REVA UNIVERSITY
Bengaluru, India

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING

A Project Report
on

IMPLEMENTATION OF SAEFE(Secure And Efficient File Exchange) PLATFORM

Submitted in fulfillment of the requirements for the award of the Degree of

BACHELOR OF TECHNOLOGY
IN
Computer Science AND Engineering

Submitted by

Shivam Sharma	(R19CS304)
Shivani Yadav	(R19CS306)
Somrit Basnet	(R19CS313)
Sk Md Sahil	(R19CS461)

Under the guidance of

Dr. Argha Sarkar
Associate Professor, School of CSE

May 2023

Rukmini Knowledge Park, Kattigenahalli, Yelahanka, Bengaluru-560064

www.reva.edu.in

REVA UNIVERSITY
Bengaluru, India

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING

A Project Report on

Implementation of the SAEFE Platform using Blockchain Technology

Submitted in fulfilment of the requirements for the award of the Degree of

Bachelor of Technology

Submitted by

Shivam Sharma	(R19CS304)
Shivani Yadav	(R19CS306)
Somrit Basnet	(R19CS313)
SK MD Sahil	(R19CS461)

Under the guidance of

Dr. Argha Sarkar
Associate Professor, School of CSE

2023

Rukmini Knowledge Park, Kattigenahalli, Yelahanka, Bengaluru-560064
www.reva.edu.in

DECLARATION

We, Mr. **SHIVAM SHARMA**, Ms. **SHIVANI YADAV**, Mr. **SOMRIT BASNET**, Mr. **SK MD SAHIL**, students of **Bachelor of Technology**, belonging to **School of Computer Science and Engineering**, REVA University, declare that this Project Report / Dissertation entitled **"Implementation of the SAEFE Platform using Blockchain Technology"** is the result the of project / dissertation work done by us under the supervision of DR. **ARGHA SARKAR,** associate professor at **School of Computer Science and Engineering, REVA University.**

We submitting this Project Report / Dissertation in partial fulfilment of the requirements for the award of the degree of Bachelor of Engineering in Computer Science and Engineering by the REVA University, Bangalore during the academic year 2022-2023.

We declare that this project report has been tested for plagiarism, and has passed the plagiarism test with the similarity score less than 20% and it satisfies the academic requirements in respect of Project work prescribed for the said Degree.

We further declare that this project / dissertation report or any part of it has not been submitted for award of any other Degree / Diploma of this University or any other University/ Institution.

Signature of the candidates with dates

1. *Shivam Sharma (09/05/2023)*
2. *Shivani Yadav(09/05/2023)*
3. *Somrit Basnet(09/05/2023)*
4. *Sk Md Sahil(09/05/2023)*

Certified that this project work submitted by Shivam Sharma, Shivani Yadav, Somrit Basnet and Sk Md Sahil has been carried out under my guidance and the declaration made by the candidate is true to the best of my knowledge.

Signature of Guide

Signature of Director of School

Date: …………….

Date: …………….

Official Seal of the School

REVA UNIVERSITY
Bengaluru, India

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING.

CERTIFICATE

Certified that the project work entitled **Implementation of the SAEFE Platform using Blockchain Technology** carried out under my guidance by **Shivam Sharma, R19CS304, Shivani Yadav, R19CS306, Somrit Basnet, R19CS313, Sk Md Sahil, R19CS461,** are bonafide students of REVA University during the academic year 2022-2023, are submitting the project report in partial fulfilment for the award of **Bachelor of Technology** in Computer Science And Engineering during the academic year **2022-2023.** The project report has been tested for plagiarism, and has passed the plagiarism test with the similarity score less than 20%. The project report has been approved as it satisfies the academic requirements in respect of Project work prescribed for the said Degree.

Signature with date

Dr. Argha Sarkar
Guide

Signature with date

Dr. AshwinKumar UM
Director

External Examiners

Name of the Examiner with affiliation **Signature with Date**

1.

2.

ACKNOWLEDGEMENT

Any given task achieved is never the result of efforts of a single individual. There are always a bunch of people who play an instrumental role leading a task to its completion. Our joy at having successfully finished our mini project work would be incomplete without thanking everyone who helped us out along the way. We would like to express our sense of gratitude to our REVA University for providing us the means of attaining our most cherished goal.

We would like to thank our Hon'ble Chancellor, **Dr. P. Shyama Raju** and Hon'ble Vice-Chancellor, **Dr. M Dhanamjaya** for their immense support towards students to showcase innovative ideas.

We cannot express enough thanks to our respected Director, **Dr. Ashwinkumar U M** for providing us with a highly conducive environment and encouraging the growth and creativity of each and every student. We would also like to offer our sincere gratitude to our Project Coordinators for the numerous learning opportunities that have been provided.

We would like to take this opportunity to express our gratitude to our Project Guide, **Dr. Argha Sarkar**, for continuously supporting and guiding us in our every endeavour as well for taking a keen and active interest in the progress of every phase of our Project. Thank you for providing us with the necessary inputs and suggestions for advancing with our Project work. We deeply appreciate the wise guidance that sir has provided.

Finally, we would like to extend our sincere thanks to all the faculty members, staff from School of Computer Science and Engineering.

Shivam Sharma

Shivani Yadav

Somrit Basnet

Sk Md Sahil

Contents

LIST OF TABLES

LIST OF ILLUSTRATIONS

ABSTRACT

In this era of data it is very essential to develop a mechanism to facilitate people to exchange data with each other however sharing data among different party could become an impossible task due to the risk of security concerns. Currently data sharing occurs with the help of a trusted third party which acts as a mediator between the two party but having a third party risks the security and transparency between the two parties. So in this paper we try to propose a method which is decentralized , secure and fast which can help us to deal with the all the limitations we currently face in the data sharing technology. To establish a decentralized connection between the two parties we make use of the blockchain technology and add several encryptions to the data to make it nearly impossible for the hackers to decode and tamper the data. Hence in this paper we will be trying to highlight the importance of blockchain in the field of data sharing thus allowing us to build a safe pathway for exchanging the data among the peers.

Keywords: Blockchain, IPFS, SHA, AES, smart contract.

1. INTRODUCTION

The amount of data in this world has been increasing exponentially by the. years. According to a study the amount of data in the year 2020 was 59 zettabytes the which is expected to grow up to 175 zettabytes by the year 2075. Working with such large amount data has always been a tedious task specially transferring data from to another. Data sharing is an important aspect of data handling. Every day, millions of bytes of date is shared. Data Sharing although it might seem like a simple task but is a very sensitive task.

Data sharing basically means transferring data from one person to another. To facilitate this a sender needs to access a platform or network which would allow him to make a connection with the receiver. It is a very simple mechanism, but it is extremely important that we make use of correct protocols and mechanisms to ensure that the data's integrity, security, and reliability is maintained.

Currently data sharing among peers is possible only with the help of trusted third-party applications. This method of using third party applications involves several disadvantages such as the lack of decentralized network, proper encryptions, and lack of trustworthiness. Third party applications also lack transparency which gives those apps the monopoly to access the data and even tamper with it. All these issues scare the consumer and does not give them confidence to share their confidential data through these apps.

In this paper we try to find a solution for the data sharing problem that can help us avoid all the limitations of these previous mechanisms which hinders the secure communication. In our project we make use of the blockchain technology. Blockchain is a collection of nodes which collectively forms a decentralized network which connects different parties without need of a third-party application. Another advantage of using blockchain is that it is a secure network which makes it nearly impossible to tamper with.

The next most essential step in data sharing is encryption of the data. Having a secure connection is not just enough so we need to provide a second layer of protection. There are various encryption techniques, but we tend to use Advanced Encryption Standard

(AES) because it is the most secure version and updated form of Data Encryption Standard (DES) & 3DES encryption algorithm. Along with AES we also make use of Secure Hash Algorithm (SHA) which is an inbuilt feature of Interplanetary File System (IPFS).

All together combination of all these mechanisms helps us to achieve our aim of creating a platform which can facilitate users to securely share their confidential data with their peers without having to worry about issues of data leaking and tampering.

2. LITERATURE SURVEY

Blockchain technology has introduced novel ways of creating secure, decentralized, and tamper-proof file sharing systems. Blockchain-based file transfer systems are decentralized, secure, and tamper-proof systems that use blockchain technology to store and manage the file transfer records. The files are encrypted using cryptographic algorithms such as AES, and the digital signature is generated using SHA-256. The files are stored on a decentralized network, such as IPFS, which ensures redundancy and availability of the files. These systems eliminate the need for a centralized intermediary, thus reducing the risk of data breaches and increasing the efficiency of the file transfer process. Additionally, the use of blockchain technology ensures the immutability and authenticity of the files, making it an ideal solution for sensitive data transfers.

By combining these technologies, the proposed file transfer system can leverage the strengths of each technology. AES provides strong encryption for the file transfer, SHA-256 ensures message authentication to prevent tampering or data corruption during transfer, and IPFS enables decentralized and efficient storage and distribution of the files. The proposed file transfer system can provide a secure and efficient file transfer mechanism for a wide range of applications. The system can benefit from the strengths of each technology and offer a robust solution to file transfer challenges. Future work can focus on improving scalability, security, and usability of the system.

