**3.Data Security Issues or Challenges**

The data is stored within the organization, in enterprise computing. The data is stored in the CSP’s side in cloud computing. Thus, cloud computing must employ additional security procedures to check whether the data is safe or not and ensure that no data breaches due to security vulnerabilities.

In the life cycle of the data, there are six stages. They are Create, Store, Use, Share, Archive and Destroy. The data can move between the stages, after the data is created. Security of the data in all the stages of its life cycle is very important. All the stages of the data are self-explanatory. There are some other names for the stages. The store and archive stages are 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 is called as data-after-delete. All these stages are self-explanatory. Encryption is one of the general methods to secure the data in the data-in-transmit stage. Data-after-delete or data remanence is one of the neglected issues. The residual physical representation of the data that has been deleted is defined as data remanence. After the deletion of the storage media, there will be some physical features to allow the data to reconstructed. Data lineage which is tracing the data path, is important for auditing, in cloud computing. Especially, it is important in public cloud apart from the stages of the data.

CIA triad is the short form of the three important assets of the data. The assets are Confidentiality, Integrity and Availability. Authentication, authorization and nonrepudiation are another three important properties associated with people who access the data [14]. Data privacy of the data which belong to CSC are not revealed to unauthorized parties on any case is denoted by Confidentiality[15]. The confidence that the data stored in the cloud is not fiddled by unauthorized parties is denoted by the Integrity of data . Integrity is also applicable during the data is in transit. Whenever the CSC needs data, the data should be available to them without any delay or deny is denoted by Availability of data. These three are the basic data security properties and these are tested in the pubic cloud deployment model. The own data of the person is accessible when the person has Authentication. Determine a person has rights to access the data is called as Authorization. The users must be authenticated before carrying out the activity which are authorized to do. Non repudiation is the assurance which defined that authenticated users cannot deny after performing in the data. The following fig. 2 illustrates the four major categories of data security issues in cloud computing.

3.1. Security Challenges in the CIA Triad

Because the data is the core component for any business, the loose of Confidentiality, Integrity and Availability (CIA) will be created a big impact in the business of the cloud computing . Data integrity is the assurance which is given to the digital information, is uncorrupted and only authorized users can access the data. Therefore, integrity maintains the accuracy, consistency and trustworthiness of data[16]. Because of the multi-tenant architecture and the distributed nature of the infrastructure, maintaining CIA is more complicated in cloud computing. The following steps are very valuable to maintain a proper CIA in cloud computing.

* After the creation of the data, classify the data, identify the sensitive data, characterize policies, and create access methods for various kinds of data. And also, produce policies for data archive and data destroy.
* Store the data which are secure with proper physical and logical security protection, as well as the backup and recovery plan.
* Identify the type of data which are going to be shared, whom and how it are going to be shared and define data sharing policies. Data sharing policies are called as Service Level Agreements (SLA) in cloud computing.
* Establish a correct action plan to protect the data from being corrupted or hacked due to network or communication devices.

According to Aldossary and Allen, integrity should be checked not only at data, but also at the competition level [4]. According to Aldossary and Allen, integrity should be checked not only at data, but also at the competition level [4]. Only the authorized applications are permitted to access the data and use it for computation is described by Computation integrity. Any irregularity from normal computing should be avoided. Loss of confidentiality and integrity are avoided effective identity and Access Management (IAM). Loss of data and data inaccessibility causes loss of availability. Cloud computing utilizes few techniques similar to scalability and high availability at the architecture level. To improve data security related to the CIA triad at different stages of the data lifecycle, there are different methods and procedures are followed.

* When the data is in rest and transit use data encryption. Utilize strong encryption algorithms similar to Advanced Encryption Standard (AES) and Rivest Shamir Adleman (RSA) algorithms. Various kinds of encryption methods are defined in [4]. Amazon S3 utilizes one of the greatest encryption algorithms, 256-bit AES [9].
* To provide confidentiality against attacks from a cloud provider encryption methods are used . However encryption methods are unable to protect data against configuration errors and software bugs [4]. Hash methods are used to figure out accidental and intentional data changes. Although these changes consume more bandwidth and time-consuming.
* Third Party Auditing (TPA) will be engaged to check the data integrity. Many researchers [4] claims to audit data integrity by third-party auditors because of the specialization of them.
* Provable Data Possession (PDP) scheme was initiated by Ateniese et al. to investigate statistically the accuracy of the data without regaining the data outsourced to cloud storage [20]. PDP limitations were overwhelmed by Ateniese et al. themselves at [21, 22], Wang et al. at [23] and Sookhak et al. at [24].
* It is not a good point to store the encryption keys along with the encrypted data.
* To access data, implement a proper Identity and Access Management (IAM) techniques for users.
* To address availability issues, make use of data duplication, redundancy, backups and resilient systems.
* Involve a failover strategy if the service fails with the CSP.
* If other methods are not effective, use data dispersion technique to address the availability issue. The data is stored as fragments and can be reconstructed when there was a requirement to use fragmentation techniques.

