**ABSTRACT**

With the increasing popularity of cloud-based data services, data owners are highly motivated to store their huge amount of potentially sensitive personal data files on remote servers in encrypted form. Clients later can query over the encrypted database to retrieve files while protecting privacy of both the queries and the database, by allowing some reasonable leakage information. To this end, the notion of searchable symmetric encryption (SSE) was proposed. Meanwhile, recent literature has shown that most dynamic SSE solutions leaking information on updated keywords are vulnerable to devastating file-injection attacks. The only way to thwart these attacks is to design forward-private schemes. In this paper, we investigate new privacy-preserving indexing and query processing protocols which meet a number of desirable properties, including the multi-keyword query processing with conjunction and disjunction logic queries, practically high privacy guarantees with adaptive chosen keyword attack (CKA2) security and forward privacy, and the support of dynamic data operations, etc. Compared to previous schemes, our solutions are highly compact, practical and flexible. Their performance and security are carefully characterized by rigorous analysis. Experimental evaluations conducted over a large representative dataset demonstrate that our solutions can achieve modest search time efficiency, and they are practical for use in large-scale encrypted database systems.

**SYSTEM ARCHITECTURE:**

****