IARJSET

ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁙ Peer-reviewed & Refereed journal ⁙ Vol. 11, Issue 5, May 2024

DOI: 10.17148/IARJSET.2024.11583

Blockchain based Document Storage and Authentication System

Mr. Sachin Dighe[1], Aditya Mehta[2], Bhaveshsingh Rathod[3], Rishabh Mishra[4]

Assistant Professor, Department of Computer Engineering, Sinhgad Institute of Technology and Science, Pune, India[1].

Student, Department of Computer Engineering, Sinhgad Institute of Technology and Science[2-4].

Abstract: The “Blockchain based Document Storage and Authentication system” is designed to enhance data security and integrity. The system incorporates user registration, document uploading, admin approval, document verification and face capturing functionalities to provide a comprehensive and secure document management solution. Users register on the platform, upload documents that are encrypted and store on the blockchain, undergo admin approval for verification and can verify document authenticity through blockchain transactions, Additionally, users can utilize face capturing for biometric authentication. This system leverages blockchain technology to ensure transparency, immutability and enhanced security in document storage and authentication processes.

Keywords: Blockchain, Hashing, Ethereum, Document Verification, Digital Signature, Cryptography, Certificate Authentication, Governance

I. INTRODUCTION

In the realm of digital document management, the integration of blockchain technology has emerged as a groundbreaking solution for enhancing security, transparency and trust in data transactions. This project focuses on developing a robust blockchain-based document storage and authentication system that revolutionizes traditional document management practices. By leveraging the decentralized and immutable nature of blockchain, this system aims to provide users with a secure platform for storing, verifying, and authenticating documents with unparalleled integrity. At the core of this project lies the utilization of cryptographic hashing algorithms to create unique identifiers for each document, ensuring data integrity and tamper-proof records. Through the implementation of manual document verification processes can be executed seamlessly, reducing the risk of fraud and unauthorized access. By incorporating digital signatures and timestamp features, users can authenticate documents and establish a transparent audit trail of transactions, bolstering trust and accountability within the system.

Furthermore, this system introduces innovative features such as face capturing for biometric authentication, adding an extra layer of security to document verification processes. With a focus on user registration, document uploading, admin approval and verification workflows, this project aims to streamline document management while upholding the highest standards of security and authenticity. By combining cutting-edge blockchain technology with advanced encryption methods, this system sets out to redefine the landscape of document storage and authentication, paving the way for a more secure and efficient digital document management ecosystem.

II. RELATED WORK

[1] In their study, Xingxiong Zhu. (2019) explored the benefits of cryptographic key pairs private and public keys for verifying the authenticity of digital documents. Furthermore, They investigated that the broader applicability of blockchain technology in various domains, including the Internet of Things for data tracking, supply chain management, property registration, and document protection. Significantly, the authors underscored blockchain's capacity to bolster trust in the financial realm through the facilitation of secure credit reporting mechanisms.

[2] Leible and colleagues explored the potential and advantages of integrating blockchain into open science platforms. Their work explored the various sectors that could benefit from blockchain implementation and assessed the impact of blockchain on different industries thus far.

[3] To mitigate potential societal risks, Shah et al. (2019) proposed a theoretical framework for verifying academic certificates using blockchain technology. Their model integrates encryption techniques with private and public keys, alongside digital signatures with timestamping functionalities for verifying digital certificates. Authors delineated a system for issuing and authenticating birth certificates via blockchain.

[4] Blockchain emerges as an advanced technology offering heightened convenience and security compared to centralized data storage systems. In this paradigm, information is not stored in a single location but rather replicated across a network of interconnected computers, each acting as an independent database node. This peer-to-peer network ensures tamper-proof data management. Modifications to any record (block) necessitate altering all subsequent blocks, as each block cryptographically references the previous one using a secure hash function.

Additionally, each node or block undergoes encryption using robust hash algorithms, with every block storing the hash code of its predecessor, establishing a continuous chain of interconnected blocks within the network. Given blockchain's increasing global traction owing to its distributed and decentralized characteristics, Joshi and colleagues conducted a comprehensive survey centered on the fundamental hurdles and prospects in blockchain technology. Their work investigated the fundamental challenges and opportunities associated with blockchain technology, while also delving into security and privacy considerations.

