Blockchain-Based Secure Healthcare Data Sharing System with Access Control

ROWTHU SUPRIYA

PG Scholar. Department M.Sc(CS), DNR College, Bhimavaram, Andhra Pradesh

A.Naga Raju

Lecturer in M.Sc(CS), DNR College, Bhimavaram, Andhra Pradesh

ABSTRACT

In the modern healthcare ecosystem, the secure storage and sharing of patient data have become critical challenges. With increasing digitization, sensitive medical records are frequently accessed, shared, and stored across multiple platforms, raising concerns about data privacy, integrity, and unauthorized access. Traditional centralized systems are vulnerable to data breaches, tampering, and single points of failure. To address these issues, this project proposes a Blockchain-Based Secure Healthcare Data Sharing System with Access Control.

The system leverages blockchain technology to ensure secure, transparent, and tamper-proof storage of patient records. Each patient's data is stored along with a unique blockchain hash generated using the SHA-256 cryptographic algorithm. This ensures that any modification to the data can be easily detected, thereby maintaining data integrity. The blockchain implementation includes essential components such as block creation, proof-of-work consensus mechanism, and chain validation.

The system is developed using the Django web framework and integrates with a MySQL database for storing structured patient data. It provides different interfaces for hospitals and patients. Hospitals can log in, create patient profiles, and define access permissions, while patients can view their records securely. Access control is enforced by specifying authorized users who can retrieve specific patient data.

A key feature of the system is the use of a proof-of-work algorithm to validate transactions before adding them to the blockchain. Each block contains transaction data, timestamp, previous hash, and a nonce value. The mining process ensures that only valid transactions are recorded, enhancing system reliability.

Additionally, the system includes a revenue mechanism that tracks data access by authorized users. Each time a hospital accesses patient data, a small revenue value is incremented, demonstrating a potential model for incentivized data sharing.

The system also incorporates search functionality, allowing hospitals to retrieve patient data based on specific medical conditions while ensuring access restrictions are maintained. The integration of blockchain ensures that all transactions are immutable and traceable.

In conclusion, this project provides a robust solution for secure healthcare data management by combining blockchain technology with web-based application development. It enhances data security, ensures transparency, and provides controlled access, making it a reliable system for modern healthcare environments.

Keywords: Blockchain, Healthcare Data Security, Access Control, Data Privacy, SHA-256, Django Web Application, Secure Data Sharing, Patient Records, Decentralized System, Proof of Work

I. INTRODUCTION

The healthcare industry is increasingly relying on digital systems to store and manage patient information. Electronic Health Records (EHRs) have replaced traditional paper-based systems, enabling faster access and improved coordination among healthcare providers. However, this digital transformation has also introduced significant challenges related to data security, privacy, and integrity.

Healthcare data is highly sensitive and includes personal details, medical history, diagnostic reports, and treatment records. Unauthorized access or tampering with such data can have serious consequences, including identity theft, misdiagnosis, and loss of trust. Traditional centralized databases are vulnerable to cyberattacks and data breaches, as they rely on a single authority for data management.

Blockchain technology has emerged as a promising solution to address these challenges. It is a decentralized and distributed ledger system that ensures data immutability, transparency, and security. Each transaction in a blockchain is recorded in a block, which is linked to previous blocks using cryptographic hashes. This makes it extremely difficult to alter or delete data once it has been recorded.

This project aims to develop a Blockchain-Based Secure Healthcare Data Sharing System that ensures safe storage and controlled access to patient records. The system uses SHA-256 hashing to generate unique identifiers for each block, ensuring data integrity. A proof-of-work mechanism is implemented to validate transactions before adding them to the blockchain.

The system is built using Django, a powerful web framework that supports rapid development and secure application design. It integrates with a MySQL database to store patient information and uses role-based access control to restrict data access. Hospitals can create and manage patient records, while access is granted only to authorized entities.

One of the unique features of this system is the integration of access control with blockchain technology. Each patient record includes a list of authorized users, ensuring that only

permitted entities can view the data. Additionally, the system tracks data access and updates revenue metrics, providing insights into data usage.

Overall, this project demonstrates how blockchain can be effectively used to enhance healthcare data security. It provides a scalable and efficient solution that addresses the limitations of traditional systems and supports secure data sharing in modern healthcare environments.

II. LITERATURE SURVEY (WITH EXISTING METHODS)

The application of blockchain technology in healthcare has gained significant attention in recent years. Researchers have explored various approaches to improve data security, privacy, and interoperability using decentralized systems.

Traditional healthcare systems rely on centralized databases, which are prone to security vulnerabilities such as unauthorized access, data breaches, and single points of failure. Studies have shown that these systems often lack transparency and fail to provide adequate data integrity mechanisms.

Blockchain technology addresses these issues by providing a decentralized and tamper-proof data storage mechanism. Each block in the blockchain contains a cryptographic hash of the previous block, ensuring data immutability. Research has demonstrated that blockchain can enhance trust and transparency in healthcare systems.

Several existing solutions use blockchain for electronic health record management. These systems allow patients to control access to their data while ensuring secure sharing among healthcare providers. Smart contracts have also been used to automate access control and data sharing processes.

Another area of research focuses on cryptographic techniques such as SHA-256 for securing data. Hashing ensures that even minor changes in data result in completely different hash values, making it easy to detect tampering.

Proof-of-work consensus mechanisms have been widely studied for validating transactions in blockchain systems. Although computationally intensive, they provide a high level of security by ensuring that only verified transactions are added to the chain.

Despite these advancements, many existing systems face challenges such as high computational cost, scalability issues, and lack of user-friendly interfaces. Additionally, integration with existing healthcare infrastructure remains a challenge.

The proposed system builds upon these research efforts by combining blockchain technology with a web-based application framework. It provides a simple yet effective implementation of blockchain for secure healthcare data sharing, along with user-friendly interfaces and access control mechanisms.

III. EXISTING SYSTEM

Existing healthcare data management systems primarily rely on centralized databases to store and manage patient records. These systems are typically controlled by hospitals or healthcare organizations, which act as central authorities. While such systems provide basic functionality for storing and retrieving data, they suffer from several limitations.

One of the major drawbacks of centralized systems is their vulnerability to cyberattacks. Since all data is stored in a single location, attackers can target the system to gain unauthorized access to sensitive information. Data breaches in healthcare systems have become increasingly common, highlighting the need for more secure solutions.

