Fidelis: Verifiable Keyword Search with No Trust Assumption.

Laltu Sardar
Institute for Advancing Intelligence
TCG CREST, Kolkata, India

&

Subhra Majumder
TU Wien
Vienna, Austria

July 11, 2023

tcg crest
Inventing Harmonious Future

Dependency on Cloud Computing and Storage Services

Small and Medium Enterprises

SME using Cloud Computing for
Cost & Security effectiveness

- Easier to process requests and Faster to respond
- Data survivable probability Increases

Can we TRUST Cloud Service Providers?

TRUST?

Read Data

Sell Data

Hacked

Manipulation

tcg crest
Inventing Harmonious Future

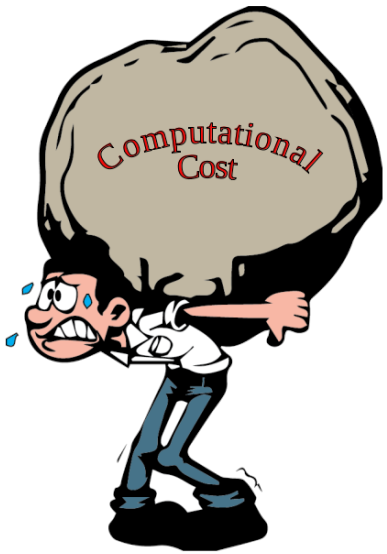
How to be SAFE? Trivial Solution

Encrypt Data

Send Encrypted Data

Store in cloud

Download all data → Decrypt → Search → Re-encrypt → Upload



Cloud can't Search!

tcg crest
Inventing Harmonious Future

What we Need → Ability to Query

1. Encrypt Data

2. Send Encrypted Data

3. Store in cloud

4. User Sends

Query Trapdoor

5. Cloud Search

over Encrypted Data

6.User received

Result/Response

tcg crest
Inventing Harmonious Future

System Model

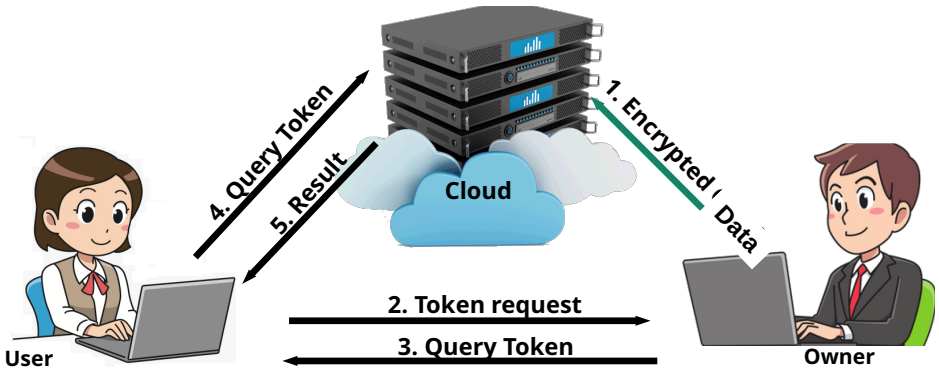
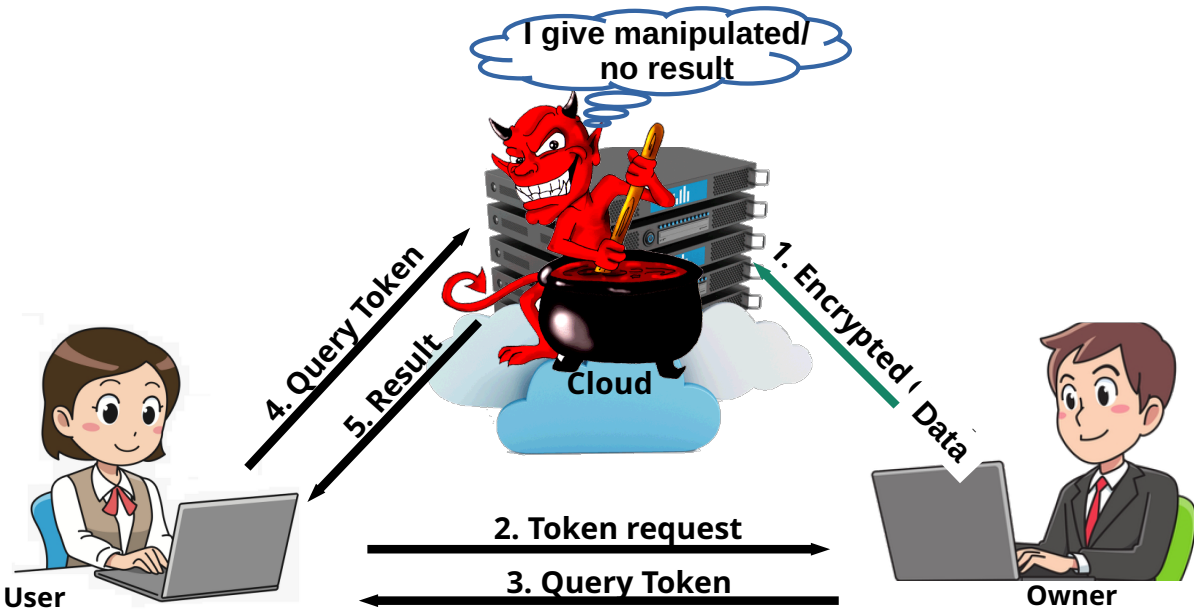


