International Journal of Multidisciplinary Engineering in Current Research - IJMEC
Volume 8, Issue 12, December-2023, http://ijmec.com/, ISSN: 2456-4265

ENHANCING SECURITY OF DATA IN CLOUD STORAGE USING DECENTRALIZED BLOCK CHAIN

CHINNALAXMANI VANI, Mrs. M. ANUSHA

[1]B.tech Student, Department Of Electronics and Computer Engineering, J.B Institute of Engineering and Technology

[1]Assistant Professor, Department Of Electronics and Computer Engineering, J.B Institute of Engineering and Technology

Abstract: Nowadays, large amount of data is stored on the cloud which is required to be protected from the unauthorized users. To maintain the privacy and security of data various algorithms are used. The objective of every system is to achieve confidentiality, integrity, availability (CIA). However, the existing centralized cloud storage lacks to provide these CIA properties. So, to enhance the security of data and storing techniques, decentralized cloud storage is used along with blockchain technology. It effectively helps to protect data from tampering or deleting a part of data. The data stored in blockchain is linked to each other by a chain of blocks. Each block has its hash value, which is stored in next block. For this purpose, SHA-512 Hashing algorithm is used. Hashing algorithm is used in many aspects, where the security of data is required such as message, password verification, digital certificates and in blockchain. By the combination of these methods and algorithms, data becomes more secure and reliable. However, with the help of various algorithms, the security of the data can be enhanced. Also, Advance Encryption Standard (AES) is used to encrypt and decrypt the data due to the significant features of this algorithm.

I. INTRODUCTION

Data security, integrity, and trust in cloud computing can be significantly enhanced by implementing decentralized blockchain technology. By using consensus mechanisms and hashing algorithms, the system can protect against unauthorized access, tampering, and modifications, ensuring data anonymity and transparency. Additionally, blockchain's ability to track and audit transactions promotes transparency and accountability in the cloud computing environment. Furthermore, its decentralized nature offers enhanced resilience against potential cyber threats. However, it is important to note that the choice of blockchain architecture, such as permissioned or permissionless, public or private, will depend on the specific requirements and objectives of the cloud computing system. By carefully designing the architecture, organizations can maximize the benefits of blockchain technology while minimizing potential challenges and vulnerabilities.

The problem statement can be broken down into key components:

a. Data Security: The primary objective is to enhance the security of data stored in cloud storage. This includes safeguarding against unauthorized access, data breaches, and data corruption.

b. Decentralization: Implementing a decentralized blockchain network to ensure that data is not stored on a single centralized server but distributed across a network of nodes, making it more resilient to attacks.

c. Data Integrity: Ensuring data integrity by implementing mechanisms such as cryptographic hashing and digital signatures to verify the authenticity and integrity of data stored in the blockchain.

d. Access Control: Implementing robust access control mechanisms to allow only authorized users or entities to access and modify the stored data.

e. Privacy Protection: Protecting the privacy of data owners by implementing privacy-preserving techniques, such as zero-knowledge proofs or encryption, to ensure that sensitive information remains confidential.

II. LITERATURE SURVEY

Data breaches and privacy violations have become a major concern in cloud computing. While traditional methods of securing data rely on centralized servers, they are increasingly susceptible to cyberattacks. In response, researchers have explored decentralized blockchain technologies as an alternative approach to enhance security in cloud computing. The integration of blockchain technology with cloud computing presents a promising solution to address the security challenges faced by the latter. By leveraging the inherent decentralization and cryptographic security of blockchain, organizations can ensure data integrity and confidentiality while also maintaining the scalability and efficiency of cloud computing services.

Cloud storage has become increasingly popular in recent years due to its convenience and accessibility. However, it also poses significant security risks, as sensitive data can be accessed by unauthorized parties if not properly protected. The existing literature on data security in cloud storage has identified various vulnerabilities and proposed different solutions to address them. One common approach is to use encryption techniques to protect data while it is being stored or transmitted. Another approach is to use access control mechanisms to restrict the users who can access the data.

Blockchain technology has emerged as a potential solution for enhancing the security of data in cloud storage. The decentralized nature of blockchain makes it difficult for hackers to tamper with the data, as any changes made to the data would be immediately visible to all participants in the network. Additionally, the use of smart contracts can automate the enforcement of access control policies, reducing the risk of human error. However, the literature also highlights some limitations of using blockchain for data security, such as scalability issues and the high computational costs of performing cryptographic operations on the blockchain.

III. ANALYSIS

3.1 Introduction

We have conducted experiments on our collected dataset and extensive results have demonstrated that our model outperforms all other existing models. In the future, we will investigate more tasks under this framework, such as event summarization and event attribute mining in social media.

IV. DESIGN

4.1 Introduction

Design Engineering deals with the various UML [Unified Modelling language] diagrams for the implementation of project. Software design is a process through which the requirements are translated into representation of the software. Design is the place where quality is rendered in software engineering. Design is the means to accurately translate customer requirements into finished product.

4.2 UML diagrams

4.2.1 Use Case Diagrams

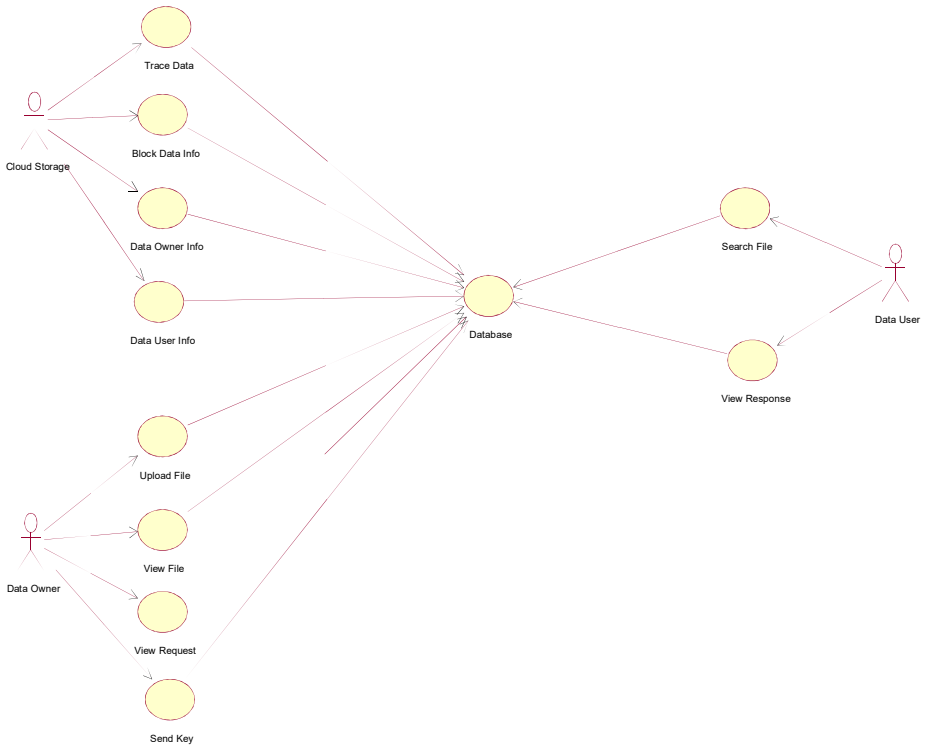

Fig: 4.2.1

EXPLANATION:

The main purpose of a use case diagram has an actor has a data owner and data users. Data owners has a perform a upload a file. it will view a own files. Data owner has a view requests from the users. Data owner can also sends a keys. Data user has a search a files. Data users can also view response of the owner. Data user has a encrypt a data. Data user has a file key request and then file it has a download. Cloud has a stored data it will have a trace and blocks a data.

