ISSN No:-2456-2165

Improving Security Techniques for Shared Data in Cloud Computing

Amit Vikram
M. Tech (Software Engineering (SE)Student)
Department of Information Technology
Babasaheb Bhimrao Ambedkar University
Lucknow, India

Abstract:- A Today's, time there are large number of users associated in social media sites. They uses various number of social networking software and app. People connected with another people who they know but sometimes they also attached with unknown people. People shares their ideas with another people from social networking sites. There are different types of data for sharing. In these data's some data's are very common and general which does not effect on the privacy but some data are very confidential which should not shared to every people .During in this situation when the confidential data are shared it can be misused by another people. So it is necessary that there should be some restriction apply to social networking sites for data security. There should be data uses authority so that only authorized person can share the important data. There should be validation requirement so that unauthorized person cannot access or share the data. It is very necessary thing to secure the data of social networking sites and also the value of social networking sites.

I. INTRODUCTION

In the social networking sites there are large number of data in datasets. There are big challenges to manage the data and analyse the data which is more important or not. There are big target how to secure a data. There are different types of data for sharing. In these data's some data's are very common and general which does not effect on the privacy but some data are very confidential which should not shared to every people .During in this situation when the confidential data are shared it can be misused by another people. So it is necessary that there should be some restriction apply to social networking sites for data security. One of them is privacy. In these datasets there are also a shared data. So presently due to no restriction, any person who are associated with social networking sites can share any types of data to one another. There should be data uses authority so that only authorized person can share the important data .There should be validation requirement so that unauthorized person cannot access or share the data. It is very necessary thing to secure the data of social networking sites and also the value of social networking sites.

In cloud computing there are large numbers of data stored which are stored in network, storage area, devices etc and access on demand by the user. Here data and application are maintained by central remote server and internet and allows consumers to use application without installing and with the help of internet, user access the data which are stored in other computer or in mail.

II. FEATURES OF CLOUD COMPUTING

A. Big Area Network Access

In cloud computing there are large no of users who access their devices such as Laptops, Tablets, Android Sets and their Personal Computer in cloud computing environment in big area network.

B. Quick Services Availability

In this case there should no requirement of any person meet for help to consumer. Consumer can get help in quickly with server response in network data storage.

C. Place Independence Customer

There are no control over the resources location but may have some control at big level of abstraction. Consumer can control the stored data of country or state.

D. Pooled Resources

Many providers served to multiple consumer for help with the model of computing resources. It will dynamically assigned on demand of consumer

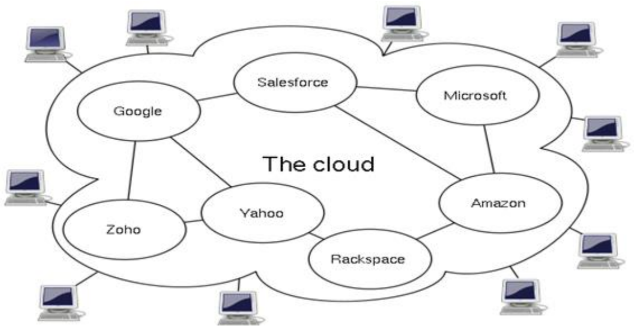

Fig 1:- Cloud Computing With Number Of Computer System

E. Data Security

Data security is a method or process of protect the data from unauthorized users access and data corruption throughout its various lifecycle .When we secure the data there are many things such as data encryption, tokenization and key management practices which protect data across all applications and platform.

F. Data Classification

Data are classified in many forms which are following:

- *Confidential*

Confidential data means it could not share with unauthorized person.

- *Sensitive*

Access of sensitive information should be granted to those who have a valid purpose for accessing such information..

- *Public*

It may include information which are collected for the purpose of public release with knowledge and consult of the individuals the information is about.

III. DATA SECURITY TECHNOLOGIES

A. Data Classification

Classification is the foundation of data security. It helps to prioritize the data i.e.it means which data is most important. There are many tools such as data mining tools which support both user driven and automated classification capabilities.

B. Data Access Policies

In data access policies only right data has been access by only authorize key members. The tools helps to discover sensitive data

C. Cloud Data Protection

In cloud data there is a hub of data where bulk data are available for accessing. There is main challenge of protection of data in data hub. In this case for protection point of view we use data in encrypted form.

D. Two-Factor Authentication

In two factor authentication, there is a password for accessing data which is used by only authorize user. If the password is guessed correctly by hacker, the second step will be automatically stopped and if the password is stolen, attackers cannot get into the account.

E. Tokenization

In tokenization, we use credit card, debit card very securely i.e. cvv and card number should not be share.