In [1]. "Design and Implementation of a File Transfer System using IPFS and Blockchain" by Carlos Diaz, Juan Carlos Hurtado, and Felipe Restrepo, published in the IEEE Latin America Transactions in 2018. The paper presents a novel file transfer system that combines Interplanetary File System (IPFS) and blockchain technologies to achieve a decentralized and secure file sharing mechanism. In the paper the authors discuss about the related work on IPFS and blockchain-based file sharing systems and highlight the limitations of existing systems. They then propose a novel file transfer system that utilizes IPFS for storage and sharing of files and blockchain for maintaining a ledger of transactions and ensuring file integrity. The authors provide a detailed description of the system architecture and components, including the client, server, and blockchain components.

The authors evaluate the performance of the system in terms of throughput, latency, and resource utilization. The experimental results show that the proposed system provides a decentralized and secure file sharing mechanism with high throughput and low latency. The paper concludes by highlighting the benefits of the proposed system and suggesting future work to improve scalability and security by incorporating advanced blockchain technologies. Overall, the paper presents a valuable contribution to the field of decentralized file sharing systems by combining IPFS and blockchain technologies to address the limitations of centralized file sharing systems. The proposed system has the potential to provide a secure and decentralized file sharing mechanism for a wide range of applications.

In [2]. "A Decentralized File Transfer System Based on IPFS and DHT" by Chenggang Xu, Wei Wu, and Sheng Liu, published in the Journal of Networks and Computer Applications in 2019. The paper presents a decentralized file transfer system based on Interplanetary File System (IPFS) and Distributed Hash Table (DHT) technologies. The proposed system is designed to overcome the limitations of centralized file sharing systems by providing a decentralized, secure, and efficient file transfer mechanism. The authors discusses the limitations of centralized file sharing systems, such as data loss, single point of failure, and data tampering. They then propose a novel file transfer system that utilizes IPFS and DHT to address these limitations. The proposed system consists of four components: client, tracker, IPFS node, and DHT node.

The authors provide a detailed description of the system architecture and components, including the data flow and communication protocols between components. They also present an evaluation of the performance of the proposed system in terms of throughput, latency, and resource utilization. The experimental results show that the proposed system provides a decentralized, secure, and efficient file transfer mechanism with high throughput and low latency.

The paper concludes by highlighting the benefits of the proposed system and suggesting future work to improve scalability and security by incorporating advanced encryption and authentication mechanisms. Overall, the paper presents a valuable contribution to the field of decentralized file sharing systems by combining IPFS and DHT technologies to address the limitations of centralized file sharing systems. The proposed system has the potential to provide a decentralized, secure, and efficient file transfer mechanism for a wide range of applications.

In [3]. "File Transfer Security System Based on SHA-256 and AES Algorithms" by P. M. Narayanan, V. N. Senthilkumar, and S. Arulselvi, published in the International Journal of Engineering and Technology in 2018. The paper presents a file transfer security system based on the SHA-256 and AES algorithms to address the security concerns in file transfer systems. The proposed system provides a secure and efficient file transfer mechanism by using SHA-256 for message authentication and AES for encryption. The authors discusses about the limitations of existing file transfer systems and the need for secure file transfer systems. They then propose a novel file transfer security system that utilizes SHA-256 and AES algorithms. The proposed system consists of three components: sender, receiver, and security module. The authors provide a detailed description of the system architecture and components, including the encryption and decryption algorithms used for file transfer. They also present an evaluation of the performance of the proposed system in terms of throughput, latency, and resource utilization. The experimental results show that the proposed system provides a secure and efficient file transfer mechanism with high throughput and low latency.

The paper concludes by highlighting the benefits of the proposed system and suggesting future work to improve scalability and security by incorporating advanced encryption and authentication mechanisms. Overall, the paper presents a valuable contribution to the field of secure file transfer systems by combining SHA-256 and AES algorithms to address the security concerns in file transfer systems. The proposed system has the potential to provide a secure and efficient file transfer mechanism for a wide range of applications.

In [4]. "AES-based File Transfer System for Secure Communication" by Tarek Saadawi, Shashikala Tapaswi, and Sherali Zeadally, published in the Journal of Computer Security in 2010. The paper presents an AES-based file transfer system for secure communication to address the security concerns in file transfer systems. The proposed system provides a secure and efficient file transfer mechanism by using the Advanced Encryption Standard (AES) algorithm. The authors discusses about the limitations of existing file transfer systems and the need for secure file transfer systems. They then propose a novel file transfer system that utilizes AES for encryption. The proposed system consists of two components: sender and receiver. The authors provide a detailed description of the system architecture and components, including the encryption and decryption algorithms used for file transfer. They also present an evaluation of the performance of the proposed system in terms of throughput, latency, and resource utilization. The experimental results show that the proposed system provides a secure and efficient file transfer mechanism with high throughput and low latency.

The paper concludes by highlighting the benefits of the proposed system and suggesting future work to improve scalability and security by incorporating advanced encryption and authentication mechanisms. Overall, the paper presents a valuable contribution to the field of secure file transfer systems by utilizing the AES algorithm to address the security concerns in file transfer systems. The proposed system has the potential to provide a secure and efficient file transfer mechanism for a wide range of applications.

In [5]. "A Secure and Efficient File Transfer System using Hybrid Cryptography" by P. Rajesh and K. R. Babu in 2019. The paper proposes a novel approach for a secure and efficient file transfer system using hybrid cryptography. The authors propose combining symmetric key cryptography (AES) and asymmetric key cryptography (RSA) to provide enhanced security and efficiency. The paper begins by discussing the need for secure file transfer systems and the importance of cryptography in achieving this goal. The authors then provide an overview of symmetric and asymmetric key cryptography and explain their strengths and weaknesses. They propose combining the two techniques to leverage their respective strengths, resulting in a more secure and efficient file transfer system. The proposed system is designed to provide confidentiality, integrity, and authentication of transferred data. The system uses AES to encrypt data at the sender's end and RSA to encrypt the AES key. The encrypted data and key are then transmitted to the receiver, who decrypts the key using RSA and then uses it to decrypt the data using AES.

The paper provides a detailed description of the proposed system's architecture and workflow, including the encryption and decryption processes. The authors also conducted experiments to evaluate the system's performance in terms of security and efficiency. The results show that the proposed system provides robust security and efficient data transfer compared to other existing systems. The paper concludes by highlighting the strengths of the proposed system and its potential for practical implementation in various scenarios that require secure and efficient file transfer systems. However, the authors also acknowledge the need for further research to optimize the proposed system's performance and ensure its scalability for large-scale file transfer applications. Overall, the paper provides a comprehensive overview of the proposed hybrid cryptography-based file transfer system, its architecture, and its evaluation results, making it a valuable contribution to the field of secure file transfer systems.

In[6]. Secure File Transfer using Blockchain Technology" by J. Lee and J. Lee (2019) proposes a secure file transfer system that uses blockchain technology to ensure data integrity and confidentiality in file transfer. The paper highlights the limitations of traditional file transfer methods, such as email or cloud storage, and proposes blockchain as a solution to these limitations. The paper begins by providing an overview of blockchain technology and its applications in various fields. The authors then describe the proposed file transfer system, which consists of three modules: the file upload module, the file download module, and the blockchain module. The file upload module encrypts the file and uploads it to the blockchain, while the file download module decrypts the file and downloads it from the blockchain. The blockchain module ensures the integrity and confidentiality of the file transfer by using cryptographic techniques to secure the file.

In[7]. File sharing and storage using blockchain technology" by H. Gupta and R. Jain (2018) proposes a file sharing and storage system that uses blockchain technology to provide secure and efficient file transfer and storage. The paper highlights the limitations of traditional file sharing methods and cloud storage solutions and proposes blockchain as a solution to these limitations.

The authors evaluate the performance of the proposed system by measuring the time required for file transfer and the storage space required for the blockchain and file storage system. The results show that the proposed system is efficient in terms of file transfer time and storage space. The paper also discusses the security implications of the proposed system, including the possibility of attacks on the blockchain network and the distributed file storage system. The authors propose several measures to mitigate these attacks, such as using consensus algorithms, encryption techniques, and access control policies.

In[8]. "A blockchain-based file transfer system for P2P networks" by E. Y. Kim et al. (2019) proposes a blockchain-based file transfer system for peer-to-peer (P2P) networks. The paper highlights the limitations of traditional P2P file transfer systems and proposes blockchain as a solution to these limitations. Overall, "A blockchain-based file transfer system for P2P networks" provides a comprehensive overview of the proposed system and its potential applications in P2P file transfer. The paper presents a novel approach to secure and efficient file transfer using blockchain technology, which could be beneficial in various fields that require secure and efficient P2P file transfer.

In[9]&[10] "A Data Transfer Protocol Using SHA-3" by S. M. Jaffar et al. (2019) proposes a data transfer protocol that uses SHA-3 for secure and efficient data transfer and Data Transfer Based on SHA-1 Hash Algorithm" by X. Gu et al. (2017) proposes a data transfer method based on SHA-1 hash algorithm for secure and efficient data transfer. Overall, both papers demonstrate the potential of using SHA for secure and efficient data transfer. "A Data Transfer Protocol Using SHA-3" focuses on the use of SHA-3, which is a relatively new hash function, and provides a novel approach to data transfer protocol design. "Data Transfer Based on SHA-1 Hash Algorithm" provides a detailed analysis of using SHA-1 for data transfer and compares it with other hash functions. Both papers highlight the importance of secure and efficient data transfer in various fields and provide insights into the design and evaluation of data transfer protocols and methods that use SHA.