Another limitation is the lack of data integrity. In traditional systems, it is difficult to verify whether data has been altered or tampered with. This can lead to serious issues such as incorrect medical records and misdiagnosis.

Access control in existing systems is also limited. Although some systems provide role-based access, they often lack fine-grained control over who can access specific data. This can result in unauthorized data sharing and privacy violations.

Furthermore, existing systems do not provide transparency in data access. There is no reliable way to track who accessed the data and when, making it difficult to ensure accountability.Additionally, these systems often lack interoperability, making it challenging to share data across different healthcare providers. This leads to inefficiencies and delays in patient care.

In summary, existing healthcare data management systems are limited by security vulnerabilities, lack of transparency, and inefficient access control mechanisms. These shortcomings highlight the need for a more secure and decentralized approach, which the proposed blockchain-based system aims to address.

IV. PROPOSED METHOD

The proposed system introduces a Blockchain-Based Secure Healthcare Data Sharing platform designed to enhance data security, integrity, and controlled access in healthcare environments. The system replaces traditional centralized storage with a decentralized blockchain structure, ensuring that patient data remains tamper-proof and transparent.

In this system, each patient record is treated as a transaction and stored within a block. These blocks are linked together using cryptographic hashes generated through the SHA-256 algorithm. This ensures that any modification in the stored data will result in a change in the hash, making unauthorized alterations easily detectable.

The system incorporates a proof-of-work (PoW) consensus mechanism to validate transactions before adding them to the blockchain. This process involves solving

computational puzzles to generate a valid hash that meets predefined difficulty criteria. Only verified transactions are added to the blockchain, ensuring data authenticity.

A key feature of the system is role-based access control. Hospitals and authorized entities can access patient data only if they are included in the predefined access list. This ensures privacy and prevents unauthorized data sharing. Additionally, the system logs every data access operation, providing transparency and accountability.

The platform is implemented as a web application using Django, enabling easy interaction for users. Hospitals can create patient profiles, define access permissions, and search records, while patients can securely view their information.

Furthermore, the system includes a revenue mechanism that tracks data access by authorized users, demonstrating a model for incentivized data sharing.

Overall, the proposed system enhances healthcare data management by integrating blockchain technology with secure access control, ensuring privacy, transparency, and reliability.

V. IMPLEMENTATION

The implementation of the Blockchain-Based Healthcare Data Sharing System is carried out using Python, Django framework, and MySQL database. The system integrates blockchain logic with web-based functionalities to provide a secure and user-friendly platform.

The core component of the system is the blockchain module, which includes two main classes: Block and Blockchain. The Block class represents a single block in the chain and contains attributes such as index, transaction data, timestamp, previous hash, and nonce. The compute_hash function generates a SHA-256 hash of the block's contents, ensuring data integrity.

The Blockchain class manages the entire chain. It initializes with a genesis block and maintains a list of unconfirmed transactions. The proof_of_work function is used to generate a valid hash by iterating the nonce value until the hash satisfies the difficulty condition. The add_block function verifies the block before appending it to the chain.

The web application is developed using Django views. Different views are implemented to handle user interactions such as creating profiles, logging in, accessing data, and searching records. The CreateProfileData view allows hospitals to create new patient records. It collects input data, generates a blockchain transaction, mines a block, and stores the resulting hash in the database.

The system uses MySQL as the backend database to store patient information, including personal details, medical records, access permissions, and blockchain hash values. Database operations are performed using SQL queries through the mysql.connector library.

User authentication is implemented for hospitals, ensuring that only authorized users can access the system. Session management is handled using file-based storage to track logged-in users.

The PatientDataAccess view allows hospitals to search for patient records based on medical conditions. It verifies access permissions before displaying data and updates revenue values for each access.

The frontend is developed using HTML templates, providing a simple and intuitive interface. Data is displayed in tabular format for better readability.

Error handling and input validation are incorporated to ensure system robustness. The modular design allows easy integration of additional features such as advanced consensus mechanisms or cloud deployment.

VI. ALGORITHMS

The system uses several algorithms to ensure secure data storage, validation, and access control.

1. Blockchain Hashing Algorithm (SHA-256)
Input: Block data (transactions, timestamp, previous hash, nonce)
Process:
Convert block data into JSON string
Apply SHA-256 hashing
Output: Unique hash value
Purpose: Ensures data integrity and immutability
2. Proof-of-Work Algorithm
Input: Block data
Process:
Initialize nonce = 0
Generate hash
Increment nonce until hash starts with predefined zeros
Output: Valid hash
Purpose: Validates transactions before adding to blockchain
3. Block Validation Algorithm
Input: New block and proof
Process:
Check previous hash match
Verify hash using PoW criteria
Output: Boolean (valid/invalid)
Purpose: Ensures chain consistency

4. Access Control Algorithm
Input: User identity and access list
Process:
Compare logged-in user with allowed users
Grant or deny access
Output: Authorized data access
Purpose: Protects patient privacy
5. Revenue Update Algorithm
Input: Patient ID
Process:
Increment revenue value in database
Output: Updated revenue
Purpose: Tracks data usage

These algorithms ensure security, transparency, and efficient system operation.

VII. SYSTEM DESIGN

The system design follows a layered architecture combining blockchain technology with web-based application design. It ensures modularity, scalability, and security.

1. Architecture Overview

The system is divided into three layers:

Presentation Layer: User interface (HTML templates)
Application Layer: Django views and blockchain logic
Data Layer: MySQL database
2. Module Design

a) User Authentication Module
Handles login and session management for hospitals and users.

b) Patient Profile Module
Allows creation and storage of patient records with blockchain hash.

c) Blockchain Module
Manages block creation, hashing, and validation.

d) Data Access Module
Controls access to patient records based on permissions.

e) Search Module
Enables searching patient data based on medical conditions.