[5] The digital revolution has demonstrably enhanced record-keeping security and streamlined administrative processes by reducing time and effort required for maintenance.However, despite these advancements in security, instances of fraud persist, as exemplified by recent incidents such as the discovery of fake birth certificate schemes in Delhi, India.

[6] Zhu, X., & Fan, T propose a user authentication model that leverages multidimensional biometric and behavioral features. This approach utilizes real-time feedback technology based on a user's dynamic behavioral characteristics to detect and authenticate user activity on their terminal device. By analyzing and processing the interactive behavioral data collection, analysis, and processing, a network identity system grounded in legal identity is established.

III. PROPOSED WORK

A. Problem Statement:

The traditional methods of document storage and authentication are plagued with issues of security vulnerability, data tampering and lack of transparency. This project aims to develop a blockchain-based document storage and authentication system that ensures data security, immutability and transparency while streamlining document verification processes.

By harnessing the decentralized and tamper-proof nature of blockchain, this system seeks to eliminate the risks associated with centralized storage and authentication methods, providing users with a reliable and trustworthy platform for managing their digital documents.

B. Objectives:

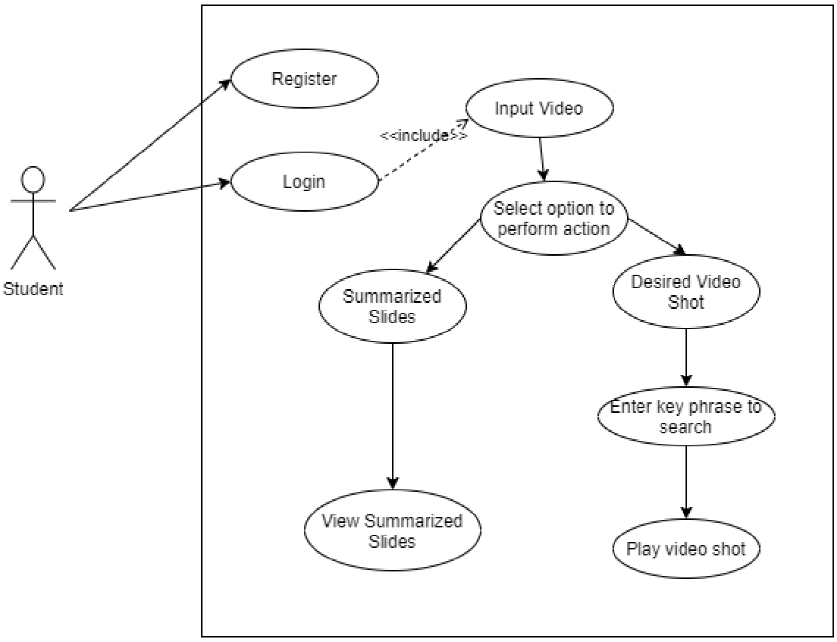
1. Enhanced Document Storage
2. Improved Verification Efficiency
3. Ensure Data Integrity
4. Increase Transparency and Trust
5. Facilitate Decentralized Authentication
6. Enhance Traceability
7. Improve Access Control
8. Support Regulatory Compliance

