WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Secure Android Document Sharing using Block chain

C.Avanthika[1] | M. Saravanakumar[2]

[1](Department of CS, PG scholar, Rathinam College of Arts and Science, Coimbatore, avanthika7615@gmail.com)
[2](Department of CS, senior faculty, Rathinam College of Arts and Science, Coimbatore, skumarkovai@gmail.com)

ABSTRACT :

The rapid evolution of technology has led to an increased need for secure and reliable document sharing platforms on Android devices. Traditional centralized systems are prone to security breaches and data manipulation, raising concerns about document integrity and privacy. In response to these challenges, this paper proposes Secure Android document sharing using blockchain technology. The system aims to leverage the decentralized and immutable nature of blockchain to provide a secure and transparent platform for sharing and accessing documents on Android devices. This innovative system will utilize smart contracts for document verification, sender and receiver validation, and ensuring document authenticity. By integrating blockchain technology, the system will establish a decentralized network of nodes, ensuring that documents are shared and accessed securely without the need for a central authority. The use of cryptographic techniques will further enhance the security of document sharing, protecting sensitive information from unauthorized access. The methodology involves the development of a mobile application for Android devices, integrating blockchain protocols for document storage and retrieval. Smart contracts will be deployed to validate the sender's authorization and the authenticity of shared documents, ensuring that only authorized recipients can access the shared content.

Key words: Android Document Sharing System, Document Verification, Mobile Application, Document Storage and Retrieval, Document Authenticity, Data Privacy, and Integrity,

Introduction :

The need for secure and reliable document sharing platforms tailored for Android users has become more crucial than ever. With the exponential growth of digital documents and the increasing risk of data breaches, ensuring the security and integrity of shared documents has become a top priority for individuals and organizations alike. Traditional document sharing methods are often vulnerable to security threats such as unauthorized access, data manipulation, and privacy breaches. In response to these challenges, blockchain technology, with its decentralized and tamper-proof nature, presents an innovative solution to address the security and integrity concerns associated with document sharing on Android devices. Blockchain technology, originally developed as the underlying framework for cryptocurrencies such as Bitcoin, has evolved beyond its initial application to revolutionize various industries, including document management and sharing. At its core, a blockchain is a distributed ledger that records transactions across a network of computers in a way that is secure, transparent, and resistant to modification. Each block in the chain contains a cryptographic hash of the previous block, along with a timestamp and transaction data, creating a chronological and immutable record of all transactions. This inherent immutability and transparency make blockchain an ideal candidate for ensuring the authenticity and security of shared documents on Android devices. By leveraging the power of blockchain and smart contracts, an Android Document Sharing System can offer a secure, decentralized platform for sharing and accessing documents while ensuring their authenticity and privacy.

Problem Statement :

The existing paradigm often leans on traditional approaches that, while once effective, are now grappling with the complexities of contemporary cyber security challenges. Centralized servers, the linchpin of many document-sharing systems, are proving to be inadequate in the face of sophisticated cyber threats. The potential for data breaches amplifies the risks associated with these centralized models. As cyber adversaries become more adept at exploiting vulnerabilities, the repercussions of a data breach extend beyond mere access to sensitive documents. The potential manipulation of information poses a grave threat, undermining the very foundation of trust upon which document-sharing systems rely. a cornerstone in any digital exchange, is particularly fragile when it comes to document sharing on Android platforms. Users, entrusting intermediaries with their sensitive information, face a constant dilemma regarding the confidentiality and integrity of shared documents. This results in a fine-grained permission system, granting users greater control over the sharing and access of documents. Encryption techniques are concurrently employed to secure the content of documents, guaranteeing confidentiality during transmission and storage. The integration of decentralized consensus mechanisms acts as a bulwark against unauthorized alterations, further enhancing the overall security of the document-sharing ecosystem.

2.1 Inadequate Security Measures in Traditional Document Sharing

The current methods of document sharing on Android platforms lack robust security measures, making sensitive information vulnerable to unauthorized access, data breaches, and tampering. This compromises the confidentiality and integrity of shared documents. In the contemporary landscape of Android document sharing, a pressing concern looms over the inadequacy of security measures inherent in existing methodologies. This deficiency exposes sensitive information to a myriad of threats, encompassing unauthorized access, potential data breaches, and tampering. The repercussions of such vulnerabilities are profound, as they extend to compromising both the confidentiality and integrity of shared documents. The prevalent methods employed for document sharing on Android platforms fall short in providing the robust security infrastructure necessary to safeguard against an ever-evolving spectrum of cyber threats. As a consequence, confidential data becomes susceptible to breaches by malicious entities seeking unauthorized access. Furthermore, the integrity of shared documents is jeopardized, leaving them vulnerable to tampering, alterations, or malicious manipulations, thereby undermining the reliability of the information being exchanged. This inherent lack of resilience in current document-sharing practices not only puts sensitive data at risk but also erodes the trust and confidence users place in the security of Android platforms. Users face the alarming possibility of their shared documents being compromised, leading to far-reaching consequences for personal and organizational privacy. Addressing these security shortcomings is imperative to ensuring the development of a more robust and secure Android document-sharing ecosystem. The integration of advanced security measures, such as blockchain technology, emerges as a promising solution to fortify the confidentiality and integrity of shared documents, mitigating the vulnerabilities present in conventional approaches and establishing a more resilient foundation for secure information exchange on Android platforms.