3. Data Flow Design
User logs into system
Hospital creates patient profile
Data is converted into blockchain transaction
Block is mined and added to chain
Hash is stored in database
Authorized user requests data
System verifies access and displays data
4. Database Design
Patients Table:
Patient ID
Name, Age, Problem
Access Control
Blockchain Hash
Revenue
5. Component Design
Input Component: User forms
Processing Component: Blockchain + Django logic
Output Component: Data display tables
6. Security Design
SHA-256 hashing for data integrity
Proof-of-work for validation
Access control for privacy
Session tracking for authentication
7. Scalability

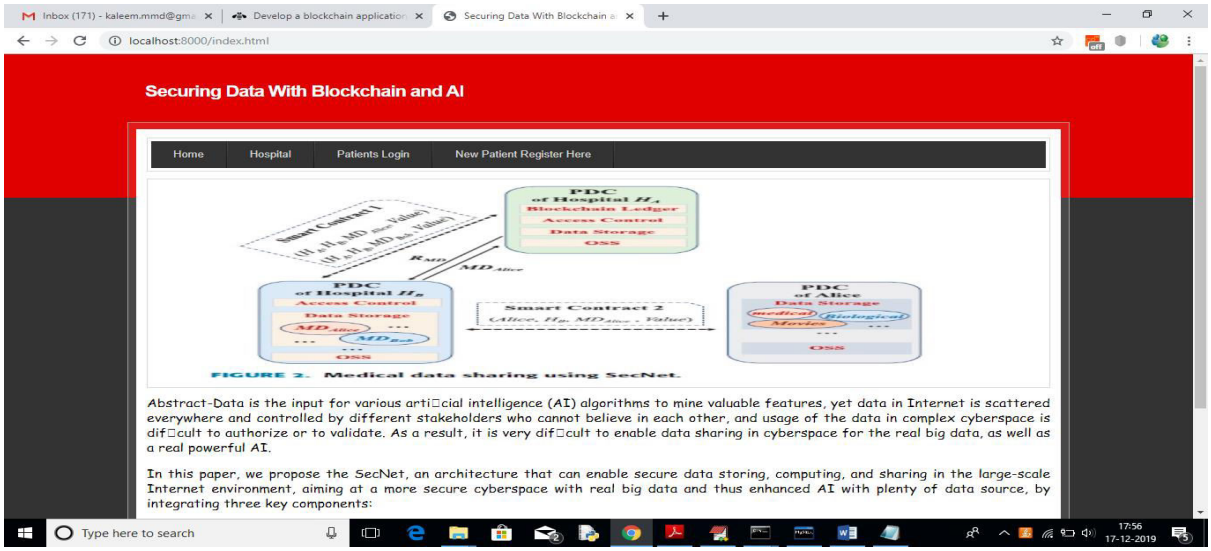
The system can be extended by:

Using distributed blockchain networks
Integrating cloud storage
Adding smart contracts

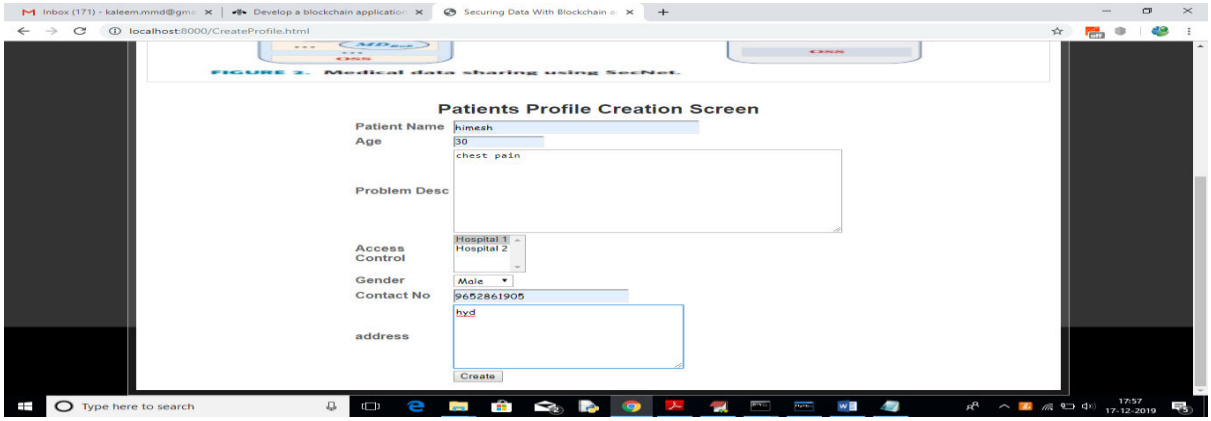
Overall, the design ensures secure, transparent, and efficient healthcare data management.

SYSTEM DESIGN IMAGES

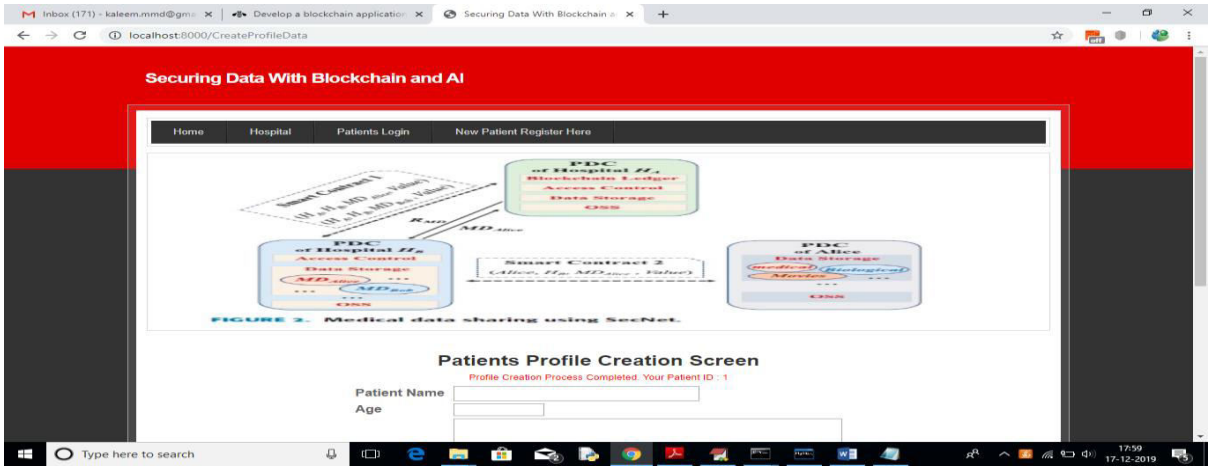
Deploy code on DJANOGO and start server and run in browser to get below screen