C. Diagrams:

1. Use Case Diagram:

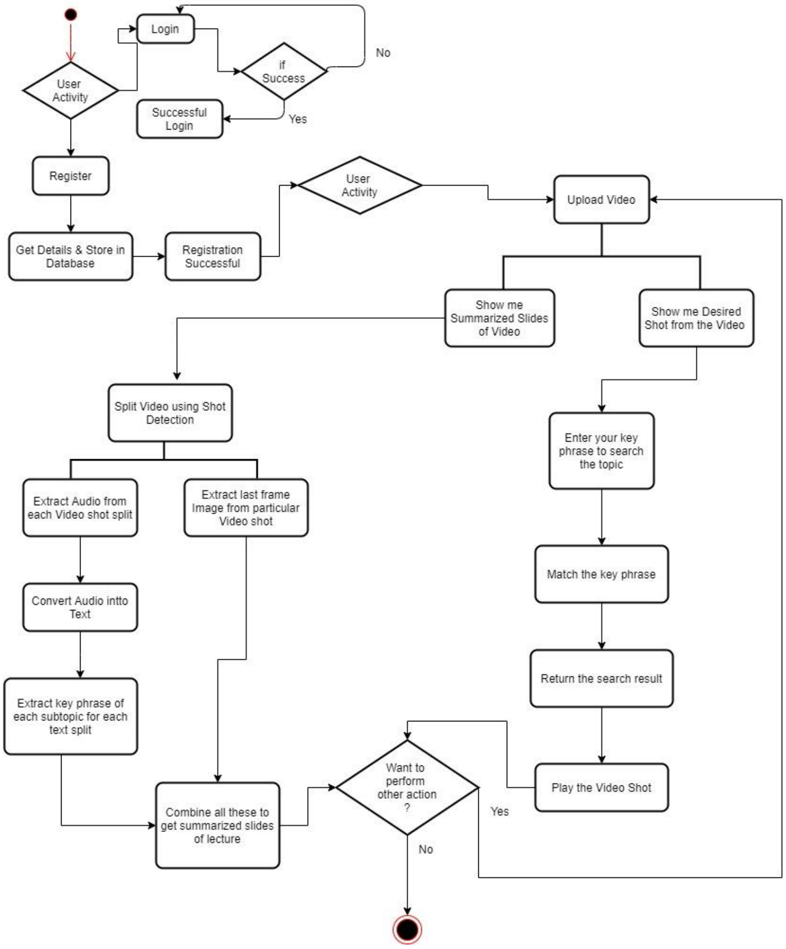
The use case diagram portrays the dynamic behaviour of a system, encapsulating its functionality by incorporating use cases, actor and their relationships. It models the tasks, services and functions required by a system or subsystem of an application.

DOI: 10.17148/IARJSET.2024.11583



2. **Activity Diagram:**

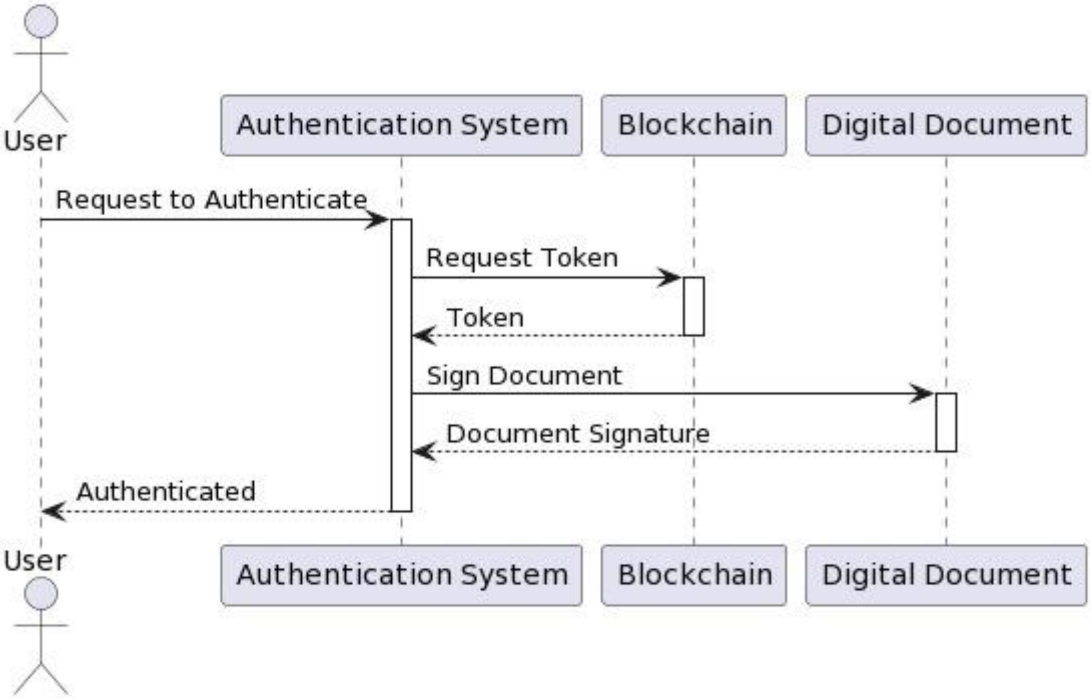
Illustrates the flow of control in the system and shows the steps involved in the execution of a use case. User activity decides the flow of control. Activities have predefined flow and execute as per conditions.


