Secure Data Search via Searchable Encryption Using HYPERLEDGER FABRIC Smart Contracts

Mălina Bulină

Supervised by Dr. Kaitai Liang and Dr. Roland Kromes

Cyber Security Group, Delft University of Technology

INTRODUCTION

I. Encryption
- protects data from attackers
- reduces search capabilities

II.Searchable Encryption (SE)
- allows keyword search over encrypted data [1]
- trapdoors are encrypted queries used for search delegation
- majority of SE schemes model server as honest-but-curious

III.Hyperledger Fabric (HLF)
- permissioned distributed ledger (DL) platform
- provides trust, immutability, transparency and provenance
- DLs are immutable databases shared across network of peers
- ledgers: data about current & historical state of a set of objects

IV. Smart Contracts (SC) [2]
- automated transaction protocols for asset manipulation
- based on predefined conditions
- known as chaincode (CC)

OBJECTIVE

How can SE be implemented using HLF Smart Contracts?

METHODOLOGY

I. Literature Review

II. Protocol Design
- Learn the requisite frameworks and concepts
- Develop a model using the open-source network [3]
- Implement the algorithm
- Evaluate the performance

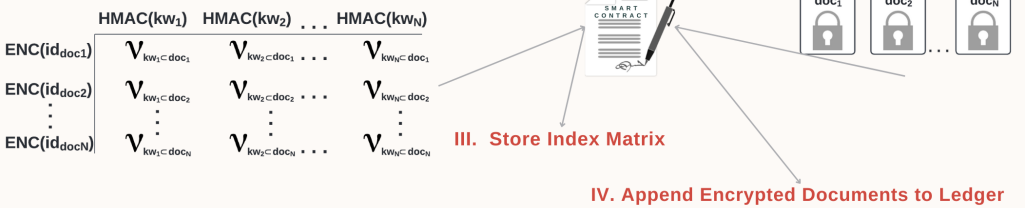
III. Log findings and draw appropiate conclusions

SYSTEM MODEL*

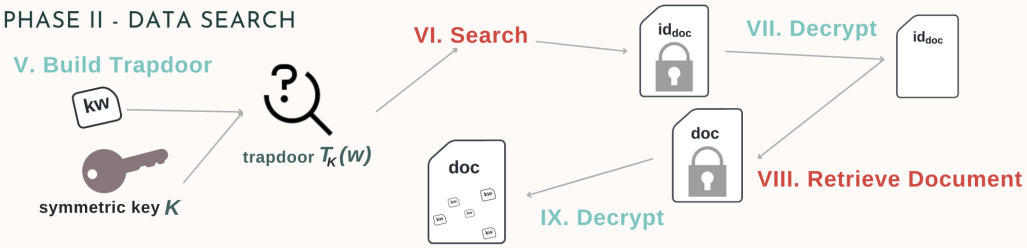
PHASE I - DATA APPENDMENT

I. System Initialisation

II. Build Index Matrix



PHASE II - DATA SEARCH



RESULTS

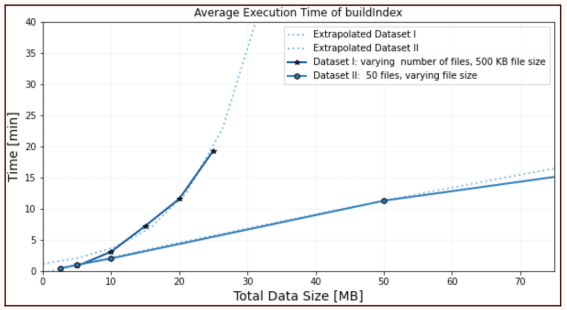


Figure 1. Time performance of two datasets. Dataset1 consists of 5 sets of 10, 20, 30, 40, and 50 files of size 500 KB. Dataset2 contains 5 sets of 10 files, each having size 250 KB, 500KB, 1MB, 5MB, and 25MB, respectively.

CONCLUSION

- **buildIndex** is faster for datasets with smaller number of files
- search takes ms to execute
- suitable for **larger files**
- single-writer/single-reader architecture

FUTURE WORK

- multi-writer/multi-reader architecture
- support multiple-keyword documents
- extend range of assets
- implement **dynamic** SE

* *methods written in **orange** are run by SC*
*methods written in **turquoise** are run locally*
the model was built upon the the PBSE scheme

References

[1] E. Androulaki et al., "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains" Proceedings of the Thirteenth EuroSys Conference, 2018.
[2] N. Szabo, "Smart Contracts: Building Blocks for Digital Markets," 1996.
[3] Hyperledger Fabric: Using the Fabric Test Network.
[4] S. Tahir and M. Rajarajan, "Privacy-preserving searchable encryption framework for permissioned Blockchain Networks", pp. 1628–1633, 2018.