MIJST
MIST International Journal of Science and Technology

Decentralized LRM System Architecture with Biometric Authentication and Digital Certificate Verification through Blockchain Technology

Shakil Mosharrof[1], Farhan Nasif Nizami[1], Mahdi Mohtasim[1], Mahdi Adib[1], M. Akhtaruzzaman[*2], Md Shofiqul Islam[3], Muhammad Towfiqur Rahman[4], and Hosney Jahan[5]

[1]Department of Computer Science and Engineering, Military Institute of Science and Technology, Dhaka, Bangladesh
[2]Department of Computer Science and Engineering, Daffodil International University, Savar, Dhake-1216, Bangladesh
[3]Institute for Intelligent Systems Research and Innovation (IISRI), Deakin University, Warun Ponds, Victoria, Australia
[4]Department of Computer Science and Engineering, University of Asia Pacific (UAP), Dhaka, Bangladesh
[5]Department of Computer Science and Engineering, East West University, Aftabnagar, Dhaka-1212, Bangladesh

***Corresponding Email:** *akhtaruzzaman.cse@diu.edu.bd*

ARTICLE INFO

Article History:

Received: 11th April 2025
Revised: 29th October 2025
Accepted: 03rd November 2025
Published: 30th December 2025

Keywords:

Blockchain-based LRM,
Land record management,
Ethereum,
Biometric,
Fingerprint authentication,
Smart-contracts,
Decentralized architecture

ABSTRACT

Managing land records is a fundamental duty of a government, ensuring the accuracy, consistency, integrity of ownership, and reliable transaction of data. Conventional paper-based or centralized digital technology-based land record systems are unable to hold the system trust, efficiency, and consistency, thus mostly demonstrate errors, fraud, and corruptions. On the other hand, blockchain technology presents a transformative solution. It offers transparent, tamper-proof, secure, and reliable approach for Land Record Management (LRM) system. In this study a blockchain-driven LRM system architecture with distributed ledger technology is presented. The proposed strategy enhances security and trust by ensuring transparency, acceptance, and accountability. The study also designs the smart-contracts algorithm in detail that facilitates land registration, ownership transfers, verification, and streamlining processes. The proposed architecture ensures automated functionalities with little human intervention, uplifting the system security. Moreover, the proposed blockchain architecture integrates finger-print biometric authentication that boosts the system strength in terms of security through identity verification. This mitigates the risks of errors, fraud, illegal modification, and unauthorized access. This article outlines a blockchain-based LRM framework and verified through implementation and testing, reflecting the potentiality of viable adoption of this advanced technology.

1. INTRODUCTION

Land ownership records and registry are one of the common and essential activities for a society. Traditional centralized land registry and management is mostly overwhelmed with opaqueness, inefficiency, unauthorized transactions, and identity falsification, which often result in property disputes, financial losses, erosion of property rights, and sometimes life threatens. Such consequences not only affect legitimate landowners, but also exacerbates socio-economic inequalities. To address these issues, modern technology-based well-architecture system is undoubtedly essential to ensure a secure, transparent, equitable, and reliable conduction of these important activities.

Promising solution to the structural and functional insufficiencies of the existing LRM system can be proposed through decentralized networks (*Hasan, Alam, and Tanha, 2022*). Blockchain technology has the decentralized and unalterable nature and sufficient to ensure the secure, transparent, trustworthy management of land documents and records (*Beuria et al., 2020; Singh et al., 2020*). Cryptographic validation of the technology ensures the integrity of record transactions, resistant to fraudulent and unauthorized access (*Bouraga, 2025*). Moreover, the smart-contract algorithm of the blockchain network ensures seamless functionalities of land registry workflow, automating traditional processes of deed authentication, transferring title, performing registration, etc. (*Nandi et al., 2020*). The integration of biometric authentication; for example, finger-print verification, facial recognition, iris scans, etc.; in the blockchain-based distributed LRM boosts and reinforces the trust in managing property transactions (*Aquib et al., 2020*). Traditional verification is vulnerable to manipulation (*Khan et al., 2020*), while biometric authentication-based decentralized immutable architecture of the technology ensures super secure framework for access control and transaction verification.

To enhance transparency, security, and automation in LRM process, this manuscript presents a blockchain network-based LRM system framework with detail design of smart-contracts algorithm. By conducting a comprehensive analysis, the study identifies existing gaps and key challenges that leads to inefficiencies and security vulnerabilities in the traditional land registry models. The key contribution of this study is to propose a decentralized LRM system architectural workflow encapsulating cryptographic security, smart-contracts algorithm, consensus mechanisms, and fingerprint based biometric authentication within a decentralized network of blockchain technology. The study also implements the proposed architecture and examines the prototype through testing and result analysis, reflecting a resilient, tamper-proof, and efficient LRM system. Advanced registration, reliable owner transfer, immutable audit, and robust access control are the significant features of the proposed framework.

2. RELATED WORKS

Now a days, blockchain applications are lingering beyond the digital currencies with smart-contract enabled systems influencing various domains including the LRM. Among several attempts over the last decade, Bangladesh launched the first digital LRM system in 2011 as a pilot project (*Hasan, Alam, and Tanha, 2022*). Even with some advancements, the project is still not mature enough to be a completely successful digitization endeavor. While online application submissions continue to be the major method of digital contact, current initiatives are mostly focused on digitizing archive materials, like Manchitra (maps), Khatiyan (ledger), and daag number (serial number) (*Hasan, Alam, and Tanha, 2022*). A double layer hybrid blockchain structure was also proposed in the country where Ethereum smart-contacts was incorporated to improve transparency, synchronization, and accessibility in land record management. A study conducted by Beuria et al. (*Beuria et al., 2020*) highlighted the decentralized architecture of blockchain network. The study emphasized the role of distributed automated ledger mechanism to record the transactions across multiple nodes to confirm any changes with permission from all the dependent blocks. The integrity and security of land register systems are reinforced by this unalterable structure.

Various approaches including formal verification, runtime monitoring, static analysis, etc. were explored in a study conducted by Singh et al. (*Singh et al., 2020*). The authors tried to improve contract reliability by formulating the blockchain smart-contracts to overcome the security vulnerabilities. Key challenges like scalability, correctness, and the evolving nature of the blockchain network were also emphasized in this study with some important directions like interdisciplinary research in developing a robust and secured framework for smart-contracts.

Another study by Nandi et al. *(Nandi et al., 2020)* analyzed the uses of Ethereum in blockchain-based systems, demonstrating its relatively low transaction processing time, making it viable for real-life applications. The research also highlighted the vulnerabilities of traditional database systems in maintaining records, highlighting their susceptibility to security breaches. Additionally, the study found that implementing blockchain would cost individuals only \$0.36 per transaction, which is about thousand times less than the cost of the conventional system in India. However, the fluctuating nature of Ethereum gas fees shows uncertainty in transaction costs, posing a challenge to the consistent pricing.

Aquib et al. (2020) proposed three key stakeholders, the Registrar Department, the Revenue Department, and National Database and Registration Authority (NADRA), to collect data from both buyers and sellers and submit it to the blockchain system, creating an immutable ledger that cannot be modified or altered without authorization. The study suggested a private blockchain architecture for LRM in Pakistan to address the limitations of existing systems. Integration of the registrar, revenue, and national ID departments was the aim of the proposed system to modernize the workflows. To demonstrate the system feasibility, the prototype was implemented on Hyperledger. However, the study failed to address the challenges of scalability and viability of practical adoption. Another recent study conducted by *Khan et al., (2020)* emphasized the advantages of blockchain technology in providing unalterable land records without proper validation and authentication. The study recommended to include cryptocurrency-based land asset liquidation features.

A certificate verification system on blockchain-based network was studied by Suganthe et al. (*Suganthe et al., 2021*) where Ethereum platform with smart-contracts was used. Pereira et al. (*2021*) also introduced similar architectural framework based on blockchain network for land administration in Bangladesh. The architecture accumulated the blockchain features with the functionalities of the Land Administration Systems (LAS) through testing based on an Ethereum prototype with smart-contracts. However, their evaluation was limited to simulations, lacking real-life adoption of the system. Sen, Mukhopadhyay, and Karforma (*2021*) presented a blockchain system for property registration that integrates government entities as peers and utilizes smart contracts for the execution of transactions. The performance evaluation was conducted on Hyperledger Fabric, focused on latency and throughput metrics. Sahai, and Pandey (*2020*) also proposed a blockchain-based framework for land registration that employed smart contracts written in Solidity to automate registration and transfer transactions. They established the process by developing a sample decentralized application called DApp.

Through the above literature studies, it is evident that a sever attempts on designing blockchain-based land registry system framework were conducted. At this stage, it is imperative to determine the gaps of the current focus in improving the advanced framework of the distributed land registry management system based on the blockchain network. A structured summary of the studied literatures is presented in Table 1.

The proposed system architecture presented in this study aims to develop a blockchain-based framework for land registry management systems that enhances transparency, trust, predictive capabilities, reliability, control, security, cost-efficiency, and ease to access. Integration of blockchain features, such as immutability, decentralization, and consensus mechanisms into land registry operations, the proposed framework ensures that all nodes maintain a consistent, verifiable record of land transactions, accessible anytime anywhere. Smart contracts automate the processes like ownership transfer and access control through multi-party authorization. Furthermore, storing historical transaction data enhances predictive analytics, while data duplication across nodes boosts the reliability of the system. The biometric verification and certificate scanning subsystem further strengthens the security, transparency, reliability, and trust. Consensus mechanisms improve control eliminating the need for third-party involvement, while encryption and multi-node storage boost security. The decentralization nature of the system facilitates quick and easy access of land records by the users. Ultimately, the goal is to create a blockchain-based system that provides significant advantages in land administration, such as increased transparency, trust, security, and efficiency.

Table 1: Finding the gaps of the studied literatures

Ref.	Objectives	Outcomes	Limitations
Hasan, Alam, and Tanha, (2022)	To implement blockchain for LRM in Bangladesh.	Prototype developed using Ethereum for transparency and accessibility.	The project has not reached full maturity.
Beuria et al., (2020)	To highlight decentralized nature of and its role in securing LRM.	Blockchain provides immutable records, improving security and integrity in land registry systems.	No direct application to LRM, focus on blockchain technical nature.
Singh et al., (2020)	To formalize blockchain smart contracts to mitigate vulnerabilities.	Explored formal verification, runtime monitoring, and static analysis to ensure contract reliability.	Challenges in scalability, correctness, and the evolving nature of blockchain.
Nandi et al., (2020)	To evaluate Ethereum for real-world blockchain applications in land records.	Low transaction processing time, making Ethereum suitable for real-world applications.	Ethereum's fluctuating gas fees introduce uncertainty in transaction costs.
Aquib et al., (2020)	To propose a private blockchain architecture for LRM in Pakistan.	Integration of departments like the Registrar, Revenue, and NADRA, using blockchain to create an immutable ledger.	Scalability and real-world adoption challenges remain unaddressed.
Khan et al., (2020)	To explore benefits of blockchain for immutable LRM	A cost-effective solution, with blockchain providing a secure and efficient LRM system.	Lack of detailed implementation or practical deployment.
Suganthe et al., (2021)	To implement a blockchain-based certificate verification system.	Ethereum-based smart contract system for secure and efficient certificate verification.	Limited to certificate verification, not directly related to land records.
Pereira et al., (2021)	To develop an architecture for land administration in Bangladesh.	Ethereum prototype tested for smart contract-based land registration and verification.	Simulated evaluation, no real-world adoption studies.
Sen, Mukhopadhyay, and Karforma, (2021)	To create a blockchain system for property registration with government.	Smart contracts for transaction execution and government entities, evaluated on Hyperledger Fabric for latency and throughput.	Limited evaluation focused on performance metrics, no real-world deployment.
Sahai, and Pandey (*2020*)	To develop a blockchain framework for LRM with smart contracts in Solidity.	A DApp demonstrated for automating registration and transfer transactions using smart contracts.	Limited scope, no real-world adoption or comprehensive evaluation beyond DApp demonstration.