3. POSITIONING

I. Problem Statement

There is a growing need for secure and efficient data transfer platforms to ensure that data is transmitted safely between parties. Existing data transfer platforms often lack security features, leading to data breaches and compromising sensitive information. Additionally, there are issues of data tampering, loss, and redundancy. These issues can lead to a lack of trust between parties and can impact the overall reliability of the data transfer system.

Blockchain technology has shown great potential in addressing these issues, as it provides a secure and immutable way of storing and transmitting data. However, there are still challenges that need to be addressed when implementing blockchain-based data transfer platforms, such as scalability, interoperability, and user-friendliness.

The traditional encryption systems have also lost their charm and are easily decoded using the technology available in today’s time but with advancing technology we have also seen the advancement in encryption techniques. We need to figure out which of the encryption techniques would be best fit to help secure data while transferring.

Therefore, the problem statement for this project is to develop a data transfer platform using blockchain that addresses these challenges and provides a secure and efficient way of transmitting data between parties. The platform should be scalable, interoperable, user-friendly, and should ensure the privacy and confidentiality of the transmitted data.

4. PROJECT OVERVIEW

I. Objectives

The main objective of the project is to create a web application named “SAEFE” which will allow users to connect to the blockchain which will be a shared network that will connect the sender and receiver. After connecting to the blockchain the web application should allow users to either upload data or download data based on the users demand. The web application should allow its users to securely transfer data from one point to another and avoid any kind of tampering that can affect data’s reliability, security and integrity. The web application must provide a smooth experience to its user and give them a hassle free experience to transfer files.

II. Goals

Our goal is to develop a platform that will empower its users with features like

Enhanced data security: By using blockchain technology, data sharing can be more secure as it offers a tamper-resistant, decentralized system that can prevent unauthorized access, modification, or deletion of data.

Increased transparency: Blockchain allows for a transparent system that provides a comprehensive and immutable record of all data transactions, enabling data owners and users to trace and audit data usage.

Efficient data sharing: Blockchain-based systems can streamline the data sharing process, as they enable automated and secure data exchange among multiple parties in real-time, eliminating the need for intermediaries.

Improved data ownership: Blockchain technology can enable users to have greater control over their data and how it is shared, allowing them to monetize their data or selectively share it with trusted parties.

5. METHODOLOGY

Blockchain can be regarded as a record where all the transactions between the parties is stored. It is a decentralized system where the records are kept in blocks which are linked together and is secured using cryptography. These blocks use the hash value to identify the data in the blocks This hash is used to link the previous blocks which is very difficult to temper. Blockchains are generally used to record transactions for cryptocurrency or storing votes to prevent it from being tempered.

IPFS is a network for storing, sharing, and distributing files. It as a decentralized System which is more efficient and resilient then the HTTP-based web protocols. Nodes are used in IPFS as the files are split into small pieces and distributed across the nodes. A unique cryptographic hash for each file is required for the verification and retrieval of the data in the file. This is possible because for any two different contents of same data has the same hash.

AES (Advanced Encryption Standard) is a widely used symmetric key encryption algorithm, which means that the same key is used to encrypt and decrypt data. AES works by dividing plain text into 128-bit blocks, then applying a series of mathematical operations to each block using a 128, 192, or 256-bit key. The length of the key determines the number of encryption cycles performed. Decryption is just the reverse process, and each encryption cycle takes place in reverse order. AES is considered very secure and there are no known practical attacks that can break the encryption when strong keys are used.

SHA-256 (Secure Hash Algorithm 256) is a widely used cryptographic hash function that generates a fixed-size 256-bit (32-byte) message digest or hash value from an input message of arbitrary length. The SHA-256 algorithm has several properties that make it useful in cryptographic applications. First, it is a one-way function, which means that it is impossible to reverse the hash and determine the original input message. Second, even small changes in the input message can result in completely different hashes, which is useful for tracking data changes. Finally, the algorithm produces a fixed-length hash value, which is useful for verifying data integrity. SHA-256 has a wide range of applications, including digital signatures, message authentication codes, and password safekeeping.

6. PROJECT IMPLEMENTATION

I. Architectural Design

The first step in data encryption is to upload the required files to the IPFS platform. Once a file is uploaded to IPFS, IPFS then generates a hash of the data and returns it to the owner. In our proposed case, system nodes are created and their public and private key pairs are generated and stored in a smart contract. When the owner receives the hash function of the original data from IPFS, it starts searching the smart contract for verified system nodes that have the responsibility of providing decryption services to clients. Only the data sharing platform is equipped with the ability to provide users with the requested services provided by the owner. When the owner receives the hash function, it starts dividing it into "k" shares. After these shares are created, the owner then generates "n" numbers of random keys to use for encryption. After encrypting all these shares with the appropriate keys, they are then stored on the blockchain and supplemented with other important information such as authorized recipients of the files and much more. Data security is provided by cryptographic hashing because hashing is inherently insecure as it is just a unique fingerprint that simply represents some data, so if the hash was accessed by an unauthorized client who did not commit the digital content, the entire data could be file directly loaded from IPFS. The owner will lose the business completely. In the proposed scenario, only clients who have injected resources and are authorized by worker nodes can decrypt the hash. The overall process of an owner uploading files to IPFS is shown in Figure 1. This whole process means completing the complete architecture of the data sharing process using our platform.

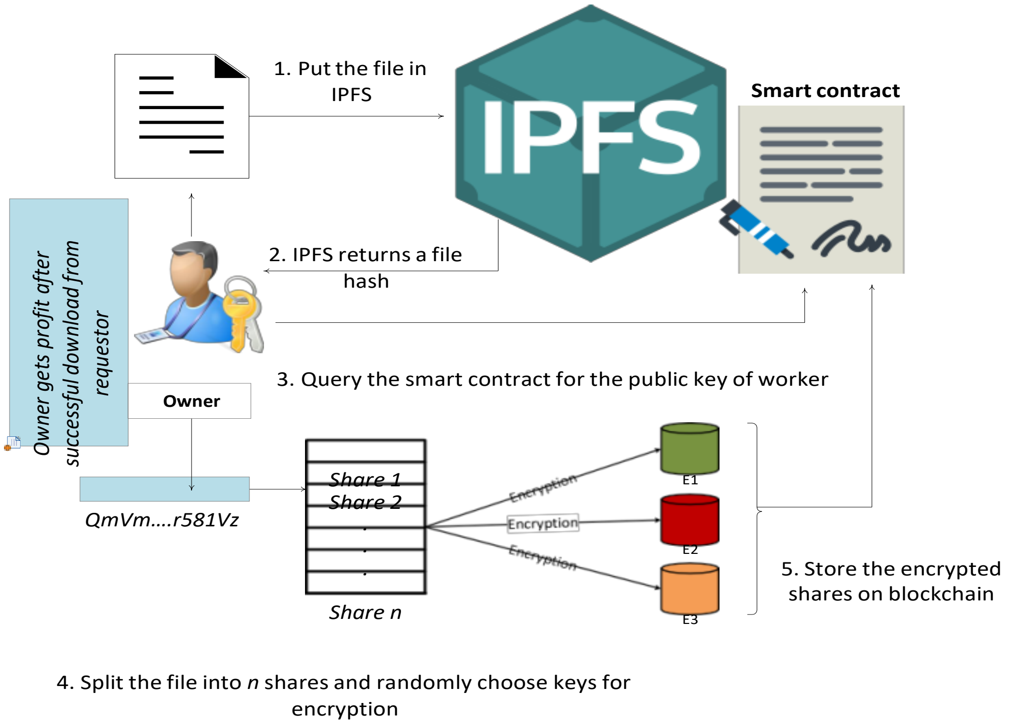

1. Put the file in IPFS
IPFS
Smart contract
2. IPFS returns a file hash
Owner gets profit after successful download from requestor
Owner
3. Query the smart contract for the public key of worker
QmVm....r581Vz
Share 1
Share 2
.
.
.
Share n
Encryption
Encryption
Encryption
E1
E2
E3
5. Store the encrypted shares on blockchain
4. Split the file into *n* shares and randomly choose keys for encryption

Fig 1: System Architecture

II. Entity Relationship Model

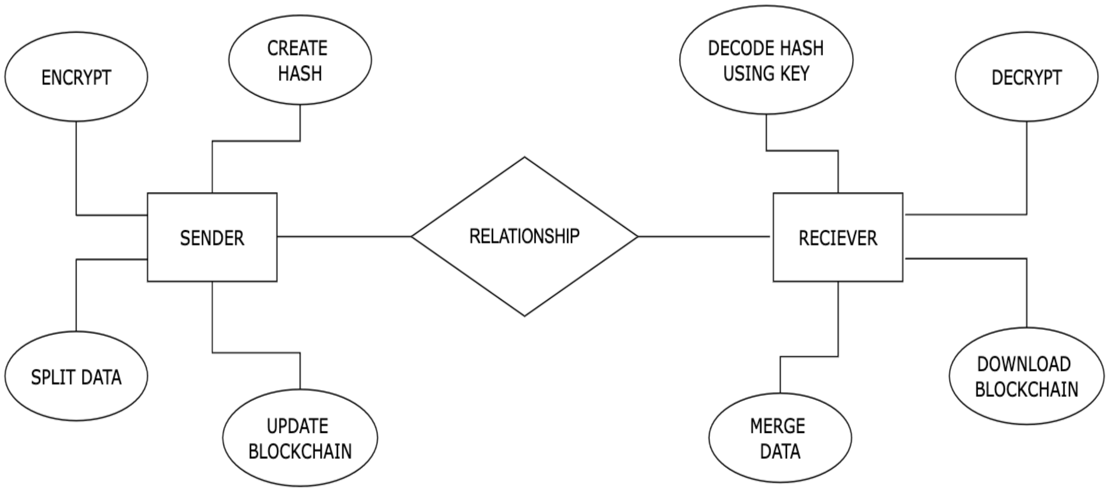


Fig 2: E-R Model

III. Sequence Diagram

The process starts when the client wants to access the data, so it sends a request to the system. The request made by the user is combined with the customer's digital signature. The New applicants are first verified by the system using an Rivest-Shamir-Adleman (RSA) algorithm. RSA is an asymmetric algorithm which generates a public key and a private key pair where the private key is kept secret and confidential whereas on the other hand public key is shared to all other authorized users. If the recipient is not an authorized user or identified as a non-valid requester, then the smart contract is terminated automatically, and the system ignores the received request. While in the other case when the requestor is a valid user, system starts retrieving the encrypted data from the blockchain and decrypts them using their private keys. The most essential point to note here is that if the owner chooses their public key when sharing the data over IPFS, the system can only decrypt the share on behalf of the recipient. After decryption, the recipient can obtain the hash value of the original IPFS file by reconstruction. This marks the completion of the whole process with user obtaining the desired data they requested for to the system.

