Survey on Cloud computing: security threats, vulnerability and mitigation

Asha Kumari
M.Tech/CSE,
VIT University,Vellore,India

Sonam
M.Tech/CSE,
VIT University,Vellore,India

Kalyani Singh
M.Tech/CSE,
VIT University,Vellore,India

Abstract-- **Cloud computing is used for providing buoyant IT services to any particular user or organizations with the help of distributed computing pattern. Cloud computing offers an inventive business model with the help of features like elasticity, flexibility, multitendancy, scalability, layer dependency stack, centralized data storage and processing of these data. In future, we can think of cloud as an uncomplicated operating system that runs on web browsers and allows users to access and process their data virtually or remotely unlike our traditional operating system. Implementing cloud as an operating system can reduce the complexity of managing data and resources because application and data can directly 'live and run' on the internet without first storing on hard drives. In this survey research paper, we provide the security issues of using cloud computing as a single cloud and provide architecture of multi cloud which is more secure architecture of using cloud computing as a service.**

Keywords**: cloud computing, multi cloud, security, attacks, depsky architecture**

I. Introduction

Cloud computing can be defined as the application or service which uses distributed environment network or internet providing services to the users and organization. We can think of cloud computing in terms of these two concepts:

Abstraction and virtualization

Abstraction mainly deals with the process of hiding the details of system implementation and physical location of system.

Virtualization is the method of storing and processing of centralized stored data though this pooling and sharing of resources can be achieved.

1.1. Definition:

According to NIST:

Cloud computing is a model for enabling ubiquitous, convenient, on- demand network access to a shared pool of configurable computing resources that can be rapidl provisioned and released with minimal management effort or service provider interaction.

1.2. Characteristics of cloud:

According to NIST there are five essential characteristics of cloud:

1. On- demand self service
2. Broad network access
3. Resource pooling
4. Rapid elasticity
5. Measured services

1.3. Benefits of cloud are:

Low cost, easy maintenance, reliability, increased productivity, low barrier to entry, application programme interface, device and location independence, elasticity, agility.

1.4. Components of cloud:

The different components of clouds are:

a. **Clients :**

Clients are the end users who interact with cloud and clients are of two type:

I. Thin clients:

Thin clients are the computers which does not have any storage space. So there is high level of security at this level because no data are stored on thin client and data is present in data centers.

II. Thick clients:

Thick clients are the machines which are virtually connected to the server and more vulnerable to security attacks.

III. Mobile clients

Mobile clients are those which can run their application using laptop or phones.

b. **Data centers:**

Data center can be considered as the space where the data are stored.

c. **Internet:**

Internet connection is used to access the data which is stored in the cloud storage.

d. **Distributed servers:**

1.5. Cloud computing model:

Cloud computing model categories into two categories:

1. Deployment model
2. Service model
3. Cloud cube model.

1.5(a) Deployment model:

This model consists of:

A. **Private cloud**: this cloud infrastructure operated or managed by single organization or any third party and it may be internally or externally
B. **Public cloud**: this is pay per page model and deployed over the network as public cloud for the open access to public
C. **Hybrid cloud**: this model consist of two or more deployment model for advantage of multiple deployment model
D. **Community model**: this deployment model is generally used when there is a common issue from group of communities or organization

E. **Distributed model**: this deployment model set up at different location and user can access data remotely from any location by connecting to the single network.

F. **Intercloud**: this model is similar to 'network of network' and provides interoperability between cloud service providers.

G. **Multicloud**: this deployment is heterogeneous architecture of different cloud services to reduce security risk and providing more flexibility to cloud services.