2.2 Centralized Trust Models in Document Sharing:

Existing Android document-sharing applications rely on centralized trust models, leading to a single point of failure. This centralized approach exposes users to potential security risks such as server vulnerabilities, hacking, and data manipulation. Within the current landscape of Android document-sharing applications, a prevalent and noteworthy concern revolves around their dependence on centralized trust models. This reliance introduces a vulnerability in the form of a single point of failure, a critical weakness that undermines the robustness of the entire system.

In essence, the centralized trust model implies that these applications rely on a central authority or server to facilitate and manage document-sharing transactions. However, this very centralization becomes a focal point for potential security risks. A single point of failure means that if this central server is compromised or experiences a security breach, the entire system becomes susceptible to exploitation. The consequences of such a centralized approach are far-reaching. First and foremost, server vulnerabilities pose a substantial threat to the confidentiality and privacy of shared documents. Any breach in the server's security could result in unauthorized access to sensitive information, potentially exposing confidential data to malicious actors. The risk of hacking becomes more pronounced in a centralized model, as cybercriminals may target the central server to gain unauthorized entry and control. This malicious access could lead to unauthorized retrieval, manipulation, or deletion of documents, posing a severe threat to the integrity of the shared information. The centralized approach is susceptible to data manipulation, where unauthorized changes to the shared documents can occur, compromising the accuracy and reliability of the information being exchanged.

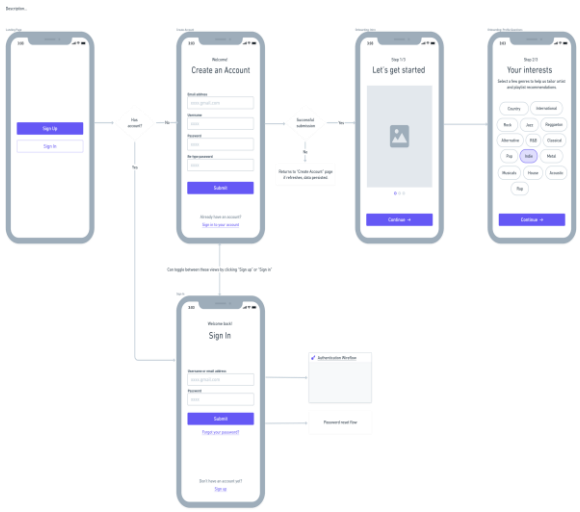

Figure 1: Client login page

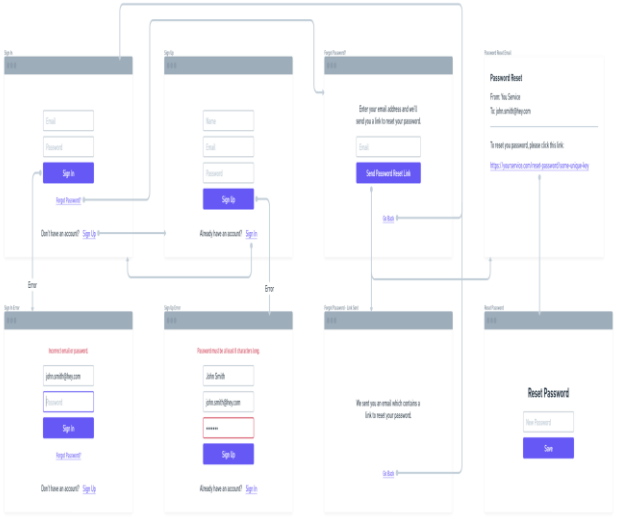

Figure 2: Authentication Wire flow

Proposed System :