Login
No
if Success
User Activity
Successful Login
Yes
Register
User Activity
Upload Video
Get Details & Store in Database
Registration Successful
Show me Summarized Slides of Video
Show me Desired Shot from the Video
Split Video using Shot Detection
Enter your key phrase to search the topic
Extract Audio from each Video shot split
Extract last frame Image from particular Video shot
Match the key phrase
Convert Audio intto Text
Return the search result
Extract key phrase of each subtopic for each text split
Want to perform other action ?
Play the Video Shot
Yes
Combine all these to get summarized slides of lecture
No

DOI: 10.17148/IARJSET.2024.11583

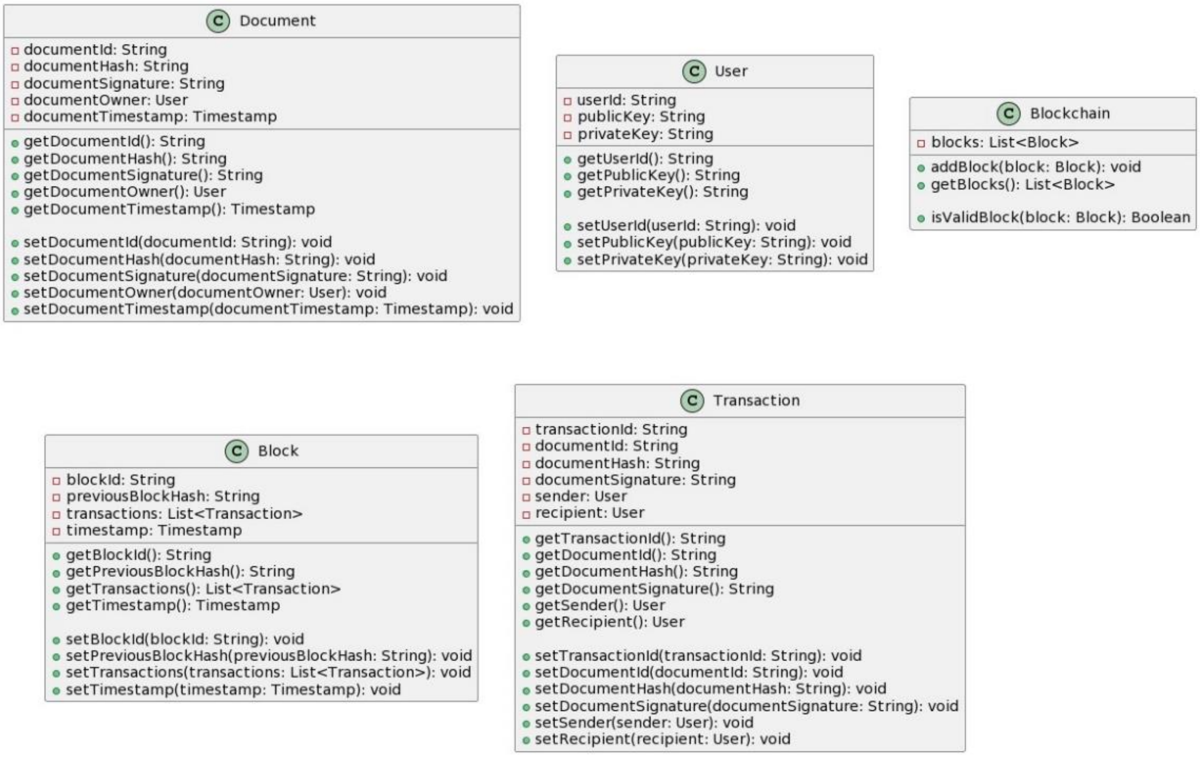
3. **Sequence Diagram:**

High level interaction between active objects in a subject is visualized using a sequence diagram. The sequential flow of a system and the exchange of messages between the objects are shown.



