

B. TECH. PROJECT REPORT

on

Smartphone based Land Records Retrieval System

By
Naman Jain
Pranshu Maheshwari
Saksham Tanwar



DISCIPLINE OF COMPUTER SCIENCE AND ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY INDORE
April 28, 2021

Contents

1	Introduction	3
1.1	Generic Application	3
1.2	Disadvantages of a centralized database	3
1.3	Advantages of using Blockchain	5
1.4	IPFS	6
1.5	Motivation	6
1.6	Proposed Solution	7
1.7	Organisation of Dissertation	8
2	Advantages of Decentralized Solutions	9
2.1	Blockchain	9
2.2	IPFS	9
2.3	Related Works	9
3	Chapter 3	11
3.1	Records Server	12
3.1.1	Add Land Record	13
3.1.2	Transfer Land	15
3.1.3	Split Land Record	15
3.1.4	Query Records	15
3.1.5	Query Records	19
3.2	Smartphone Application	19
3.2.1	Sequence Flow	19
3.3	LRSP Server	25
3.3.1	Sequence Flow	25
3.3.2	Usage	26
3.4	Verification Server	29
3.4.1	Types of Certificates	29
3.4.2	Sequence Flow	30
3.5	Blockchain	31
3.5.1	Data Format	32
3.5.2	Create Land Record	33
3.5.3	Transfer Land Ownership	34
3.5.4	Split Land Record into Two Records	34
3.5.5	Get all records in a village/sub-district/district/state	36
3.5.6	Get ownership history of a land	36
4	Chapter 4	38
4.1	Records Server	38
4.2	Verification Server	38
4.3	LRSP Server	39
4.4	Smartphone Application	39
4.4.1	Android	39

4.4.2	iOS	40
4.5	IPFS	41
4.6	Blockchain	41
5	Chapter Five	42
5.1	Conclusion	42
5.2	Future Work	42

1 Introduction

1.1 Generic Application

A typical application can be broken down into three logical layers namely:-

- **Presentation Layer:** It is the layer responsible for display information and collect information from the user.
- **Business Logic Layer:** In this layer, information collected from presentation layer is used to perform the various calculations and operations needed to be performed by the application.
- **Data Layer:** This layer is responsible for storing and retrieving data to be used by other layers.

Data Layer is typically implemented using a database, which is an organized collection of data. A database can be of two types : Centralized and Distributed.

1.2 Disadvantages of a centralized database

Most applications require data in some form or another and need to store the said data for future use, this is where databases come into picture. A database is an organized collection of data, generally stored and accessed electronically from a computer system. Access to this data is usually provided by a "database management system" (DBMS) consisting of an integrated set of computer software that allows users to interact with one databases and provides access to all of the data contained in the database. DBMS's provide various functions that allow management of a database and its data such as Data definition which defines the database model i.e. the logical structure of the data model, Updating of actual data which includes insertion, modification, and deletion of the actual data, Retrieval of actual data which may or may not include data processing and Administration which includes allowing access to various users, enforcing data security and various other checks. [1] A database model is a type of data model that determines the logical structure of a database and fundamentally determines in which manner data can be stored, organized and manipulated. The most popular example of a database model is the relational model, which uses a table-based format. The ACID (Atomicity, Consistency, Isolation and Durability) database design is one of oldest and most important database design. A relational database that fails to follow the ACID model cannot be considered reliable.

Databases can be categorized in many categories depending on how they store data, where it is stored and the additional functionality the DBMS can provide on the stored data. Broadly databases can be categorized into two major categories centralized and distributed. They both have their advantages and disadvantages. A centralized database is a database that is located, stored, and

maintained in a single location and has a single DBMS but can be accessed by the users distributed in the network. A distributed database system consists of a collection of local databases, geographically located in different points (nodes of a network of computers) and logically related by functional relations so that they can be viewed globally as a single database [2]. There are two types of distributed databases homogeneous and heterogeneous. In a homogeneous distributed database all the locations store the database identically i.e. all locations have the same management system and schema. Whereas in heterogeneous distributed database different locations can have different management software, schemas. For a database management system to be distributed, it should be fully compliant with the twelve rules introduced by C.J. Date in 1987 [3]: local autonomy; the absence of a dependency from a central location; continuous operation; location independent; fragmentation independent; replication independent; distributed query processing; distributed transaction management; hardware independent; operating system independent; independent of communication infrastructure; independent of database management system.

If a centralized database is used to store the data then the whole system is prone to Single Point of Failure, if for some reason the database fails the whole system will fail. As all the data is stored in a single location, if there are no precautionary measures taken then a hardware failure can lead to complete data loss. The databases are also vulnerable to cyberattacks which can cause data loss, data leaks, data inconsistency and many other vulnerability. This makes centralized database dubious with very low reliability. But at the same time, centralized database ensures data consistency and easy management in compliance with ACID design [4].

A major advantage of distributed database is that by sharing a database across multiple nodes can obtain a storage space extension and also can benefit from multiple processing resources. A distributed database system is robust to failure to some extent. Hence, it is reliable when compared to a centralized database system. It is also more robust compared to a centralized database as it doesn't have a single point of failure, if a node fails another node or group of nodes can provide the necessary data. But to make this possible complex software's are required which incur additional costs and processing overheads. Maintaining data integrity is difficult and hence minimum redundancy and ACID properties are more relaxed than compared to a centralized database [4]. Distributed environment also faces problems such as fragmentation and data replication. A data fragment constitutes some subset of the original database. A data replica constitutes some copy of the whole or part of the original database. The fragmentation and the replication can be combined: a relationship can be partitioned into several pieces and can have multiple replicas of each fragment [5].

1.3 Advantages of using Blockchain

Blockchain is a type of decentralized database where the data is stored in blocks and each block is linked to the previous block using its cryptographic hash, thus forming a chain. As the blockchain grows in size, it becomes more and more difficult to tamper the data in these blocks. Blockchain based databases are more trustworthy, reliable and secure than traditional databases.

A blockchain based system is decentralized. Hence, a centralized authority is not necessary. Decentralized systems are also resilient to single point of failure. A blockchain network comprises of various nodes, each maintaining its own copy of database. Hence, all the data is replicated, shared and synchronized across all the nodes in the network. This makes the data almost tamper proof as it will be very costly and thus highly unlikely for a malicious person to change the data across the whole network. No node can directly write data to the blockchain as it can make the data inconsistent, to avoid this the blockchain network uses a consensus algorithm which helps all the nodes in the network to come to a consensus and commit the data in the blockchain. This helps to keep all the nodes in the network to get synchronized with each other.

The data that is committed to the blockchain is immutable. After some data is inserted into the blockchain, it is very difficult to delete or alter it. This is realized by including, in each block, the cryptographic hash of its previous block. Because of this immutability, a blockchain database only supports create and read operations in contrast to traditional databases which supports create, read, update and delete (CRUD) operations. To update the database state, a subsequent write is required. Old writes persist in the blockchain forever, making it convenient to trace how the blockchain database state is updated over time. This makes it possible to trace the actions that resulted in a particular database state.

Another benefit of blockchain is that it provides transparency to the data stored in it. This is achieved by replicating the blockchain data among multiple nodes present in the blockchain network. Nodes in the blockchain network not only can view the data already committed to the blockchain but can also participate in the process of validating the data to be committed in the blockchain. The transparency also helps users to cross verify some data against the blockchain.

A blockchain ledger is logically a single public ledger. Since every node updates its copy of blockchain ledger in sync with each other and after consensus is reached, the whole network logically act as one single public ledger. This removes the complications present in traditional systems where different participants or organizations maintains multiple ledgers which needs to be reconcile and synchronized time to time.

Systems that are deployed on public blockchain network are more cost efficient as compared to the traditional systems. This is because the system utilizes the processing power and resources of a large number of nodes that are already connected to the blockchain network, thus significantly reducing the cost needed for setting up and maintaining centralized servers present in traditional systems.

Blockchain based systems are more secure and resilient to cyber attacks, which can cause data loss, data leaks, data inconsistency and many other vulnerability, than traditional systems. Whenever a new block is introduced in the blockchain, its hash value is calculated which also includes the hash of its previous block. If a malicious user fraudulently tries to tamper the data inside a block, not only its hash value changes, but the hashes of the following blocks get changed too. This, along with the fact, that the data is stored in multiple nodes present in the blockchain network, makes it very difficult to tamper the data present in the blockchain.

1.4 IPFS

The Interplanetary File System (IPFS) [6] is a peer to peer distributed file system for sharing and storing data. IPFS provides a high throughput storage system where each file is uniquely identified by a cryptographic hash. In IPFS, multiple users store a piece of each others' data and actively participate in making it available in the network. In contrast to HTTP which uses location based addressing, IPFS uses content based addressing. In content based addressing, user request data using its content identifier instead of the location where it is stored.