4.2.2 Class Diagram

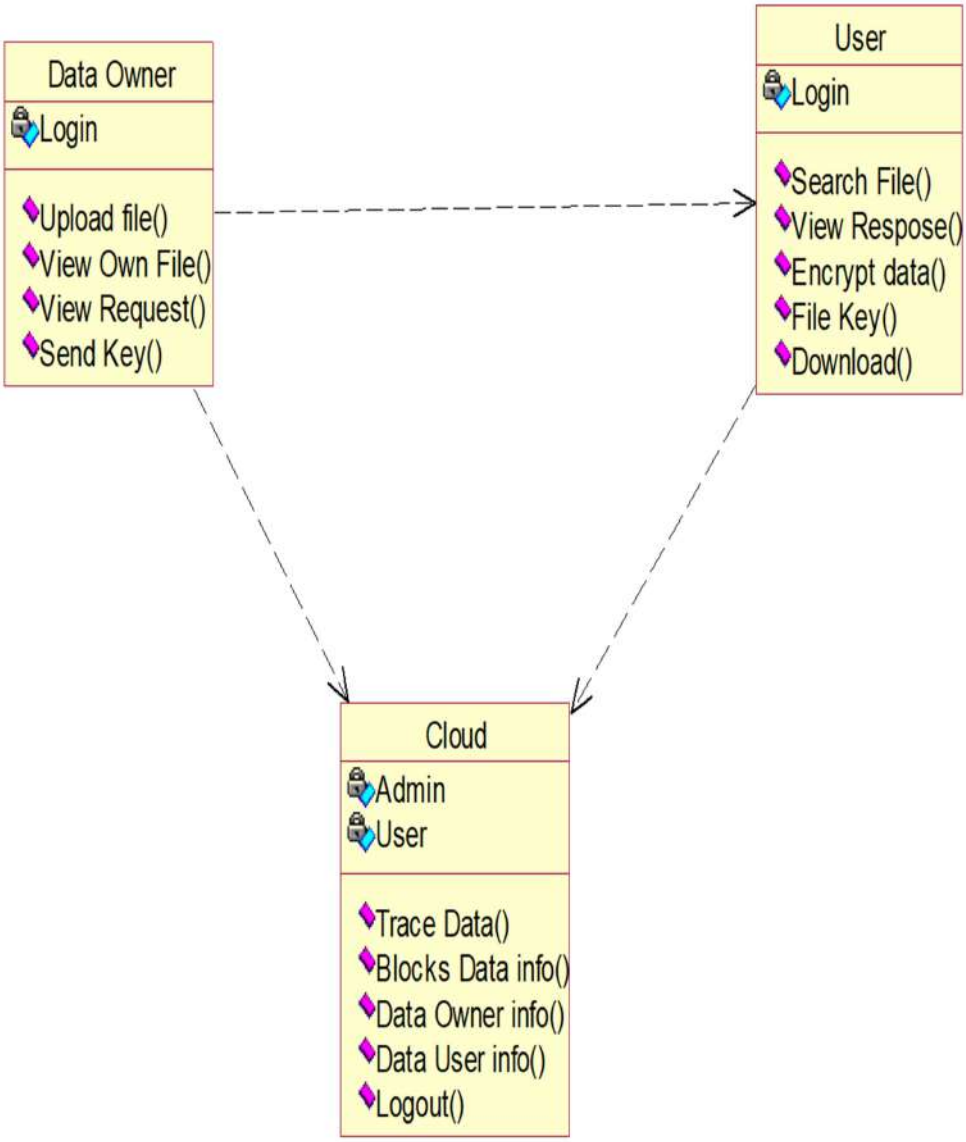

Fig: 4.2.2

EXPLANATION:

In this class diagram represents data owner has a class it has a attributes and operations performs in the cloud. User has the attributes it was also have operations search file view responses and it will have a encrypt data. It has file keys to download owner data. In cloud has a trace and blocks a data information.

4.2.3 Sequence Diagram:

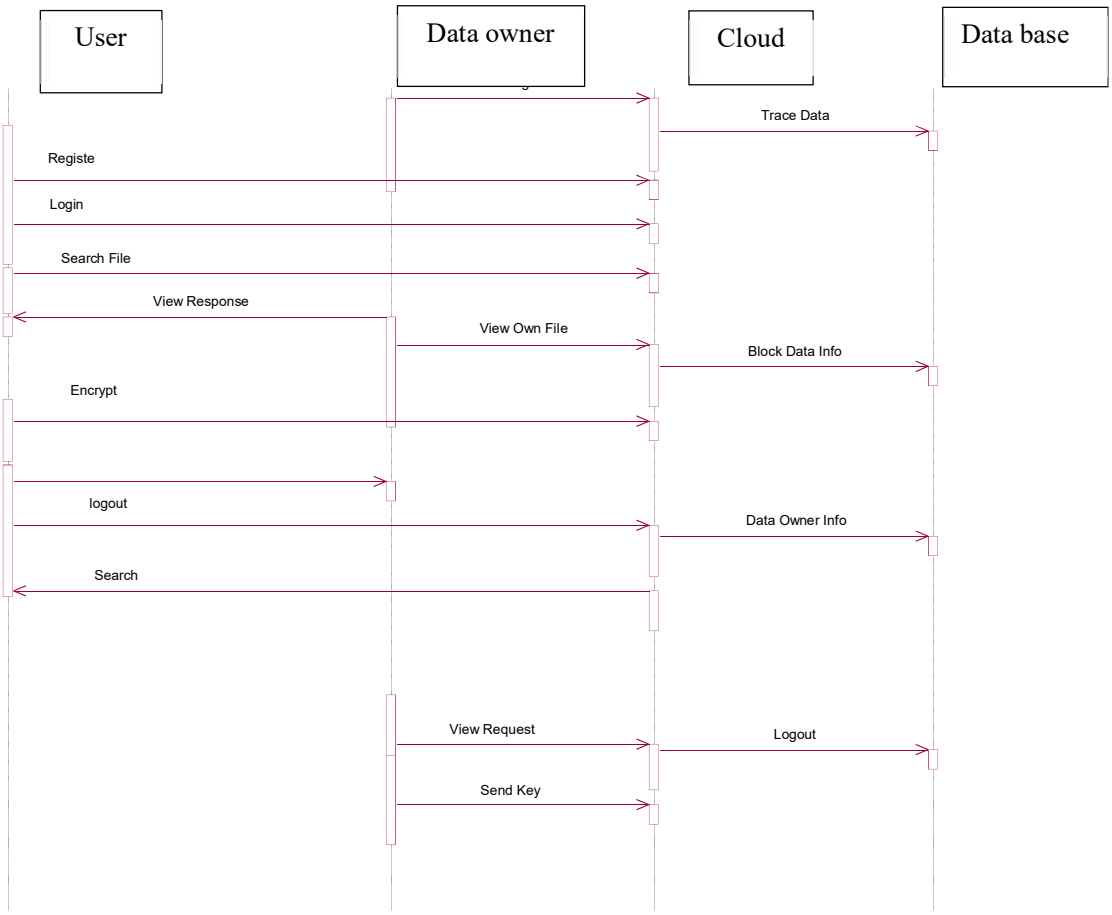

Fig: 4.2.3

EXPLANATION:

Sequence diagrams are graphical representations user has a register and login. Data user has a search files. Data users can also view response of the owner. Data user has a encrypt a data. Data user has a file key request and then file it has a download. Data owner has a register and then login. Data owners has a perform a upload a file. it will view own files. Data owner has a view a request from the users. Data owner can also sends a keys. Cloud has a stores a data it will have a trace and blocks a data. All information has a gather at a cloud storage database.

