ISSN:2231-0711

Neelam Sharma et al | IJCSET(www.ijcset.net) | May 2016 | Vol 6, Issue 5, 153-160

Security from Insider Theft on Cloud Computing

Neelam Sharma[1], Sonia Batra[2]

[1,2]*Affliated to MDU Rohtak: M.Tech Computer Science and Engineering*
World College of Technology and Management
Gurgaon, Haryana, India

Abstract-Cloud Computing is not a new term it is basically up gradation of grid computing. It involves the concept Virtualization and service on de that can be easily access by remote computer system and cloud servers. The main importance of cloud computing is to connect people on this geographical area. Cloud Computing having lots of attractive features like scalability, service on demand, Efficiency, High Performance, Easy to Deploy, Easy to use, No need to buy resources, cheap services and Ready to use services, No maintenance by users. There are lots of services provided by cloud computing like cloud system can be public, private, hybrid or a community can handle the cloud system. It means a cloud system can be managed personally, by an organization etc. Popular and broadly used cloud services are Software as Service (SaaS), Platform as Service (PaaS) and Infrastructure as Service (IaaS). All the services are either provided by cloud service provider on demand bases or available on rental charges. It is completely based on the subscription selected by the user. To access all these services a user only requires an internet connection on their system. With all these features cloud technology has some drawbacks which make organization to think whether they should adopt it or not. Most of the drawbacks are related to security issues. In cloud computing users or organization going to store their data on remote resources for that they needed to be hundred percent sure that their data is in right hands and will not be reveal by any people. As this is new technology all the vulnerability in system is not checked yet and may have some security holes, which is biggest issues for organization that's stop them to adopt this technology. According to NIST [1] Cloud computing is a model for convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. In cloud computing data and applications are maintained with the use of central remote server and internet and allow consumers to use the applications without installing and also with the help of internet cloud computing allows customers to access their personal data which are stored in some other computer. Yahoo email, Gmail, or Hotmail etc. are examples of cloud computing. The email management software and the server are fully managed and controlled by the CSP Google, Yahoo etc. and are all on the cloud (Internet)

Keywords: **Cloud Computing, virtualization, Software as Service, Insider Theft, Cloud Security**

INTRODUCTION

To define cloud computing is very difficult as it covers vast area, but in simplest term it can be defined as ***computing via Internet***. In which user uses assets and services on rental basis. It can be defines as "**services on demand**". It consists of highly effective, powerful machines which can have large no of connection at a time over network. The work that people or organization are doing on their personal system and keep their all data within their system, is now being done remotely by using cloud computing. And it is cautiously beneficial also as organization need not to purchase resource in spite of that they can use it on rental basis. Cloud Computing is provided that virtualization that users are using software or system at their home but actually they are using remote system. Maintenances task of resources and security of data which is concerned by specific person before shifting to cloud computing is now under Cloud Service Provider.

Resources which are too costlier and difficult for users to use are now become simple and cheap. Functionality such as High Processing power, software packages, sharing of resources on Cloud computing are on charge basis or free of cost. These functionalities make Cloud computing briskly growing technology.

Most of the IT companies understand the power of cloud computing and implement it and others are in process to adopt it. Cloud computing architecture is basically highly effective, powerful processing system, it may be network of system or grid of system that provides high processing power that are given to users and on their demand. Cloud Computing user interface is alike to web interface. Clients only need to have browser and high speed internet connection to use cloud computing.

Because of the striking features of cloud computing many organizations are using cloud storage for storing their critical information. The data can be stored remotely in the cloud by the users and can be accessed using shrill clients as and when required. One of the major issue in cloud today is records security in cloud computing. Storage of data in the cloud can be unsafe because of use of Internet by cloud based services which means less control over the stored data. One of the major concern in cloud is how do we grasp all the benefits of the cloud while maintaining security controls over the organizations assets.

