iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** V **Month of publication:** May 2020

DOI: http://doi.org/10.22214/ijraset.2020.5458

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue V May 2020- Available at www.ijraset.com

Boosting Security for Cloud Storage

Pooja Sharma[1], Vaibhav Jha[2]
[1]*Manav Rachna International Institute Of Research And Studies*

Abstract: ***Due to enhancement in various technologies many companies are adopting them to boost their profits and continue their business operation without any failure. Cloud computing is one of the emerging technology which provides on demand availability of data in the form of Saas(Software as a Service), Iaas (Infrastructure as a Service) and Paas (Platform as a Service) without involving organization more on hardware or infrastructure part. Cloud storage is one of these service that provides several other benefits from cost optimization by pay as you go to data redundancy and high availability of data by creating replica of data to use in an emergency situation in case of failure. Rapid enhancement in cloud technology and varied benefits provided by cloud platforms leads many organizations to migrate on cloud storage from On-premises. Cloud storage access via internet it is more prone to cyber threats so it becomes very important to adopt security measures in order to secure it. These threats include loss of intellectual property, several malware attacks, contract breaches with business partner; customers trust issues, data unavailability and many more. Data security is very important as it ensures the quality of services so many cloud service providers mainly focus on it. Data is secure with respect to data security models. These security models converts the data in real time to encrypted format before sending it to cloud storage so that if some unauthorized person gains access to these cloud platform he can only view it as an encrypted format so there is no leakage of sensitive information from cloud storage. Cloud security models involve data integrity, Multi factor authentication, tokenization, firewall, malware detection and encryption algorithms. This paper lays emphasis on how secure is to migrate whole data of an organization to cloud storage, various security threats associated with cloud storage, ways to protect these threats, various cloud security models and analysis of security of various cloud platforms. CIA triad i.e Confidentiality, Integrity and Authenticity is mandatory to keep in mind in order to migrate data securely on cloud platforms. Unauthorized user should not access the data in any case, due to data diddling data must not be altered. So we will see in this paper several benefits of cloud storage platforms such as Amazon S3, Google Docs, Oracle Cloud Storage, Microsoft Azure Storage, Google Drive, Docker and so on ,various risk associated with these cloud storage platform as well as how can we mitigate them using certain techniques and adopting some security measures.***
Keywords: Cloud Computing, cloud storage, Cloud Security, Confidentiality, Authenticity, Data Diddling.

I. INTRODUCTION

In traditional computing everything data, software , libraries are stored in computer hardware only we can only access them if we have access to the system so companies need to invest their money on buying systems, servers, data centre (for backups) and if there is no need of the server in future it would be complete wastage of money. Companies also have to lay most of its concentration in building infrastructure for their business which again requires lot of money and human resource. But now a day due to advancement in technologies this method of computing is changed many companies are now migrating to cloud. Using cloud computing technique user can access data using internet from anywhere around the globe. Organizations do not need to lay emphasis on their infrastructure so they can focus more on their business operations, they can access servers, Virtual machine, Virtual network when there is need of it. Basically Cloud computing is on demand based services of storage, applications without actually buying it. It provides pay as you go service to the user. Instead of buying their own infrastructure or On Premises(Data Centres) ,Organizations can rent it from cloud service providers such as Microsoft Azure, Amazon Web Services.

Some benefits of cloud computing are as follows:

1) *Cost Optimized:* Cloud computing provides services which organizations do not need to actually buy it they can simply rent it on pay as you go basis means whatever and for what duration we are going to use that service we have to only pay for that duration only not for the duration which we have not use the service. By this way cloud computing saves money of an organization.
2) *Scalability:* Scalability means flexibility to add or remove resources or services according to the need of user. If there is much traffic the user can automatically add some more resources like the way flipkart do on big billion day.

3) *Business Continuity:* In case there is some natural calamity on particular data centre or someone has stolen the data, cloud computing provide measure for business continuity by making replicas of the data and softwares or some essential stuff on different data centres which is known as zones.
4) *Traffic Management:* Cloud computing services can automatically manage the traffic using traffic manager or load balancers.
5) *Quality Control:* Consistency of data, recording each and every updates or patches, by avoidance of Human errors can be maintained in a cloud-based system because all data, documents are stored in one single place in single format.

