

**CHENNAI – PONDICHERRY**

**SECURE FINE-GRAINED ACCESS CONTROL AND DATA SHARING FOR DYNAMIC GROUPS IN CLOUD**

**Abstract:**

Cloud computing is an emerging computing paradigm that enables users to store their data into a cloud server to enjoy scalable and on-demand services. Nevertheless, it also brings many security issues since cloud service providers (CSPs) are not in the same trusted domain as users. To protect data privacy against un trusted CSPs, existing solutions apply cryptographic methods (e.g., encryption mechanisms) and pro- vide decryption keys only to authorized users. However, sharing cloud data among authorized users at a fine-grained level is still a challenging issue, especially when dealing with dynamic user groups. In this paper, we propose a secure and efficient fine-grained access control and data sharing scheme for dynamic user groups by (1) defining and enforcing access policies based on the attributes of the data; (2) permitting key generation center (KGC) to efficiently update user credentials for dynamic user groups; and (3) allowing some expensive computation tasks to be performed by untrusted CSPs without requiring any delegation key. Specifically, we first design an efficient revocable attribute- based encryption (RABE) scheme with the property of ciphertext delegation by exploiting and uniquely combining techniques of identity-based encryption (IBE), Attribute-based Encryption (ABE), subset-cover framework and ciphertext encoding mech- anism. We then present a fine-grained access control and data sharing system for on-demand services with dynamic user groups in cloud. The experimental data shows that our proposed scheme is more efficient and scalable than the state-of-the-art solution.