International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622
International Conference on Industrial Automation and Computing (ICIAC- 12th & 13th April 2014)

RESEARCH ARTICLE OPEN ACCESS

An Efficient Private Search Technique Using SADS Algorithm

Ms. Vrushali S. Sakharkar *, Dr .G. R. Bamnote **
*(Department of Computer Science, PRMIT &R, Badnera

ABSTRACT
The ability to securely share sensitive information between untrusting parties is a prerequisite for many real-world applications . There exist many large collections of private data that must be protected on behalf of the entities that hold them or the clients they serve. For example, two intelligence agencies might be willing to cooperate by sharing documents about a specific case. So the documents should be exchanged securely. the privacy implications of two practical extensions applicable to any keyword-based private search system are designed & analyzed. The efficiency is evaluated by building them on top of a private search system, called SADS.A secure anonymous database search (SADS) system that provides exact keyword match capability. By using , re-routable encryption along with Bloom filters1 and deterministic encryption SADS lets multiple parties efficiently execute exact-match queries over distributed encrypted databases in a controlled manner. SADS' performance, privacy guaranties and functionality are improved. The extended SADS system offers improved efficiency parameters that meet practical usability requirements in a relaxed adversarial model.

Keywords **–** encrypted Bloom filters, private information retrieval, anonymity, database, deterministic encryption, encrypted search

I. INTRODUCTION

Often, different parties possess data of mutual interest. They might wish to share portions of this data for collaborative work, but consider the leak of unrelated portions to be a privacy issue for themselves or their clients. Thus, methods that provide a well-defined and secure sharing of the data between untrusting parties can be useful tools. One such method that we introduce in this paper, is the ability for a client to search the information residing on another server without revealing to the server his identity or the content of his query. At the same time, it is desirable to guarantee that query capability is only granted to appropriate clients and that they do not learn anything unrelated to the query. An efficient SADS scheme is designed and provide for it proofs of security and performance evaluation. SADS system uses third parties and relaxed definitions of security to circumvent these inherent efficiency costs. SADS is extended in two ways: its search capabilities beyond exact keyword match and provide a modular framework for adapting the system to meet varying security and efficiency needs. Existing systems for encrypted search provide privacy guarantees but at a provably high cost in efficiency. Using SADS as the foundational building block, a system is developed which is capable of creating flexible query systems that deliver strong cryptographic and privacy preserving guarantees. Although the framework can support more general queries, here on the specific functionality of keyword search is focused which allows an authorized client to anonymously and securely query a server for documents containing a desired keyword.

Although it sounds similar to existing work on encrypted search, the SADS system differs in a significant manner: In SADS scenario, the client and the owner of the data are different parties. This constitutes a different adversarial model. The database must be protected from the client. Additionally, to protect the identity of the querier which also introduces new issues, such as how to ensure that the data owner can prevent arbitrary unauthorized parties from sending queries.

II. SECURITY ARCHITECTURE

Problem Setting and Requirements

The strongest security definition for a generic encrypted search scheme in the setting of data sharing guarantees that the querier receives only the matching results while none of the other parties in the protocol learns anything. The goal of the protocol is to meet the following requirements:

Correctness:

The query's output consists of all the matches, namely the indices of all documents containing the keyword. A tolerated probability of expected error (false positives or negatives) may be specified.

Client Security: The data owner does not learn any information about the query

(keyword).

Server Security: The querier learns nothing about the data except for the speci_ed output (matches) for his query.

Server Access Control: Only parties authorized by the data owner can submit queries and receive outputs for this data.

Client Anonymity: The data owner learns no information about the identity of the querier as chosen from amongst the pool of authorized parties. This also precludes information about linkage of two queries coming from the same client

SYSTEM DESIGN

The secure anonymous database search (SADS) scheme provides the following search capability: it allows a search client (C) with a keyword to identify the documents of a database owner/server (S) containing the keyword without learning anything more or revealing his query. For this purpose the architecture of the system involves two semi-trusted parties: index server (IS) and query router (QR), which facilitate the search.

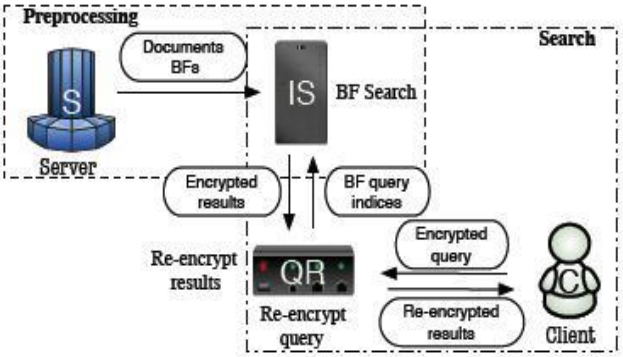

Figure 1: SADS overview.

The scheme works as follows: the database owner computes search structures for his database — a Bloom filter (BF) per document built from the encryptions of all words of the document. Each authorized client receives keys that he uses to submit queries and decrypt the results; the QR receives corresponding transformation keys for the queries of that client. To submit a query, C computes an encryption of his query and sends it to QR. QR verifies that the client is authorized, re-encrypts the query with the corresponding transformation key, computes and sends the BF indices obtained from the encryption to IS. IS performs search across the BFs it stores, encrypts the identifiers of the matching documents and sends them to the QR; QR transforms the encryptions and delivers them to the client, who decrypts them to obtain his search results.

III. FUTURE CHALLENGES

System designers must consider the desired security and privacyrequirements at a semantic level and carefully consider the optimal tolerance for semantic false positive and false negative errors, which is often a non-trivial compromise. There are many interesting research issues worth further investigation. The works mentioned above have a common characteristic: they relax the privacy guarantees to achieve higher efficiency performance. While there are formal privacy definitions for searchable encryption that reveal the access pattern , for as-strong-as possible schemes, how to formally analyze the privacy level given various known background information remains an interesting and important open problem.

IV. Conclusion

Here, a solution for the problem of secure anonymous database search is proposed which addresses the issue of allowing untrusting parties to search each other's private data when there are legitimate reasons for this. A major goal is to achieve practical efficiency while still achieving the maximal security and privacy guarantees that the efficiency requirement permits. For this purpose, a security architecture with distributed limited trust among two intermediary parties is utilized, which is considered viable in practical situations where one have authorities regulating the controlled data sharing without learning any private information of the participants.

References

[1] O. Goldreich, S. Micali, and A. Wigderson. How to play any mental game. In STOC '87: Proceedings of the nineteenth annual ACM symposium on Theory of computing, pages 218{229, New York, NY, USA, 1987. ACM.

[2] Andrew Chi-Chih Yao. Protocols for secure computations. In FOCS, pages 160{164, 1982.}

[3] Andrew Chi-Chih Yao. How to generate and exchange secrets (extended abstract). In FOCS, pages 162{167,1986.

[4] Benny Chor, Eyal Kushilevitz, Oded Goldreich, and Madhu Sudan. Private information retrieval. J. ACM, 45(6):965{981, 1998.

[5] Yan cheng Chang and Michael Mitzenmacher. Privacy preserving keyword searches on remote encrypted data. In ACNS, volume 3531, 2005.

[6] Reza Curtmola, Juan Garay, Seny Kamara, and Rafail Ostrovsky. Searchable symmetric encryption: improved de_nitions and e_cient constructions. In CCS '06: Proceedings of the 13th ACM conference on Computer and communications security, pages 79{88, New York, NY, USA, 2006. ACM.