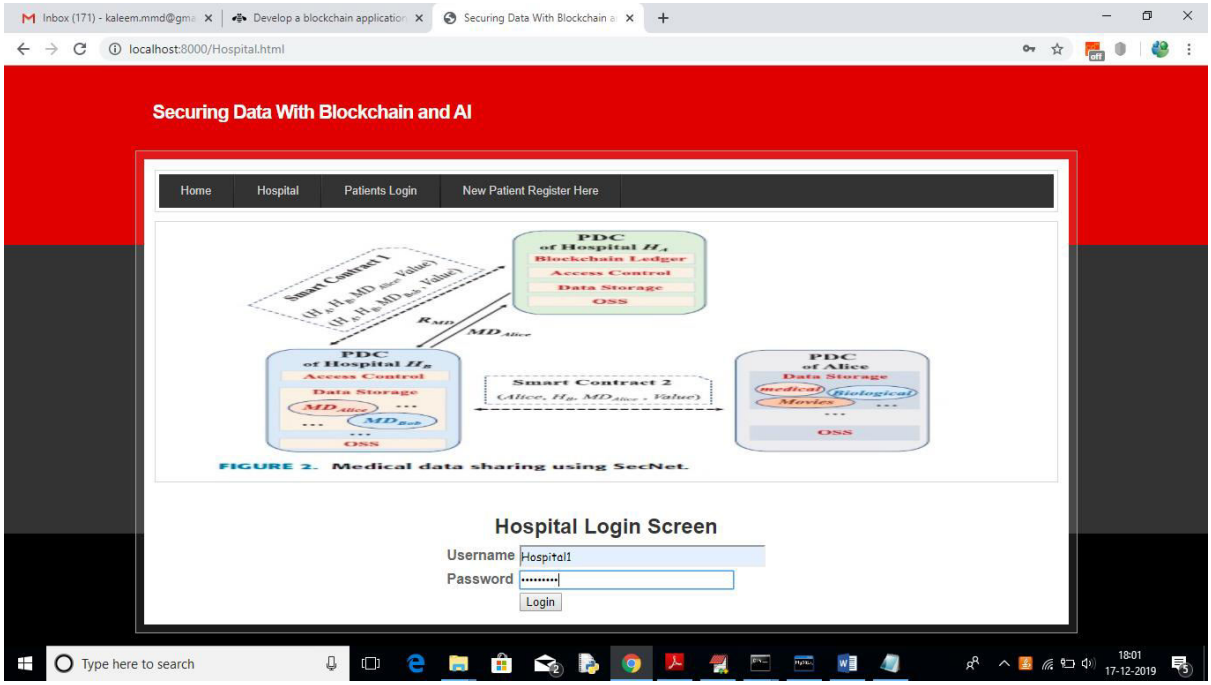
In above screen click on 'New Patient Register Here' link to get below screen



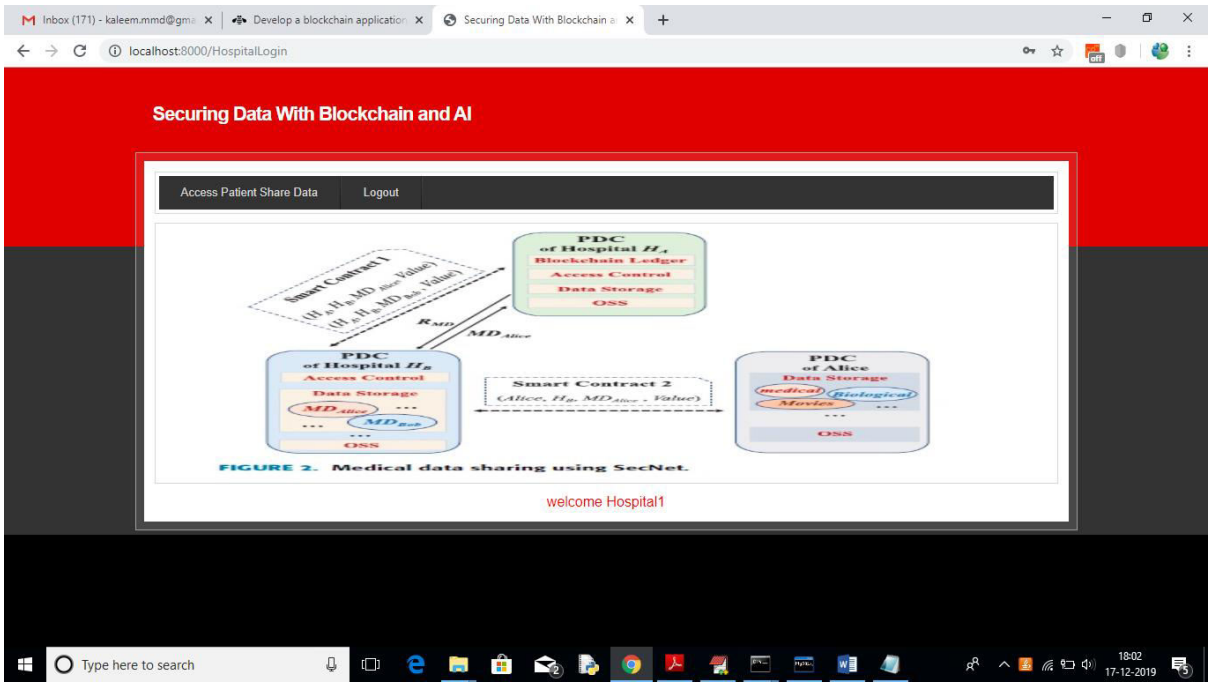
In above screen I am adding patient disease details and selecting 'Hospital1' to share my data and if you want to share with two hospitals then hold 'CTRL' key and select both hospitals to give permission. Now press 'Create' button to create profile



