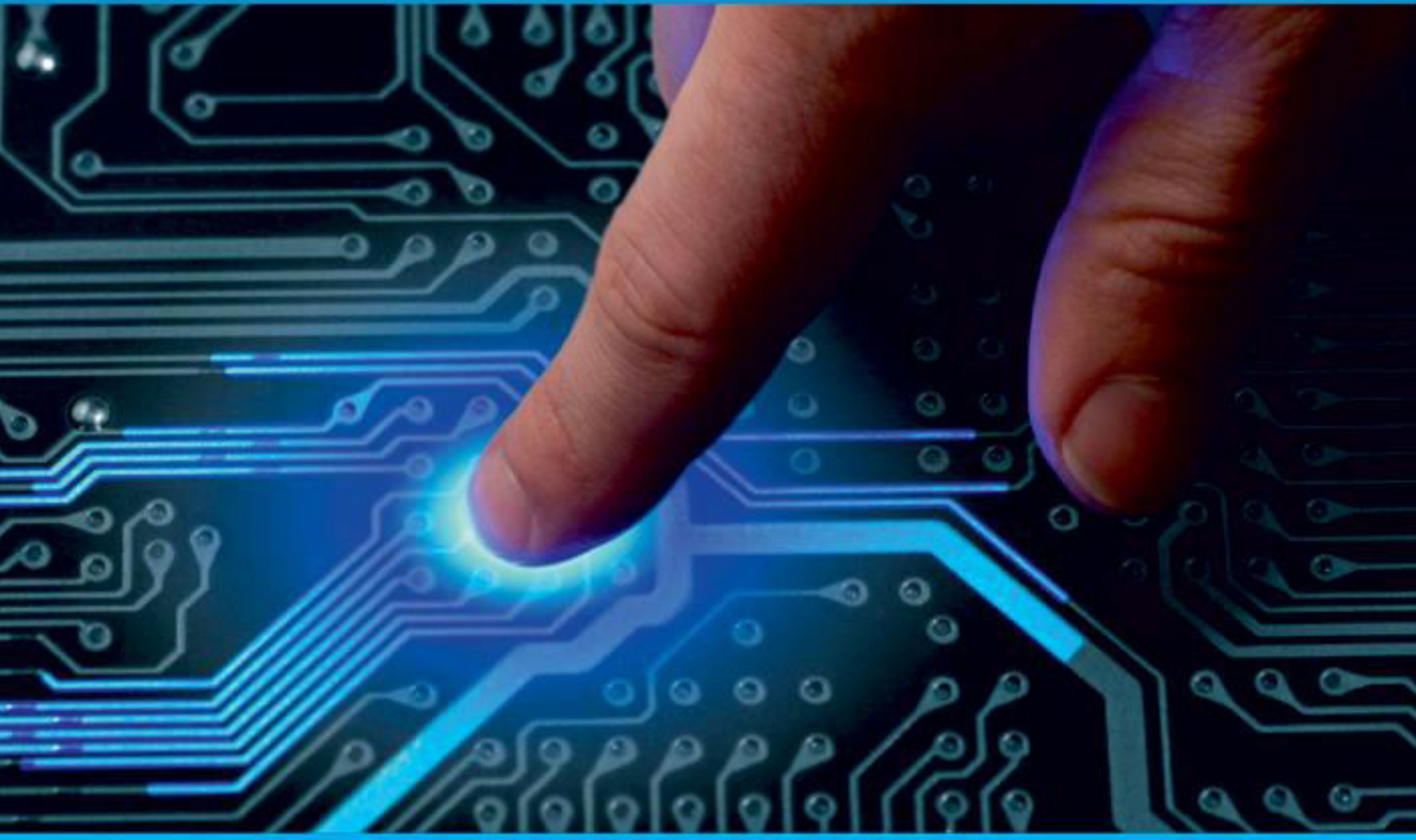
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 6, June 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

| DOI: 10.15680/IJIRCCE.2023.1206021 |

Secret Image Sharing and Fake Image Detection using Block Chain Technology

Prof. Bhoomika K S, Muskan J B, Nisarga K R, Sirisha S

Department of Computer Science & Engineering, Nagarjuna College of Engineering and Technology, Bengaluru, India