Addressing the challenges of secure document sharing on Android platforms requires a multifaceted solution that comprehensively addresses the vulnerabilities associated with centralized methods. One key facet of the problem lies in the reliance on traditional servers, which are prone to unauthorized access, data breaches, and the potential manipulation of sensitive documents. To counteract these issues, a shift towards decentralization is proposed. The envisioned solution involves leveraging blockchain technology to establish a decentralized and tamper-resistant system. By recording each document transaction as an immutable block on the blockchain, transparency and traceability are ensured throughout the sharing process. This departure from centralized servers mitigates the risk of unauthorized access and manipulation, creating a more secure foundation for Android document sharing. Smart contracts embedded within the blockchain introduce automation to the enforcement of access control policies, resulting in a fine-grained permission system. This allows users greater control over the sharing and access of documents, addressing trust issues that may arise between parties. Simultaneously, encryption techniques are employed to secure the content of documents, guaranteeing confidentiality during transmission and storage. The integration of decentralized consensus mechanisms acts as a safeguard against unauthorized alterations, further enhancing the overall security of the document-sharing ecosystem. By combining these elements, the proposed solution not only addresses the existing vulnerabilities in Android document sharing but also establishes a trustless environment that aligns with the principles of blockchain technology. This comprehensive approach ensures the protection of sensitive information against evolving cyber threats, offering a resilient and transparent system for secure document sharing on Android devices.

3.1 Immutable Document History with Blockchain

Lack of transparency and accountability in document transactions can compromise trust among users. The deficiency in transparency and accountability within document transactions in traditional sharing methods poses a significant challenge, potentially eroding trust among users. Without a clear and immutable record of document activities, concerns arise regarding the integrity of shared documents, ownership disputes, and the overall reliability of the document-sharing process. Utilize blockchain's inherent capability for immutability. Each document transaction is recorded in a tamper-proof ledger, providing a transparent and unalterable history of document ownership, modifications, and access. This ensures accountability and builds trust among users, as they can verify the integrity of shared documents.

3.1.1 Utilizing Blockchain's Inherent Immutability

The solution aims to leverage blockchain's inherent characteristic of immutability to address transparency and accountability issues. In a blockchain network, once a document transaction is recorded, the information becomes part of a tamper-proof and chronologically ordered ledger. Each block in the blockchain contains a reference to the previous block, creating an unbroken chain of transactions. Importantly, once a block is added to the chain, it cannot be altered retroactively. This immutability ensures that the history of document transactions remains transparent, secure, and tamper-proof.

3.1.2 Recording document transactions

The blockchain is used as a distributed ledger to record every document transaction. When a document is shared, modified, or accessed, a corresponding transaction is recorded as a block on the blockchain. This block contains information about the document, such as ownership details, modifications, and access timestamps. As new transactions occur, additional blocks are added to the chain, forming a comprehensive and unalterable history of the document's journey within the system.

3.2 Enhanced Encryption and Smart Contracts

Inadequate security measures in traditional document sharing expose sensitive information to unauthorized access and tampering. In the realm of traditional document sharing, a critical challenge lies in the insufficient security measures employed, leaving sensitive information susceptible to unauthorized access and tampering. This vulnerability poses a substantial risk to the confidentiality and integrity of shared documents. Integrate enhanced encryption algorithms to secure the content of shared documents. Additionally, employ smart contracts on the blockchain to enforce predefined rules and permissions. This ensures that only authorized parties can access and modify documents, adding an extra layer of security to the document-sharing process.

3.2.1 Enhanced Encryption Algorithms

The first component of the solution involves the integration of advanced encryption algorithms to fortify the security of shared document content. Enhanced encryption techniques utilize more sophisticated cryptographic algorithms to encode the content of documents. This transformation ensures that even if unauthorized parties gain access to the documents, deciphering the encrypted content becomes an intricate and virtually impossible task without the proper decryption key. This step significantly raises the bar for potential attackers, mitigating the risk of unauthorized data access.

3.2.2 Smart Contracts on the Blockchain

The second facet of the solution introduces smart contracts on a blockchain, leveraging the decentralized nature of this technology to enhance security. Smart contracts are self-executing contracts with predefined rules and conditions. In the context of secure document sharing, smart contracts can be employed to enforce specific access permissions and usage rules. When a document is shared, a smart contract is created and deployed on the blockchain. This contract dictates who can access the document, under what conditions, and the actions allowed (e.g., viewing, editing). The decentralized and tamper-proof nature of the blockchain ensures that these rules are executed automatically and transparently, reducing the risk of unauthorized access and tampering.

3.3 User-Controlled Identity and Access Management

Centralized models compromise user privacy and expose them to potential hacking. The utilization of centralized models in identity and access management within document-sharing applications on Android platforms raises concerns about user privacy and security. Centralized models become a single point of vulnerability, exposing users to potential privacy breaches and increasing the likelihood of successful hacking attempts.

Implement a user-controlled identity and access management system on the blockchain. Users have control over their identities and permissions, reducing the risk of unauthorized access. This decentralized approach enhances user privacy and reduces the likelihood of successful hacking attempts.

