# Security Challenges in Cloud Computing

Sarthak Kathuria, Souradeep Banerjee

**Abstract**- Cloud computing is a rapidly developing internet dependent technology that is becoming increasingly popular day by day due to the vast amount of advantages it brings along with itself. Its main idea is centered on providing highly scalable computing services, storage or application-based services via the internet on demand and on a pay-per-use basis. Security issues such as data theft, data loss is very much prevalent these days. Natural disasters lead to the damage of the cloud data servers leading to permanent loss of important information. Sometimes it also happens that cloud service provider don't use their own servers for data storage and rent the same for flexibility.

**Index Terms**—Cloud Computng, Cloud Security Issues, Intellectual Property, Deployement Model, Identity Management System, SQL Injection, Denial of Service.

## 1 INTRODUCTION

With the progression of time, IT (Information Technology) industries and Digital information dependent businesses keep on driving technology from one stage to a new one. For instance, the Internet was developed due to this need of IT community to find a better and effective way of communication and data transfer and hence the result is one of the most popular technology now-a-days which has allowed the global interconnection of a huge number of systems and users and facilitated the sharing and managing of resources and data from anywhere and anytime.

Cloud computing has surfaced as another such technology which aims to bring about a revolution in terms of internet-based services and how we handle resources and acquire them. But cloud computing just didn't prop up as a wild out of the box idea. Rather it is a result of years of attempting and trying to figure out a way to release users from the needs and limitations forced on them by IT Infrastructure including computer hardware, storage and software. The attempts lead to conceiving of various technologies like time-sharing utilities in 1960s and development of network computing and commercial grid computing in 1990s. These technologies served as predecessors to cloud computing which is the latest brainchild of the ideology which is shares with these technologies. This ideology has since progressed from just to better organize infrastructure and decrease the burden on the users to include requirements of increasing the capabilities of a system on fly without having to invest in new infrastructure, licensing of any new software or training of new personnel.

Cloud computing model's central ideology is based around providing easy, affordable, on-demand internet or network-based access to a remotely available pool of configure as pre-requirement computing resources such as networks, storage solutions, servers and applications that can be provisioned quickly and dispatched with minimal management effort or human resource usage. By doing so, they also ensure that they are able to reduce overall client-side requirements (hardware and software) and complexity as a whole. Although initially this idea was confined to only the academic and research area, it later was transposed and popularized in the industry by market giants like Microsoft, Amazon and Google by launching their own implementations of the idea. These are some of the Cloud service providers (CSP's) who, much in the same fashion to Internet Service Providers (ISP's) (who offer internet services to their customers), offer cloud platforms and virtualized computing resources for their customers to use and create their own applications and web services. In general providers of cloud services offer three broad categories of services which include: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service. These services which the cloud service providers host are delivered to the customers via internet which they access from servers through web browser. The past few years have seen many organizations both big and small move towards IT solutions that include cloud computing due to many of its attractive features and benefits like on demand and real-time availability of services and virtual infrastructure on a pay-per-use basis which means that the consumer of the resource will have to pay for the resources on consumption basis and not on the basis of the total duration of the lease. This makes it possible for new start-ups to enter the market. Also, it is not mandatory for the user to require a certain degree of knowledge or pre-mediated expertise to control the infrastructure or services leased from the cloud service providers as efficient abstraction is provided be the CSP's. Analogous to other services available on the internet, Cloud model also offers services with a high degree of scalability, higher throughput, good quality of service and high computing power. Due to its unparalleled advantages, Cloud computing has amassed a substantial following fairly quickly and is being adopted by all sorts of organizations and businesses regardless of their size to gain advantage in the rapidly changing markets to and to ensure that they are always maintain their position on the leading edge of technology and keep on dispensing fruitful services to their consumers. are introduced by the usage of cloud computing, but a great deal of risks and issues are also associated with implementation, management, disaster recovery, business continuity, regulation and legislations and lack of standards and guidelines in cloud computing technologies.

Many IT watchdogs have cited that security and the paranoia surrounding them is the top challenge which is preventing adoption of cloud of a wide and popular basis services. Management of cloud services always under pressure to ensure adequate mitigation of risks to reduce the negative impact they have on business. The above-mentioned risks come into picture as a result of various nuances and provisions of the cloud computing model such as outsourcing the user data to remote

servers which are owned and run by the cloud service providers. This raises a question over the trust worthiness of the CSP and leaves the security of User's data compromised. Also, other security challenges such as – web application vulnerabilities, SQL (Structured Query Language) injection and cross-site scripting exist which puts the user Data at risk. This is in addition to physical access and privacy control issues that rise up as a consequence of third-party control over physical data, identity and credential management procedures.

This Chapter study will focus primarily on highlighting the various security issues and challenges that exist due to cloud service delivery models and to discuss some workarounds and preventive measures to mitigate and minimize the risks and security lop holes involved with the use of cloud computing technologies.


Fig 1: Cloud Computing and its various physical components

This paper is organized as follows:
First of all, we will discuss the various security challenges that are rampant in the cloud service models like DDOS attacks, Data Breaches, Data Loss, Insecure Access Points, etc. We will also discuss the absence of transparency to the cloud users which is a major source of customer discontent and then move onto the challenges related to cloud service models and various network capabilities and the possibilities they possess. After the various challenges have been highlighted, we move on to deliberate upon the various solutions to the various security loop-holes present. Finally, we conclude the chapter report with a summary of the things that have been discussed throughout the report.