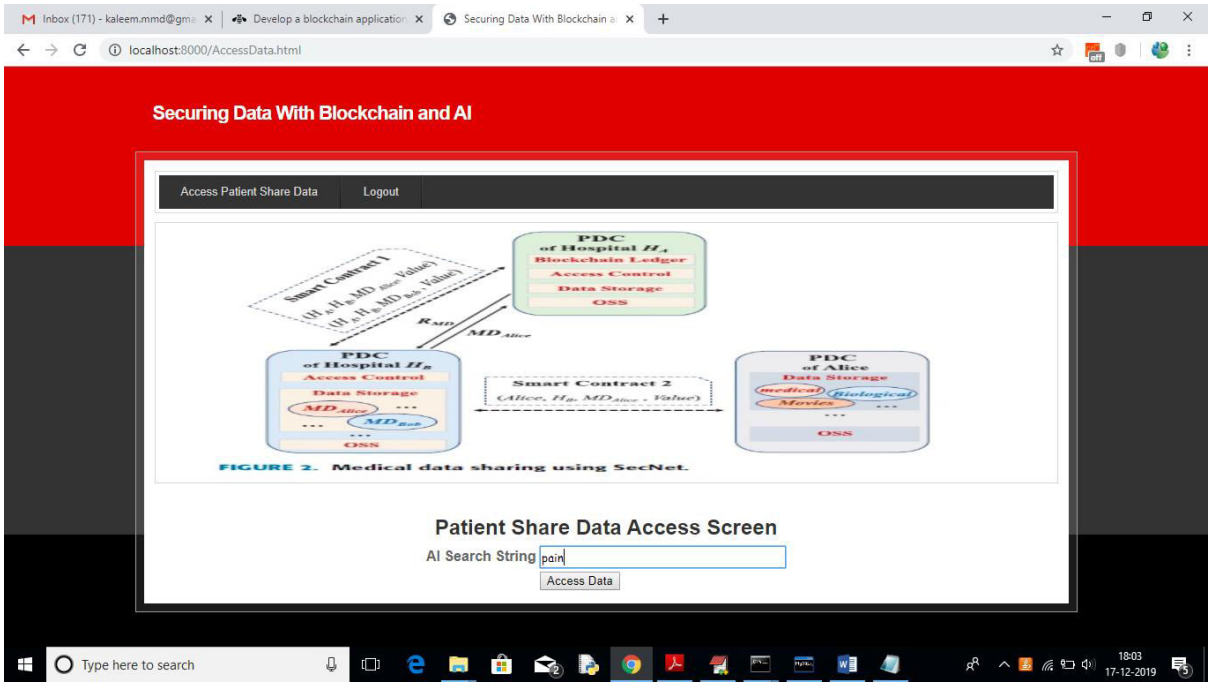
In above screen one patient is created with patient ID 1 and now Hospital 1 can login and search and access this patient data as patient has given permission to Hospital1



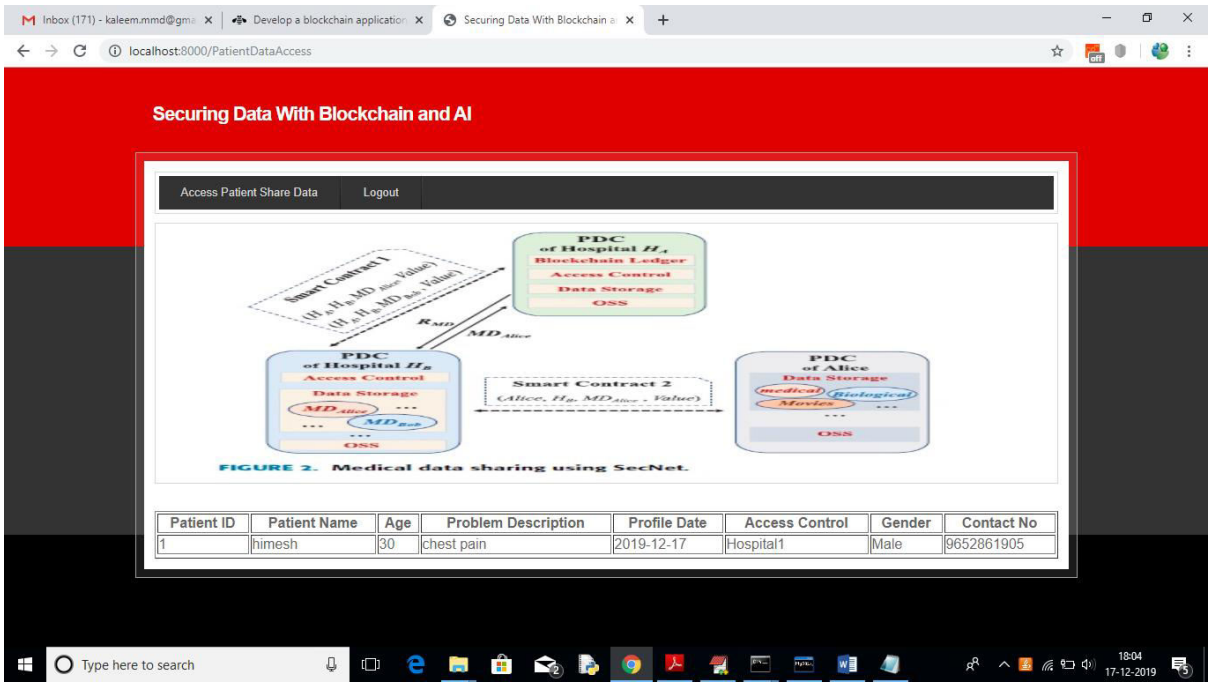
In above screen to login as Hospital1 click on 'Hospital' link to get above screen. Use 'Hospital1' as username and 'Hospital1' as password to login as Hospital1 and use Hospital2 to login as Hospital2. After login will get below screen