IPFS uses Distributed Hash Table (DHT) [7] to enable routing and discovery of peers and content on the network. The hash table is split across all the participating nodes in the IPFS. These nodes coordinate with each other to enable efficient lookup and retrieval of data on the network. IPFS stores data using a data structure called Merkle DAGS [6]. Each node in a Merkle DAG stores the cryptographic hash of each of its children. Thus, altering a node's data changes the hash value of the node as well as all its ancestors in the DAG. This makes the data stored on the IPFS immutable.

1.5 Motivation

In India, currently if person is asked to prove if he/she is the owner of a piece of land then all they can show for it is a sale deed which just proves that the person was the owner at a particular time, but that person cannot prove that he/she is still the owner of that land. For proving the same he/she has to go to various government offices and collect various document showing that no sale

deed has been registered for that land after the one which the person has. When a person wishes to buy land in India, they have to be very careful and perform various checks such as

- Check if the deed title is in the name of the seller and if he/she has the full right to sell it
- Procure a Encumbrance Certificate from sub-registrar's office where the deed is registered which declares that the land is free of any legal hassle and unpaid dues
- Check if the Property tax and other bills are paid in full and the seller has the respective original receipts
- Check if the loan on the land has been completely repaid

If a buyer is lethargic in verifying these documents he/she can be easily duped into buying a disputed land parcel or it may even happen that the land in question did not even legally belong to the said seller, that is the seller was not the genuine owner of that land provided fake documents. As these documents are mostly maintained offline as hard copies these cases occur often.

Getting all the information such as the sale deeds and ownership history for a land parcel is very cumbersome, a simple solution to this problem is a smart-phone application with which users/potential buyers can get land ownership history and related documents for a particular land parcel. These documents and data can be stored in a database by the government and will be updated every time a new sale deed is registered i.e. owner for a land parcel changes. This makes the process of acquiring the documents in question very easy and hassle free.

Indian government launched Digital India Land Record Modernization Programme in 2008. Main aim of this programme is to create a system of updated land records, automated and automatic mutation, integration between textual and spatial records, inter-connectivity between revenue and registration, to replace the present deeds registration and presumptive title system with that of conclusive titling with title guarantee [8]. In addition to this, Indian government also plans on storing the digital records on a private blockchain and provide a system where citizens can view the ownership details and complete history of the property before going in for the purchase [9].

1.6 Proposed Solution

To tackle this problem of accessing land records, a smartphone based solution is proposed. Users can request land records for a particular land parcel by visiting the land parcel or marking it on the map. Land records are stored on a private blockchain which provides methods to access the data. For help in migrating

old records to the new system, scanned documents can be uploaded. These documents are stored in a private IPFS cluster with their Content Identifier (CID) is stored on the blockchain. A verification portal is also part of the solution where users while accessing records will be given verification code which users can use to generate a digitally signed PDF for verifying the land records.

1.7 Organisation of Dissertation

A brief introduction to our proposed solution and the motivation behind it was discussed in chapter one. Chapter one also provided the generic application architecture and contrasted the centralized databases with blockchain databases. Chapter two provides an introduction to the various offerings of the blockchain technology that is makes it useful for the proposed solution. Chapter two also provides a summary of related works. Chapter three describes the proposed solution's architecture including the various actors/users of the solution, various submodules as part of the solution and how they interact with one another. Chapter four provides details regarding the deployment of the proposed solution. Chapter five concludes with the main contributions of this work and proposes direction for future work.

2 Advantages of Decentralized Solutions

2.1 Blockchain

[10] discusses various complications present in the current land record management system in India. The existing land records in India are not administered properly due to which they often are not consistent with the ground truth. Various departments, at the village or District level, are involved in maintaining ownership history of land. Often, the data present with different departments are not in sync with each other which results in discrepancies. Such discrepancies often result in conflicts in land ownership, double spending problem, etc. The data is also susceptible to alteration by corrupt officials.

Blockchain provides a potential solution to various complications present in the current land record management system. Being a distributed database, Blockchain based land record system is resilient to single point of failures. Data is replicated across multiple nodes in the Blockchain network. Hence, it prevents any undesirable data loss as was seen during Haiti 2010 Earthquake [11].

A Blockchain ledger contains transactions that are endorsed by appropriate authorities. These transactions, being committed in a chronological order, provides a verifiable audit trail for legal investigations [12]. Once committed to the Blockchain, the transactions cannot be modified or deleted, hence providing a trusted source of information.

Blockchain is a shared ledger. Each participant has a copy of the ledger. With necessary permissions, a participant can commit data into the ledger which, after getting validated by other nodes, gets reflected across the entire Blockchain network. This removes the complications present in the current land record management systems where different departments maintain land data which needs to be reconcile and synchronized regularly.

2.2 IPFS

IPFS, being distributed, is resilient to single point of failure. It is more secure to DDos attacks than centralized system. Multiple nodes can simultaneously participate in distributing a particular file resulting in better throughput. The data retrieved from IPFS can be verified by calculating its hash. Hence, data stored on IPFS is self-verifiable. Data can be pinned on multiple nodes to ensure it persists on IPFS. This makes IPFS resilient to data loss.

2.3 Related Works

To tackle the problem of accessing and verifying the land ownership records, this paper proposes a smartphone based solution. Using which users can request

land ownership records for a particular land parcel by taking the advantage of the GPS module available in smartphones. These land ownership records are stored in a permissioned blockchain and to make it backwards compatible i.e. migrating old records to the new system, scanned copies of the documents can be stored in permissioned IPFS cluster with their Content Identifier (CID) stored on the same blockchain. Now whenever users want the ownership history of a land parcel they use the smartphone application, mark the piece of land and after successful completion of the process they get a PDF report with the ownership history of that said land parcel. This PDF report also contains verification codes for each ownership record they hold, these verification codes can then be used on a verification portal to generate a digitally signed PDF verifying that the given information is true. This solution hence provides a trustful and hassle free mechanism for people to access and verify land ownership records.

3 Chapter 3

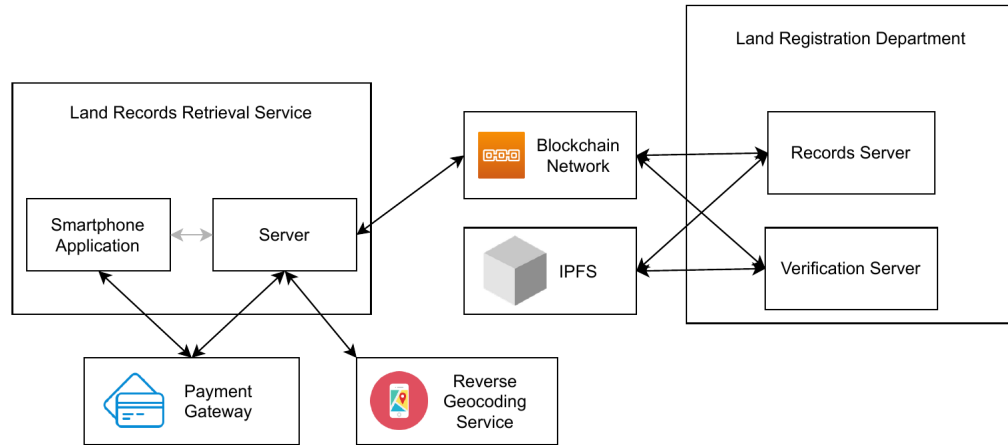


Figure 1: Overall Architecture

Overall solution architecture consists of the following (as seen in Figure 1):-

- **Land Records Retrieval Service :-** Responsible for providing land records service to the users who want to obtain land records by visiting the land parcel itself or marking the land on map.
 - **Smartphone Application :-** Provides a user interface for users to interact with where users can request land records for a particular land by marking the point on map.
 - **Server :-** Backend server for the Smartphone Application. It interacts with the blockchain network to compile the summary of the land records requested by the users.
- **Payment Gateway :-** Razorpay payment gateway service is used to process payments.
- **Reverse Geocoding Service :-** MapMyIndia's reverse geocoding API is used to get a particular place's State, District, Sub-District and Village from GPS Coordinates.
- **Blockchain Network :-** Blockchain network is responsible for storing all the land records consisting of details about all the land parcels and their transactions.

- **IPFS :-** Since blockchain network is not ideal for storing files, IPFS is used to store files such as certificates and scanned documents.
- **Land Registration Department :-** Responsible for adding records to the blockchain and providing a verification portal where users can obtain digitally signed certificates to verify land records.
 - **Records Server :-** Responsible for serving the website using which Land Records can be added to the blockchain.
 - **Verification Server :-** Responsible for serving the website using which Land Records can be verified by allowing users to download digitally signed certificate that contain the information stored on blockchain.