Cloud computing is a powerful technology that uses the idea of storing data across the internet rather than locally. It also helps the customer to pay as per usage. All the resources such as Datacentres, servers, storage devices, networking devices are being virtualized into one single platform and provide service to the users using various cloud service modules such as SaaS, PaaS, IaaS and XaaS. As per a recent survey the value of the cloud market has gone up to $210B in 2016, whereas it was only $76.9B in 2010. Cloud Architecture provides with four types of deployment models- Public, Private, Hybrid and Community cloud. Based on the needs, customer can choose the deployment model which suits his organization. Despite Cloud Computing being such a powerful tool, there are some flaws in the system which makes the users to think twice before opting for it. Many reasons are there which makes it risky for the users to use cloud for storing their private data and information:

- Cloud Service providers doesn't have transparency in how user's data is being stored and handled.
- Existing security algorithms may not be able to provide protection against the newly emerging threats.
- There is every chance of unauthorized access of the user's data among the service providers which may lead to data leak.

These types of makes the user hesitate to use Cloud Computing as a solution for their organization and thus leads to the loss of Cloud Service Providers.

## 2 VARIOUS SECURITY CHALLENGES

### 2.1 Data Loss

As we need to store data sometimes. Hard drives were only pool to store few decades ago. Now in modern era we use to store the data in cloud because of its features likes affordable prices, massive storage and remote accessibility. Data keep within the cloud is lost for reasons apart from malicious attacks. Associate accidental deletion by the cloud service supplier, or a physical catastrophe like a fireplace or earthquake, will cause the permanent loss of client information unless the supplier or cloud shopper takes adequate measures to keep a copy information, following best practices in business continuity and disaster recovery. Due to massive usage of cloud however, the cloud data is vulnerable to threats as the internet as a whole.

### 2.2 Breach of Data

Breach of data may occur as a result of poor maintenance of the servers, poor management of security or intended attacks by the cyber-hackers. This data may contain information that was not meant to go public, or some data about the person health data, money data, in person classifiable data, or some other knowledge which may be of great value to some other organization. Possibility of data breach has highest possibility in case of cloud computing though it is not unique for this field only.

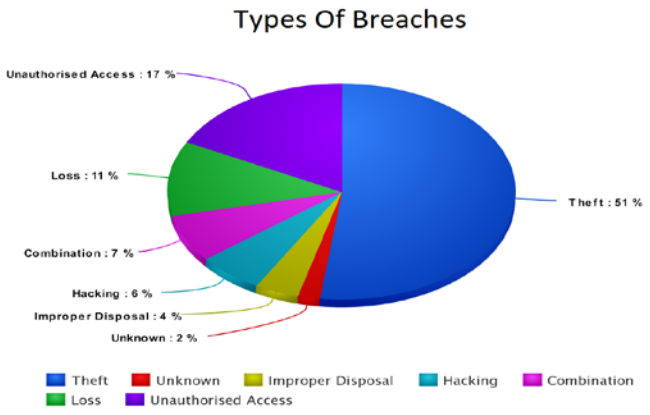



Fig 2: Different types of Breaches

### 2.3 Security Challenges

Security has the top most priority for any organization who is implementing Cloud services to resolve their storage issues. Data confidentiality, integrity availability are the various aspects of Cloud security that needs to be taken care of. Security issues related to deployment models, service modes and Network issues are being discussed below:

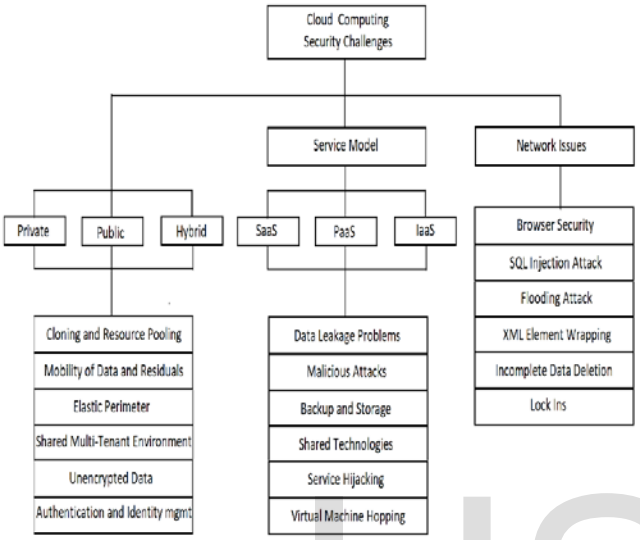



Fig 3: Different types of cloud security challenges

## 3 DEPLOYMENT MODEL CHALLENGES

Public, private, hybrid and community are the four main cloud deployment modules which are available for the users and depending on their requirements, they choose on of the above as a cloud computing solution. For the sake of improving accessibility inside an organization, a group of users and departments are being allowed to share the same resources but this leads to data breaching problems. Authenticity and Identity management is one of the toughest problems to handle in this case. Security issues mainly occur in public, private and hybrid cloud models. Various security problems related to the cloud computing models are being discussed below:

- Public Cloud: Public Cloud is being continuously being attacked with several hacking attempts. It has always been the target of most of the hackers, larger than private cloud. It also has the attention of the best security persons available in the market. Choice of CSP (Cloud Service Provider) plays a very important role here. The customer should have a well verified and defined SLA (Service Level Agreement) with the CSP. He should also take care of the facts that how much robust is the security provided by the CSP, security of the client being used on the Laptop or System for accessing the cloud, etc. The channel between the CSP and the customer also needs to be secure and encrypted since data has to cross multiple networks before reaching the cloud. Sometimes it happens so that the CSP are unable to describe the procedures followed by them for security reasons which makes the users doubtful.
- Private Cloud: Private Cloud is the most secure cloud development available in the market. Still there are some security issues in this deployment model which needs to be discussed:
  - Integrity and Security of the Hypervisor being used in this case must be taken care of.
  - Amount of automation being used needs to be under strict vigilance.
  - Deployment of new patches and configuration management must be properly dealt with.

  The organizations which have implemented Private cloud in their systems must ensure that they have full control of the new environment. Data such as health and financial data must be protected from unauthorized access when they are being accessed by international organizations.
- Hybrid Cloud: Hybrid Cloud is the most complex system of deployment module available out there. It is the combination of public and private cloud. Managing such a complex system requires a lot of experience and little experience may cause greater risks in this case. Another point is the coordination between the public and private CSP is good enough and both of them are in proper compliance with one another. Existing authentication and identity management systems much work on both the private and public cloud otherwise it may lead to security breaches.

| Model | Security issues | Cost issues | Control issues | Legal issues |
|---|---|---|---|---|
| Public | i)Least secure ii)Multi-tenancy iii)Transfers over the net | Setup:Highest Usage: lowest (pay for what you use) | Least control | Jurisdiction of storage |
| Private | Most secure | i)Setup: High ii)New operational processes are required | Most control | -- |
| Hybrid | Control of security between Private and Public clouds | -- | Least control | Jurisdiction of storage |

Fig 4: Issues in Deployement Models

### 3.2 Service model challenges

As demonstrated in this document, the numbering for sections upper case Arabic numerals, then upper case Arabic numerals, separated by periods. Initial paragraphs after the section title are not indented. Only the initial, introductory paragraph has a drop cap.

SaaS, PaaS, IaaS and XaaS are the different kinds of cloud service models which are available in the current scenario. But each of them has their own security vulnerabilities which are needed to be taken care of. Otherwise, data breaches may occur and users may have privacy issues.

- SaaS involves the use of Web browser for delivering applications. As we know, malwares are very much prevalent in the internet and if the web browser gets infected with such a malware then user loses control over the access of his data.
- In case of PaaS, developers use the hardware platform being provided by the cloud service providers and so the security of the PaaS applications must be maintained properly by upgrading them regularly. Legal issues related to data storage in different places must also be taken care of by the developer.
- In case of IaaS, user gets the required computer hardware from the Cloud service provider and then performs operation on it. Cloud service provider does not provide any reliability on where the data is being stored which means probability of physical attacks on the data storage environment is quite high.

### 3.3 Network Challenges

Network plays the most vital role in case of providing access to vast centralized resources which are being virtualized for the sake of cloud computing. Through network, users can remotely access these resources from their own system and do their work. But the use of word 'remotely' brings in the chances of various network attacks over the internet:

- Browser Security: When the user sends any login request through the web browser, the browser makes use SSL encryption for the authentication of the user. SSL uses point to point transmission and this means an intermediate host can decrypt the data. If a hacker makes uses of such an intermediate host and decrypts the login credentials of the user then he can login in to the server as a valid user and tamper with user data.
- SQL injection: SQL injection is a special type of attack being used by the hackers to retrieve data from the servers using special characters in the SQL queries. It involves modification of the server-side SQL query with some malicious code such as 'OR'1'='1'— which enables the attacker to override the authentication process and thus gain access to the database. This happens since 1=1 always return true and it may cause return of the full table. The worst possible things that an intruder can do with SQL injection are modification of the database, altering with the database's integrity, and even deleting the whole database.

- Flooding Attack: This type of attack is done by the hacker openly. A well know feature of the cloud computing system is vigorous scalability. The cloud system tries to allot as much resources as possible to server the incoming requests and as a result meet the clients' requirements. The hackers use the advantage of this feature. Flooding attack basically involves sending a vast number of illogical requests to the server at the same time which misleads the server to consume all the available resources to serve those requests and eventually be unable to serve normal requests of the users. At this point the hacker attacks the server with DoS.

- XML signature element wrapping: XML Signature is being used to sign a part of the SOAP web service request or message. The parts of the message which are being modified are being referenced with separate IDs in the message header. In order to validate the XML signature, the recipient must find the element in the request which has the same matching ID. XML signature wrapping attack involves a middle man who copies an existing SOAP body and inserts it into the header. He then alters the SOAP body according to his own request without changing the wsu ID. The recipient sees that the reference id is correct but he doesn't know about the alters being done internally. This leads to loss of privacy of the user internally without his notice.

- Incomplete Data Deletion: In case of cloud computing data is being stored in remote servers and copies of these data(replica) are also being stored in multiple sites for data availability and backup. Now there may be a scenario where user deletes a particular data that he doesn't want any more. In this case the cloud service provider needs to ensure the other replicas of the data are also being deleted at the same time. Otherwise they may be used for malpractices and thus result in unauthorized access.

