**ABSTRACT**

Cloud computing is considered as the hopeful standard for distributing IT facilities as computing benefits. Several industries like banking, healthcare and education are moving towards the cloud due to the effectiveness of services provided by the pay-per-use pattern based on the resources equivalent to process power used, transactions administered, bandwidth consumed, knowledge transferred, or storage space occupied etc. Cloud computing is totally in web dependent technology wherever client data is kept and maintained within the cloud provider’s data center like Google, Amazon, Microsoft, Akamai, etc. Inadequate control over the data may procure several security concerns and threats which include data leakage, insecure interface, sharing of resources, data availability and insider attacks, which leads to cybercrimes in cloud environment. On the off chance that the organizations and clients are given web get to, they can get to their own records specifically from any side of the world. This innovation supports fruitful computing by coordinating information storage, processing and transfer speed... In Cloud, security of information isn't ensured and even the information can likewise be gotten to by the third party. There is a need to consequently, we have planned a protected document stockpiling framework with effortlessness, legitimacy and security. Nearly it is connected in everything which required giving consent to just affirmed approvals Consequently, we have planned a protected document stockpiling framework with effortlessness, legitimacy and security. Nearly it is connected in everything which required giving consent to just affirmed approvals on averting information release, warning for security mischance and security occurrence reviews. Cloud security needs to be enriched with the conventional methods like firewalls, Virtual Private Networks (VPN) and Security policies to get a carefully designed ripe administration from it. In any case, Cloud computing brings new difficulties, issues and dangers to the business. From many research it is observed that security is the main problem of cloud adoption. The dread of losing control of corporate information and the danger of data breaches in the cloud can possibly disturb the adoption of cloud services. Security issues must be addressed and new technologies must be produced in order to open cloud computing benefits. For retrieving the data in the cloud, clients need more security for guarding their data. Encryption and Hashing technique is being used in the cloud environment by carrying a key exchange process done with key encryption key and data encryption key to provide security. Also SHA3 hashing function is used for accomplishing data integrity and security in the cloud. This Proposed method looks in to an attack model based on threat model to overcome the Multi-tenancy situation. Additionally, resource allotment method will accomplish the balance between both the advantages gained from Multi-Tenancy and Security. To minimize the security threats and preserve the privacy, reliability and authenticity of data which is stored in cloud, Encryption and hashing techniques will be used. Consequently, we have designed a protected file storage system with effortlessness, legitimacy and security. Nearly it is connected in everything which required giving permission to just certified authorizations. In the database, the password is stored as a message digest. This sort of storing password should be carefully designed. The encryption procedure makes the data secure and it prevents clarity by unauthorized persons and furthermore it sets up a system to remove imposture. This system has been designed in such a way, if the one-way hash function gets cracked, it will lead to get the encrypted data alone. The usage of hash function makes impossible for any overlooked changes on data. After the deployment of RSA and SHA3 (Keccak) before Storage, the data becomes impervious to access or changes by any third party and to the capacity framework. In this manner by creating a two factor security verification of data which is stored in cloud will be a protected environment for the multitenant users to protect their data from cybercrimes. This will help the clients information to be more secured in the cloud platform.