1.5(b) Service model:

Services	Definition	Benefits	Obstacles
IaaS	Infrastructure as a service provides hardware to the organizations as PaaS and SaaS offers application to the customers and the infrastructure which is offered by service provider can be dynamically scaled up and down.	Computer hardware, utility computing billing, network, service level agreements, internet connectivity.	complexity, synchronization, integrity, labour cost, standard
PaaS	Platform as a service is a delivery model and known as cloud ware which supplies resources necessary for building any application from internet and there is no need of installing software.	collaboration, database integration, scalability, security, web service integration, storage and state management	Lack of portability and interoperability among providers.
SaaS	Software as a service can be defined in terms of use and reuse of services of any component and provide access to data with the help of available network or software.	smaller staff, web reliability, more bandwidth, security, customization, familiarity with world wide web	availability of open source application and cheaper hardware
DBaaS	Database as a service offers space for running our database by reducing the cost and complexity.	power, ease of use, management and integrity	security and synchronization
DaaS	Data as a service is based on the concept that data is provided to the customer on demand regardless of physical or geographical locations of users.	cost effectiveness, data quality, agility	generally data is not available for download
STaaS	Storage as a service offers storage space on rent to an organization.	less expensive, object storage architecture, copying virtual images from the cloud	attack surface area, supplier stability, accessibility
SEaaS	Security as a service offers set of rules or policies to protect applications and data of users.	privacy, legal issues, availability, physical and personal security	end of service, intellectual property, data loss
TEaaS	Test environment as a service model offers infrastructure for testing software.	quick availability of infrastructure, unlimited storage, reduced execution time of application	

1.5(c). Cloud cube model:

There are four dimensions in the cloud cube model:

a. **Physical location of the data:** Internal (I) / External (E) determine your organization's boundaries.
b. **Ownership:** Proprietary (P) / Open (O) is a measure of not only the technology ownership, but of interoperability, ease of data transfer, and degree of vendor application lock-in.
c. **Security boundary:** Parameterized (Per) / De-parameterized (D-p) is a measure of whether the operation is inside or outside the security boundary or network firewall.
d. **Sourcing:** In sourced or Outsourced means whether the service is provided by the customer or the service provider.

1.6. Benefits of cloud in future:

Imperviousness to new engineering ideas is inescapable, and cloud computing is no exemption. Yet today, distributed computing has developed to the level where it is a reasonable innovation, prepared to grasp and bring advantage to your organization.

The reason why distributed computing chance is currently includes:

a. Economic need
b. Support from real standard programming
c. Demand from little business for top of the line characteristics
d. Demand from big business clients for more financially savvy arrangements
e. Need for synergistic instruments
f. Cloud engineering has effectively passed the demonstration

To technologists, the eventual fate of cloud computing is not difficult to understand, because we have the point of interest of history. To really comprehend the fate of cloud computing innovation, we just need to analyze the authentic development of prior processing stages. The cloud is advancing in a hefty portion of the same courses, with its framework, stages and programming.

More vital is the impact of the cloud on the individuals who use it. We may even say that cloud computing is arriving at “discriminating mass.” That is, it has come too far to return it in the flask. It’s here, the engineering is prepared, and it is as of now rolling out sensational improvements to the way individuals work together, the way we work, and even the way we think. It is making another class of business visionaries and introducing second dotcom blast.

1.7. Future expectation of cloud computing:

a. Cloud framework commoditize, and costs fall.
b. Open guidelines rise as predominant in cloud stages.
c. Home sourcing gets to be standard.
d. Corporate methods get to be decentralized.
e. A new wave of enterprise rises.
f. Smart telephones advance with cloud applications.
g. The days of multi-million dollar undertaking programming activities arrives at an end.
h. Cloud registering infiltrates all territories of business administration.
i. Big-name organizations battle for new personalities.
j. Social systems administration frameworks will advance into synergistic administration frameworks.

1.8. Companies providing different cloud services:

a. AMAZON: elastic compute cloud (EC2), simple storage service (S3), simple queue service (SQS), simple DB.
b. GOOGLE: Google App engine
c. MICROSOFT: windows azure, Microsoft SQL servers, Microsoft .NET services, live services, Microsoft share point service and Microsoft dynamics CRM services.

