IJIRCCE

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



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 10, Issue 8, August 2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.165

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 8, August 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1008039 |

Android Privacy Enhanced Document Sharing System using Blockchain and IPFS Technology

[*1]Oluyinka I Omotosho, [2]Gabriel O. Olatoye

[1]Department of Cyber Security Science, Ladoke Akintola University of Technology, Ogbomosho - Nigeria

[2]Department of Computer Science, Ladoke Akintola University of Technology, Ogbomosho - Nigeria

*Corresponding Author: oiomotosho@lautech.edu.ng

ABSTRACT: The widespread adoption of smartphones has replaced desktop computers and laptops as the first component of the computer, due to mobility, regular communication and application versatility. Mobile devices include extensive data storage including sensitive objects such as verification credentials, photos, videos, personal information, activity details, and much more. Therefore, protecting data stored on mobile devices becomes a serious problem. In this Paper, the safety of the Android storage model between 2013 and 2018 are investigated and severalthreats are found in literature that can be classified as physical or software threats. Recently, in the block-chain has hit the top levels recently. While most of the buzz has been around for block-chain use like crypto currencies and ICOs, the technology itself is exciting. The block-chain provides democratized trust and authentication protocols that have already disrupted banking and are at risk of adding healthcare, financial services, social apps and more. This work however use the BlockChain Technology and IPFS to store Hash values and files, secure file transfers can also be obtained.

I. INTRODUCTION

In recent years, technical innovation and related research on collaborative techniques for sharing users data among organizations has accelerated [1]. File sharing is the practice of distributing or providing access to digitally stored information. Though, various users and organizations have long relied on the internet as a medium of sharing or publishing data with each other. Most often, data warehouse is provided to store large files and is adopted by organization, individuals, but has been identified as associated with huge risk, because it is managed by a single user. Examples of such repository technologies include Blogs [20]. Other technologies that spring up because of the rise of Web 2.0 encourage multiple data sharing among individuals. Flicker permits its users to upload, organize and share photos. Wikipedia as one of the most popular online encyclopedias permits its users to share knowledge by modifying the encyclopedic entries. Also, Google Groups provides repository where users can post messages and share files.Another major challenges faced with the conventional way of file sharing, management and storage techniques (such as manual filing or sharing of images, documents etc) is that users have little control over or even knowledge of the type of file being shared, even if it contains a virus. Moreover, users do not or sometimes don't remember the names of these files, the files contents, and their storage locations, this increases the risk of lost.

Smartphones have become conduits for our most personal information and data. When one wants to install an app on their device, they have to allow the apps to access their camera, internet, location etc. This can lead to privacy issues and affect the user privacy. For example, granting privileges to location leads to tracking the user through their phone.Study also reveals that Android phones constantly snoop their users. With the notable exception of /e/OS, even when minimally configured and the handset is idle these vendor-customized Android variants transmit substantial amounts of information to the OS developer and also to third parties (Google, Microsoft, LinkedIn, Facebook, etc.) that have pre-installed system apps. The summary table 1.1 indicates, sensitive user data like persistent identifiers, app usage details, and telemetry information are not only shared with the device vendors, but also go to various third parties, such as Microsoft, LinkedIn, and Facebook.

More importantly, this concerns the collection of data for which there's no option to opt-out, so Android users are powerless against this type of telemetry.This is particularly concerning when smartphone vendors include third-party apps that are silently collecting data even if they're not used by the device owner, and which cannot be uninstalled. Currently, the model also includes a local private IPFS network, which improves the efficiency of content publishers to upload NDN encryption knowledge files. In the model, the file content is stored in the private IPFS network, and the content owner and the corresponding hash value are stored on the blockchain to achieve efficient real storage. The model also includes a local private IPFS network, which improves the efficiency of content publishers to upload NDN

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 8, August 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1008039 |

encryption knowledge files. In the model, the file content is stored in the private IPFS network, and the content owner and the corresponding hash value are stored on the blockchain to achieve efficient real storage.

Table 1.1 Summary of Data Collection by Individual Android OS variant. (Source: Trinity College Dublin).

	Samsung	Xiaomi	Realme	Huawei	LineageOS	/e/OS	Google
Long-lived Device Identifiers	IMEIs, hardware serial numbers	IMEIs, Secure DeviceID, MD5 hash of Wifi MAC address	IMEI, deviceID, guid	hardware serial number, device RSA cert	-	-	IMEI, hardware serial number, Wifi MAC address
Resettable Identifiers Relinkable to Device	Samsung Consumer ID, Firebase IDs	VAID, Google Ad ID	VAID, OAID, device_id, registrationId, Google Ad ID, Firebase IDs	-	-	-	AndroidID, Google Ad ID
Third-Party System App Data Collectors	Google, Mobile Operator, Microsoft, LinkedIn, Hiya	Google, Mobile Operator, Facebook	Google, Heytap	Google, Daily Motion, Avast, Qihoo 360, Microsoft	Google	-	
Main Telemetry Collectors (By Data Volume)	Google, Samsung, Microsoft	Google, Xiaomi	Google, Heytap	Google, Microsoft	Google	-	
Loggers of App Usage Over Time	Samsung	Google, Xiaomi	-	Google, Microsoft	-	-	
Loggers of Apps Installed On Handset	Google, Samsung	Google, Xiaomi	Google, Realme, Heytap	Google, Huawei	Google	-	

To solve these issues we hereby propose a smart android based document sharing system over blockchain technology that ensures easy document sharing along with authenticity and reliability of a tamper proof system. Using blockchain technology for data sharing aims to solve this problems and provide users with more control over their data. They can choose to stay anonymous and perform all transactions with the assurance of the data being secure and unaltered in the process. With its increased data security and transparency, Blockchaincan minimize the cases of fraudulent transactions and app based data breaches. The technology is also simple to implement and allows for low-cost mobile app development.

