VIVA-TECH INTERNATIONAL JOURNAL FOR RESEARCH AND INNOVATION
ANNUAL RESEARCH JOURNAL
ISSN(ONLINE): 2581-7280

A One stop APP for Personal Data management with enhanced Security using Interplanetary File System (IPFS)

Madhura Ranade[1], Abdulkadir Sadriwala[2] ,Aniket Yadav[3], Harsh Purohit [4]
[1]*(Dept of Electronics & Tele-communication, VIVA Institute of Technology, Mumbai University,India)*
[2]*(Dept of Electronics & Tele-communication, VIVA Institute of Technology, Mumbai University,India)*
[3]*(Dept of Electronics & Tele-communication, VIVA Institute of Technology, Mumbai University,India)*
[4]*(Dept of Electronics & Tele-communication, VIVA Institute of Technology, Mumbai University,India)*

Abstract : In today's digital era, the use of physical documents has been replaced by software files for various administrative and everyday purposes. To keep up with this trend and provide a secure and efficient platform for managing documents, this thesis/project proposes a platform that utilizes hashing and IPFS technology for secure document management. The proposed system allows users to upload and store documents on a remote cloud storage server, and share them via QR codes. Upon request, the document owner can grant access to the receiver to view and download the document. The system provides two levels of security to protect user's data and documents. This proposed system can be implemented through an Android application. Overall, the proposed system provides an efficient, secure, and modern approach to document management.

Keywords **-** *Android Application , cloud storage , hashing service , IPFS technology .*

I. INTRODUCTION

In the current era of digital technology, many tasks such as ordering food, shopping, booking tickets, hotels, rides, and more can be done online without the need for physical contact. However, for various procedural tasks such as admission to educational institutions, real estate transactions, organizational procedures, administrative procedures, and more, physical documents or copies of files are often required to be managed and submitted. As a result, personal information has been increasingly necessary to be handled and managed for various purposes. Personal information can refer to information or opinions about an individual, whether recorded in a material form or not, and including information or opinions forming part of a database, whether true or not, whose identity is apparent, or can reasonably be ascertained, from the information or opinion. Personal information can include obvious details such as identity cards, medical records, financial records, bank details, or salary details, as well as less apparent information that can still relate to an individual, such as a car or a piece of land.

During this digital age, it has become increasingly important for individuals to have access to their personal information at all times. However, carrying physical documents everywhere is impractical. To address this issue, a solution has been developed - an app that allows individuals to store and access personal information, which can be easily shared when needed. For instance, during a medical emergency, individuals can use the app to provide relevant identification and medical records to hospital staff instead of searching for physical documents. This system provides a secure, efficient, and convenient way of managing and sharing personal information. It can be used to store various types of documents, such as identification cards, medical records, financial records, and other important documents. The app also provides reminders for document renewals and ensures that sensitive

information is only shared with authorized parties. Overall, this system is an efficient and safe way of managing personal information in the digital age.

II. REVIEW OF LITERATURE SURVEY

Yogle Chen et.al have studied and presented an Improved P2P file system scheme based on IPFS and Blockchain. The main aim was to propose animprovedP2P file system scheme based on IPFS and blockchain. Authors address the high-throughput problem for individual users in IPFS by introducing the role of content service providers. Its method was that the authors provided a novel zigzag based storage model to improve the block storage model that IPFS provides. Moreover, they introduced blockchain to combine IPFS with this storage model. [1]

Morteza Alizadeh have used Efficient decentralized data storage based on Public Block chain and IPFS. The primary objective was to use the IPFS distributed hash table technology to store information immutably and in a decentralized manner to mitigate the high cost of storage its ideas was a storage system based on immutable data and allowing removal of data from malicious users in the DHT. Efficiency is improved by decreasing the overall processing time in the blockchain with the help of DHT technology and introducing an agreement service that communicates with the blockchain via a RESTful API. [2]

T. Rama Reddy et.al proposed a reliable method of securing and verifying the credentials of graduates through Blockchain. Its fundamental purpose was to create a mechanism using blockchain technology which can store the genuine certificates in digital form and verify them firmly whenever needed without delay. The design of a prototype of blockchain based credential securing and verification system developed in ethereum test network and it concluded that this system can be used by all the universities and colleges, in order to provide extra security to the certificates and the students' data. [3]

Quhong Zheng et.al. have presented an innovative IPFS based storage model for Blockchain. It proposed an IPFS based data storage type model to solve the problem of increasing storage space and bandwidth of blockchain which causes prevention of nodes from joining the network. Its method was that the miners of the blockchain network can deposit the transaction data into the IPFS network and pack the returned IPFS hash of the transaction into the block. [4]