- Locks In: One more problem in the network security is the vendor lock-in problem. If there is a need to move database of the customer from one cloud environment to another, it can't be done directly. At first changes done to the database for the previous cloud environment are needed to be rolled back and data base needs to be customer's site before mobbing it to the new cloud environment.

## 4 Susceptible issues in security

In spite of making a software top class and mostly secure, there is every chance of existence of some minor security bugs which may be exploited by the cyber hackers to tunnel their way through the system security and steal sensitive information associated with the customer. These security drawbacks put the whole system at risk along with all other services provided by the CSP. With the advent of multi-tenant solutions, services from CSPs are being integrated together and then being provided to the user thus opening up more possibilities of back-doors through which the hackers can easily establish their motives.

## 5 FURTHER INCESSANT THREATS

APTs or the Advance Persistent Threats that are a type of continuous and silent cyber-attacks that are being done on a specific entity. APTs are a type of self-learning mechanisms which develop and idea of the defence system mechanism supposed to stop them and then evolve over time to bypass those security firewalls. They camouflage their way into the network traffic to get hold of the specific information that it wants to steal.

## 6 INSUFFICIENT DUE DILLIGENCE

When executives produce business ways, cloud technologies and repair suppliers should be thought of developing a decent roadmap and list for due diligence once evaluating technologies and suppliers is important for the best likelihood of success. Organizations that rush to adopt cloud technologies and select suppliers while not performing arts due diligence expose themselves to variety of risks.

## 7 ABBUSE OF CLOUD SERVICES

Various instances such as poorly secured cloud deployment models, free trial periods of the cloud service providers, and fake account sign ups via fake payment methods may expose the system models to threatening attacks. Misuse of Cloud resources may lead to DoS-Denial of Service attacks, email spamming, etc.

## 8 DOS (DENAIL OF SERVICE)

DoS attacks is a specific type of attack which disables a user to access some of the cloud services or applications temporarily. It causes the cloud servers to consume more power, more memory, more disk space in order to serve the incoming requests from the attacker and thus being unable to serve the requests of other genuine user.

## 9 LOCATION OF DATA SEGREGATION AND DISPOSAL

Two more important matters to be taken care of in cloud deployment are location of the data and segregation. There may be some terms and conditions in the contracts that compels the CSPs to ensure that data is being held and processed in a very proper way. In this case there may be some vulnerabilities in the process which are needed to be taken care of:

1. Sometimes it may happen that the cloud service provider may need to handover data to some third-party authorities.
2. The CSP may require to pay taxes to the local authorities as a result of the earnings via data transactions.
3. Several natural calamities such as earthquake, floods, etc may lead to security threats for data of the customers.
4. Economic problems such as sudden rise in the price or sudden deduction of the same greatly affects the CSPs services and conditions.

Arrangements in Cloud Computing such as Central storage end up providing attackers with a rich and abundant target of information. This makes it possible for the attackers to swipe a considerable amount of information or gain access to confidential information of customer organisations in a single attack. Absence of adequate segregation of data may lead to many customers to find themselves suffering from a security breach due to an incident that should have, otherwise, been limited to a single customer. Virtualization itself is a run-time method of segregation for processing data and is one of a number of technologies which serve as an enabling foundation for cloud computing. Many of the security concerns and issues which are prevalent in the sphere of virtualization are also relevant in cloud computing as well regardless of whether the cloud service provider implements virtualization or not. Security of data thus falls upon having adequate security controls in each and every of the layers of the virtualized environment. In addition to that, secure freeing and relinquishing of memory and storage to prevent data loss is also important in a multi-tenant environment where systems need to be reused.

The hypervisor layers between the hardware and virtual machine / guest OS also has privileged access to the layers lying above themselves. It also now exerts a great deal of control over hardware since now the hardware manufacturers often implement hypervisor functions directly into chipsets and CPUs. Cloud users, therefore would like to have the facility to assess cloud service provider's operational features of the virtualization technologies and whether their risk profile can be tolerated.

Cloud service Providers that offer data storage facilities typically provide, by their specific Service Level Agreements, either guarantees service objectives that ensure high availability of that data. This is achieved by the Cloud Service Providers by maintaining multiple copies of the data. Cloud storage may not always be useful for those customers who intend to delete their data from the Cloud servers. Judging the type of data being saved in the cloud servers, users may need the CSPs to delete those data following industrial standards. In the case that the CSP doesn't use any policy that restricts the amount of media data to be stored on the server, the customer should himself implement some kind of media organization techniques in order to comply with the necessary standards. This may also force the customer to prevent the data from getting transferred to the cloud server.

## 10 HETEROGENOUS PROPERTY OF CLOUD

There are different methods through which a Cloud Service Provider implements the heterogenous property in cloud. Cloud providers use numerous physical and logical resources to run the cloud environment. Virtualization of these resources help us to provide high-level heterogeneous behaviour of the system.

However, if we use a single infrastructure to manage different verticals with different system needs and protection policies then it can create an issue in management. If a customer subscribes to IaaS service from one CSP, PaaS service from another CSP and SaaS service from some other CSP, then it is very obvious that issues will arise in establishing coordination between each of those CSP in turns of security and trust issues. The considerations made by one CSP for their service may not be feasible with the other CSPs and this might become dangerous for the whole cloud environment. Moreover, no uniformity exists in the level of security treatment every element provides, thus generating integration challenges. In a multi-tenant setting, the protection needs for each tenant may dissent, which can make a multi-tenant cloud one purpose of compromise. In addition, every tenant might have completely different trust relations with the provider and some tenants could truly be
malicious attackers themselves thus generating complicated trust problems.