4.2.4 Activity Diagram:

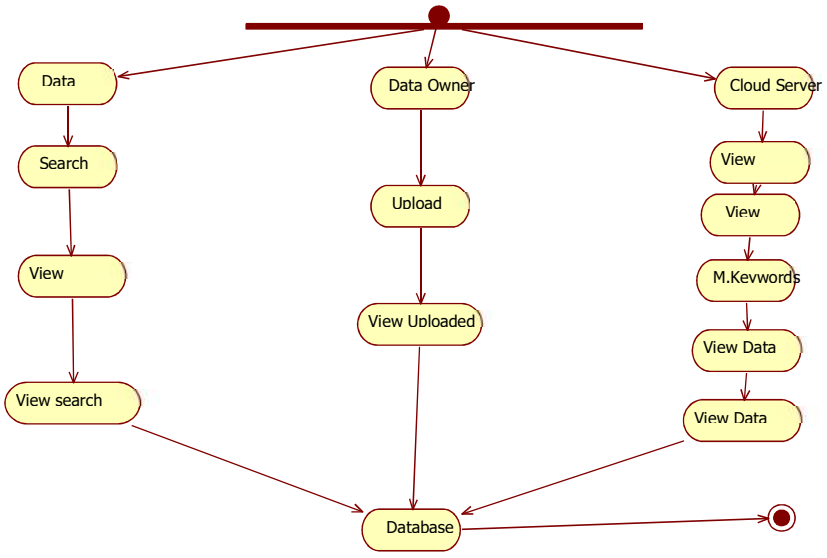

Fig: 4.2.4

4.2.5 State Diagram:

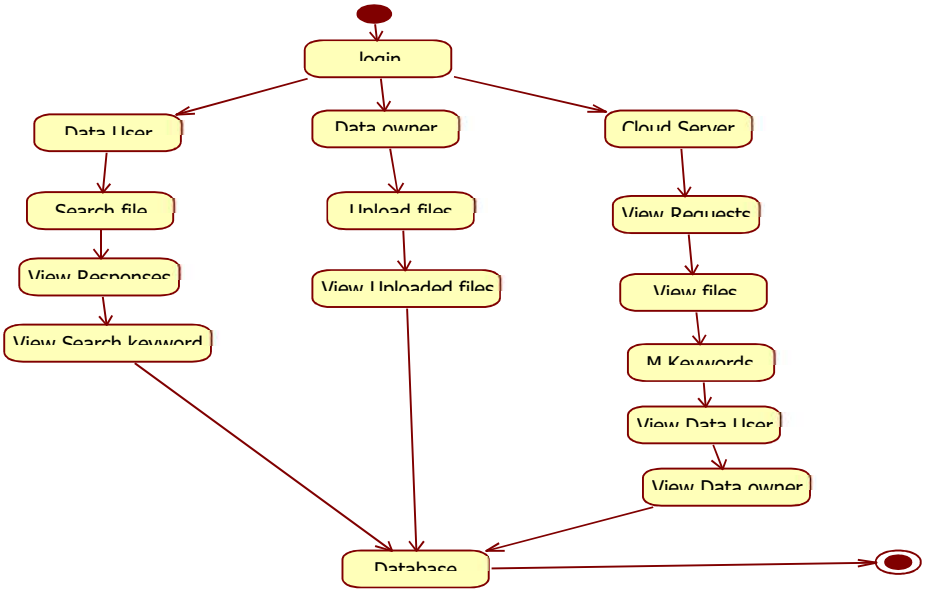

Fig:4.2.5

EXPLANATION:

State diagram are a loosely defined diagram to show workflows of stepwise Data user has a search a files. Data users can also view response of the owner. Data user has a encrypt a data. Data user has a file key requests and then file it has a download. Data owner has a register and then login. Data owners has a perform a upload a file. it will views a own files. Data owner has a view a requests from the users. Data owner can also sends a keys. Cloud has a stores a data it will have a trace and blocks a data. It has a gathers at a database.