One of the Cloud computing models is Cloud storage which provide platform to store data, software and applications on some cloud storage platform which can be access through Internet These cloud computing vendors manages and operates data storage as a service. This data is only delivered when there is demand of it with just-in-time without any delay; it saves costs, and eliminates the need of an organization to actually buying and managing their own data storage infrastructure. This service provides you an agility, durability, and global scalability with accessibility of data anytime and anywhere around the globe. There are several requirements of cloud storage services which are as follows:

a) *Durability:* There should be no loss of data in case of any natural calamities or human mistake it should be available each and every time without failure.
b) *Availability:* Data should be delivered on time when there is need of it. The ideal cloud storage service should maintain the right balance of cost and retrieval times.
c) Security: Data should be not accessible to any un-authorize user in any case. Cloud storage should maintain CIA triad it should follow certain techniques or model to achieve it.

In this paper we are going to determine the architecture of cloud storage platforms, benefits of cloud storage, types of cloud storage, risk associated while migrating data on cloud storage platform and what are the cyber threats associated when data is already present in cloud storage platform, different security models and security analysis of current cloud platforms.

II. CLOUD STORAGE ARCHITECTURE

Architecture of Cloud storage is same as cloud computing in scalability, interfaces and it is based on virtualized infrastructure. Cloud storage architecture contains Public API's, Object Storage, Logical storage pools, virtual compute servers, physical storage servers and different cloud service locations for replication. Cloud Storage architecture is shown below:

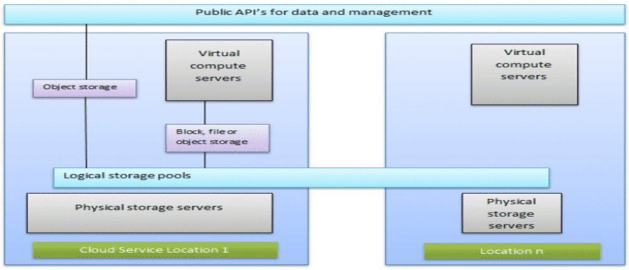


Fig 1 Cloud Architecture

Cloud storage architectures are primarily about delivery of storage on demand in a highly scalable and multi-tenant way. Generically, cloud storage architectures consist of a front end that exports an API to access the storage. In traditional storage systems, this API is the SCSI protocol; but in the cloud, these protocols are evolving. There, you can find Web service front ends, file-based front ends, and even more traditional front ends (such as Internet SCSI, or iSCSI). Behind the front end is a layer of middleware that I call the storage logic. This layer implements a variety of features, such as replication and data reduction, over the traditional data-placement algorithms (with consideration for geographic placement). Finally, the back end implements the physical storage for data. This may be an internal protocol that implements specific features or a traditional back end to the physical disks. Cloud storage architectures are primarily about delivery of storage on demand in a highly scalable and multi-tenant way. Generically, cloud storage architectures consist of a front end that exports an API to access the storage. In traditional storage systems, this API is the SCSI protocol; but in the cloud, these protocols are evolving. There, you can find Web service front ends, file-based front ends, and even more traditional front ends (such as Internet SCSI, or iSCSI). Behind the front end is a layer of middleware that I call the storage logic. This layer implements a variety of features, such as replication and data reduction, over the traditional data-placement algorithms (with consideration for geographic placement). Finally, the back end implements the physical storage for data. This may be an internal protocol that implements specific features or a traditional back end to the physical disks.

Cloud storage architectures are primarily about delivery of storage on demand in a highly scalable and multi-tenant way. Generically, cloud storage architectures consist of a front end that exports an API to access the storage. In traditional storage systems, this API is the SCSI protocol; but in the cloud, these protocols are evolving. There, you can find Web service front ends, file-based front ends, and even more traditional front ends (such as Internet SCSI, or iSCSI). Behind the front end is a layer of middleware that I call the storage logic. This layer implements a variety of features, such as replication and data reduction, over the traditional data-placement algorithms (with consideration for geographic placement). Finally, the back end implements the physical storage for data. This may be an internal protocol that implements specific features or a traditional back end to the physical disks. Cloud storage architectures focuses on delivery of storage on demand with scalability and multi-tenancy. Cloud storage architectures consist of a front end, middleware and backend. Front end layer exports an API so that it can access the storage. Middleware is the second layer it is responsible for data reduction as well as replication. It is basically the storage logic of cloud storage architecture. The last layer is the back end layer that is responsible for implementation of the physical storage for data**.**

Cloud storage architecture contains

1) Virtual Compute Server: It is cost effective this compute server can be shared by different operating systems.
2) Physical storage server: It is type of server where data is stored or it can be retrieved. It can be stored on your actual data centre or stored as replica on different data centres.
3) Data Service Location: It is the location where actual data is stored on data centre.
4) Object storage: It is type of storage where data is stored as distinct unit.
5) Logical Storage pools: Logical storage pool is collection of disk or volumes on which data is stored.