4. **Class Diagram:**

The class diagram represents the relationship between classes. Each class contains some attributes and functions. System is the interfaces in the class diagram to be used with summary slides, desired shots and the web portal.


C Document
documentId: String
documentHash: String
documentSignature: String
documentOwner: User
documentTimestamp: Timestamp
getDocumentId(): String
getDocumentHash(): String
getDocumentSignature(): String
getDocumentOwner(): User
getDocumentTimestamp(): Timestamp
setDocumentId(documentId: String): void
setDocumentHash(documentHash: String): void
setDocumentSignature(documentSignature: String): void
setDocumentOwner(documentOwner: User): void
setDocumentTimestamp(documentTimestamp: Timestamp): void
C User
userId: String
publicKey: String
privateKey: String
getUserId(): String
getPublicKey(): String
getPrivateKey(): String
setUserId(userId: String): void
setPublicKey(publicKey: String): void
setPrivateKey(privateKey: String): void
C Blockchain
blocks: List<Block>
addBlock(block: Block): void
getBlocks(): List<Block>
isValidBlock(block: Block): Boolean
C Block
blockId: String
previousBlockHash: String
transactions: List<Transaction>
timestamp: Timestamp
getBlockId(): String
getPreviousBlockHash(): String
getTransactions(): List<Transaction>
getTimestamp(): Timestamp
setBlockId(blockId: String): void
setPreviousBlockHash(previousBlockHash: String): void
setTransactions(transactions: List<Transaction>): void
setTimestamp(timestamp: Timestamp): void
C Transaction
transactionId: String
documentId: String
documentHash: String
documentSignature: String
sender: User
recipient: User
getTransactionId(): String
getDocumentId(): String
getDocumentHash(): String
getDocumentSignature(): String
getSender(): User
getRecipient(): User
setTransactionId(transactionId: String): void
setDocumentId(documentId: String): void
setDocumentHash(documentHash: String): void
setDocumentSignature(documentSignature: String): void
setSender(sender: User): void
setRecipient(recipient: User): void

IV. RESULT AND DISCUSSION

Users will benefit from heightened security measures provided by blockchain technology, ensuring the integrity and confidentiality of stored documents. The system will create tamper-proof records, enabling users to verify the authenticity and integrity of documents with ease. Utilizing digital signatures will streamline the authentication process, reducing the risk of fraud and unauthorized access. Blockchain's decentralized nature will promote transparency in document transactions, fostering trust among users.

It explores how the system's security features impact data protection and privacy, comparing it to traditional storage methods. Discuss user feedback and experiences with the system, highlighting areas of improvement and user satisfaction. Addresses how the system aligns with data protection regulations and compliance standards, ensuring legal adherence. Evaluate the system's scalability and performance under varying loads, discussing any bottlenecks or areas for optimization.