This digital ledger blockchain technology promises to be particularly suited for mobile apps, facilitating smooth peer-to-peer transactions. Furnishing dedicated and unaltered records of transactions solely based on mobile app needs, along with offering lower-cost solutions and automating time-consuming processes, blockchain is now nigh-indispensable to mobile app development, ushering in the era of Mobile Blockchain.

This digital ledger blockchain technology promises to be particularly suited for mobile apps, facilitating smooth peer-to-peer transactions. Furnishing dedicated and unaltered records of transactions solely based on mobile app needs, along with offering lower-cost solutions and automating time-consuming processes, blockchain is now nigh-indispensable to mobile app development, ushering in the era of Mobile Blockchain.

II. RELATED WORK

Blockchain is a digital ledger of transactions that get duplicated and distributed over the entire network. It offers a decentralized system for managing data and transactions in a peer-to-peer network. Unlike the traditional way of sharing data through clouds in Web 2.0, the decentralized system allows the distribution of data divided into blocks. Each block is then protected from intruders attempting to alter the data. Every change in the data needs to be validated by all peers or miners (users) in the network using advanced cryptography techniques [20].

Data sharing is a crucial step to gain maximum benefit from the strengths of research. A lot of data sharing mechanisms are proposed and discussed in literature. There is no sufficient work available that focuses on the incentive mechanism to promote data sharing. To cover these limitations, authors in [21] conducted a review on medical and health data to uncover the incentive mechanisms with the pre- and post- results after empirical analysis. According to survey, a single incentive is tested for medical and health data to analyse the rate of data sharing. Therefore, it is concluded that more incentive based researches need to be performed to encourage data sharing.

Data sharing in blockchain can provide organizations with a secure way to store and distribute data. Given the decentralized nature of this network, there are no owners in the blockchain database, and the data travels through the peer-to-peer network secured by an immutable cryptographic signature. Blockchain helps make the data difficult to hack or change.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 8, August 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1008039 |

A distributed digital ledger (blockchain) system holds immutable encrypted and hashed authenticated data, with any changes or errors traceable back to their source. The data is stored in a distributed and redundant fashion in the blockchain, and each node verifies each transaction. Therefore, it is hard for malicious parties to attack and manipulate the data to their advantage. Thus, blockchain does not require a trusted central server or entity and it is often called "trustless[2].

In recent era, blockchain such as; bitcoin [3], Ethereum [7] and Zcash [8] are considered as hot and fundamental technologies of cryptocurrency. As a result, researchers and industrialists are paying more attention to establish a trust based model in a decentralized manner. Although blockchain was developed as a platform for virtual currency, the applications of the technology have since quickly evolved to numerous fascinating use cases. Many industries, including in the financial technologies (fintech) and banking sectors, commercial supply chains, healthcare, building industries, etc. are now working on incorporating blockchain (distributed ledgers) technology as a core of their data-management systems. In contrast to the centralized system, blockchain technology can be totally transparent to the users and very promising to incentivize users for data sharing. It also naturally supports building up incentives for users to share their data, in terms of rewards (micro-payments or credits) encoded in the smart contracts.Blockchain can be used for file Sharing and the Platforms can technically improve the file sharing system. Neverthelesss it may involve different approaches to affer secure and effective hosting. Such include the Interplanetary File System (IPFS) [21].

IPES was originally designed to optimize the current hypertext transfer protocol and then gather computer devices with the same file system together to form a huge distributed system [21]. At the same time, IPFS provides both a global node network and a more secure and efficient private shared network. This content search mechanism assigns a unique hash value to each file in the network based on the file content and maintains a distributed hash table to find the required file. For large storage files, IPFS will automatically slice files into multiple servers for storage and synchronously download and splice files upon request to speed up file access. In the model designed in this paper, an IPFS private storage network composed of three nodes was constructed to improve the overall efficiency of the model.

III. ETHEREUM SMART CONTRACT

A "smart contract" is simply a program that runs on the Ethereum block-chain. It's a collection of code (its functions) and data (its state) that resides at a specific address on the Ethereum block-chain. Smart contracts are a type of Ethereum account. This means they have a balance and can be the target of transactions. However they're not controlled by a user, instead they are deployed to the network and run as programmed. User accounts can then interact with a smart contract by submitting transactions that execute a function defined on the smart contract. Smart contracts can define rules, like a regular contract, and automatically enforce them via the code. Smart contracts cannot be deleted by default, and interactions with them irreversible.

IV. DESIGN ARCHITECTURE AND APPLCATION WORKFLOW

In this section, the Design of an Android based Privacy Enhanced Document Sharing System using Blockchain and IPFS Technologyis discussed. Our design architecture and the implementation work flow of this research work.