Sun Jianjun et.al. have published a paper on Research and Application of data sharing platform integrating Ethereum and IPFS technology. This paper was aimed at proposing a data sharing platform under a new technology environment to ensure data security, user rights protection and highspeed data processing. Its method was that this system combines the decentralized and irreversible characteristics of the ethereum blockchain and then integrated IPFS distributed storage technology. [5]

Emmanuel Nyaletey et.al have shown how to use Block IPFS Blockchain enable Interplanetary File System for Forensic and Trusted Data Traceability. The focus was on complementing IPFS with blockchain technology, by proposing a new approach to create a clear audit trail to reduce security related concerns. In this the Block IPFS system was implemented by integrating the blockchain technology with IPFS distributed file system by storing the hash of files in blockchain nodes for efficiency as well as security.[6]

Fahim, Khandaker Marsus et.al presented a method for a reliable method of securing and verifying the credentials of graduates through Blockchain Its main purpose was to link all personal information of a person to a centralized database .Creating a system in which personal information of a person to a centralized database. Creating a system in which personal data can be accessed and securing data using passwords. The process discussed is very useful for underdeveloped and developed countries. [7]

A paper titled "Research on personal information management" was published by Chen Zhong in 2013. Development and some relevant definitions of personal information, point of series of problems and their measures. The method is having group decisions and in group people are from different cultures and places having different ideologies and thus giving maximum relevant and ethical solutions to the problems. [8]

Mohammed Rustom et.al. presented a methodology for a conceptual framework for an interactive personal information management system 2011. Its main purpose is the importance of visualization techniques that have been proposed in the PIM field in general, and it shows the main factors that have influence on visualizing an interactive PIM system interface. This study is looking to improve user simulations for automated desktop search evaluation for both large collections of photographs and video. It concludes that as described personal information lifecycle processes which may affect the re-finding of information. [9]

A paper having title "Research in data security technology based on cloud-storage" was presented by Ronghzi Wang. Its purpose is to provide a secure storage system based on how to ensure the data visibility when data integrity and data are not complete .So their user can save it and use it whenever wanted securely. Its method is to program using boot passwords to solve the old data encryption in the problem of key preservation and

management system design by correcting tornado data redundancy code delete code in order to solve problems and recover lost data. Cloud storage in rapid development at the same time also brings a series of negative issues, especially data security issues, which seriously hindered the further extensive application of cloud storage. [10]

III. WORK FLOW

The flowchart is displayed in Fig.1. It makes use of three services in the backend to create desired feature of system. It also provides the users with enhanced experience. The initial phase involves creation of mobile application. Flutter framework is used for this purpose. It is a hybrid app development framework which can be used to create multiple platforms applications. Various other software tools are also used for the development.