II. EXISTING SYSTEM DRAWBACK

1. Security Issues:-

a. Vulnerabilities:

S. No.	Vulnerabilities	Description
1.	Session Riding	It is the process of hijacking the current session of users by sending session key on behalf of users and gaining unauthorized access in the session.
2.	Virtual Machine Escape	Due to multiple VMs running in parallel in operating system of cloud tough task to manage all the entire VMs at a time. In this attack, instance of VMs is created and attackers run code on a VM.
3.	Reliability Availability of Services	Cloud is not perfect in terms of reliability and availability. Amazon S3 in February 2008 goes down for several which leads to data loss and access issue.

4.	Insecure Cryptography	Cryptographic algorithm can easily break by attacker in VM environments. As Unix based VMs, generates random number for a millisecond from which it is not easy to form strong encryption key.
5.	Data Protection and Portability	Sensitive data is not protected in cloud environment and stored data in cloud is also not portable.
6.	Vendor Lock-In	Due to lock-in feature clients are dependent on service provider for product and services which cause incapability of client to deal with one another.

b. Threads

SN.	Threats	Description	Example	Impact	Remediation
1.	Abuse and Nefarious use of cloud	Illusion of unlimited space storage capacity and network to use.	Zeus botnet Info Stealer Trojan horses spam.	Fraud detection capabilities are limited weak registration system.	Stricter initial registration and validation processes, comprehensive introspection of customer network traffic, Enhanced credit card fraud monitoring.
2.	Insecure Interfaces and APIs	Cloud as APIaaS provide software interfaces to the user to directory interacted with cloud services Malicious attack leads to non availability of service or interfaces.	Improper authentication, Inflexible access controls, limited Monitoring and logging capabilities, API dependencies.	Security issues associated with management, monitoring, orchestration and usage of cloud services. Confidentiality, integrity availability and accountability.	Security model of cloud provide interfaces dependency chain associated with API Strong authentication and access control encrypted transmission.
3.	Malicious Insider	This is always inside the organisation due to general lack of transparency into provider and user.	No public example available at this time.	Financial impact, brand damage productivity losses access and ability to modify organisation assets.	compliance reporting strict and comprehensive supply chain management security breach notification process
4.	Data loss or leakage	Phishing, exploitation of software, fraud methods can lead to the access to our account or services.	No public example	Comprising the integrity and confidentiality of deployed cloud data stolen credential.	Two factor authentication proactive monitoring Security policy and SLAs Prohibiting the sharing of account information.
5.	Unknown Risk Profile	Due to reduction of software ownership and maintenance allows companies to focus on their core business strength leads to explore of unknown profile.	Heartland breach IRS and Amazon	Internal security procedure, patching auditing configuration hardening.	

c. Attacks

S. No.	Attacks	Description	Mitigations
1.	Zombile Attack	Large number of request on internet is called Zombile which are flooded over the network for requesting access to the network. This lead to Denial of Service (DoS) or DDoS (Distributed Denial of Service) to the servers.	Authentications and Authorisation of IPS/IDS
2.	Service Injection Attack	In this, an attacker tries to inject malicious services by blocking the functionality of cloud services.	Strong isolation between VMs Service integer checking module
3.	Virtualization Attack	This attack can be done by VM escape or Root kit in hypervisor. In VM escape attack attacker get access to the host OS and the other VM's running on physical machine. In VM-based root kit attackers get control over any VM running on host machine.	VM attacks can be monitored by IPS(Instruction prevention System) and IDS(Instruction detection System)
4.	Man-in-the middle Attack	This attack is possible if SSL is not properly configured and attackers can access the delay and communication among data centre.	Proper SSl configuration ,authorization of communication parties
5.	Metadata Spoofing Attack	In this attack, attackers modify the WSDL file at delivering time.	Strong invocation code flow WSDL
6.	Phishing Attack	Attackers can manipulate the web link and redirecting user to false link and accessing the sensitive data.	Better authentication protocol
7.	Backdoor Channel Attack	It is a passive attack for accessing the user data remotely.	Isolation and authentication between VMs.
8.	Malware Injection Attack	This attacks include malicious file execution, insecure communication, broken authentication cross site scripting etc.	Authentication of data and encryption of data
9.	Wrapping Attack	This attack is done by translating the SOAP message between user and web servers.	SOAP message security validation mechanism

2. Leak of sensitive information:

Less scrupulous service providers might even share that data with a marketing firm. And other providers may, by way of their agreement with you, be allowed to access and catalog your information and use it in ways you never intended.