Users which use the proposed solution :-

- **Land Information Seeker :-** These users need to access land information, they can be the prospective buyers for a particular land looking to validate the current owner's claim on the land.
- **Land Registration Department Admins :-** These users enter information on the blockchain. Only these users can enter information to the blockchain.

3.1 Records Server

This serves a web application that allows users in Land Registration Department to enter and query land records on blockchain. To support migration of old land records onto the new platform, uploading scanned documents with each transaction such as adding a land record, transferring a land or splitting a land record is supported. All the documents are stored in the IPFS.

For each land record, a PDF certificate, digitally signed by the Land Registration Department, is generated which includes all the information about the land such as the current owner, khasra number etc. This certificate is stored in the IPFS.

For each land transfer, a PDF certificate, digitally signed by the Land Registration Department, is generated which includes all the information related to the land transfer. This certificate is stored in the IPFS. In a land transfer, land record certificate is also updated to reflect the current owner.

This web application provides following operations to the user :-

- **Add Land Record :-** Add a land record.
- **Transfer Land :-** Transfer land ownership.

- Split Land :- Splits a land record into two separate land records, useful in cases when a part of land needs to be transferred.
- Query Records :- Users can query records in any particular State, Sub-District, District or Village.
- Query Ownership History :- Users can query ownership history of a particular land.

Records server is implemented using Express framework, a NodeJS module.

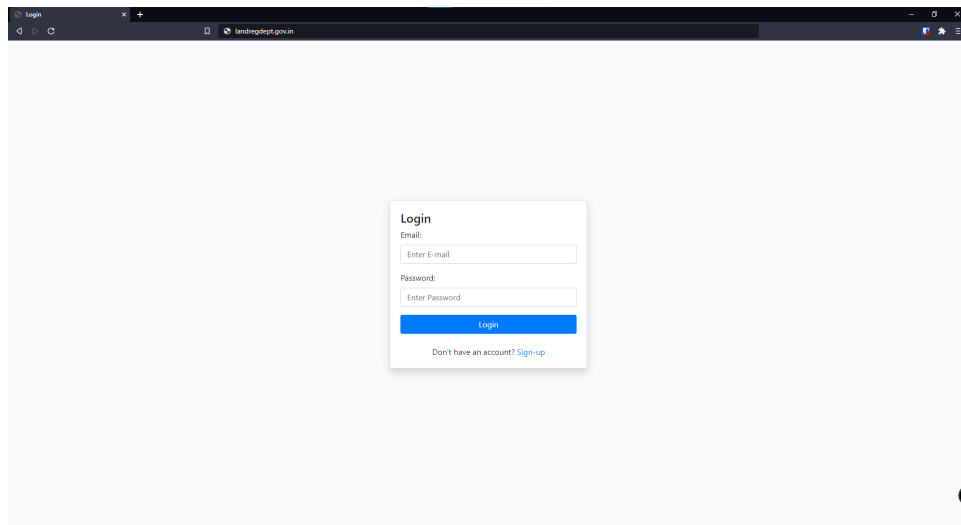


Figure 2: Login Page for the Records Server

3.1.1 Add Land Record

Adding a land record entails:-

1. Get input from user.
2. Generate certificate from the details.
3. Upload certificate to IPFS and receive CID for the certificate.
4. Create land record on the blockchain

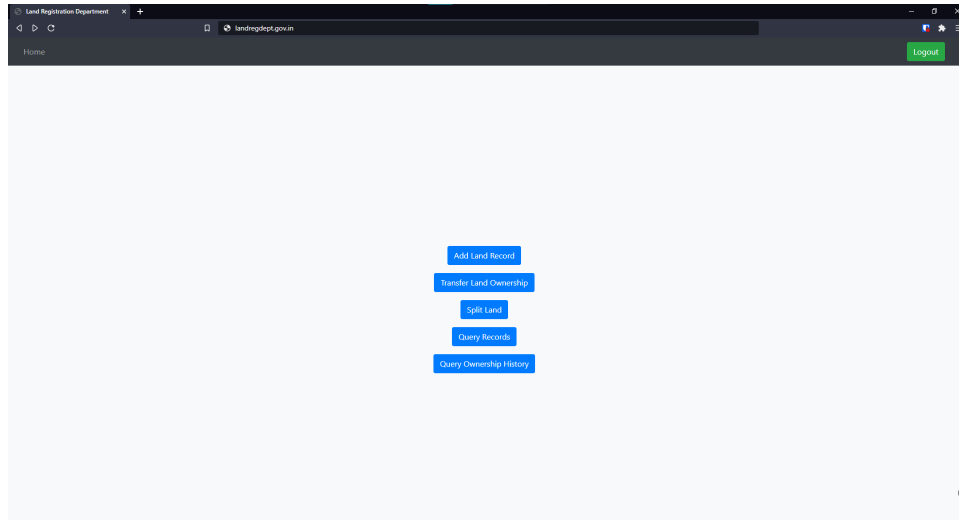


Figure 3: Home Page

A screenshot of the 'Add Land' web page. The browser's address bar shows 'landregdept.gov.in/form/add'. The page has a dark header with a 'Logout' button. The main content area is light gray. A white form titled 'Add Land' is centered on the page. The form contains the following fields: 'State' (dropdown menu), 'District' (dropdown menu), 'Sub-District' (dropdown menu), 'Village' (dropdown menu), 'Khata Number' (text input), 'Number of Points' (text input), 'Land Area' (text input), 'Khata Number' (text input), 'Owner Name' (text input), and 'Other Docs' (text input with a 'Choose Files' button and the text 'No file chosen'). A blue 'Submit' button is at the bottom of the form.

Figure 4: Add Land Records web page

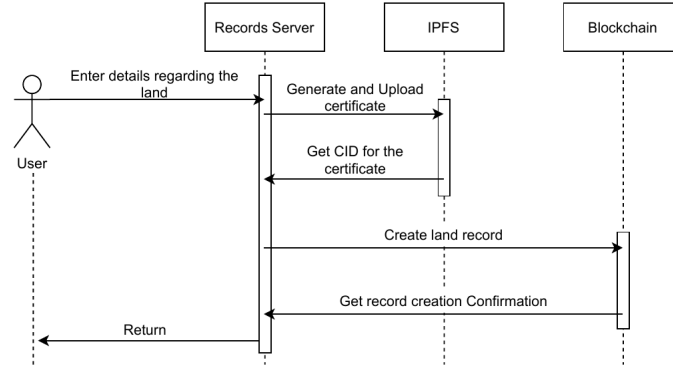


Figure 5: Sequence Diagram for adding land record

3.1.2 Transfer Land

Transferring a land record entails :-

1. Get input from user.
2. Generate land transfer certificate containing details about the land transfer.
3. Generate land record certificate containing details about the land and current owner.
4. Upload certificates to IPFS and receive CIDs for the certificates.
5. Create land transfer record and update land record on the blockchain.

3.1.3 Split Land Record

Splitting a land record entails :-

1. Get input from user.
2. Generate certificates for the two land records.
3. Add two new land records and mark old land record as expired on blockchain.

3.1.4 Query Records

Users can query all the records in a particular village, sub-district, district or state. Querying records entails :-

1. Get input from user.
2. Query records from blockchain.

Figure 6: Transfer Land

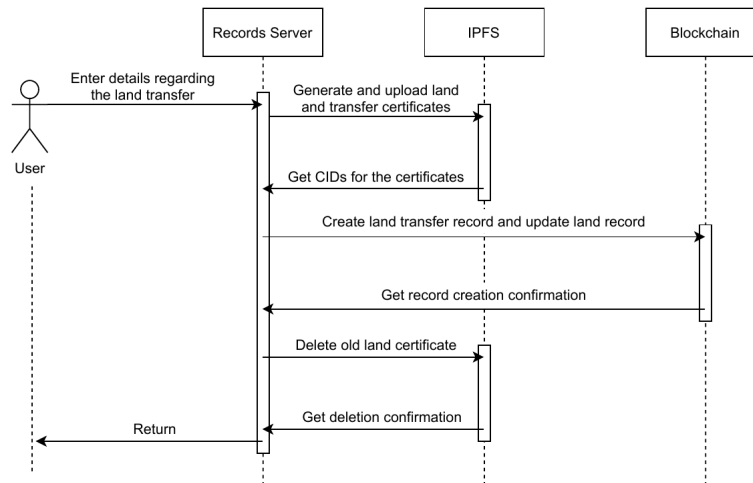


Figure 7: Sequence Diagram for transferring land

Split Land

State:

District:

Sub-District:

Village:

Khata Number:

New Khata Number A:

Number of Plots in Land A:

Land Area A:

New Khata Number B:

Number of Plots in Land B:

Land Area B:

Other Decs A: No file chosen

Other Decs B: No file chosen

Figure 8: Split Land Record

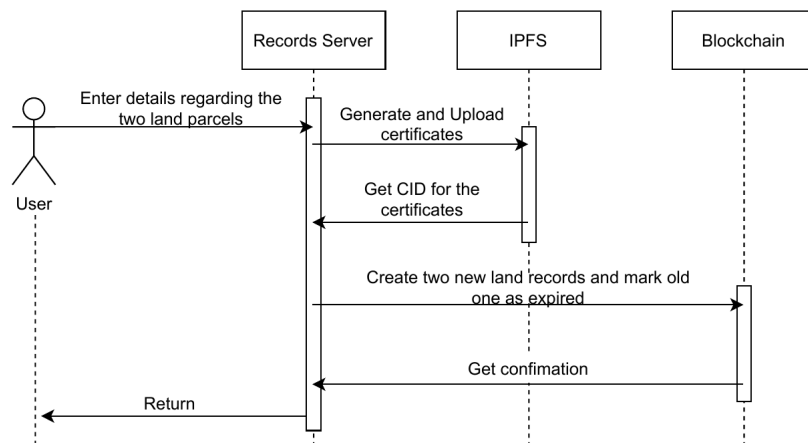


Figure 9: Sequence diagram for splitting a land record

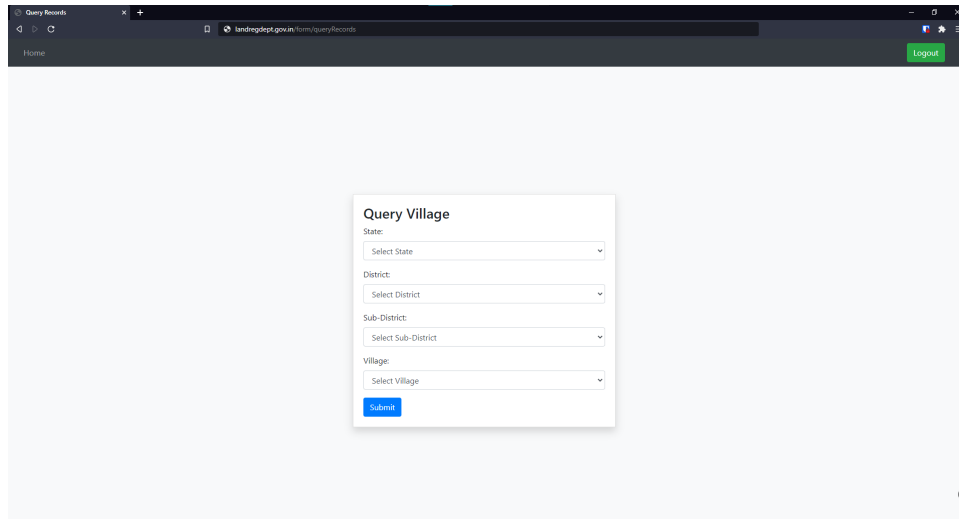


Figure 10: Query Land Records

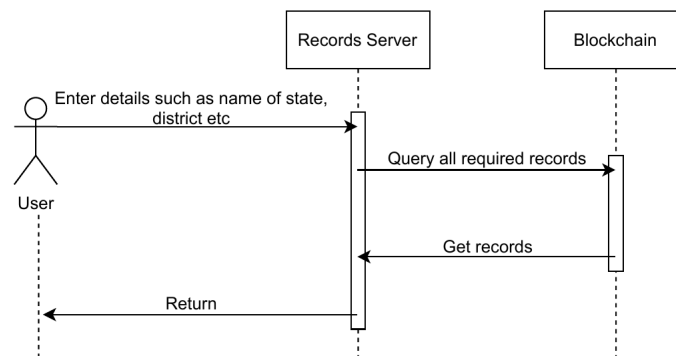


Figure 11: Sequence diagram for querying records

3.1.5 Query Records

Users can query ownership history of a particular land. Querying records entails :-

1. Get input from user.
2. Query records from blockchain.

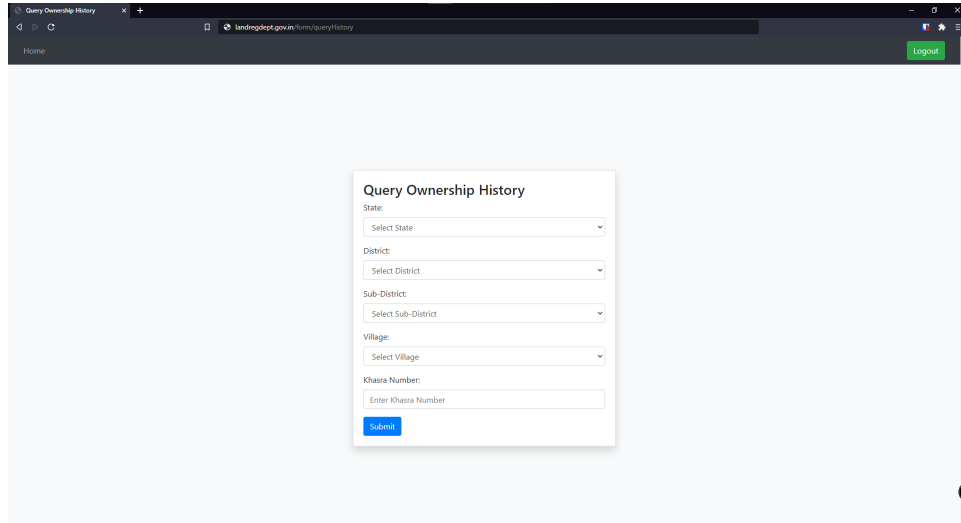
A screenshot of a web browser displaying a form titled "Query Ownership History". The form is centered on a light gray background. It contains several dropdown menus for "State", "District", "Sub-District", and "Village", each with a "Select" label. Below these is a text input field for "Khasra Number" with a placeholder "Enter Khasra Number". A blue "Submit" button is at the bottom of the form. The browser's address bar shows "landregdept.gov.in/form/query/history" and a "Logout" button is visible in the top right corner.

Figure 12: Query Land Ownership History

3.2 Smartphone Application

This application is used to interact with LRSP Server and provide a user friendly mechanism for the users to request land ownership history records. The application is built using React Native which is a JavaScript library that is used to build cross-platform applications using a single React code base i.e. we can build both Android and iOS application using the same code base.

3.2.1 Sequence Flow

Initially the user have to login to the application using a email and password, if they are new to the platform they can register a new account as seen in the Figure 15.

After successful authentication the user is redirected to a screen as shown in Figure 16 where they can request the land ownership history of a land parcel by placing the marker anywhere in the land area and pressing Submit button. The

