Title: This a LaTeX Template

Boyang Wang
M12345678

Firstname Lastname
M12345678

ABSTRACT

To maintain search functionalities without losing data privacy on untrusted remote servers, e.g., public clouds, many Searchable Encryption (SE) schemes have been proposed to search over encrypted data without decryption. Normally, a SE scheme leaks access pattern by default in order to provide correct search results to users. Unfortunately, by utilizing access pattern, some recent attacks, such as *range injection attacks*, can easily recover the plaintexts of encrypted data through a set of injected range queries.

ACM Reference Format:
Boyang Wang and Firstname Lastname. 2018. Title: This a LaTeX Template. In *Proceedings of ACM XXXXX, XX, XX, XX, XX 2018 (ACM XXXXX'18),* **??** pages.
https://doi.org/10.475/123_4

1 INTRODUCTION

Searchable Encryption (SE) [**? ?**] aims to search encrypted data on an untrusted server without decrypting data. More specifically, with SE, a data owner, e.g., a company, can encrypt a dataset before storing data on an untrusted server, e.g., a public cloud. When this data owner or a user would like to search encrypted data on the server, it can submit a search token, i.e., the encrypted version of a query, to the server. With a search token, the server can return encrypted files/tuples matching to this query without accessing data or queries in plaintext. In addition to its implementation on public servers, SE could also act as the last line of defense minimizing data leakage on internal servers when security breaches, such as the recent leakage of Equifax's 143 million Social Security numbers, happen in practice.

Many SE schemes have been proposed to efficiently support different types of queries, including keyword queries [**? ? ? ? ? ?**] and range queries [**? ? ? ?**], over encrypted data. For example, while both data and queries are encrypted with a SE scheme, a user can retrieve encrypted files/emails containing a sensitive keyword, such as "Alzheimer", or it can retrieve encrypted records of patients' confidential information where attribute age is between $(40, 50)$, from an untrusted server. Several secure data systems, such as CryptoDB [**?**] and Google Encrypted BigQuery [**?**], have been implemented in practice based on existing SE schemes.

2 RELATED WORKS

Related works ....

3 ANOTHER SECTION

This is another section.

4 ANOTHER SECTION

This is another section.

5 CONCLUSION

The natural leakage of a SE scheme, access pattern, could compromise encrypted data if range injection attacks are implemented. Instead of completely hiding access pattern, which would require extremely high and unbearable costs with existing generic countermeasures (e.g., Oblivious RAM), we propose two novel and lightweight mechanisms to alleviate access pattern leakage and mitigate the impact of range injection attacks with affordable tradeoffs.

ACM XXXXX'18, XX 2018, XX, XX, XX

ACM ISBN 123-4567-24-567/08/06…$15.00
https://doi.org/10.475/123_4