3. THEORETICAL BACKGROUND

3.1 Blockchain Technology and Use Cases

Blockchain technology, a distributed ledger system, was first proposed in 2008. Its primary goal was to enhance security through decentralization of data while creating a comprehensive global index (*Jesus et al., 2018*). Each blockchain consists of multiple blocks, containing a header and a main body. The block header includes a timestamp, a random number (nonce), the current block number, the hash of the previous block, and other metadata (*Yin et al., 2018*). Moreover, the block body stores network data in the form of a Merkle tree. The conceptual diagram of Blockchain and its workflow are presented in Figure 1.

The framework of blockchain proposed by Sen, Mukhopadhyay, and Karforma (*2021*) was for property registration within e-governance systems. They highlighted the key advantages of blockchain technology, including data immutability, decentralization, and transparency, which address challenges in existing electronic property record systems, such as security risks, data integrity issues, and single points of failure. The framework leverages smart bcontracts and a permissioned blockchain network to facilitate secure and efficient property registration and information sharing among government agencies and stakeholders.

Thamrin *et al.* (*2021*) propose a Blockchain-based land certificate management system in Indonesia to address fraud, lack of transparency, and inefficiencies in the existing paper-based system. Their framework follows a three-phase approach, starting with a public blockchain, transitioning to a hybrid model, and ultimately implementing a fully integrated hybrid blockchain. They also present a detailed blueprint for developing smart contracts for the public blockchain phase using Ethereum.

Smart-contracts are independent programs embedded in a blockchain that automatically execute and enforce agreements once predefined conditions are met. By removing the need for intermediaries, they enhance security, transparency, and resistance to tampering, that ensures reliable and efficient transactions (*Buterin et al., 2014; Khan et al., 2020; Khan et al., 2021*). They facilitate network automation and the seamless transition from paper contracts to digital ones. Unlike traditional contracts, smart contracts encode agreements into codes, confirming trust through automated transactions without central oversight (*Singh et al., 2020; Singh et al., 2022*). To prevent manipulation, the blockchain network replicates the smart contracts among all nodes. In the blockchain platform, smart contracts can reduce human errors and contract disputes. Sahai, and Pandey (*2020*) demonstrated a comprehensive analysis of blockchain and smart-contract applications for property registration system in India addressing the key challenges, including lack of transparency, accountability, and delays.

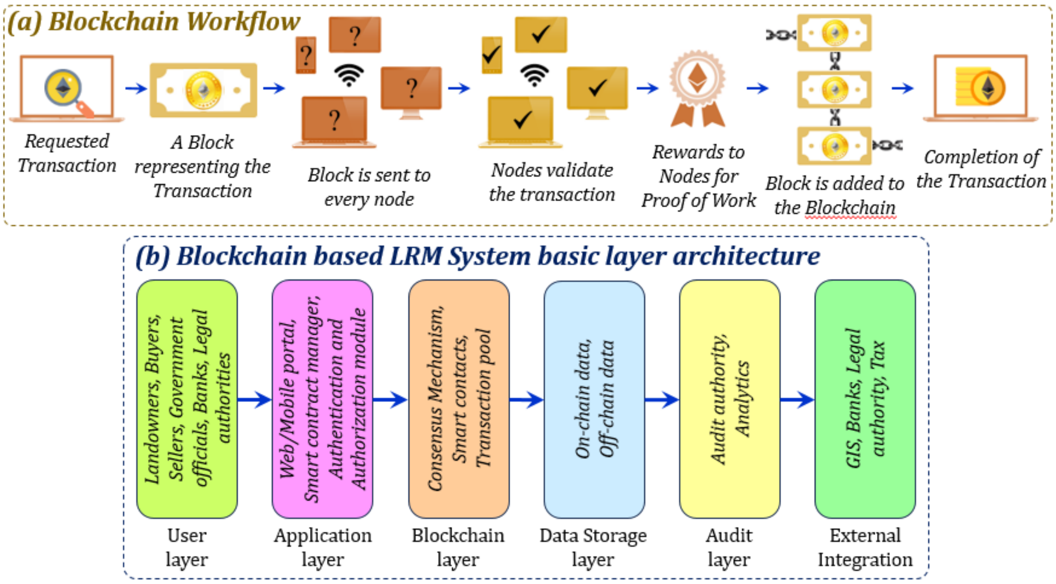


Figure 1: Conceptual architecture of Blockchain workflow and Blockchain based LRM system layers

3.2 IoT integration with blockchain network

With the ability to handle unauthorized access and privacy issues, blockchain technology can eradicate Internet of Things (IoT) security problems. The aim of the relevant research is to enhance decentralization, simplify interactions, and enable autonomous coordination among IoT devices (*Jesus et al., 2018; Kollu et al., 2022*). Furthermore, blockchain integration may be able to successfully encounter the Stalker Attack, which is recognized as one of the common dangers to any IoT setup.

Blockchain is often recognized for its effectiveness in minimizing the distributed denial of service (DDoS) attacks within the IoT networks. However, some studies have examined existing limitations of blockchain-based systems in rebutting the DDoS threats (*Beuria et al., 2020*). At the same time, some have proposed possible solutions to the security and privacy challenges in IoT interconnections integrated with blockchain technology (*Mohanta et al., 2020*). Along with privacy issues pertaining to data collection and processing in IoT applications, the study examined a number of security threats, including replay, node capture, and man-in-the-middle attacks.

Blockchain helps in developing safe and dependable IoT network especially for memory and power supply management (*Reyna et al., 2018*). At the same time, Dorri, Kanhere, and Jurdak, (*2017*) have seen some additional downsides, like resource restrictions, centralization issues, and maintaining user privacy for data exchange, of a traditional IoT network setup. The authors delineated that the decentralized nature, concealment, and security features make the system promising to overcome the challenges in IoT based systems.

3.3 Blockchain with Authentication Systems

Authentication-based systems are evolving with advancements in blockchain technology, decentralized applications, and edge computing. Padrón Núñez (*2021*) examined the legal implications of key platform components, including biometric sensors, OLED displays, and NodeMCU development kits, alongside the Ethereum blockchain, smart contracts, and IPFS. The study proposed a biometric-based work attendance tracking and logging system leveraging blockchain technology. Moreover, quantum-resistant transaction authentication mechanism can be integrated into blockchain systems to eliminate threats from quantum computing (*Yin et al., 2018; Acquah et al., 2020*). This approach employs lattice-based cryptography to improve the security of digital signatures while maintaining efficiency. In solving the tiny integer problem, the bonsai-tree technology based lightweight, non-deterministic wallets with safe proof were designed. Outcomes of the study supported the post-quantum cryptography techniques for the blockchain network architecture, ensuring long-term robustness and safety.

Fingerprint profile protection would enhance safety if the profile is encrypted and stored as a decentralized manner ensuring data integrity and immutability. This can be achieved through blockchain as the technology offers recording of encrypted template hashes. A blockchain application for e-voting system with fingerprint-based biometric authentication was studied by Ibrahim et al. (*2021*) proposing a secure voter verification system. The study reflected data integrity, transparency, access control, and data security, through a central node network-based authentication and transactions. Although, the research highlighted some challenges related to voter privacy, scalability, and some issues on security risks, it identified some strategies to overcome those challenges.

Similarly, a decentralized biometric authentication system was studied by Lee and Jeong (*2021*) where they have demonstrated that the fragmented and distributes information of biometric signature across nodes truly minimizes the breach risks. The study also examined the performance overhead and scalability, comparing with the traditional methods. The outcomes of the research ensured the viability of the approach having minimal computational impact. It also highlighted the role of the blockchain network in securing the overall system through biometric authentication.

Biometric authentication methods offer significant advantages over password-based systems by providing enhanced security and convenience (*Jain, Bolle, and Pankanti, 2006; Pournaghi et al., 2018*). When a user places their fingerprint on the scanner, an optical sensor captures a digital image, from which distinct biometric features are extracted to generate a mathematical template. This template is then compared to stored templates to verify the user identity within predefined security thresholds, ensuring reliable and accurate authentication. To verify a certificate of land ownership on the blockchain, the certificate identifier or transaction number is required. This unique identifier of the certificate can be utilized as a verification system linked to the blockchain for land records. The verification system uses the certificate ID and retrieves the corresponding blockchain record. The blockchain record includes the land information, the owner's name, date of the transaction, document hashes, and khatiyan (ledger) hashes and daag numbers (serial number assigned to each plot of land). The system checks that the record is on the distributed ledger and that the land registry authority confirms the digital signature. The certificate is authentic and unaltered. The blockchain record also includes the original land certificate hash or digital identifier. This hash can be calculated independently from the displayed certificate document and compared to the hash recorded in the blockchain. This verifies the authenticity of the certificate document. After verifying the certificate's blockchain record and document hash, the system can validate that the presented certificate accurately identifies the land parcel's proprietor based on the blockchain land records.

4. DESIGN OF THE INITIAL MODULES

There are five modules or subsystems in the blockchain based Land Record System, as shown in Figure 2. The Stakeholder Management System holds and manages the necessary information about the stakeholders like identity, ownership, etc. The Fingerprint Module ensures that the fingerprints of the users are taken for verification and validation purposes. The Scanner Module converts the land record certificates into digital form and sends to the system. The Hash Generator module generates public and private hashes to identify blocks and transactions uniquely. The Nodes Management System of blockchain ensures the retrieval of the land record information from the blockchain and shown to the users. After each transaction, the system keeps adding nodes accordingly.

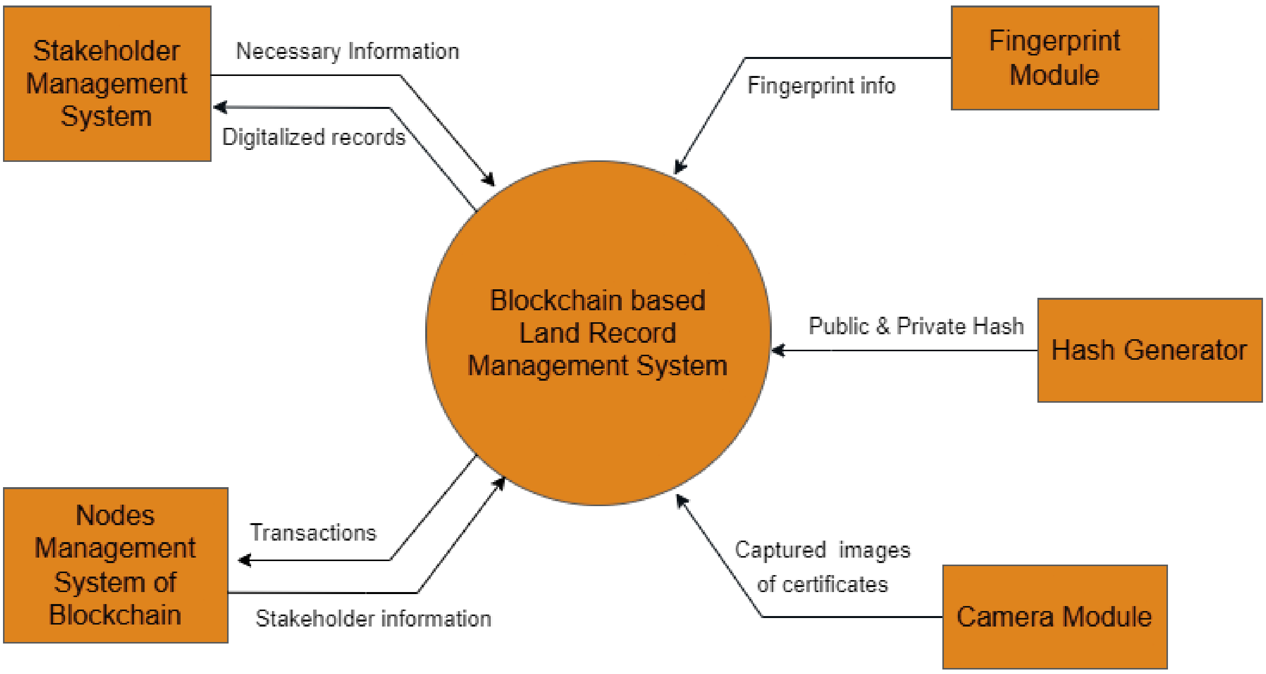


Figure 2: Five Subsystems of LRM System

The key features of the user panel are viewing and editing profiles, viewing Khatians, paying taxes, applying for tokens for land registration or ownership transfer, and viewing their transaction history. The user can sign using a valid National Identification (NID) and password if the user owns an account. Otherwise, the user needs to sign up using a valid NID through One-Time Password (OTP) verification. Then the user is able to update the basic information in the profile, apply for a new token for a new land registry or ownership transfer, pay taxes and necessary fees online, and view certificates and Khatians. The user state diagram is demonstrated in Figure 3.

