Journal Report (Draft v1)

A Paillier Approach to Secure Land Purchasing using Multi-party Skyline Queries

Abstract

The abundance of available data can cause information overload, making it difficult for consumers to make the best decisions. This is especially true when buying land online, as buyers must sort through a wide range of land alternatives in different places at different price points. Furthermore, because seller data pertains to landowners, it is sensitive by virtue of its commercial nature. Thus, it is essential to provide information anonymity, seller anonymity, and data privacy.

To find dominant—that is, ideal—land datasets, this study suggests a system that makes use of multiple skyline query methods, including bitmap, index, closest neighbor (NN), and block nested loop (BNL). Differential decryption keys are shared among several authorities to ensure data privacy. The framework uses a hybrid network-based approach with strategies like re-encryption and shuffling in addition to the Paillier cryptosystem for seller and information anonymity. Finally, following registration, the seller is given an anonymous identity.

The framework's efficacy is exhibited by means of the screening procedure, confidentiality protocols, and outcome evaluation. Land buyers can therefore find the best possibilities more easily because of this. This document provides an overview of the suggested system.

Introduction

The landscape of land purchasing is rapidly transforming with the rise of online platforms. These platforms offer immense convenience for both buyers and sellers. Buyers gain access to a wider selection of properties, enabling them to compare options and make informed decisions. Sellers benefit from increased visibility and a wider pool of potential buyers. However, this digital shift also introduces significant challenges.

One major hurdle for buyers navigating online land marketplaces is information overload. Presented with a vast amount of data on various land options, each with its own unique set

of attributes like area, price, location, and amenities, buyers can struggle to identify properties that best fulfill their specific needs and preferences. Traditionally, sifting through countless listings requires a significant investment of time and effort, often leaving buyers feeling overwhelmed and unsure of their choices.

Furthermore, the security and privacy of sensitive land information is paramount in this online environment. Landowners entrust platforms with details concerning their property, which can be considered commercially sensitive. Additionally, anonymity is crucial for sellers, protecting them from unwanted solicitations or potential competitive disadvantages. These privacy concerns pose a significant barrier to wider adoption of online land purchasing platforms.

This paper proposes a novel framework aimed at revolutionizing online land purchasing by addressing these critical challenges. Our framework leverages the power of multi-party skyline queries to efficiently identify the most desirable land options for buyers. Skyline queries operate on datasets containing multiple attributes, enabling users to define their preferences and retrieve only the properties that consistently outperform others based on these criteria. This significantly reduces information overload and empowers buyers to make well-informed decisions with greater ease.

To ensure the security and privacy of sensitive land information, our framework utilizes the Paillier cryptosystem. This homomorphic encryption scheme allows for secure computations on encrypted data. Data remains encrypted throughout the entire process, eliminating the need for decryption and minimizing the risk of exposure. Additionally, we incorporate mixed network techniques to further enhance anonymity for both sellers and the information itself. Through these innovative approaches, our framework fosters a secure and trustworthy environment for online land purchasing.

This paper provides a comprehensive exploration of our proposed framework. We delve into the technical details of its design, analyze its security properties, and evaluate its efficiency through performance benchmarks. Ultimately, this framework empowers buyers to navigate the complex world of online land purchasing with confidence, while safeguarding the privacy and security of all parties involved.

Methodology

A. Overview of the Proposed Framework

The system involves several entities: two mix servers COH1 (Cryptographic

Operation Handler 1) and COH2 (Cryptographic Operation Handler 2), an assistant ICSP (Information Collector and Service Provider), multiple landowners (LOn), and buyers (users).
Each LOn receives an anonymous unique identity IDn from ICSP after completing online registration. Each LOn can have multiple datasets (DAn1, ..., DAnj), where j denotes the number of datasets, and each dataset has uniform data types.

COH1 and COH2 generate their own Paillier cryptographic key pairs. These key pairs are used to perform encryption, re-encryption, shuffling, and decryption of the datasets.

B. Individual Stages

1. User Registration: Registration of landowners (LOn) will be conducted under ICSP, inheriting the mechanism of anonymous credentials for owner anonymity: Each LOn submits their legitimacy (name, email, address, etc.) privately to ICSP. If ICSP is convinced, it provides a random unique anonymous credential IDn to LOn. The LOn can appear anonymously to everyone thereafter.
2. Data Encryption and Submission: This stage comprises the encryption of datasets by the owners using the Paillier cryptosystem, submission of the encrypted datasets, and approval of the posted datasets on the website:

   Key Generation: COH1 and COH2 generate their Paillier public/private key pairs. The public keys are denoted as $PK1$ and $PK2$ and the private keys as $SK1$ and $SK2$. Data Encryption: Each LOn encrypts its datasets (DAn1, ..., DAnj) using the public keys PK1 and PK2. The Paillier encryption scheme ensures the privacy of the data.
   Submission: The encrypted datasets are submitted to ICSP along with the anonymous identity IDn.
   Confirmation: When LOn finds its dataset on the website, it places a unique confirmation code on the specified location of the website.
3. Re-encryption and Shuffling
   In the proposed framework, re-encryption and shuffling of encrypted data are used to anonymize the datasets:

   Re-encryption: ICSP sends the encrypted datasets to COH1 and COH2 for re-encryption. Both handlers re-encrypt the datasets using their respective public keys.
   Shuffling: The Fisher-Yates shuffle algorithm is used to shuffle the re-encrypted

datasets. Decryption: COH1 and COH2 then decrypt the shuffled datasets using their private keys (SK1 and SK2) to retrieve the original datasets.
Posting: The decrypted datasets are posted on the website with unique identities for each landowner.