V. Output Screens

Fig: 5.4.1 Home Page

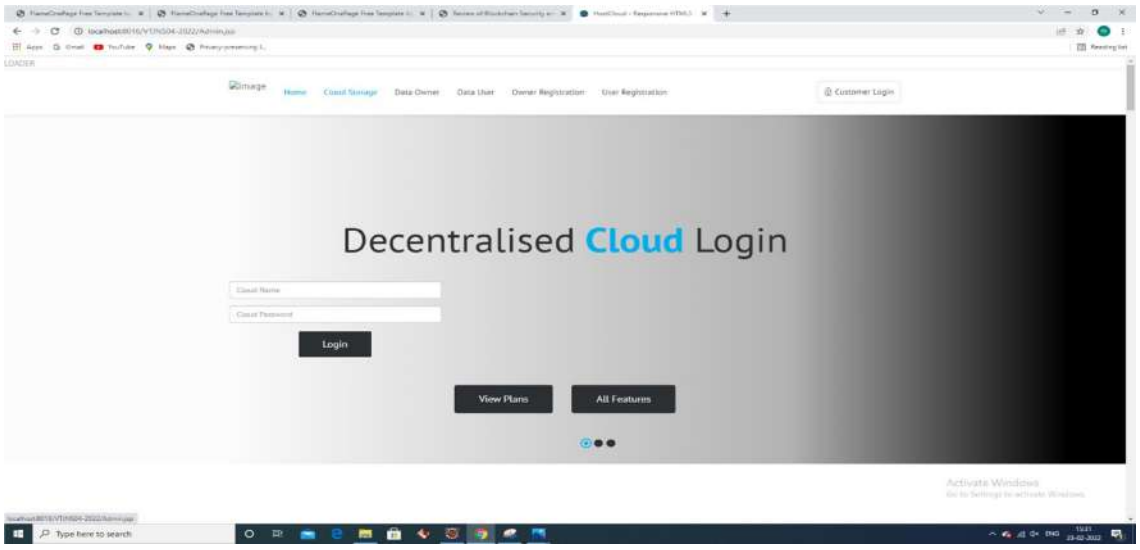

Fig:5.4.2 Cloud Login Page

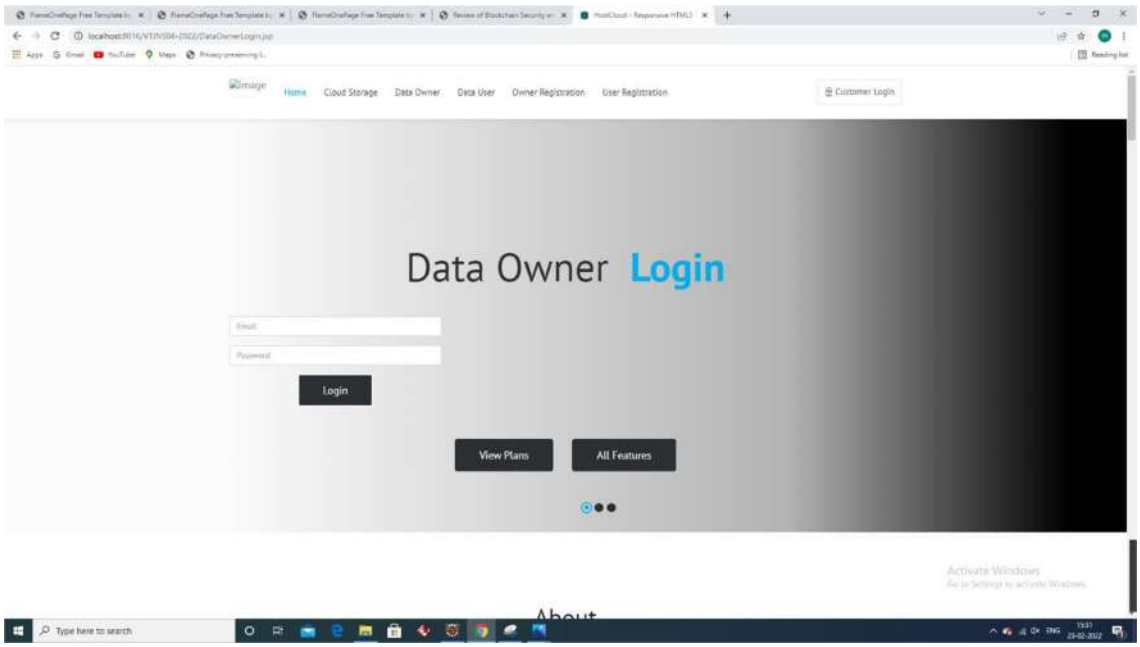

Fig: 5.4.3 Data Owner Login Page

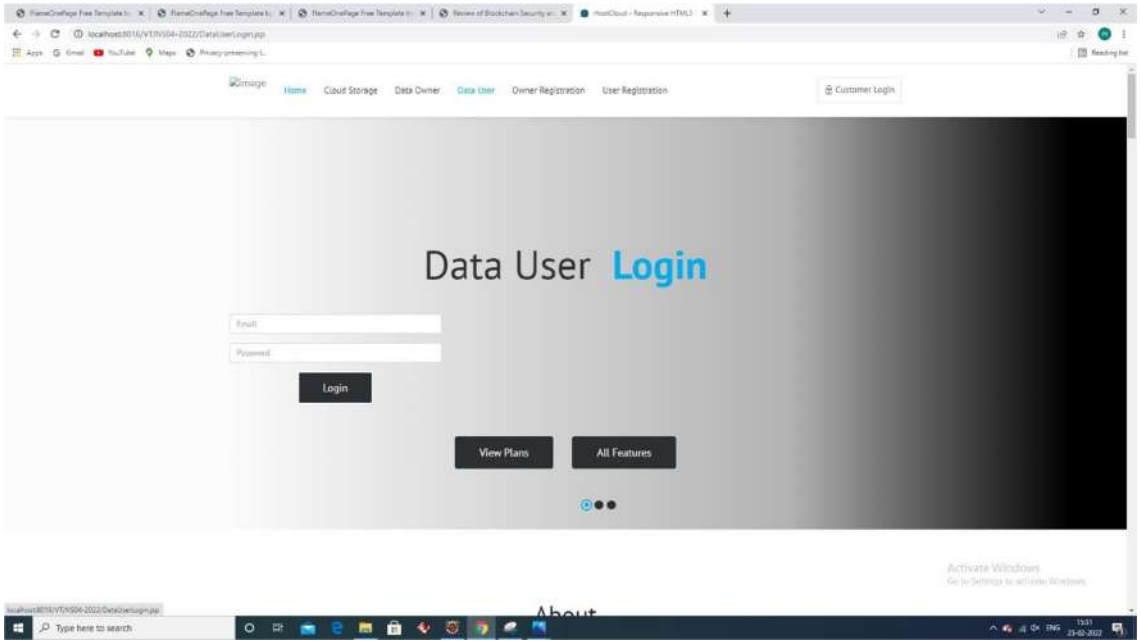

Fig: 5.4.4 Data user Login

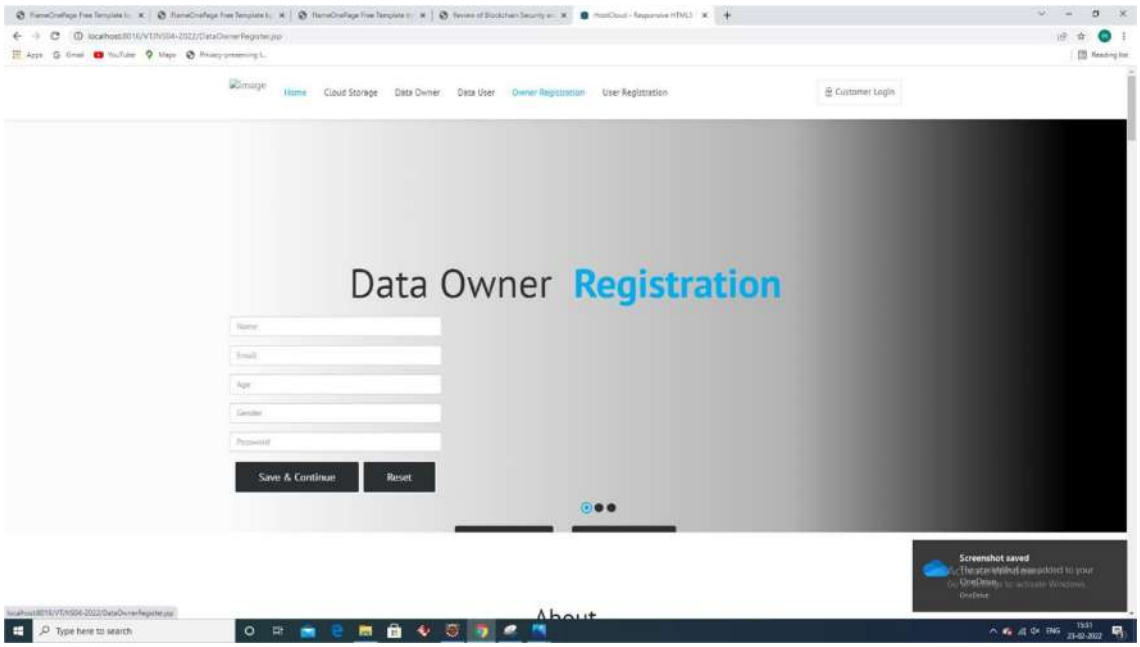

Fig: 5.4.5 Data Owner Registration page

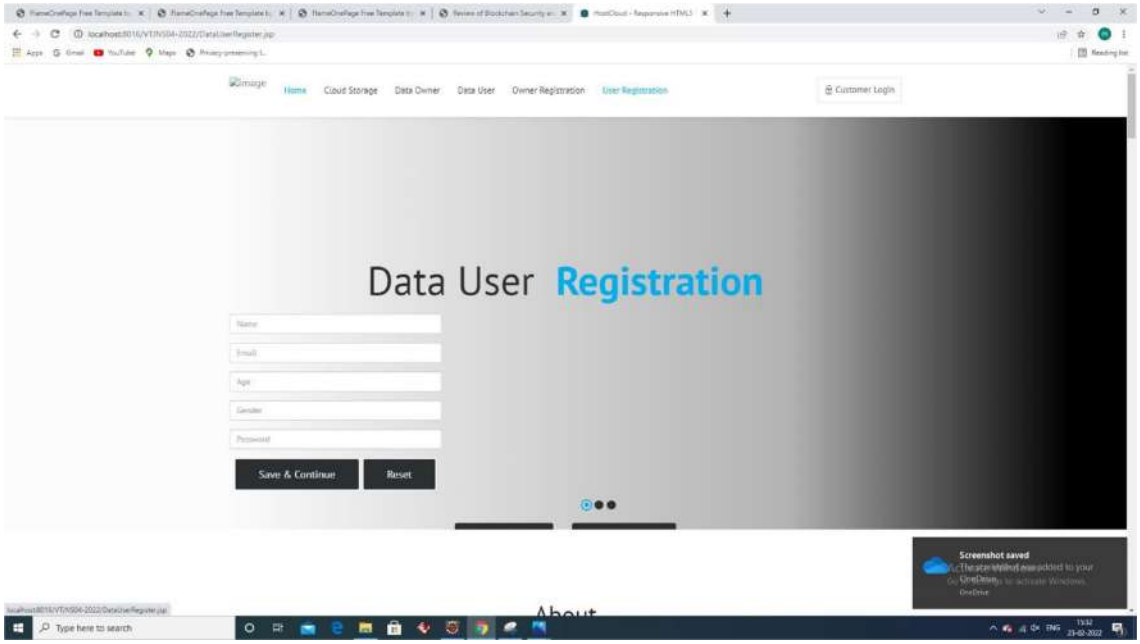

Fig: 5.4.6 Data user Registration page

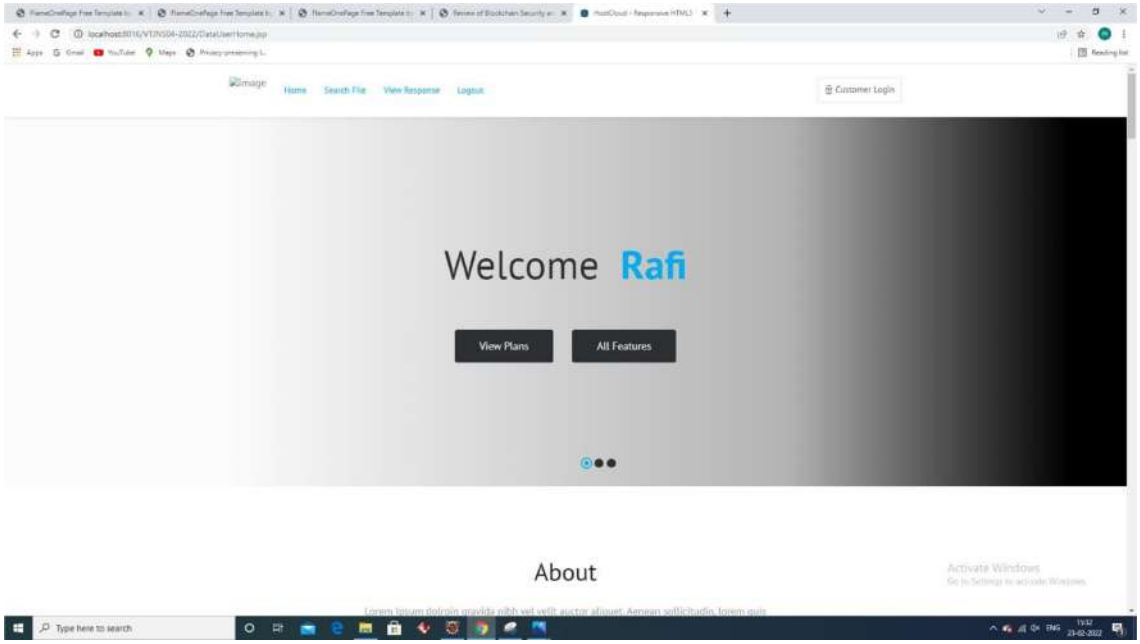

Fig: 5.4.7 Data user Home page

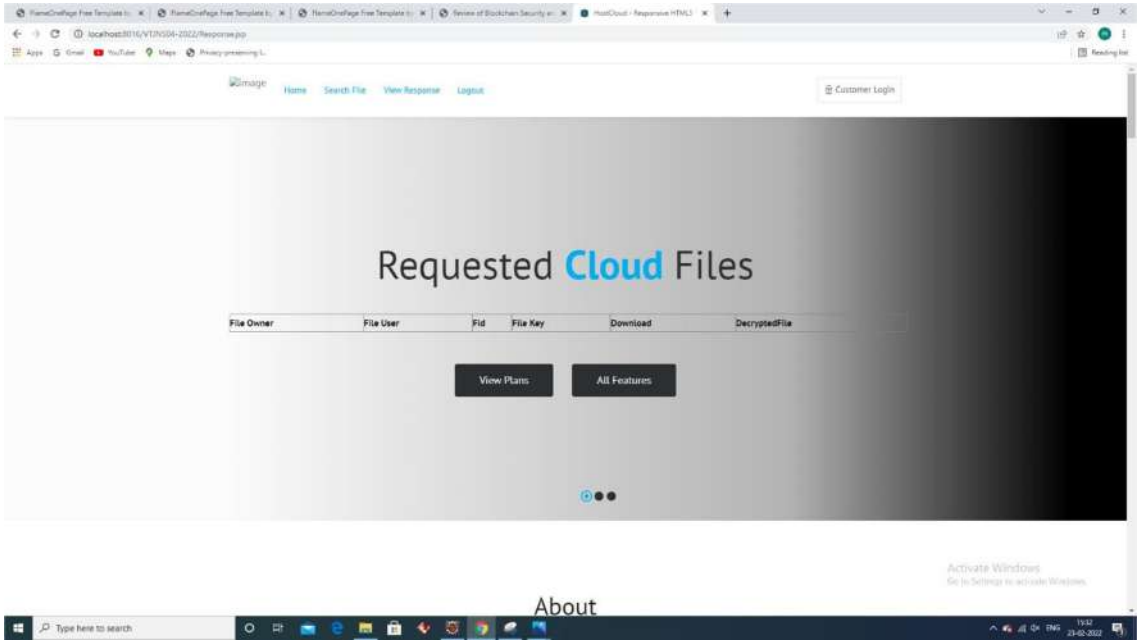

Fig:5.4.8 Data User Cloud files Login page

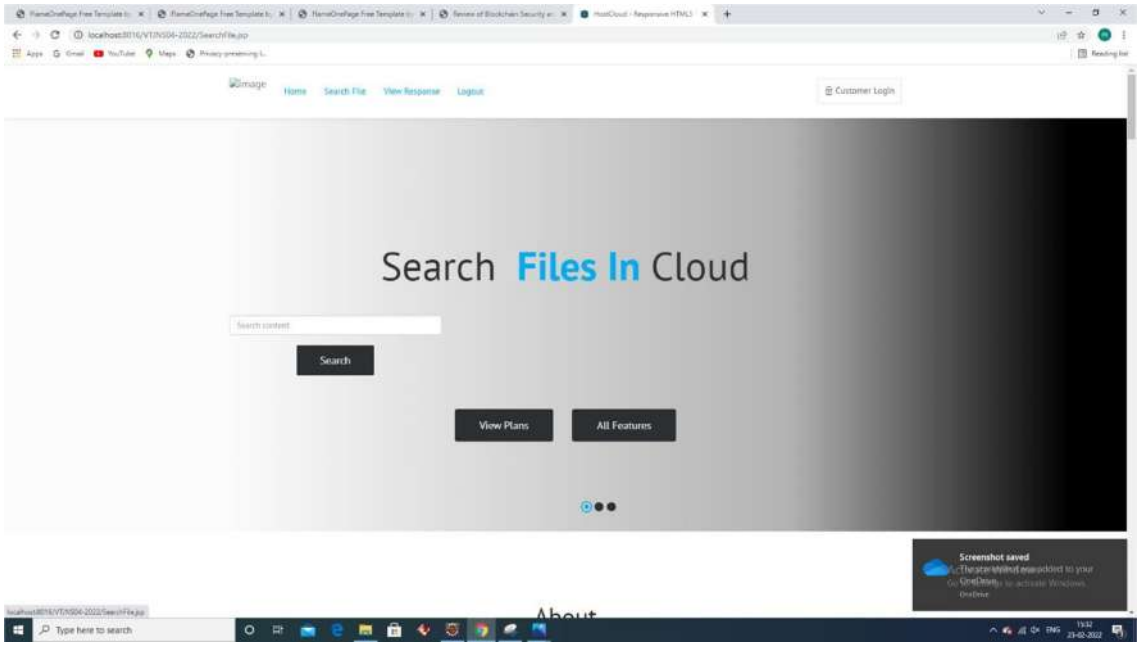

Fig: 5.4.9 Data User Search page

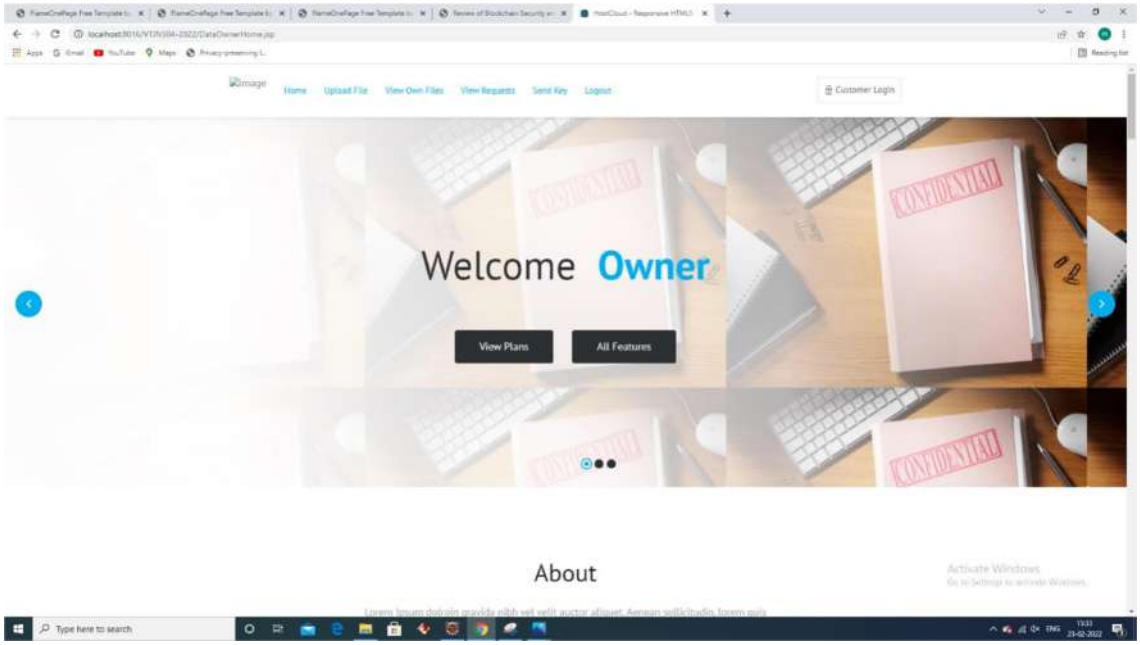

Fig: 5.4.10 Data Owner Home page

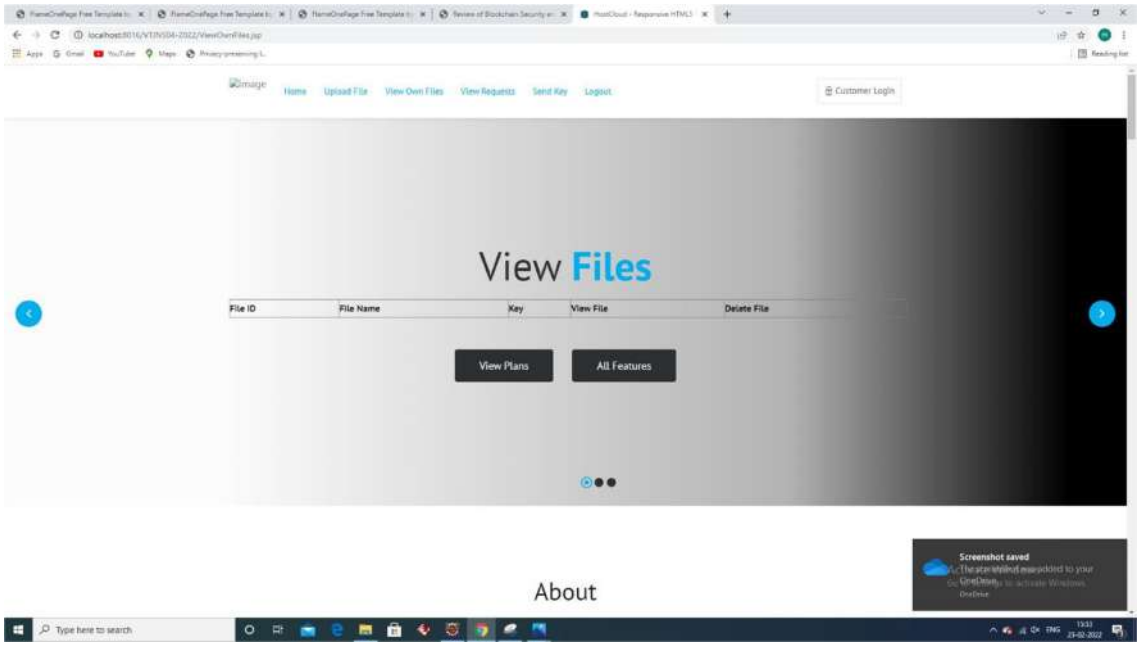

Fig: 5.4.11 Data Owner View Files Login page

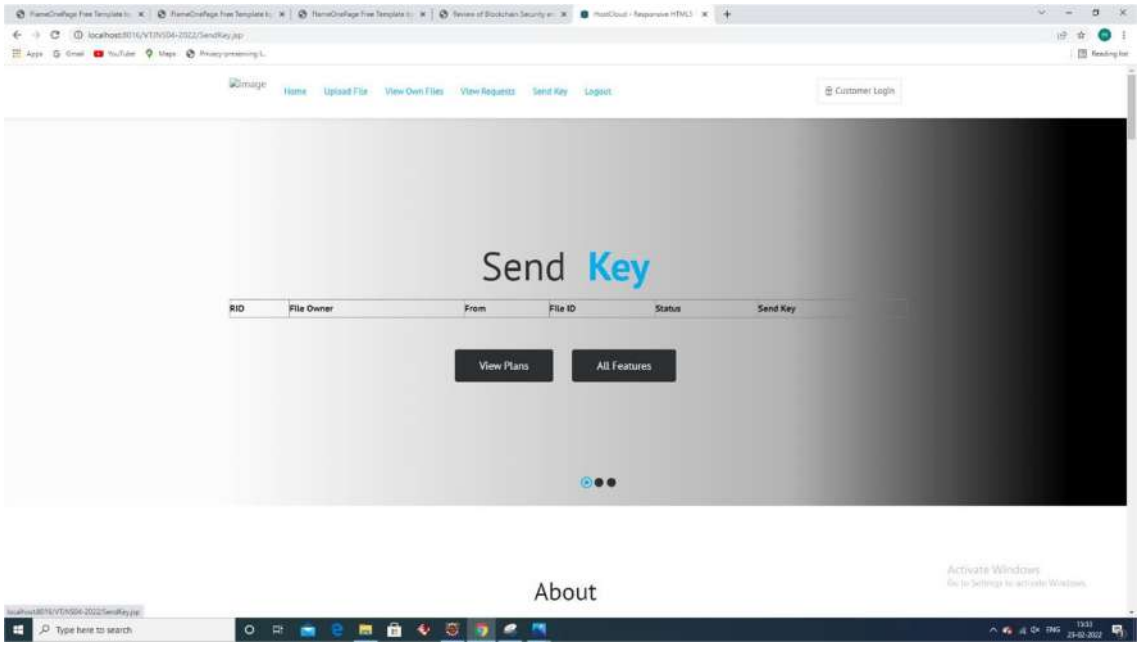

Fig: 5.4.12 Data Owner Send Key page

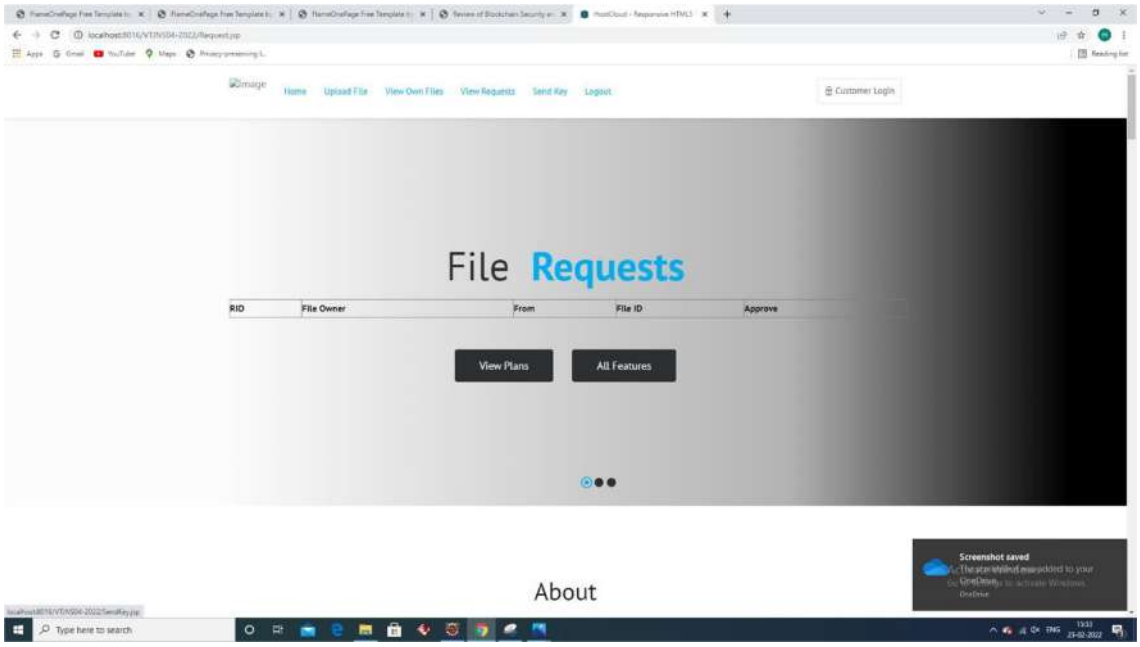

Fig: 5.4.13 Data Owner File Request page

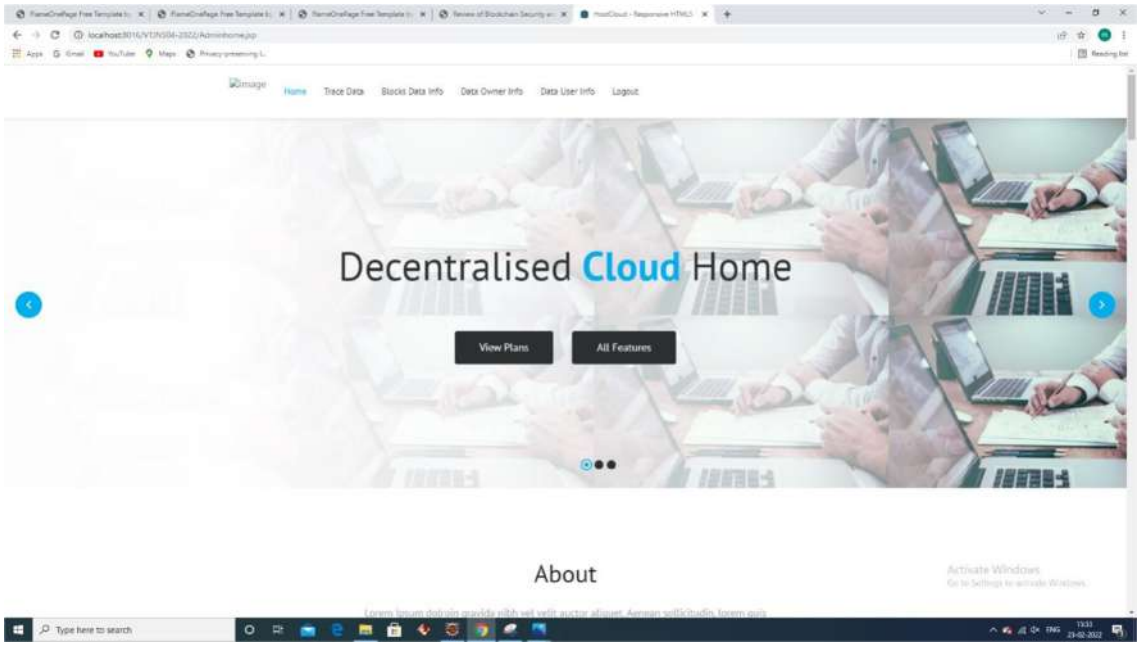

Fig: 5.4.14 Decentralised Cloud Home page

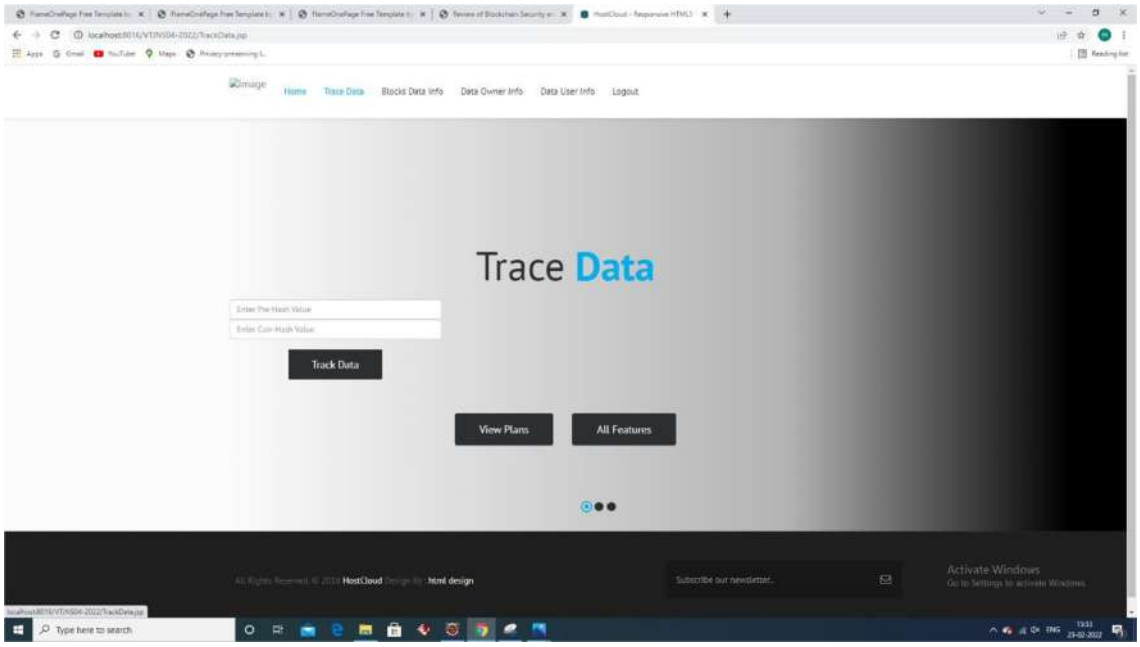

