**SYSTEM ANALYSIS**

**Existing System**

Although the existing schemes aim at providing integrity verification for different data storage systems, data dynamics has not been fully addressed. How to achieve a secure and efficient design to seamlessly integrate these two important components for data storage service remains an open challenging task in Cloud storage.

**DISADVANTAGES OF EXISTING SYSTEM:**

Although the infrastructures under the cloud are much more powerful and reliable than personal computing devices, they are still facing the broad range of both internal and external threats for data integrity.

Second, there do exist various motivations for CSP to behave unfaithfully toward the cloud users regarding their outsourced data status.

In particular, simply downloading all the data for its integrity verification is not a practical solution due to the expensiveness in I/O and transmission cost across the network. Besides, it is often insufficient to detect the data corruption only when accessing the data, as it does not give users correctness assurance for those unaccessed data and might be too late to recover the data loss or damage.

Encryption does not completely solve the problem of protecting data privacy against clous service provider but just reduces it to the complex key management domain. Unauthorized data leakage still remains possible due to the potential exposure of decryption keys.

**Proposed System:**

proposed the use of the convergent encryption, i.e., deriving keys from the hash of plaintext. Then, Storer et al. pointed out some security problems, and presented a security model for secure data deduplication. However,these two protocols focus on server-side deduplication and do not consider data leakage settings, against malicious users.

Advantage:

1. As a rising subject, cloud storage is playing an increasingly important role in the decision support activity of every walk of life.
2. Get Efficient Item set result based on the deduplication.