## 11 CONSOLIDATION OF POLICIES & REGULATION OF TRUST

We know that there are various renowned Cloud Service Providers around the world who work with each other and integrate their modules so as to produce combined services, there is a possibility that they have unique security policies and privacy management methods of their own and thus we should not be able to find any uniformity in their policies. So, we need to ensure that this type of dynamic integration of services provided by multiple CSPs must be provided with mechanisms to ensure that there are least possibilities of security breaches and there should be a monitoring system which constantly tracks this combined system for any kind of faults or breaches. Studies reveal that even if the domain policies of each of the individual CSPs are being verified, still there are some cases of security breaches through the system. Thus, the CSP should check the access policies on a regular basis for any kind of loop hole that may result in security breaches.

In the context of cloud computing, the interaction between various service providers may be effective, short-term and rigorous at the same time. Thus, we need to develop a frame of trust so that we can get hold of an inclusive set of parameters that will help in developing and improving the trust issues and sharing activities among the different service providers. The implementation of the policies of the cloud must be able to serve and handle challenges such as managing policy evolution, maintaining heterogenous property without any issue, etc.

## 12 AUTHORIZATION USING IDM

By using the different cloud services, users are simply accessing their personal data and information on a cloud platform and so it may be accessible to numerous other services across the World Wide Web. This is where the IDM or the Identity management system comes into play. The IDM authenticates the user with the services based on the different credentials and characteristics. Organizations need to monitor the access control of their data and keep a record of which data is being used by whom and if it is being done in a proper manner. Attackers are becoming more advanced and stealthy day by day, devising more intensive and effective techniques to steal data from the organizations, trying to stay under the radar till they can any more valuable information without the knowledge of the organization. The IDM is just a mechanism in order to make sure that the identity of the users using the front service, is being protected from being exposed to the other services which are also in the picture. User identity must be tied to back-end directories for better results.

## 13 MANAGING THE SERVICES SECURELY

In cloud computing, the cloud service providers try to access the needs of the customers and then accordingly design the services for them which can best serve their needs. Though the cloud providers use the standard WSDL available online, the normal WSDL cannot fully meet the needs of the customers and the cloud service description. Issues like quality of service, price and SLA are some key points in this point of view. These issues need to be accessed properly while designing the services without violation of existing policies. The existing problems compels us to design a well-defined cyber insurance policy that will take care all types of vulnerabilities.

## 14 MANAGING ACCESS AND ACCOUNTING

Variety of Services like Non-uniformity and the likewise demand properly analysed access to the management policies, particularly access management services because of the need of the various requirements of cloud computing domain, are meant to be versatile enough to capture dynamic, attribute or credential-based access requirements and to enforce the principle of least privilege. Such access management methodologies and services may have to be forced to integrate privacy-protection schemes and solutions expressed through complicated rules. It is of paramount importance that the access system used in cloud servers is properly handled and its advantage scattering is done zealously. It is our responsibility to make sure that the cloud deployment models are providing us with the proper interfaces, which makes use of a policy-neutral access management specification and a social control framework that may include a predefined address across domain access problems. The models for access management should be ready to list the significant features of the SLAs. The feature-based model of clouds asks for correct accounting of user and maintenance activities that generate privacy problems and as a consequence customer may not be forced to let a supplier maintain such elaborate accounting records other than those for request functions. The outsourcing and multi-tenancy aspects of cloud models may accelerate customers' fears regarding accounting logs, access management techniques and non-uniformity in accounting and variety of services. Such of these access management services may have to be compelled to integrate privacy-protection necessities being implemented involving complicated rules. We also need to make sure that the utility model of the cloud makes sure of all the repairs that need to be done in the system which may cause privacy problems.

## 15 SOLUTIONS TO SECURITY CHALLENGES

In order to fight the above-mentioned challenges, we need to ensure that the CSP or the cloud service provider does every possible check in the system and make it as much secure as possible for the user to use his cloud services without the chance of any data leak of foreign attacks. For this we are going to discuss some possible solutions or steps that may be taken by the company to ensure data security.

First of all, let us talk about the cloud deployment models. We will discuss the probable solutions of each of the Public, Private and Hybrid clouds in details:

- **Public Cloud**: The first job is to be done by the user who is applying for the particular CSP. He needs to ensure that the cloud service provider he is opting for must have proper industrial certifications such as SAS 70 Type II and ISO/IES:27001. These certifications actually increase the probability of the CSP being more responsible and service efficient. The customer should also have contracts with the CSP such as proper SLA which should have requirements such as four nine's availabilities (99.99%) and also properly describe what will be the penalties that will be given by the CSP in case of any security breach since it may be really dangerous from customer's end. CSP should also properly describe the different methods and processes that are being undertaken to make it sure that the probability of cyber-attacks and data leaks is minimum. Use of third-party systems by the CSP must also be in the notion of the users and CSP should also previously state what they will do in case the third-party system fails. Encryption practices should also be properly monitored since it is the most important part of the process of transmission of data between server and the receiver.