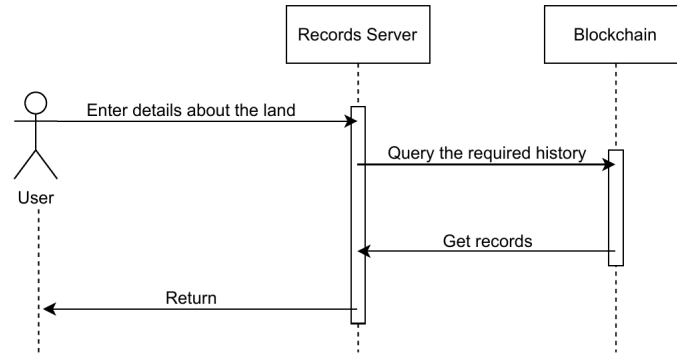


Figure 13: Sequence diagram for querying land ownership history

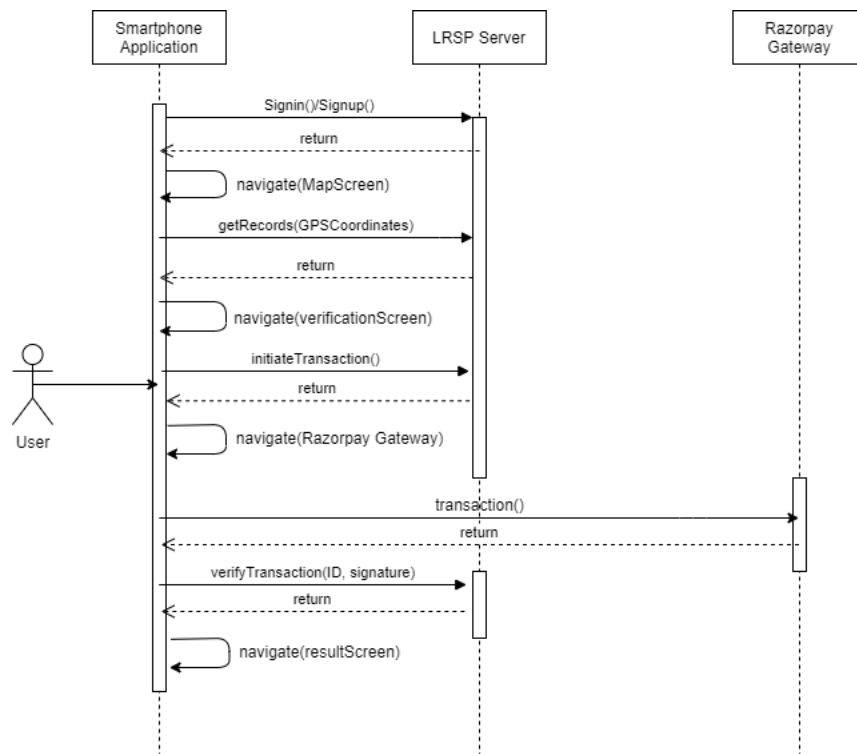


Figure 14: Sequence diagram for smartphone application

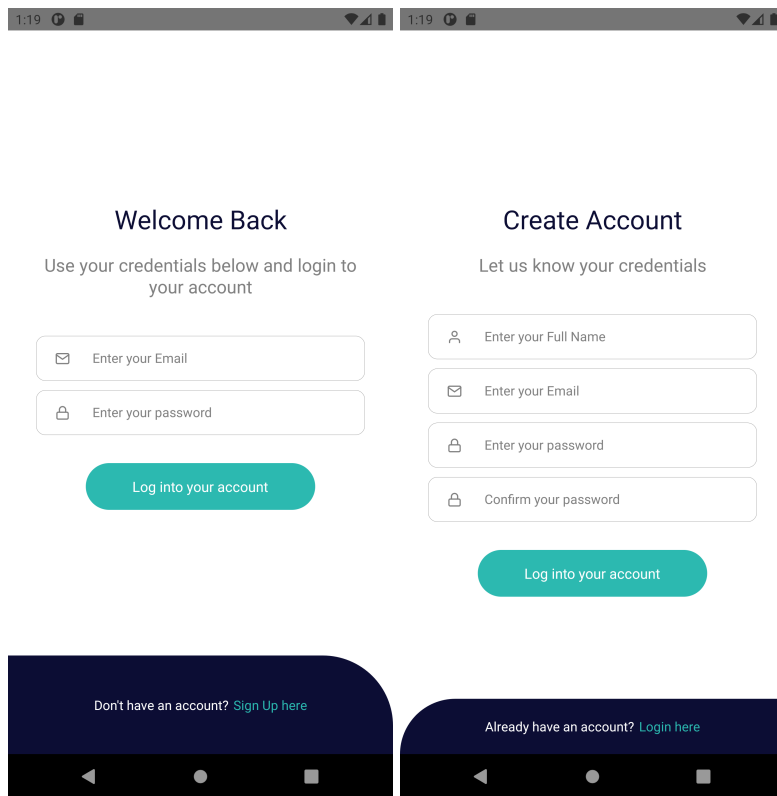


Figure 15: Login and Signup Screen

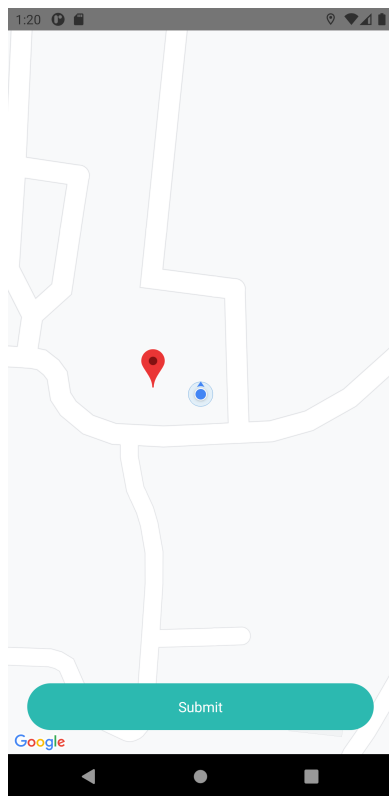


Figure 16: Request Screen



Figure 17: Confirmation Screen

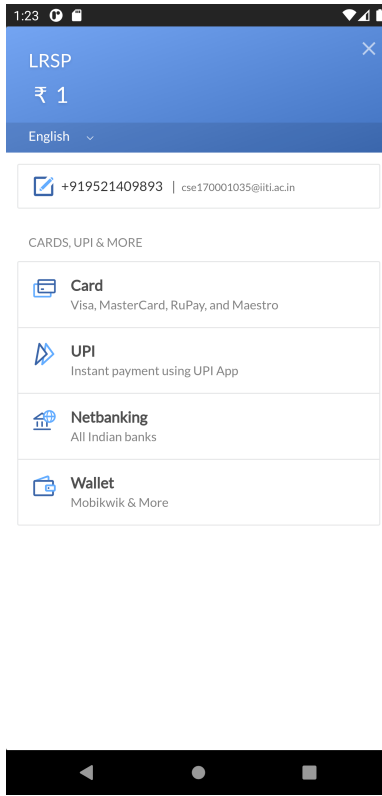


Figure 18: Payment Screen

app then makes a GET request to the LRSP server's /landrecord endpoint with the marked GPS coordinates as the parameters and in response receives the data for the land parcel which then displayed in a confirmation screen (Figure 17) where user confirms if the data fetched is for the correct land parcel and if so proceeds with payment by pressing on the Continue with Payment button. By pressing on the button the user initiates a transaction with the payment gateway i.e Razorpay gateway and is redirected to the said gateway as shown in Figure 18. If the transaction is completed successfully then the Payment ID and Payment Signature of the transaction are sent to the LRSP server via a GET request to the /payment/verify endpoint for verification. If the transaction is successfully verified then the app redirects to a Success screen (Figure 19) and the ownership history report of that land parcel is emailed to the user. If the payment transaction fails for any reason then an failure screen (Figure 20) is displayed prompting the user to redo the process.

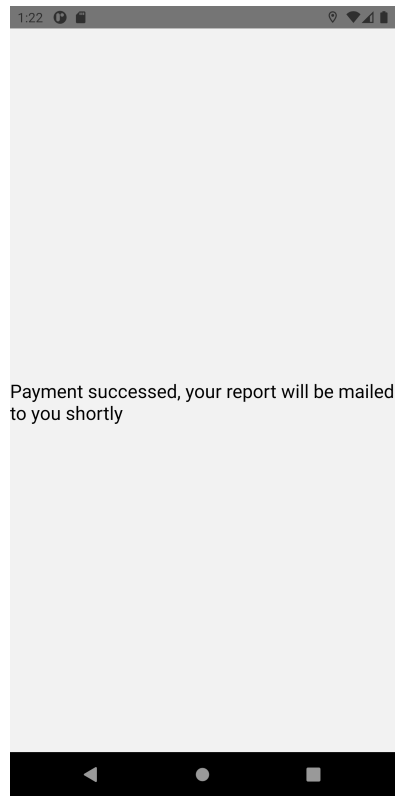


Figure 19: Payment Success Screen

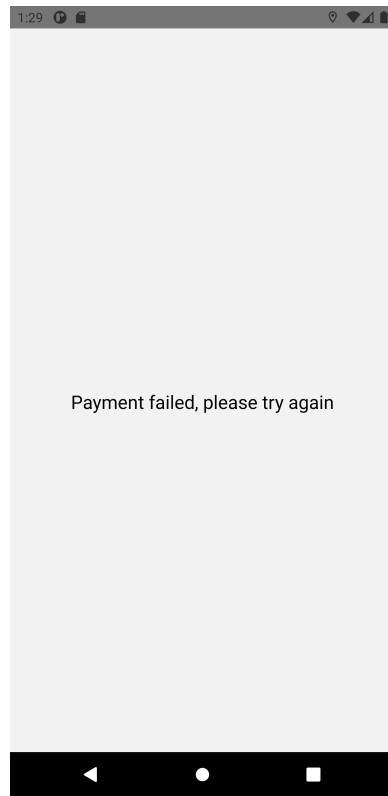


Figure 20: Payment Failure Screen

3.3 LRSP Server

It is a Node server that interacts with the smartphone application to provide the requested land record to the user. It acts as an intermediary between the LRSP smartphone application and the Blockchain network. The application sends GPS coordinates to the LRSP server requesting for the land record. The server resolves it and fetches the corresponding land record information from the Blockchain. The land record is mailed to the user once the user completes the payment. It supports HTTPS for secured interaction.

The server also provides user authentication functionality to the LRSP system. It uses a centralized database to register users with the system. It uses JWT-based stateless authentication to allow access to protected routes.

LRSP server is implemented using Express framework, a NodeJS module.

3.3.1 Sequence Flow

The server resolves the GPS coordinates obtained from the application to get the corresponding State, District, Sub-District and Village information. This is accomplished by using an external Reverse Geocoding service. The server interacts with the Blockchain network to fetch the corresponding record. The records are queried at village, sub-district and district levels in order. Once the record is found, the PDF is generated and mailed to the user after payment is verified. The generated PDF contains the hash IDs of the certificates stored on IPFS. To validate the land record, the user can request for these certificates from the verification server.