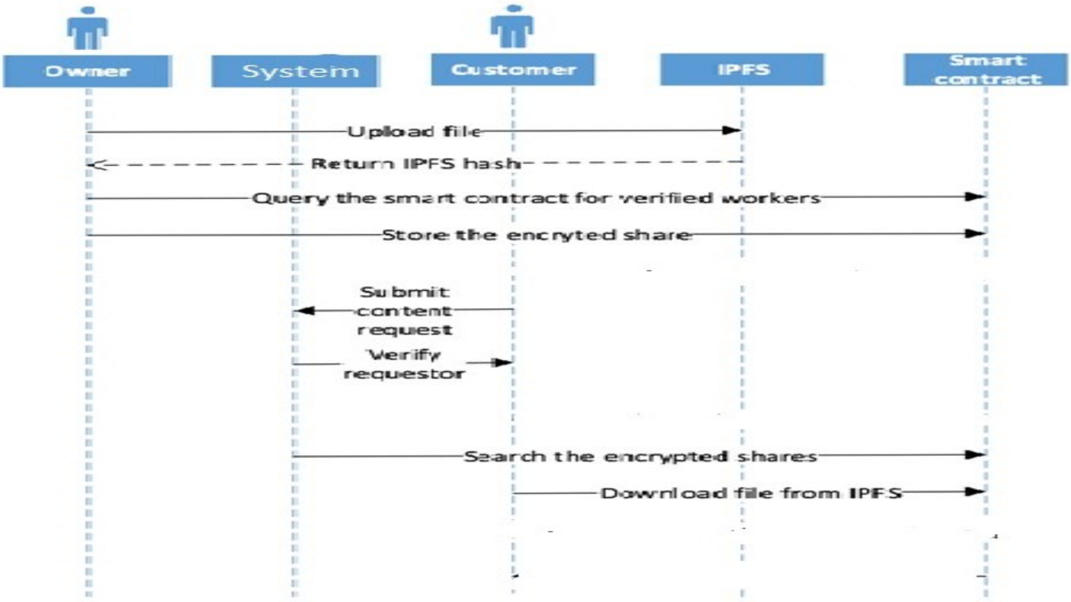


Fig 3: Sequence Diagram

IV. Description of Technology Used

Blockchain:

Blockchain is a decentralized, distributed ledger technology that records and verifies transactions in a secure, transparent, and tamper-proof manner. It operates on a peer-to-peer network of computers, where each computer maintains a copy of the ledger, ensuring that there is no central point of control.

One of the key features of blockchain is its security. Each block in the chain is linked to the previous block using cryptographic algorithms, making it difficult to alter the contents of the ledger without the consensus of the network. This makes blockchain an ideal solution for applications that require secure and tamper-proof record-keeping, such as financial transactions, supply chain management, and voting systems.

Blockchain technology is also known for its transparency. As each node on the network has a copy of the ledger, any changes made to the chain are visible to all participants, creating a transparent and auditable record of all transactions.

Inter Planetary File System (IPFS):

IPFS, or Inter Planetary File System, is a distributed peer-to-peer protocol designed to create a global, decentralized file system that is faster, more secure, and more reliable than traditional HTTP-based protocols.

IPFS is a protocol, hypermedia, and file sharing peer-to-peer network for storing and sharing data in a distributed file system. IPFS uses content-addressing to uniquely identify each file in a global namespace connecting IPFS hosts.

One of the key benefits of IPFS is its ability to reduce duplication of content. When a file is added to IPFS, it is broken up into chunks and hashed using a cryptographic algorithm. Each chunk is then given a unique content-based address that can be used to retrieve the chunk from any node on the network that has a copy of it. This means that if multiple users add the same file to IPFS, only one copy of the file is stored on the network, reducing redundancy, and improving efficiency.

AES Encryption:

AES (Advanced Encryption Standard) is a widely used symmetric-key encryption algorithm used for securing sensitive data. It was first adopted by the US government as a replacement for the previous encryption standard, DES (Data Encryption Standard), and is now widely used in industries and organizations around the world.

AES encryption involves three key steps:

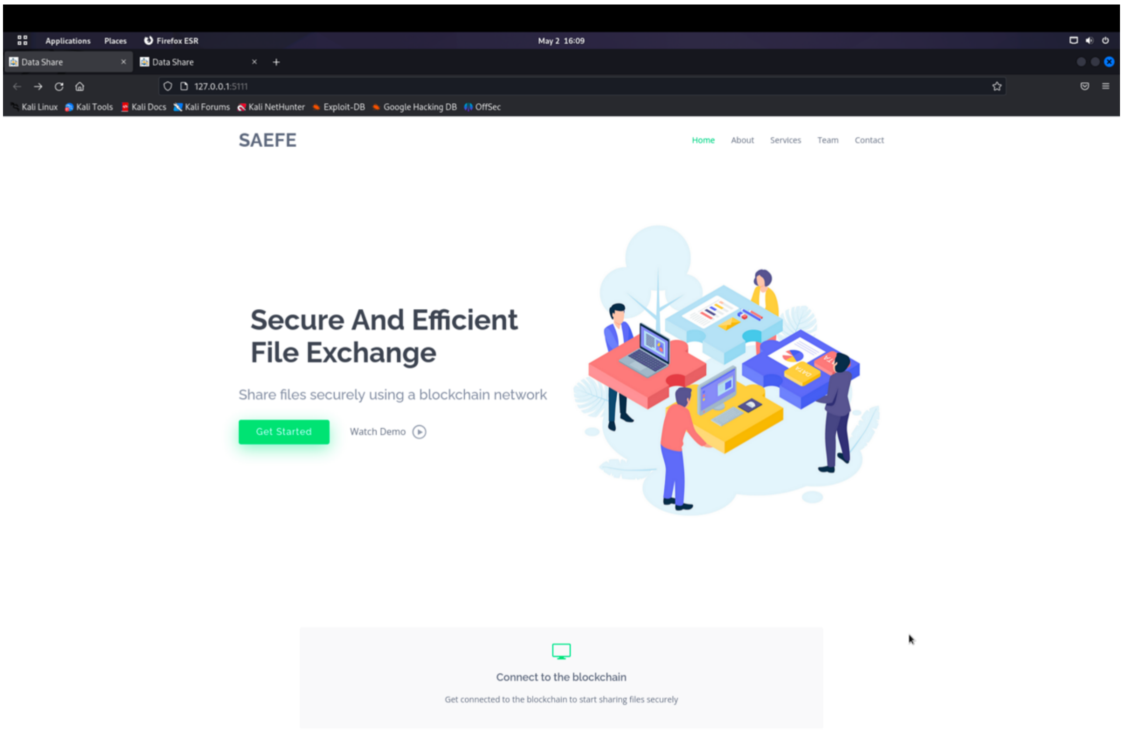
Key Generation: The first step in AES encryption is key generation, where a random secret key is generated. This key is used to encrypt and decrypt the data, and it is important to keep it secure.

Substitution: The second step is substitution, where the input data is replaced with a set of predefined substitution tables. This helps to increase the randomness of the output and makes the encryption more secure.

Permutation: The third and final step is permutation, where the output of the substitution step is rearranged using a set of permutation tables. This step adds additional randomness to the output and makes it even more difficult to crack.

7. RESULT AND ANALYSIS

The Home Page of our website is depicted in Fig 4, which will act as a portal for the users to establish connection with each other and accessing the multiple functionalities. It allows user to connect to the blockchain.