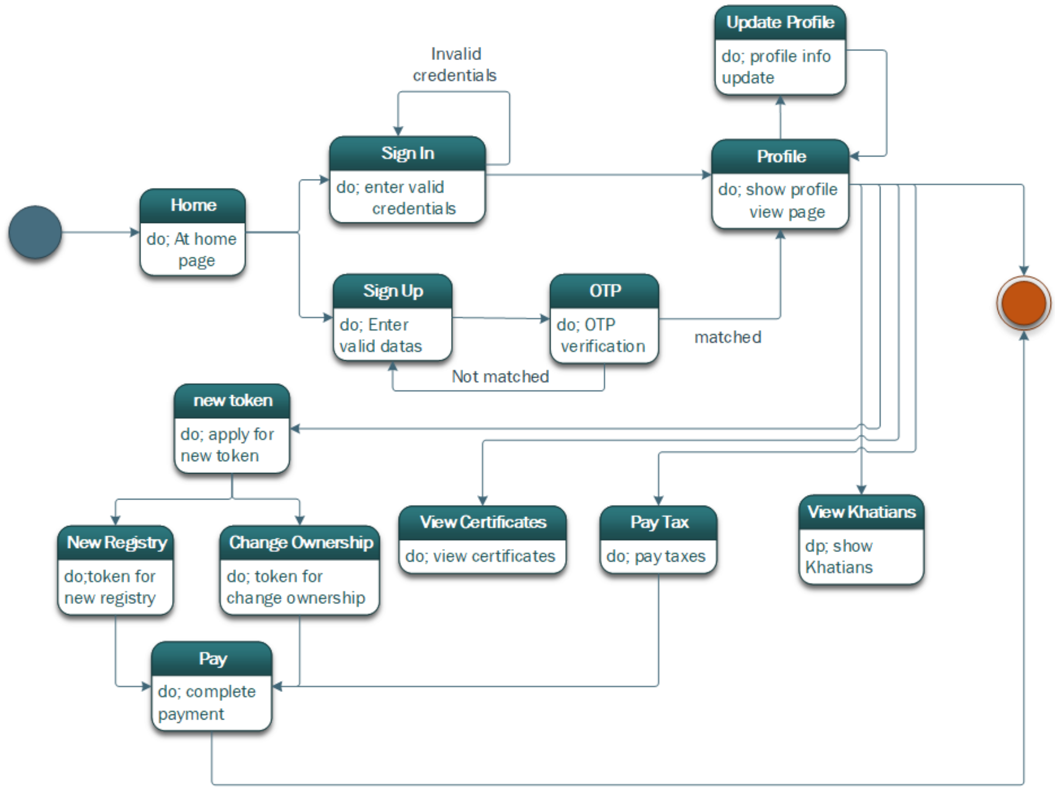


Figure 3: User State Diagram

The key features of the admin panel are verifying users through fingerprint data, uploading users' certificates, adding new Khatians, mutating previous Khatians, updating plot information, and viewing all transaction history. The admin can verify a new user by scanning his fingerprint data and saving it in the database. The certificates and the plot information are uploaded by the admin and the user is verified. The admin can perform the ownership update operation by validating all the new stakeholders, processing payment, and uploading the new Khatians. The admin can also view the history of the transactions. The admin state diagram is shown in Figure 4.

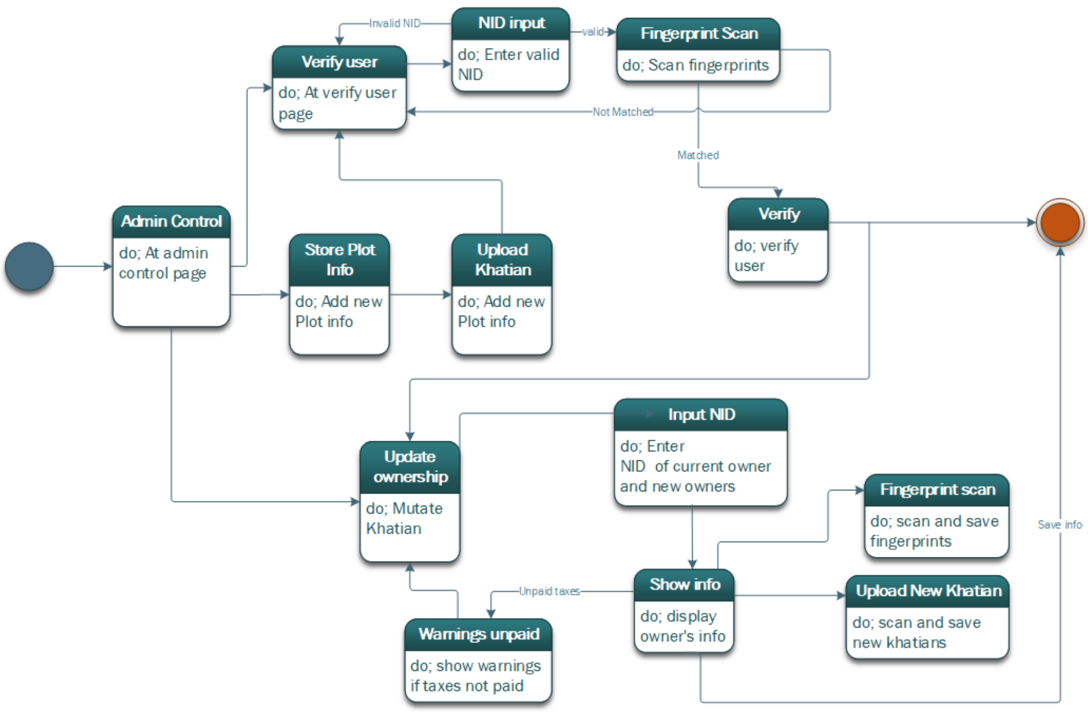


Figure 4: Admin State Diagram

The sequence diagrams of the user authentication system, fingerprint sensor, and scanner module demonstrate a detailed insight of user interactions with the authentication system, verification using fingerprint sensor, and scanning and uploading certificates. The user authentication sequence, shown in Figure 5, outlines the process of creation and authentication of a profile on the website. A user signs up and logs in with valid credentials. The system then guides them through entering additional profile information, storing it successfully, and allowing them to view their completed profile page. If login credentials are invalid, the system prompts the user to try again.

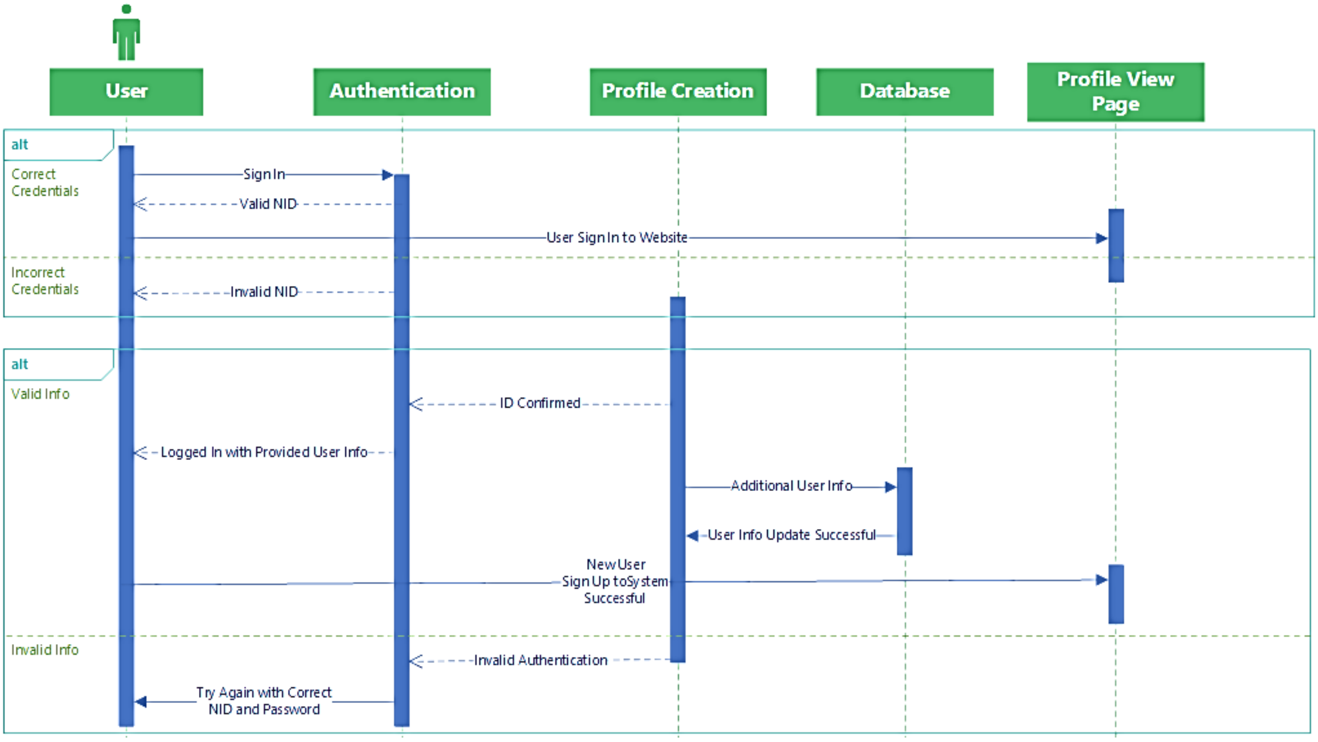


Figure 5: User Authentication Sequence

The fingerprint interaction sequence shows the enrolment process of a fingerprint. The user places their finger on the sensor twice. The sensor captures images of the fingerprint and stores them for future identification. Finally, the system returns a unique identifier associated with the enrolled fingerprint. The sequence diagram is presented in Figure 6.

The sequence diagram of the scanner module shows the process of scanning certificates and storing them into the database, potentially on a blockchain for safekeeping. The admin initiates the process through the inputs of certificates. A copy of the scanned data is uploaded to a blockchain for tamper-proof storage. The corresponding sequence diagram is depicted in Figure 7.