4.1 Application Work Flow

The application workflow is implemented as follows:

The ethereum smart contract is programmed and built using remix IDE for testing and debugging before deploying to local ethereum test net (see figure 4.1), after successful deployment of the ethereum smart contract, we implemented a web3js with nodejs backend server to connect and interact with the smart contract on the local ethereum test net, then the application is built using react native technology which is a frame work that rely heavily on Java to render native components (collection of functioning user interface design), to endure secure communication between the application and the web3 backend server, we implement a secure http API with nodejs backend service and communicate via http request method which include the GET,POST ,PUT AND DELETE.

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 8, August 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1008039 |

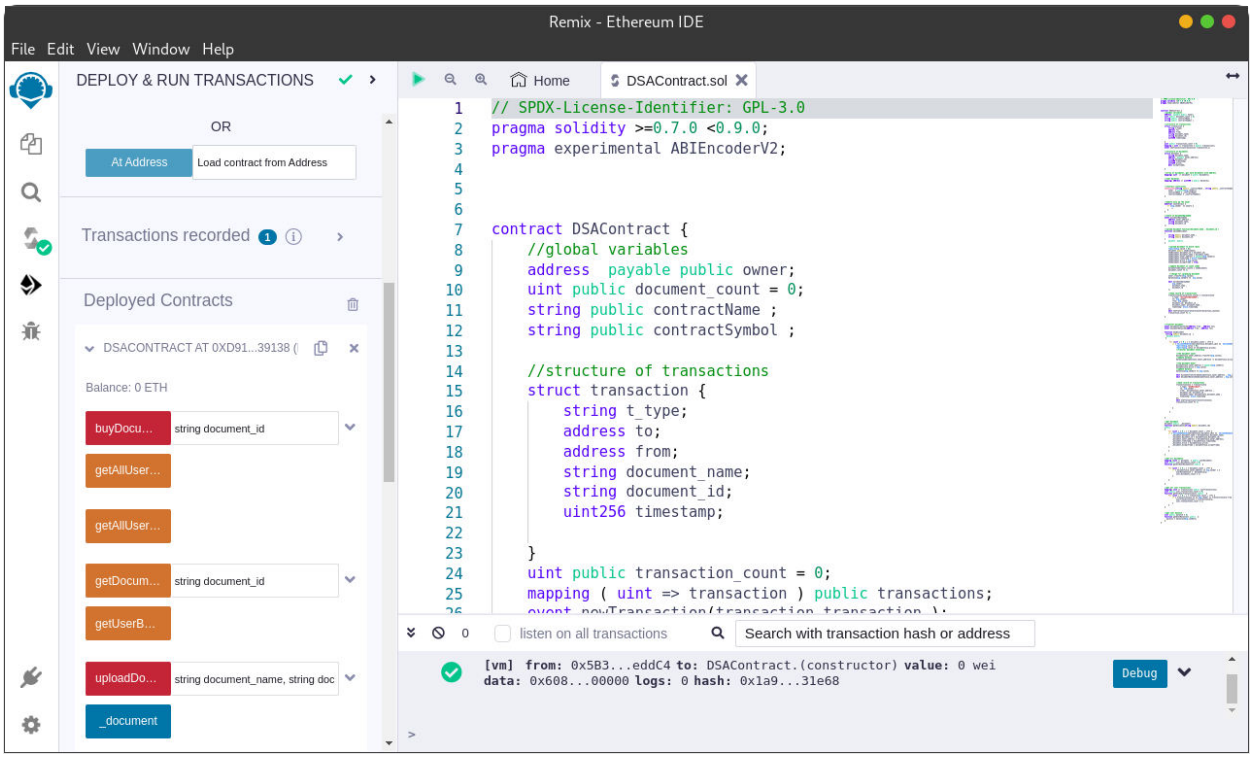


Figure 4.1: Etherum Smart contract using Remix IDE

Ganacheethereum is a service that provide local or private ethereum test net, ganacheethereum test net run on localhost with the address 192.168.0.192:8525, we have a Nodejs backend service running on a local network address at 192.168.0.192:8088 and an IPFS json and rpc running on 192.168.0.192:5004. These services are running on the same machine, sharing the same IP address but a different port numbers, for effective workflow of the application these services runs on the same LAN network with the android devices the application is run on. Please note that the above addresses and port numbers can varies base on different machine and LAN setup (See Figure 4.2)..