3.2. Security Challenges in the Authentication and Access Control (AAC)

Directory Access Protocol (LDAP), the credentials are stored in the server, in enterprise computing. The authentication is done same as the enterprise computing via a virtual private network in a private cloud. In public cloud, internet is used to connect to CSP, The applications from the same CSP (resource pooling) and CSC can be accessed from anywhere through any devices. Thus, the authentication in private cloud is less vulnerable than public cloud. Effective security for the public cloud cannot be provided by a Password-based authentication. Many methods such as a brute force attack, dictionary attack, phishing or social engineering attack can cracked passwords. Hence, in a public cloud ensure that the CSP should include highly secured authentication methods. APIs accept tokens instead of passwords. Users connect to cloud services through APIs in cloud computing. Authentication is also applicable to machines in cloud computing. Machines need to authorize certain automated actions like online backup, patching and updating systems and remote monitoring systems [26]. Since various devices are accessed by the cloud applications, there is a need for strong authentication method such as RSA token, OTP over the phone, smart card / PKI, and biometrics, for the original identity confirmation and determine the type of credentials [6]. Identifiers and attributes will be enabled with a strong level of authentication to be passed on to the cloud application. To avoid security issues related to AAC there are a some methods and standards. The following methods are important to mitigate AAC security challenges.

* Apply single-sign-on policy.
* Multi-factor authentication are active which allows both identity and access management and it is used Amazon Web Services (AWS) [9].
* Biometric authentication is to be the most secure form single-sign-on authentication.
* RSA cryptosystem accepts different authentication models like two-factor authentication, knowledge-based authentication and adaptive authentication. The beyond methods are very effective for the protection of data in cloud computing [28].
* Intrusion Detection System (IDS), firewalls as well as segregation of obligations is implemented on the different network and cloud layers to enable proper access control in cloud computing for the protection of the data [28].
* There are numerous third-party identity management solutions. Utilize some third-party solutions such as Microsoft Azure Active Directory, Okta identity management and McAfee cloud identity manager. In Recent Times, Identity-Management-as-a-Service (IDaaS) solutions are getting more popular in the corporate infrastructure [29].

3.3. Security Challenges Due to Broken Authentication, Session and Access Controls

Due to inappropriate implementation of authentication and session management in the application domain, broken authentication and session control threat arises. For the example user credentials are not properly secured. Attacker takes benefit of the situation and compromise passwords, keys, session tokens or to exploit other implementation flaws to assume another identity of users[30]. Commonly, the privileged accounts are targeted by the attackers. When there is a lack of enforcement of limitation on which authenticated users are allowed to access, broken access control threat occurs . Using this loophole, attackers can access the account of another user, view sensitive files, modify the data and change access rights [30]. The above methods can be used to reduce these challenges.

* Implement a single set of solid authentication and session management controls.
* Avoid Cross-site Scripting (XSS) flaws which are used to steal session IDs.
* Check Access – Each use of a straightforward reference from an untrusted source must be verified for access control to make sure that the user is authorized for the requested resource.
* Use user or session indirect object references – the coding pattern precludes attackers from directly aiming unauthorized resource.
* Automated verification – Apply automation to verify proper authentication deployment.

3.4. Other Data Related Security Issues

Through Data location, Multi-tenancy and Backup, other data related security issues happen in cloud computing. The data is stored in a diverse geographic location with various legal jurisdictions in cloud computing. There will be a thread to the CSC’s data, if the data location is not safe physically and logically. Data is vulnerable to malicious insiders and external hackers to avoid these kind of situations. Multiple users can store the data in the same location using physical or virtual storage concept due to the multi-tenant nature of the cloud computing . Because of this scenario, a user can intrude into another user’s data location. All data, especially the sensitive data should be regularly backed up and tested for proper data recovery in cloud computing. A Backup is a form of data-at-rest. Strong encryption schemes are used to protect backup data (especially the sensitive data) [4]. There are two types of backup. They are on-site backup and cloud-based backup. The backup plan is selected based on the cost, type of business and data. On-site backup is cheaper, easier to set up and runs faster. If any natural disasters happens, then all the data including the backup will lost. To avoid the issue cloud-based backup is used. CSC’s data is stored off-site with the cloud. The following methods will help to overcome other data related security issues.

* Be aware of the logical and physical location of CSC data, otherwise at least any state, country and data center is attention to all possible regulatory, contractual and other jurisdictions
* Determine location and jurisdictional policies to regulate the data location.
* To separate the data from different users, accept smart data segregation techniques.
* To avoid data leakage, use great encryption techniques for the data backup.