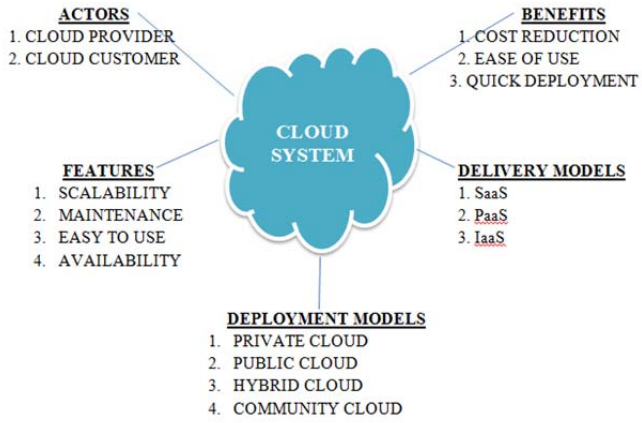

Figure 1: Cloud System

1.1 Basic Cloud Computing Architecture

Cloud computing architecture is very similar to Web Server. The architecture of cloud computing can be defined as the "***collection of components and subcomponents which are required for computing in cloud***".[2] The working of these subcomponents is totally based on the front end which contains altered types of client that may be a thin client, a thick client or any mobile devices and also on the back end which consists of storage and servers, a loud delivery model and a network which is a main component. The arrangement of all these components is termed as cloud computing architecture. As told above cloud computing usually involves of two ends that are a front end and a back end. These components are linked with each other with the service of a network which is known as internet. The front end can be defined as a way in which the communication is conventional between the user and the system. On the other hand, the cloud itself is known as the back end. Front end is a pool of comprises of a client side computer, network of an enterprise and software's which are used to access the cloud, whereas the back end is a pool of thousands of servers, computer , storage space etc. that all develop the services of cloud.[3]

It consist of three parts –
1. Cloud Servers
2. Internet Connection
3. Browser.

CLOUD SERVERS:

Cloud Servers are involves of hardware and software. In terms of hardware Cloud servers are highly efficient and influential processing machines that have processing power of super computers and can handle large no of connections of users at time. It may be network of powerful machines or may be single device. In terms of Software Virtualization of resources and APIs conferring to demand of user are designed that are easy to access and understand.

INTERNET CONNECTION:

Cloud is internet based technology that means deprived of internet connection we cannot use cloud. Internet is the only way that connects user to cloud machines. Cloud can be used on Intranet in any association or it can works on LAN. To enjoy cloud technology High Speed Internet connection is required.

BROWSER:

It is application which must be mounted on user's personal computer to access cloud.It is front end where Cloud API executes and users intermingle with cloud services.

1.1 Basic Cloud Computing Architecture

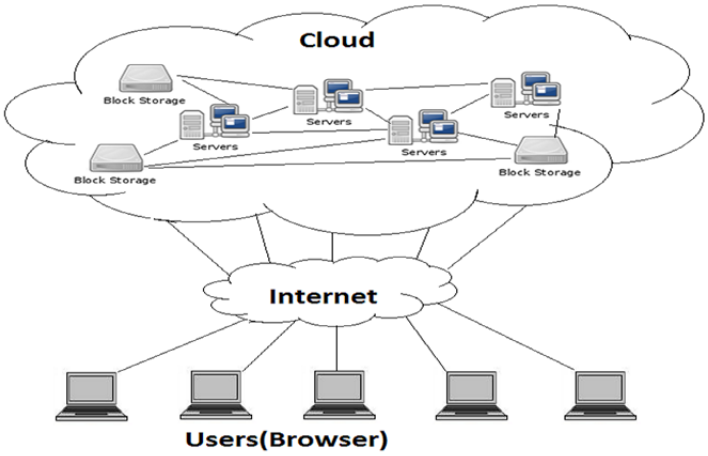

Figure 2: Basic Architecture of Cloud.

1.2 ACTORS

Cloud Provider:
A cloud provider (service provider) is an individual that is responsible for everything required for making a cloud service available.

Cloud Consumer:
A cloud consumer is either a cloud service holder or a cloud service consumer. Cloud service holder is the individual or organization who subscribes for a cloud service. If there is any charge associated with the service, the cloud service holder will be responsible for the bills. Cloud service consumer is an individual or application who admittances a cloud service.