Private data has certainly been released. In 2006, AOL released search terms of 650,000 users to researchers on a public web page. In 2007, Microsoft and Yahoo! released some search data to the U.S. Department of Justice as part of a child pornography case. Obviously, no one wants predators to get away with their crimes, but consider the implication if your data was innocently mixed in with the data that Yahoo! and Microsoft provided the government, and you were wrongly pulled into an investigation.

3. Application not ready

In some cases the applications themselves are not ready to be used on the cloud. First, the application might require a lot of bandwidth to communicate with users. The application might also take a lot of effort to integrate with your other applications. If you try to relocate it to a cloud, you may find that the savings are erased by the additional effort required to maintain the integration. In this case it may end up being more cost effective to continue to host it locally.

III. Problem Definition

1. Need of securing cloud Architecture

The Internet was outlined basically to be strong; it was not intended to be secure. Any circulated application has a much more noteworthy assault surface than an application that is nearly hung on a Local Area Network. Cloud computing has all the vulnerabilities connected with Internet applications, and extra vulnerabilities emerge from pooled, virtualized, and outsourced assets. Regions of cloud computing that they felt were remarkably troublesome:

a. Data integrity
b. Auditing
c. e-Discovery for lawful consistence
d. Privacy
e. Recovery
f. Regulatory agreeability

Your dangers in any cloud sending are needy upon the specific cloud administration model picked and the sort of cloud on which you send your applications. To assess your dangers, you have to perform the accompanying investigation:

1. Figure out which assets (information, administrations, or applications) you want to move to the cloud.

2. Focus the affectability of the asset to hazard. Hazards that need to be assessed are loss of security, unapproved get to by others, loss of information, and intrusions in account.

3. Focus the danger connected with the specific cloud sort for an asset. Cloud sorts incorporate open, private (both outer and inward), half and half, and imparted group sorts. With each one sort, you have to consider where information usefulness will be kept up.

4. Consider the specific cloud administration display that you will be utilizing. Distinctive models, for example, IaaS, Saas, and PaaS require their clients to be in charge of security at diverse levels of the administration stack.

5. In the event that you have chosen a specific cloud administration supplier, you have to assess its framework to see how information is exchanged, where it is put away, and how to move information both well and done with the cloud. You may need to think about building as a flowchart that demonstrates the general system of the framework you are planning to utilize or are presently utilizing.

One method for keeping up security is to have "golden" framework picture references that you can come back to when required. The capacity to take a framework picture disconnected from the net and investigate the picture for vulnerabilities or trade off is precious. The bargained picture is an essential legal sciences device. Numerous cloud suppliers offer a depiction emphasize that can make a duplicate of the customer's whole surroundings; this incorporates machine pictures, as well as applications and information, system interfaces, firewalls, and switch access. In the event that you feel that a framework has been bargained, you can supplant that picture with a known decent form and contain the problem. Many sellers keep up a security page where they list their different assets, confirmations, and qualifications. One of the more created offerings is the AWS Security Centre, where you can download a few backgrounders, white papers, and detailed analyses identified with the Amazon Web Service's security controls and instruments.

2. Benefits of securing the cloud architecture:

This is not to recommend that your information is unsecure on the cloud. Suppliers do try to guarantee security. Something else, verbal and rehash business will wilt up. Yet the very nature of the cloud loans it to requiring some exceptionally solid security rehearses.

2. Centralized Data

We've discussed the phantom of information misfortune by being in one spot. Notwithstanding, there are some great security qualities that accompany incorporating your information. Just in practice, you make your framework all the more inalienably secure.

3. Reduced Data Loss

More than 12,000 laptops are lost in American airplane terminals consistently. It's awful enough to lose your information, however it’s particularly terrible for organizations that lose exclusive information or other mission-discriminating data.