- **Private Cloud**: Private cloud implementation typically uses virtualization technologies in order to increase the utilization of the users and thus makes it possible to provide the users with more memory, network bandwidth and other resources. Now virtualization always involves the use of hypervisor. So, we need to take care of all the possible vulnerabilities of the hypervisor and also manage the patches properly that are to be installed on the system. Network based access controls are to be taken care of in this case so that users in the organization are allowed to access only those data which they need to. The most dangerous and lethal attacks that occur on the system mostly come from within the system and so in this case we need to make sure that the internet traffic inside the system is treated on a same level as that outside the system. The host operating system must be kept secure from all the virtual machines and we need to make sure that there is no back channel that the users can use to access the host operating system of the hypervisor through the VMs. The host operating system must have all kinds of the firewalls and security system in order to ensure no unauthorized attack occurs from the outside, and all the patches needed to be installed are to be downloaded from a single trusted source on the intranet. These steps for the host operating system are taken in order to ensure that access to the hypervisor is not compromised.
- **Hybrid Cloud:** Hybrid cloud involves the use of both public and private cloud at the same time and so it is very important to manage this cross-platform deployment. Managing more than one CSP is not an easy thing and all security features transfers are to be done manually. We need to keep sure that the authentication process of both the clouds are being performed properly. Data leak probability is highest in this case since data needs to travel between two separate CSP's on the internet. So, for this, encryption needs to be done extensively. Alongside all of these we need a monitoring technology in order to gain visibility into various possible data breaches and they should cover both private and public cloud.

Now let us talk about the cloud service models i.e. SaaS, PaaS, IaaS. Though implementation of these models provides scalability, productivity, etc. still security issues are there since data is being sent out beyond the system firewall. Let us briefly discuss the measures that we should take in each of these service models:

- **PaaS**: PaaS enables the customer organizations to run world class web applications without having the infrastructure to run it. The PaaS users have root or administrative access to the servers during their sessions and during these sessions if the hackers are able to infiltrate the channel between the users and the server then they can get unauthorized access to the server and thus change configuration of the servers. So the channel between the PaaS server and the user must be hardly encrypted and there should a filtering method to decide who will get access to the terminal and who won't. Another point is there are some rules and regulations which forces encryption of private data whenever it is sent to some third-party systems. Cloud Service provider in this case is one type of third party and so we need to think some kind of solution which provides automatic encryption of private data while it is being sent to the Cloud server.
- **SaaS**: SaaS or Software as a Service is used by the users to connect to and run cloud-based applications in their own system environment. Now in this case, the hacker is not only interested in breaking inside the network but also wants to gain access to all the organizational data. So, phishing and malware attacks are very common in this case. So, companies who are implementing SaaS should not be completely depended on the CSP for security purposes but also implement procedures and processes of their own in order to ensure protection from these kinds of attacks. Employees must be trained to identify any kind of phishing attempts or malware software in the network and take necessary steps in the event of breach. Single sign-on systems are also very handful to eliminate the need of multiple passwords. In the event of a user leaving or joining an organization there is only one password to authorize it rather than multiples of them which may be very difficult to manage.
- **IaaS:** In this case the resources or infrastructure which are available in the data centres of the cloud service provider are being hosted by the CSP on the internet for the

customers to use. So, in this case also encryption process is of top priority in order to secure the channel between the user and CSP and thus protect the inbound and outbound data traffic from any kind of attacks. Furthermore, the compliance standards between the CSP and the customer must be evaluated properly and the method that the CSP follows to perform the task of monitoring should also be known to the user.

At the end comes the Network threats that we need to take care of which are of top priority. Network plays the most important role in transmitting data in cloud computing and so it is most important to ensure that the network on which the cloud operations are being carried out is kept secure. Some of the measure that we can take in order to minimize the risks are listed below:

- Encryption processes need to be checked and updated on a regular basis so that it keeps in pace with the possible new attacks that are emerging every day. Transmission of data from the user to the cloud must be shielded using a cryptographic protocol that supports end point authentication. The sender and the receiver compare their cryptographic hashes or fingerprints using an out of band communication channel which is expected to be secure. All these efforts and measures are taken to decrease the possibility of Man in the middle attacks. We can also encrypt these transmissions using SSL/TLS server authentication in order to prevent tampering with data in the middle. A reliable VPN and a proxy server can also increase the security of the whole process.
- Intellectual property (IP) protection is also one of the major tasks and must have the highest level of encryption and security protocols to follow. Data classification leads to the discovery of possible threats to IP and accordingly we should take steps to prevent them. Regular audits must be conducted by third party organizations in order to make sure the network infrastructure is secure enough to protect these IP.
- The user should use a separate intruder detection system of his own even though the cloud service provider is providing top class security. At the end it is also the responsibility of the company to keep its applications and information secure. All the activities must be logged properly and checked regularly to avoid any suspicious activity in the network.
- Another important task is to get visibility in to the incoming and outgoing traffic of the cloud server. This is done in order to decrease the chances of occurrence of malwares in the enterprise. If some dangerous malware gets into our PaaS or IaaS then it can gain access to the user login credentials and thus get full access to all confidential data and also edit them.
- Last but not the least the users must be aware of all the third-party applications that are being allowed to gain access to their cloud server and also about the apps that are being approved by the admin. No such third-party apps must be there in the system which scans on incoming and outgoing traffic for private data.