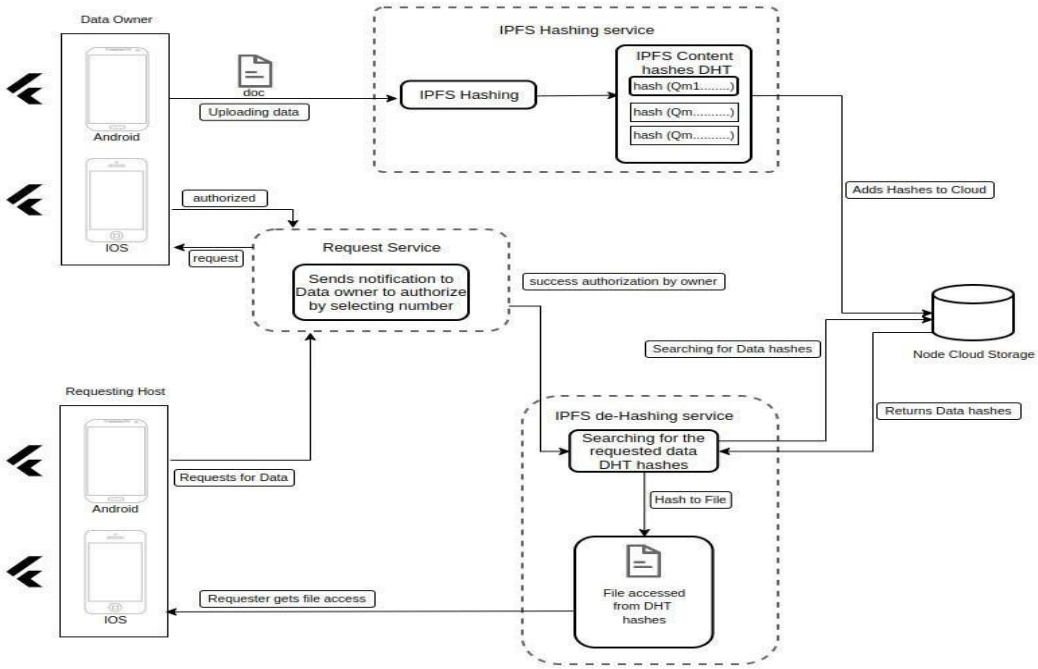


Fig.1. System workflow-chart

The proposed system is aimed at providing users higher degree of security coverage. This will provide protection for one's personal data. The facility of sharing these document is also provided in the app. The proposed app will be able to perform numerous functions as follows.

- Data security: The app will provide authenticated access to user which will ensure protection of their data.
- Data Storage: The cloud storage facility will be provided to users for storing their personal documents.
- Data sharing: The users of proposed app will be able to share their data directly with other users or government authorities for document verification.

The app will be capable of storing data in various formats such as images, text and PDFs etc. The shareable QR code can be generated to access the stored information. Once the owner has given permission to view the files, documents will be visible to the officials.

IV. METHODOLOGY

The working of the proposed system can be explained in following steps.

a. IPFS Hashing service:

This service is the first important part of the system which is responsible for hashing. This process assigns the simple values for object information mapping. This is very useful for encryption of user's data documents. This also ensures appropriate cloud storage. The documents uploaded by user are given to hashing functions. Then, they are forwarded to Interplanetary File System (IPFS).

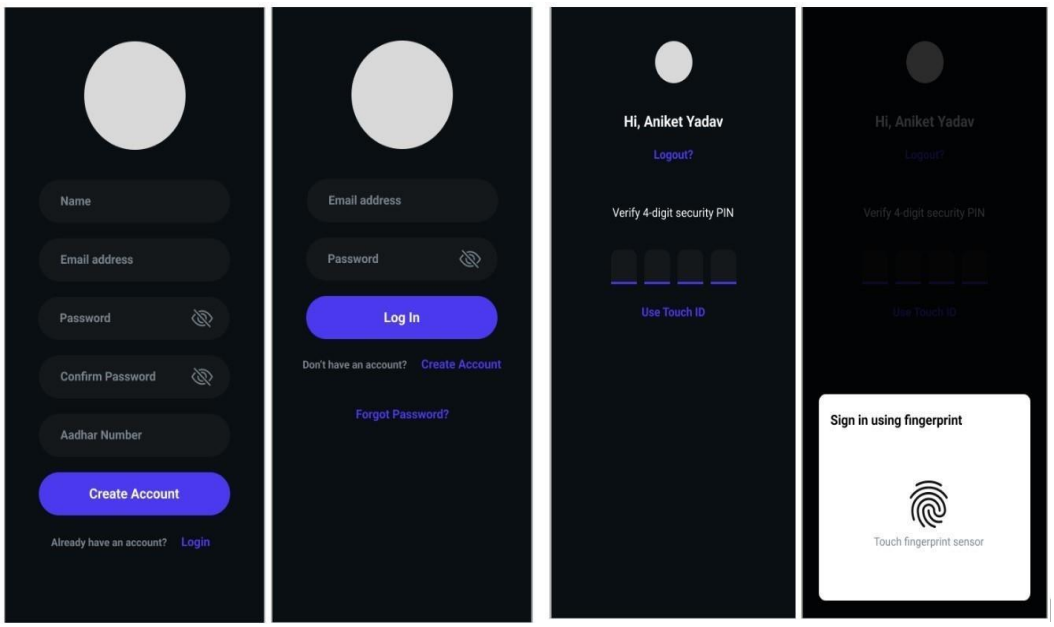
IPFS provides Content Identifier to locate the file. The data hash table is created which stores the file and corresponding key pairs.

b. Request service:

The access of stored document can be obtained by request service. When a person scans the QR code the request process is initiated. The QR code is generated with the dynamic link with reference to Data Hash Table. The acknowledgement for access permission will then be sent to owner of that document. Once the owner permits the access, corresponding document will be visible to the one who have scanned QR code.