ABSTRACT: Blockchain is a new technology for sharing information and applications. Through distributed consensus, timestamping, and data encryption, it may exchange distributed information in distributed systems without requiring mutual confidence, enhancing data sharing and application performance. The big data remote monitoring imaging system can make full use of this technology, and the common node storage system of many systems can be controlled consistently and effectively to increase the system's economic efficiency. This system provides important research tools and creates a distributed architecture using blockchain technology. This system's primary goals are to identify duplicate images and reduce the blockchain's storage capacity. allows for the widespread sharing of information in dispersed systems; it functions flawlessly even in the absence of mutual trust. To increase operational efficiency, it makes use of decentralized consensus techniques, timestamping, and data encryption. Its potential integration with big data remote sensing imaging systems is especially encouraging since it makes it easier to manage storage for nodes that are shared by several systems, improving economic efficiency. This system introduces important research methodologies and is a distributed architecture pioneer using blockchain technology. Keywords: hash generation, subtraction approach, blockchain, sharing, image, and image cloud storage of remote monitoring.

I. INTRODUCTION

The amount of remote sensing data generated in our nation is increasing exponentially due to the swift advancement of aviation remote sensing technology and platforms. Separate production platforms were developed for various procurement platforms. Platforms for image sharing and remote mapping have been methodically created. They are all using centralized management. The jobs are complex and the system is large. Corresponding information is unchangeable and traceable. Both the response time and the complexity of the answer are slow. The capacity of data sharing services is significantly impacted by this type of decentralized construction and independent support, which runs counter to the development trend of data integration and widespread use. It also restricts the potential applications of remote sensing. Permissionless ness, data dependability, and decentralization are features of blockchain technology. Ensuring the security, integrity, traceability, and modification of the data exchange application process can be greatly enhanced by its application potential. The current independent support model and dispersed architecture significantly reduce the usefulness of information sharing services. This strategy goes against the current trend of widespread use and data integration, which restricts the potential advantages of remote sensing applications. In light of these difficulties, blockchain technology is showing promise as a revolutionary remedy.

Blockchain technology provides decentralization, data integrity, and failover, and has tremendous potential to enhance the security, integrity, traceability, and tamper proof of data sharing applications. By implementing blockchain, the field of remote sensing can adapt to today's trends indata management, which opens up new opportunities for innovation and maximizes the benefits of remote sensing data.

II. LITERATURE SURVEY

With cloud computing and storage services, data is not only stored in the cloud, but is routinely shared among multiple groups of users. However, it is difficult to develop an effective mechanism to verify the integrity of such shared data while maintaining identity privacy. In this paper, we propose Knox, a privacy-preserving auditing mechanism for cloud-stored data shared amongmultiple users in a group. In particular, we use group signatures to create homomorphic authenticators so that a third-party auditor (TPA) can verify the integrity of data shared by users without obtaining the entire data. At the same time, the identity of the signatory in each common data block is kept private by the TPA. With Knox, the number of users in a group does not affect theamount of data used for authentication or the time it takes to review it. Additionally, Knox uses homomorphic MACs to reduce the amount of space used to store such authentication information. Our test results show that Knox can effectively verify the correctness of data shared between multiple users.[1]

We present a simulation model of the Bitcoin peer-to-peer network, a widely used decentralized electronic currency system. The model makes it possible to estimate the feasibility and cost of attackson the Bitcoin network at the full scale of 6,000 nodes. The simulation model is based on the unmodified code of the main segments of the Bitcoin reference application, which is used by 99% of the nodes. Model parameterization is based on large-scale measurements of a real network.