Figure: System Model

1. **Owner**: The owner of the database. Multiple owner can exists.
2. **User**: The users of the database. Sometimes owner is the only user.
3. **Cloud**: The storage and computation service provider.

Query: Given a keyword, return all files that contains the keyword.

What if the Cloud become Malicious?



Then, the Cloud can

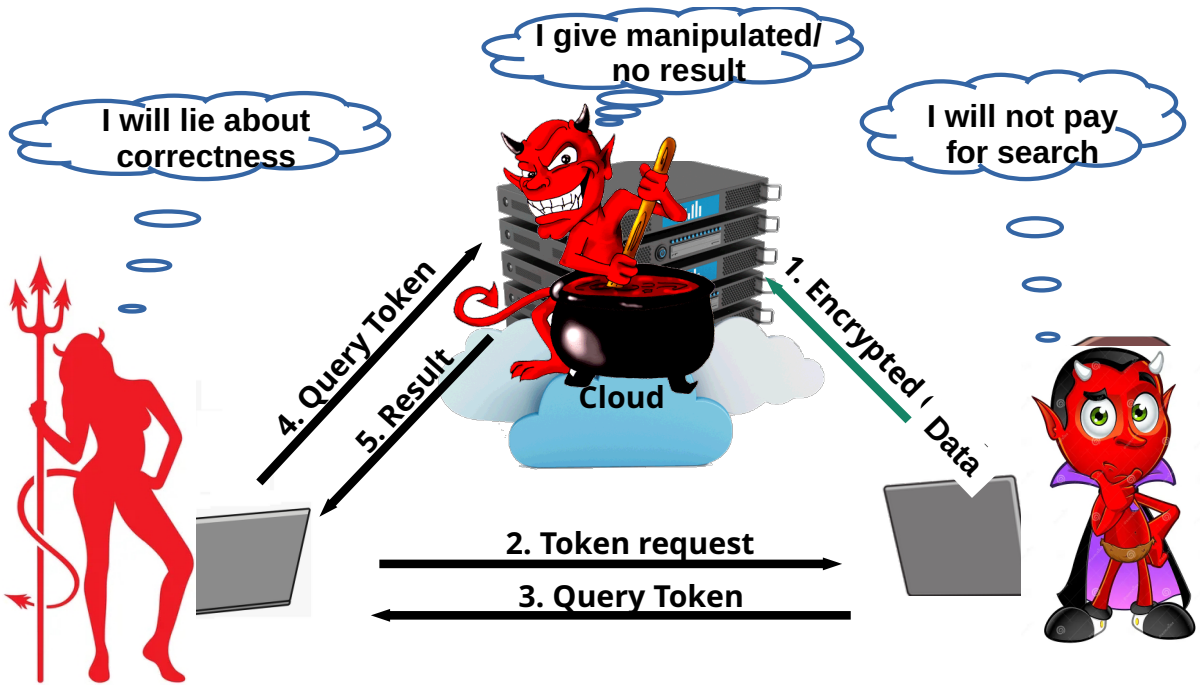
1. send random result, without searching.
2. Intentionally can send manipulated result

Solution?

1. Numerous solution exists.
2. Results from malicious cloud can be verified by anyone, including honest client

tcg crest
Inventing Harmonious Future

What if the Clients become Malicious too?