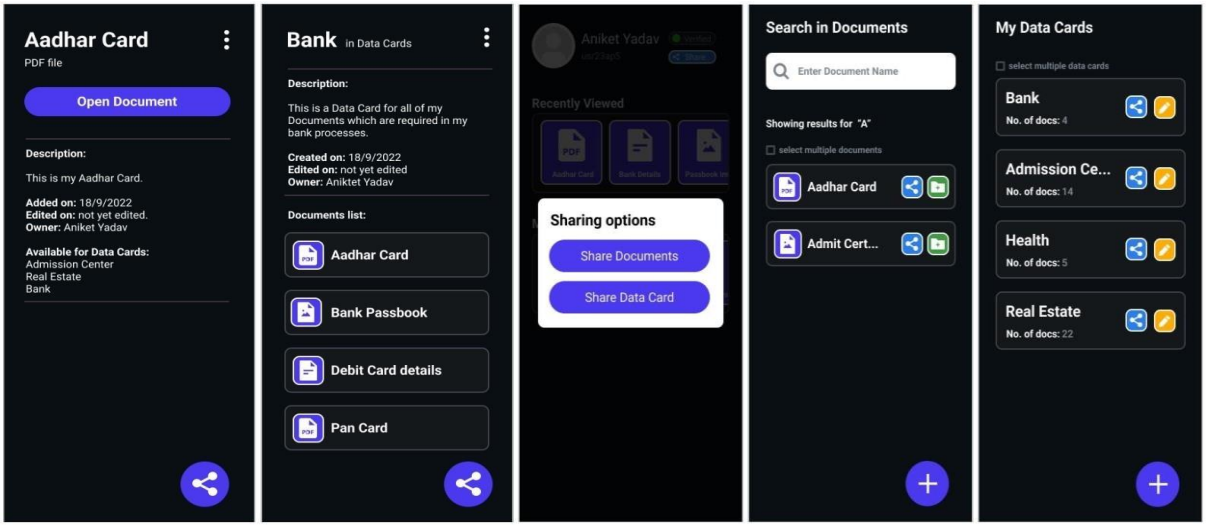
V. RESULTS

The project "**A One stop APP for Personal Data management with enhanced security using IPFS**" has been designed and has been started to develop, with major completion of the application's user interface. The data models for this system have been created and are successfully implemented inside the application along with the user interface to make it possible for the application to work on the local state before implementing and integrating the main backend services with this application. The major screens of the application have already been designed and implemented inside the application whose screens for different sections are shown below.



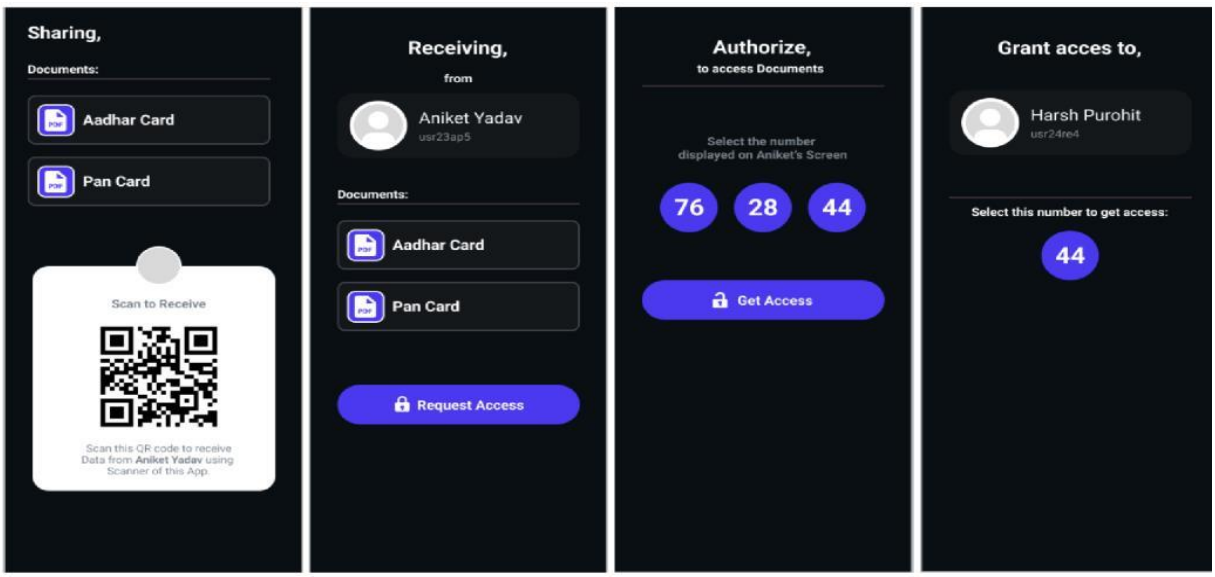
1) **Authentication section**

For the authentication part, the user can create a new account or can sign-in into an existing account(1st and 2nd screens). And whenever the user opens the app, the user will always be prompted to verify themselves either by a pin or their fingerprint id(3rd and 4th screen).