Secure And Efficient File Exchange

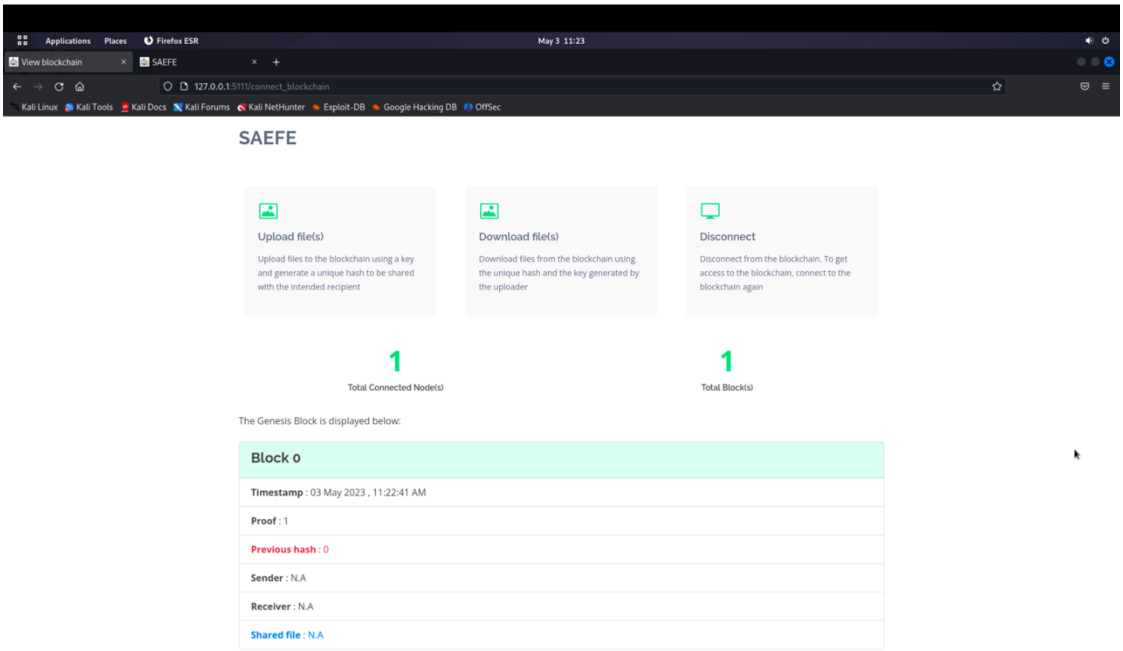
Share files securely using a blockchain network

Connect to the blockchain

Get connected to the blockchain to start sharing files securely

Fig 4: Home Page of the Web Portal

The next page depicted in the figure 5 displays all the option a user can choose to perform such as uploading , deleting or disconnecting from the blockchain.



SAEFE

Upload file(s)

Upload files to the blockchain using a key and generate a unique hash to be shared with the intended recipient

Download file(s)

Download files from the blockchain using the unique hash and the key generated by the uploader

Disconnect

Disconnect from the blockchain. To get access to the blockchain, connect to the blockchain again

1 Total Connected Node(s)

1 Total Block(s)

The Genesis Block is displayed below:

Block 0

Timestamp : 03 May 2023 , 11:22:41 AM

Proof : 1

Previous hash : 0

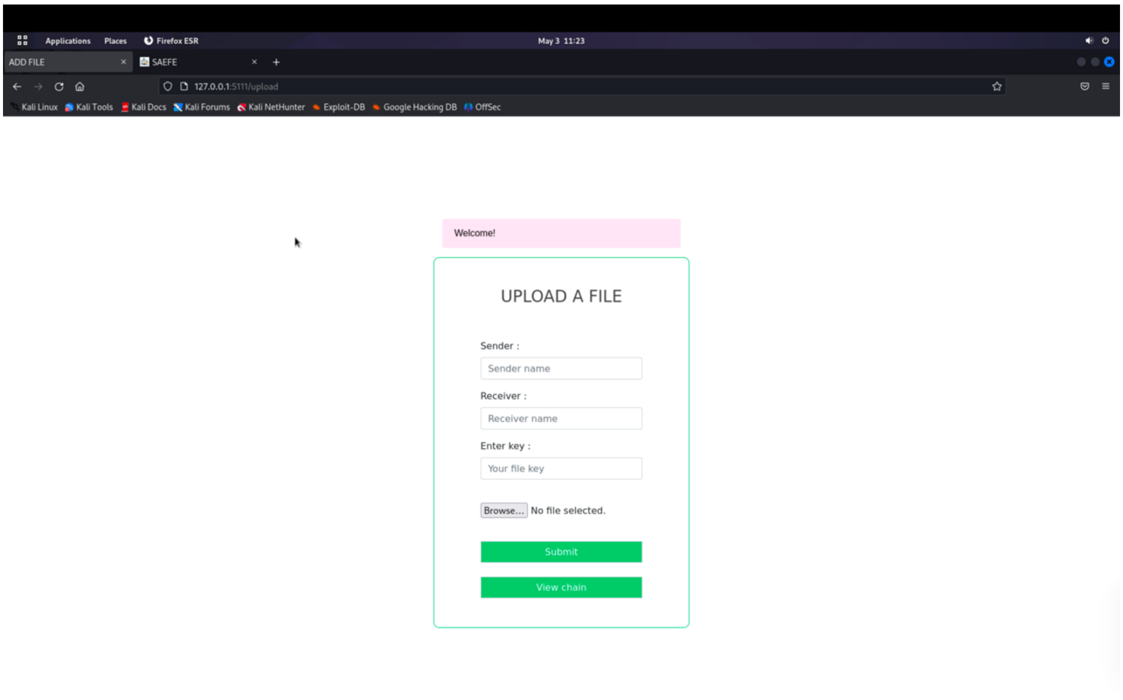
Sender : N.A

Receiver : N.A

Shared file : N.A

Fig 5: Option display page

The next two screenshots figure 6 and figure 7 displays the portal which will facilitate users to download and upload the file into the blockchain.



Welcome!

UPLOAD A FILE

Sender : Sender name

Receiver : Receiver name

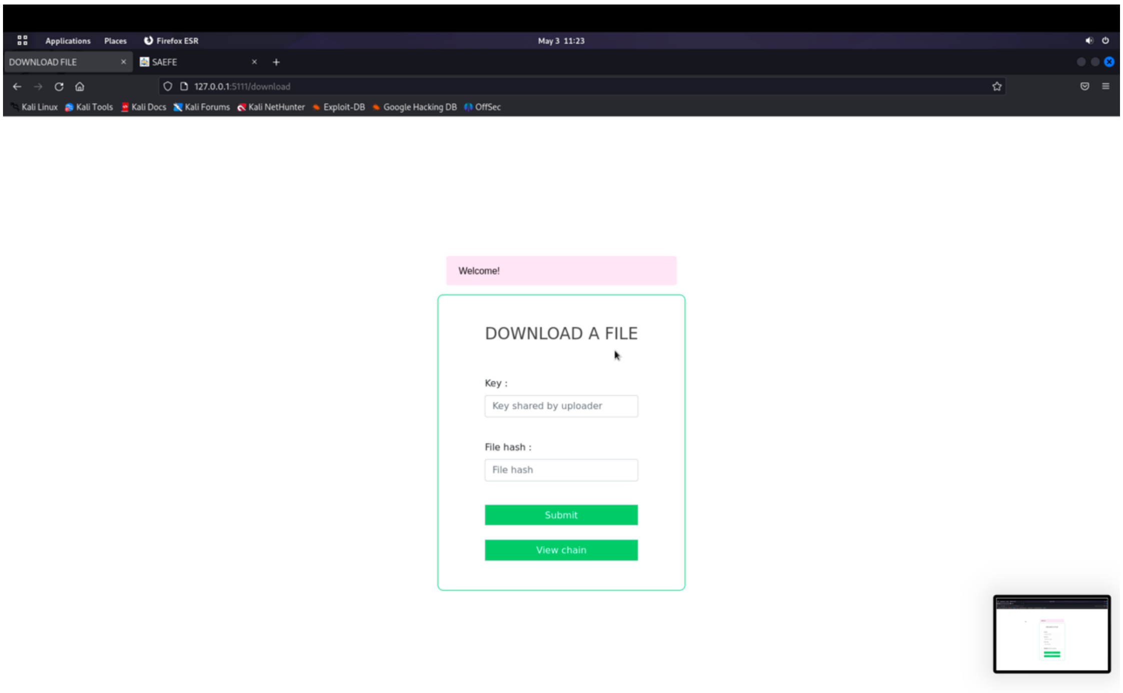
Enter key : Your file key

Browse... No file selected.

Submit

View chain

Fig 6: Uploading page



Welcome!

DOWNLOAD A FILE

Key :

Key shared by uploader

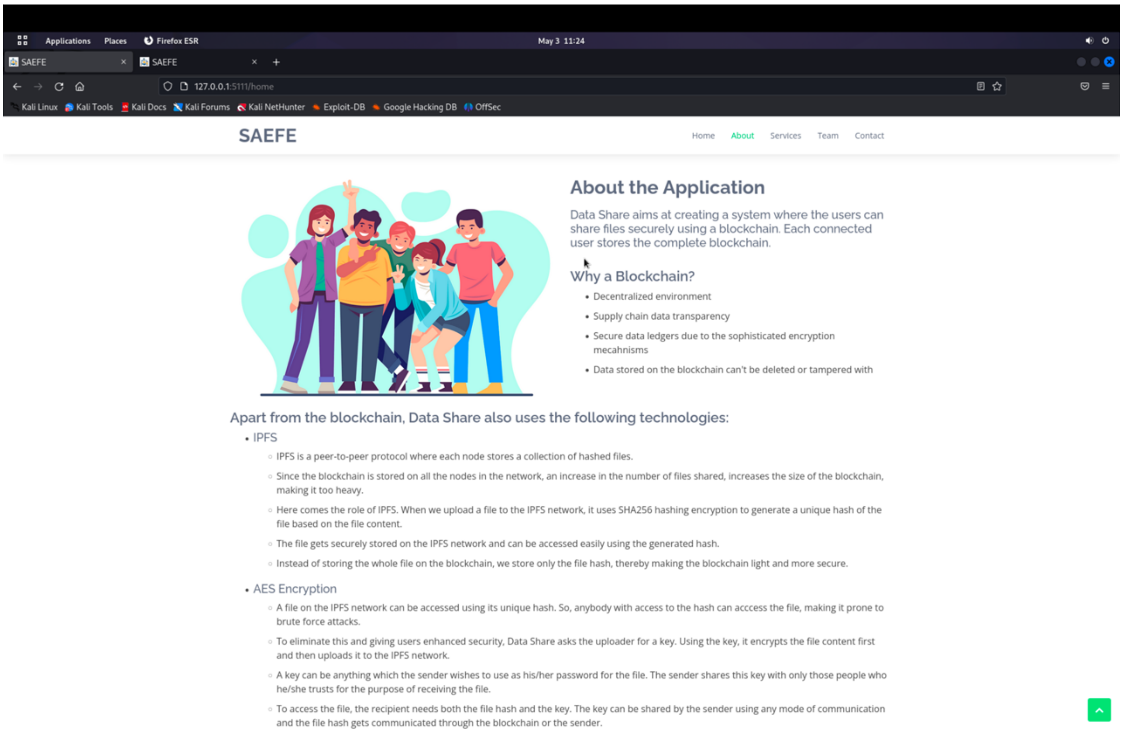
File hash :