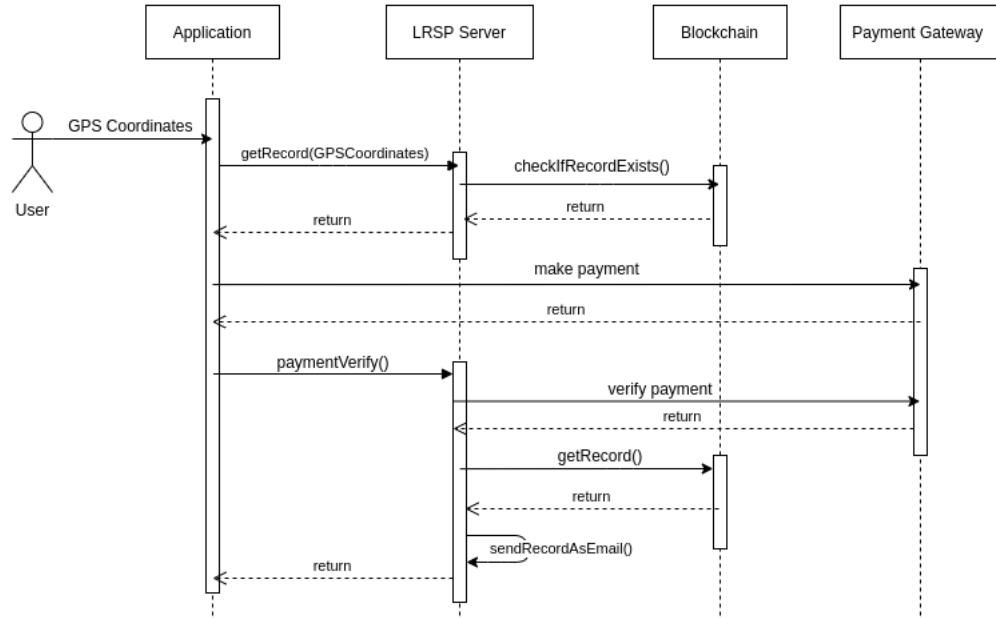


Figure 21: LRSP server sequence diagram

3.3.2 Usage

Following are the web endpoints exposed by the LRSP server:

- **POST** /signup:

This endpoint is used to register a new user to the LRSP server. If successful, it returns the jwt access token in the response body. The jwt token expires in 1 hour.

Request Paramaters:

- name: user name
- email: user email address
- password: user password

Success Response:

```
{
  "success": "true"
  "token": <jwt_token>
}
```

- **POST** /login:

This endpoint is used to get the jwt access token to access protected endpoints. The jwt token expires in 1 hour.

Request Paramaters:

- email: user email address
- password: user password

Success Response:

```
{
  "success": true
  "token": <jwt_token>
}
```

- **GET** /landrecord

This endpoint is used to get the land information corresponding to a particular GPS coordinates that includes khasra no, subdistrict, district, state and vertex points of land boundary.

Require Authentication: True

Request Parameters:

- lat: GPS coordinate latitude
- lon: GPS coordinate longitude

Success Response:

```

{
  "success": true,
  "data": {
    "khasra": "1",
    "village": "abu said",
    "subDistrict": "ajnala",
    "district": "amritsar",
    "state": "punjab",
    "points": [
      {
        "lat": "31.894083",
        "lon": "74.834157"
      },
      {
        "lat": "31.894229",
        "lon": "74.835573"
      },
      {
        "lat": "31.892662",
        "lon": "74.835723"
      },
      {
        "lat": "31.892708",
        "lon": "74.833642"
      }
    ]
  }
}

```

- **GET** /payment/initiate

This endpoint is used to initiate a payment request to obtain the requested land record.

Require Authentication: True

Request Parameters:

- khasraNo: khasra no of land
- village: Village name corresponding to land.
- subDistrict: Sub-District name corresponding to land
- district: District name corresponding to land
- state: State name corresponding to land

Success Response:

```
{
  "order_id": 1234
  "amount": 100
}
```

- **GET** /payment/verify

This endpoint is used to submit details about the successful transaction to the server for verification.

Require Authentication: True

Request Parameters:

- order_id:
- razorpay_order_id:
- razorpay_payment_id:
- razorpay_signature:

Success Response:

```
{
  "success": true,
}
```

3.4 Verification Server

The verification server provides a portal to obtain the PDF certificates issued by Land Registration Department. The certificates are digitally signed by the respective authorities and contains information regarding land records and transactions. These certificates provide a proof for land ownership and transactions and can be used for validation purposes.

Verification server is implemented as a Node server using ExpressJS.

3.4.1 Types of Certificates

Land Registration Department issues two types of certificates:

- *Land Ownership Certificate* :- This certificate is issued corresponding to each land parcel and provides the ownership detail of a land.
- *Land Transaction Certificate* :- This certificate is issued for each land transaction and provides the land transaction details such as information about previous and new owner, sale price, etc.

3.4.2 Sequence Flow

The sequence flow of verification server comprises of the following steps:

1. Get input from the user which includes IPFS hash of the certificate and record details.
2. Fetch the corresponding record from the Blockchain network.
3. Validate the provided certificate IPFS hash against the one associated with the record in the Blockchain.
4. If certificate hashes matched, fetch the stored certificate from IPFS.
5. Add digital signature to certificate with timestamp and send it to user.

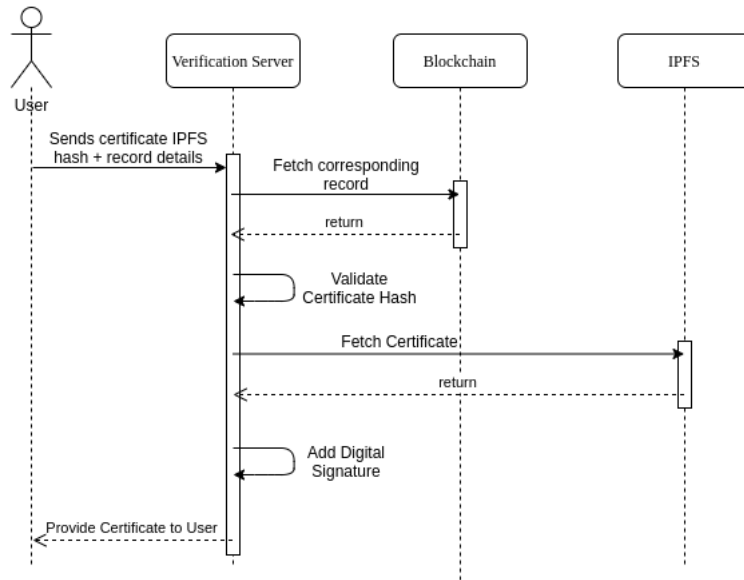


Figure 22: Verification server sequence diagram

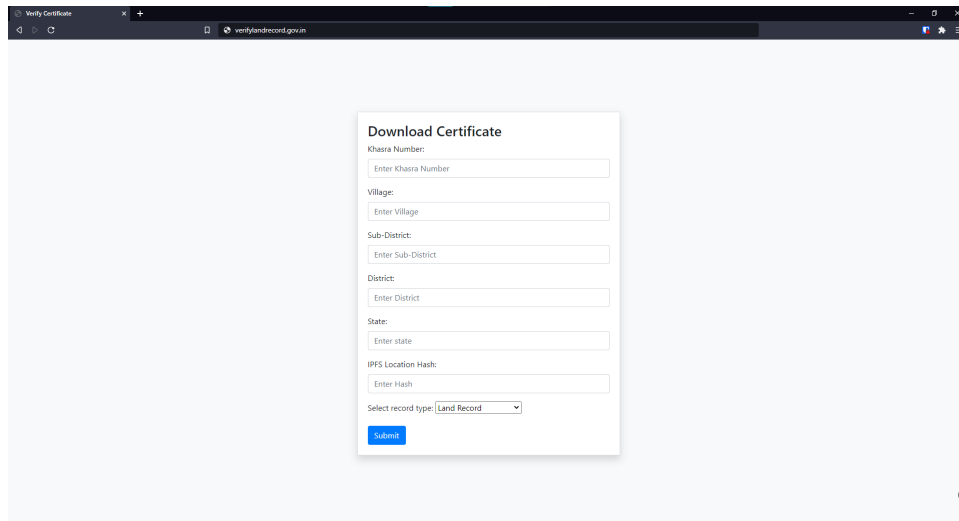


Figure 23: Home Page

3.5 Blockchain

All land records and land transfer information is stored on blockchain. Blockchain is implemented using Hyperledger Fabric.