Cloud Broker:
A cloud broker is an entity that intervenes between cloud providers and cloud consumers. The goal of a service broker is to provide the cloud consumer a service that is more appropriate for its needs. This can be done by simplifying and refining the service and contract, aggregating multiple cloud services or providing value-added services. One can consider cloud brokers as a superior cloud provider.

Cloud Auditor:

A cloud auditor is an independent party who inspects a cloud service stack to provide an assessment on security, privacy and availability level of the corresponding cloud services and ensures that the corresponding SLAs (Service Level Agreement) are filled. The particulars and scope of auditing process is normally specified in the service contract.

1.3 CLOUD COMPUTING SERVICE MODELS

As definition of Cloud Computing states it is computing via Internet. Cloud Service vendor provides resources and services to user on charge basis. These services may be software's like Google docs, ERPs, management and commercial software, or it may be Web servers, database servers, Operating system or it may be server database server and storage in terms of hardware.

Cloud Services are classified into three categories:
SaaS
PaaS
IaaS

1.3.1. SaaS (Software as Service):

As the name recommend software is key service that is provided to users by Cloud Service Provider.In this Cloud Service Provider progresses or install Software on cloud and available these software to users on rental basis. It is the front layer in architecture of cloud computing which represents front end solicitation of cloud computing. Among all types of services it is tranquil service to use and users need to consider very few things to use it. Most of the application of SaaS is directly accessible via web browsers while some are established for Desktop Application. SaaS is the tranquil services on cloud and need not extra software to install on your machines to use it. Cloud Service Provider design these provision with care that user can user them very easily. Software as a services are the software solicitations that are developed by CSP. These services are given to users on charge basis for limited time. These services are owned by user but software is maintained by CSP though maintenance of these applications is under CSP. There are lot of SaaS services are in arcade some are free of cost and some are on rental basis. Example of SaaS is Gmail an email amenities. In this Full software package is developed by Google and maintenance is also completed by Google. Users only need to use it.

1.3.2. PaaS Platform as a Service:

If we consider Service Model as layer architecture than we can say Platform as Service is layer afterwards Software as service layer. Platform as service means providing platform like web server, Operating system etc. In fact Platform provides environment for the development of software applications on cloud. It's just like to acquisitions web service for deploying website on server in which we get platform like SQL Server, PHP Server.

All the software services are developed on the basis of accentuate platform. Platform as a service is provided via virtual machines fitted on cloud. In which different kinds of Operating system or additional platform are installed. Microsoft Azure is a good example of platform as service in which we get azure server which fixed with several servers like SQL server, PHP web server, apache server and other tools that helps developers to create their own application and software on cloud. Though platform like Operating system, storage servers are provided by CSP on payment basis for limited time.

1.3.3.IaaS Infrastructure as Service

It is the bottom abstraction layer of service model. It is also identified as Hardware as a Service. All the physical devices like server, network devices, storage disk comes beneath IaaS. In this CSP offers Infrastructure only and users need to set their own platforms like operating systems, database servers, web servers and need to develop their own software packages. All kind of terms and condition to use this software is made by users only. Security, resource pooling like issues are handled by users only.[4]

In this CSP are at posterior stage and its only maintain infrastructure. All type of hardware is given to users on rental basis. User sets their personal firewall, their own Operating system and develops their own software's. Application Databases and Security issues are bring about by cloud users. CSP only sets instruction for using infrastructure so that users can use their service efficiently. Operating System, Virtualization, Data-Centers, Networking are coped by Cloud Service Providers.

1.4 TYPES OF CLOUD COMPUTING

We can categorize cloud in four different categories. These categories are on the basis of their Service models we define above are applied on all types of cloud.

They are listed as:

1.4.1. Public Cloud:

As the name suggest it's for public or we can say it is used by general community where every resource and services are available to public on the basis of their subscription to CSP. It is also well-known as Shared Cloud as resources and services are shared among large no of users. Example of combination of SaaS and Public Cloud is Google Docs where each operator can create there document and share among other users. In this Google Docs is Software on Public cloud that is freely accessible to all users. Example of grouping of PaaS and Public Cloud is Windows Azure. Example of grouping of IaaS and Public cloud is Amazon EC2 Cloud. Usually Public Cloud services are provided by large organization or by government.

