JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Banking Document Sharing using Blockchain based on Document Identity

[1]Anjali Devi, [2]Sudhanshu Vashistha
[1]M.Tech Scholar, [2]Assistant Professor
[1]Department of Computer Science Engineering,
[1]Global Institute of Technology, Jaipur

Abstract : The proposed system offers a solution that addresses the issue of document sharing security by combining blockchain technology, the Blake2B algorithm, and multi-level security checks. The system begins with a user authentication phase, which ensures the legitimacy of users. To authenticate users, the system employs Aadhar verification, fingerprint authentication, and a rotation pattern generated from images. These multi-level security checks enhance user identification and minimize the risk of unauthorized access. Once user authentication is successful, the document sharing phase commences. In this phase, the system utilizes the Blake2B algorithm to generate a File Sharing Key. This key is derived from the Blake2B hash of the user's Aadhar, Fingerprint, the shared document, and the rotation pattern. By utilizing the File Sharing Key, the system guarantees that only authorized individuals can access the shared document. The effectiveness of this approach has been validated through research papers and evaluated using pattern strength checking tools, which measure years and bits of entropy. By incorporating multi-level security checks, the proposed system significantly enhances document sharing security in the banking sector. The Aadhar verification, fingerprint authentication, and rotation pattern provide additional layers of security, making it considerably more challenging for malicious actors to manipulate or forge documents. The evaluation of pattern strength ensures the system's ability to provide robust security measures.

Index Terms **– Blake2B, File Sharing, Bio-Metric.**

I. INTRODUCTION

Blockchain is a digital ledger technology that enables multiple parties to maintain a shared database without the need for a central authority. It ensures transparency, security, and immutability of data through cryptographic algorithms and consensus mechanisms. Although blockchain gained popularity with cryptocurrencies like Bitcoin, its applications extend beyond that. [1]

Blockchain serves as a decentralized digital ledger that records transactions or data across multiple computers or nodes. Each transaction, known as a block, is cryptographically linked to the previous block, forming a chain of blocks. This structure ensures the integrity and immutability of the recorded information. While blockchain is commonly associated with cryptocurrencies, its applications extend to various industries. It can be employed in supply chain management, voting systems, healthcare records, identity management, intellectual property protection, and more. The advantages of blockchain include enhanced security, transparency, trust, efficiency, and reduced reliance on intermediaries. Nevertheless, it's essential to consider factors like scalability, energy consumption, regulatory compliance, and privacy concerns when evaluating the feasibility of implementing blockchain solutions for specific use cases. [1]

Importance of Blockchain:

- Transparency and Trust: Blockchain offers a transparent and auditable record of transactions. Participants in the network can verify and validate information, fostering trust among all involved parties.
- Security and Immutability: Advanced cryptographic techniques secure data on the blockchain. Once recorded, it is nearly impossible to alter or tamper with information without network consensus. This ensures data integrity and immutability.
- Decentralization: Blockchain operates in a decentralized manner, eliminating the need for a central authority. This reduces the risk of manipulation or a single point of failure.[1]
- Efficiency and Cost Savings: By removing intermediaries and automating processes, blockchain streamlines operations, reduces paperwork, and enhances efficiency. This leads to significant cost savings, particularly in areas requiring trust, verification, and reconciliation.
- Smart Contracts: Blockchain platforms support the execution of smart contracts—self-executing agreements with predefined rules. They enable automation, enforceability, and programmability, improving transaction efficiency and reliability. [2]

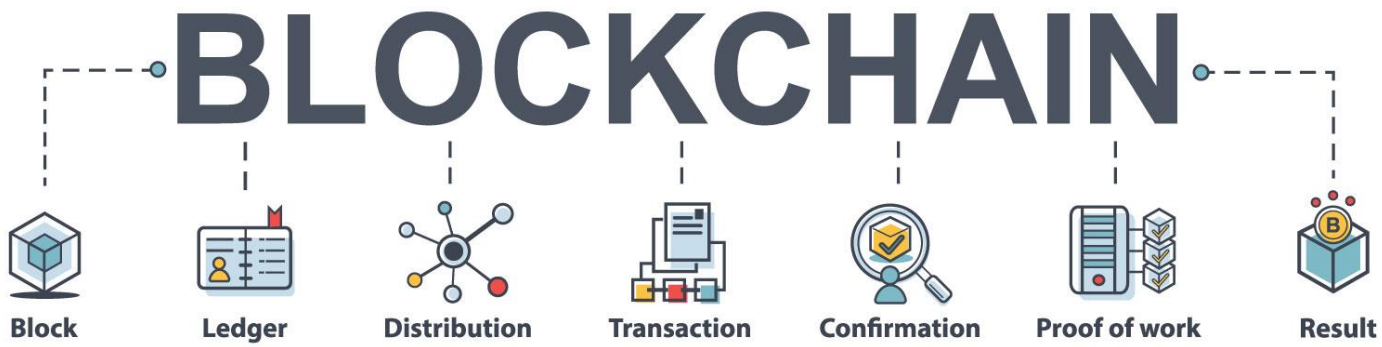

Fig 1. Blockchain

Importance of Blockchain in Document Sharing in Banks:

In the context of document sharing in banks, blockchain offers several significant benefits:

- Security and Privacy: Banks handle sensitive and confidential information. Blockchain's cryptographic algorithms and distributed nature ensure high security and resistance to unauthorized access. It grants access only to authorized parties, enhancing privacy and data protection.
- Data Integrity and Traceability: Blockchain provides an immutable record of document transactions, ensuring integrity and traceability. Changes made to a document are recorded, creating an auditable trail and preventing unauthorized modifications. [2]
- Streamlined Processes: Blockchain automates and streamlines document sharing processes. Smart contracts establish predefined rules, automating verification, approval, and authentication. This reduces manual intervention, accelerates processes, and improves efficiency.[2]
- Enhanced Collaboration: Banks collaborate with various stakeholders. Blockchain offers a secure and transparent platform for sharing documents, facilitating seamless collaboration and reducing the need for intermediaries.
- Regulatory Compliance: Banks operate in a highly regulated environment. Blockchain assists in compliance by providing a tamper-proof and auditable record of document transactions. It simplifies audits and regulatory reporting, reducing the compliance burden.[3]

Overall, blockchain technology has the potential to revolutionize document sharing in banks by enhancing security, privacy, efficiency, and compliance. It improves trust, transparency, and operational processes, leading to better customer experiences.

.

II. Literature Review

Giraldo, F. D. et al. (2020): The paper asserts that blockchain technology has the potential to enhance trust in digital transactions. It explores the applications of blockchain in commercial, industrial, and service systems, with a particular focus on Ethereum smart contracts and public/private key cryptography for secure and anonymous transactions. The paper provides a proof of concept for a blockchain-based voting system tailored for elections, aiming to improve trust among stakeholders.[4]

Teja, J. R. (2020): The author highlights the resource-intensive nature of maintaining valid and accurate documents through intermediaries. To address this issue, the paper suggests utilizing blockchain technology, which enables the creation of immutable ledger entries to track document alterations and ensure traceability. It proposes the use of Merkel tree algorithms for efficient data storage. [5]

Shree, J. et al. (2020): The paper introduces a smart and secure purchasing system that integrates ERP (Enterprise Resource Planning) and focuses on a self-billing application to eliminate long waiting lines for customers. It leverages blockchain technology to ensure product traceability throughout the supply chain. Additionally, an RFID item tracker is included to detect unauthorized removal of goods from the shop, thereby mitigating theft risks.[6]

Li, G., Sun, S., and Li, X. (2020): This paper presents a blockchain-based method for verifying electronic invoices as an alternative solution for addressing tax-related issues such as overstatement and false declarations. The proposed method utilizes artificial intelligence-based automatic identification technology and graphic image processing technology to enable efficient, reliable, and impartial verification of invoices on the blockchain.[7]

Rajashekaragouda and Dakshayini (2020): The authors propose a revolutionary blockchain-based supply-chain system to overcome the limitations of traditional systems. The system ensures transparent record-keeping and source tracing of products without relying on a trusted third party, thanks to distributed and immutable ledger technology. Hyperledger Fabric is used as an example to demonstrate the effectiveness of this solution. [8]

III. PROPOSED ALGORITHM

Algorithm for User Identification Process:

1. Input:
   - User's digital identity document (Aadhar card or driving license)
   - User's fingerprint scan
   - Set of pictures for the rotation pattern
2. Generate Hash for Digital Identity Document:
   - Generate BLAKE2b-512Hash for the uploaded digital identity document.
3. Generate Hash for Fingerprint:
   - Generate BLAKE2b-512Hash for the user's fingerprint scan.
4. Generate Picture Rotation Pattern String:
   - Present the set of pictures to the user.
   - For each picture, allow the user to rotate it at different angles (90, 180, 270, 360 degrees).
   - Record the rotation angles chosen by the user for each picture.
   - Concatenate the rotation angles to form a string pattern.
5. Generate Blockchain:
   - Combine the generated digital identity document hash, fingerprint hash, and picture rotation pattern string.
   - Create a blockchain by hashing the combined data.
6. Store Blockchain on Multiple Servers:
   - Distribute and store the generated blockchain on multiple servers.