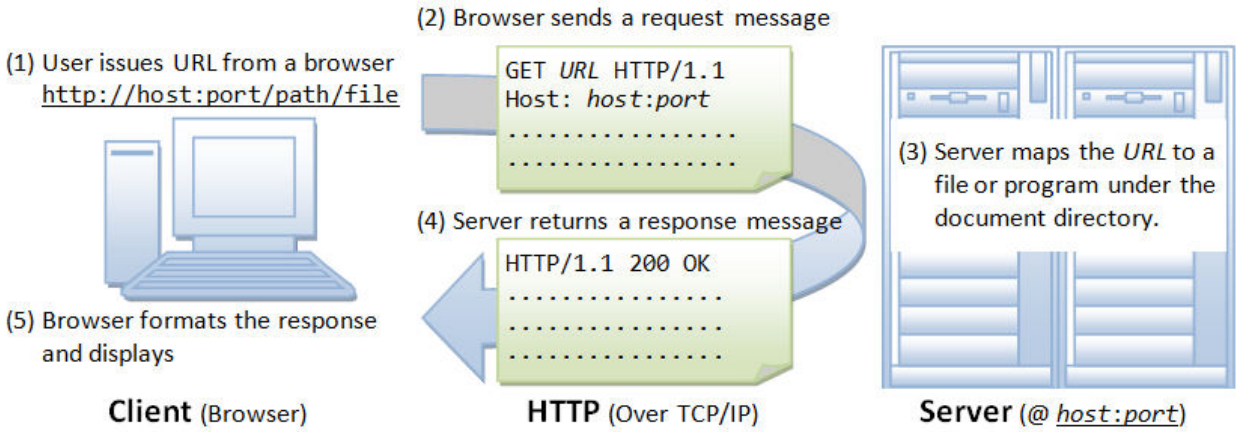


Figure 4.2 http request Processing

4.2 Architectural design

After setting up the application different services which defines the workflow of the application, here we bring the different services together to communicate to form the network architecture for the successful implementation of the application, with the help of fetch API in Nodejs we build an API (application programming interface) which serves as

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 8, August 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1008039 |

the point of communication and data exchange for the services we have running during the setup (See Figure 4.3. The simple architecture is as follows.

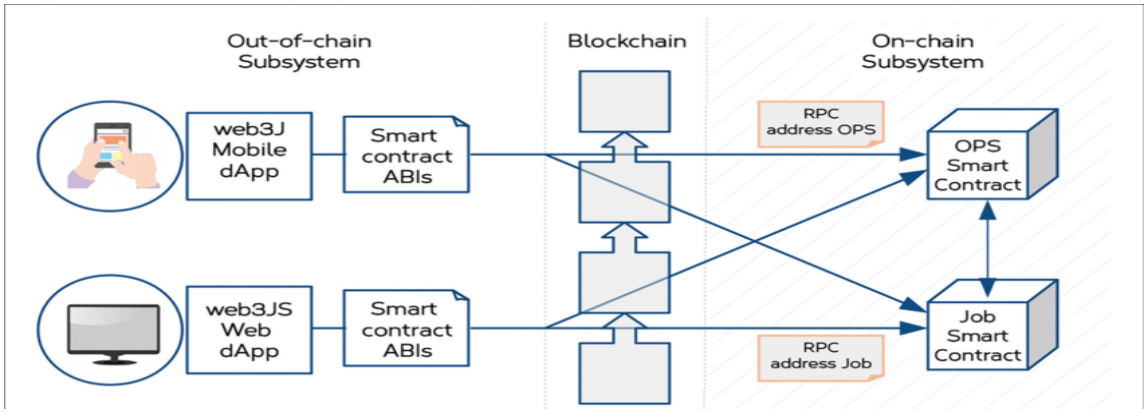


Figure 4.3Application Network Architectural Design

The application network architecture system is broken into two subsystem which are Out-of-Chain subsystem and On-chain subsystem.

4.2.1 Out-Of-Chain Subsytem

This subsytem consist of the web3Js Mobile DApp (decentralize app) and the Smart contract ABIs (Application Binaries Interfaces), Mobile DApp is the UI where users use to interact with the block-chain smart contract, it consist of buttons and graphical components for easy navigation and user friendly interaction.

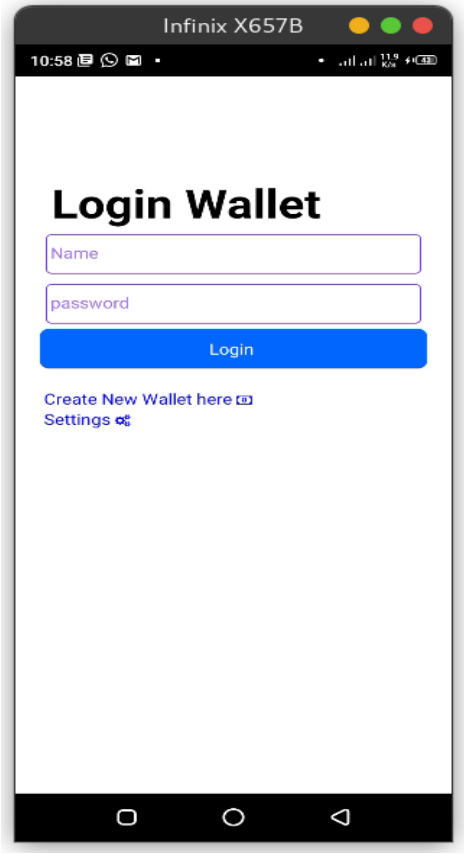


Figure 4.4 Mobile Dapp User Interface

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 8, August 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1008039 |

Smart Contract ABIs are methods or procedures which performs operations on the ethereum block-chain these operations can be reading or writting into the block-chain network.

```
//call getUserBalance() method from contract
let tx_ =  await contract.methods.getUserBalance().send(tx);
console.log(tx_)
let balance = await contract.methods.balance().call(tx);
res.send({balance: balance, status: 200});
res.end();
```

Figure 4.4: Interacting with the smart contract ABIs

4.2.2 In-Chain Subsytem

This system consist of the smart contract API which runs on a nodejs server backend, it provides API calls that directly interact with the smart contract on the block-chain network, for operations the requires reading and writing to blocks on the block chain a gas price fee is charge. Figure 5.4 shows node Server running the API Request.