5. DESIGN OF THE PROPOSED ARCHITECTURE

The proposed LRM system is based on blockchain technology which is designed to handle various challenges that arise while managing the land registry and records. This proposed architecture includes various tasks, like authentic registration, reliable transfer of property ownership, production of certificates, etc. The overall architectural workflow diagram is presented in Figure 8.

Initially, landowners begin the procedures of registering their lands within the system by providing their identity and relevant information regarding ownership. Blockchain then stores the information within its distributed network system, establishing a permanent and secure data repository of land ownership.

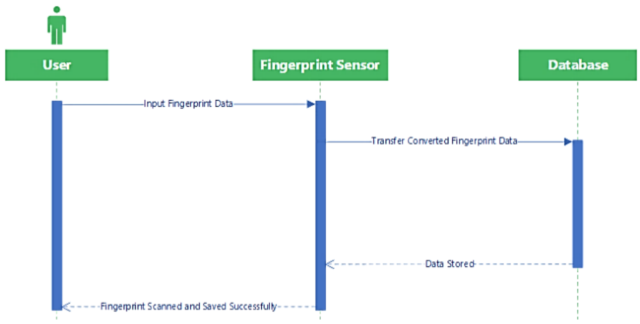


Figure 6: Fingerprint Sensor Interaction

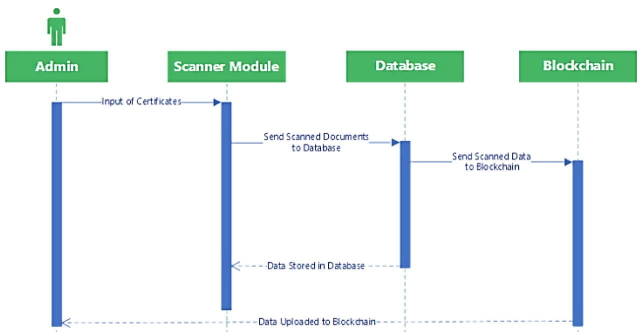


Figure 7: Scanner Module Interaction

During the ownership transfer process, the owners complete the registration with the submission of their identification and ownership information to the system. Subsequently, the system transfers the ownership rights of the land to the newly designated owner, simultaneously updating the nodes on the blockchain. This process establishes a secure and immutable, yet easily accessible record of the transaction, ensuring the transparency of the transfer of ownership.

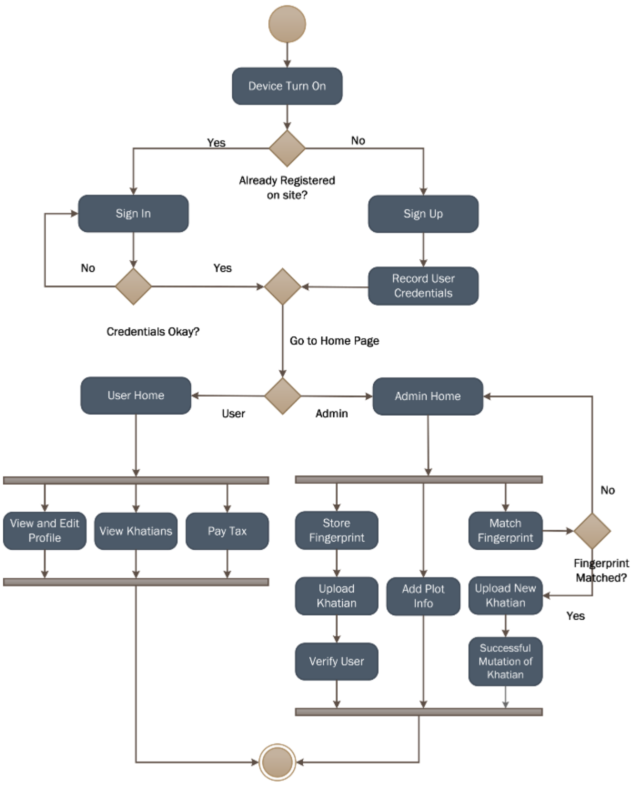


Figure 8: Overall architectural workflow of the proposed system

The system is able to produce certificates of land records and stores them securely in the blockchain node-network. Every user has permission to access these certificates. On the other hand, only the authorized users can allow and facilitate the retrieval of the records. The proposed system through the nodes of the blockchain verifies each transaction and guarantee its security and integrity.

The workflow diagram also explains the vital stages of the administration process of land records. It offers a well-defined practice for the land registration, ownership transfer, and protected storage of certificates. The proposed system offers two user options or types, general users and administrative users. The registered users without any administrative permission are considered as general users. They are able to conveniently view land certificates, transactions, and other information related to their own land records.

Access to the administrative users is restricted only to those who have the administrative access permission. These users are not only responsible for enrolling new users in the system, but also use the user ID and fingerprint for identification purposes. They are also responsible for storing and controlling data within the blockchain network as well as executing transactions as per the user requirements. Moreover, the administrator plays a key role in verifying user identity and validity while ensuring proper documentation of any changes.

6. INTEGRATION OF SYSTEM HARDWARE

Necessary hardware integration focuses on two key components, a JM-101 fingerprint reader and a LiDE-120 document scanner, which improves the system functionality and security. The fingerprint sensor confirms accurate user identification and verification by capturing fingerprints during registration and authentication. Software drivers and libraries facilitate continuous communication between the sensor and the system. The document scanner enables efficient scanning of land records and certificates. Custom software components were developed to manage scanning operations while ensuring data confidentiality and integrity. Figure 9 shows the basic hardware integration of the development and test environment setup. The JM-101 fingerprint module with Arduino-nano (*Akhtaruzzaman, 2021; Baki et al., 2023*) micro-controller is shown in Figure 10. Algorithm 1 is presenting the code-snippet of Biometric Authentication procedures.

Figure 9: Basic environment setup with necessary hardware connections

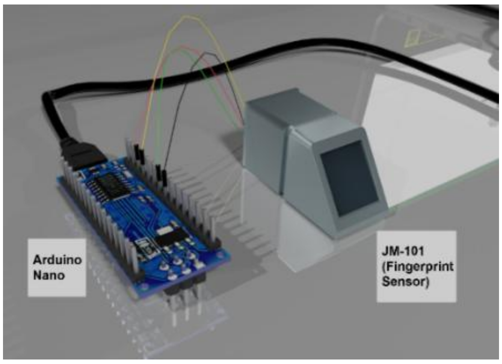


Figure 10: JM-101 Fingerprint Module integrated with Arduino-nano

Algorithm 1: Biometric Authentication

```
getFingerprintEnroll( ):
//Create an object of Adafruit Fingerprint
finger ← Adafruit Fingerprint(&mySerial)
// Give Fingerprint 1st time...
temp ← -1
while temp != FINGERPRINT_OK do
        temp ← finger.getImage()
end while
finger.image2Tz(1)
// Remove Finger...
temp ← 0
while temp != FINGERPRINT_NOFINGER do
```

```
        temp ← finger.getImage()
end while
// Give Fingerprint 2nd time...
temp ← -1
while temp != FINGERPRINT_OK do
        temp ← finger.getImage()
        finger.image2Tz(2)
end while
// Create and Store Model and return ID of fingerprint
finger.createModel()
finger.storeModel()
return finger.fingerID
Function getFingerprintID():
temp ← finger.getImage()
if temp != FINGERPRINT_OK then
        return -1
end if
temp ← finger.image2Tz()
if temp != FINGERPRINT_OK then
        return -1
end if
temp ← finger.fingerFastSearch()
if temp != FINGERPRINT_OK then
        return -1
end if
return finger.fingerID
```

7. ALGORITHM DESIGN AND IMPLEMENTATION

The proposed method for managing the land records registry is a solid foundation that will make the land registry safer and more open. Users can quickly sign up and create legal accounts, adding an additional layer of trust and speed to the LRM process. The user registration process is mainly a three steps process, Providing personal information, Fingerprint verification, and Document scanning.

In the first step, upon accessing the website of the system, individuals are directed through the initial registration procedure where the users are required to enter their personal information. Subsequently, they obtain an OTP by electronic mail. The One-Time Password acts as an essential security mechanism for the purpose of verifying user identities.

The second step is to ensure maximum security. It is necessary for individuals to undergo a verification process at their respective local land register office, whereby they are required to provide their fingerprints and land record certificates. A registrar administrator provides assistance to users. The system employs a matching algorithm to compare and save hexadecimal values derived from fingerprints, providing evidence of user identification. The verified fingerprints are securely stored on the blockchain. Example of fingerprint verification page is displayed in Figure 11.

Third step is required to present their land record certificates to the administrator for the purpose of scanning. The scanned copies are securely preserved within the database of the land registration office, therefore guaranteeing both the accessibility and integrity of crucial documents. An example scanned document is shown in Figure 12.

The user registration system architecture with blockchain attachment is demonstrated in Figure 13. The process algorithm is designed through necessary smart contact functions, as shown in the Algorithm 2.

The *uploadUserInfo()* function is a smart contract method that allows only authorized users to upload personal information linked to a unique NID. It accepts several parameters, including the NID, full name, parents' names, email, date of birth, fingerprint ID, and address. The function first verifies that only the contract owner can execute it and ensures the NID is not already registered to prevent duplicates. If both checks pass, it standardizes certain string inputs by converting them to uppercase and stores the data in a mapping structure indexed by the NID, using bytes32 for efficient blockchain storage. Finally, it marks the user as registered by setting a Boolean flag to true. The function's flowchart is shown in Figure 14.

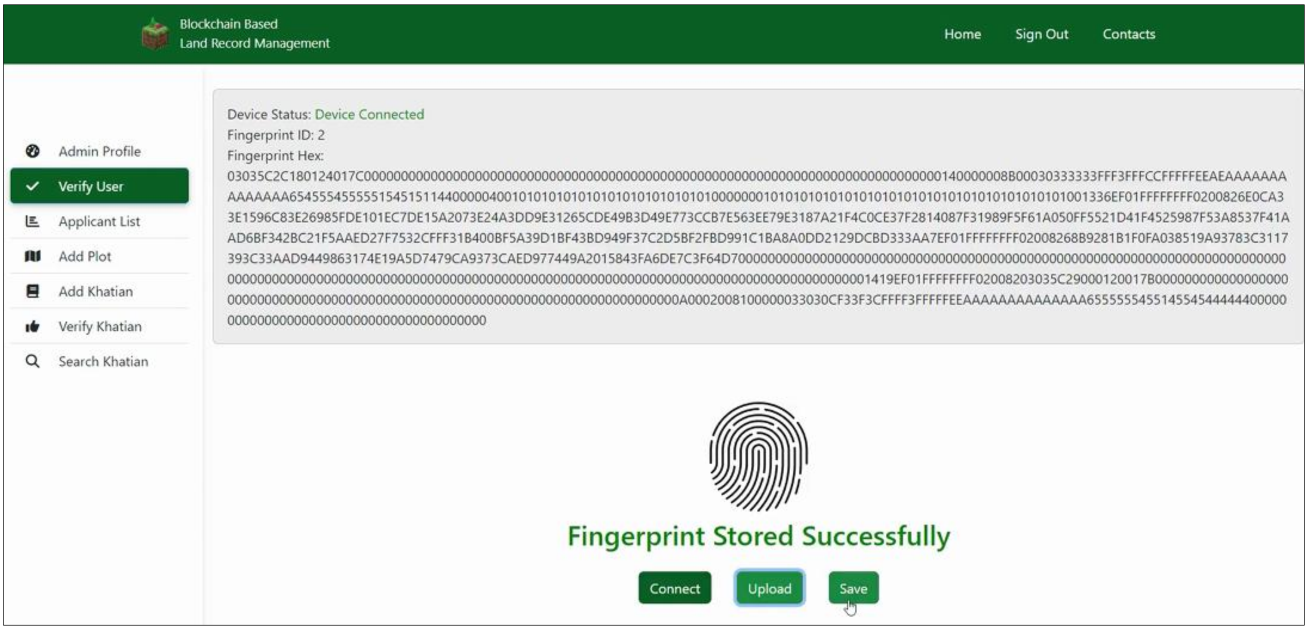
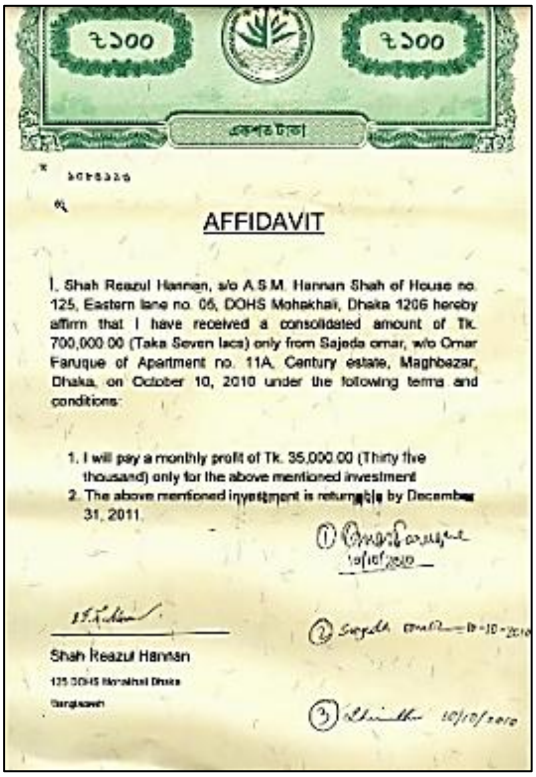