Fig: 5.4.15 Trace Data page

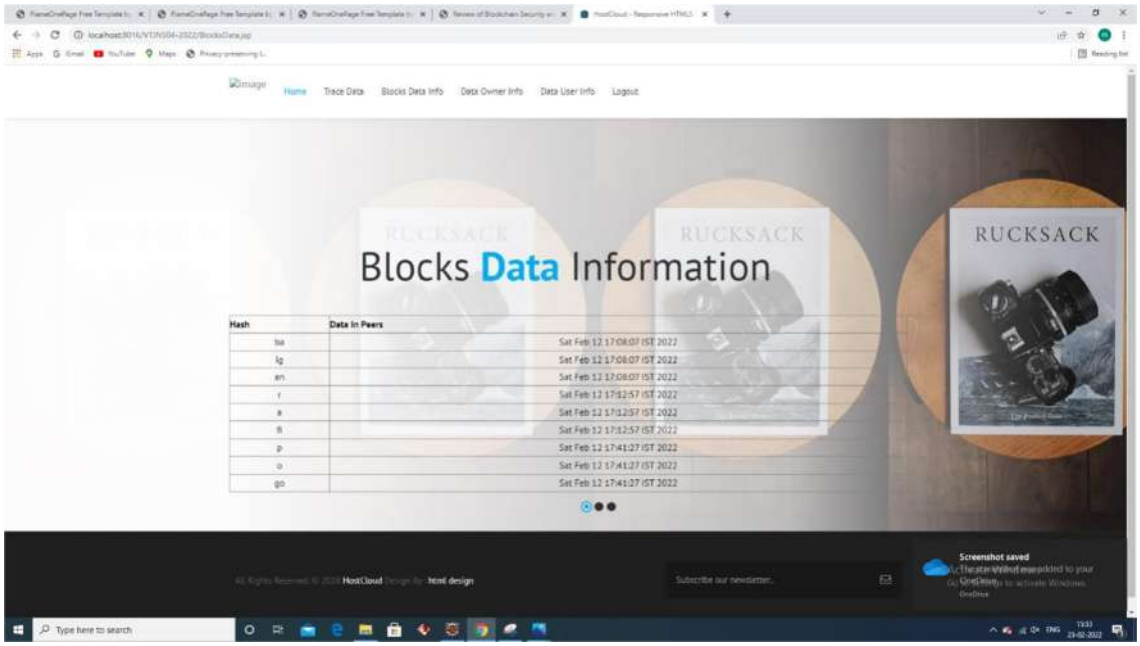

Fig: 5.4.16 Block Data page

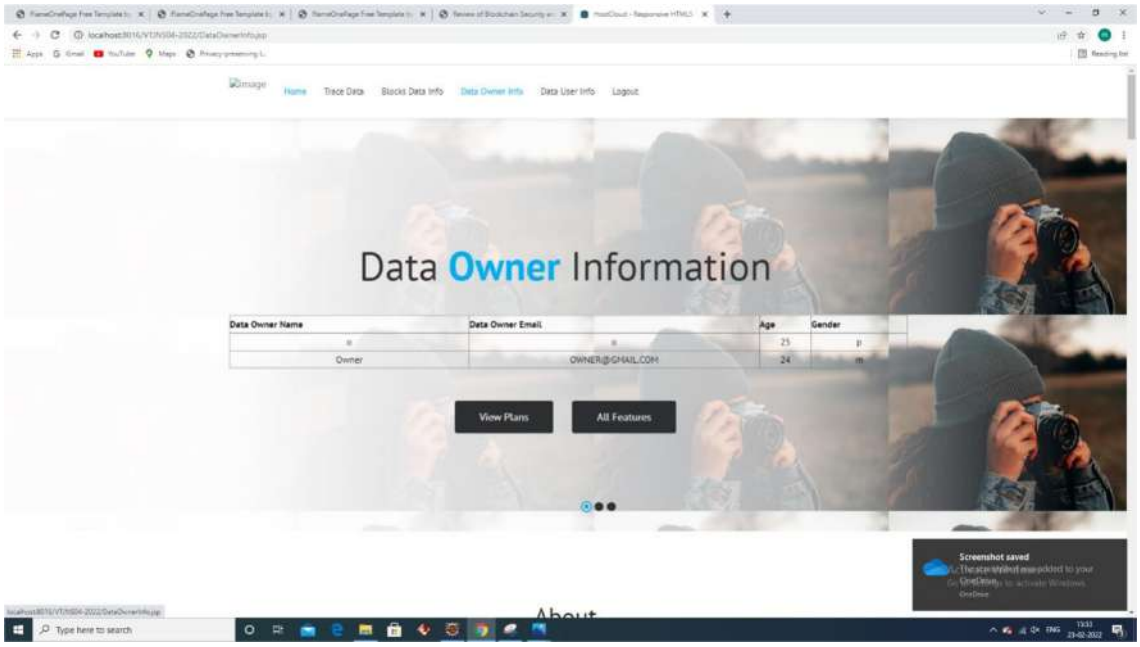

Fig: 5.4.17 Data Owner Information page

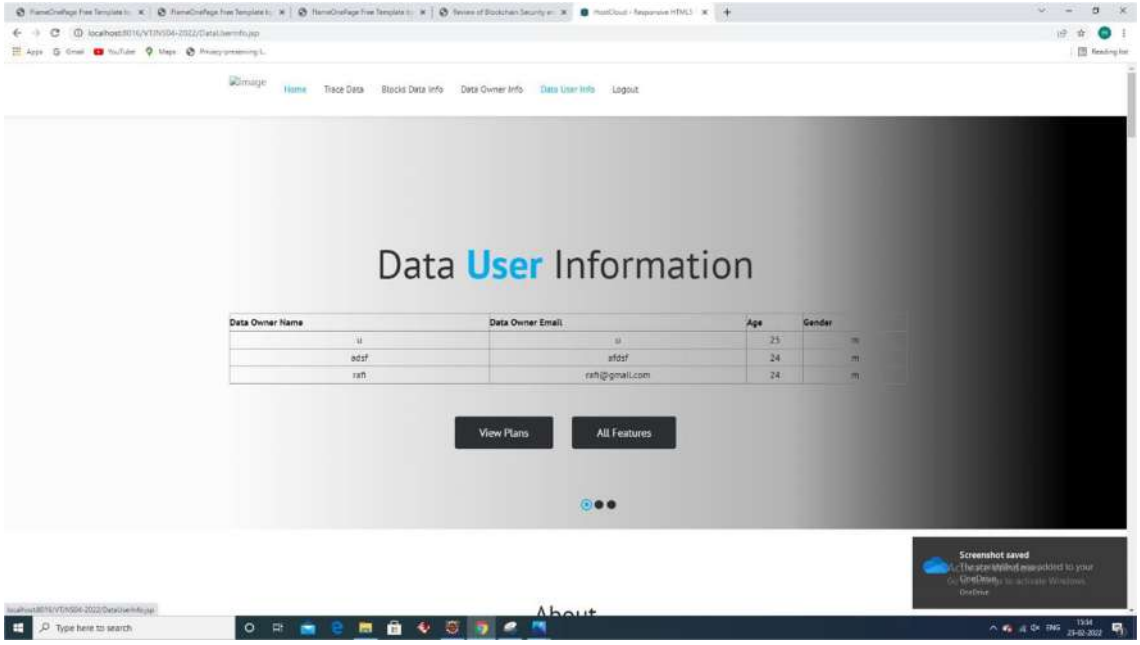

Fig: 5.4.18 Data User Information page

TEST CASES:

S.NO	Test Scenario	User Action	Expected result	Actual Result	Remarks

1	Registration	Users registering into the system.	Register into the system.	Successfully alert registered message.	Pass
2	Login	Entered correct password.	1. Log into the system. 2. Alert generated.	1.Successfully logged in. 2.Successfully generated the alert.	Pass
3	Data User	Search File, View Responses and View Search Keyword	Messages sending data user alert is generated.	Successfully generated the alert and massages sending	Successful
4	Data Owner	Upload a Files and View Uploaded Files	Data owner has to actions	Successfully generated the alert to data owner message	Successful
5	Cloud Server	View Requests, View Files, M. Keywords, View Data Users and View Data Owners	Massages Alert is generated	Successfully generated the alert for cloud server massages	Successful