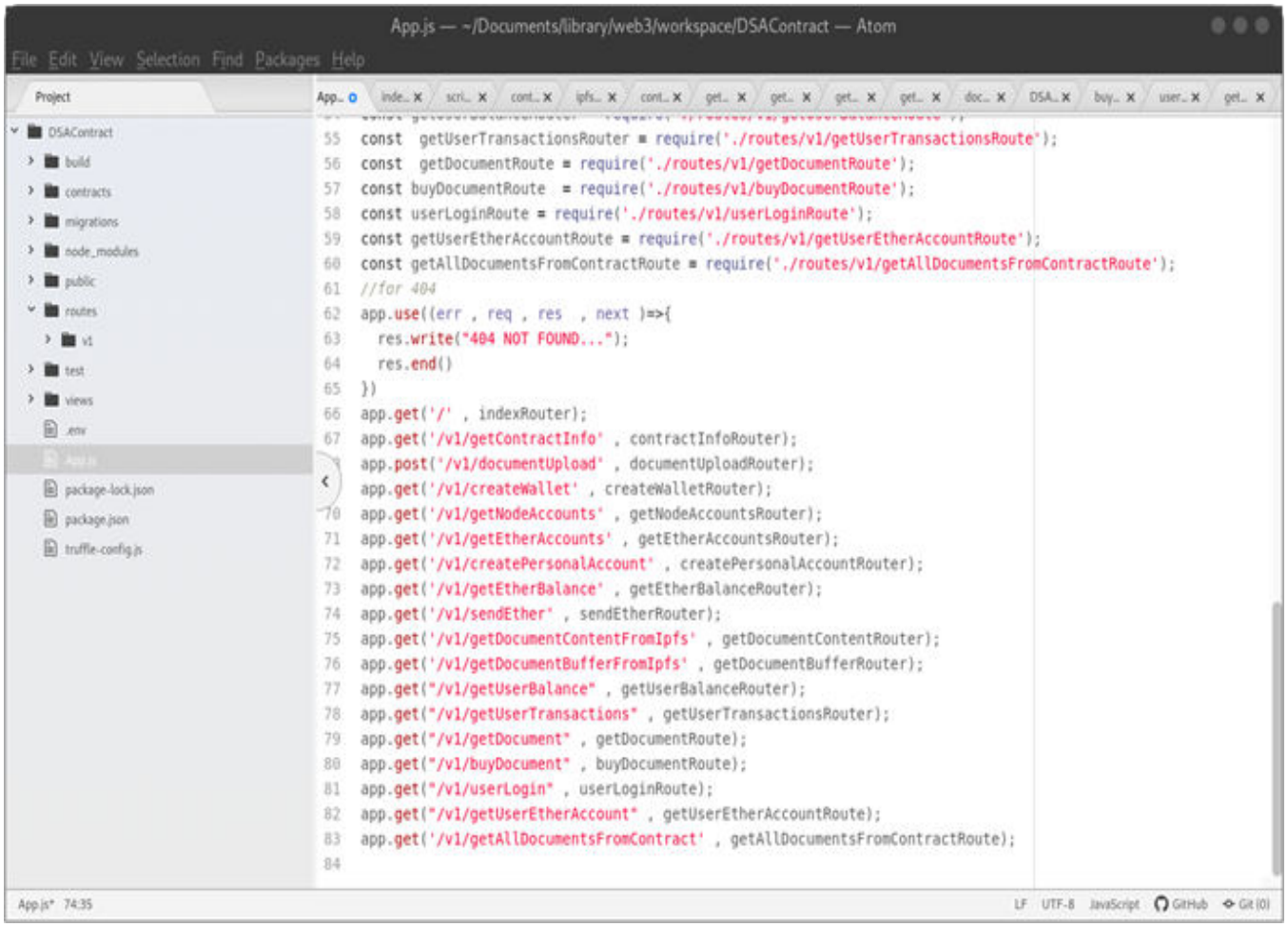


Figure 4.5: Implementing API requests to node server

4.2.3 Blockchain

This part of the architecture deals with the mining and processing of transactions on the block-chain by each nodes, it include writing and updating the distributed ledgers to keep records of transaction and validation. For this research there is a need for an ethereum smart contract account which is the ethereum account that owns (i.e deploy the smart contract to the private ethereum test net) the smart contract, also each users using our document sharing application will fund their wallet with the smart contract token by paying an ether (a currency on the ethereum block chain) to upload document to

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 8, August 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1008039 |

the block-chain server and make it available to the public for sharing, users can share any document on the server based on the amount of token it requires to become the owner of the document, after successful sharing of the document by the user, the new user becomes the owner of the document where a token balance is sent to the former owner of such document.

Running ganacheethereum by default provide list of ethereum accounts which come with 1000ETH balence for testing and implementation this save the need to spend real money on funding our ethereum account with ether. We can now pick an account from the given ethereum accounts provided by ganacheethereum to deploy the smart contract to the private ethereum block-chain network. After successful deployment we import the account to the metamask wallet for visualization, We also import another account for sending ether to perform document sharing by the users using the document sharing application. Figure 4.6 shows the codes for deploying an etherum smart contract to private test net.

```
   Deploying 'DSAContract'
   ----------------------
   > transaction hash:    0xc966ad6b0351fd2cf42e27af9d24a6f3cf2559f7bf
4594d6c683752fd822ac4d
   > Blocks: 0            Seconds: 0
   > contract address:    0x2165E79b0bbCC5ce5587B06b9441ED87B661F7bA
   > block number:        1
   > block timestamp:     1673691481
   > account:             0xcF6C8463115EA9228AD2e08ce7245D7Ee9D3A2B7
   > balance:             999.99097524325
   > gas used:            2674002 (0x28cd52)
   > gas price:           3.375 gwei
   > value sent:          0 ETH
   > total cost:          0.00902475675 ETH

   > Saving artifacts
   -------------------------------------
   > Total cost:       0.00902475675 ETH
```

Figure 4.6: Deploying an ethereum smart contract to private ethereum test net

V. IMPLEMENTATION DETAILS

In this section, the implementation details are provided. The proposed system is a private network of Ethereumblockchain. Ethereum is open source distributed platform that makes efficient use of solidity. A programmable language that allows to write smart contracts (scripting language).

