**SYSTEM ANALYSIS**

**EXISTING SYSTEM:**

In existing framework single calculation is utilized for information encode and unravel reason. Yet, utilization of single calculation isn't achieve elevated level security. On the off chance that we utilize single symmetric key cryptography calculation than we need to confront security issue on the grounds that in this kind of calculation applies a solitary key for information encode and interpret. So key transmission issue happen while sharing key into multiuser climate. Public key cryptography calculations achieve high security however most extreme postponement is required for information encode and translate.

* more data storage needs turning over to the cloud, finding a secure and efficient data access structure has become a major research issue
* Security techniques are not applied in the protection of offloaded data from attacks.
* Once uploaded and shared, the data owner inevitably loses control over the data, opening the door to unauthorized data access.

**PROPOSED SYSTEM:**

Selectively sharing data files on the cloud becomes a burden on the data owner as the hierarchy grows (the access privileges increase in number) and/or as the access restrictions become more complex due to an increase in the sensitivity of the file segments. A trivial solution involves the data owner to use public key encryption. This solution would require the data owner to encrypt the same part of the data file once for each data user being granted access then upload the resulting cipher texts to the cloud. The data users would then fetch their uniquely encrypted parts of the file from the cloud and utilize their private keys to decrypt them. This method ensures that no unprivileged data user will gain access to any part of the data file even if that user is able to download the cipher texts from the cloud. However, on a large scale, public key encryption becomes an inefficient solution due to the increase in the number of encryptions and large storage spaces required. Therefore, the challenge is to provide the data owners with an efficient, secure and privilege-based method that allows them to selectively share their data files among multiple data users while minimizing the required cloud storage space needed to store the encrypted data segments.

* Requiring less network communication.
* We present multiple data file partitioning techniques and propose a privilege-based access structure that facilitate data sharing in hierarchical settings.
* A new security layer is added to encrypt the data of the task before transferring to the cloud side by using AES encryption technique.