

**CHENNAI – PONDICHERRY**

**Catch You if You Misbehave: Ranked Keyword Search Results Verification in Cloud Computing**

**Abstract:**

With the advent of cloud computing, more and more people tend to outsource their data to the cloud. As a fundamental data utilization, secure keyword search over encrypted cloud data has attracted the interest of many researchers recently. However, most of existing researches are based on an ideal assumption that the cloud server is “curious but honest”, where the search results are not verified. In this paper, we consider a more challenging model, where the cloud server would probably behave dishonestly. Based on this model, we explore the problem of result verification for the secure ranked keyword search. Different from previous data verification schemes, we propose a novel deterrent-based scheme. With our carefully devised verification data, the cloud server cannot know which data owners, or how many data owners exchange anchor data which will be used for verifying the cloud server’s misbehavior. With our systematically designed verification construction, the cloud server cannot know which data owners’ data are embedded in the verification data buffer, or how many data owners’ verification data are actually used for verification. All the cloud server knows is that, once he behaves dishonestly, he would be discovered with a high probability, and punished seriously once discovered. Furthermore, we propose to optimize the value of parameters used in the construction of the secret verification data buffer. Finally, with thorough analysis and extensive experiments, we confirm the efficacy and efficiency of our proposed schemes.

**Existing System:**

Cloud computing brings a lot of benefits, for privacy concerns, individuals and enterprise users are reluctant to outsource their sensitive data, including private photos, personal health records, and commercial confidential documents, to the cloud. Because once sensitive data are outsourced to a remote cloud, the corresponding data owner directly loses control of these data. The Apple’s iCloud leakage of celebrity photo has furthered our concern regarding the cloud’s data security. Encryption on sensitive data before outsourcing is an alternative way to preserve data privacy against adversaries. However, data encryption becomes an obstacle to the utilization of traditional applications, e.g., plaintext based keyword search.

Existing schemes share a common assumption, i.e., data owners foresee the order of search results. However, in practical applications, numerous data owners are involved; each data owner only knows its own partial order.Without knowing the total order, these data owners cannot use the conventional schemes to verify the search results.

**Proposed System:**

We formalize the ranked keyword search result verification problem where multiple data owners are involved and the cloud server would probably behave dishonestly.

We propose a novel secure and efficient deterrent based verification scheme for secure ranked keyword search.

We propose to optimize the value of parameters used in the construction of verification data buffer.

We give a thorough analysis and conduct extensive performance experiments to show the efficacy and efficiency of our proposed scheme.