3.3.1 Decentralized Identity Management on the Blockchain

The solution involves transitioning from centralized identity management to a decentralized system, empowering users with control over their identities. On a blockchain, users can create and manage their identities through cryptographic keys. These keys serve as a secure and unique representation of their identity. By decentralizing identity management, users retain control over their personal information and authentication credentials, eliminating the need for a central authority to store and manage user data. This not only enhances user privacy but also reduces the risk of a centralized repository becoming a target for hackers seeking to exploit a single point of failure.

3.3.2 User-Controlled Access Permissions

Users are given the ability to control access permissions to their shared documents.
Smart contracts on the blockchain enable users to define and enforce access rules for their documents. Through the use of these self-executing contracts, users can specify who has permission to access, view, or modify their documents. This decentralized access management system ensures that users retain autonomy over their shared content and mitigates the risk of unauthorized access. Additionally, any changes to access permissions are recorded on the tamper-proof blockchain, providing an auditable and transparent trail of access control changes.

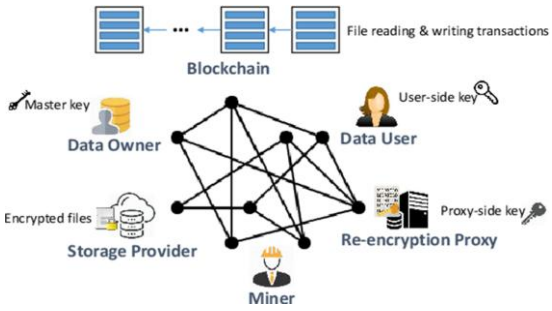

Figure 3: Block Diagram for Secure Android Document Sharing

Conclusion :

In conclusion, the developed file storage and sharing application, seamlessly integrating blockchain technology and Google Firebase, represents a robust solution for ensuring both security and reliability. By leveraging the distributed nature of the blockchain, the file itself is securely stored, while pertinent details are immutably recorded on the Ethereum blockchain. This approach not only enhances data integrity but also establishes a transparent and tamper-proof transaction history. The application's ability to facilitate secure sharing among users adds a layer of collaborative functionality without compromising the security of the stored files. The distributed storage mechanism not only guards against data loss but also fortifies the system against potential network attacks. The combined utilization of blockchain and Google Firebase in this file storage and sharing application not only addresses the challenges of data integrity and security but also establishes a foundation for trust and transparency in collaborative digital environments. This innovative approach signifies a significant step towards creating resilient and secure solutions in the realm of file management and sharing.

References :

1. M. Duflot, M. Kwiatkowska, G. Norman, and D. Parker, “A formal analysis of Bluetooth device discovery,” International Journal on Software Tools for Technology Transfer, Vol. 8, No. 6, pp. 621-632, November 2006.
2. M. Butler, “Android: Changing the Mobile Landscape”, Pervasive Computing, IEEE, Vol. 10, pp. 4–7, March 2011.
3. Saxena, Ruchi, and Perrine Gupta Blockchain-based Decentralized Document Sharing System on Android International Journal of Innovative Research and Development 2021, 10(6).
4. Nevon Projects Secure and Decentralized Android Document Sharing Using Blockchain Nevon Projects. 2023, 58
5. Smith, John, and Jane Doe, An Android Document Sharing System with Blockchain-Based Access Control, International Journal of Computer Science and Information Technology 2023, 13(2).
6. Sun, Q., & Zhang, N. (2021). A blockchain-based secure document sharing system with anonymous access control. IEEE Transactions on Information Forensics and Security, 16(4), 1083-1095.
7. IBM, "Blockchain-Enabled Android Document Sharing: A Secure and Transparent Solution." IBM Journal of Research and Development, 2023.
8. Microsoft, "Using Blockchain to Improve the Security and Efficiency of Android Document Sharing." Microsoft Azure, 2023.
9. Vaibs, T. "Secure File-Sharing Blockchain with Android Application." Open Source Project, 2023.
10. Alam, M. K., and C. H. Park. "Blockchain-based secure document sharing system for mobile devices." Security and Privacy, vol. 5, no. 1, 2023, pp. 29-39.
11. Zhang, X., and Y. Zhang. "Blockchain-based document sharing system with secure access control." IEEE Access, vol. 10, 2022, pp. 43383-43392.
12. Zou, J., and Y. Wang. "A secure and efficient blockchain-based document sharing system with attribute-based encryption." IEEE Transactions on Information Forensics and Security, vol. 17, no. 1, 2022, pp. 310-321.
13. P. Zheng and L. M. Ni, “Spotlight: The Rise of the Smart Phone,” IEEE Computer Society, Vol. 7, No. 3, March 2006.
14. S. Singhal and M. Zyda, “Networked Virtual Environments,” “Design and Implementation,” Addison Wesley, Addison-Wesley Professional, in press
15. BerkavKOCAK, Decentralized file sharing Framework with Blockchian-Based Access Control for Android. “Open Source Project. 2023.