1.4.2. Private Cloud:

It is kind of cloud which is established for single organization. In this type of cloud, services are accomplished by third party or by organization by themselves. Maintenance, safety are managed by organization only. People working in organization can use the amenities and resource of cloud while others are restricted to use. Main benefit of private cloud over public cloud is that control over all services and resources in hands of organization, they can customize services and resources according to their organization needs.

1.4.3. Community Cloud:

It is an extension to private cloud community cloud has comparable features to private cloud in terms of services and resources but it is used by large quantity of user than private cloud users. Community cloud is amalgamation of three or four private cloud which has common features. Community clouds are overseen by a community or by third party and different organization users can use community cloud.

1.4.4. Hybrid Cloud:

As the name suggests this kind of clouds are arrangements of other kind of cloud (private, public, community). Its conglomerates the features of public and private cloud and community cloud. Its advantage is that every type of user where insider or outsider of organization can access the cloud services and resources.

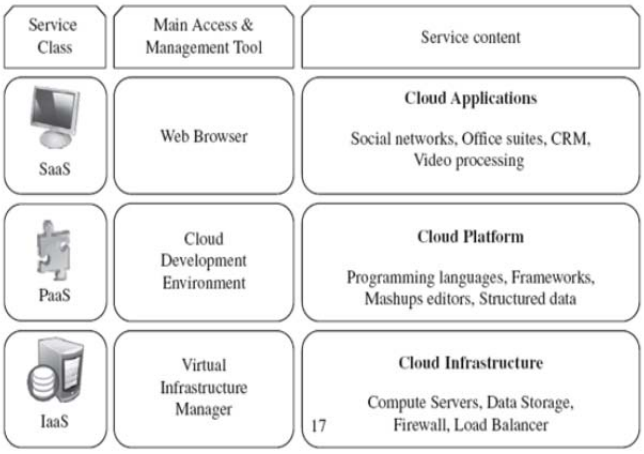

Figure 3 The cloud computing stack [5]

1.5 SECURITY

Security is one of the most vis-à-vis issues of Information technology Issue. To keep organizational or user data is primary apprehension. If organization's data is not safe on cloud then there is no use of ever-changing from old technology to cloud technology. There are lot of Non-Profit Organization (NPO) which are serving and creating awareness about security issues of cloud computing. One of such organization is CSA (Cloud Security Alliance) that publish a report in each year concerning most popular security issues in cloud computing. In 2013 CSA reports they identified nine notorious security threats to cloud which can harm user's individual data without eloquent them.

Those are as follows:

1. Misuse of Cloud Computing (Cloud Abusing)
2. Weak and insecure Application Programming Interface (API)
3. Insider Theft
4. Vulnerabilities in shared cloud services.
5. Data Damage and loss
6. Data Breaching.
7. Eavesdropping
8. Service Denial Attack
9. Brute Force Attack

These are most implementation security issues reported by CSA. In spite of these security issues there are much more issues which we will explain in coming sections.

- **Misuse of Cloud:**
  Some Malicious persons can practice cloud computing for illegal and criminal activities. Use of cloud for illegal tenacities is called cloud abuse. Some malicious user can use cloud to host harm code or can use to provide plagiarized data to large no of users. Most of the time some malicious user creates advertisement on cloud that attracts users and queried for their personal information. These personal information is then use for illegal chore or sending spam's on users address. This type of advertisement on Cloud is a kind of cloud abuse. Sometimes Cloud can be used for performing such chore which is not possible on users system for example if a malicious user want to decode some data by using brute force attack than that user can use cloud platform to perform his task. So this kind of actions also comes in the category of cloud abuse. Another instance of misuse of cloud computing is "http://wpacracker.com" this website is used to check the security of WPA-PSK network protection security. Which typically takes four to five days to crack on usual machine but with the help of wpacracker.com which is on cloud can crack it in 20 to 30 day. This kind of service on cloud is termed Insecurity as a service.