❖ *Different Security Work On Data Security*

A. Network Security

It is a technique where technical team develop a mechanism of a whole computer network security so that any confidential data could not be hacked or stolen.

B. Application Security

Application which works on a computer system should be password protected. Password should be encrypted form.

C. Mobile Security

Mobile should have a locked system. It should be open only by patterns or given password.

IV. RELATED WORK

A. In Network Data Sharing, Distributed Authentication & Authorization:

- *Authorization*

Authorization is a security mechanism to obtain the accessing of internet by only authorize user in different level of internet accessing where they use different types of important file, document in networking during file sharing.

In computer network system, access control policy devided in two phases:

- Policy definition phase where access is authorized.
- Policy enforcement phase where access request are permitted or not permitted.

- *Authentication*

Authentication verifying the identity of person who access any confidential data during the accessing of net or in a system . A common example is entering a User Name & Password when we log into a website. Enter the correct login lets the website know:

- Who we are and
- That it is actually we accessing the website.

There are so many users with mobile devices and small gadgets, such as sensors, actuators, and robots, are generating tremendous amount of data. This is known as big data, which is characterized by the following five aspects: volume, variety, velocity, value, and complexity. Big data has attracted significant attention regarding the development of business applications, including internet of things (IOT) service and photo/video sharing. It is growing rapidly as one of the major segments of the current IT industry. One of the foundations of big data applications is the data sharing service that provides data to various entities efficiently. Currently, most of big data sharing services are designed based on internet technologies, which were designed originally for end-to-end communications.

Most of these are implemented based on centralized servers/ clouds. Thus, big data is distributed from distant servers/clouds to users, possibly through similar paths. Because of this, the current big data sharing applications result in large redundancies and duplicate traffic, as well as high latency. Take a big data provision service platform for example. The various data, such as transportation, healthcare, and habit data for local users is generated, stored, and processed. The data might be generated periodically, resulting in a considerable data volume, and the big data services after analysis are targeted mostly at these local users. Obviously, it is costly to store all data in remote servers/clouds and then provide a return service.

B. Phases of Cloud Computing

In cloud computing environment there are five major actors in cloud computing based on their participation as shown in Fig (a).. Cloud consumer or cloud service consumer (CSC) is the one who gets the service from a cloud provider and pays for the service as per the use. Cloud provider or cloud service provider (CSP) is the one who provides the cloud services to the CSC. Cloud auditor manages cloud services independent assessments, information system operations, all securities and performance of the cloud implementations .Cloud broker is the one who interacts between CSP and CSC to make the business happen. Cloud carrier is the one who provides the connectivity and cloud services from CSP to CSC.

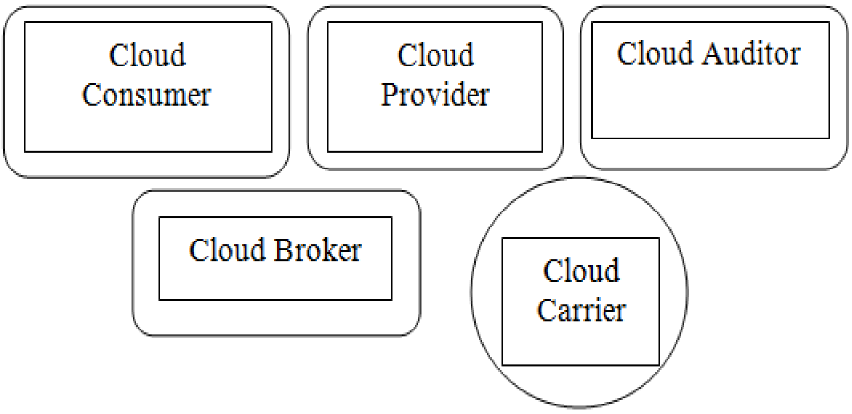

Fig 2

V. PROBLEMS OF SECURITY DATA AND DIFFICULTIES

In enterprise computing, data is stored within their organization and it is fully under the control of the enterprise. The data is stored outside the customer's place (in the CSP's side).It must employ additional security measures apart from the traditional security checks to ensure that data is safe and no data breaches due to security vulnerabilities.

A. Data Security Basics

There are six stages in the life cycle of data: Create, Store, Use, Share, Archive and Destroy. Once the data is created, it can move freely between any stages. Data should be secured in all the stages of its life cycle from its creation to its destruction. The store and archive stages are also called as data-at-rest, the use stage is called as data-in-use, the sharing stage is called as data-in-transit and the destroy stage can be called as data-after-delete. All these stages are self-explanatory. Generally, encryption is one of the methods in the data-in-transmit stage to protect the data. One of the neglected issues is data-after-delete and this is also called as data remanence. Data remanence is the residual physical representation of the data that has been deleted. After a storage media is deleted, there may be some physical characteristics that allow the data to be reconstructed. Tracing the data path (data lineage) is important for auditing in cloud computing, especially in the public cloud apart from the above stages.

