**Secure File Storage On Cloud Using Hybrid Cryptography**

**Abstract:** The proposed model is liable to meet the required security needs of data center of cloud. Blowfish used for the encryption of file slices takes minimum time and has maximum throughput for encryption and decryption from other symmetric algorithms. The idea of splitting and merging adds on to meet the principle of data security. The hybrid approach when deployed in cloud environment makes the remote server more secure and thus, helps the cloud providers to fetch more trust of their users. For data security and privacy protection issues, the fundamental challenge of separation of sensitive data and access control is fulfilled. Cryptography technique translates original data into unreadable form. Cryptography technique is divided into symmetric key cryptography and public key cryptography. This technique uses keys for translate data into unreadable form. So only authorized person can access data from cloud server. Cipher text data is visible for all people.

* **Software Requirements:**
* Os : Windows 7 or above
* Framework : Anaconda3
* Language : Python
* IDE : Spyder
* **Hardware Components:**
* Processor – Core i3
* Memory – 2GB
* Internet Connection

**\begin{frame}**

**\frametitle{Face recognition processing flow}**

**\begin{figure}**

**\centering**

**\includegraphics[width=1.10\textwidth]{img1.jpg}**

**\label{fig:Face recognition processing flow.}**

**\end{figure}**

**\end{frame}**