Figure 11: An example of fingerprint verification page



AFFIDAVIT

I, Shah Reazul Hannan, s/o A.S.M. Hannan Shah of House no. 125, Eastern lane no. 05, DOHS Mohakhali, Dhaka 1206 hereby affirm that I have received a consolidated amount of Tk. 700,000.00 (Taka Seven lacs) only from Sajeda omar, w/o Omar Faruque of Apartment no. 11A, Century estate, Maghbazar, Dhaka, on October 10, 2010 under the following terms and conditions:

1. I will pay a monthly profit of Tk. 35,000.00 (Thirty five thousand) only for the above mentioned investment
2. The above mentioned investment is returnable by December 31, 2011.

Shah Reazul Hannan
125 DOHS Mohakhali Dhaka
Bangladesh

Figure 12: Sample of a scanned Certificate for uploading and verification

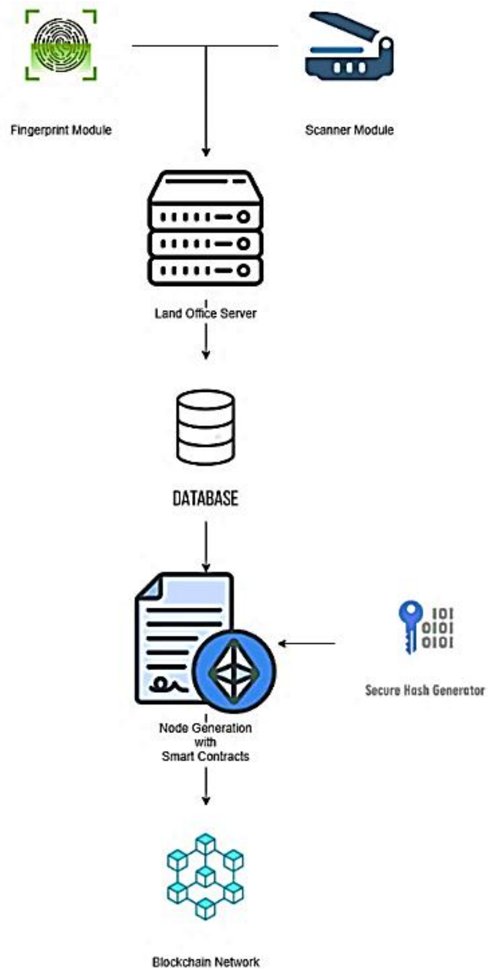


Figure 13: User registration system architecture

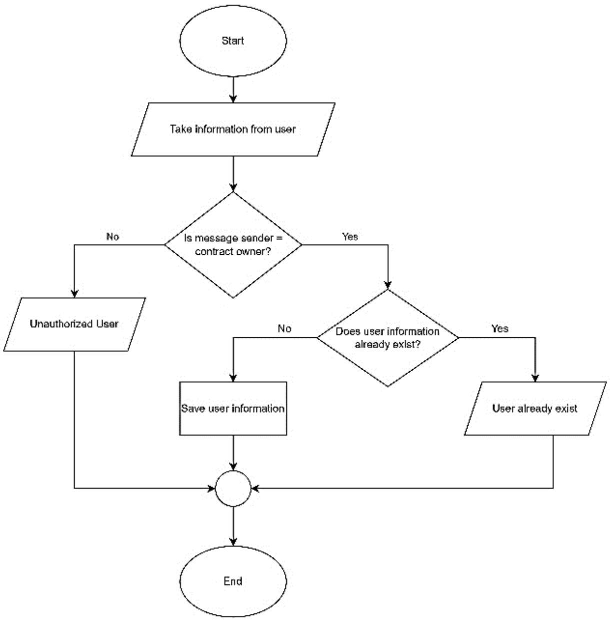


Figure 14: Flowchart of *uploadUserInfo( )* function

The *getUserInfo( )* function retrieves user information from the smart contract by querying the blockchain. It allows authorized users to access stored personal data linked to a specific NID if the user is registered. The function's flowchart is shown in Figure 15.

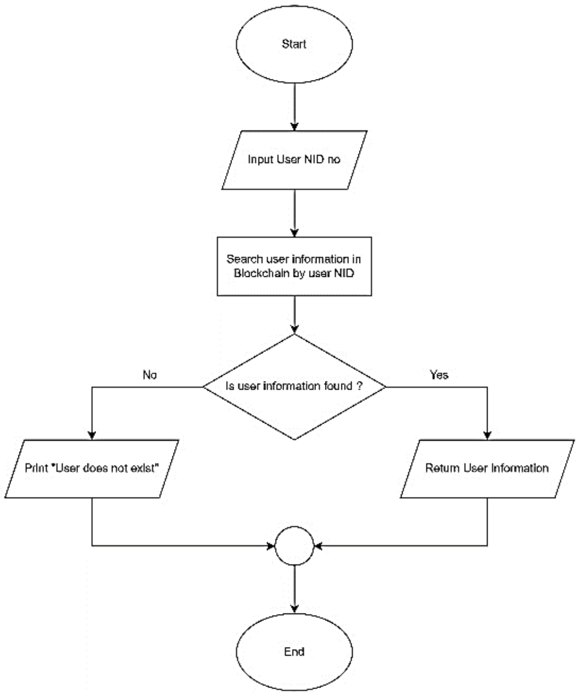


Figure 15: Flowchart of *getUserInfo( )* Function

The *addPlotInfo( )* function records plot details in the smart contract. It accepts parameters such as geographical location (Division, District, Thana), numeric identifiers (JLNo, plot number), plot type, and area. The function then generates a plot hash using the keccak256 algorithm for secure identification. The function first ensures that only the contract owner can add plots, reverting with an error if unauthorized. It then converts the Division, District, and Thana strings to uppercase. If the plot is not already recorded, the function stores the provided details in the plot information mapping, using the plot hash as the key. The flowchart of the function is shown in Figure 16.

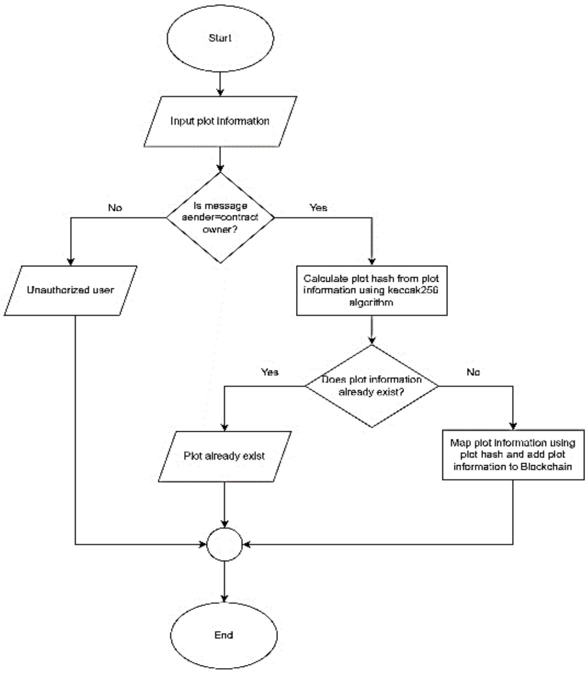


Figure 16: Flowchart of *addPlotInfo( )* Function

The *getPlotInfo( )* function retrieves plot details from the smart contract using a unique plot Hash. Before fetching the data, it verifies whether the plot exists. If not, it reverts with an error message. The function's flowchart is shown in Figure 17.

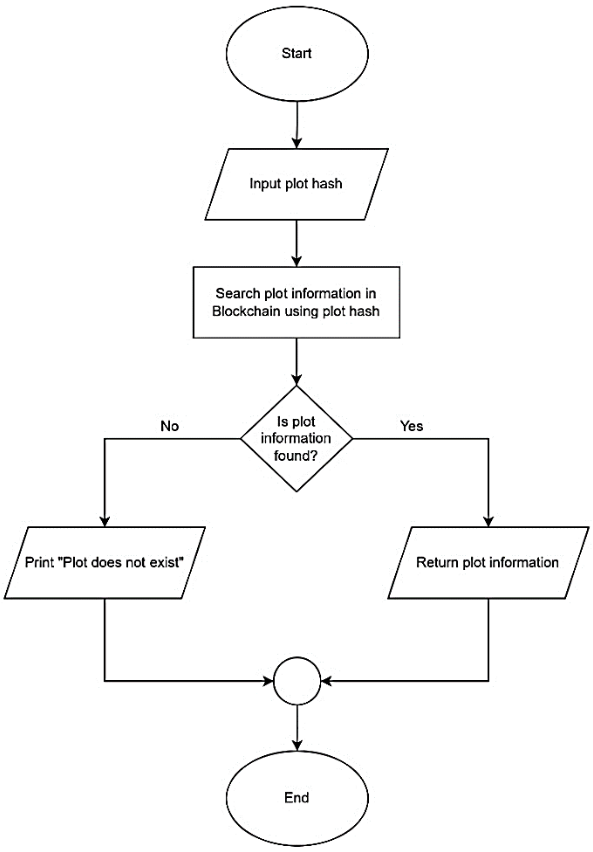


Figure 17: Flowchart of *getPlotInfo( )* Function

The *addNewKhatianInfo( )* function records khatian details in the smart contract. It accepts parameters such as khatian ID, plot hash, owner NIDs, land area, and ownership percentages. The function first ensures that only the contract owner can execute it. If the plot hash is valid, it generates a khatian hash using the keccak256 algorithm based on the plot hash and khatian ID. It then verifies that the khatian hash does not already exist and checks the validity of each owner's NID, converting them to bytes32 format. Finally, it stores the khatian details in the khatianInfo mapping, using the khatian hash as the key. The flowchart is shown in Figure 18.

The *addKhatianInfoFromOld( )* function is designed to add Khatian entries, similar to the *addNewKhatianInfo( )* function. However, this function includes additional functionality to handle the transfer or sale of land from one owner to another.

