12. SECURITY

As promising as it is, cloud computing also faces various security issues, which include access of sensitive data, data segregation, privacy, authentication, identity management, policy integration, bug exploitation, recovery, accountability, visibility under virtualization, malicious insiders, management console security, account control, and multi-tenancy issues (Phankokkruad M., 2012).

There are many security challenges for cloud computing because it encompasses many technologies, which include networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management. Therefore, security issues for these systems and technologies are applicable to cloud computing.

As the ownership and operations of each layer of the cloud are distributed between service providers and clients; security responsibility of the data in the cloud faces the biggest challenge. In this chapter, we look into the factors that can affect security and the support the system to be available to ensure security.

The security of the cloud is ensured in many levels, but the scope of intrusions makes it necessary to understand the factors that affect cloud security to ensure that it is a usable system of advanced data processing by all industries and the resistance that is faced by some sectors towards cloud computing is broken down.

The momentum of cloud computing makes it an enormous and essential requirement to study these factors and arrive at solutions.

- **Range of Cloud Devices**

The range of cloud devices has added to the requirement of expanding the security operations of each layer of the cloud. The cloud is available through not only computers, mobiles, smart phones but and gadget that can be connected to the Internet by service providers. This increases the task of having to ensure that databases are not cracked by using any one of the ranges of devices that can perform cloud functions.

- **High-Speed Broadband Access**
The cloud has one vital area that is the broadband access that it requires. This access is now available easily through service providers and has substantially increased the security risks as of now.

- **Data Centers and Server Farms**

Cloud services require large computing facilities, and the data is distributed through server farms connecting multiple locations of geographic distribution without any break in link through the Internet. It also has brought with it’s speed the ability of accessing the data during the access or connection route as well as from the number of locations that provide cheap servers.

- **Storage Devices**

The huge data storage capacity of the cloud has enabled companies to store their data in the cloud's infrastructure which effectively means that the companies do not have direct control over their own data. The storing capacity has given rise to the change from the fixed direct access storage device (DASD) to storage area networks (SAN)s.

- **Cloud Delivery Model**

The cloud delivery model leaves scope for data access, especially in the public cloud formation and the hybrid cloud formation when new features appear that may not be compatible to the applications written and might change the action of the instruction because of the new features that appear.

**12.1 Infrastructure Security**

This must not be confused with the SaaS infrastructure security by non security persons as the dimensions of the infrastructure are far larger than that. This security concern in infrastructure is when the client starts the migration of the data to the cloud formation.

**12.2 Network Level**

A private cloud client will have the tools necessary to protect the data and the entire infrastructure s it will be inbuilt into the private cloud for the sole use of the client only. There is greater cloud security in a private cloud as compare to public cloud, community cloud and hybrid cloud.
The security infrastructure takes on an entirely different dimension when it is a public cloud, and this is an area of concern because of the accessibility and the ability to bypass regulators and export data or import data. It also has to be worked out how the client’s network topology will interact with the service providers’ network topology; there interaction sometimes gives leaks in data accessibility. There are four different risks involved in this case:

- To ensure the integrity and the confidentiality of the data this is in traNIST to and from the public cloud provider.
- To ensure proper access control and its secure level with the access that the service provider provides to access the data in the cloud.
- To ensure the availability of the Internet access to the cloud that the service provider is putting the organization on to access the data.
- To replace the existing network with domains.

12.3 Data Confidentiality and Integrity

Resources and data that were confined to a private network are now in a public domain belonging to a third party cloud service provider which, in effect, means that a client organization has to handover licenses to the service provider without fully being sure that it might be used for other purposes without the knowledge of the client organization.

It is also important to have agility between different cloud providers to avoid a lock in; service providers, on the other hand, should not release their client data to any agency without the specific approval of the client organization.

The inability to pinpoint the geographical location of a user profile can also create security risks for the client organization as the warning alone from the PaaS security system is not enough to lock down the intruder. By the time the location is identified the intruder has probably accessed his requirement and logged out.

This aspect of being able to access data from any location is a benefit but with it one must also have the security structure in place before putting the data of the organization into the hands of the service providers.
The layers of the cloud’s infrastructure have their own security systems in place, but it still know absolutely clear how the three security systems interact or what is the full extent of the interaction. Again this is a grey area as it also depends on what kinds of applications have been written and which service provider is providing the service. Cloud security is basically about risk management. There are many challenges in the security system still, and cloud computing is evolving rapidly to find the solution to all the challenges that are still apparent in cloud computing security.

Many companies that need secure data storage such as in financial institutions to avoid losses that sometimes run into billions of dollars the security is the first concern. It is evident that the business world is becoming more and more uncertain as the news systems of cyber threats emerge. Systems are unable to deploy the systems that have been used earlier to protect then data systems or the leaks that take place. There are so many areas that require data security that one must understand the entire aspect of infra-structure security to know how to secure the system and the storage of data in the cloud.