Then, the Client can

1. falsely claim incorrectness
2. avoid service fee

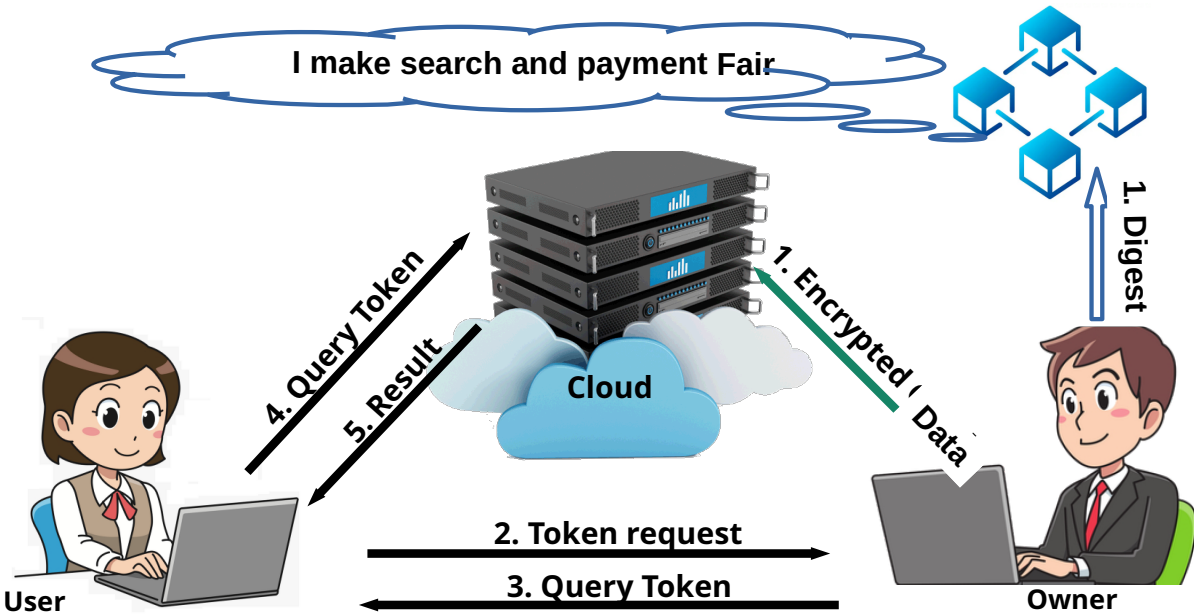
Solution? Consensus based protocol

- Most considers users malicious but owner trusted
- Guo et al. [1] Gave a solution but require O(DB) storage in Blockchain

