Updated Methodology

(This section describes the overview of the proposed framework and the individual stages of the work using the Paillier cryptosystem and Fisher-Yates shuffling algorithm.)

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.