- **Weak and Insecure Application programmable Interface:**
  Data and services of cloud are accessed through Application programmable interface. Weakly designed and faults in API tends to exposure of services and data to unwanted users. For instance vulnerability in Apache Web Server can lead to a user to have access on full server. Some times in shared cloud services, data can be shared among various users because of malfunction in API and sometimes because of rewritten of privacy setting of users. Most of the epochs it has been that designing API without all security measures lead to weak API. But sometime by

intention weak API are planned for malicious activities.

- **Insider Theft:**
  Even though users can trust on CSP but cannot trust on his employees as everyone is not good. Some malicious employee of company can crisscross individual data or can steal individual data for some illegal work. Even some CSP company can provide our data to other corporation to earn money. This type of insecurity is called insider threat. For example giving Platform as a service to some user or firm can lead to data theft. One good example is Applications on Facebook if once authorizations are provide to applications they can fetch all information related to users. So now problem is to find answer of such problem. Third party to preserve credential or data may be the solution. Zero Trust Security model is upright solution to such problem in which all data and passwords are keep in encrypted form.
- **Security Issues in Shared Cloud:**
  One of the most critical threats to Cloud technology is to produce cloud and its services themselves.
- **Issues due to virtualization:**
  Due to virtualization architecture users of IaaS service have capability to create many virtual machines on same server. Users can set their virtual machine on same server and if once they mounted their virtual machine on same server they will be able to apply many attack and can easily find out information concerning keystroke timings, CPU cache use and network traffic rates.
- **Combined Services:**
  Some services on cloud (public or community) are created on other service and dependent on other services. In such kind of services users' information are shared among all the services that composed service which user is exhausting. This lead user to shared personal information to such service provider to which he was not assuming. And Backend services can misuse their personal information without knowing the users.
- **Data damage and loss:**
  Data is most important part of cloud services so gigantic concern should be given to its security. Data damage and loss can be done in two ways first of them is due to natural reason and second is due to artificial problems. Data loss due to natural reason like servers are damage due to earth quake at server location, Fire in server room, physical reparations to server, problems in hardware so that data cannot recovered this type of problem can be solved using facsimile servers but that lead to insecurity and doubled the cost. Data damage due to artificial problems is attacked by malicious user and he might delete all data or overwrite all data even he may move all data. A malicious user can change access permissions of data so that unique users cannot access his data that is equal to data damage. Some malicious user can change services such that they will be able to get all data by user which was fictional to be stored on cloud storage. Solution to such problem is systematic checking of API of cloud services. And make secure access controller list so that it should not be easily available to malicious users.
- **Data Breaching:**
  It is topmost most security threat in CSA report. To explain the potential of this threat, Computer Security Alliance refers to some research paper that describe how a user on IaaS can set his own virtual machine on same server and by using parallel-channel effectiveness information, how a malicious user can excerpt important cryptographic keys of users. Weak API or some flaws in conniving cloud service also lead to data breaching. If there is some flaw in API than malicious user have a lot of chances to get information about services and user of that amenities that may lead malicious user to rewrite permissions of data of service users. Data breaching can be caused by service or account hijacking, by applying brute force attack or by applying SQL injection malicious user can takeover users account which is too dangers, if once they hijack users account than for CSP it is very difficult to identify that whether services are accessed by pioneering user or by malicious user. In such situation regular checking of services does not make any variance.
- **Eavesdropping:**
  As per dictionary eavesdropping gist is to listen others private conversation without knowing them. But in terms of computer technology eavesdropping meaning is to listen others chat, messages, and audio on phone without the knowledge of users. Eavesdropping is also well-known as MIMA (Man in the middle attack). In this a malicious persons makes individual networks to a cloud user that seems like original connection of cloud to user by this malicious person redirect all your conversation and data to his storage devices. It's just like phishing of websites in which user get the same webpage like unique one so that users enter his data and data should go to malicious user storage devices.

