PROJECT TITLE

An Efficient Multi-User Searchable Encryption Scheme without Query Transformation over Outsourced Encrypted Data

Presented By

1. T.sandhya
2. M.santosh
3. B.surendra kumar
4. P.madavi

Project coordinator: srikar sir

Guide: Pavan sir

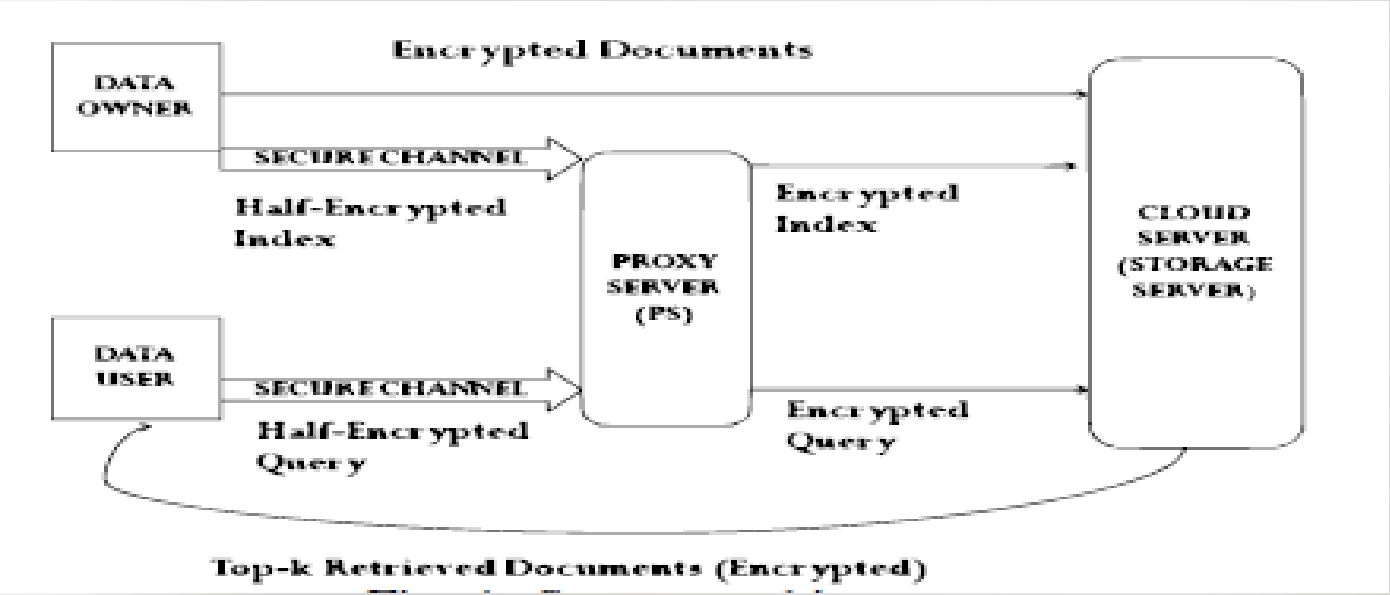
Trainer

ABSTRACT

Searchable encryption schemes provide security and privacy to the cloud data. The existing SE approaches enable multiple users to perform search operation by using various schemes like broadcast encryption .Attribute-based encryption however, these schemes do not allow multiple users to perform the search operation over the encrypted data of multiple owners. Some SE schemes involve a proxy server that allow multiple users to perform the search operation proxy server approach that performs the search operation without transforming the user queries. This approach also returns the top-k relevant documents to the user queries by using Euclidean distance similarity approach. based on the experimental study, this approach is efficient with respect to search time and accuracy.

.

SYSTEM ARCHITECTURE:



EXISTING SYSTEM:

1. The first Searchable Encryption SE scheme was proposed byD. X. Song using symmetric key encryption algorithm.

2. Identity-Based Encryption BE scheme allows multiple users to perform the search operation over the encrypted data. Another schemes up porting multiple users' search operation is proposed by using CP-ABE. Keyword authorization based approach in supports search operation by multiple users.

3. Multi-Keyword Ranked Search approach over the data of multiple owners is proposed. This approach supports search operation in a multi-owner and multi-user environment ,which allows multiple users to perform the search operation over the data of multiple owners

DISADVANTAGES OF EXISTING SYSTEM:

1. These approaches support search operation in a single owner and a single user environment,
2. which allows only a single user to perform the search operation over the data of single owner.
3. All these schemes support search operation in a single owner and multiuser environment,
4. which allows the multiple users to perform the search operation over the encrypted data of a single owner.