Likewise, what number of laptops utilizes truly solid efforts to establish safety, in the same way as entire circle information encryption? On the off chance that the smart phone can be successfully traded off, the data will be in the hands of the hoodlum. By keeping up information on the cloud, utilizing solid access control, and constraining worker downloading to just what they have to perform an undertaking, distributed computing can restrain the measure of data that could conceivably be lost.

Observing if your information is kept up on a cloud, it is less demanding to screen security than need to stress over the security of various servers and customers. Obviously, the risk that the cloud would be broken puts all the information at danger, yet in the event that you are aware of security and keep up on it, you just need to stress over one area, as opposed to a few.

4. Instant Swap over

On the off chance that your information is bargained, while you are leading your examination to discover the guilty parties, you can in a flash move your information to an alternate machine. You additionally don't have to invest the time clarifying to your C-level administration that the framework will be down because of an occurrence. When you perform the swap over, its consistent to your clients. You don't need to invest hours attempting to imitate the information or fix the break. Abstracting the equipment permits you to do it immediately.

5. Logging

In the cloud, logging is moved forward. Logging is normally considered late in the amusement, and issues create with storage room. On a cloud, you don't have to think about the amount stockpiling you'll need and you will probably keep up logs from the get-go, if for no other explanation than to check your utilization. Likewise, you can utilize more praiseworthy logging procedures. For example, a C2 review trail can be utilized. This is by and large seldom utilized as a result of the execution hit your system would take. Notwithstanding, in the cloud, you can achieve that level of granularity.

6. Secure Builds

When you created your own particular system, you needed to purchase outsider security programming to get the level of insurance you need. With a cloud arrangement, those instruments can be packaged in and accessible to you and you can create your framework with whatever level of security you covet.

Additionally, you can perform your patches and updates disconnected from the net. As you fix a server picture, you can keep it safe disconnected from the net, and when you are prepared to put the virtual machine on the web, you can advantageously do that. At last, the capacity to test the effect of your security changes is upgraded. You just perform and disconnected from the net test the form of your creation surroundings. This permits you to verify the progressions you make aren't negative to your system before you put it on the web.

6. Improved Software Security

Sellers are prone to create more effective security programming. Since you're charged for your CPU cycles, you're going to perceive and screech if the cost is excessively high. Thusly, the seller would like to lose your business and is going to be more slanted to create more productive security programming. Also, the merchant will be prone to take a gander at the whole security setup and tune wherever workable for a more proficient framework. They realize that the security merchant who conveys the more proficient item will win.

7. Security Testing

Saas suppliers don't bill you for the greater part of the security testing they do. It's imparted among the cloud clients. The final result is that on the grounds that you are in a pool with others (you never see them, yet they are there), you get to acknowledge lower costs for security testing. This is likewise the case with PaaS where your designers make their own particular code, yet the cloud code–scanning instruments check the code for security shortcoming.

IV. Solution Methodology

1. **Single cloud architecture**

Users are using multiple accounts and also having various service providers with different username and password. So in that case network user uses the same password everywhere, which may inherent security risks. It may cause user to lose throughput and also overhead. Therefore today enterprise uses Single Sign On technology to address the password eruption. Organizations are suggested to use SSO for cloud purpose to modernize security management and apply strong authentication. User can access multiple applications and services using a single login in cloud environment and thus facilitate strong authentication at user level.

2. Defense in Depth Security Approach

Security tools like firewalls and email gateways, has evolved into adding virtual private networks(VPNs), virtual local area network(VLAN) segmentation, authentication and intrusion detection systems(IDS) which are essential to handle growing number of threads in corporate network. Virtual firewalls appliances should be used which allow network admin to check all level of traffic. IPS is used to protect network from internal threads.

3. Increase Availability

Availability is use to analyze the system is working properly. Cloud service can be accessed all the time, even during failure and maintenance. In that case data can be available all the time and reducing the time when network is not working and increases throughput. This is possible by using high availability technologies in network infrastructure as active/active clustering, dynamic server load balanced and ISP load balancing.