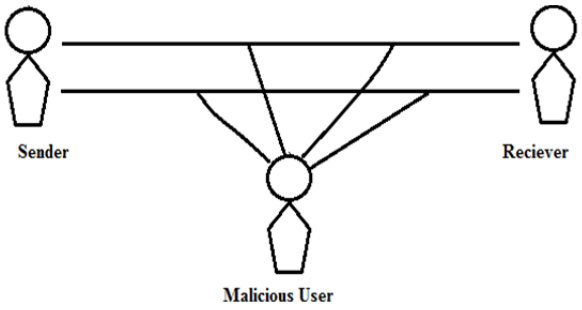

Figure4: Eavesdropping(man in middle attack).

- **Service Denial Attack:**
  When a user is not able to access his amenity due to high load on cloud server caused by malicious user is called Denial of service attack. It is one of the oldest security threats in computer networking but in today era when cloud computing is becoming popular its

threat is snowballing. As cloud are designed for twenty four hours availability, but attacks like DOS makes it unreachable. Generally these kinds of attacks are applied on those services which are most prevalent and accessed by many people at a time. In this kind of attack malicious user set machineries (botnet) that makes large no of request to cloud service at a time that in turn create load on server and become irresponsive and service seems to be temporarily down. But a malicious user can not permanently down a service because of huge cost are needed to apply DOS attack as it requires high processing power system and resources.

Brute Force Attack:

In this kind of attack malicious user tries to attack on data or security authentication by applying different blends of characters set. It's similar playing in dark. It can be applied via thesaurus attack also. In this kind of attack if user acquire your encrypted data than he will design such system where he can decrypt your data applying different kind of combination of password to reveal original data.

Some Other Issues that affects Security: Every cloud service provider and user signs a term and condition paper that puts some circumstances for using cloud services. Some service level agreements are also recognized for privacy of users. Let's consider these one by one.

- **SLA Service Level Agreement:**
  Users believe that Cloud service provider should trail terms and conditions, and always securely store their data. But the terms and conditions set by cloud service providers are not according to consumer's organization rules that may lead to doubtful condition in users and consumers organization minds. Even some time cloud service retailer change their policies without knowledge of their users that is illegal too. So when users don't know about the new terms and condition than how they can trail terms and conditions. For instance in new terms and conditions CSP puts limitation of uploading of maximum size of data is 10 MB, but users are using these service because he can upload large files on cloud though in such condition cloud is just wastage for him and now he can't do anything because he don't have full control over cloud.
- **User's privacy Expectations:**
  For a citizen of a country, privacy of their life, home and their substantial is right, in similar way privacy of their data and information is also their right. All users expect that their data on cloud will be protected and will not be shared with anyone even not with cloud service provider. for the same motive most of the cloud service providing company follows zero trust security model according which all the personal as well as users data are kept in encrypted form so that neither insider or outsider except owner can read the information and data.

1.6 Advantage and Disadvantage of Cloud Computing

Cloud Computing is one of the fastest developing technologies in today's era. Most of the industrialists and individuals are adopting it since of its large number of advantages over traditional computing technology. Features providing by cloud computing attracting users and industrialist towards its adoption.

Some of advantages of cloud computing is as follows:

- Reduced Cost
- Guaranteed Availability
- Recovery and Backup
- On-Demand Services
- Easy to Use
- Flexible Storage Capacity
- Less Maintenance
- Scalability
- Location independent Access

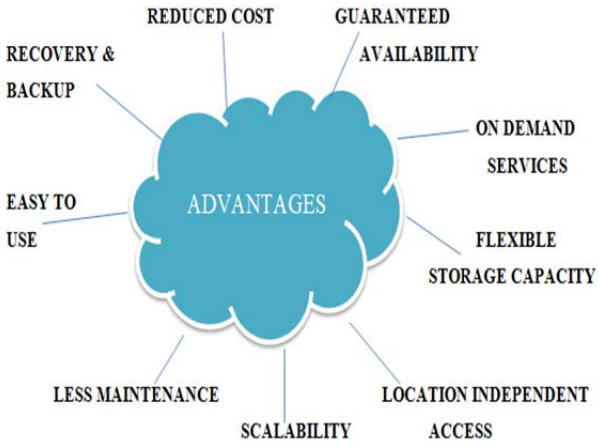

FIGURE 5: Advantages of cloud computing

Reduced Cost:

One of the important benefits of using cloud is reduction in cost. By using cloud, organizations want not to buy their own infrastructure, platform and software. Even the investment on rental service is very less than purchasing their individual resources. Cost of Maintenance and new development in resources are abridged.