A. Types of Cloud Storage Systems

There are so many types of cloud storage systems like block storage system, file storage systems and Object storage system. So it is utmost important to analyze purpose and type of data to be stored because all these storage systems are used to store different types of data in different format and these all have certain and limitations too.

1) *Block Storage System:* Example of block storage system is Amazon EBS .It basically stores raw data of equal size volumes. In block storage the data is divided from user's environment and spread among different volumes so that it can be used easily whenever it is needed. This type of storage is generally used in email servers, virtual servers and so on.
2) *File Storage System:* In this storage system data stored is well structured and it is stored in single piece of volume. Here data is stored in particular hierarchy. It is one of the oldest forms of storage used in NAS (Network Attach Storage).
3) *Object Storage System:* It is used to store unstructured data like videos, audios and photos. It can be accessible by using HTTPS by creating easier way to access data using authentication, permission and properties.

B. Deployment Model Of Cloud Storage

Deployment model of cloud storage system used to define how cloud storage system is deployed and what the accessibility of cloud storage system is. Different deployment models of the cloud storage systems are:

1) *Public Cloud:* Public cloud storage example is Microsoft Azure and it is basically operated and managed by mostly third party cloud storage provider and it is delivered via internet. In this you will share hardware and software with different organization.
2) *Private Cloud:* This type of cloud storage is only used by one organization. In this storage everything from hardware to software is managed on private network. It is more flexible because it helps organization to customize it according to their need.
3) *Hybrid Cloud:* Basically it is combination of both private and public cloud storage. This also provides cloud bursting service when there is much load on private cloud it can switch to public cloud to meet the requirement.

C. Service Models Of Cloud Storage System

Service model provide details what type of service is provided by cloud service providers this can be in form of infrastructure, software and platform. Different types of cloud storage services are as follows:

1) *Infrastructure as a Service (IAAS):* This provide complete infrastructure including server and data centre. This prevents unnecessary expenditure by letting you know about for what you have paid for. This will increase or decrease resources as per the demand. Examples of IAAS are Amazon EC2, Google Compute engine, etc.

2) *Software as a Service (SAAS):* This service provides applications which can be use by any user with subscription using Internet. User doesn't need to install it on their systems. Examples of software as a service are Microsoft outlook, Gmail, etc.
3) *Platform as a Service:* Platform as service provides platform to the user so that he can develop application for his own need using different hardware and software on web service provider. It is build using virtualization technique and it can be accessible to multiple users. Examples of PaaS services are Amazon Elastic Beanstalk, Amazon EC2, RDS, etc.

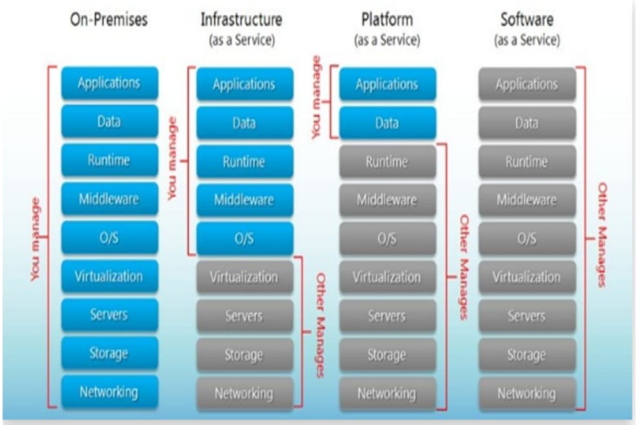


Fig 2 Cloud Service Model

III. RISKS ASSOCIATED WITH CLOUD STORAGE SYSTEM

As we know we can access cloud services, data, hardware and software through internet. Data stored on cloud storage system is more vulnerable to cyber attack if proper security measures are not adopted by cloud service providers. We have to follow certain guidelines and security measures while migrating data over cloud or accessing it because of several risk associated with it. Some security risks associated with cloud storage system are as follows:

1) *Confidential Data Loss:* In a recent survey it has came into picture than more than 21% of company data is very sensitive and requires severe protection. So there is major risk associated with data loss in cloud storage system.
2) *Loss of Control Over The Actions Of End:* In this type of risk cloud service provider or an organization is blank about end user action because they can illegally company's data for some illegal work.
3) *Malware Infections:* In this risk attacker can add malicious file along with data in cloud storage so that they can hamper the sensitive data of the company.
4) *Cloud API Vulnerability:* Vulnerability in the API of cloud can also be the reason for data breaches in the cloud storage system. This will also hamper the security of cloud storage system.
5) *Weak Cryptography:* Although Cloud service providers use encryption algorithms such as AES, RSA for data encryption but it is for limited time frame. Attackers can use different encoding techniques to decode the data.

IV. TYPES OF ATTACK ON SECURITY OF CLOUD STORAGE SYSTEM

There are so many attack vectors on data stored in cloud storage system but in this paper we will have glance at some of the attack vectors of cloud storage system because attackers are continuously developing latest vectors to attack sensitive data stored on cloud storage system. Some of the attack vectors are as follows:

1) Malware Injection Attacks: In this attack, attackers want to have access of user's information stored in the cloud storage system. This can be done by injecting some malicious code or file to the cloud storage system by infecting service module to SaaS, IaaS and PaaS. Examples of malware injection attack are SQL injection and cross site scripting attack.
2) Insider Attack: Insider attack is very dangerous because attacker is someone who is an employee or someone who has administrator privileges. So it is mandatory to develop secure architecture for cloud storage system with multiple level of authentication.
3) Denial of service attacks: It is most dangerous type of attack vector as many users will suffer from it. Denial of Service attack means making services, data or system unavailable to the users. If zombie machines are used it can effect multiple users.
4) Man in the Middle Attack: When someone is using personal or unprotected network attacker can have access to the cloud storage system. In this attack user does not know their system has hacked.

5) Cloud Services Abuse: Example of this type of attacks are Brute force attack and DoS attack. Attacker can use these attacks to gain access to the cloud storage of company after that they can do anything using this.
6) Account or service hijacking: Account hijacking can be done by using phishing technique, spyware and cooking poisoning. Attackers can have user's credentials to compromise cloud storage system of the user.
7) Spectre and Meltdown: In this type of attack attacker can read the information from the kernel of operating system. Attacker can read encrypted data using JavaScript code from memory by hampering the weakness or vulnerability in cloud storage system.

V. DATA SECURITY MODEL IN CLOUD STORAGE SYSTEM

There are three types of data in cloud storage system which is as follows:
1) Transmission Data: This type of data is known as transit data.
2) Storage Data: This data is basically archive data or data at rest which is not so frequently used.
3) Processing Data: Data which is being processed in order to complete an action is known as processing data.

Due to complexity in the different data type it is important to have secure architecture for data in cloud storage system.
The data security model in cloud storage system has three layered architecture where each and every layer performs its responsibility to enhance security of data storage system. Different cloud storage security layers are:
a) *Authentication Layer:* This layer ensures that only right or authorized person should have access to sensitive data. In case of private cloud storage system it provides multi factor authentication like MFA but one factor authentication in public cloud storage.
b) *Encryption Layer:* This layer ensures the encryption of data while transmitting and receiving the data so that attacker can't get access to the sensitive data. It uses one symmetric encryption algorithm for the protection of data.
c) *Recovery Layer:* Recovery layer is responsible for speedy recovery of encrypted data so that there is no chance of failure.