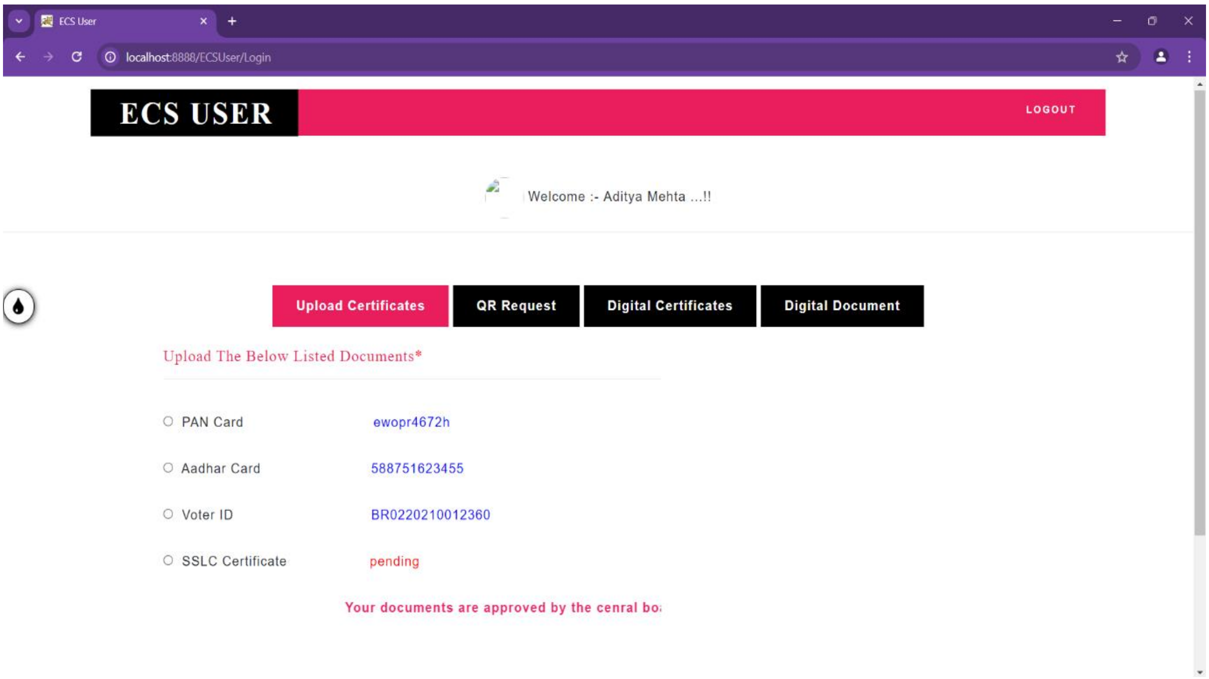
The blockchain based document storage and authentication system has the potential to revolutionize data management practices by offering enhanced security, transparency and efficiency. By analyzing the results of its usage and engaging in insightful discussions, you can showcase the system's effectiveness and pave the way for further advancements in blockchain technology.

User Registration on Platform

When users register on the platform, they access the registration page and provide their personal information. They then create a unique username and password, and the system generates a unique user ID and public-private key pair for each registered user. Finally, users receive a confirmation email to activate their account, completing the registration process.

Uploading Document on platform

Authenticated users can access the document upload section, where they select the document they wish to upload. The system encrypts the document using the user's public key, hashes it, and stores it on the blockchain network. Once the upload is complete, users receive a confirmation of the successful document upload, along with the transaction details.



Welcome :- Aditya Mehta ...!!