IV. IMPLEMENTATION AND RESULT ANALYSIS

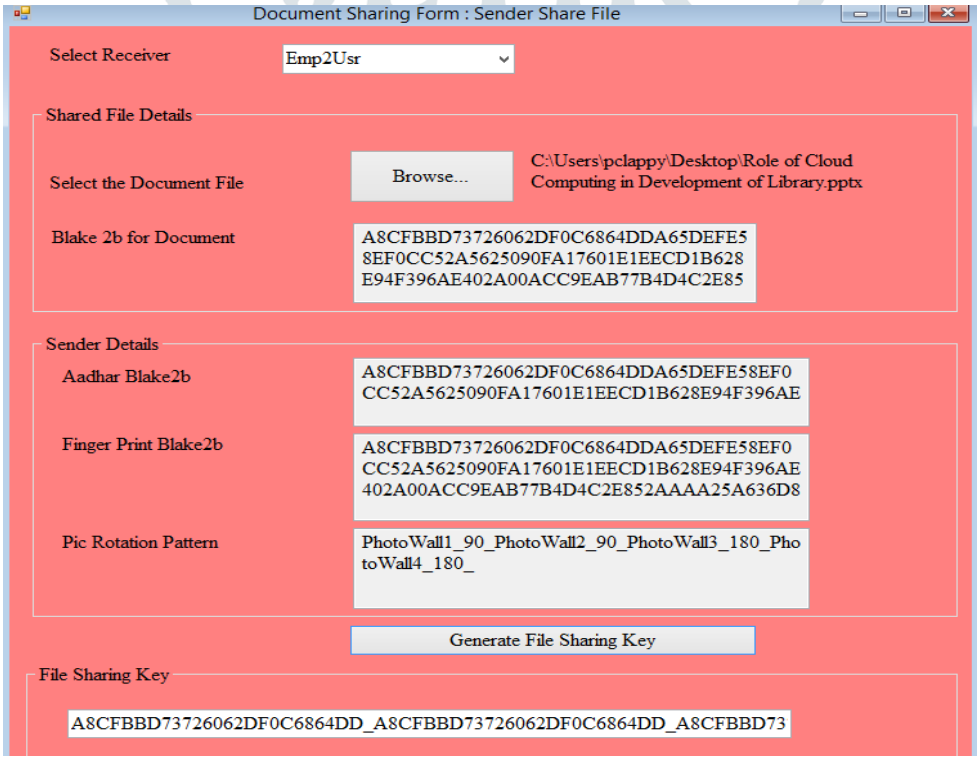

Fig 2. Document Sharing in Implementation

The proposed system for Document Sharing offers users two options for login and registration, allowing them to select their preferred method based on their account status and preferences.

To simulate the exchange of data between two users in the system, the process can be outlined in the following steps:

- User Account Creation: Initially, two user accounts need to be created within the Document Sharing System. During registration, users will provide necessary details like a unique username, email address, and password. The system will then verify the information and create the user accounts accordingly.
- User Login: Once the user accounts are successfully created, both users can proceed to log into the Document Sharing System. They will be required to enter their respective usernames or email addresses, along with their passwords, to securely access their accounts.

- File Upload: After logging in, users will have the option to upload files for sharing purposes. They can select specific files from their local devices and upload them to the system's storage. The system ensures the secure and encrypted transfer of files to maintain data integrity.
- File Sharing: Once the files are uploaded, users can initiate the sharing process. They will specify the recipient(s) by entering their usernames or email addresses. The system will verify the recipient(s) and grant them access to the shared files.
- Access and Download: Upon receiving access, recipients can log into their Document Sharing System accounts and navigate to the shared files section. From there, they can securely view and download the files stored in the system to their local devices.
- Collaboration and Commenting: The Document Sharing System may include collaboration features that enable users to interact with the shared files. These features can encompass commenting, version control, and real-time editing, facilitating efficient collaboration between users.
- Tracking and Notifications: Throughout the data exchange process, the Document Sharing System keeps track of activities related to file sharing, including uploads, downloads, and collaboration. The system may also send notifications to users to inform them about new shared files, comments, or any other relevant updates.

By following these steps, users can effectively exchange data and collaborate within the Document Sharing System, ensuring the secure and efficient sharing of files.