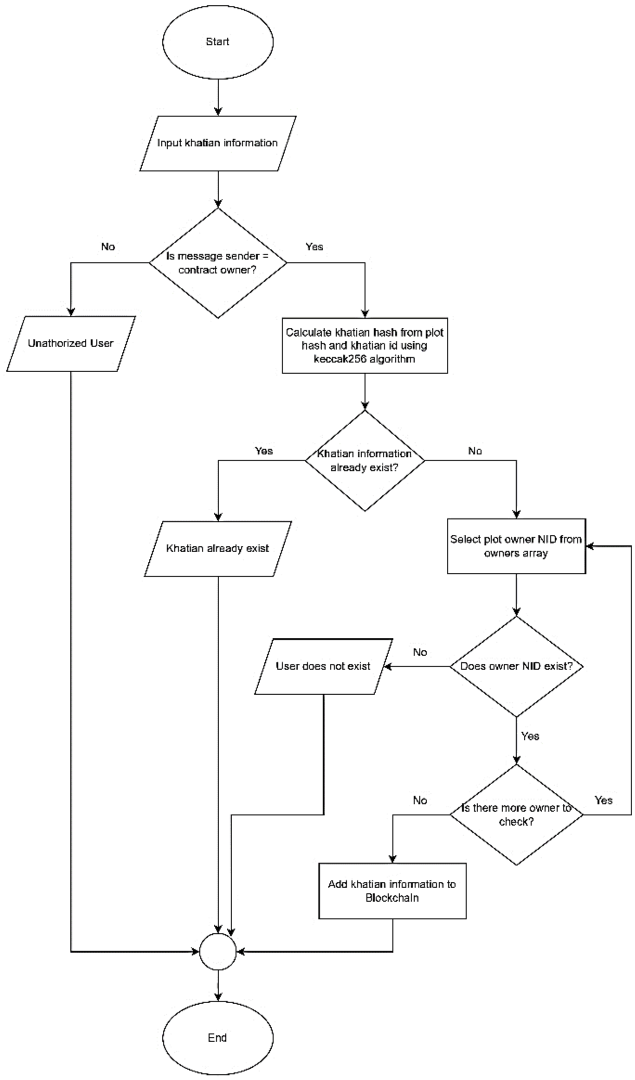


Figure 18: Flowchart of *addNewKhatianInfo( )* Function

Similar to the *addNewKhatianInfo( )* function, this function authorizes the contract owner, calculates khatian hash, and validates the owners' NIDs. It also checks if the buying land area is less or equal to the land area mentioned in the previous khatian. If every requirement is fulfilled, the owners of the land are updated according to the new khatian. The flowchart is given in Figure 19.

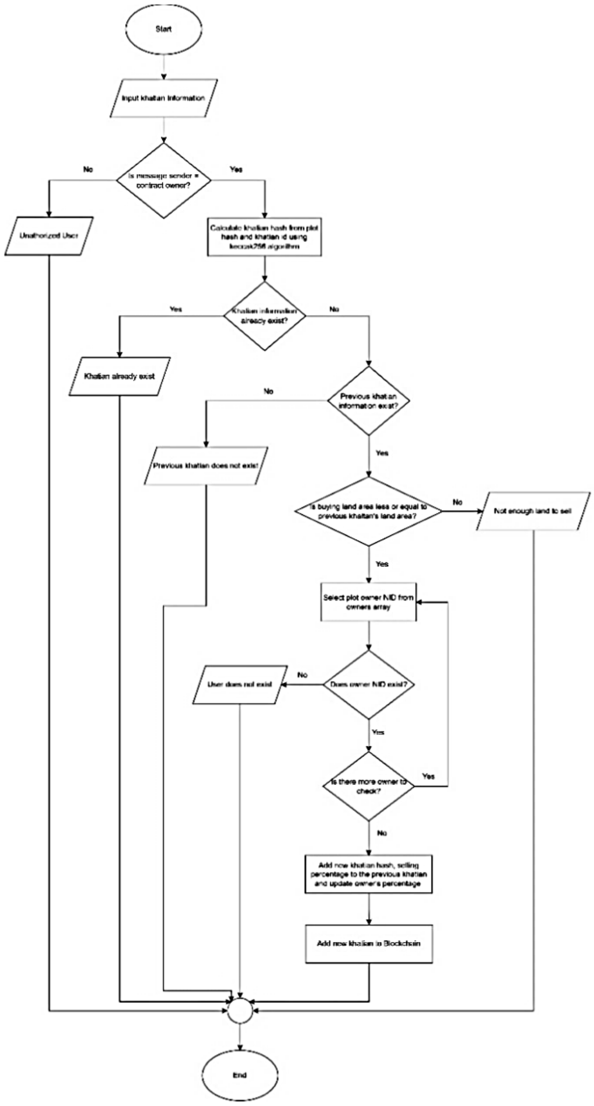


Figure 19: Flowchart of *addKhatianInfoFromOld( )* Function

Next, the *getKhatianInfo( )* function retrieves information about a specific khatian using the khatian hash, which is a unique identifier for each khatian. If the khatian hash exists in the system, the function returns the khatian information associated with the khatian hash. The corresponding flowchart is given in Figure 20.

Algorithm 2: Smart Contract

```
Function uploadUserInfo(user):
if msg.sender == contractOwner then
        if user info[nid].isExists==false then
                user info[nid] = user
        else
                User already exists
else
        Sender is not authorized
end if
Function getUserInfo(nid):
if user info[ nidbyte].isExist == true then
        return user info[nid]
else
        User does not exist
end if
Function addPlot(plot):
if msg.sender == contractOwner then
        if plot info[plothash].isExists== false then
                plot info[plothash] = plot
                plot array.push(plot)
        else
                Plot already exists
        end if
else
        Sender is not authorized
end if
Function addKhatianNew(khatian):
if msg.sender == contractOwner then
        khatian info[khatianhash] = khatian
        for owner in owners list
                khatian of users[owner].push(khatianhash)
        end
        khatian array.push(khatianhash)
else
        Sender is not authorized
end if
Function addKhatianFromOld(khatian):
if msg.sender == contractOwner then
        khatianinfo[buy from].sellTo.push(khatianhash)
        khatianinfo[buyFrom].sellPercentage.push(percentOwn)
        khatian info[buyFrom].percentOwn == percentOwn;
        khatian info[khatianhash] = khatian
        for owner in owners list
                khatians of users[owner].push(khatianhash)
        end
        khatian array.push(khatianhash)
else
        Sender is not authorized
end if
Function getKhatianInfo(khatianhash):
if khatian info[khatianhash].isExist == true then
        return khatian info[khatianhash]
else
        Khatian does not exist
end if
```

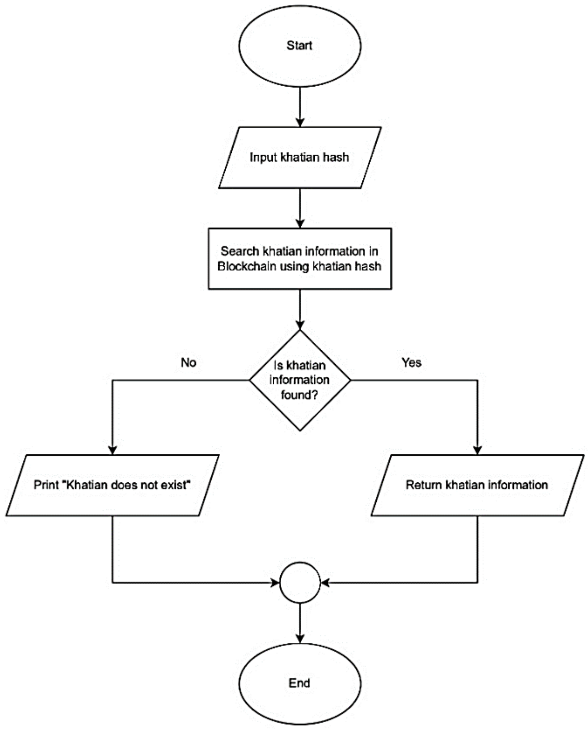


Figure 20: Flowchart of *getKhatianInfo()* function

The smart contract provides several functions for interaction. The *uploadUserInfo()* function stores user details such as name, parents' names, date of birth, address, email, and fingerprint hash in a mapping, using the NID as the key. The *getUserInfo()* function retrieves user data if the NID exists in the system. The *addPlot()* function records plot details, including plot number, JL number, plot type, and address. The *getPlot()* function retrieves plot information if a matching plot hash exists. For khatian management, *addKhatianNew()* adds new khatian records, while *addKhatianFromOld()* transfers ownership from a previous owner. The *getKhatianInfo()* function retrieves stored khatian details.

The interface of the system is designed to prioritize user-friendliness and simplicity, enhancing the efficiency of property transactions. The provided screenshots of the designed interface, Figure 21 to Figure 34, demonstrate improvements in accessibility for land management.

