The hashing used is SHA2 because it is more secure than SHA-1
The encryption mode used for symmetric encryption is GCM because This GCM is combination of CTR mode was used because it produces a nonce which is guaranteed does not repeat itself thus securing data further and Carter-Wegman MAC. It uses authenticated Encryption with tag and word
It can offer parallel Encryption and Decryption and Random read access which is well suited for distributed systems where parallel processing takes place.
I chose this mode because it is the most secure mode today.