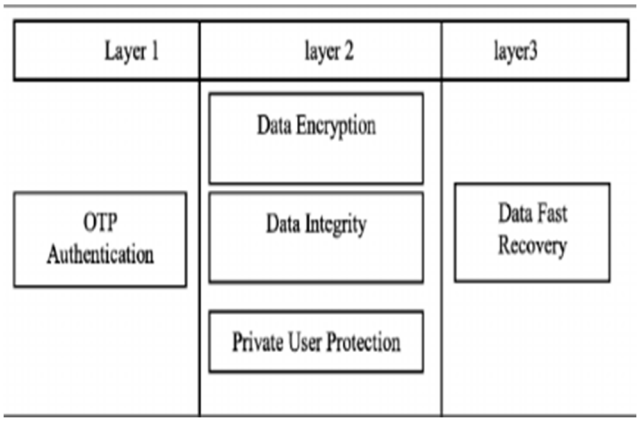


Fig 3 Data Security Model

We can improve this model by adding some security software to the cloud storage system. This software helps the user to select best and fastest encryption algorithm between eight encryption algorithms namely RC4, RC6, We compare between eight encryption methods based on P_MARS, AES, DES, 3DES, Two-Fish and Blowfish so that there is more security.

VI. WAYS TO IMPROVE SECURITY OF CLOUD STORAGE SYSTEM

Security of data in cloud storage system should be improved so that unauthorized user can not gain access of sensitive information. Cloud service provider as well as cloud user should be very responsible for security of data. There are several ways to improve security of cloud storage system some of them are as follows:

1) *Enhance Security Policies:* It is very important to make some security policies between vendors and user so that user should also understand their role in data security. Vendor should inform user about their role and what security measures they can adopt to secure their data.
2) *Secure Access and APIs:* Secure API using scripts ,recipes and templates should be only use in order to gain access to the cloud storage. This can be done by using VPNs or limited IP addressing

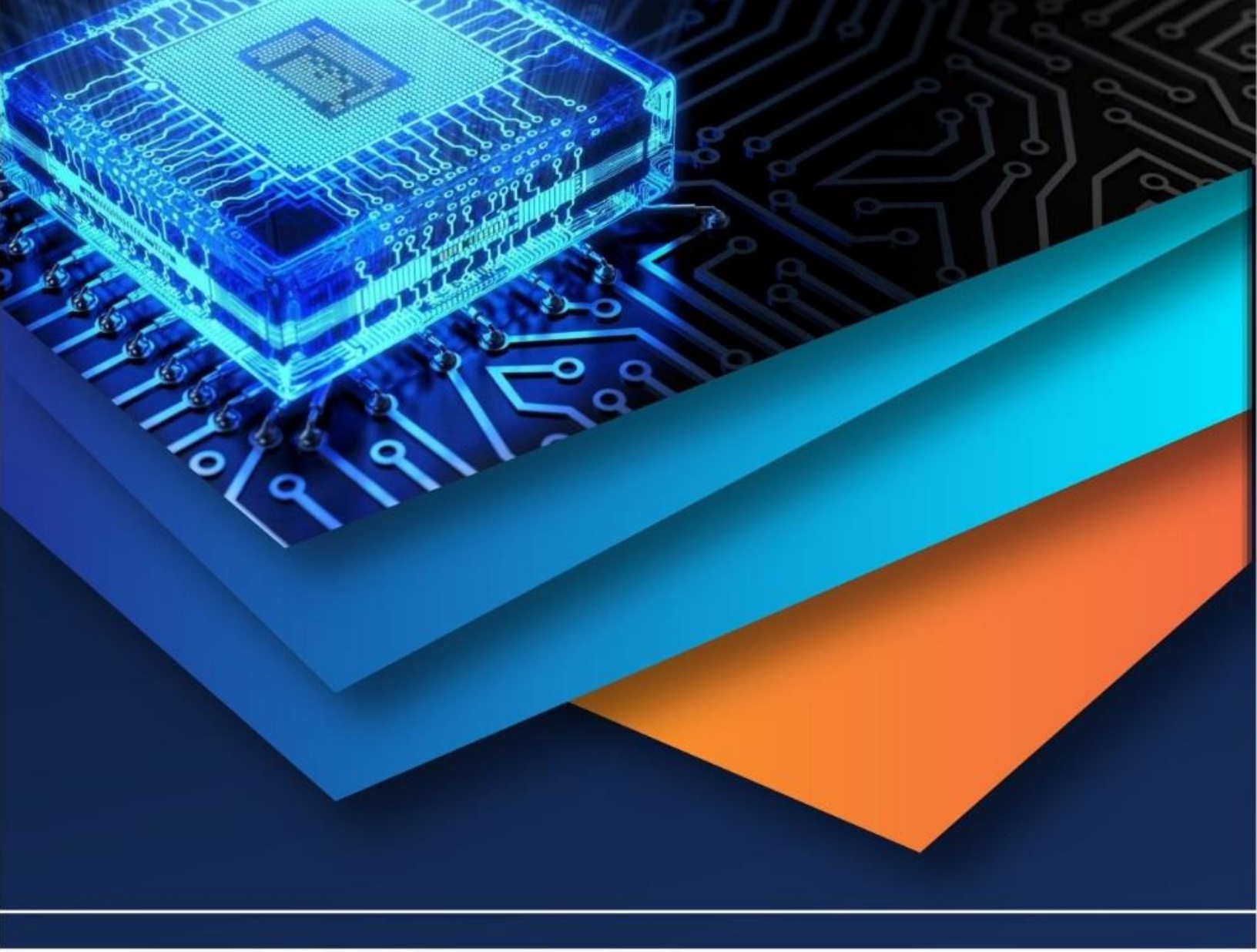
3) *Use Strong Authentication:* Strong authentication is very effective in cloud security because unauthorized user cannot get access to the data. Multi factor Authentication is used to enhance more security if in case user credential has been stolen still attacker can't access the sensitive data. This can be done in the form of 'One time Password'.
4) *Implement Access Management:* Roles should be assigned as per the need in order to secure cloud storage. Cloud Developers should provide permission to different administrations according to their roles as well as duties.
5) *Protect Data:* End to end encryption should be use so that there are zero chances of man in the middle attack. Proper encryption algorithms should be use while storing data, retrieving it and transmitting it to some other user. Salting and hashing can be use as strong encryption algorithms.
6) *SIEM and SOC System:* Proper SIEM and SOC system should be use so that attack can be detect at early stage and proper action can be taken immediately.