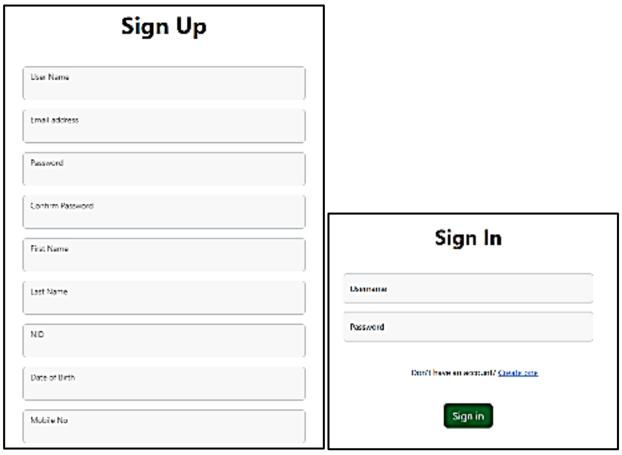


Figure 21: Signup and Login interface

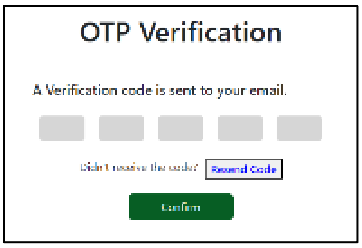


Figure 22: OTP verification interface

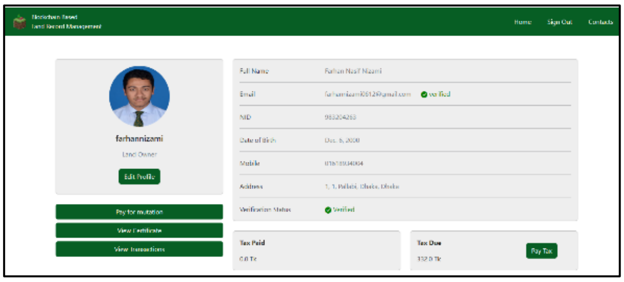


Figure 23: Customer Profile view

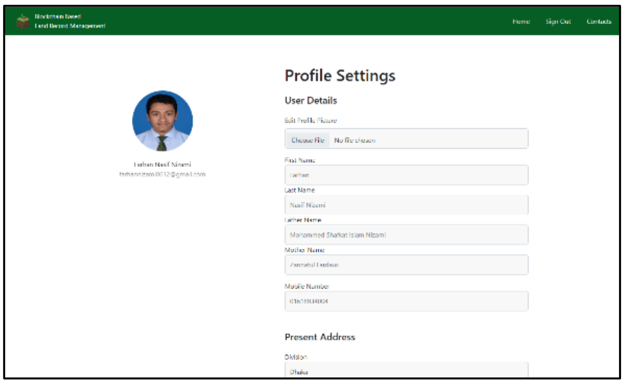


Figure 24: Customer Profile Setting Interface

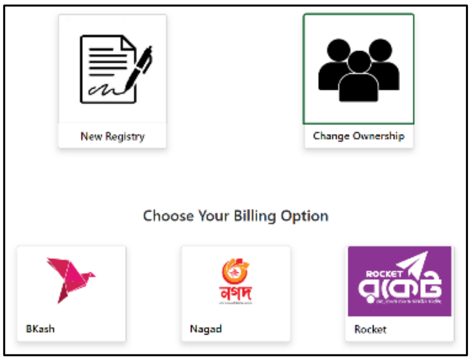


Figure 25: Customer Tax Payment options page

Figure 26: Customer View Certificate Page

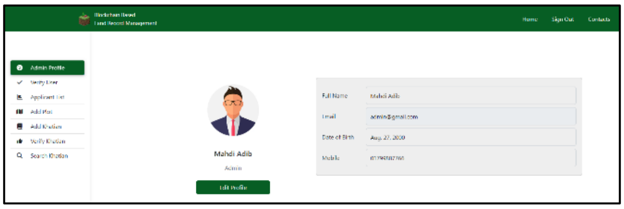


Figure 27: Admin Profile Page

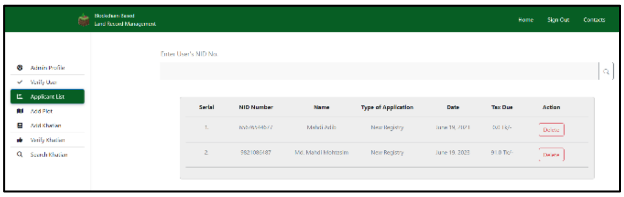


Figure 28: Admin Applicant List Page

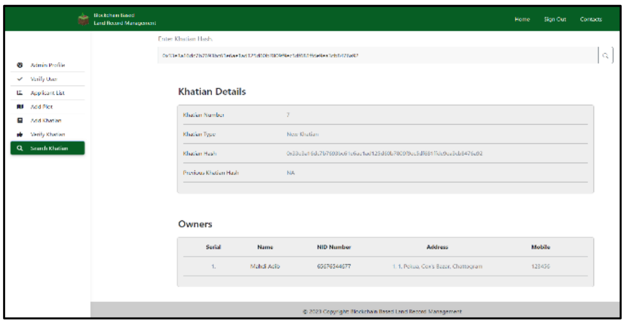


Figure 29: Admin Search Khatian interface

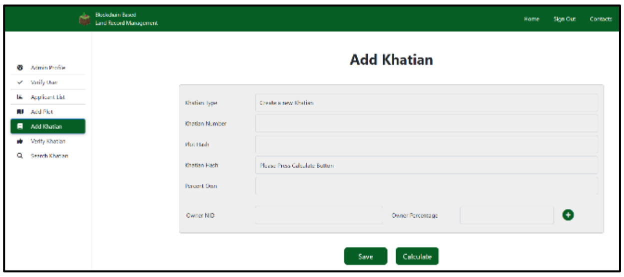


Figure 30: Admin Add Khatian interface

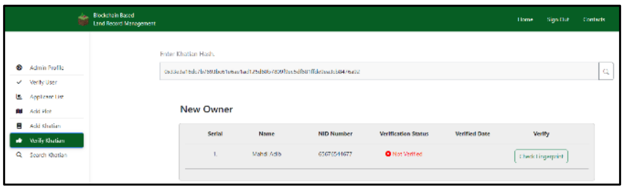


Figure 31: Admin Verify Khatian page

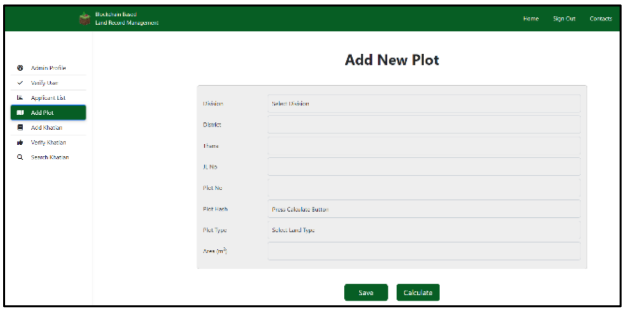


Figure 32: Admin Add Plot interface

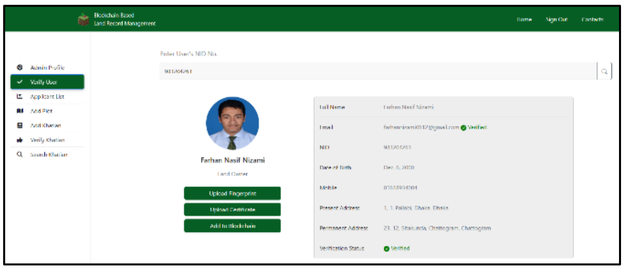


Figure 33: Admin Verify User Page

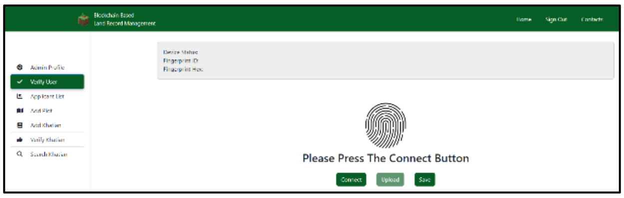


Figure 34: Admin Verify User Fingerprint Page

8. RESULTS AND DISCUSSIONS

When a smart contract is deployed on Ethereum and an event is triggered, a block is generated. Mining and verifying this block, before adding it to the chain, require computational power, quantified as gas fees. Additionally, a specific amount of Ether is needed for transactions (*Kollu et al., 2022; Hobeck et al., 2024*). The computational cost has been calculated for five fundamental operations in the system: deploying the migration function, deploying the smart contract, constructing land, acquiring land, and listing land for sale. Figures 35 and 36 display histograms illustrating gas consumption and Ethereum costs for each function, with color codes assigned to each function for clarity. These figures provide a visual representation of the computational requirements for different operations.

Table 2 presents a feature comparison with existing works. All transactions were conducted on an ASUS laptop running Windows 10 (Version 1803), equipped with a 6-core 2.40GHz Intel Core i7 processor and 16GB RAM. Interaction between the user interface and the Ethereum test network was facilitated using the Web3 framework.

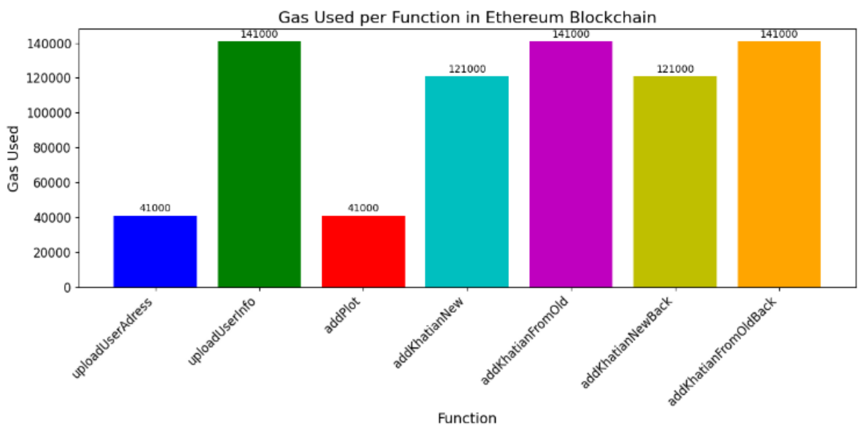


Figure 35: Gas Used per Function

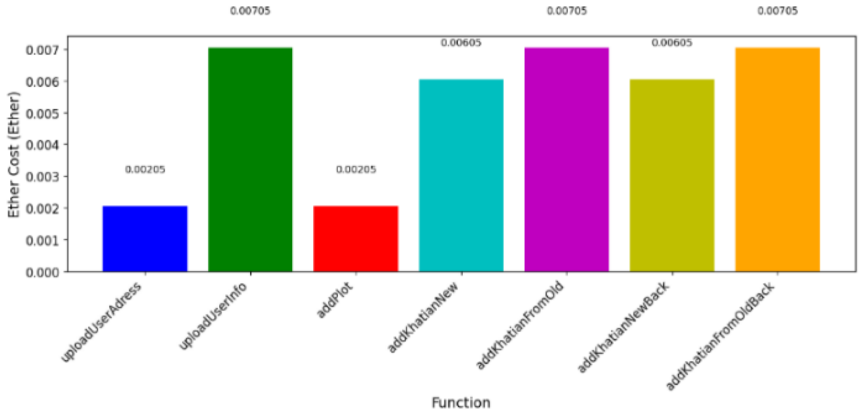


Figure 36: Ether cost per function

Table 2: Feature Comparison of developed system vs. existing systems

Features	**Hasan, Alam, and Tanha, (2022)**	**Nandi et al. (2020)**	**Thamrin et al. (2021)**	**Aquib et al. (2020)**	**Proposed System**
Country	Bangladesh	India	Indonesia	Pakistan	Bangladesh
Challenge	Increase efficiency, improve accessibility to land records	Maintaining proper land ownership/transfer records, including fraud, disputes, and inefficiencies in the current paper-based system	Ease the complexity around project and execution control	Address limitations of traditional land record system	Ensure transparency, and prevent corruption while decentralizing the recording process
Digitization level	Varies across different phases of the system	Publicly-verifiable ledger system	Land database available	Not fully digitized	Varies across different phases of the system
Proposed model	Incremental three-phase permissioned blockchain	Incremental two-phase hybrid blockchain with consensus mechanism	Single phase public blockchain	Incremental private blockchain	Single phase hybrid blockchain
Hardware Integration	N/A	N/A	N/A	Biometric scanners	Fingerprint sensor, Document scanner
Land division and Ownership transfer& Land division and transfer	Land division and transfer	Ownership transfer	Ownership transfer	Land division and transfer	Plot division, fractional ownership transfer
Project Implementation	Ethereum as prototype	Ethereum as conceptual study	Ethereum as prototype	Hyperledger Fabric and Hyperledger Composer Government Initiated Seek feedback from real deployments	Ethereum based blockchain network
Experimental Result	Reduces the number of required travels, improves data accessibility, cost of operations	Improves cost of transactions, and time complexity	NA	Satisfactory feedback from test users	Satisfactory feedback from test users

9. CONCLUSION

This study introduces an efficient and secured approach in tracking land records using Blockchain technology. In contrast to traditional centralized registry systems, the proposed framework offers absolute transparency, automation, and security. The method incorporates biometric fingerprint authentication, digital land certificates verification, and a blockchain network to record immutable transactions. A comprehensive architecture is presented, including user and administrator interfaces, hardware integration of sensors and scanners, smart contracts for operations, and user interfaces. This approach demonstrates blockchain-based processing strategies, like decentralization, cryptographic security, and consensus mechanisms that will transform traditional land record management process into an advanced technological improvement. By recording land transactions in a distributed and tamper-proof ledger, the system reduces the risk of fraud and delays compared to paper-based and centralized digital systems. The integration of sensory tools, e.g. biometrics authentication and document automation further strengthen the credibility of the proposed architecture. Overall, this system represents a significant advancement in the application of blockchain technology that reforms traditional land record management through a state-of-the-art technological application.

To ensure the scalability of the proposed system,

- Modular Blockchain architecture can be design for dynamic scaling of the increasing number of land transactions with ensuring the data integrity and consensus efficiency.