CONCLUSION

Project Conclusion:

As per the literature and study we can say that there are certain limitations of centralized storage. So to enhance the security of data we can use decentralized cloud storage. This paper suggests a secure and efficient way to store data on cloud. Block chain-based cloud storage with data encryption gives data security in decentralized structure. The proposed model is suitable to implement the block chain structure. The algorithms used to implement the system model is efficient and required less time and give high security for the data which is being stored on cloud. This kind of architecture makes the system more robust and resistant to different security attacks which are performed by unauthorized users who try to steal and disclose the information in data files of user for their benefits.

Future enhancement:

Though the proposed system is capable of providing security, reliability to data using decentralized cloud and blockchain technology, there are more and various security issues to it. Blockchain technology also gets attacked by different attacks such as Fork problem or scale of blockchain etc. So more focus can be given to avoid these attacks in future.

REFERENCES:

[1] Edoardo Gaetani, Leonardo Aniello, Roberto Baldoni, Federico Lombardi, Andrea Margheri, and VladimiroSassone - Blockchain-based Database to Ensure Data Integrity in Cloud Computing Environments, In Proceedings of the First Italian Conference on Cybersecurity (ITASEC17), Venice, Italy.

[2] Ako Muhamad Abdullah - Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data, Article · June 2017, ResearchGate publication.

[3] Anita V. Mithapalli, Swati S. Joshi - A Framework for Secure Data Storage and Retrieval in Cloud Environment, ISSN: 2249 – 8958, Volume-9 Issue-2, December, 2019, International Journal of Engineering and Advanced Technology (IJEAT).

[4] MeilianaSumagita and Imam Riadi - Analysis of Secure Hash Algorithm (SHA) 512 for Encryption Process on Web Based Application, International Journal of Cyber-Security and Digital Forensics (IJCSDF) 7(4): 373-381 The Society of Digital Information and Wireless Communications (SDIWC), 2018 ISSN: 2305-001