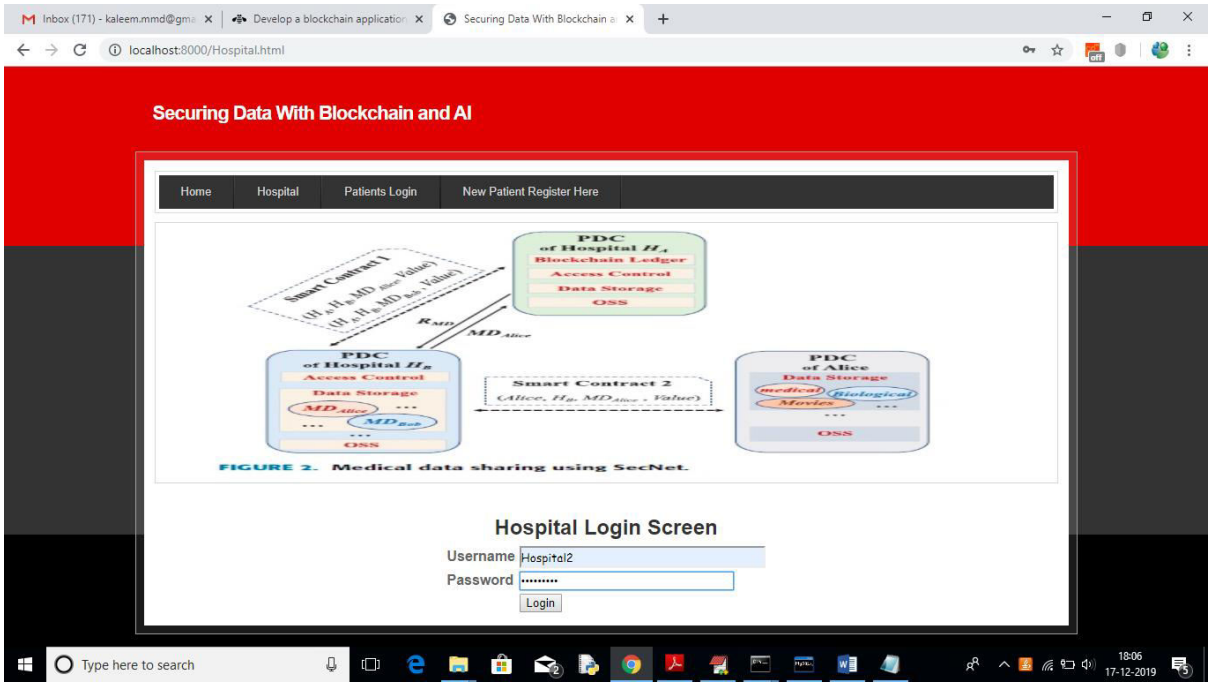
In above screen click on 'Access Patient Share Data' link to search for patient details



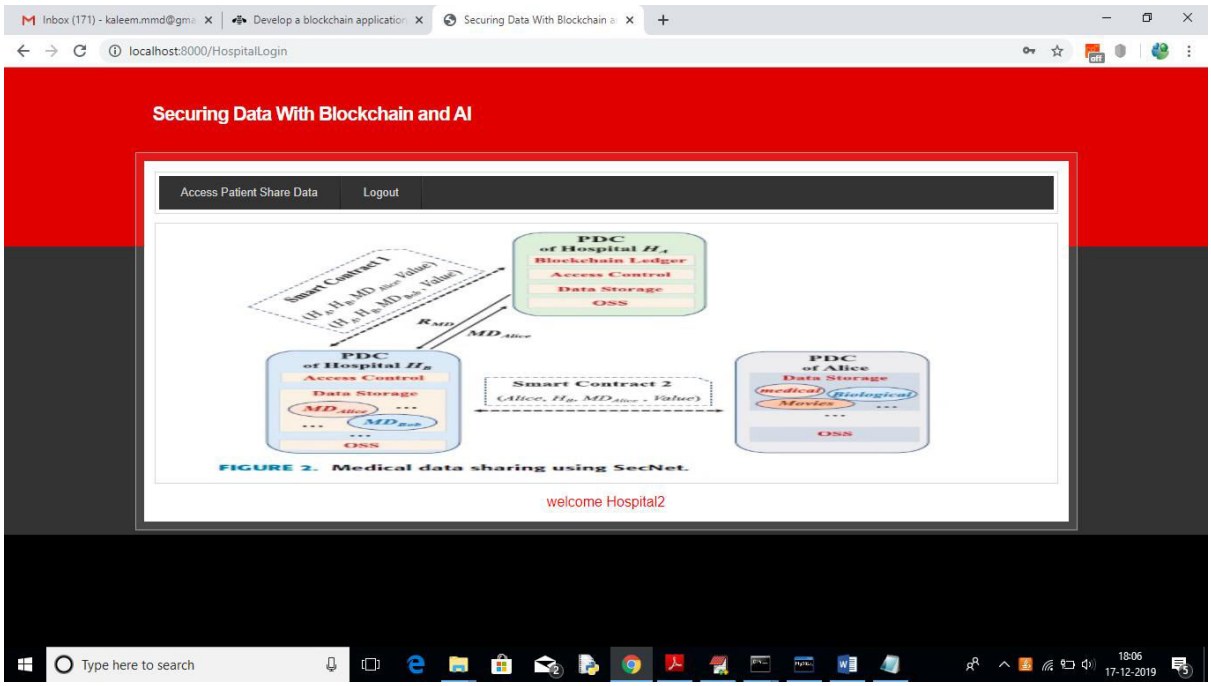
In above screen I want to search for all patients who are suffering from 'pain' and then click on 'Access data' button to get below screen



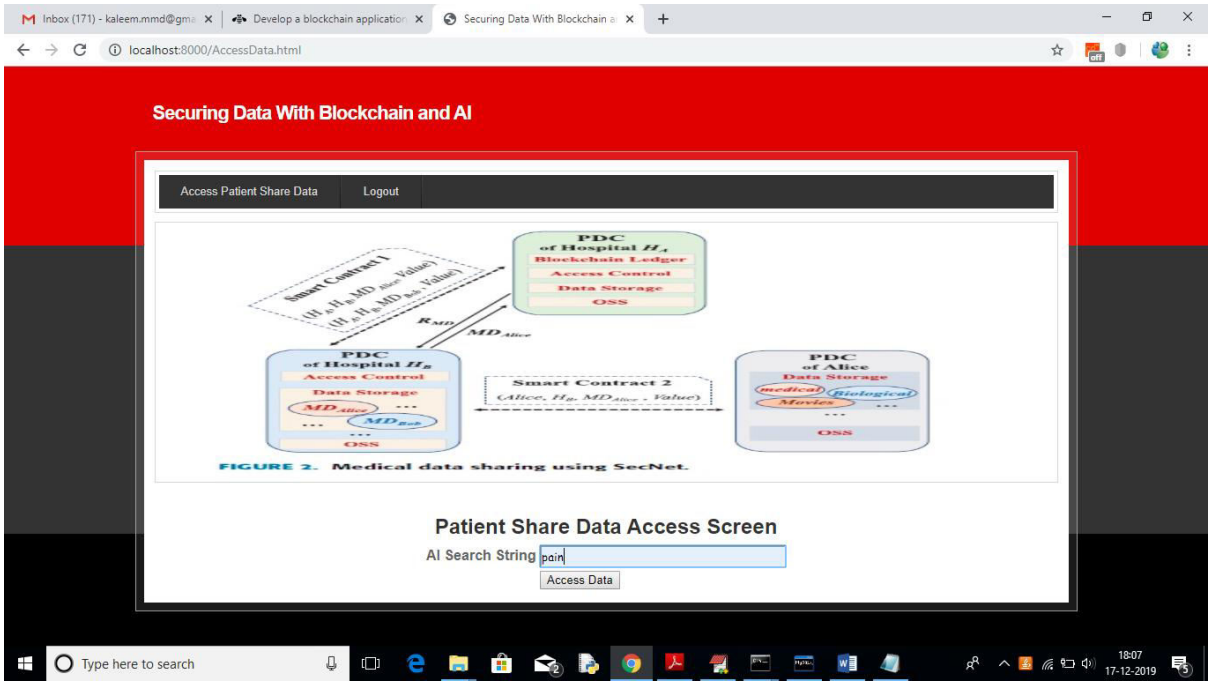
In above screen Hospital1 getting details of patient and Hospital2 not having permission so it will not get details. To see this logout and login as 'Hospital2'



