**Forward Secure Public Key Encryption with Keyword Search for Outsourced Cloud Storage**

**ABSTRACT**

Cloud storage has become a primary industry in remote data management service but also attracts security concerns, where the best available approach for preventing data disclosure is encryption. Among them the public key encryption with keyword search (PKSE) is considered to be a promising technique, since clients can efficiently search over encrypted data files. That is, a client first generates a search token when to query data files, the cloud server uses the search token to proceed the query over encrypted data files. However, a serious attack is raised when PKSE meets cloud. Formally speaking, the cloud server can learn the information of a newly added encrypted data file containing the keyword that previously queried by using the search tokens it has received, and can further discover the privacy information. To address this issue, we propose a forward secure public key searchable encryption scheme, in which a cloud server cannot learn any information about a newly added encrypted data file containing the keyword that previously queried. To better understand the design principle, we introduce a framework for constructing forward secure public key searchable encryption schemes based on attribute-based searchable encryption. Finally, the experiments show our scheme is efficient.