12.4 Government and Risk Management

Compliance of regulations and government requirements are essential to ensure that during any confusion, the government can be relied upon for support and action to the best of their ability. Despite the security measures that the service provider provides to the client organization it is still important to have an offsite back up by the organizations to ensure that there is no lock in or freeze on their database for any reason. In the case of any eventuality, the company should be able to rely on a third party data storage or be able to shift data from one service provider to another within minutes in the case of pre-tempting any type of data freeze.

12.5 Data Residency and Jurisdiction

The jurisdiction of the data is another area that remains unclear and is open to interpretation. The organization could be in one country. The business requirement could be in another country, and the dispute could be in yet another country from where the client organization operates. In such a situation, it is an opportunity to interpret the situation and the stance and keeps the database mobile moving from one storage provider to another to avoid detection.
On the same classification, there is also the security issue of the data residency which at times is hard to ascertain because the security requirements where the organization is may have one set or compliances, where the data is stored that location could be having an altogether new set of regulations, and the location of the actual business functions would require further regulatory compliances and all because it raises the question of the data residency.

12.6 Compliance and Audit

From the above we understand the complexities of jurisdiction and also regulatory compliances. It is quite clear that client organization will be subjected to at least three sets of regulatory compliances of not more be able to secure the database of the organization and also to be able to access it.

How do the internal auditors audit the organization when the data is not stored in the actual premises physically is a question that challenges all types of solutions for it? Secondly, in external audits the client organization will be subjected to at least two external audits of different locations. Besides being a time-consuming process the organization has to be subjected two at least two sets of compliances at the minimum.

12.7 Access Control

The methods of access control must be very secure and the authentication process as well as the authorization process must be without a weak link. A weak kink would mean a leak in the security system which would also mean that intruders and hackers can access without the organization even knowing. Most of the activities take place at night, which also means that the security provider has to be alert to the period of such happenings.

12.8 Shared Resources and Data Segregation

Shared resources are another area that needs to be securities the reason being that the same data is running on several virtual machines at the same time. The contention of shared resources is when the data has an impact on the non-deterministic levels on the performance behavior of the Virtual machines and the platforms.
12.9 Security Incident Management

The process of segregating data into several servers for better utilization also lays open the security system during the process of data segregation. During the process itself, it is possible to add another server to the multiple servers that are already receiving the segregated data. Segregation of data takes place internally inside the private cloud of the client organization.

In the public cloud, however, the It operations wants to start up a separate application, but IT compliance wants a control over the database also which is why clients are waiting to see what the outcome of this trend will be before they commit to the cloud migration process.

The purpose of segregation is entirely for security reasons. Data needs to be segregated so that in the advent of a legal issue the cloud provider the data and also the client organization have a better hold in the legal mandate requirements.

Many closely-held companies have not yet put their data in the cloud process because they feel that the storage of data in a cloud will lay the company open to provide their data against a legal mandate whereas under the regulations for companies, a closely held company does not have to make it’s financials or any aspect of it’s functions public.

12.10 Physical Security

Anyone who has access to the cloud service provider has access to the client organizations’ data. Security is not just virtual there is a host of physical activities that are necessary to secure the data. Insiders can also be a threat. Server thefts from data centers in 2008 hit the industries the world over. Besides the costs of bribery for data are very low it never goes beyond a few hundreds of dollars, it. However, it had been in millions that would have been a deterrent in itself. The fact that is most often overlooked is that for all the bullet-proof systems to secure the database in a cloud all that is required to circumvent this issue is a legal mandate or a simple official piece of paper from the government in power. In June 2011, Instapaper lost the use of their server because the FBI decided they needed it to hunt down spies and terrorists.

Along with moving to the cloud computing process for efficiency, storage, speed and perhaps around the clock optimization what the client organizations need to remember
is that are effectively giving up the full control of their private data as of today when they move to cloud processing. Even the encrypted data to be moved to the cloud as to be decrypted first four applications and that puts the data in a physical danger of being stolen. No matter how securities the data and the process are the physical security needs do not get diluted because they are in a cloud formation, in fact. How can one be sure as the data is being managed by an outsider who is the service provider, and in the case of a breach of trust under what sections of law do you hold the service provider accountable, who has the possession of the data? Who can claim ownership of the data when an incident takes place?

However, these questions have been arisen at a certain level of security solutions, and so one cannot trust the memory of a CPU either unless it is encrypted!

12.11 Privileged Access

A privileged access user is someone who has access to an organization’s sensitive data because the IT functions and the database storage has been outsourced to an external cloud unit, and the management of that data is done by a data administrator. Now virtually and physically an external person is an internal person who has the privilege of accessing the company’s data without repeated access requests.

This is a danger for the client organization as earlier discussed. Trust levels are thin layers and when to come to government agency compliance. How long would it take for the service provider to release the data of the client organization so that it can save itself and ensure that none of its servers will be held captive by government agencies in their constitutional capacity.

