conduct monitoring/auditing duties. The code of the monitor is signed to produce a "proof of compliance" as well as a "statement of compliance" provided by the monitor. When this evidence of enforcement is obtained by the data user, it will check that the proper display code is operating and that the cloud service has met with access control policies.

e. **Selecting a suitable place for storage:**

Users do not realise where the data is processed, relying on cloud storage, which would add further protection challenges. Firewalls and monitoring and avoidance of intrusions will hold most intruders away, and data protection makes the data secure, so when we end our service or when the cloud company goes out of business, we don't know where the data goes. The key that enables cloud infrastructure systems to pass the most rigorous safety standards is dedicated hardware. Therefore, they can choose trustworthy service providers as the customer chooses cloud storage providers, and they ought to read the privacy statements carefully.

f. **Establishing universal requirements for safety:**

Currently, this issue has been recognised by several policymakers and organisations, and they are interested in exploring the creation of a shared standard to encourage the popularity of cloud computing. Security requirements, which not only require technological standards, can also include safety standards for the development of a protected mechanism for the security of privacy.

**g. Choosing trustworthy equipment suppliers:**

Given their own long-term growth and their own integrity, by understanding which server and data centre the data is being held at, you will evaluate them with any relevant protection measures in place, a company with advanced technological and operation would not reveal user details.

## V. Considerations And Future Work

We are studying the issue of cloud protection management. Our mission is to avoid the cloud paradigm from being implemented by the protection management systems of cloud users and cloud providers. We need to collect numerous protection criteria from various viewpoints and different layers of information and map security requirements to the cloud infrastructure, security patterns and compliance regulation processes to be able to solve this issue and provide cloud providers and customers with input on the existing security status.

Protection is a critical component of offering a secure platform and therefore enabling cloud technologies to be utilised and data and business operations to be transferred to virtualized infrastructures. In most computer contexts, many of the security problems found are observed: authorization, network security and regulatory standards, for example, are not an innovation. However, due to features such as multi-tenancy and resource sharing, the effect of such problems is compounded in cloud computing, as activities by a single client may influence all other users that eventually share the same services and interfaces. In the other hand, in such a setting of high delivery of dynamic networks and web-based software, effective and stable virtualization poses a new task, demanding more nuanced approaches.

Through isolating virtual machines and the related infrastructure while adopting best practises in terms of legal regulations and enforcement with SLAs, it is strategic to build new frameworks that have the necessary protection standard. Such solutions can, among other criteria, employ the detection of virtual machines, include sufficient differentiation of dedicated resources coupled with continuous observation of mutual resources, and analyse any effort to manipulate cross-VM and data leakage.

## VI. CONCLUSION

Cloud lies face down to diverse security risks, ranging from network level threats to threats at the device level. These security risks need to be monitored in order to maintain the cloud safe. In addition, cloud-based data is often vulnerable to a range of risks and different challenges, such as protection concerns, compatibility issues, anonymity, and data privacy. Both the cloud service provider and the user can guarantee that the cloud is secure enough against any external risks, so that the customer and the cloud service provider can have a good and shared understanding. In addition, cloud service providers need to guarantee that all SLAs are fulfilled and that human mistakes on their side can be reduced, allowing for smooth running. Different protection problems pertaining to the three key resources offered by a cloud storage environment are presented in this paper and the strategies to avoid them have been explored.

## References:

[1] *Song, D., Wagner, D., and per rig, A. Practical Techniques for Searches on Encrypted Data. In IEEE Symposium on Research in Security and Privacy. 2000.*

[2] *L. Wang, G. Laszewski, M. Kunze and J. Tao, "Cloud computing: a perspective study", J New Generation Computing, 2010, pp 1-11.*

[3] *Harjit Singh Lamba and Gurdev Singh, "Cloud Computing-Future Framework for emanagement of NGO's", IJoAT, ISSN 0976-4860, Vol 2, No 3, Department Of Computer Science, Eternal University, Baru Sahib, HP, India, July 2011.*

[4] *R. Maggiani, Communication Consultant, Solari Communication, "Cloud Computing is Changing How we Communicate," 2009 IEEE International Professional Conference, IPCC, pp. 1-4, Waikiki, HI, USA, July 19- 22, 2009. ISBN: 978-1-4244-4357-4.*

[5] *Ertaul, L. and Singhal, S. 2009. Security Challenges in Cloud Computing. California State University, East Bay.*

[6] *http://computer.howstuffworks.com/internet/basics/internet-infrastructure.htm*

[7] *An Information-Centric Approach to Information Security. http://virtualization.sys-con.com/node/171199.*

[8] *http://www.idc.pt/resources/PPTs/2007/IT&Internet_Security/12.EMC.pdf*

[9] *Boneh, B., Di Crescenzo, G., Ostrovsky, R., and Persiano, G. Public Key Encryption with Keyword Search. In EUROCRYPT. 2004.*

[10] *Boneh, D and Waters, B. Conjunctive, Subset, and Range Queries on Encrypted Data. In The Fourth Theory of Cryptography Conference (TCC 2007), 2007*

[11] *Shen, E., Shi, E., and Waters, B. Predicate Privacy in Encryption Systems. In TCC. 2009.*

[12] *Shi, E. Bethencourt, J., Chan, H., Song, D., and Perrig, A. Multi-Dimensional Range Query over Encrypted Data. In IEEE Symposium on Security and Privacy. 2007.*

[13] *TrendMicro (2010) Cloud Computing Security - Making Virtual Machines Cloud-Ready. Trend Micro White Paper*

[14] *Genovese S (2009) Akamai Introduces Cloud-Based Firewall.http://cloudcomputing.sys-con.com/node/1219023*