**PROPOSED SYSTEMS**

System overview

We employ the use of a hybrid system to protect the data, which combines the efficiency of a symmetric-key system with the convenience of a public-key system. In particular, the proposed dual access control systems are both in Key/Data Encapsulation Mechanism (KEM/DEM) setting. The message is encrypted by an efficient symmetric-key encryption scheme, while the inefficient public-key scheme (i.e., the CP-ABE) is used only to encrypt/decrypt a short key value.

To achieve the security requirements of anonymous data sharing, confidentiality of shared data and access control on shared data, we employ the CP-ABE technique as the basic building block. Specifically, we present the construction based on the CP-ABE scheme in [36] due to its efficiency and elegant construction. To achieve the security requirements of anonymous download request and access control on download request, we design an effective mechanism that the cloud can judge whether a data user is authorized or not without revealing any sensitive information (including the identity of the data user, the plaintext of the outsourced data) to it. In the first system, the cloud needs the help of the authority during the judgement on the download request (sent by a data user). As a result, the authority needs to be always online. However, the authority may not be always online. This leads to the second (enhanced) system where the authority can be offline after the parameter initialization procedure. In particular, we employ the SGX technique to replace the role of the authority during the access control on download request procedure.in some other cases in practice,