## 16 PREVENTION MEASURES TO STOP LOSS OF DATA IN CLOUD COMPUTING

Duplication**:** It ought to go while not oral communication, cloud offers the worth of information at any time or place; however, it's still your responsibility to own copies of your information.

- **Secure Cloud Backup**: Services like Carbonite, CrashPlan, and BackBlaze create mature suppliers of secure storage. Additionally, to the present, your supplier could provide its own backups in Associate in nursing encrypted and secure location break away your main data. As an example, if you're seeking a cloud accounting supplier, intact offers essential safety features creating your information accessible among hours within the case of emergency.
- **Sneakernet**: an off-the-cuff term, this includes things as easy as taking home a tape every night with backups of information or hiring a messenger to firmly transport information to s safety safety-deposit.
- **Network connected Storage (NAS):** If your business has multiple workplace locations, you'll deploy 2 compatible network-attached storage (NAS) devices at every location and set them to synchronize or make a copy to every different over the network.
- **Disaster Hardened Storage**: Disaster-proof enclosures give the final word in native backup protection. Typically, Fireproof, on-site, and encrypted to a tee, bound native backups even will send backups to the cloud.

**Backup Regularly**—Define a Backup Strategy**:** Depending on the kind of backup you decide on, it's vital to develop a weekly commit to backup important business information. No matter supply of backup you decide on, follow the following tips to confirm your backup goes with efficiency and firmly.

- Check Backup Settings and Strategy often
- Pay attention to What You make a copy
- Choose Multiple Solutions to Backup information
- Have Enough (but not too much) space for storing
- Again, rule of thumb ought to be to backup most significant files:
- Databases, monetary info, etc. a minimum of once per day; however different sources advocate doing complete backups every week, with differential or progressive backups daily. opt for your backup strategy, keep on with it, and check on the strategy to create positive that you just area unit maintaining with the trends.

Guarantee recover is simple: A shocking a part of the backup method is that some corporations can create it improbably straightforward to backup, however improbably advanced or valuable to recover information. Before you commit your information to a marketer, conclude however quickly you'll be able to dig back within the event of information loss or disruption, what the restore method seems like and what reasonably support you'll expect to receive if you run into any problems.

this may assist you set expectations for the business and may assist you minimize period of time.

Understanding this and making certain that everything you would like to grasp is roofed within the Service-Level Agreement (SLA), you'll set yourself up for fulfillment within the cloud. Providers provide decisions of storage service levels, and storage services ought to embrace on-demand quantifiability to stay applications running, snapshots for crash-consistent native and/or offline backup, offered off-site backup and/or disaster recovery and high convenience storage while not disruption attributable to maintenance/upgrades.

**Have Associate in Nursing Exit Strategy:** With relevancy the recent breach going code hosting supplier out of business, it's turning into a lot of and a lot of vital to manage information. Cloud backup and storage corporations give nice choice in an exceedingly secure atmosphere, however it's vital that you just area unit ready if one thing ruinous happens. Organizational Security Management**:** The security and management models currently in existence as well as the knowledge security life-cycle models require considerable modification once the enterprises adopt cloud computing. Especially, shared governance-based systems may become a major issue if not addressed properly. In spite of the potential cases of mistreatment in cloud, it would amount to less coordination amongst totally different types of communities of interest among the consumer organizations. Dependence on external and un-trusted entities may also lead to escalation of fears regarding timely responses to security incidents and delays in implementing systematic business continuity and prompt disaster recovery plans. Similarly, cost-benefit issues and risk can be involving external parties. Consequently, customers are supposed to contemplate upon newer risks introduced by a perimeter-less set-up, like knowledge discharge within multi-tenant clouds and some resiliency problems like their provider's economic instability and occurrence of native disasters. Similarly, the likelihood of Association in nursing corporate threat is considerably enhanced once outsourcing brokerage information and processes to clouds are deployed. Also, among multi-tenant environments, one tenant can become a primly targeted attack victim, which may lead to resounding of the effect on the tenants in the opposite sphere. Existing life-cycle models, risk analysis methods, management processes, penetration testing techniques, and repair attestation must be re-evaluated and re-instated to make sure that shoppers will fancy the potential advantages of clouds. The information security space has minute yet vital problems in establishing implementable security metrics for consistent and realistic measurements that will eventually facilitate risk assessment methodologies.

We should reassess best practices and develop standards to make sure the establishment and deployment of secure clouds. These problems make it imperative to have a well-structured and governed cyber insurance trade, however, the nature and mechanism of cloud computing makes this prospect very complicated and difficult to achieve.

**Cryptographic approaches:** Cryptographic approaches used while deployment and usage policy rules should be thought of during deployment. Once somebody requests access to information, the system is ought to check its policies and rules and reveal check whether the recipients are happy with the policies. Cryptologic techniques currently in existence may be used for information security, but privacy protection and outsourced computation should be given special attention since both are comparatively new analysis domains. It has just dawned on the industry to address the Information root problems. In some cases, information associated with a specific hardware element (storage, processing, or communication) should be in relation with a bunch of data.