5.1 Simulation Setup

The specifications for implementation setup are: Intel(R) core(TM) m3-7Y30 CPU@1.61 GHz, 8 GB RAM, 64 bit operating system and X64-based processor. The programming language is solidity to write smart contract. Front-end web GUI is developed using Bootstrap 4.0 and Javascript for user interactive forms. The primary tools used to develop this system is given below: Visual Studio Code A lightweight cross-platform code editor designed by Microsoft for multiple operating systems. It allows powerful debugging with a variety of tools, highlighted syntax, intelligent completion of code, build in Git control and code refactoring. Ganache A blockchain-based emulator used to execute several tests and commands. It controls the blockchain operation by inspecting the states of system. Formerly, its name was Test RPC, which was later renamed to ganache. It provides information such as; Visual MNEMONIC (key phrase for ganache accounts) and account addresses. Metamask It is a browser extension that allows a connectivity to distributed web. Instead of running the full Ethereum node, it run Ethereum decentralized applications in browser.

5.2 Test Procedure

This section the implementation testing procedure. This affirms that the application workflow and architecture correctly and well integrated. The aim is to be able to share any type of document's ownership from one user to the other.

An Implementation Testing Procedure includes the following:

1. User A upload a document to the blockchain network with the token cost of the document, by doing this, User A is charged with ether which is sent to the smart contract owner. (see Fig 5.1a & b)
2. User B wants to share the document to himself by paying an ether cost to become the owner of the document. (see Fig 5.2a & 5.2b)
3. User A receive the ether charged from User B and hand over the document owner ship to User B. (see Fig 5.3a& 5.3b)
4. The ethereumblockchain validates this transactions and update ledgers.

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 8, August 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1008039 |

5. User A is now credited with ether for the document he previously owned, and User B becomes the new owner of the document.(See Figure 5.4)

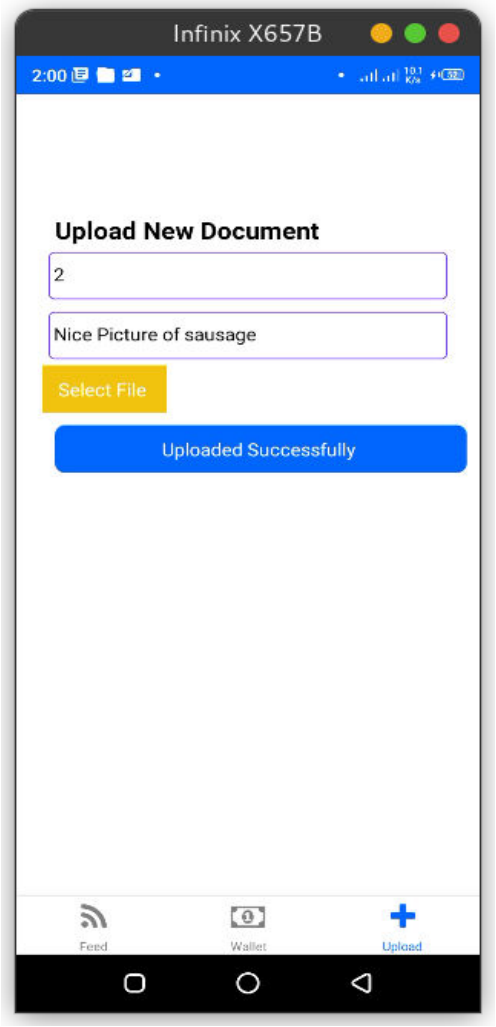


Fig 5.1a:(UserA upload a document to the blockchain)

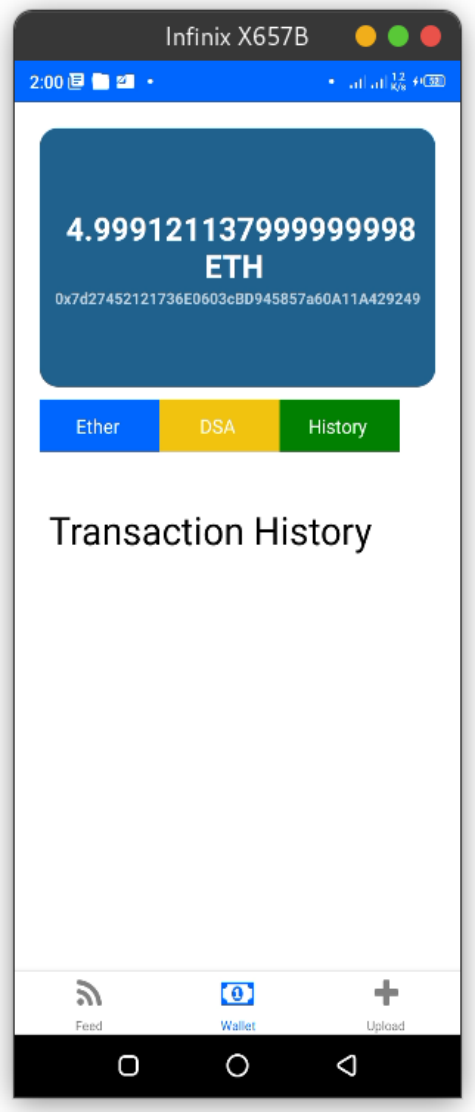


Fig 5.1b: UserA is charged ether for uploading document)