We present preliminary validation results that show a reasonable agreement of message propagation in the Bitcoin network compared to simulation results. We use the model to study the feasibility of a network fragmentation attack and show that the attack is sensitive to the turnover of the attackingnodes[2]

Both the public and business sectors are currently embracing the technology. In addition, we are witnessing the emergence of the Internet of Things due to advancements in hardware and software. Additionally, there needs to be synchronization and communication between various IoT devices. However, we anticipate that there might be some restrictions and synchronization issues when utilizing the present server-client approach in scenarios where more than hundreds or tens of thousands of IoT devices are connected. Therefore, we suggest building an Internet of Things system using blockchain technology. Blockchain enables us to manage and set up Internet of Things devices.

RSA public key cryptosystems are used to handle keys; private keys are kept on individual devices while public keys are kept on Ethereum. We specifically selected Ethereum as our blockchain platform since we can create our own Turing-complete code for Ethereum to run on it thanks to its smart contract. This makes it simple for us to establish a key management system and control how IoT devices are configured. Despite the fact that most blockchain platforms allow us to use the account just as a key management system, we still go with Ethereum since we have more sophisticated control over the system. Instead of using a comprehensive IoT system with thousandsof IoT devices, we employ a small number of IoT devices as a proof of concept. But in our further investigation, we hope to use blockchain technology to construct a comprehensive Internet of Thingssystem.[3]

III. SYSTEM DESIGN & MODELING

4.1 System architecture

A WebApp application's overall hypermedia structure is identified by its system architecture. The objectives established for the WebApp, the information to be displayed, the visitors' users, and the developed navigation philosophy are all referred to as architectural design. Content items' display and navigational structures are the main emphasis of content architecture. The framework of an application to control user interaction, perform internal processing, affect navigation, and display content is known as WebApp architecture. The framework of the development environment, where the application has to be implemented, defines the WebApp architecture.

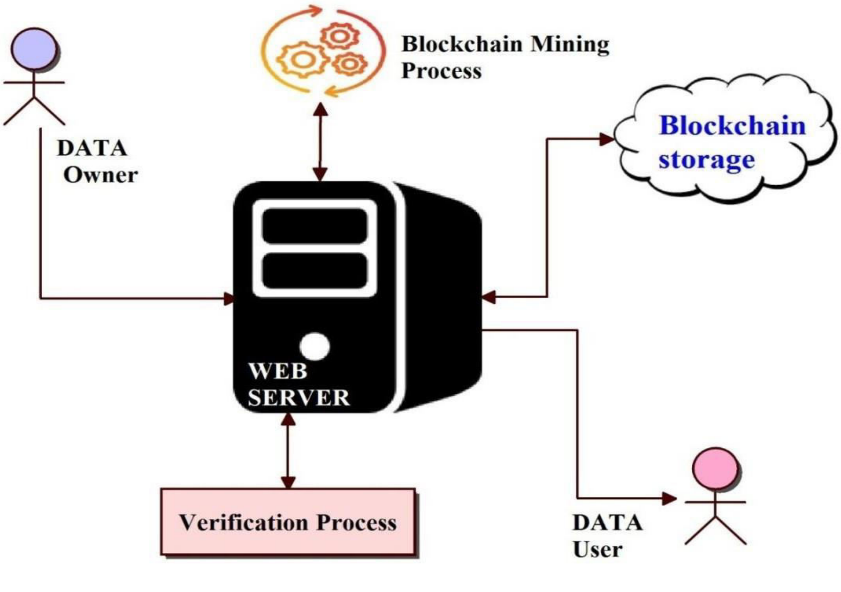


Fig 4.1: System architecture

4.2 USE CASE DIAGRAMSA

A use case is a collection of hypothetical situations that explain how a source and a target interact. The relationship between actors and use cases is depicted in a use case diagram. Use cases and actorsare the two primary parts of a use case diagram. The use case diagrams are displayed in the picture below.

