ABSTRACT

**ABSTRACT**

Cloud storage is a model of net worked storage system where data is stored in pools of storage which are generally hosted by third parties. Data stored in the cloud can be accessed at any time from any place as long as there is network access. Storage maintenance tasks, such as purchasing additional storage capacity, can beoffloaded to the responsibility of a service provider. The security of the scheme is still guaranteed if the leakage of the secret key is up to certain bits such that the knowledge of these bits does not help to recover the whole secret key. However, though using leakage resilient primitive can safeguard the leakage of certain bits. we propose a novel two-factor security protection mechanism for data stored in the cloud. Our mechanism provides. Our system is an IBE (Identity-based encryption)- based mechanism. That is, the sender only needs to know the identity of the receiver in order to send an encrypted data (ciphertext) to him/her. No other information of the receiver (e.g., public key, certificate etc.) is required. Then the sender sends the ciphertext to the cloud where the receiver can download it at any time. Our system provides two-factor data encryption protection. In order to decrypt the data stored in the cloud, the user needs to possess two things. First, the user needs to have his/her secret key which is stored in the computer. Second, the user needs to have a unique personal security device which will be used to connect to the computer (e.g., USB, Bluetooth and NFC). It is impossible to decrypt the ciphertext without either piece. More importantly, our system, for the first time.It provides security device (one of the factors) revocability.