- Integration of Layer-2 protocol, like sidechain or rollups, for offloading transaction processing from the principal Blockchain may improve throughput while reducing latency.
- Using AI driven data optimization and machine learning (*Islam et al., 2024; Akhtaruzzaman et al., 2025*) will help to predict transaction pattern and may optimize data storage, caching, and retrieval ensuring faster integration of blocks.
- Implementing upgradable smart contact for land transactions in supporting the evolving policies as well as regulatory requirements while keeping the existing records safe and secure.
- Implementation of Decentralized Identity (DID) can be considered to authenticate landowners and officials preventing identity fraud in transactions.
- Adopting post-quantum cryptographic method would provide the system extra strength against advanced security threats.
- Investigating the relation and existence of Phi (Φ) the Golden Ratio (*Akhtaruzzaman, and Shafie, 2011; Akhtaruzzaman et al., 2024*) could open another dimension of the relevant research.

ACKNOWLEDGMENTS

Authors also would like to express their gratitude to the Department of Computer Science and Engineering, Military Institute of Science and Technology (MIST), Department of Computer Science and Engineering, Daffodil International University (DIU), and Quantum Robotics and Automation Research Group (QRARG), Dhaka, Bangladesh for their support and guidelines in conducting the project and improving the content of the article.

DATA AVAILABILITY STATEMENT

Datasets generated during the current study are available from the corresponding author upon reasonable request.

FUNDING DECLARATION

This research was self-funded.

ETHICS APPROVAL

This study is an engineering experimental investigation. The MIJST Research Ethics Committee has confirmed that formal ethical approval was not required.

ETHICS, CONSENT TO PARTICIPATE, AND CONSENT TO PUBLISH

Not applicable.

COMPETING INTERESTS

The authors declare that they have no competing interests.

AUTHOR CONTRIBUTIONS

Author 1: Shakil Mosharrof - Conceptualization, Design, Analysis, Implementation, Testing, writing initial draft;

Author 2: Farhan Nasif Nizami - Implementation, Testing, Analysis, Editing;

Author 3: Mahdi Mohtasim - Analysis, Implementation, Testing, Editing;

Author 4: Mahdi Adib - Analysis, Implementation, Testing, Review and editing;

Author 5: M. Akhtaruzzaman - Conceptualization, Design, Analysis, writing original draft, Supervision;

Author 6: Md Shofiqul Islam - Mentoring, Analysis, Review and editing;

Author 7: Muhammad Towfiqur Rahman - Mentoring, Review and editing;

Author 8: Hosney Jahan - Mentoring, Review and editing;

ARTIFICIAL INTELLIGENCE ASSISTANCE STATEMENT

No AI tools were used. The authors take full responsibility for the accuracy and integrity of the manuscript.

CONFLICT OF INTEREST DECLARATION

The authors declare that they have no conflicts of interest.

REFERENCES

Acquah, M. A., Chen, N., Pan, J.-S., Yang, H.-M., & Yan, B. (2020). *Securing fingerprint template using blockchain and distributed storage system. Symmetry, 12*(6), 951. https://doi.org/10.3390/sym12060951

Akhtaruzzaman, M. (2021). *Force-sensitive classic toothbrush: System analysis, design, and simulation. Electrica, 21*(2).

Akhtaruzzaman, M., & Shafie, A. A. (2011). Geometrical substantiation of Phi, the golden ratio and the baroque of nature, architecture, design and engineering. *International Journal of Arts*, 1(1), 1-22

Akhtaruzzaman, M., Shahryer, F., Halder, S., & Tanvin, J. U. (2025). Modeling a fuzzy expert system for predicting customers' behavioral intention for restaurant business through parallel prediction of perceived values and satisfactions. International Journal of Information Technology, 17(2), 1007-1014.

Akhtaruzzaman, M., Tanvin, J. U., Shafie, A. A., Shahryer, F., & Haldar, S. (2024). Application of phi (ϕ), the Golden Ratio, in Computing: A Systematic Review. *IEEE Access*.

Aquib, M., Das Dhomeja, L., Dahri, K., & Malkani, Y. A. (2020). *Blockchain-based land record management in Pakistan.* In *Proceedings of the 2020 3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)* (pp. 1–5). IEEE. https://doi.org/10.1109/iCoMET48670.2020.9073992

Baki, R. F., et al. (2023). *Intelligent Head-bot, towards the development of an AI based cognitive platform. MIJST, 11*(2), 1–14.

Beuria, M. K., Sharma, P. K., Dangra, J., Bulla, C. M., & Abadar, K. (2020). *Applicability of blockchain towards mitigation of distributed denial of service attack in IoT*. European Journal of Molecular & Clinical Medicine, 7(10), 3432–3442

Bouraga, S. (2025). CASCADE – Framework for the early-phase development of blockchain-based applications*. Business & Information Systems Engineering.* https://doi.org/10.1007/s12599-024-00912-4

Buterin, V., et al. (2014). *A next-generation smart contract and decentralized application platform* (White paper, Vol. 3, No. 37, pp. 1–2). Ethereum Foundation. https://ethereum.org/en/whitepaper

Dorri, A., Kanhere, S. S., & Jurdak, R. (2017). *Towards an* *optimized blockchain for IoT.* In *Proceedings of the Second International Conference on Internet-of-Things Design and Implementation* (pp. 173–178). IEEE. https://doi.org/10.1109/IoTDI.2017.7984551

Hasan, M. M. U., Alam, M. M., & Tanha, K. J. (2022). *Decentralized blockchain-based land deed verification and reservation system in Bangladesh*. In 2022 25th International Conference on Computer and Information Technology (ICCIT) (pp. 971–975). IEEE. https://doi.org/10.1109/ICCIT57492.2022.10055779

Hobeck, R., Klinkmüller, C., Bandara, H. M. N. D., et al. (2024). On the suitability of process mining for enhancing transparency of blockchain applications. *Business & Information Systems Engineering.* https://doi.org/10.1007/s12599-024-00903-5

Ibrahim, M., Ravindran, K., Lee, H., Farooqui, O., & Mahmoud, Q. H. (2021). *ElectionBlock: An electronic voting system using blockchain and fingerprint authentication.* In *2021 IEEE 18th International Conference on Software Architecture Companion (ICSA-C)* (pp. 123–129). IEEE. https://doi.org/10.1109/ICSA-C52604.2021.00029

Islam, M. S., Al Farid, F., Shamrat, F. J. M., Islam, M. N., Rashid, M., Bari, B. S., ... & Karim, H. A. (2024). Challenges issues and future recommendations of deep learning techniques for SARS-CoV-2 detection utilising X-ray and CT images: a comprehensive review. *PeerJ Computer Science*, 10, e2517.

Jain, A. K., Bolle, R., & Pankanti, S. (Eds.). (2006). *Biometrics: personal identification in networked society* (Vol. 479). Springer Science & Business Media.

Jesus, E. F., Chicarino, V. R., De Albuquerque, C. V., & Rocha, A. A. D. A. (2018). A survey of how to use blockchain to secure internet of things and the stalker attack. *Security and communication networks*, *2018*(1), 9675050

Khan, S. N., Loukil, F., Ghedira-Guegan, C., Benkhelifa, E., & Bani-Hani, A. (2021). *Blockchain smart contracts: Applications, challenges, and future trends. Peer-to-Peer Networking and Applications, 14*, 2901–2925. https://doi.org/10.1007/s12083-021-01156-0

Khan, R., Ansari, S., Sachdeva, S., & Jain, S. (2020, August). *Blockchain-based land registry system using Ethereum blockchain. Journal of Xi'an University of Architecture & Technology, 12*, 3640–3648

Kollu, P. K., Kumar, K., Kshirsagar, P. R., Islam, S., Naveed, Q. N., Hussain, M. R., & Sundramurthy, V. P. (2022). *Development of advanced artificial intelligence and IoT automation in the crisis of COVID-19 detection. Journal of Healthcare Engineering, 2022*(1), 1987917. https://doi.org/10.1155/2022/1987917

Lee, Y. K., & Jeong, J. (2021). *Securing biometric authentication system using blockchain. ICT Express, 7*(3), 322–326. https://doi.org/10.1016/j.icte.2021.04.004

Mohanta, B. K., Jena, D., Ramasubbareddy, S., Daneshmand, M., & Gandomi, A. H. (2020). *Addressing security and privacy issues of IoT using blockchain technology. IEEE Internet of Things Journal, 8*(2), 881–888. https://doi.org/10.1109/JIOT.2020.2963312

Nandi, M., Bhattacharjee, R. K., Jha, A., & Barbhuiya, F. A. (2020). *A secured land registration framework on blockchain.* In *Proceedings of the 2020 Third ISEA Conference on Security and Privacy (ISEA-ISAP)* (pp. 130–138). IEEE. https://doi.org/10.1109/ISEA-ISAP49340.2020.235432

Padrón Núñez, J. (2021). *Biometric work attendance management and logging with a blockchain system* (Doctoral dissertation, ETSIS_Telecomunicacion)

Pereira, S. N., Tasnim, N., Rizon, R. S., & Islam, M. N. (2021). *Blockchain-based digital record-keeping in land administration system.* In *Proceedings of the International Joint Conference on Advances in Computational Intelligence (IJCACI)* (pp. 431–443). Springer. https://doi.org/10.1007/978-981-16-0961-3_36

Pournaghi, S. M., Zahednejad, B., Bayat, M., & Farjami, Y. (2018). *NECPPA: A novel and efficient conditional privacy-preserving authentication scheme for VANET. Computer Networks, 134*, 78–92. https://doi.org/10.1016/j.comnet.2018.01.019

Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). *On blockchain and its integration with IoT: Challenges and opportunities. Future Generation Computer Systems, 88*, 173–190. https://doi.org/10.1016/j.future.2018.05.046

Sahai, A., & Pandey, R. (2020). *Smart contract definition for land registry in blockchain.* In *Proceedings of the 2020 IEEE 9th International Conference on Communication Systems and Network Technologies (CSNT)* (pp. 230–235). IEEE. https://doi.org/10.1109/CSNT49383.2020.9150791

Sen, S., Mukhopadhyay, S., & Karforma, S. (2021). A blockchain based framework for property registration system in e-governance. *International Journal of Information Engineering and Electronic Business*, *11*(4), 30

Singh, A., Joshi, K., Shuaib, M., Bharany, S., Alam, S., & Ahmad, S. (2022). *Navigation and speed regulation aimed at travel through immersive virtual environments: A review.* In *2022 IEEE International Conference on Current Development in Engineering and Technology (CCET)* (pp. 1–6). IEEE. https://doi.org/10.1109/CCET55037.2022.9845678

Singh, A., Parizi, R. M., Zhang, Q., Choo, K.-K. R., & Dehghantanha, A. (2020). *Blockchain smart contracts formalization: Approaches and challenges to address vulnerabilities.* Computers & Security, 88, 101654. https://doi.org/10.1016/j.cose.2019.101654

Suganthe, R. C., Shanthi, N., Latha, R. S., Gowtham, K., Deepakkumar, S., & Elango, R. (2021). *Blockchain enabled digitization of land registration.* In *Proceedings of the 2021 International Conference on Computer Communication and Informatics (ICCCI)* (pp. 1–5). IEEE. https://doi.org/10.1109/ICCCI50826.2021.9402475

Thamrin, R. M. H., Harahap, E. P., Khoirunisa, A., Faturahman, A., & Zelina, K. (2021). *Blockchain-based land certificate management in Indonesia. ADI Journal on Recent Innovation, 2*(2), 232–252.

Yin, W., Wen, Q., Li, W., Zhang, H., & Jin, Z. (2018). *An anti-quantum transaction authentication approach in blockchain. IEEE Access, 6*, 5393–5401