File hash

Submit

View chain

Fig 7: Download Page



About the Application

Data Share aims at creating a system where the users can share files securely using a blockchain. Each connected user stores the complete blockchain.

Why a Blockchain?

- Decentralized environment
- Supply chain data transparency
- Secure data ledgers due to the sophisticated encryption mecahnisms
- Data stored on the blockchain can't be deleted or tampered with

Apart from the blockchain, Data Share also uses the following technologies:

- IPFS
  - IPFS is a peer-to-peer protocol where each node stores a collection of hashed files.
  - Since the blockchain is stored on all the nodes in the network, an increase in the number of files shared, increases the size of the blockchain, making it too heavy.
  - Here comes the role of IPFS. When we upload a file to the IPFS network, it uses SHA256 hashing encryption to generate a unique hash of the file based on the file content.
  - The file gets securely stored on the IPFS network and can be accessed easily using the generated hash.
  - Instead of storing the whole file on the blockchain, we store only the file hash, thereby making the blockchain light and more secure.
- AES Encryption
  - A file on the IPFS network can be accessed using its unique hash. So, anybody with access to the hash can acccess the file, making it prone to brute force attacks.
  - To eliminate this and giving users enhanced security, Data Share asks the uploader for a key. Using the key, it encrypts the file content first and then uploads it to the IPFS network.
  - A key can be anything which the sender wishes to use as his/her password for the file. The sender shares this key with only those people who he/she trusts for the purpose of receiving the file.
  - To access the file, the recipient needs both the file hash and the key. The key can be shared by the sender using any mode of communication and the file hash gets communicated through the blockchain or the sender.

Fig 8: About Page

8. COST OF THE PROJECT

Table 1: Cost of the Project

S.NO	**COMPONENT**	**COST**
1	IPFS	Not Applicable
2	VS Code	Not Applicable
3	Python	Not Applicable
4	Flask	Not Applicable
5	SHA-256 & AES	Not Applicable
6	Publication	Rs 7000
7	Web Hosting Service	Not Applicable
Total Cost		Rs. 7000 /-

9. CONCLUSIONS

In conclusion, data sharing using blockchain and IPFS (Interplanetary File System) has become a safe and efficient way to share data over networks. Blockchain technology provides a decentralized and immutable ledger that guarantees data integrity and authenticity, while IPFS provides a distributed file system that enables fast and reliable access to shared data. By combining these technologies, data sharing becomes more secure, transparent, and efficient, allowing organizations and individuals to exchange data without the need for intermediaries or central authorities. This not only reduces the cost and complexity associated with traditional methods of data sharing, but also improves data privacy and control.

However, there are also limitations and challenges associated with data sharing using blockchain. Scalability, storage capacity, energy consumption, cost, and lack of standardization are some of the key limitations that need to be addressed. In addition, ensuring data privacy, confidentiality, and compliance with regulations can be challenging in some use cases.

Moreover, blockchain and IPFS technology can be applied in various fields, such as healthcare, finance, supply chain management, and more, where data security and privacy are crucial. data sharing using blockchain technology has the potential to transform how data is shared and managed, but it requires careful consideration of the specific use case, as well as a thoughtful and strategic approach to implementation and management. As the demand for secure and reliable data sharing continues to grow, the use of blockchain and IPFS technology is expected to increase, providing more innovative solutions to the data sharing challenges of today and tomorrow.

Overall, data sharing using blockchain technology has the potential to transform how data is shared and managed, but it requires careful consideration of the specific use case, as well as a thoughtful and strategic approach to implementation and management. While blockchain is not a silver bullet for all data sharing challenges, it is a powerful tool that can be leveraged to improve the security and transparency of data sharing in many contexts.

10. PROJECT LIMITATION

Blockchain technology has many benefits, including transparency, security, and decentralization, it also has some limitations when it comes to data transfer. While blockchain technology has been touted as a solution to various problems related to data transfer and security, it also has some limitations when it comes to data transfer. The project also have these limitations which are needed to be solved in the future. Main limitations are mentioned below.

One of the biggest limitations of blockchain technology is scalability. Blockchain networks are designed to be decentralized and secure, which makes it difficult to increase the speed and volume of data transfer. As the number of users and transactions on the network increases, it becomes slower and more expensive to transfer data.

Storing data on a blockchain can be expensive, as each transaction needs to be recorded and verified by network participants. This can limit the amount of data that can be stored on the blockchain.

Data stored on a blockchain may be subject to regulatory requirements, such as data protection laws or industry-specific regulations. Meeting these requirements can be challenging, as blockchain technology is still relatively new and may not be well-understood by regulators.

The process of validating transactions on a blockchain network requires a lot of computational power, which consumes a significant amount of energy. This makes it an expensive and unsustainable solution for data transfer, especially for large-scale applications.

AES and SHA are widely used and considered to be strong cryptographic algorithms they do have some limitations. It is important to carefully consider the specific use case and threat model when selecting and implementing cryptographic algorithms.

Overall, while blockchain technology has potential for secure data transfer, it is not without limitations, especially when it comes to scalability, storage capacity, energy consumption, cost, and lack of standardization.

11. REFERENCES

[1] Understanding Blockchain Technology Abstracting the Blockchain https://ieeexplore.ieee.org/courses/details/EDP521

[2] Understanding Blockchain Technology: The Costs and Benefits of Decentralization https://ieeexplore.ieee.org/courses/details/EDP522?t ag=1

[3] An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends https://ieeexplore.ieee.org/document/8029379

[4] Integrating blockchain for data sharing and collaboration in mobile healthcare applications X Liang, J Zhao, S Shetty, J Liu… - 2017 IEEE 28th Annual https://ieeexplore.ieee.org/document/7749510

[5] Chen, Y.; Li, H.; Li, K.; Zhang, J. An improved P2P file system scheme based on IPFS and Blockchain. In Proceedings of the 2017 IEEE International Conference on Big Data (Big Data), Boston, MA, USA,11–14 December 2017; pp. 2652–2657.

[6] Dai, M.; Zhang, S.Wang, H. Jin. A low storage room requirement framework for distributed ledger in the blockchain. IEEE Access 2018, 6, 22970–22975.

[7] L. Yue, H. Junqin, Q. Shengzhi, and W. Ruijin, “Big data model of security sharing based on blockchain,” in Proc. 3rd Int. Conf. Big Data Comput. Commun. (BIGCOM), 2017, pp. 117–121.

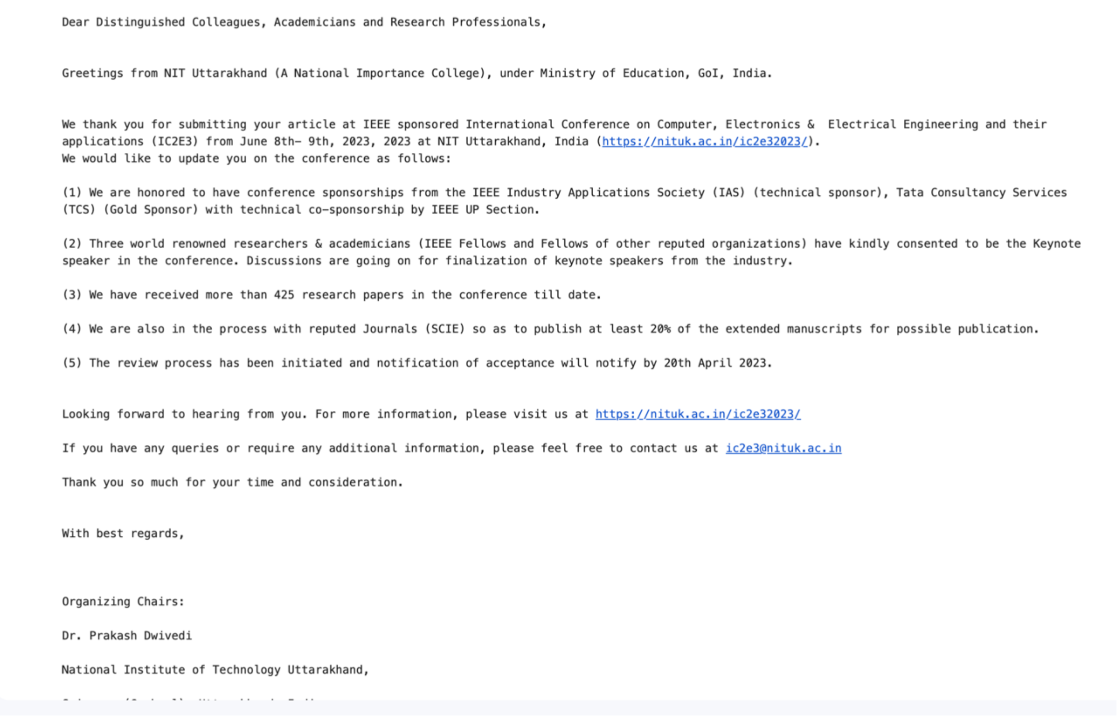
[8] Z. Li et al., “Consortium blockchain for secure energy trading in the industrial Internet of Things,” IEEE Trans. Ind. Informat., vol. 14, no. 8, pp. 3690–3700, Aug. 2018.