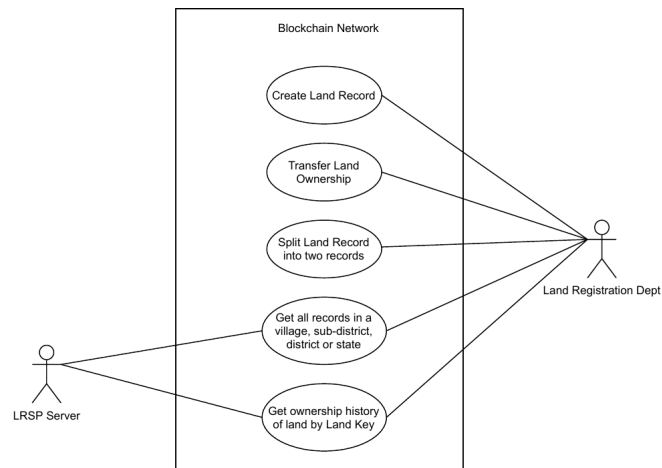


Figure 24: Use Case diagram for blockchain

Figure 24 shows the various use cases supported by the blockchain. These are implemented by writing smart contracts for each of the five operations shown.

3.5.1 Data Format

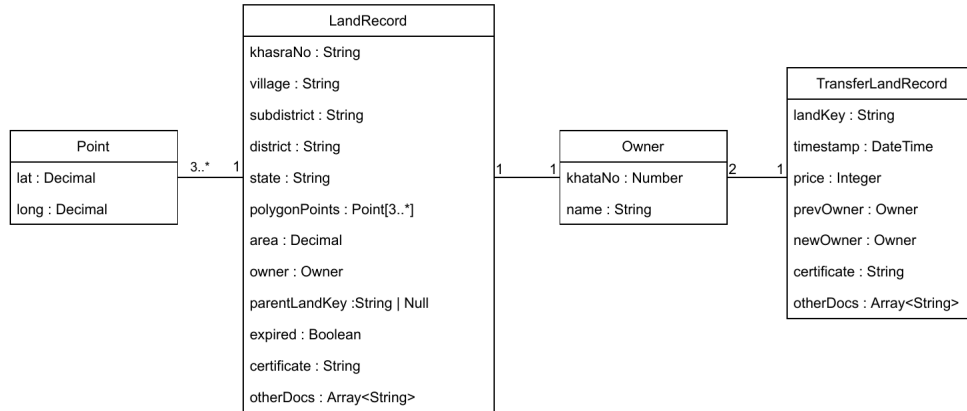


Figure 25: Blockchain Data Format

Point stores coordinates of a particular point and has the following fields :-

- **lat** - Latitude
- **lon** - Longitude

Owner stores details about a land owner and has the following fields :-

- **khataNo** - Khata Number
- **name** - Name of Owner

LandRecord stores details about a particular land. Each land record is uniquely identified by a land key which is constructed as :- *state:district:subdistrict:village:khasraNo*. Following fields are present in a LandRecord :-

- **khasraNo** - Khasra Number
- **village** - Name of the Village
- **subdistrict** - Name of the Sub-District
- **district** - Name of the District
- **state** - Name of the State

- **polygonPoints** - Coordinates of the vertices of the land polygon
- **area** - Area of land parcel in sq m
- **owner** - Current land owner
- **parentLandKey** - In case the land record is formed after splitting from another land, this stores the land key of the land from which this record was created
- **expired** - Boolean to store whether the record is expired or not
- **certificate** - CID of the certificate file stored in IPFS
- **otherDocs** - Array of CIDs of the files uploaded to IPFS with the land record

TransferLandRecord stores details about a particular land transfer and has the following fields :-

- **landKey** - Land key of the land to which this transfer record belongs
- **timestamp** - UNIX timestamp of the transaction
- **price** - Selling Price of land in Rupees
- **prevOwner** - Seller of the land
- **newOwner** - Buyer of the land
- **certificate** - CID of the certificate file stored in IPFS
- **otherDocs** - Array of CIDs of the files uploaded to IPFS with the land transfer record

3.5.2 Create Land Record

Creating a land record entails :-

1. Check if land already exists for given Khasra Number, Village, Sub-District, District and State. If yes, throw error.
2. Create LandRecord data structure with the information provided and store it on the blockchain.

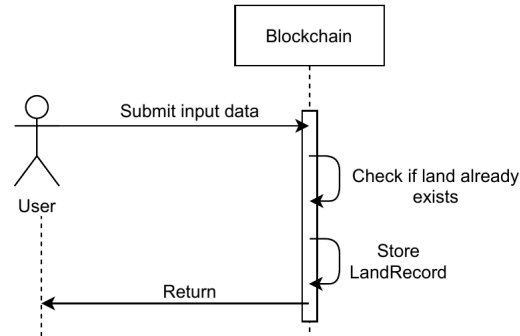


Figure 26: Sequence Diagram for Creating a land record

3.5.3 Transfer Land Ownership

Transferring land ownership entails :-

1. Get land record stored on blockchain for given Khasra Number, Village, Sub-District, District and State.
2. Check if land record is expired. If yes, throw error.
3. Check if land's current owner is same as land seller. If no, throw error.
4. Update LandRecord data structure with new owner details and store it on the blockchain.
5. Create TransferLandRecord with the information provided and store it on the blockchain.

3.5.4 Split Land Record into Two Records

Splitting a land record into two records entails :-

1. Get land record stored on blockchain for given Khasra Number, Village, Sub-District, District and State for the land record which will be splitted.
2. Check if that land record is expired. If yes, throw error.
3. Mark the land record as expired.
4. Create two new LandRecord data structures with the information provided.
5. Update original land record and add the two new records on the blockchain.

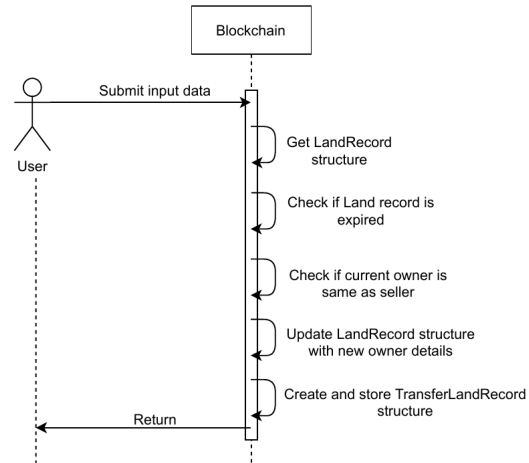


Figure 27: Sequence Diagram for Transferring Land Ownership

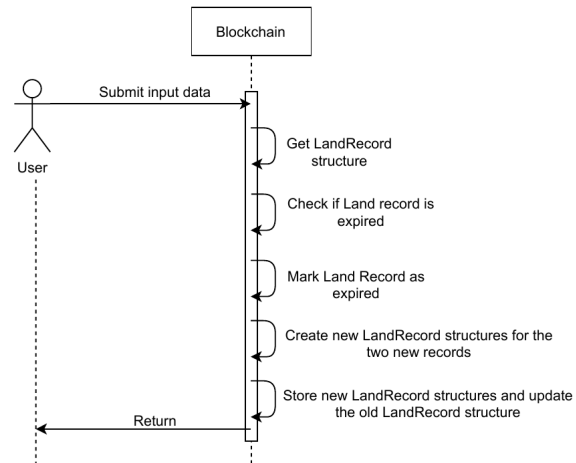


Figure 28: Sequence Diagram for Splitting a land record

3.5.5 Get all records in a village/sub-district/district/state

Getting all records in a village/sub-district/district/state entails :-

1. Get records from blockchain with the information provided.
2. Return the records.

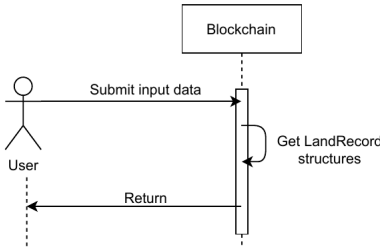


Figure 29: Sequence Diagram for Getting all records in a village/sub-district/district/state

3.5.6 Get ownership history of a land

Getting ownership history of a land entails :-

1. Get land record stored on blockchain for given Khasra Number, Village, Sub-District, District and State. If record does not exist, throw error.
2. Get all TransferLandRecord data structures stored on blockchain for the given record.
3. If parentLandKey field of LandRecord is not empty, Get all TransferLandRecord data structures stored on blockchain for the parent land.
4. Repeat the above steps for each parent land till a LandRecord is reached which does not have a parentLandKey field.