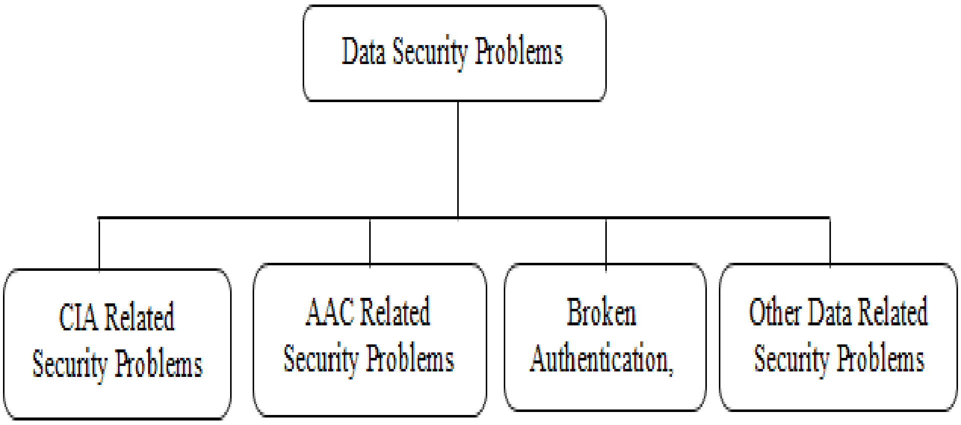
Data Security Problems
CIA Related Security Problems
AAC Related Security Problems
Broken Authentication,
Other Data Related Security Problems

Fig 3

- ➢ CIA: Confidentiality, Integrity And Availability
- ➢ AAC: Authentication & Access Control

- *Security Challenges in the CIA Triad* Confidentiality, Integrity and Availability (CIA) losses can make a big impact in the business of the cloud computing because the data is the core component for any business. Data integrity shows corrected digital information and only be accessed authorized persons. Thus, integrity involves maintaining the accuracy, consistency and trustworthiness of data over its entire life cycle. Maintaining CIA is easier in enterprise computing but in cloud computing it is more complicated because of the multi-tenant architecture and the distributed nature of the infrastructure. The following steps can be used to maintain a proper CIA in cloud computing:

- Once the data are created, classify the data, identify the sensitive data, define policies, and create access methods for different types of data. Also, create policies for data archive and data destroy.
- Store data with proper physical and logical security protection, including the backup and recovery plan.
- Identify which type of data can be shared, whom and how it can be shared and define data sharing policies These policies in cloud computing is known as Service Level Agreement.
- Create a corrective action plan in case data is corrupted or hacked due to network or communication devices, security flaws while data is in transit.

B. Difficulties Of Security in the Authentication and Access Control (AAC):

Authentication and Access Control (AAC) is the process of verification and confirmation on user's identity to connect, to access and use the cloud resources. In enterprise computing, the credentials are stored in the server in the form of Active Directory (AD) or Lightweight Directory Access Protocol (LDAP).Authentication done virtually through private network in private cloud. In public cloud, customers use the internet to connect to CSP(Cloud Service Provider), applications from different users can co-exist with the same CSP(Cloud Service Provider) (resource pooling) and CSC(Cloud Service Consumer) can access the applications from anywhere through any devices. So In public cloud, authentication is too weak and without protection than private cloud . A Password-based authentication does not provide effective security for the public cloud. Passwords can be cracked using many methods such as a brute force attack, dictionary attack, phishing or social engineering attack. So it is very important that the CSP (Cloud Service Provider) should include highly secured authentication methods in a public cloud. Customers connected to cloud services in cloud computing through APIs and API's are designed to accept tokens compare to passwords. In cloud computing, authentication applies to not only users but also to machines. Machines need to authorize certain automated actions like online backup, patching and updating systems and remote monitoring system. Since the cloud applications are accessed through various devices, there should be a strong authentication method like RSA token, OTP over the phone, smart card / PKI, biometrics, etc., for original identification confirmation and show their value.. This will enable identifiers and attributes with a strong level of authentication to be passed on to the cloud application and the risk decisions can be made for access management. There are a number of methods and standards available to avoid security issues related to AAC.

C. Key Related Security Issues:

➢ There are large no. of possibilities of internal attacks in cloud platform. Without the knowledge of end user key can be access or stolen by employer.

➢ All keys needs to be securely managed. There will be challenge to take key with their index properly.