[9] Y. Yuan and F.-Y. Wang, “Towards blockchain-based intelligent transportation systems,” in Proc. IEEE 19th Int. Conf. Intell. Transp. Syst. (ITSC), Nov. 2016, pp. 2663–2668.

[10] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung, “Blockchain-based decentralized trust management in vehicular networks,” IEEE Internet Things J., to be published.

12. COPIES OF ARTICLES

I. Conference Paper Submittance



Dear Distinguished Colleagues, Academicians and Research Professionals,

Greetings from NIT Uttarakhand (A National Importance College), under Ministry of Education, GoI, India.

We thank you for submitting your article at IEEE sponsored International Conference on Computer, Electronics & Electrical Engineering and their applications (IC2E3) from June 8th- 9th, 2023, 2023 at NIT Uttarakhand, India (https://nituk.ac.in/ic2e32023/).
We would like to update you on the conference as follows:

(1) We are honored to have conference sponsorships from the IEEE Industry Applications Society (IAS) (technical sponsor), Tata Consultancy Services (TCS) (Gold Sponsor) with technical co-sponsorship by IEEE UP Section.

(2) Three world renowned researchers & academicians (IEEE Fellows and Fellows of other reputed organizations) have kindly consented to be the Keynote speaker in the conference. Discussions are going on for finalization of keynote speakers from the industry.

(3) We have received more than 425 research papers in the conference till date.

(4) We are also in the process with reputed Journals (SCIE) so as to publish at least 20% of the extended manuscripts for possible publication.

(5) The review process has been initiated and notification of acceptance will notify by 20th April 2023.

Looking forward to hearing from you. For more information, please visit us at https://nituk.ac.in/ic2e32023/

If you have any queries or require any additional information, please feel free to contact us at ic2e3@nituk.ac.in

Thank you so much for your time and consideration.

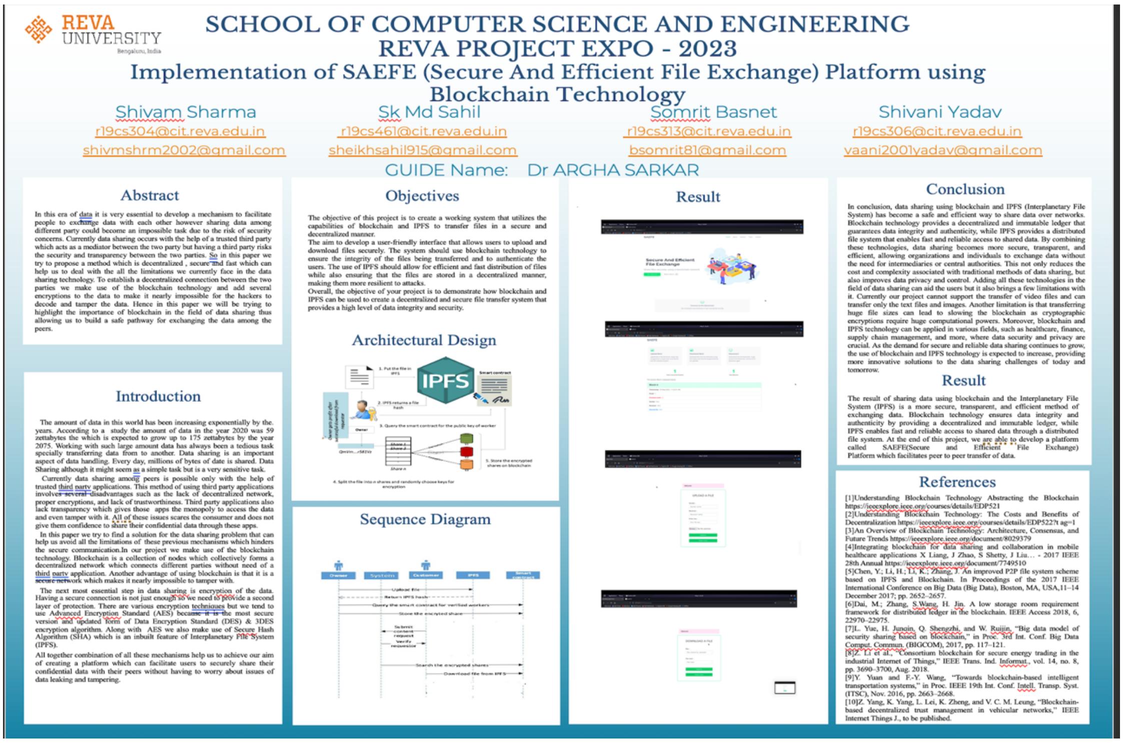
With best regards,

Organizing Chairs:

Dr. Prakash Dwivedi

National Institute of Technology Uttarakhand,

II. REVA Project-Expo Poster



REVA UNIVERSITY
Bengaluru, India

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING
REVA PROJECT EXPO - 2023
Implementation of SAEFE (Secure And Efficient File Exchange) Platform using Blockchain Technology

Shivam Sharma
r19cs304@cit.reva.edu.in
shivmshrm2002@gmail.com

Sk Md Sahil
r19cs461@cit.reva.edu.in
sheikhsahil915@gmail.com

Somrit Basnet
r19cs313@cit.reva.edu.in
bsomrit81@gmail.com

Shivani Yadav
r19cs306@cit.reva.edu.in
vaani2001yadav@gmail.com

GUIDE Name: Dr ARGHA SARKAR

Abstract

In this era of data it is very essential to develop a mechanism to facilitate people to exchange data with each other however sharing data among different party could become an impossible task due to the risk of security concerns. Currently data sharing occurs with the help of a trusted third party which acts as a mediator between the two party but having a third party risks the security and transparency between the two parties. So in this paper we try to propose a method which is decentralized , secure and fast which can help us to deal with the all the limitations we currently face in the data sharing technology. To establish a decentralized connection between the two parties we make use of the blockchain technology and add several encryptions to the data to make it nearly impossible for the hackers to decode and tamper the data. Hence in this paper we will be trying to highlight the importance of blockchain in the field of data sharing thus allowing us to build a safe pathway for exchanging the data among the peers.

Introduction

The amount of data in this world has been increasing exponentially by the. years. According to a study the amount of data in the year 2020 was 59 zettabytes the which is expected to grow up to 175 zettabytes by the year 2075. Working with such large amount data has always been a tedious task specially transferring data from to another. Data sharing is an important aspect of data handling. Every day, millions of bytes of date is shared. Data Sharing although it might seem as a simple task but is a very sensitive task.

Currently data sharing among peers is possible only with the help of trusted third party applications. This method of using third party applications involves several disadvantages such as the lack of decentralized network, proper encryptions, and lack of trustworthiness. Third party applications also lack transparency which gives those apps the monopoly to access the data and even tamper with it. All of these issues scares the consumer and does not give them confidence to share their confidential data through these apps.

In this paper we try to find a solution for the data sharing problem that can help us avoid all the limitations of these previous mechanisms which hinders the secure communication.In our project we make use of the blockchain technology. Blockchain is a collection of nodes which collectively forms a decentralized network which connects different parties without need of a third party application. Another advantage of using blockchain is that it is a secure network which makes it nearly impossible to tamper with.

The next most essential step in data sharing is encryption of the data. Having a secure connection is not just enough so we need to provide a second layer of protection. There are various encryption techniques but we tend to use Advanced Encryption Standard (AES) because it is the most secure version and updated form of Data Encryption Standard (DES) & 3DES encryption algorithm. Along with AES we also make use of Secure Hash Algorithm (SHA) which is an inbuilt feature of Interplanetary File System (IPFS).

All together combination of all these mechanisms help us to achieve our aim of creating a platform which can facilitate users to securely share their confidential data with their peers without having to worry about issues of data leaking and tampering.

Objectives

The objective of this project is to create a working system that utilizes the capabilities of blockchain and IPFS to transfer files in a secure and decentralized manner.
The aim to develop a user-friendly interface that allows users to upload and download files securely. The system should use blockchain technology to ensure the integrity of the files being transferred and to authenticate the users. The use of IPFS should allow for efficient and fast distribution of files while also ensuring that the files are stored in a decentralized manner, making them more resilient to attacks.
Overall, the objective of your project is to demonstrate how blockchain and IPFS can be used to create a decentralized and secure file transfer system that provides a high level of data integrity and security.