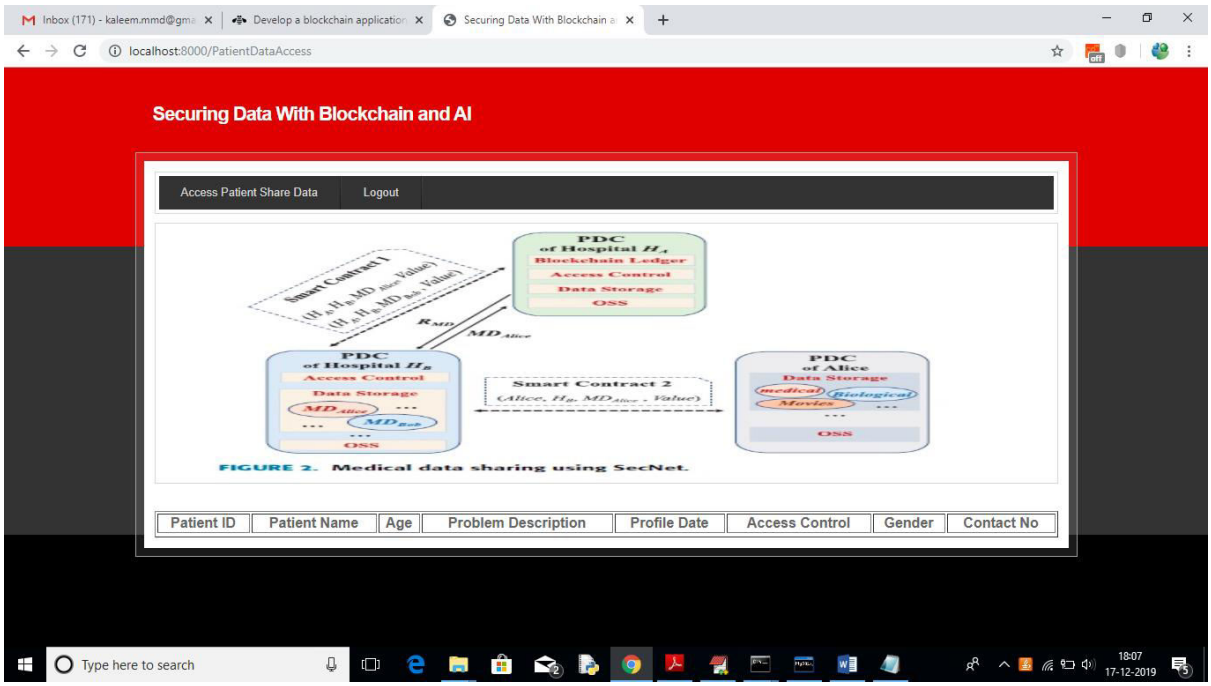
In above screen 'Hospital2' is login, after login will get below screen



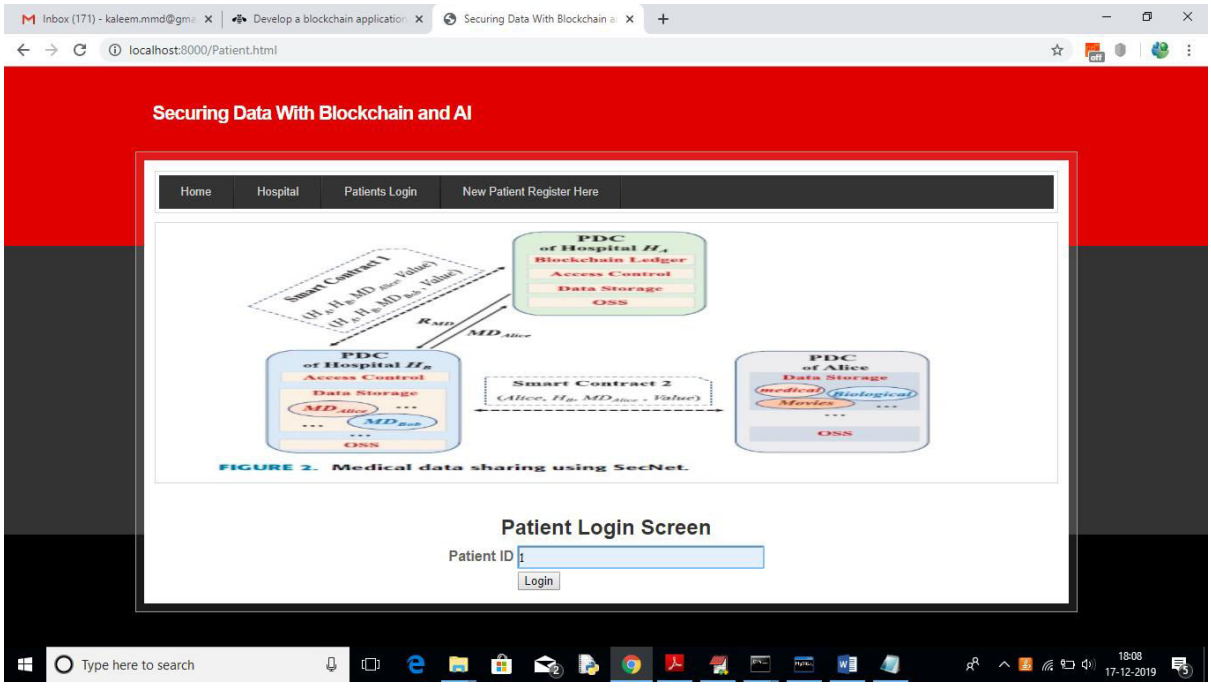
Now click on 'Access Patient Share Data' link and search for same pain disease