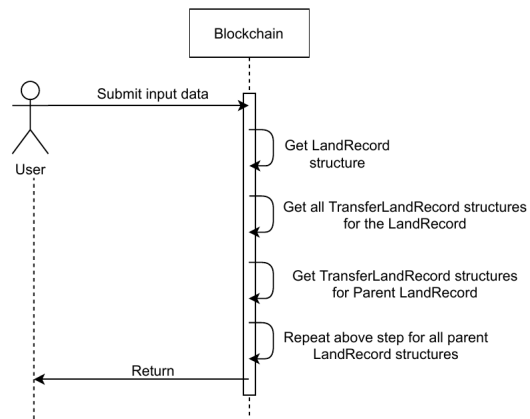


Figure 30: Sequence Diagram for Getting ownership history of a land

4 Chapter 4

4.1 Records Server

Records server is implemented using NodeJs module Express. It is written in typescript and needs to be transpiled.

Records server requires the following environment variables :-

- **CERT** :- Path to P12 certificate file used to sign the PDF documents (certificates)
- **IPFS_CLUSTER** :- Link to IPFS cluster node

```
1      # Install required NodeJs modules
2      npm install
3
4      # Transpile
5      npm run build
6
7      # Start server
8      CERT=<cert_path> IPFS_CLUSTER=<ipfs_cluster_link> node dist
9      /app.js
```

Listing 1: Records Server

4.2 Verification Server

Verification server is implemented using NodeJs module Express. It is written in typescript and needs to be transpiled.

Verification server requires the following environment variables :-

- **CERT** :- Path to P12 certificate file used to sign the PDF documents (certificates)

```
1      # Install required NodeJs modules
2      npm install
3
4      # Transpile
5      npm run build
6
7      # Start server
8      CERT=<cert_path> node dist/app.js
9
```

Listing 2: Verification Server

4.3 LRSP Server

LRSP server is implemented using NodeJs module Express. It is written in typescript and needs to be transpiled.

LRSP server uses the following external services :-

- **MongoDb :-** A running MongoDB instance is required for user authentication purposes. Provide the URI to the MongoDB database in the file *src/setup/db.ts*. To set up a MongoDB instance locally, follow [this](#).
- **Reverse Geocoding Service :-** The server is using **MapMyIndia** Reverse geocoding service. Provide the MapMyIndia API Key in the file *src/services/coordResolver.ts*
- **RazorPay Payment Integration :-** RazorPay Payment service is used to initiate and verify the payment.

LRSP server requires the following environment variables :-

- **RZRPAY_KEY_ID**
- **RZRPAY_KEY_SECRET**

```
1      # Install required NodeJs modules
2      npm install
3
4      # Transpile
5      npm run build
6
7      # Start server
8      RZRPAY_KEY_ID=<razorpay_key_id> RZRPAY_KEY_SECRET=<
9      razorpay_key_secret> node dist/main.js
```

Listing 3: LRSP Server

4.4 Smartphone Application

The smartphone application is built using React Native a NodeJS module, it is written in Typescript. To build Android APK, Linux, Windows and macOS are the supported development OS but to build iOS IPA only macOS is supported.

4.4.1 Android

To build Android APK, Android Studio is required with the following installed along with it :-

- Android 10 (Q) SDK
- Android SDK Platform 29

- Android Virtual Device
- If not already using Hyper-V: Performance (Intel ® HAXM)

After successful installation of Android Studio the following environment variable needs to be set :-

- **ANDROID_HOME** to the Android SDK install location

4.4.2 iOS

To build iOS IPA, version 10 or newer of Xcode is required which can be installed from the Mac App Store and after installation, Xcode Command Line Tools needs to be installed from the Xcode Preferences tab. Along with Xcode, CocoaPods needs to be installed which is a dependency manager for Swift and Objective-C Cocoa projects. It can be installed using the command mentioned in Listing 4.

```
1      # Install cocoapods
2      sudo gem install cocoapods
3
```

Listing 4: Cocoapods installation

```
1      # Install required NodeJS modules
2      npm install
3
4      # Start Metro Bundler
5      npx react-native start
6
7      # Build and run Android debug apk
8      npx react-native run-android
9
10     # Build and run iOS debug apk
11     cd ios; pod install; cd ..; npx react-native run-ios
12
13     # Build Android release apk
14     cd android; ./gradlew assembleRelease
15
```

Listing 5: Smartphone Application

To publish the Android APK to the Play Store, a Google Developer account is required. After building a release APK the same can be uploaded on the Play Store Console from where it is published on the Play Store.

To build a release version of the app for iOS, an Apple developer account is required. After signing in using the developer account in the Xcode, a build button is available which builds a release IPA for iOS and pushes it to App Store Connect where the IPA is inspected by Apple for any guideline violation. Upon successful inspection, the app can be published to the App Store using the App Store Connect Console.

4.5 IPFS

A private IPFS network is set up. IPFS-Cluster is used to manage the cluster. This requires two environment variables to be provided :-

- **SWARM_KEY** :- Required for private ipfs network, can be generated by following point 2 in this [link](#).
- **CLUSTER_SECRET** :- Required to manage the private IPFS cluster

These can be provided in a .env file in the same directory as the docker-compose.yml file. Make sure that the init.sh file can be executed.

```
1      # Modify init.sh file permissions to allow execution
2      chmod 740 init.sh
3
4      # In local development environment, network can be started
5      by using the command:-
6      docker-compose up
```

Listing 6: IPFS

4.6 Blockchain

Smart contract and applications that interact with blockchain run on the test net using the commercial paper [example](#) replacing the smart contract and applications with our implementations.

One can follow the tutorial in the example linked and replace the smart contract with the implementation on the github repo for our project.

LRSP server run as organization 1(digibank) application.

Verification Server and **Records Server** run as organization 2(magnetocorp) application.

5 Chapter Five

5.1 Conclusion

Traditional land record retrieval system had many shortcomings as discussed in Chapter one. To address these shortcomings, we proposed a Blockchain based solution. The proposed solution takes into account various features of Blockchain technology like immutability, security, transparency, etc. to overcome the shortcomings present in traditional land record retrieval system. The Blockchain based solution makes it convenient to reconcile and synchronized data across various government departments, thus eliminating discrepancies in data. The proposed solution facilitates the retrieval and verification of ownership history of land parcel and associated documents digitally. To validate the integrity of land record, the user can request for a digitally signed certificate from the Verification portal as a proof of trust. This eliminates the need of cumbersome processes and delays that exist in the current system to verify land ownership of a land parcel. The Blockchain based solution, being immutable and transparent, makes the land data tamper-proof. This checks the corruption that exists in government departments.

5.2 Future Work

In the proposed solution, we are using Hyperledger Fabric [13] which is a private permissioned Blockchain. This entails configuring and deploying our own distributed network infrastructure for production usage. Various components needs to be set up and configured to deploy the solution at production level. This includes certificate authorities (CA), Membership Service Providers(MSP), ordering services, peer and ordering nodes, etc. The current system has been tested on dummy data. The land information needs to be digitized and fed into the system database to test the system in real scenario. The current solution can be extended to facilitate buying and selling of land assets through smart contracts thus eliminating the need of middlemen or brokers.

References

- [1] Wikipedia.
- [2] M.T. Ozsu and P. Valduriez. *Principles of Distributed Database Systems*. Springer, New York, 3rd edition, 2011.
- [3] C. Date. *An Introduction to Database Systems. Vols. I and II*. Addison-Wesley Publishing Co., 4th edition, 1987.
- [4] Mirela Liliana Moise Nicoleta Magdalena Iacob (Ciobanu). Centralized vs. distributed databases. case study. *Academic Journal of Economic Studies*, 4:119–130, 2015.
- [5] Korth H.F. Silberschatz, A. and S. Sudarshan. *Database System Concepts*. McGraw-Hill, 6th edition, 2010.
- [6] Juan Benet. Ipfs - content addressed, versioned, p2p file system. 07 2014.
- [7] Klaus Wehrle, Stefan Götz, and Simon Rieche. 7. distributed hash tables. volume 3485, pages 79–93, 01 2005.
- [8] Department of land resources.
- [9] Centre of excellence in blockchain technology.
- [10] Vinay Thakur, M.N. Doja, Yogesh K. Dwivedi, Tanvir Ahmad, and Ganesh Khadanga. Land records on blockchain for implementation of land titling in india. *International Journal of Information Management*, 52:101940, 2020.
- [11] Christopher Mellon J. Michael Graglia. Blockchain and property in 2018: At the end of the beginning. 2018.
- [12] Emma Sahlin and Rebecka Levenby. Blockchain in audit trails : An investigation of how blockchain can help auditors to implement audit trails. 2018.
- [13] Elli Androulaki, Artem Barger, Vita Bortnikov, Christian Cachin, Konstantinos Christidis, Angelo Caro, David Enyeart, Christopher Ferris, Genady Laventman, Yacov Manevich, Srinivasan Muralidharan, Chet Murthy, Binh Nguyen, Manish Sethi, Gari Singh, Keith Smith, Alessandro Sorniotti, Chrysoula Stathakopoulou, Marko Vukolic, and Jason Yellick. Hyperledger fabric: A distributed operating system for permissioned blockchains. 01 2018.