12.12 Continuity Services

The key benefit of the cloud is that it allows the continuation of services at a very high speed. The cloud continuity is a feature that has great importance when it comes to a period of recovery from a disaster.

As compared with the cloud the traditional methods of recovery are very expensive and this is why most client organizations have migrated or are in the progress of migration because of the facilities that are offered in the continuity of services.
With the servers located in various locations, and the geographical proximity is not a necessity the client required can be moved from one location to another so that there is no breakdown in service and this also helps the security requirement because during a break down the chances of breaching a client.

Organization is easier than when it is in the process of a continuous service. Continuity of a system is needed to ensure that the system’s chance of being outraged is less than when there is a disaster. The problem that arises in this area is like when the modesty of a woman is outraged, there is an outrage, there is evidence of an outrage, but defining it in terms to pinpoint the offender is hard to come by. For this reason, it is important to maintain the continuity of the services so that the environment of the system is secure at a least as secure as it can be as of today.

In this particular segment of security, it is important to understand the service level agreements that have been signed, and everything should be thrashed out before instead of finding that the client organization has to read between the lines of every sentence to really be able to grasp the full extent of the continuity that can be provided as well s the security environment in which it will be provided.

Privileged data is precious to all companies and many things are best left, unread and unseen. One needs a very secure environment to function without insertions of disciplinary action, and every level of service provided by the cloud.

Every client organization has critical business functions and these critical functions just freeze altogether without the feature of almost 99.99% continuity that the service providers are able to provide the client organizations when they migrate to the cloud computing system.

**12.13 Data Disposal**

A critical part of securing intellectual property is data disposal. It is important to eliminate data that is no longer required. Failing to do so can breach data disposal policies and also compliance problems, which means added costs for the client organization? There are basically three options of destroying data. One option is overwriting, which can cover up old data with new one, degaussing, which erases the magnetic field of the storage media and physical destruction which means employing physical means like destroying a disk or shredding a disk.
The data destruction market has not much transformed in the past few years. There are no new methods have yet come out, but only new technologies for old methods are implemented. Different companies use distinct method of data destruction but whatever the combination of data destroying method it will be one of the three existing methods until a new method comes out. 69% of data that is stored according to David Hill is data that is unnecessary. The data may be useless but the storage space costs IT money, and it is important to reduce the amount of data that is stored, when the company does not have any requirements for it.

It makes economic sense for and also security sense to destroy data and reduce the amount of data in the storage space of the company so that particular space can be sued for data that is required for the processes of the client organization.

12.14 Injection Based Attacks

Injection's vulnerabilities allow a malicious and vindicator to insert specific commands into the application or code of the system so that the behavior becomes abnormal and outside the behavior pattern that should be seen. The attacks usually exploit a system when it asks for commands to process something at a later date. The most common types of injection consist of SQL injection, command injection, Cross site scripting as well as path and LDAP scripting.

Zero-day malware which is hard to detect, and at the same time it is hard to understand the full impact and when one cannot understand the full impact, one cannot understand the full implications either. There are so many versions being developed, and many companies have landed looking down into the barrel and still not realizing that it is all gone!

Cyber-criminal mentality is very specific. They are generally very impatient and prefer to go for soft target in which they can access the data immediately and quickly covering the risk involved. On the same not it is possible for the company to also cover it’s data from intruders. It is not a question of putting in tough security systems that are as far as can be seen bullet proof. It is a question instead of putting in a complex system that will take time to crack, and the usual algorithms will not work. Complicating the intrusion into a system puts an intruder off in general. The cybercrime mind gets putt off and looks for targets that are less lengthy and time
After discussing the security parameters, we can say that:

- The cloud security environment is as fluid as the clouds in a real sky. However, the cloud environment in the entire infrastructure is fairly secure so long as the applications are not injected or the system is not broken into by hackers and information spies.
- Every component of cloud component can be secured except the security as it stands today even though there are existing solutions and better technology coming up. The area of cloud security will require are larger areas of more complicate security systems as the new cloud formations are confirmed.
- The system environment is safe but the environment in which it is functioning is not entirely safe, which are difficult to address unless:
  - A cyber-criminal is given high rewards for cracking an intruder’s security instead of their own.
  - Unless the security providers and the legal interpretations of do’s and don’ts of cloud computing become clearer.
  - No doubt more and more organizations are going to get into cloud computing, and then we will have to find a solution to the who’s who list not in the Fortune 500 but who’s who list in the cloud 500 lists.

There is every possibility that the larger players may receive tremendous backing in the form of investments to be able to buy air space to function within without government regulations and external audits suddenly swooping down on their database. This would not be just a virtual exercise but a physical reality and hence the entire cloud environment not just the process but the service provider, and the system will be owned by one big private cloud owner or a hybrid cloud which of course will make the system and the security environment bullet proof!