4. Data Privacy

Now bray et al. proposed a client based privacy management tool that provides model that is user centric to control information of user in cloud database. Data loss prevention (DLP) helps in controlling migration of data at cloud and it also identifies if some sensitive data is leaked.

5. Data Integrity

Data communication cost is high therefore user don't want to download data but user can change the data capacity in cloud server with CSP (cloud service provider) in his request. Storage level must be flexible as its design and structure is concerned.

6. Virtual machine protection

We can't protect cloud using virtual machine by using firewalls and antivirus. They should be insulated from other network segment to protect virtual machine. Illegal internal access is restricted by using intrusion prevention systems and unauthorized external access should be protected by using secure remote access technologies like IPSec or SSL VPN.

7. SSL VPN(secure socket layer virtual private network)

An SSL VPN (Secure Sockets Layer virtual private network) is a VPN that can be used with a standard web browser. As compared to the traditional IPsec (Internet Protocol Security) VPN, an SSL VPN does not require you to install specialized client software on end users' computers.

SSL is a protocol for managing the security of message transmission on the Internet. SSL is included as part of popular web browsers and most web server products. It employs a public and private key encryption system from RSA.

An SSL VPN cloud computing connection between your data center and the cloud provider secures your data without a lot of the Public Key Infrastructure (PKI) overhead that comes from an IPsec-based VPN solution. Most SSL VPN gateways provide an on-demand client, so there's very little management overhead on the client side and it's easy for the end user to use.

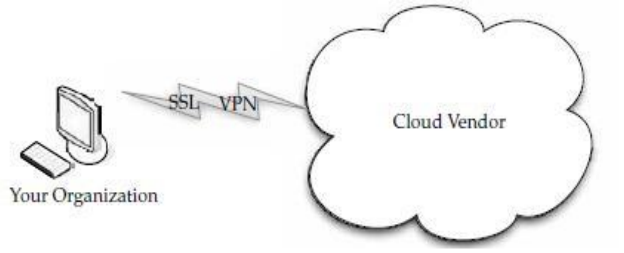
Better Security Practices:

An SSL VPN also makes sure that end users are compliant with your organization's security policies through the use of endpoint security. Those measures include:

- Requiring antivirus software to be running
- Verifying that OS patches have been installed
- Checking to see if malware or bots are running

The SSL VPN is a great security solution because it secures access to your applications in a simple, inexpensive, and efficient way. And if you were so inclined, you can offer your employees more chance to telecommute.

Fig: SSL VPN secure cloud architecture



8. Security mapping:

The cloud service model you choose determines where in the proposed deployment the variety of security features, compliance auditing, and other requirements must be placed. To determine the particular security mechanisms you need, you must perform a mapping of the particular cloud service model to the particular application you are deploying. These mechanisms must be supported by the various controls that are provided by your service provider, your organization, or a third party. It's unlikely that you will be able to duplicate security routines that are possible on-premises, but this analysis allows you to determine what coverage you need.

A security control model includes the security that you normally use for your applications, data management, network, and physical hardware. You may also need to account for any compliance standards that are required for your industry. A compliance standard can be any government regulatory framework such as Payment Card Industry Data Security Standards (PCI-DSS), Health Insurance Portability and Accountability Act (HIPPA), Gramm–Leach–Bliley Act (GLBA), or the Sarbanes–Oxley Act (SOX) that requires you operate in a certain way and keep records.

Essentially, you are looking to identify the missing features that would be required for an on-premises deployment and seek to find their replacements in the cloud computing model. As you assign accountability for different aspects of security and contract away the operational responsibility to others, you want to make sure they remain accountable for the security you need.

