CS6290: Reading Summary 1

Student A

Dept. of Computer Science

ID:12341000

I. SUMMARY OF PAPER [1]

A. Problem Statement

Guidelines: Here you should explicitly summarize the problem targeted by the paper. A rough and brief example might be as follows. The paper targets the problem of searching encrypted outsourced data on the cloud. Particularly, how to enable a client to perform search and get the correct search result when both the cloud database and query keywords are encrypted?

B. Problem Significance

Guidelines: Here you should explain why the problem targeted by the paper is important and has value. In particular, what is the motivation of this paper?

C. State of the Art

Guidelines: Here you should describe the state of the art as reflected in the paper at that time.

D. Contributions

Guidelines: Here you should summarize the contributions of the paper in your own words. For example, you may evaluate the contributions from the following perspectives: novelty of problem formulation, novelty of the technical solution, depth of theoretical analysis of the technical solution, positiveness of experimental evaluation result, etc.

E. Remaining Questions

Guidelines: Here you should try to discuss any remaining questions to be solved or any possible future directions based on the result of the paper.

II. SUMMARY OF PAPER [2]

A. Problem Statement

Guidelines: Here you should explicitly summarize the problem targeted by the paper. A rough and brief example might be as follows. The paper targets the problem of searching encrypted outsourced data on the cloud. Particularly, how to enable a client to perform search and get the correct search result when both the cloud database and query keywords are encrypted?

B. Problem Significance

Guidelines: Here you should explain why the problem targeted by the paper is important and has value. In particular, what is the motivation of this paper?

C. State of the Art

Guidelines: Here you should describe the state of the art as reflected in the paper at that time.

D. Contributions

Guidelines: Here you should summarize the contributions of the paper in your own words. For example, you may evaluate the contributions from the following perspectives: novelty of problem formulation, novelty of the technical solution, depth of theoretical analysis of the technical solution, positiveness of experimental evaluation result, etc.

E. Remaining Questions

Guidelines: Here you should try to discuss any remaining questions to be solved or any possible future directions based on the result of the paper.

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.
[2] R. Curtmola, J. A. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," in *Proc. of ACM CCS*, 2006.