Upload The Below Listed Documents*

○ PAN Card ewopr4672h

○ Aadhar Card 588751623455

○ Voter ID BR0220210012360

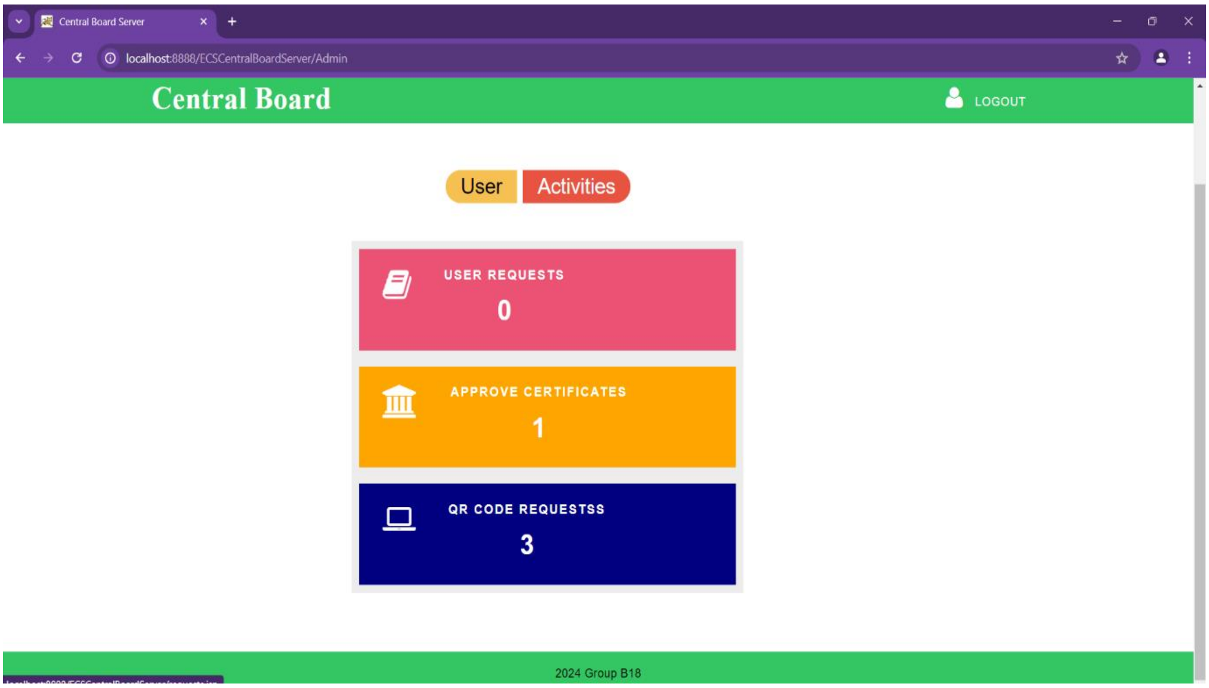
○ SSLC Certificate pending

Your documents are approved by the cenral bo

Approval of Documents by Admin

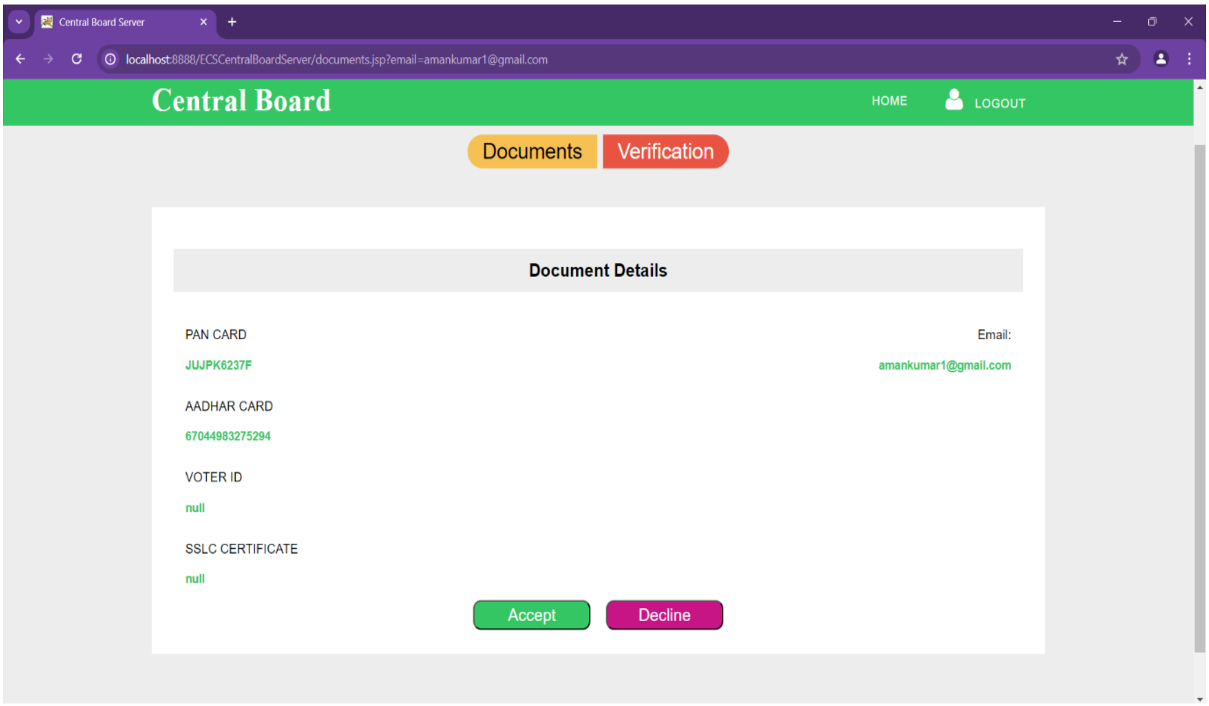
The administrative team reviews the uploaded documents to verify their authenticity and legitimacy. After approval, the documents are marked as verified in the blockchain network, and users are notified of the document approval status via email or in-platform notifications. This ensures that only legitimate documents are stored on the platform.