USE THE DATA REQUIRER OF THE CASE DIAGRAM

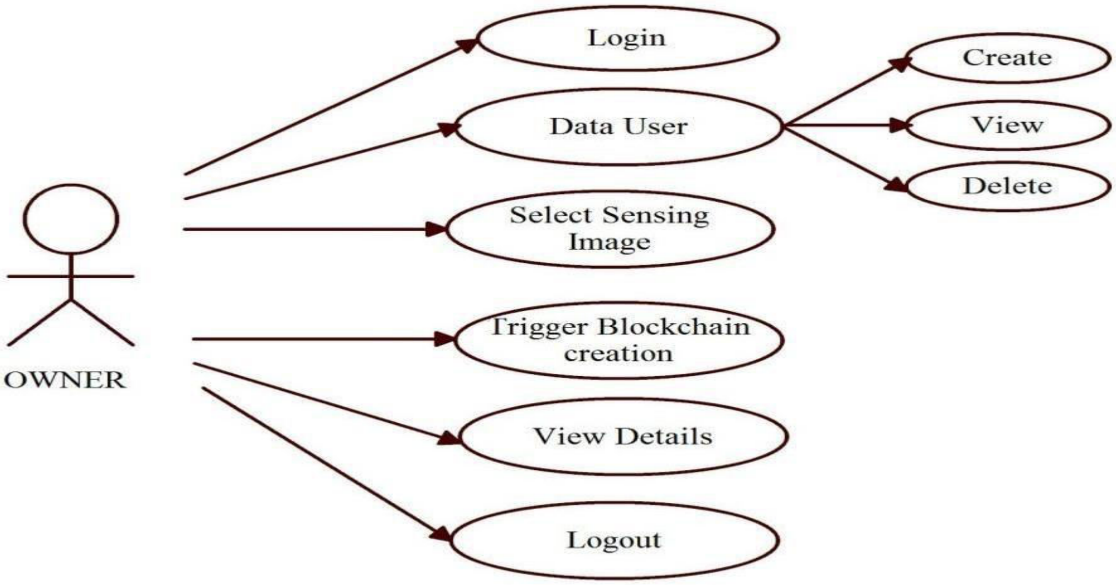


Fig 4.2: Use Case Diagram for Data Owner

Use Case Diagram for User

A total of nine use cases and an act, or named data user, are depicted in the use case diagram belowFigure 4.3. A user can log in to the portal, and a data user can create an account, view an account, and when an account is deleted, choose a self-identification image to upload and run the blockchain. He can also view account information and log out of the portal.

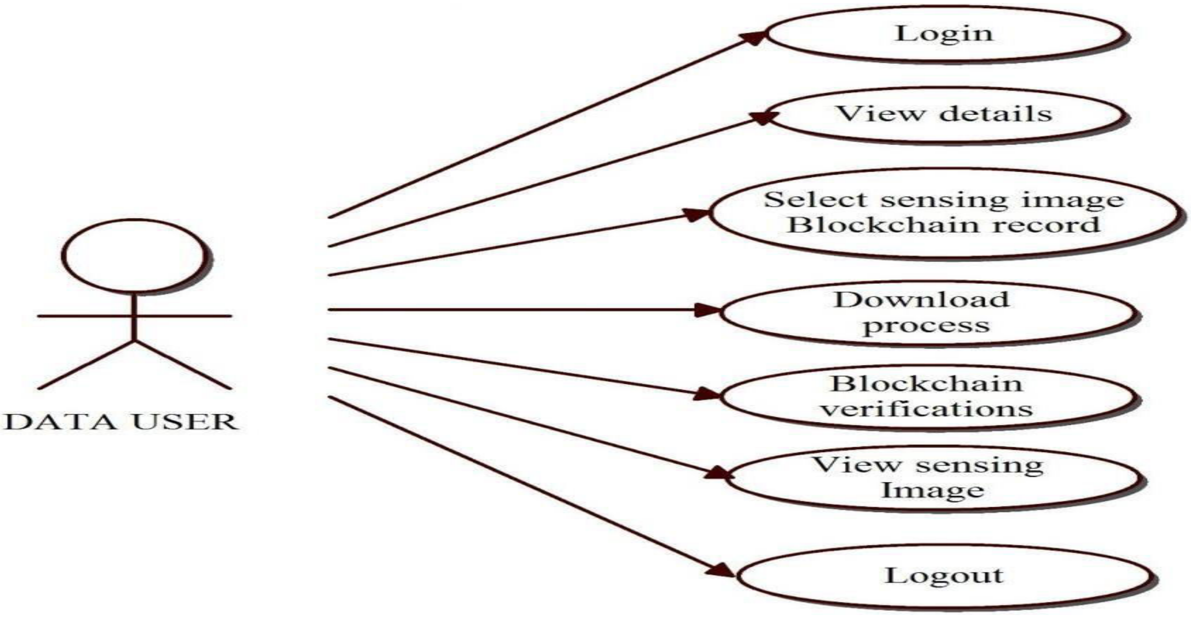
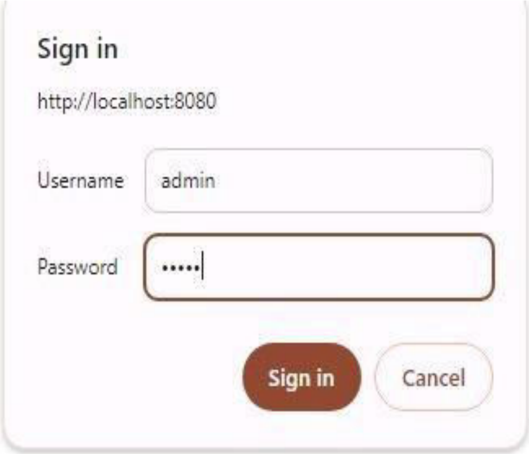


