**LITERATURE SURVEY**

1. **Achieving efficient conjunctive keyword searches over encrypted data**

**AUTHORS:** L. Ballard, S. Kamara, and F. Monrose

We present two provably secure and efficient schemes for performing conjunctive keyword searches over symmetrically encrypted data. Our first scheme is based on Shamir Secret Sharing and provides the most efficient search technique in this context to date. Although the size of its trapdoors is linear in the number of documents being searched, we empirically show that this overhead remains reasonable in practice. Nonetheless, to address this limitation we provide an alternative based on bilinear pairings that yields constant size trapdoors. This latter construction is not only asymptotically more efficient than previous secure conjunctive keyword search schemes in the symmetric setting, but incurs significantly less storage overhead. Additionally, unlike most previous work, our constructions are proven secure in the standard model.

# 2) Secure Conjunctive Keyword Search over Encrypted Data

**AUTHORS:** P. Golle, J. Staddon, and B. Waters

We study the setting in which a user stores encrypted documents (e.g. e-mails) on an untrusted server. In order to retrieve documents satisfying a certain search criterion, the user gives the server a capability that allows the server to identify exactly those documents. Work in this area has largely focused on search criteria consisting of a single keyword. If the user is actually interested in documents containing each of several keywords (conjunctive keyword search) the user must either give the server capabilities for each of the keywords individually and rely on an intersection calculation (by either the server or the user) to determine the correct set of documents, or alternatively, the user may store additional information on the server to facilitate such searches. Neither solution is desirable; the former enables the server to learn which documents match each individual keyword of the conjunctive search and the latter results in exponential storage if the user allows for searches on every set of keywords.We define a security model for conjunctive keyword search over encrypted data and present the first schemes for conducting such searches securely. We propose first a scheme for which the communication cost is linear in the number of documents, but that cost can be incurred “offline” before the conjunctive query is asked. The security of this scheme relies on the Decisional Diffie-Hellman (DDH) assumption. We propose a second scheme whose communication cost is on the order of the number of keyword fields and whose security relies on a new hardness assumption.

**3) Securing sift: Privacy-preserving outsourcing computation of feature extractions over encrypted image data**

**AUTHORS:** S. Hu, Q. Wang, J. Wang, Z. Qin, and K. Ren

Advances in cloud computing have greatly motivated data owners to outsource their huge amount of personal multimedia data and/or computationally expensive tasks onto the cloud by leveraging its abundant resources for cost saving and flexibility. Despite the tremendous benefits, the outsourced multimedia data and its originated applications may reveal the data owner's private information, such as the personal identity, locations, or even financial profiles. This observation has recently aroused new research interest on privacy-preserving computations over outsourced multimedia data. In this paper, we propose an effective and practical privacy-preserving computation outsourcing protocol for the prevailing scale-invariant feature transform (SIFT) over massive encrypted image data. We first show that the previous solutions to this problem have either efficiency/security or practicality issues, and none can well preserve the important characteristics of the original SIFT in terms of distinctiveness and robustness. We then present a new scheme design that achieves efficiency and security requirements simultaneously with the preservation of its key characteristics, by randomly splitting the original image data, designing two novel efficient protocols for secure multiplication and comparison, and carefully distributing the feature extraction computations onto two independent cloud servers. We both carefully analyze and extensively evaluate the security and effectiveness of our design. The results show that our solution is practically secure, outperforms the state-of-the-art, and performs comparably with the original SIFT in terms of various characteristics, including rotation invariance, image scale invariance, robust matching across affine distortion, and addition of noise and change in 3D viewpoint and illumination.

**4) Boolean searchable symmetric encryption with worst-case sub-linear complexity**

**AUTHORS:** S. Kamara and T. Moataz

Recent work on searchable symmetric encryption (SSE) has focused on increasing its expressiveness. A notable example is the OXT construction (Cash et al., CRYPTO ’13) which is the first SSE scheme to support conjunctive keyword queries with sub-linear search complexity. While OXT efficiently supports disjunctive and boolean queries that can be expressed in searchable normal form, it can only handle arbitrary disjunctive and boolean queries in linear time. This motivates the problem of designing expressive SSE schemes with worst-case sub-linear search; that is, schemes that remain highly efficient.

# 5) Fuzzy Keyword Search over Encrypted Data in Cloud Computing

**AUTHORS:** J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou

As Cloud Computing becomes prevalent, more and more sensitive information are being centralized into the cloud. For the protection of data privacy, sensitive data usually have to be encrypted before outsourcing, which makes effective data utilization a very challenging task. Although traditional searchable encryption schemes allow a user to securely search over encrypted data through keywords and selectively retrieve files of interest, these techniques support only exact keyword search. That is, there is no tolerance of minor typos and format inconsistencies which, on the other hand, are typical user searching behavior and happen very frequently. This significant drawback makes existing techniques unsuitable in Cloud Computing as it greatly affects system usability, rendering user searching experiences very frustrating and system efficacy very low. In this paper, for the first time we formalize and solve the problem of effective fuzzy keyword search over encrypted cloud data while maintaining keyword privacy. Fuzzy keyword search greatly enhances system usability by returning the matching files when users' searching inputs exactly match the predefined keywords or the closest possible matching files based on keyword similarity semantics, when exact match fails. In our solution, we exploit edit distance to quantify keywords similarity and develop an advanced technique on constructing fuzzy keyword sets, which greatly reduces the storage and representation overheads. Through rigorous security analysis, we show that our proposed solution is secure and privacy-preserving, while correctly realizing the goal of fuzzy keyword search.