VII. CONCLUSIONS

Data stored in cloud storage system consists of 21% sensitive data on which whole operation of an organization depends. In case if this sensitive data is breached it can result in severe loss to the company. Attackers use several tactics in order to gain access to the cloud storage using brute force attack, SQL injection and cross site scripting. It is very essential in today's world to adopt proper measures as well as proper data security models because data in cloud storage is access via internet. Focus should lay to improve this models regularly because attackers are continuously developing new ways to hijack it. Proper SIEM environment should be established so that attack can be detect at early stage and proper action can be taken as soon as possible.

REFERENCES

[1] https://www.channelfutures.com/from-the-industry/5-benefits-and-3-drawbacks-of-using-cloud-storage-for-your-baas-offering
[2] Security for cloud storage system by Kan Yang, Xiaohua Jia - 1h40m Publisher: Springer © 2014
[3] https://pdfs.semanticscholar.org/870a/34ce835d2bae03a0aeacdeb08dcd889e124c.pdf
[4] https://phoenixnap.com/blog/cloud-security-threats-and-risks
[5] https://www.researchgate.net/publication/264235525_Data_Security_Model_for_Cloud_Computing
[6] https://www.skyhighnetworks.com/cloud-security-blog/9-cloud-computing-security-risks-every-company-faces/
[7] https://www.akamai.com/us/en/resources/data-security-in-cloud-computing.jsp
[8] https://insights.sei.cmu.edu/sei_blog/2018/03/12-risks-threats-vulnerabilities-in-moving-to-the-cloud.html
[9] https://www.zdnet.com/article/what-is-cloud-computing-everything-you-need-to-know-from-public-and-private-cloud-to-software-as-a/
[10] https://aws.amazon.com/what-is-cloud-storage/
[11] https://electricalfundablog.com/cloud-storage-architecture-types/
[12] https://www.researchgate.net/publication/239732057_Cloud_Storage_Architecture
[13] https://gomindsight.com/insights/blog/types-of-cloud-storage/
[14] https://www.redhat.com/en/topics/data-storage/file-block-object-storage
[15] https://azure.microsoft.com/en-us/overview/what-is-saas/
[16] https://www.bigcommerce.com/blog/saas-vs-paas-vs-iaas/#the-three-types-of-cloud-computing-service-models-explained
[17] https://www.cloudmanagementinsider.com/top-5-cloud-computing-security-issues-and-strategies-used-by-hackers/
[18] https://www.apriorit.com/dev-blog/523-cloud-computing-cyber-attacks
[19] https://www.researchgate.net/publication/261260707_Enhanced_data_security_model_for_cloud_computing



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY