**SYSTEM ANALYSIS**

**EXISISTING SYSTEM**

The keys might be available within the cloud platform or near to the physical drive in case of FDE. The key management process does not include the cloud application user. Even though the data of user is encrypted on the physical disk, any layer present below it can access it at any time. Thus, the access of data to unauthorized users of online attacks is not prevented by FDE approach. The data cannot be learnt or leaked easily through the un-trusted applications when FHE is applied. The FHE encryption keys are owned and managed by the users. However, without seeing the data actually, computations can be performed on encrypted forms by the applications.

**DISADVANTAGES OF EXISISTING SYSTEM:-**

* There are, several security and maintenance related challenges being faced by the technologies today which cannot be resolved by applying the FDE and FHE.
* Since the access control granularity and key granularity are not lined up, it is important for a user to completely rely on the cloud provider for providing the right access control in the presence of FDE. There is no exact way defined for providing access control yet, since the encryption keys are managed by the user or third party cloud provider in case of FHE.
* There is no impact of FDE on the development of application since it is hidden behind an abstraction of physical disk

**PROPOSED SYSTEM**

In the proposed system an architecture using which the file at user’s end can be encrypted and decrypted such that the security of data during transmission can be exchanged. The Rijndael Encryption Algorithm is used along with Extensible Authentication Protocol Challenge Handshake Authentication Protocol EAP-CHAP within this paper. Cloud computing security is the major concern of clients today due to which adopting the cloud computing services to provide privacy protection and data security is necessary. Therefore, the client side security is ensured in this paper. The data can only be accessed by the authorized user by the proposed system. The decryption of data is not possible by the intruder even though he gets access to the data. Therefore, by applying the proposed technique better security algorithm is provided through encryption..

**ADVANTAGES OF PROPOSED SYSTEM:-**

* In order to protect the data from cloud infrastructure provider different techniques have been utilized by researchers. Further, the FHE techniques are applied (CHAP).
* A distributed approach through which the data stored in clouds can be secured. It is ensured here that the unauthorized access of data is not performed here. The homomorphism token is applied along with distributed verification of the erased coded data to provide security.