Identity-Based Private Matching overOutsourced Encrypted Datasets

ABSTRACT:

With wide use of cloud computing and storage services, sensitive information is increasingly centralized into the cloud toreduce the management costs, which raises concerns about data privacy. Encryption is a promising way to maintain the confidentialityof outsourced sensitive data, but it makes effective data utilization to be a very challenging task. In this paper, we focus on the problemof private matching over outsourced encrypted datasets in identity-based cryptosystem that can simplify the certificate management.To solve this problem, we propose an Identity-Based Private Matching scheme (IBPM), which realizes fine-grained authorization thatenables the privileged cloud server to perform private matching operations without leaking any private data. We present the rigoroussecurity proof under the Decisional Linear Assumption and Decisional Bilinear Diffie-Hellman Assumption. Furthermore, through theanalysis of the asymptotic complexity and the experimental evaluation, we verify that the cost of our IBPM scheme is linear to the sizeof the dataset and it is more efficient than the existing work of Zheng [30]. Finally, we apply our IBPM scheme to build two efficientschemes, including identity-based fuzzy private matching as well as identity-based multi-keyword fuzzy search.

EXISTING SYSTEM:

- In Liu et al.'s scheme, the users outsource their datasets to thecloud by hashing each element and delegate matching operationsto the cloud.

However, it's not fine-grained authorization secure,meaning that if the cloud is delegated to compute set intersectionbetween the datasets of user Alice and Bob, followed by thatbetween the datasets of user Alice and Carlos, then the cloud willget set intersection between the datasets of user Bob and Carloswithout their consent.

- The scheme proposed by Zheng et al.is a verifiable solution based on proxy re-encryption techniquebut it's also not fine-grained authorization secure.
- Recently, Adabiet al.proposed a new delegated solution by leveraginghomomorphic encryption and polynomial evaluation. However,in their scheme, the client must download and decrypt as manyas 2n ciphertexts (n is the size of dataset).

DISADVANTAGES OF EXISTING SYSTEM:

- Suppose there are two cloud users, they encrypt their datasets and outsource them to the cloud. The cloud server with the corresponding authorization token can conduct the heavy duty computational matching operations over ciphertexts.
- Runs the complex algorithm factorizing polynomials to get the result.
- It's not a practical solution for our problem.
- How to construct an efficient and secure identity-based private matching scheme over outsourced encrypted datasets is a promising open problem.

PROPOSED SYSTEM:

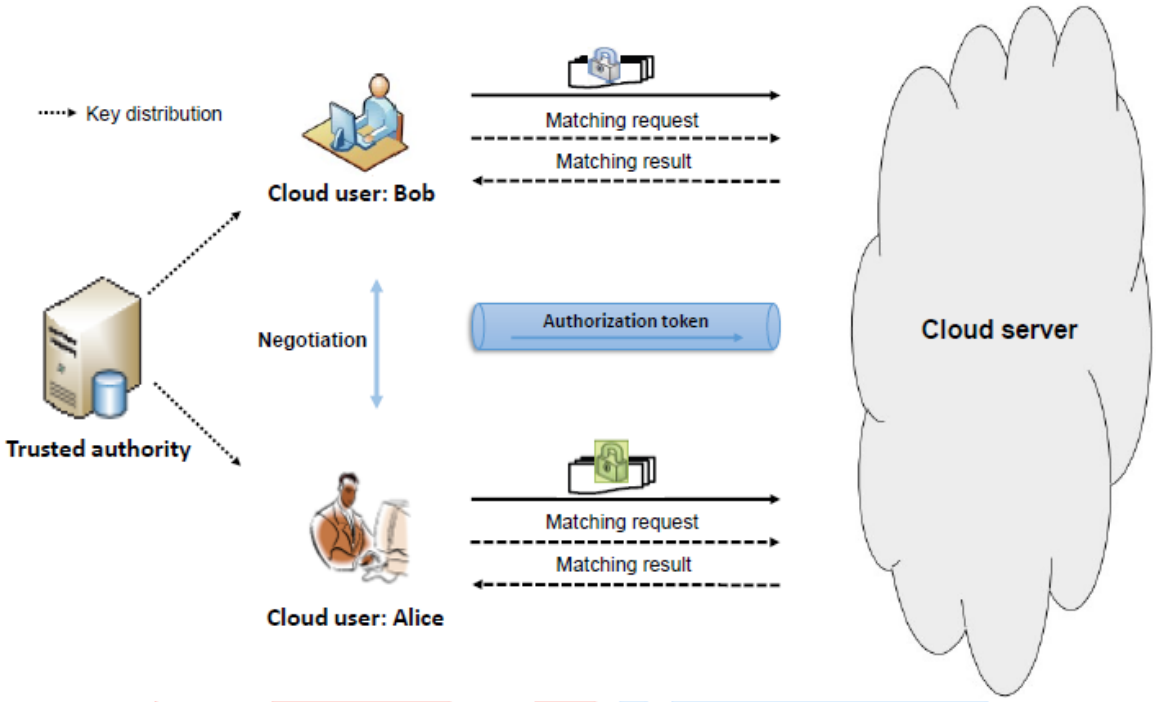
- In this paper, we focus on the problem of how the cloud carries out private matching over outsourced encrypted datasets if and only if the cloud server is authorized to do so.
- We proposea novel cryptographic primitive: identity-based private matchingover outsourced encrypted datasets (IBPM), which can simplifycertificate management due to the advantage of identity-basedcryptosystem. Identity-based encryption was applied to crossdomaindata sharing in distributed Electronic Health Records(EHR) systems, which allows users from different domainsto directly authenticate with each other.
- Our IBPM can be usedto provide privacy-preserving cross-domain EHR matching whenthe EHR data are outsourced in an encrypted form to a cloudplatform. Furthermore, with our novel primitive, users gain thefollowing controls on the private matching over the outsourcedencrypted datasets:
- A user has fine-grained control over who can do privatematching with him/her, by negotiating the correspondingauthorization token;
- A user has fined-grained control over who can performprivate matching, by choosing the semi-trusted cloud.

ADVANTAGES OF PROPOSED SYSTEM:

- We propose a novel cryptographic primitive: identity-basedprivate matching over outsourced encrypted datasets (IBPM),and formally define the framework and the security forIBPM. Then we present a concrete construction of the IBPMunder the DLN and DBDH assumptions.

- Our solution is in identity-based setting so that it cansimplify the certificate management;
- The cloud users delegate the costly private matching operationswithout giving the cloud any capability in breachingthe secrecy of the datasets;
- Our scheme realizes fine-grained authorization for privatematching over outsourced encrypted datasets. In otherwords, only the cloud server who has the authorizationtoken can perform private matching between two users'encrypted datasets. What's more, with our scheme, theusers can delegate the cloud server to check whether theyhave outsourced the same data to cloud before uploadingthe encrypted data.
- We give a rigorous security proof and implementation of ourscheme.
- Through the real experimental evaluation, we verifythat the computational cost of our scheme is linear to the sizeof the dataset and the matching algorithm is more efficientthan the existing work.
- We apply our IBPM scheme to solve the problems offuzzy private matching and multi-keyword fuzzy search,and present two efficient schemes, i.e., identity-based fuzzyprivate matching scheme and identity-based multi-keywordfuzzy search scheme.

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:

Shuo Qiu, Jiqiang Liu, Yanfeng Shi, Ming Li, Member, IEEE, and Wei Wang, "Identity-Based Private Matching overOutsourced Encrypted Datasets", **IEEE TRANSACTIONS ON CLOUD COMPUTING, 2017.**