One of the base papers for comparison, **"F. Z. Glory et al., 2019, formed the pattern on the basis of the concept then proposed on their paper, the sample pattern according to their concept is taken as",**

"Base Paper Password Pattern

{urAn29iRfan-

Proposed Password Pattern"

A8CFBBD73726062DF0C6864DD_A8CFBBD73726062DF0C6864DD_A8CFBBD73726062DF0C6864D
D PhotoWall1

Table 4.1 "Result Analysis on Basis of Time Period Comparison with Paper 1"

Website/Tool	Base Result	Proposed Result
Password Monster Tool	0.000005 trillion years	57 billion trillion trillion trillion trillion trillion trillion trillion years
Delinea.com Password Checker Tool	186 million years	32,514,707,246,498,062,000,000,000 quadragintillion years
How Secure is My Password Checker Tool	46 million years	8 septillion quadragintillion years

Table 4.2 "Result Analysis on Basis of Entropy Comparison with Paper 1"

Website/Tool	Base Result	Proposed Result
Cryptool2 Tool	83 bits	182 bits
Password. Blue Tool	43 bits	112 bits

V. CONCLUSION

In conclusion, this research presents a robust and secure document sharing system specifically designed for the banking sector. The system leverages blockchain technology, the Blake2B algorithm, and multi-level security checks to address the critical need for enhanced security in document sharing processes. By incorporating user authentication methods such as Aadhar verification, fingerprint authentication, and rotation patterns, the system ensures the legitimacy of users and reduces the risk of unauthorized

access. Additionally, the system utilizes the Blake2B algorithm to generate a File Sharing Key, which guarantees that only authorized individuals can access shared documents. The effectiveness of the proposed system is supported by the evaluation of pattern strength and validated through research papers and security tools. Overall, the system provides a comprehensive solution to enhance the integrity, authenticity, and confidentiality of shared documents in the banking sector.

REFERENCES

[1] Balamurali, A. , Harsha,M V R . , Hitesh, V S., Chaitanya, A S. (2019) , "Graphical password by image segmentation",International Journal of Innovative Technology and Exploring Engineering, 8(6S4), pp. 462–464.

[2] Chattopadhyay, A. et al. (2018) "A middle-school case study: Piloting A novel visual privacy themed module for teaching societal and human security topics using social media apps," in 2018 IEEE Frontiers in Education Conference (FIE). IEEE, pp. 1–8.

[3] Chung, W., Mustaine, E. and Zeng, D. (2017) "Criminal intelligence surveillance and monitoring on social media: Cases of cyber-trafficking," in 2017 IEEE International Conference on Intelligence and Security Informatics (ISI). IEEE, pp. 191–193.

[4] Giraldo, F. D., Milton C., B. and Gamboa, C. E. (2020) "Electronic voting using blockchain and smart contracts: Proof of concept," IEEE Latin America Transactions, 18(10), pp. 1743–1751

[5] Teja, J. R. (2020) "Proposing method for Public record maintenance using Block chain," in 2020 International Conference on Mainstreaming Block Chain Implementation (ICOMBI). IEEE, pp. 1–5.

[6] Shree, J. et al. (2020) "To Design Smart and Secure Purchasing System integrated with ERP using Block chain technology," in 2020 IEEE 5th International Conference on Computing Communication and Automation (ICCCA). IEEE.

[7] Li, L. and Qian, K. (2016) "Using real-time fear appeals to improve social media security," in 2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC). IEEE, pp. 610–611.

[8] Rajashekaragouda and Dakshayini, M. (2020) "Block-chain Implementation of Letter of Credit based Trading system in Supply Chain Domain," in 2020 International Conference on Mainstreaming Block Chain Implementation (ICOMBI). IEEE.

[9] Tse, D. et al. (2018) "Robust password-keeping system using block-chain technology," in 2018 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM). IEEE.

[10] Wang, Z. et al. (2015) "Key technology research on user identity resolution across multi-social media," in 2015 International Conference on Cloud Computing and Big Data (CCBD). IEEE, pp. 358–361.

[11] F. Z. Glory, A. Ul Aftab, O. Tremblay-Savard and N. Mohammed, "Strong Password Generation Based On User Inputs," 2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), 2019.

[12] M. H. Zaki, A. Husain, M. S. Umar and M. H. Khan, "Secure pattern-key based password authentication scheme," 2017 International Conference on Multimedia, Signal Processing and Communication Technologies (IMPACT), 2017, pp. 171-174.