Analysis of fully homomorphic encryption schemes in enhancing data security in cloud computation

Cloud computing is an emerging technological paradigm in the field of digital resource management where such in cloud environment, it involves processing critical data hosted under preferred deployment model. A computational requirement on such cloud data is to adequately address security concerns for both cloud users and providers. Fully Homomorphic Encryption (FHE) has been used to introduce computational complexity while processing data in the cloud without compromising its security. Earlier implementations of fully homomorphic encryption scheme have enabled successful operations on such encrypted data without compromising its secret key. However, this scheme introduce computational defect since the encrypted data becomes very large causing heavy burden onto computing assets in question. In this paper, we appreciate this implementation weakness and address it by incorporating a new technique whereby we defined addition- composition operation such that $f(\psi \oplus \varphi) = f(\psi) \circ f(\varphi)$ where $\circ$ is a composite function. Our approach not only improves the security requirement on the processed data but also reduces computational overheads, which make it ideal for cloud computation. Again, we are able to demonstrate superiority of our approach against previous variants of fully homomorphic encryption that has been implemented