ABSTRACT

The main aim of the project is to create a model for secured data storage on public cloud. The use of online services is expanding daily, having a significant impact on businesses switching to cloud-based services. The main concern in cloud is the amount of storage required and when scaled is it going to cut the budget that the corporation/organisation must spend. The proposed system works on multi data storage using secret key sharing algorithm. The user can upload their files on the cloud and the file is split into three parts by secret sharing algorithm. The necessary blocks are encrypted by Advanced Encryption Standard (AES) algorithm. This provides high security to the data stored on the cloud. The user can retrieve the decrypted data by requesting the domain manager for a dynamic secret key and storage protection scheme for addressing access control. In our model, all the cryptographic operations are performed on trusted IaaS compute hosts and storage protection scheme for addressing access control. This provides high security to the data stored on the cloud. This uses the cloud services more efficiently and effectively with very low downtime.

KEYWORDS - Public Cloud, Dynamic Secret key, Tenant, Random Split, Encryption, Decryption, Secret Key Sharing