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 8, August 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1008039 |



Fig. 5.2a: UserA receive 2DSA which is the token price of the uploaded document

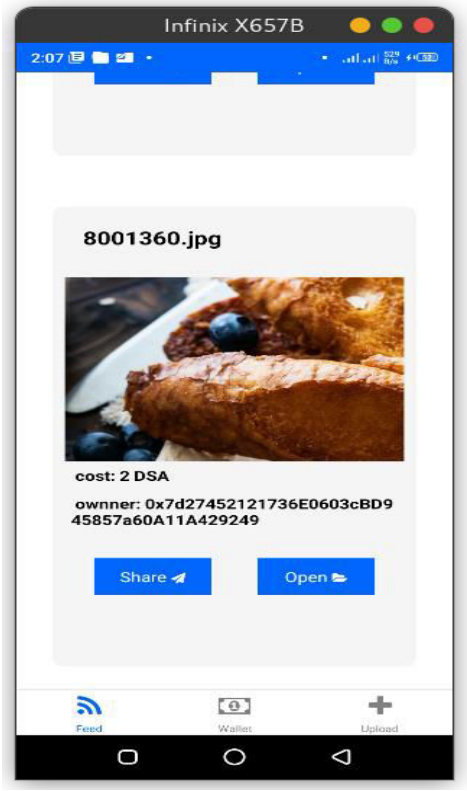


Fig 5.2b: User B can only view part of the file

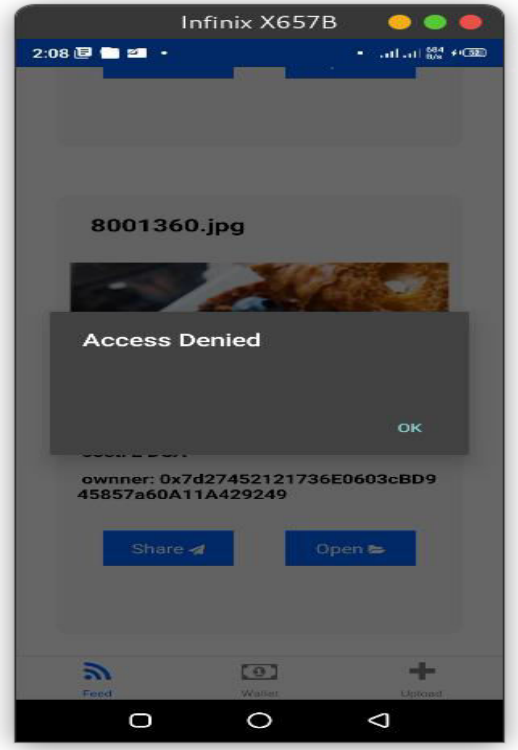


Fig. 5.3a: UserB cann0t access the document Without sharing it to himself

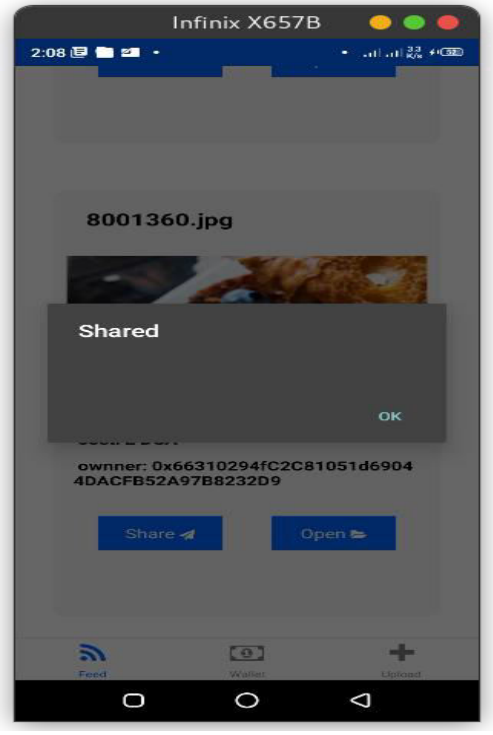


Fig 5.3b:UserBshared the document by paying ether to UserA

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 8, August 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1008039 |

