Identity Based Private Matching over Outsourced Encrypted Datasets

ABSTRACT

With wide use of cloud computing and storage services, sensitive information is increasingly centralized into the cloud to reduce the management costs, which raises concerns about data privacy. Encryption is a promising way to maintain the confidentiality of outsourced sensitive data, but it makes effective data utilization t be a very challenging task. In this paper, we focus on the problem of 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 that enables the privileged cloud server to perform private matching operations without leaking any private data. We present the rigorous security proof under the Decisional Linear Assumption and Decisional Bilinear Diffie-Hellman Assumption. Furthermore, through the analysis of the asymptotic complexity and the experimental evaluation, we verify that the cost of our IBPM scheme is linear to the size of the dataset and it is more efficient than the existing work of Zheng [30]. Finally, we apply our IBPM scheme to build two efficient schemes, including identity-based fuzzy private matching as well as identity-based multi-keyword fuzzy search.

**EXISTING SYSTEM**

* The most existing work on private matching over outsourced encrypted datasets wer presented by Liu et al. [29], Zheng et al. [30] and Adabi et al. [31]. In Liu et al.’s scheme [29], the users outsource their datasets to the cloud by hashing each element and delegate matching operation to the cloud.
* However, it’s not fine-grained authorization secure, meaning that if the cloud is delegated to compute set intersection between the datasets of user Alice and Bob, followed by than between the datasets of user Alice and Carlos, then the cloud will get set intersection between the datasets of user Bob and Carlos without their consent. The scheme proposed by Zheng et al. [30] is a verifiable solution based on proxy re-encryption technique but it’s also not fine-grained authorization secure.
* The existing system, Adabi et al. [31] proposed a new delegated solution by leveraging homomorphic encryption and polynomial evaluation. However, in their scheme, the client must download and decrypt as many as 2n ciphertexts (n is the size of dataset), and then runs the complex algorithm factorizing polynomials to get the result. It’s not a practical solution for our problem.
* **Disadvantages**
* There is less security on outsourced data due to lack of Selective security against chosen-plaintext attack.
* There is no Data integrity technique to audit outsourced data.

**PROPOSED SYSTEM**

* + In the proposed system, the system presents We propose a novel cryptographic primitive: identity-based private matching over outsourced encrypted datasets (IBPM), and formally define the framework and the security for IBPM. Then we present a concrete construction of the IBPM under the DLN and DBDH assumptions.
	+ The system also gives a rigorous security proof and implementation of our scheme. Through the real experimental evaluation, the system also verifies that the computational cost of our scheme is linear to the size of the dataset and the matching algorithm is more efficient than the existing work reported in the proposed system.
	+ The system also applies our IBPM scheme to solve the problems of fuzzy private matching and multi-keyword fuzzy search and present two efficient schemes, i.e., identity-based fuzzy private matching scheme and identity-based multi-keyword fuzzy search scheme.

**Advantages**

* The Data Security is more due to identity-based encryption.
* The Date retrieval speed so fast due to Identity-Based Multi-Keyword Fuzzy Search Technique.

**SYSTEM REQUIREMENTS**

➢ **H/W System Configuration:-**

➢ Processor - Pentium –IV

➢ RAM - 4 GB (min)

➢ Hard Disk - 20 GB

➢ Key Board - Standard Windows Keyboard

➢ Mouse - Two or Three Button Mouse

➢ Monitor - SVGA

**Software Requirements:**

* Operating System - Windows XP
* Coding Language - Java/J2EE(JSP,Servlet)
* Front End - J2EE
* Back End - MySQL