An Investigation into Search over Outsourced Encrypted Data

Student A
Dept. of Computer Science
ID:12341000

Student B
Dept. of Computer Science
ID:12341000

Student C
Dept. of Computer Science
ID:12341000

I. Introduction

Guidelines: In this section, you should abstract your target problem and present your motivation. For example, you may highlight the practical motivation for encrypted search from your literature search. Meanwhile, you may categorize the typical research directions in the field of encrypted search (e.g., dynamic encrypted search, boolean encrypted search, and encrypted ranked search). Further, you may present any particular security/practicality considerations on designing an encrypted search scheme.

If you want to use existing papers observations, please cite it like In Song et al.'s work [1], the notion of searchable encryption is introduced for the first time.

You can use figures/tables for illustration of your findings/ideas throughout the report. Table 1 and Fig. 1 are provided as examples.

II. Application Setting

A. System Architecture

Guidelines: In this subsection, you should describe the general application setting of encrypted search, e.g., how many parties are there in the real application setting, the particular role of each party, and the participation of each party (i.e., what each party does in the work flow).

B. Threat Model

Guidelines: In this subsection, you should explain the threat assumptions generally adopted by the literature on encrypted search. For example, you may clearly indicate the trust assumptions of each party involved in the application (i.e., who is trusted or untrusted?), the goal of the untrusted party (e.g., what does the adversary want to learn?), how the adversary will behave, in a semi-honest fashion or in a malicious manner?

TABLE I
Comparison of encrypted search schemes.

Scheme	Search Complexity	Index Size
[1]	...	...
...	...	...

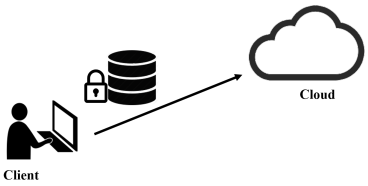

Fig. 1. Outsourcing encrypted data to the cloud.

III. Research Directions of Encrypted Search

Guidelines: In this subsection, you should introduce the typical research directions for encrypted search, describe in detail the goals of each research direction in terms of functionality and/or security. You should also specify and discuss the design challenges in each direction based on your literature study and or your personal perspectives. Besides, you should properly discuss the existing works and try to reflect the state-of-the-art. A possible organization structure is given below.

A. Basic Searchable Encryption

Goals. The description goes here.
Design challenges. The description goes here.
Related work. The description goes here.

B. Dynamic Searchable Encryption

Goals. The description goes here.
Design challenges. The description goes here.
Related work. The description goes here.

C. Boolean Searchable Encryption

Goals. The description goes here.
Design challenges. The description goes here.
Related work. The description goes here.

D. Any Other Possible Categories

Goals. The description goes here.
Design challenges. The description goes here.
Related work. The description goes here.

IV. Conclusion

The conclusion goes here.

References

[1] D. X. Song, D. A. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in *Proc. of IEEE Symposium on Security and Privacy*, 2000.