

Efficient and Expressive Keyword Search Over Encrypted

Data in Cloud

ABSTRACT:

Searchable encryption allows a cloud server to conduct keyword search over encrypted data on behalf of the data users without learning the underlying plaintexts. However, most existing searchable encryption schemes only support single or conjunctive keyword search, while a few other schemes that are able to perform expressive keyword search are computationally inefficient since they are built from bilinear pairings over the composite-order groups. In this paper, we propose an expressive public-key searchable encryption scheme in the prime-order groups, which allows keyword search policies (i.e., predicates, access structures) to be expressed in conjunctive, disjunctive or any monotonic Boolean formulas and achieves significant performance improvement over existing schemes. We formally define its security, and prove that it is selectively secure in the standard model. Also, we implement the proposed scheme using a rapid prototyping tool called Charm [37], and conduct several experiments to evaluate its performance. The results demonstrate that our scheme is much more efficient than the ones built over the composite-order groups.

EXISTING SYSTEM:

- ❖ After Boneh et al. initiated the study of public-key encryption with keyword search (PEKS), several PEKS constructions were put forth using different techniques or considering different situations.

- ❖ They aim to solve two cruces in PEKS: (1) how to make PEKS secure against offline keyword dictionary guessing attacks; and (2) how to achieve expressive searching predicates in PEKS. In terms of the offline keyword dictionary guessing attacks, which requires that no adversary (including the cloud searching server) can learn keywords from a given trapdoor, to the best of our knowledge, such a security notion is very hard to be achieved in the public-key setting.
- ❖ In a private-key SE setting, a user uploads its private data to a remote database and keeps the data private from the remote database administrator. Private-key SE allows the user to retrieve all the records containing a particular keyword from the remote database

DISADVANTAGES OF EXISTING SYSTEM:

- ❖ KPABE schemes are not designed to preserve privacy of attributes (keywords) associated with ciphertexts.
- ❖ Trapdoors are subject to the offline keyword dictionary guessing attacks.
- ❖ They are not sufficiently efficient to be adopted in the practical world
- ❖ Private-key SE solutions only apply to scenarios where data owners and data users totally trusted each other.

PROPOSED SYSTEM:

- ❖ The basic idea of our scheme is to modify a key-policy attributed-based encryption (KP-ABE) scheme constructed from bilinear pairing over prime-order groups. Without loss of generality, we will use the large universe KP-ABE scheme selectively secure in the standard model.

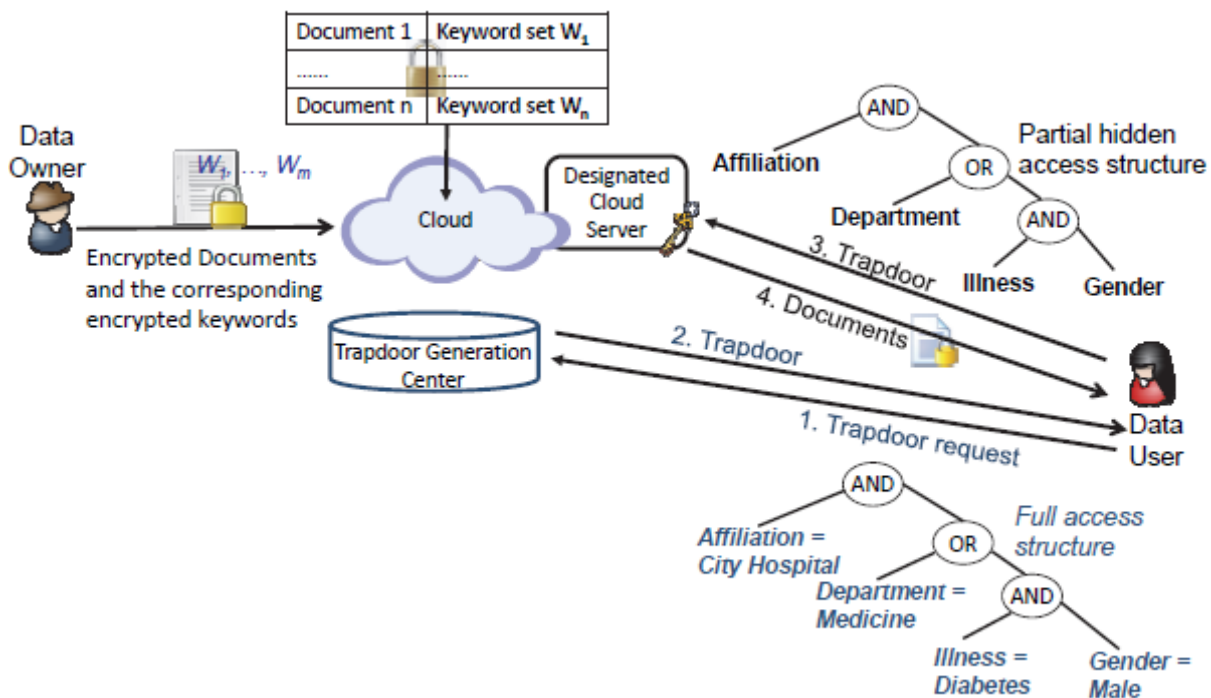
- ❖ First, to preserve keyword privacy in an access structure, we adopt the method to divide each keyword into a generic name and a keyword value. Since keyword values are much more sensitive than the generic keyword names, the keyword values in an access structure are not disclosed to the cloud server, whereas a partial hidden access structure with only generic keyword names is included in a trapdoor and sent to the cloud server.
- ❖ We equip this designated server with a public and private key pair of which the public key will be used in trapdoor generation such that it is computationally infeasible for anyone without knowledge of the privacy key to derive keywords information from the trapdoor
- ❖ We propose the first expressive SE scheme in the public-key setting from bilinear pairings in prime order groups. As such, our scheme is not only capable of expressive multi-keyword search, but also significantly more efficient than existing schemes built in composite-order groups.
- ❖ Using a randomness splitting technique, our scheme achieves security against offline keyword dictionary guessing attacks to the ciphertexts. Moreover, to preserve the privacy of keywords against offline keyword dictionary guessing attacks to trapdoors, we divide each keyword into keyword name and keyword value and assign a designated cloud server to conduct search operations in our construction.

ADVANTAGES OF PROPOSED SYSTEM:

- ❖ In addition to hiding keywords in ciphertexts, we also need to preserve keyword privacy in a trapdoor which contains an access structure as a component.

- ❖ We formalize the security definition of expressive SE, and formally prove that our proposed expressive SE scheme is selectively secure in the standard model.
- ❖ We implement our scheme using a rapidly prototyping tool called Charm, and conduct extensive experiments to evaluate its performance. Our results confirm that the proposed scheme is sufficiently efficient to be applied in practice.

SYSTEM ARCHITECTURE:



SYSTEM REQUIREMENTS:

HARDWARE REQUIREMENTS:

- System : Pentium Dual Core.
- Hard Disk : 120 GB.
- Monitor : 15” LED
- Input Devices : Keyboard, Mouse
- Ram : 1 GB

SOFTWARE REQUIREMENTS:

- Operating system : Windows 7.
- Coding Language : JAVA/J2EE
- Tool : Netbeans 7.2.1
- Database : MYSQL

REFERENCE:

Hui Cui, Zhiguo Wan, Robert H. Deng, Guilin Wang, and Yingjiu Li, “Efficient and Expressive Keyword Search Over Encrypted Data in Cloud”, **IEEE Transactions on Dependable and Secure Computing, 2017.**