**SYSTEM ANALYSIS**

**EXISTING SYSTEM:**

* Huang and Tso proposed an asymmetric encryption mechanism for databases in the cloud. In the proposed mechanism, the commutative encryption is applied on data more than once and the order of public/private key used for encryption/decryption does not matter.
* Re encryption mechanism is also used in the proposed scheme which shows that the cipher-text data is encrypted once again for duality.

**DISADVANTAGES OF EXISTING SYSTEM:**

* Data confidentiality occurs because the users do not trust the cloud providers and cloud storage service providers are virtually impossible to eliminate potential insider threat, it is very dangerous for users to store their sensitive data in cloud storage directly. Simple encryption is faced with the key management problem and cannot support complex requirements such as query, parallel modification, and fine grained authorization.
* One of the main drawbacks of cloud is that there are too much of possibility for the cloud service provider for the misuse of the data that is stored in their data center by the client. Due to this, whatever methods that are proposed don't have direct impact to reduce this problem. There will be issues continuing in the cloud computing until the cloud service provider knowledge about the data is prohibited. There is also repeated usage of OTP method in the cloud computing techniques which makes this system to an inefficient one.

**PROPOSED SYSTEM:**

1) Username and the Password provided by the client to the cloud service provider. The password is encrypted by Hybrid Encryption method such as RSA, Ceaser cipher and alphabetic encryption

2) Cloud Service Provider (CSP) authenticates the user by verifying username and password by decryption and sends with the login key for the Security Vendor.

3) User space in CSP and the memory address allocated for the user is given by the Cloud Service Provider to the Security Vendor.

4) Login key for Security vendor

5) User authenticated with key provided by Cloud Service Provider

6) User selects the encryption method for various options that CSP does not aware of and stores the data

7) Security vendor sends the encrypted data to Cloud Service Provider

**ADVANTAGES OF PROPOSED SYSTEM:**

* More Secure System
* Results show better performance evaluation when compared with existing system