2) Data management section

Data management section consists of mainly selecting different documents and data cards so after selection users will be able to share them. When clicked on the share button from Home page, a popup comes 1st screen where user can select to share either a document or data card, and after required selections, they can share them using the Sharing section.



3) Sharing/Receiving section

This section is the most important section of this app, where users will be able to share or receive the data.
When after documents/data card selection the user clicks on the share button, they will be taken to the 1st Sharing page via QR code. And when some other user scans this QR code, he is taken to the Request page where he has an option to request for access to documents. On clicking request for access, a notification page is sent to the owner app (containing a single key number), then the requester user has to select from multiple options key

numbers. On successful key number selection, the requester then gets the access to the required documents/data cards.

VI. CONCLUSION

The demand for efficient data storage is increasing rapidly, and security is also a major concern due to the high risk of data breaches leading to identity theft and other issues. To address these challenges, a proposed system offers dual-layer security, allowing users to upload and share data with others without fear of it being stolen. This proposed system can be implemented through a mobile application that utilizes the Inter Planetary File System (IPFS), enabling data to be stored in a distributed system that makes it extremely difficult to track and hack files.

Acknowledgements

Authors would like to thank the institute for availing all the required resources for doing this research.

VII REFERENCES

[1] Alizadeh, M., Andersson, K. and Schelen, O. (2020) "Efficient decentralized data storage based on public blockchain and ipfs," *2020 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE)* [Preprint].
Available at: https://doi.org/10.1109/csde50874.2020.9411599.

[2] Chen, Y. *et al.* (2017) "An improved P2P file system scheme based on ipfs and Blockchain," *2017 IEEE International Conference on Big Data (Big Data)* [Preprint]
Available at: https://doi.org/10.1109/bigdata.2017.8258226.

[3] Fahim, T.A. *et al.* (2014) "Automated Life Card Data Management to a central database," *2014 IEEE 3rd Global Conference on Consumer Electronics (GCCE)* [Preprint].
Available at: https://doi.org/10.1109/gcce.2014.7031309.

[4] Jianjun, S., Ming, L. and Jingang, M. (2020) "Research and application of data sharing platform integrating Ethereum and ipfs technology," *2020 19th International Symposium on Distributed Computing and Applications for Business Engineering and Science (DCABES)* [Preprint] Available at: https://doi.org/10.1109/dcabes50732.2020.00079.

[5] Nasar, M.R.,Mohd, M. and Ali, N.M. (2011) "A conceptual framework for an interactive personal information management system," *2011 International Conference on User Science and Engineering (iUSEr)* [Preprint].
Available at: https://doi.org/10.1109/iuser.2011.6150545.

[6] Nyaletey, E. *et al.* (2019) "BlockIPFS - blockchain-enabled interplanetary file system for forensic and Trusted Data Traceability," *2019 IEEE International Conference on Blockchain (Blockchain)* [Preprint].
Available at: https://doi.org/10.1109/blockchain.2019.00012.

[7] T,R.R. *et al.* (2020) "Proposing a reliable method of securing and verifying the credentials of graduates through Blockchain."
Available at: https://doi.org/10.21203/rs.3.rs-45633/v1.

[8] Wang, R. (2017) "Research on data security technology based on cloud storage," *Procedia Engineering*,174,pp.1340–1355.
Available at: https://doi.org/10.1016/j.proeng.2017.01.286.

[9] Zheng, Q. *et al.* (2018) "An innovative ipfs-based storage model for Blockchain," *2018 IEEE/WIC/ACM International Conference on Web Intelligence (WI)* [Preprint].
Available at: https://doi.org/10.1109/wi.2018.000-8.

[10] Zhong, C.(2013) "Research on personal information management,"*2013 International Conference on Computational and Information Sciences* [Preprint].
Available at: https://doi.org/10.1109/iccis.2013.105.

[11] B. Guidi, A. Michienzi and L. Ricci, "Data Persistence in Decentralized Social Applications: The IPFS approach," 2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 2021, pp. 1-4, doi: 10.1109/CCNC49032.2021.9369473.

[12] R. Nagaoka, J. Kishigami and Y. Kobayashi, "Encoding Content-Based Similarity in IPFS Pointer Names," 2019 IEEE 8th Global Conference on Consumer Electronics (GCCE), Osaka, Japan, 2019, pp. 1118-1120, doi: 10.1109/GCCE46687.2019.9015458.