Fig 4.3: Use Case Diagram for User

V. RESULTS

The outcome, whether presented in a qualitative or quantitative manner, is the culmination of actionsor occurrences. A functional analysis, performance analysis is a collection of fundamental quantitative relationships between performance factors.



Sign in

http://localhost:8080

Username: admin

Password: •••••

Fig 5.1: Sign in to Localhost

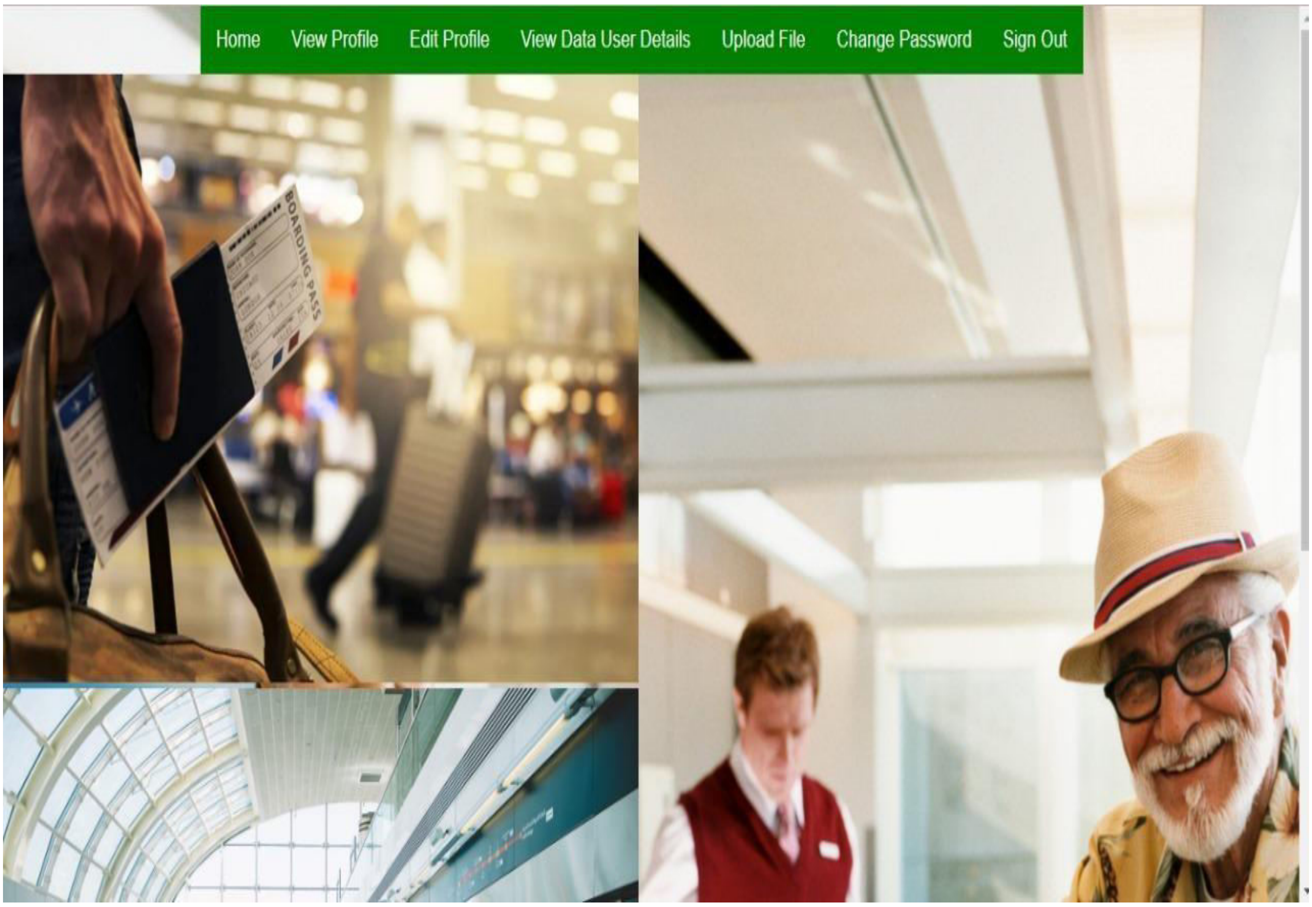
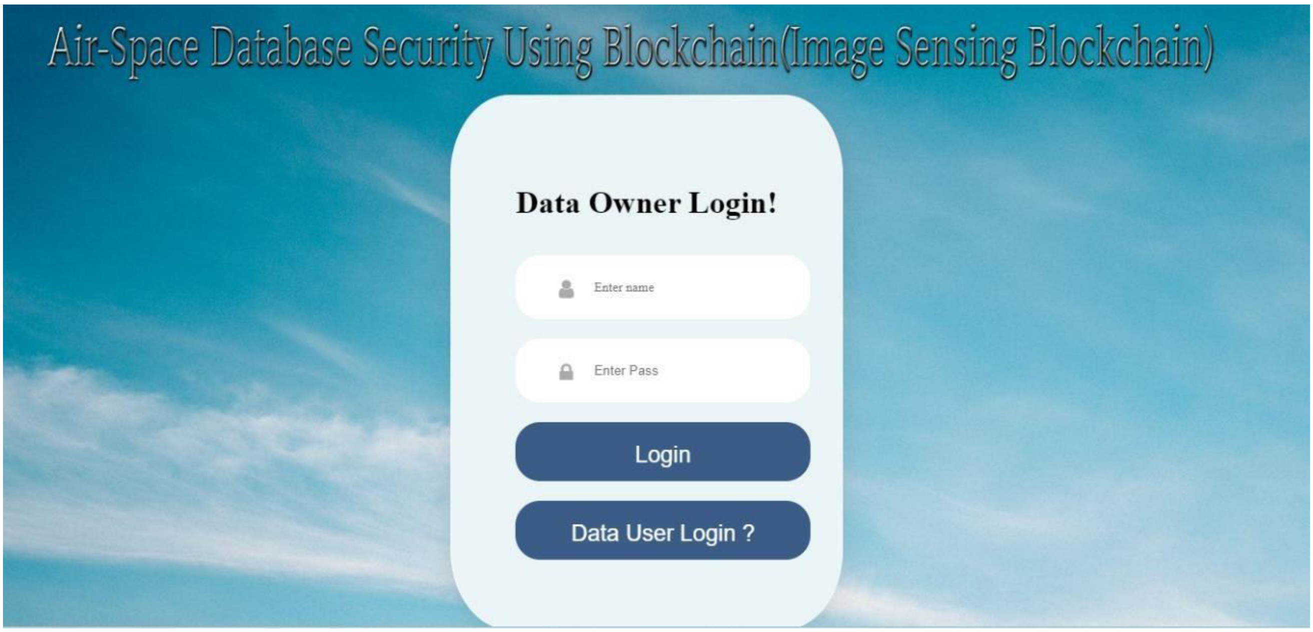