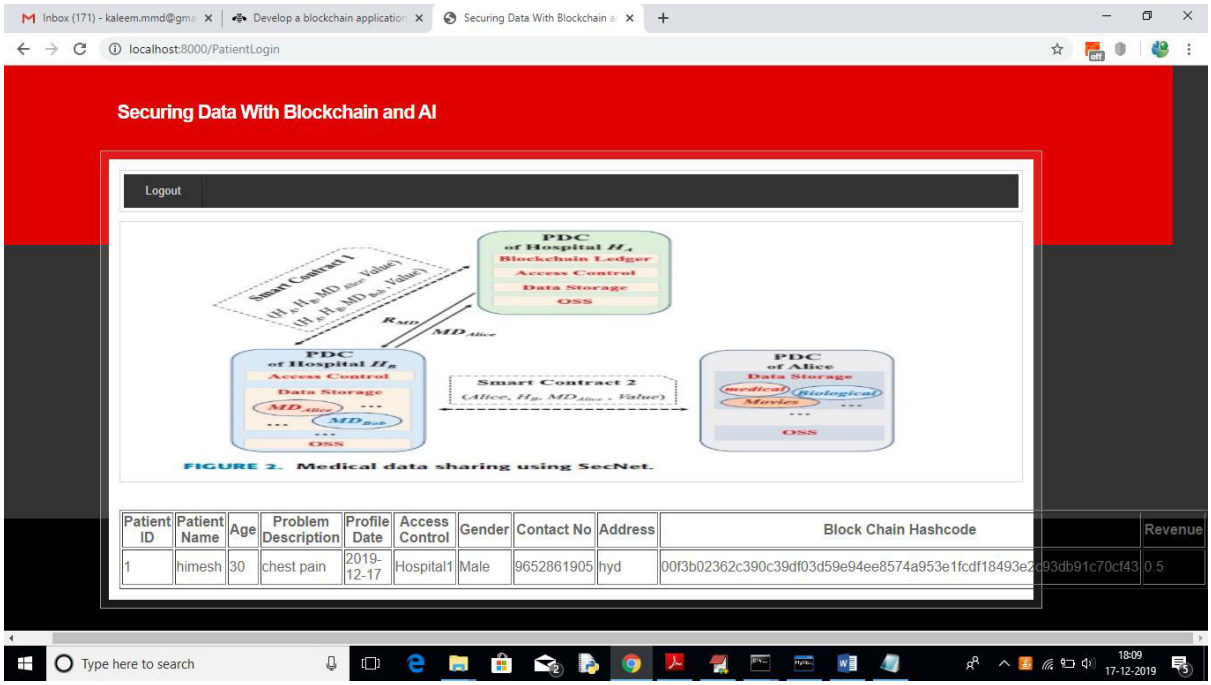
For above query will get below result



In above screen no patient details are showing as Hospital2 not having permission. So block chain allow only those users to access data who has permission. Now logout and login as patient by entering patient id in below screen



After login will get below details for patient 1



In above screen we can see patient all details and hash code generated by block chain and in last column we can see patient reward revenue as 0.5 and it will get update upon every access from hospital user.

VIII. CONCLUSION

The Blockchain-Based Secure Healthcare Data Sharing System provides an innovative solution to the challenges of data security, privacy, and integrity in modern healthcare systems. By leveraging blockchain technology, the system ensures that patient records are stored in a tamper-proof and transparent manner.

One of the key strengths of the system is its use of cryptographic hashing and proof-of-work mechanisms to validate and secure data. These features ensure that any unauthorized modification can be easily detected, thereby maintaining data integrity. The decentralized nature of blockchain eliminates the risks associated with centralized systems, such as single points of failure and data breaches.

The implementation of access control mechanisms further enhances security by ensuring that only authorized users can access sensitive patient data. This protects patient privacy and ensures compliance with data protection standards.

The system also demonstrates practical integration of blockchain with web technologies using Django and MySQL. The user-friendly interface makes it accessible to healthcare professionals, while the modular design allows for future enhancements.

Although the system provides a strong foundation, it can be further improved by incorporating advanced features such as smart contracts, real-time blockchain networks, and mobile applications. These enhancements would increase scalability and usability.

In conclusion, this project highlights the potential of blockchain technology in transforming healthcare data management. It provides a secure, efficient, and transparent system that addresses the limitations of traditional approaches and contributes to the advancement of digital healthcare solutions.

REFERENCES

1. S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008.
2. M. Swan, Blockchain: Blueprint for a New Economy, O’Reilly, 2015.
3. Tapscott and A. Tapscott, Blockchain Revolution, Penguin, 2016.
4. Dorri et al., “Blockchain for IoT Security,” IEEE IoT Journal, 2017.
5. Peterson et al., “Blockchain for Healthcare,” IBM Journal, 2016.
6. Zhang et al., “Blockchain-based EHR systems,” IEEE Access, 2018.
7. python Software Foundation, “Python Documentation,” 2024.
8. Django Software Foundation, “Django Documentation,” 2024.
9. MySQL Documentation, Oracle, 2024.
10. W. Stallings, Cryptography and Network Security, Pearson, 2017.
11. NIST, “Secure Hash Standard (SHA-256),” 2015.
12. Kumar et al., “Secure data sharing using blockchain,” IJCSIT, 2020.
13. G. Wood, “Ethereum White Paper,” 2014.
14. IBM, “Blockchain in Healthcare Report,” 2021.
15. Zheng et al., “Blockchain challenges and opportunities,” IJIT, 2018.