tcg crest
Inventing Harmonious Future

Our Contribution

We provided a blockchain based solution addressing above issues

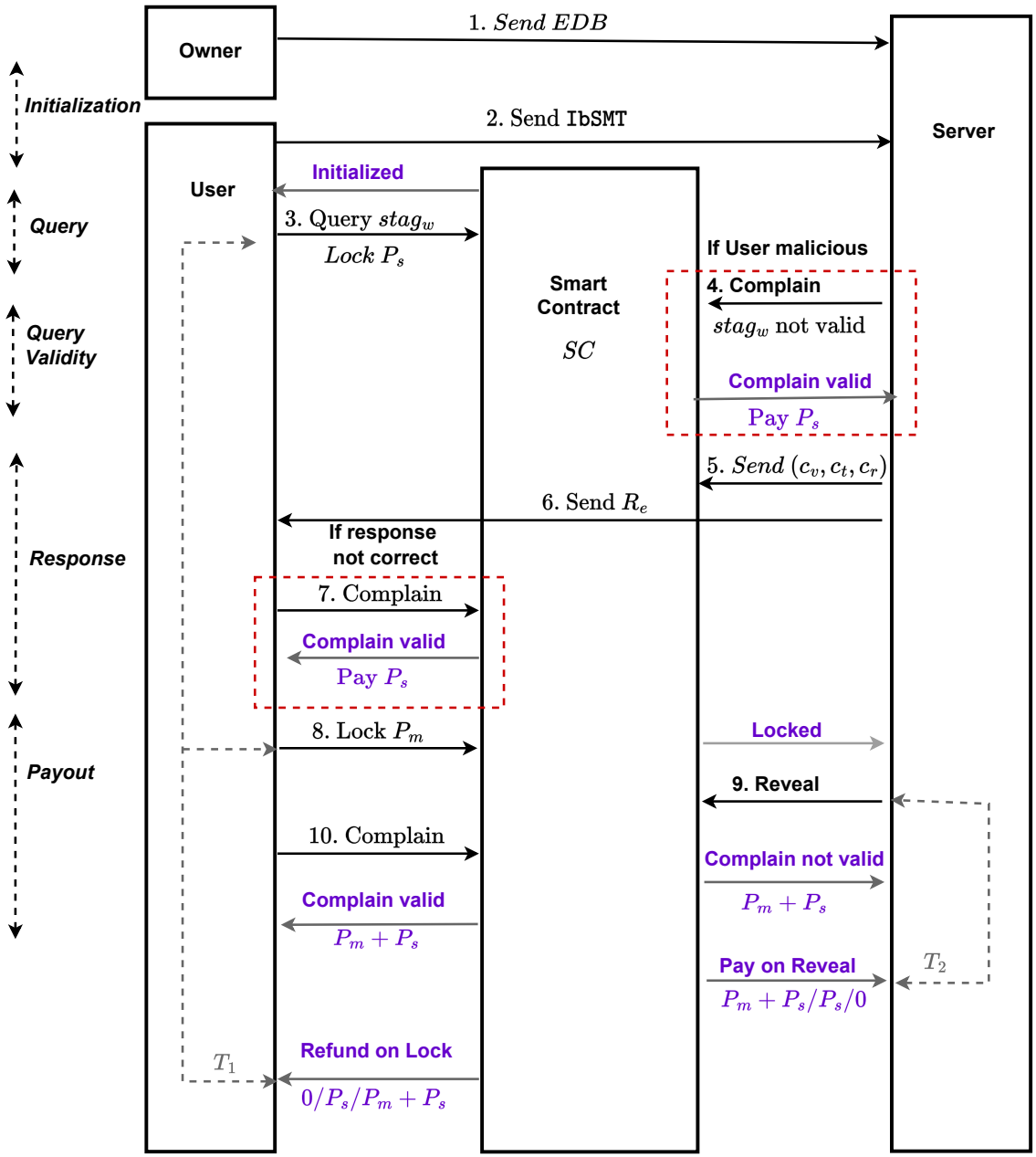


1. Owner sends digest of valid keywords to blockchain
2. From start to end of a search, blockchain is used

Our proposed scheme Fidelis

1. Enable searching when all parties are malicious
2. For every search, it requires only constant costs due to smart contract

tcg crest
Inventing Harmonious Future

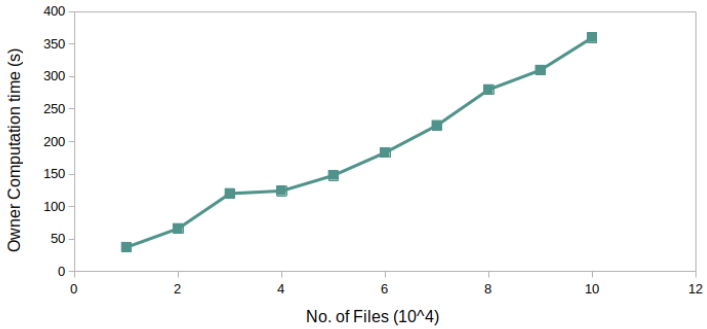


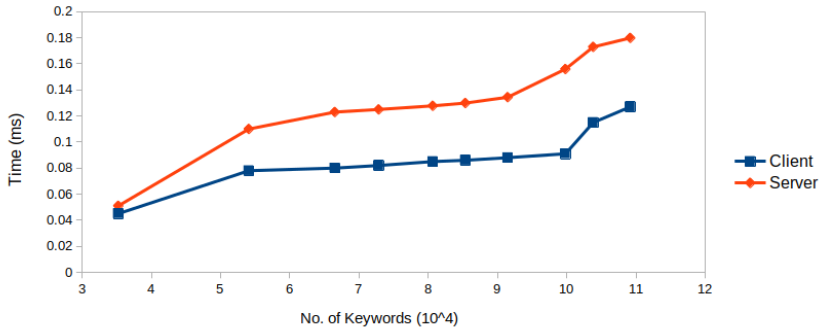
1. $stag_w \rightarrow$ search tag for keyword w,
2. $R_e \rightarrow$ encrypted result,
3. $\{c_v, c_t, c_r\} \rightarrow$ commitments,
4. $P_s, P_m \rightarrow$ payments

tcg crest
Inventing Harmonious Future

Experimental Evaluation

We implement and evaluate the protocol w.r.t. **Ethereum** and smart contracts deployed in Ropsten test network.





a. Owner's b. User and Server's Computation Time during initialization

• On **a existing keyword Searching**: `SendCommitment` takes 16s & costs is 9.5 USD same as `StoreandLock`. However, `Reveal`, takes 21s, & 10.0 USD and payment finalization takes 18s & costs 2.8 USD.

• On **a non-existing keyword Searching**: `QueryValid` execution time taken varies between 20s and 34s whereas gas cost varies from 41.3 to 43.5 USD.

These $\Longrightarrow$ Fidelis is *practical*, *efficient* and *scalable*.

tcg crest
Inventing Harmonious Future

References:

[1] Guo, Y., Zhang, C., and Jia, X. *Towards public verifiable and forward-privacy encrypted search by using blockchain*. IEEE TDSC. 2022

[2] Jiang, S., Liu, J., Wang, L., and Yoo, S. *Verifiable search meets blockchain: A privacy-preserving framework for outsourced encrypted data*, IEEE ICC 2019.

tcg crest
Inventing Harmonious Future

tcg crest
Inventing Harmonious Future

Questions?