Data security model employing hyperelliptic curve cryptography (hecc) and secure hash algorithm-3 (sha-3) in cloud computing

Devi Thiyagarajan, author

Abstrak

Data owners use the huge space offered by ‘Cloud’ Computing for storage of data and also for carrying out computations. To eliminate the burden of storing file locally, cloud stores them on remote servers using virtualization concepts. Therein arises one of the major issues in the field of cloud computing: security. Data owners lack in having direct control over files stored in the cloud and consequently, the problem of data security arises. An efficient scheme to provide data security, while storing data in the cloud has been proposed which makes use of Hyperelliptic curve cryptography (HECC) for encryption and decryption and Secure Hash Algorithm-3 (SHA-3) for data integrity verification. Implementation results clearly illustrate that HECC remains as a good alternative asymmetric key technique rather than ECC and RSA when securing documents in cloud.