Guaranteed Availability:

Accessibility of cloud service is 24*7 hours weekly. We can a use cloud service anytime we want to use. As cloud servers are maintained by Cloud Service Provider, users need not to care about its availability. CSP's service maintenance crew takes care of guaranteed availability of cloud resources. CSP sets many laying-off servers to make availability guaranteed even in failures of some servers.

Recovery and Backup:

As most of the cloud service providers used multiple servers for cloud computing and even they use replica servers so that if any case of halt or error there shouldn't be data loss or any kind of problem occurs to their user's service. As of interconnected servers it's very easy for CSP to create recovery and backup of its user's data.

On Demand Service:

It is one of the best advantage of expending cloud computing. In cloud computing users subscribe services conferring to their demand at that time. If users purchases some resources and after some time that technology is out of date then that is completely waste of money, but in cloud computing users use service on demand for shorter time, so now if some service technology is out of date users would not agonize from any loss.

Easy to Use:

Cloud services are very tranquil to use. Users need not to know about its subversive technical details. Cloud services are on the ledge service or ready to use service. Interface developed by CSP for the interaction with cloud services are very tranquil to understand and user friendly.

Flexible Storage Capacity:

In cloud computing storage capability is based on users subscription pack. But storage capacity on cloud is very elastic, as it consists of large data centers which provide very large storage capacity then our personal computer. Elasticity of storage capacity is in terms of subscription pack, if users subscribe package of large storage unit then he will get large storage unit. Cloud computing makes efficient use of resources for example if some users subscribe for large storage area but is consuming very less than on server that storage area may be used by someone else.

Less Maintenance:

Generally in cloud computing there is very less maintenance concern for users. All the maintenance correlated work is handled by cloud service providers. In Software as Service all the maintenance is through by cloud service provider. In Platform as Service maintenance of software is done by users all others preservation is done by cloud service provider. In Infrastructure as Service Applications, Security and Database are managed by users and operating system, virtualization and datacenters are kept by cloud service provider.

Performance and Scalability:

Physically cloud computing servers are similar grid computing servers, at backend all servers are interconnected to provide high processing power to their users. These processing authority and resources are given to users on the basis of their demand or subscription package. That's why cloud computing is accessible, each user can increase or decrease its resources and processing power according their usage.

Location Independent Access:

Cloud computing assets can be access from anywhere at any time. To access cloud computing resources users only need to have a system like personal computer or laptop or mobile or tablet empowered with high speed internet connection and installed with browser. For Accessing cloud services users location doesn't matter that's why cloud services are called on the pace services.

- **Disadvantage**
- Privacy and Security Issues
- Dependency on Internet
- Dependency on Vendor
-

Privacy and Security Issues:
Security is one of the biggest issues that stop organization to accept to cloud computing. As in cloud computing users are going to store their data at remote location so security of their data is most significant. So in cloud computing all type of security issues are needed to be handled by cloud service provider, therefore reliability of CSPs are important.
Privacy of their data from unauthorized and malicious users is also significant concern and it must be handled by cloud service providers.

Dependency on Internet:
Cloud computing has a lot of benefit over traditional computing technology, but all this gone in vain when users don't have internet connectivity. Cloud computing technology is accessed via internet, so to use cloud computing service a user must have internet connectivity and even presentation of individuals work is also affected by their internet connection speed. Depending on Internet brings a lot of security concerns related to network in cloud computing.

Dependency on Vendor:
Cloud Computing services are provided by CSP's which pay attention of almost all kind of maintenance tasks like security, operating system, virtualization, database, datacenters, servers. So in cloud computing users are fully dependent on vendors, so before subscribing to any retailer users must checkout its services as trials and take a note on its reliability and users review.

PROPOSED WORK

Report on the proposed work is divided into two parts:

2.1 Objective
2.2 Proposed Work

2.1 Objective
The main motive of the research paper is to increase safety of cloud application and data from insider theft.

