

**CHENNAI – PONDICHERRY**

**COOPERATIVE QUERY ANSWER AUTHENTICATION SCHEME OVER ANONYMOUS SENSING DATA**

**ABSTRACT:**

In cloud service over crowd-sensing data, the data owner (DO) publishes the sensing data through the cloud server, so that the user can obtain the information of interest on demand. But the cloud service providers (CSP) are often untrustworthy. The privacy and security concerns emerge over the authenticity of the query answer and the leakage of the DO identity. To solve these issues, many researchers study the query answer authentication scheme for cloud service system. The traditional technique is providing DO's signature for the published data. But the signature would always reveal DO's identity. To deal with this disadvantage, this paper proposes a cooperative query answer authentication scheme, based on the ring signature, the Merkle hash tree (MHT) and the non-repudiable service protocol. Through the cooperation among the entities in cloud service system, the proposed scheme could not only verify the query answer, but also protect the DO's identity. First, it picks up the internal nodes of MHT to sign, as well as the root node. Thus, the verification computation complexity could be significantly reduced from O(log2N) to O(log2N0.5) in the best case. Then, it improves an existing ring signature to sign the selected nodes. Furthermore, the proposed scheme employs the non-repudiation protocol during the transmission of query answer and verification object to protect trading behavior between the CSP and users. The security and performance analysis prove the security and feasibility of the proposed scheme. Extensive experimental results demonstrate its superiority of verification efficiency and communication overhead.