➢ Another problem related to key is availability during offline mode. In this case key should be properly order in cache so that we can get the key in offline mode.

VI. SOLUTION OF SECURITY RELATED ISSUES

- Employer access should be limited. Monitor each task of employer.
- We use encryption key for security purpose. To safe encryption key we should mail to employer. All process should be done in encrypted form in cloud environment.
- Encryption key should not store at the same place as a role of encrypted data. Sensitive customer can encrypt the key. Key should be rotate time to time.

❖ *Problem Generate During Data Sharing*

➢ *Data Misuse Problem*

There are many types of data which are confidential and non confidential. Non confidential data are general data which can be used by any person that does not effect security part. It does not generate any issues which are related to cyber security. But when we talk about confidential data this data is more important. It should not be access by any person due to security point of view. If these data access by unauthorized person it will be generating a big problem or issues. For eg. Defense related data, Banking data etc.

➢ *Help To Hacker*

Hacker hacks the data or software from our system which are more important and confidential. So when we shared a data without any restriction or security it can be transfer to any person who are in social networking sites In social networking sites there are different types of people where we don't know personally about them. There are good or bad both types of people. In these people there may be hacker who misuse our data very easily without applying any hacking technique.

➢ *Unauthorised Person Can Use Access Control:*

Data store on the cloud should be under data owner control, Only designated user can access to the data while the cloud provides should not get any right to access the data.

➢ *Integrity*

The system should detect any unauthorized changes. i.e. any changes done by unauthorized person in the database or in coding section it should not be edited.

VII. RELATED QUESTION

Q1.How we prevent confidential data in social media site during sharing online?

Q2.How we authorized other person to access confidential data?

❖ ***Ans 1.*** *Securities Jobs In Big Data Network:*

J1: Big data Integrity: Data name and data not modified by attackers who might locate at forwarding device. There should be guarantee linked between data name and data..

J2:Safe Registration :Register, user and forwarding device register securely to Network Operator and Authority. It is the foundation for further securing data publications and retrieval.

J3: Data Retrieval Safely: There is authentications from publishers or forwarding device to users are received based on interests from users and from users to publishers authentication can be performed when data is received by users during the data retrieval procedure.

J4: Flexible and Efficient Authorization: Active publisher publish big data according to publisher policy and permit authorize users to access a flexible set of big data. Meaning of flexibility means changeability and adaptability. So different data might be required and authorized for a user to access under different cases..

J5: Design should be distributed: It should be authorize to retrieval data and restrict accessing enable only for ubiquitously in-network cached big data.

❖ ***Ans 2.*** *Three principles to guide sharing security information across organization:*

A. Share Minimum Information:

In share minimum information, we cannot share whole information. We can share only a part of information. It is beneficial against risk. In this case there is limited purpose where data goal in mind but also we should think which should shared or stored, it should be less or minimum no of quantity.

B. Evaluation Of Qualitative:

In evaluation of qualitative, there are two types of constraints which are (a) Legal Constraints (b) Technical Constraints

➢ *Legal Constraints*

In legal constraints sharing of data must be flexible and it supports ethical and legal constraints and their subjective determination.

➢ *Technical Constraints*

It apply technical methods alone which cannot insure complete privacy while allowing forward progress.

C. Forward Progress Techniques:

In this technique there is participating organization is necessary to improve security and encourage to promote area of research. When information shared between two people there will b e mutual understanding between them.

There are many techniques to prevent confidential data during storing which are following:

➢ *Password Protected Shared Subject:*

When we are online we have many subjects and matter which may be shared to other people. Some subjects or matter are non confidential which may be shared to all people because it does not generate any issues. But some matter are very confidential that should not be shared to every people. It should only be shared to authorize people. So in this case matter or subject should be password protected. It means it should only be open when password enter. When matter shared to other people, it should not shown by other people. It should open only by enter the password.

➢ *Read Only Subject or Matter:*

Subject or matter should be read only mode. It means it should not be changed or modified by any person.

REFERENCES

[1]. Jose Moura , Carlos Serrao (Security and Privacy Issues of Big Data)

[2]. Gayatri.K.S., Tony Thomas, J.Jayasudha (Security Issues of Media Sharing in Social Cloud)

[3]. C. Zhang, J. Sun, X. Zhu (Privacy and security for online social networks: challenges and opportunities)

[4]. N. Ramazan , C.Patrikakis (Analysing Multimedia Content in Social Networking Environments.)

[5]. Astha Mishra(Data Security in cloud computing based on advanced secret sharing key management system)

[6]. Venkata Sravan Kumar Maddineni Shivashanker Ragi (Security Techniques for Protecting Data in Cloud