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-reputable 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 (VO) 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.

INTRODUCTION:

With the advances of wireless sensor networks and Internet of things, crowd-sensing big data is collected by scattering sensors over a vast field. As time goes by, the fast-growing data volumes make it hard for the sensors to store due to their weak storage and computing resources. It becomes a problem that how to store these crowd-sensing data economically, as well as perform queries on

it efficiently. Considering the flexible, on-demand and low-cost usage of cloud storage resources, the enterprises and individuals, i.e., data owners (DO), outsource their data to the cloud server. Thus, the users can get the information of interest by asking the cloud service provider (CSP) for searching the outsourced data, The security and privacy requirements include:

• In demand for privacy preservation, the DO tends to outsource the data anonymously. Thus in some specific application scenarios, the DO is also called as the anonymous data provider.

• The CSP provides the paid service for users. Hence in pursuit of commercial profits, the CSP requires that users cannot deny having been served by the CSP if the CSP has sent the proper query answers to the users.

• Since the CSP is often untrustworthy, the users desire urgently for an efficient query answer authentication scheme. In brief, there are three aspects of requirements: the anonymity of DO identity, the efficient verification for the users' query answers and the non-repudiation of query transaction for the CSP.