Fig 5.2: Home Page

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 6, June 2024 ||

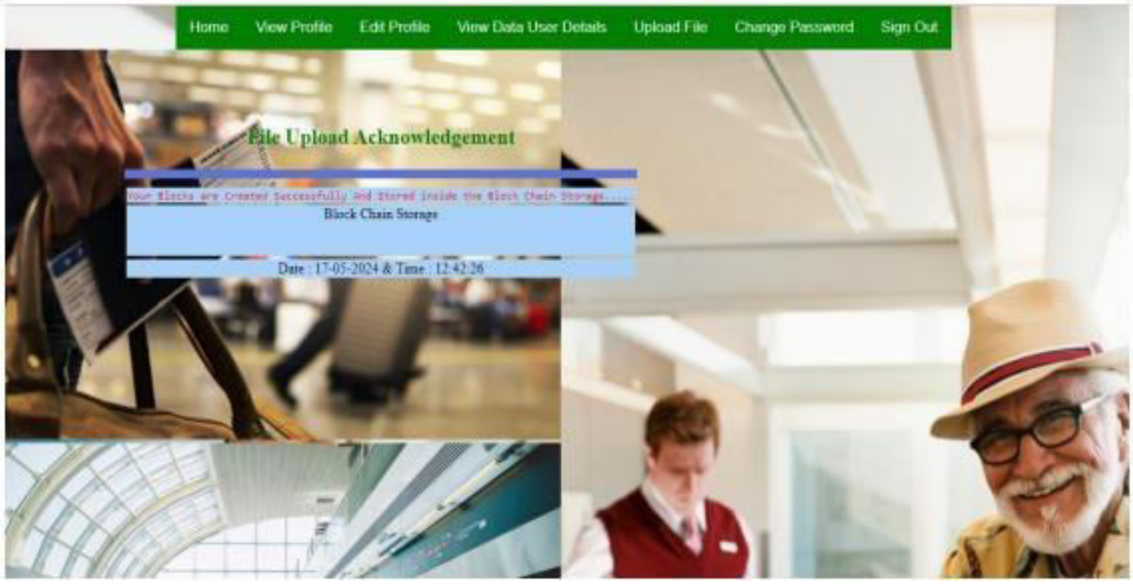
| DOI: 10.15680/IJIRCCE.2023.1206021 |



Air-Space Database Security Using Blockchain(Image Sensing Blockchain)

Data Owner Login!

Fig 5.3: Data Owner Login



File Upload Acknowledgement

Your Blocks are Created Successfully And Stored inside the Block Chain Storage....

Block Chain Storage

Date : 17-05-2024 & Time : 12:42:26

5.4: User Image Upload

The user uploads an image file by choosing it in their upload file and clicking the "send" button. Thefile name, date, and time will be shown as seen in Fig. 5.4 after the file has been loaded.

VI. CONCLUSION

Using data encryption, time-stamping and decentralized consensus mechanisms, blockchain improves the efficiency and reliability of data management. Especially in the context of large remote sensing imaging systems, blockchain can facilitate the creation of a distributed node storage system for the system, which improves economic efficiency. The proposed system aims to design a distributed blockchain-based architecture, focusing on key research technologies to detect duplicate images and minimize the storage space of the blockchain network. It highlights the transformative impact of blockchain in optimizing resource utilization and data integrity in complex information ecosystems.

REFERENCES

1. Wang B, Li B, Li H. Knox: Private Preserving Audit for Shared Data with Large Groups see in the Cloud [C]// International Conference on Applied Cryptography and Network Security. Sprinter-Publishers, 2012:507-525.
2. Till N, Philipp A, Hannes H. Simulation of Bit coin peer-to-peer transactions according to current analysis[C]// Ieee/ifip Labor Content for Security by Emerging Distributed Challenge Technology. 2015:1327-1332.
3. Swan M. Blockchain: Blueprint for the New Economy [M]. O'Reilly Media, Inc. 2015