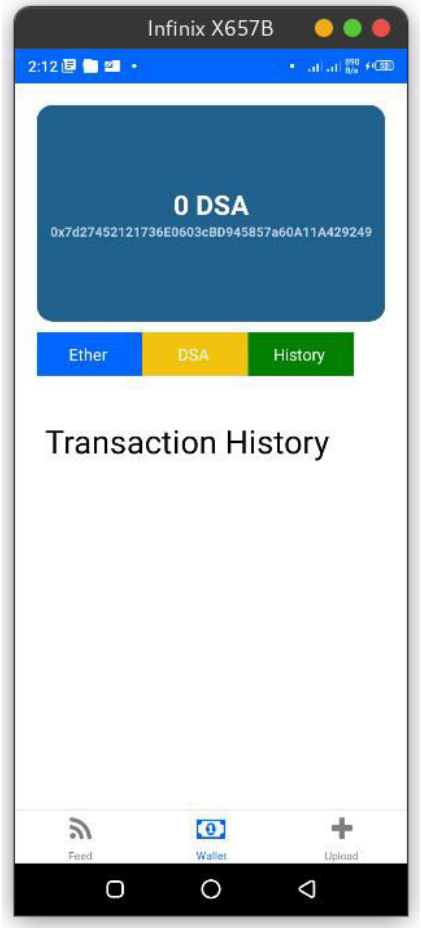


Fig 5.4: UserA receive eth from User B and now have 0DSA token)

VI. CONCLUSIONS

The project developed an Android file sharing system using Blockchain technology. The system uses several Cryptography and Network algorithms and provides two major services to client : Secure File Storage and Secret Sharing. The agreement between the parties are bound by an Ethereum Smart Contract and uses a smart contract token as a value for service. The two layers of the system can also be implemented separately as components for different use cases. The project was completed with a exciting exploration and research in Cryptography and Blockchain field.

REFERENCES

1. Shrestha, A.K.; Vassileva, J. Blockchain-Based Research Data Sharing Framework for Incentivizing the Data Owners. In International Conference on Blockchain; Springer: Cham, Switzerland, 2018; pp. 259–266.
2. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available online: Https://bitco.in/pdf/ bitcoin.pdf (accessed on 6 April 2019).
3. Crosby, M.; Pattanayak, P.; Verma, S.; Kalyanaraman, V. Blockchain technology: Beyond bitcoin. Appl. Innov. 2016, 2, 71.
4. Benet, J. Ipfs-content addressed, versioned, p2p file system. arXiv 2014, arXiv:1407.3561.
5. Shamir, A. How to share a secret. Commun. ACM 1979, 22, 612–613. Wood, G. Ethereum: A secure decentralisedgeneralised transaction ledger. EthereumProj. Yellow Pap. 2014, 151, 1–32.
6. Hopwood, D.; Bowe, S.; Hornby, T.; Wilcox, N. Zcash Protocol Specification; GitHub: San Francisco, CA, USA, 2016.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 8, August 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1008039 |

7. Wu, A.; Zhang, Y.; Zheng, X.; Guo, R.; Zhao, Q.; Zheng, D. Efficient and privacy-preserving traceable attribute-based encryption in blockchain. Ann. Telecommun. 2019, 74, 401–411.Zhang, Z.; Zhao, L. A Design of Digital Rights Management Mechanism Based on Blockchain Technology. In International Conference on Blockchain; Springer: Cham, Switzerland, 2018; pp. 32–46.
8. Ma, Z.; Jiang, M.; Gao, H.; Wang, Z. Blockchain for digital rights management. Future Gener. Comput. Syst. 2018, 89, 746–764. [CrossRef] 11. Rowhani-Farid, A.; Allen, M.; Barnett, A.G. What incentives increase data sharing in health and medical research? A systematic review. Res. Integr. Peer Rev. 2017, 2, 4.Zhu, L.; Wu, Y.; Gai, K.; Choo, K.K.R. Controllable and trustworthy blockchain-based cloud data management. Future Gener. Comput. Syst. 2019, 91, 527–535.
9. Li, J.; Wu, J.; Chen, L. Block-secure: Blockchain based scheme for secure P2P cloud storage. Inf. Sci. 2018, 465, 219–231.
14. Li, J.; Wang, X.; Huang, Z.; Wang, L.; Xiang, Y. Multi-level multi-secret sharing scheme for decentralized e-voting in cloud computing. J. Parallel Distrib. Comput. 2019, 130, 91–97.
15. Huang, Q.; Ma, Z.; Yang, Y.; Niu, X.; Fu, J. Attribute based DRM scheme with dynamic usage control in cloud computing. China Commun. 2014, 11, 50–63.
16. Sun, W.; Yu, S.; Lou, W.; Hou, Y.T.; Li, H. Protecting your right: Verifiable attribute-based keyword search with fine-grained owner-enforced search authorization in the cloud. IEEE Trans. Parallel Distrib. Syst. 2016, 27, 1187–1198.
17. Xia, Q.I.; Sifah, E.B.; Asamoah, K.O.; Gao, J.; Du, X.; Guizani, M. MeDShare: Trust-less medical data sharing among cloud service providers via blockchain. IEEE Access 2017, 5, 14757–14767. [CrossRef] 18. Hammi, M.T.; Hammi, B.; Bellot, P.; Serhrouchni, A. Bubbles of Trust: A decentralized blockchain-based authentication system for IoT. Comput. Secur. 2018, 78, 126–142.
19. Liang, W.; Tang, M.; Long, J.; Peng, X.; Xu, J.; Li, K.C. A Secure Fabric Blockchain-based Data Transmission Technique for Industrial Internet-of-Things. IEEE Trans. Ind. Inform. 2019, 15, 358–3592.
20. Introduction to Data-Sharing Through Blockchain
https://geekyants.com/blog/how-can-blockchain-technology-help-businesses-share-data/
21. Doan T.V., Bajpai V., Psaras Y., Ott J. Towards decentralised cloud storage with IPFS: Opportunities, challenges, and future directions. arXiv. 20222202.06315 [Google Scholar]



INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.165

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details