9. Multicloud architecture

Single cloud is less mainstream in clients because of danger of administration accessibility disappointment and probability of malignant insiders in the single cloud. Multi-cloud methodology is the utilization of two or more cloud to minimize the danger of administration accessibility disappointment, Loss and debasement of information, loss of protection, seller lock-in and the likelihood of malignant insiders in the single cloud. The administration inaccessibility can happen because of breakdown of fittings, programming or framework base. A multi-cloud procedure can likewise enhance general venture execution by evading "merchant lock-in" and utilizing diverse foundations to help differing accomplices and clients. The expense of utilizing various mists will be higher than that of single mists. Hence unless and until there is an outline which can make utilization of multi-mists without expanding expense, the implementation will be very unrealistic.

10. Depsky architecture:

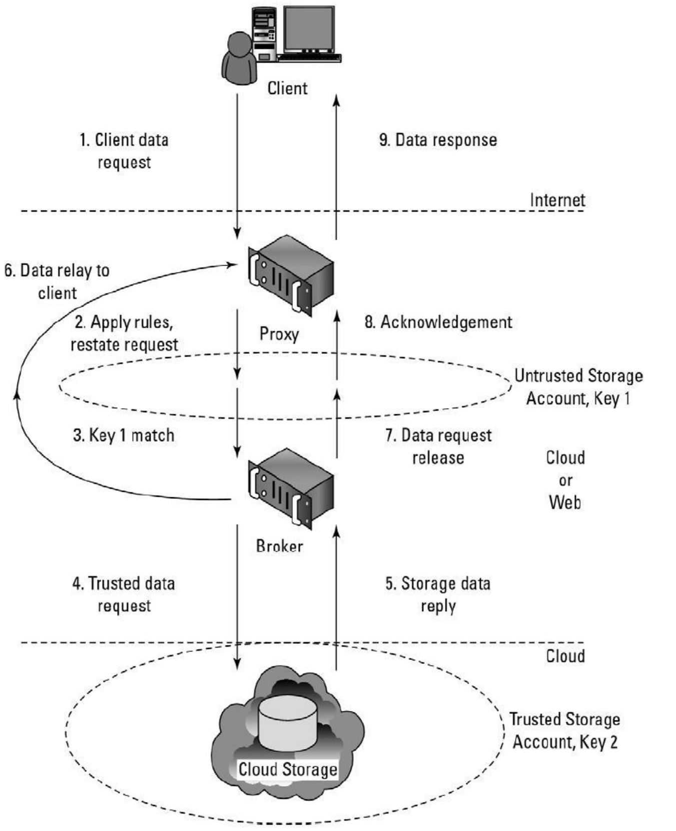
Depsky is one such building design plan that conquers all the impediments of multi-mists by taking out the prerequisite of code execution in the servers (i.e., capacity mists). It is still effective as it requires just two correspondence round-outings for every operation. Likewise, it manages information secrecy and lessens the measure of information put away in each one cloud. It utilizes an effective set of Byzantine majority framework conventions, cryptography, mystery offering, eradication codes and the differing qualities that originates from utilizing a few mists. The Depsky framework model contains three sections: reader, distributed, and number of cloud storage suppliers, where writer and reader are the customer's undertakings. A. Bessani et al., clarify the distinction in the middle of writer and reader for cloud storage. Reader can come up short self-assertively (for instance, they can fall flat by smashing, they can fizzle every once in a while and afterward show any conduct) though, authors just fizzle by slamming.

V. Discussions

Considering the points raised in the previous section, a straightforward conclusion is that cloud security includes old and well-known issues – such as network and other infrastructural vulnerabilities, user access, authentication and privacy – and also novel concerns derived from new technologies adopted to offer the adequate resources (mainly virtualized ones), services and auxiliary tools. These problems are summarized by isolation and hypervisor vulnerabilities (the main technical concerns according to the studies and graphics presented), data location and e-discovery (legal aspects), and loss of governance over data, security and even decision making (in which the cloud must be strategically and financially considered as a decisive factor).