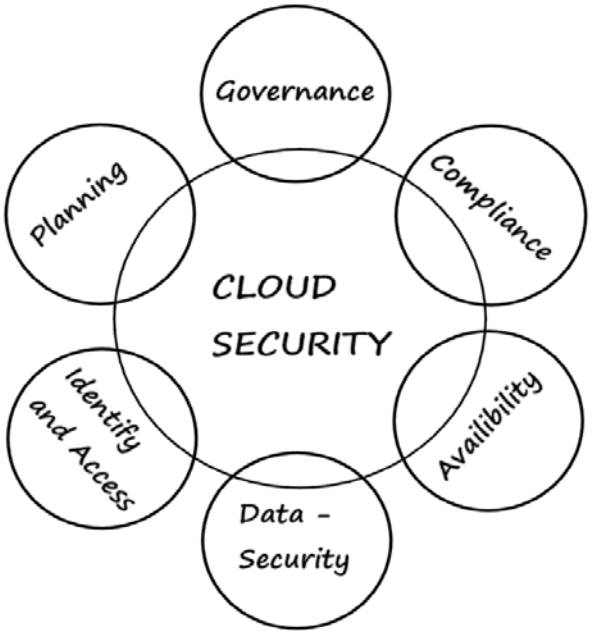
**Access management desires**: Among the numerous strategies planned up to now, role-based access management (RBAC) has been wide accepted because the most promising model due to its simplicity, flexibility in capturing dynamic necessities, and support for the principle of least privilege and economical privilege management. Furthermore, RBAC is policy neutral, will capture varied policy necessities, and is best suited to policy-integration desires. because of the extremely dynamic nature of clouds, obligations and conditions are crucial call factors for richer and finer controls on usage of resources provided by the cloud.

## 17 ACKNOWLEDGEMENT

We would like to express our deepest appreciation to all those who provided us the possibility to complete this research paper. A special gratitude we give to our semester teacher, Ms. Shelly Gupta, whose contribution in stimulating suggestions and encouragement, helped us to coordinate our technical report especially in writing this research paper.
Furthermore, we would also like to acknowledge with much appreciation the crucial role of the staff of UPES, who gave the permission to use all required equipment and the necessary materials to complete the research paper.

## 18 CONCLUSION

Cloud computing model which has taken the world by a storm since its inception has gained popularity due to its unprecedented advantages like acquisition and scaling up of internet-based services and virtual resources on demand. Other than that, cloud computing also negates the need of heavy investments on systems, infrastructure and labour. This as well as the "pay per use" ideology has proven beneficial for the users and organizations falling from all kinds of financial backgrounds as well as business structures.
One of the very few drawbacks of the Cloud Computing Model is the Security Issues that come along with it. We strongly are of the opinion that the flaws that exist in the present implementations of the model are what is keeping it from becoming more popular and preventing more users and organizations from adopting it. In the beginning of this paper we gave the back-




ground of the cloud computing model by explaining the various cloud service models based on the type of services they provide like: IAAS, PAAS, SAAS, etc. Then we moved on to discuss the various security challenges that are rampant in the cloud service models like DDOS attacks, which are meant to overload the server by flooding it with requests, and the risks posed by insecure access points like unauthorized access to the data stores and server resources. We also discuss the threat of Data Breaches and Data Loss and other such maladies that plague the Cloud Services. We have also highlighted the cause of discontent amongst the customers which arises and a result of the absence of transparency to the storage and handling of their resources. After highlighting the various challenges, we moved on to deliberate upon the various solutions to the security loop-holes present in the Cloud Model. Finally, we also provide some recommendations on how to improve upon the cloud model and make it more robust.

We are of the opinion that due to the immense complexity of the cloud it will be a mammoth task to achieve end-to-end security. The cloud computing ideology offers rampant room for development and unprecedented opportunities waiting to be harnessed and the only obstacle in sight is the security concerns. We believe that the security concerns can be surmounted by developing and imbibing new security techniques and radically tweaking older security techniques to make them compatible to work with the cloud architecture. As the popularization and development of security technologies in cloud computing is still at a nascent stage, we sincerely wish that our work will go a long way in providing a better understanding of the various challenges that plague cloud computing and will help in paving the way for further research.



## 19 REFERENCES

[1] A. Kundu, C. D. Banerjee, P. Saha, "Introducing New Services in Cloud Computing Environment", International Journal of Digital Content Technology and its Applications, AICIT, Vol. 4, No. 5, pp. 143-152, 2010.

[2] Lizhe Wang, Jie Tao, Kunze M., Castellanos A.C., Kramer D., Karl W., "Scientific Cloud Computing: Early Definition and Experience," 10th IEEE Int. Conference on High Performance Computing and Communications, pp. 825-830, Dalian, China, Sep. 2008, ISBN: 978-0-7695-3352-0.

[3] R. L Grossman, "The Case for Cloud Computing," IT Professional, vol. 11(2), pp. 23-27, 2009, ISSN: 1520-9202.

[4] B. R. Kandukuri, R. Paturi V, A. Rakshit, "Cloud Security Issues", In Proceedings of IEEE International Conference on Services Computing, pp. 517-520, 2009.

[5] Meiko Jensen, Jorg Schwenk, Nils Gruschka, Luigi Lo Iacon, "On technical Security Issues in Cloud Computing," Proc. of IEEE International Conference on Cloud Computing (CLOUD-II, 2009), pp. 109-116, India, 2009.

[6] Pring et al., "Forecast: Sizing the cloud; understanding the opportunities in cloud services," Gartner Inc., Tech. Rep.