

**HealthDep: An Efficient and Secure Deduplication Scheme for Cloud-Assisted eHealth Systems**

**Abstract:**

In this paper, we analyze the inherent characteristic of electronic medical records (EMRs) from actual electronic health (eHealth) systems, where we found that first, multiple patients would generate large amounts of duplicate EMRs and second, cross-patient duplicate EMRs would be generated numerously only in the case that the patients consult doctors in the same department. We then propose the first efficient and secure encrypted EMRs deduplication scheme for cloud-assisted eHealth systems (HealthDep). With the integration of our analysis results, HealthDep allows the cloud server to efficiently perform the EMRs deduplication, and enables the cloud server to reduce storage costs by more than 65% while ensuring the confidentiality of EMRs. Security analysis shows that HealthDep provides a stronger security guarantee than Marforio et al. 's scheme (NDSS 2014) and Bellare et al. 's scheme (USENIX Security 2013). Algorithm implementation and performance analysis demonstrate the feasibility and high efficiency of HealthDep.