Another point observed is that, even though adopting a cloud service or provider may be easy, migrating to another is not . After moving local data and processes to the cloud, the lack of standards for protocols and formats directly affects attempts to migrate to a different provider even if this is motivated by legitimate reasons such as non-fulfilment of SLAs, outages or provider bankruptcy . Consequently, the first choice must be carefully made, as SLAs are not perfect and services outages happen at the same pace that resource sharing, multi-tenancy and scalability are not fail proof. After a decision is made, future migrations between services can be extremely onerous in terms of time and costs; most likely, this task will require an extensive work for bringing all data and resources to a local infrastructure before redeploying them into the cloud.

Finally, the analysis of current trends for cloud computing reveals that there is a considerable number of well-studied security concerns, for which plenty solutions and best practices have been developed, such as those related to legal and administrative concerns. On the other hand, many issues still require further research effort, especially those related to secure virtualization.



VI. Conclusion

Both the cloud service provider and the customer should make sure that the cloud is safe enough from all the external threats, so there will be a strong and mutual understanding between the customer and the cloud service provider. The largest gaps between cloud security practice and cloud-security research theory lies in the fact that the assumptions in the research leave out some very important differences between actual cloud security and virtual machine security. Research should be centre on these gaps and differences and its removal. One of the pieces of the framework might be developing a way to monitor the cloud's management software, and another might be development of isolated processing for specific clients' applications. People's behaviour can be tracked and monitored for instance whether people allow the automated patching software to run, or updating anti-virus software definitions, or whether people understand how to harden their virtual machines in the cloud.

References

[1]. Nazia Majadi,” Cloud Computing: Security Issues and Challenges”

[2]. Grobauer B., Walloschek T. and Stöcker E., "Understand-ing Cloud Computing Vulnerabilities," *IEEE Security and Pri-vacy*, vol. 99, 2010.

[3]. Subashini S., and Kavitha V., “A survey on security issue in service delivery models of cloud computing.” *JNetwork Comput Appl* doi:10.1016 2010.07.006.

[4]. Grobauer B., Walloschek T. and Stöcker E., "Understand-ing Cloud Computing Vulnerabilities," *IEEE Security and Pri-vacy*, vol. 99, 2010.

[5]. Balachandra Reddy Kandukuri, Ramakrishna Paturi V and Dr. Atanu Rakshit, ―Cloud securityIssues‖ 9780-7695-3811-2/09 2009, IEEE computer society.

[6]. Available from: http://en.wikipedia.org/wiki/Cloud_computing.Last visited on the 15th October, 2014.

[7]. Nazia Majadi, “Cloud Computing: Security Issues and Challenges” International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013.

[8]. W.Sharon Inbarani, C.Kumar Charlie Paul, W.Andrew Jerome Jeevakumar,” A Survey on Security Threats and VulnerabilitiesIn Cloud Computing”- International Journal of Scientific & Engineering Research, Volume 4, Issue 3, March -2013

[9]. Mervat Adib Bamiah, Sarfraz Nawaz Brohi, “ Seven Deadly Threats and Vulnerabilities in Cloud Computing,” *IJAEST*,2011, pp. 87-90.

[10]. Security Guidance for Critical Areas of Focus in Cloud Computing, April 2009. DOI= http://www.cloudsecurityalliance.org/topthreats/csathreats.

[11]. The National Institute of Standards and Technology (NIST), Information Technology Laboratory definition of Cloud Computing by Peter Mell and Tim Grance, version 15, October 2009.

Authors Profile

Asha Kumari received the **B.Tech.** degree in CSE from the Singhania University Pacheri Bari ,Rajasthan India, in 2014.Currently doing **M.Tech.** in CSE in VIT University ,Vellore, India. His research interest includes Neural fuzzy logic, Communication networks

Sonam received the **B.Tech.** degree in IT from the Banasthani University Newai,Rajasthan India, in 2013.Currently doing **M.Tech.** in CSE in VIT University ,Vellore, India. His research interest includes Neural Networks and fuzzy logic, Communication networks

Kalyani Singh received the **B.Tech.** degree in IT from the Uttaranchal institute of technology Dehradun India, in 2013.Currently doing **M.Tech.** in CSE in VIT University ,Vellore, India. His research interest includes Neural Networks and fuzzy logic, Communication networks