

**CHENNAI – PONDICHERRY**

**VOD-ADAC: ANONYMOUS DISTRIBUTED FINE-GRAINED ACCESS CONTROL PROTOCOL WITH VERIFIABLE OUTSOURCED**

**DECRYPTION IN PUBLIC CLOUD**

**Abstract:**

Remote data access control is of crucial importance in public cloud. Based on its own inclinations, the data owner predefines the access policy. When the user satisfies the data owner’s access policy, it has the right to access the data owner’s remote data. In order to improve flexibility and efficiency of remote data access control, attribute-based encryption (for short, ABE) is used to realize the remote data fine-grained access control. For the low-capacity terminals, verifiable outsourced decryption is a very attractive technique. In the real application scenarios, the user’s attributes are usually managed by many authorities. When some authorized users access some sensitive remote data, they hope to preserve their identity privacy. From the two points, we propose an anonymous distributed fine-grained access control protocol with verifiable outsourced decryption in public cloud (for short, VOD-ADAC). VOD-ADAC is a novel concept which is proposed for the first time in the paper. By adopting the pseudonym technique, the user’s high anonymity can be achieved by frequently changing the independent pseudonyms at some highly social spots. This paper formalizes the system model and security model of VOD-ADAC protocol. Then, by using hybrid encryption technique of distributed ABE and symmetric encryption, a concrete VOD-ADAC protocol is designed from the bilinear pairings. Through security analysis and performance analysis, our proposed VOD-ADAC protocol is provably secure and efficient.