[5] AkshayBabrekar, Prof.Rohini G. Pise - Public Key Encryption for Cloud Storage Attack using Blockchain, International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-9 Issue-2, July 2020.

[6] Aradhana, Dr. S. M. Ghosh - Review Paper on Secure Hash Algorithm with Its Variants, DOI: 10.13140/RG.2.2.13855.05289, ResearchGate publication.

[7] AvdhutSuryakantBhise, Phursule R.N. - A Review of Role based Encryption System for Secure Cloud Storage, International Journal of Computer Applications (0975 – 8887) Volume 109 – No. 14, January 2015.

[8] AvdhutSuryakantBhise, R. N. Phursule - Developing Secure Cloud Storage System by Integrating Trust and Cryptographic Algorithms with Role based Access Control, International Journal of Computer Applications (0975 – 8887) Volume 168 – No.10, June 2017.

[9] Peiming Xu, Shaohua Tang, Peng Xu, Qianhong Wu, Honggang Hu, Willy Susilo - Practical Multi-Keyword and Boolean Search Over Encrypted E-mail in Cloud Server

[10] Jie Xu, KaipingXue, Senior Member, IEEE, Shaohua Li, Hangyu Tian, Jianan Hong, Peilin Hong, Nenghai Yu - Healthchain: A Blockchain-based Privacy Preserving Scheme for Large-scale Health Data