- To know about security issues, challenges and vulnerabilities in existing model of cloud security.
- Implement the SAAS (Software-as-a-Service) facility by developing a cloud based application which is more secure than existing one.
- To understand the basic architecture of cloud computing, it's working, its virtualization concept and all.
- To set the server in order to use deploy its applications on the cloud so that it can be used by desktop as well as mobile users.

2.2 Proposed Work

2.2.1 Basic

In this part we are describing a framework that delivers environment for securing users data or files through file encryptions technique. Our research work mainly emphasis on security of data from insider theft. Solution to keep user's data safe from insider theft is zero trust models. According to which each and every bit of users data must be reserved in encrypted form. And this approach is too effective and is being implemented by furthermost of the cloud service providers. My research work is next step to zero trust security model and improve the security of data on cloud. Problem in existing model is that if any insider has access to user's data and he/she knows the encryption algorithm than he/she can simply set a machine implementing the encryption/decryption algorithm for applying brute force attack on user's data. We know this approach takes time but in today era where processing power is not a big problem, time to decode can be diminished. Though in present model I found that insider can smear brute-force attack. My research work tries to increase security on this issue. For improving security my model advises that in spite of using single encryption algorithm for all users of cloud, CSP should use set of algorithms, but for a user only single encryption algorithm will be applied on data and the assortment of encryption algorithm for a user will be random and no information regarding the selection of encryption algorithm will be stored in database or anywhere. By applying this model user's encryption algorithm will be one from set of encryption algorithm and now if any insider attempts to apply brute-force attack on users data then in that case he need to develop machine for all encryption algorithm and time taken to decode will be augmented if decoding machine is single, otherwise he/she need to set no of machine (high processing power machines) equals to set of algorithms. As we know to decrypt data encrypted with AES takes very long time so to decrypt data without knowing the algorithm forces attacker to develop machineries for all the encryption algorithm that in turn need large and high processing power resources which is too costlier and is very difficult for an individual to buy. Second case attacker can develop encryption machine on single system but that will intensification time proportional to numbers of encryption algorithm.

CONCLUSION

Cloud computing is speedily growing technology and safety of data on cloud should be higher. My proposed model tries to upsurge safety from insider theft. Although my model is based on Storage as a Service nevertheless it can be implementing on any application on cloud (Software as a Service).SaaS is topmost most layer of service model of cloud and it's the layer which interrelates with the users. And it's the layer where security to data like encryption and decryption of data is done. For applying my proposed model with SaaS we need to develop a plugin like software which devoted with software service on cloud and contain all encryption and decryption related algorithms. So if someone opens file using service, then that files passes through plugin and get decrypted and when users hoarded his work and closes file than again file passes through that plugin and encrypt the data and store on cloud.

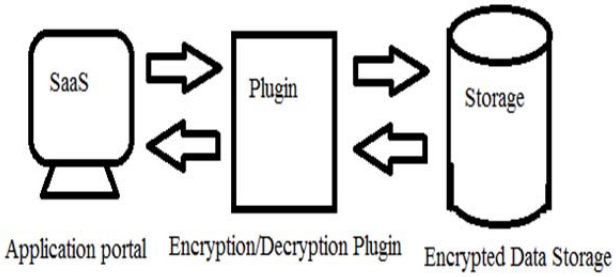

Figure 6: Proposed model implement in Software as a Service.

REFERENCE

[1] Mell, Peter, and Timothy Grance. "The NIST definition of cloud computing(draft)." NIST special publication 800.145 (2011): 7.

[2] "Cloud Computing Architecture". http://communication. howstu_works.com/cloud-computingl.htm.

[3] R. B. Bohn, J. Messina, F. Liu, J. Tong, J. Mao: *NIST Cloud Computing Reference Architecture* (2011 IEEE World Congress on Services)

[4] D. Xu, H. Liu: *Reviewing some Cloud Computing Platforms* (April. 2010, pp. 161-16)

[5] Buyya, R.,Broberg, J., & Gościński, A. (2011). *Cloud computing: Principles and paradigms*. Hoboken, NJ: Wiley.