DOI: 10.17148/IARJSET.2024.11583



Verification of Documents

When users access the document verification section, the system retrieves the document's transaction details from the blockchain network. It then verifies the document's integrity by comparing the stored hash value with the calculated hash of the retrieved document. The verification result is displayed to the user, indicating whether the document is authentic and unmodified.


Central Board Server
localhost:8888/ECSCentralBoardServer/documents.jsp?email=amankumar1@gmail.com
Central Board
HOME
LOGOUT
Documents
Verification
Accept
Decline

Document Details

PAN CARD
JUJPK6237F

Email:
amankumar1@gmail.com

AADHAR CARD
67044983275294

VOTER ID
null

SSLC CERTIFICATE
null

Face Capturing

When users access the document verification section, the system retrieves the document's transaction details from the blockchain network. It then verifies the document's integrity by comparing the stored hash value with the calculated hash of the retrieved document. The verification result is displayed to the user, indicating whether the document is authentic and unmodified.

DOI: 10.17148/IARJSET.2024.11583

V. CONCLUSION

The development of a blockchain-based document storage and authentication system presents a transformative solution to the challenges inherent in traditional document management practices. By harnessing the power of blockchain technology, this system offers enhanced security, transparency, and efficiency in storing, verifying, and authenticating documents. Through user registration, document uploading, admin approval, verification processes, and innovative features like face capturing for biometric authentication, this system sets a new standard for secure and trustworthy document management.The implementation of cryptographic hashing, smart contracts, digital signatures, and decentralized storage on the blockchain ensures data integrity, immutability, and tamper-proof records. By automating document verification procedures and streamlining user interactions, this system not only enhances security but also improves user experience and operational efficiency. The integration of biometric authentication adds an extra layer of security, further bolstering the system's robustness against unauthorized access and fraud.Overall, this blockchain-based document storage and authentication system represents a significant advancement in digital document management, paving the way for a more secure, transparent, and reliable platform for users to store and authenticate their documents. With its focus on data security, user experience, and innovative features, this system exemplifies the potential of blockchain technology to revolutionize document management practices and set new standards for authenticity and trust in the digital age.

VI. FUTURE SCOPE

The future scope of the blockchain-based document storage and authentication system is vast and promising, with opportunities for further enhancement and expansion across various domains. By integrating artificial intelligence and machine learning algorithms, the system can improve document classification and retrieval processes, while exploring IoT device integration can enhance secure data collection and storage within the blockchain network. Adapting the system to cater to different industries like healthcare, finance, and legal sectors involves tailoring workflows and security measures to meet specific industry requirements, along with developing industry-specific smart contracts and governance models for regulatory compliance. Additionally, decentralized identity management solutions based on blockchain technology can offer users self-sovereign control over their personal data and identities, potentially integrating with the document storage system for secure user authentication across platforms. Optimizing scalability and performance through alternative consensus mechanisms and off-chain storage solutions like IPFS can ensure efficient handling of document transactions and reduce network load. Embracing interoperability with other blockchain networks and legacy systems, along with exploring decentralized governance models and community engagement, will empower users and stakeholders to contribute to the system's evolution and adoption, fostering a vibrant ecosystem of secure and efficient document management solutions in the digital era.

REFERENCES

[1]. S. Leible, S. Schlager, M. Schubotz, and B Gipp ”A Review on Blockchain Technology and Blockchain Projects Fostering Open Science” In 2019

[2]. A. Prashanth Joshi, M. Han, and Y. Wang ”A survey on security and privacy issues of blockchain technology.” in 2018

[3]. W. Chen, Z. Xu, S. Shi, Y. Zhao, and J. Zhao A Survey of Blockchain Applications in Different Domains.” in 2018

[4]. K. Gilani, E. Bertin, J. Hatin and N. Crespi A Survey on Blockchain based Identity Management and Decentralized Privacy for Personal Data.” In 2020

[5]. J. Wang, S. Wang, G. Junqi, Y. Du, S. Cheng, and X. Li “A Summary of Research on Blockchain in the Field of Intellectual Property.” in 2019

[6]. S. Rouhani and R. Deters ”Security, Performance, and Applications of Smart Contracts: A Systematic Survey.” in 2019