Architectural Design

1. Put the file in IPFS
IPFS
Smart contract
2. IPFS returns a file hash
Owner gets profit after successful download from requester
Owner
3. Query the smart contract for the public key of worker
QmVm....r58Vz
Share 1
Share 2
Share n
5. Store the encrypted shares on blockchain
4. Split the file into n shares and randomly choose keys for encryption

Sequence Diagram

Result

Conclusion

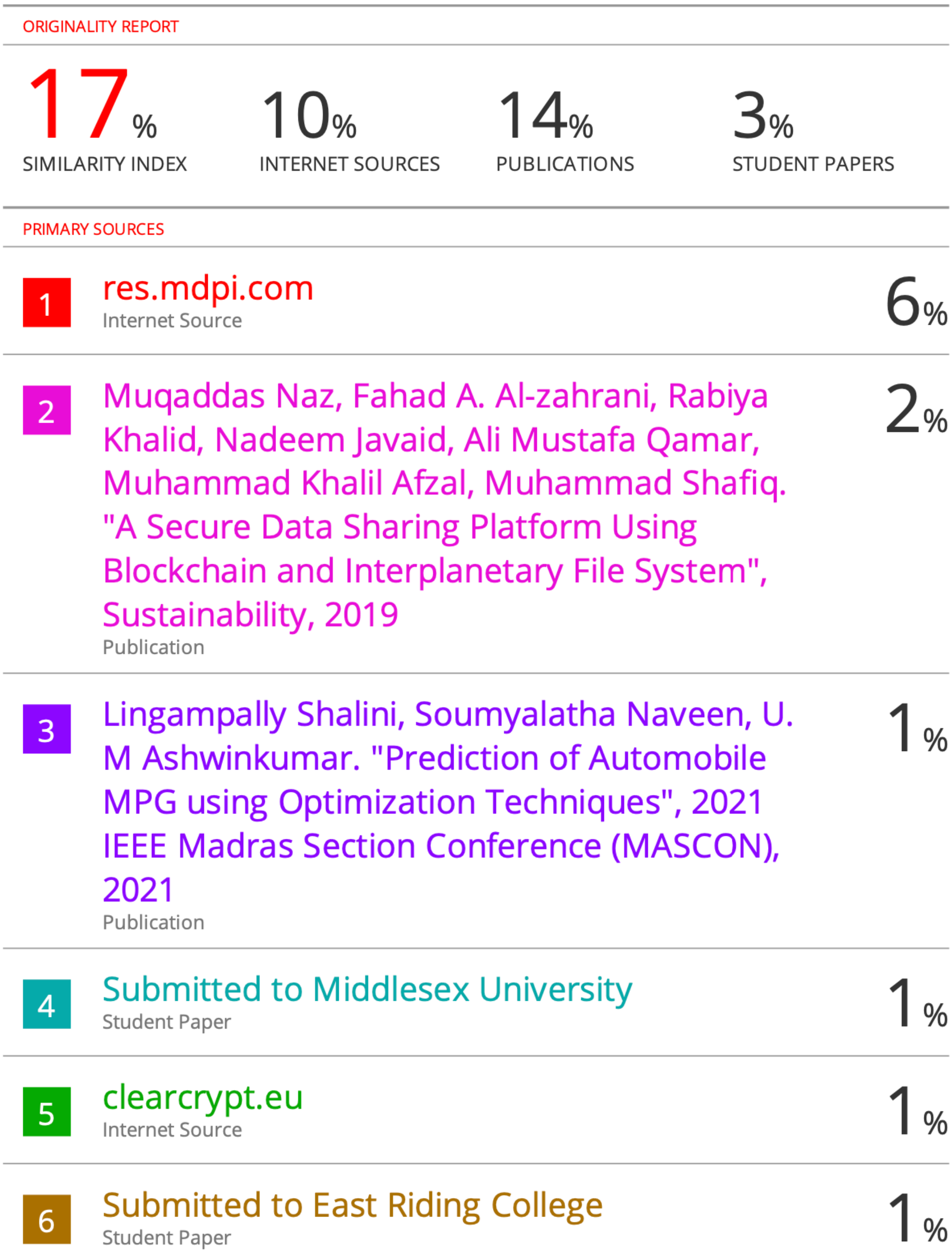
In conclusion, data sharing using blockchain and IPFS (Interplanetary File System) has become a safe and efficient way to share data over networks. Blockchain technology provides a decentralized and immutable ledger that guarantees data integrity and authenticity, while IPFS provides a distributed file system that enables fast and reliable access to shared data. By combining these technologies, data sharing becomes more secure, transparent, and efficient, allowing organizations and individuals to exchange data without the need for intermediaries or central authorities. This not only reduces the cost and complexity associated with traditional methods of data sharing, but also improves data privacy and control. Adding all these technologies in the field of data sharing can aid the users but it also brings a few limitations with it. Currently our project cannot support the transfer of video files and can transfer only the text files and images. Another limitation is that transferring huge file sizes can lead to slowing the blockchain as cryptographic encryptions require huge computational powers. Moreover, blockchain and IPFS technology can be applied in various fields, such as healthcare, finance, supply chain management, and more, where data security and privacy are crucial. As the demand for secure and reliable data sharing continues to grow, the use of blockchain and IPFS technology is expected to increase, providing more innovative solutions to the data sharing challenges of today and tomorrow.

Result

The result of sharing data using blockchain and the Interplanetary File System (IPFS) is a more secure, transparent, and efficient method of exchanging data. Blockchain technology ensures data integrity and authenticity by providing a decentralized and immutable ledger, while IPFS enables fast and reliable access to shared data through a distributed file system. At the end of this project, we are able to develop a platform called SAEFE(Secure and Efficient File Exchange) Platform which facilitates peer to peer transfer of data.

References

[1]Understanding Blockchain Technology Abstracting the Blockchain https://ieeexplore.ieee.org/courses/details/EDP521
[2]Understanding Blockchain Technology: The Costs and Benefits of Decentralization https://ieeexplore.ieee.org/courses/details/EDP522?t ag=1
[3]An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends https://ieeexplore.ieee.org/document/8029379
[4]Integrating blockchain for data sharing and collaboration in mobile healthcare applications X Liang, J Zhao, S Shetty, J Liu… - 2017 IEEE 28th Annual https://ieeexplore.ieee.org/document/7749510
[5]Chen, Y.; Li, H.; Li, K.; Zhang, J. An improved P2P file system scheme based on IPFS and Blockchain. In Proceedings of the 2017 IEEE International Conference on Big Data (Big Data), Boston, MA, USA,11–14 December 2017; pp. 2652–2657.
[6]Dai, M.; Zhang, S.Wang, H. Jin. A low storage room requirement framework for distributed ledger in the blockchain. IEEE Access 2018, 6, 22970–22975.
[7]L. Yue, H. Junqin, Q. Shengzhi, and W. Ruijin, "Big data model of security sharing based on blockchain," in Proc. 3rd Int. Conf. Big Data Comput. Commun. (BIGCOM), 2017, pp. 117–121.
[8]Z. Li et al., "Consortium blockchain for secure energy trading in the industrial Internet of Things," IEEE Trans. Ind. Informat., vol. 14, no. 8, pp. 3690–3700, Aug. 2018.
[9]Y. Yuan and F.-Y. Wang, "Towards blockchain-based intelligent transportation systems," in Proc. IEEE 19th Int. Conf. Intell. Transp. Syst. (ITSC), Nov. 2016, pp. 2663–2668.
[10]Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung, "Blockchain-based decentralized trust management in vehicular networks," IEEE Internet Things J., to be published.



ORIGINALITY REPORT

17%	10%	14%	3%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	res.mdpi.com Internet Source	6%
2	Muqaddas Naz, Fahad A. Al-zahrani, Rabiya Khalid, Nadeem Javaid, Ali Mustafa Qamar, Muhammad Khalil Afzal, Muhammad Shafiq. "A Secure Data Sharing Platform Using Blockchain and Interplanetary File System", Sustainability, 2019 Publication	2%
3	Lingampally Shalini, Soumyalatha Naveen, U. M Ashwinkumar. "Prediction of Automobile MPG using Optimization Techniques", 2021 IEEE Madras Section Conference (MASCON), 2021 Publication	1%
4	Submitted to Middlesex University Student Paper	1%
5	clearcrypt.eu Internet Source	1%
6	Submitted to East Riding College Student Paper	1%

7	Submitted to The Robert Gordon University Student Paper	1 %
8	dergipark.org.tr Internet Source	<1 %
9	napier-repository.worktribe.com Internet Source	<1 %
10	"M817 Block 2 week 9 symmetric encryption WEB097768", Open University Publication	<1 %
11	"Smart Blockchain", Springer Science and Business Media LLC, 2019 Publication	<1 %
12	"Smart Intelligent Computing and Communication Technology", IOS Press, 2021 Publication	<1 %
13	Shreeyaa Agrawal, Harsh Jain. "An approach to develop a secure and decentralized internet", 2019 International Conference on Nascent Technologies in Engineering (ICNTE), 2019 Publication	<1 %
14	apps.americanbar.org Internet Source	<1 %
15	old.rrjournals.com Internet Source	<1 %

16	www.researchgate.net Internet Source	<1 %
17	Abdulla Al Zaabi, Chan Yeob Yeun, Ernesto Damiani. "Trusting Testcases Using Blockchain-Based Repository Approach", Symmetry, 2021 Publication	<1 %
18	Miguel Pincheira, Elena Donini, Massimo Vecchio, Salil Kanhere. "A Decentralized Architecture for Trusted Dataset Sharing Using Smart Contracts and Distributed Storage", Sensors, 2022 Publication	<1 %

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		