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.2024.11581

"Documental Verification Using Blockchain"

Dipali Ghusale[1], Maya Pawar[2], Dipali Rajnor[3], Prof.S.A.Patil[4]

Student of Department of Computer Technology, Jawahar Education Society, Nashik, Maharashtra[1]

Student of Department of Computer Technology, Jawahar Education Society, Nashik, Maharashtra[2]

Student of Department of Computer Technology, Jawahar Education Society, Nashik, Maharashtra[3]

Assistant Professor of Department of Computer Technology, Jawahar Education Society, Nashik, Maharashtra[4]

Abstract: In today's world, everyone prefers submitting documents in digital format rather than in hard copy, as Digital Document Management is the current trend for submitting documents to officials, authorities, and others. This scenario sparks curiosity in verifying documents in digital settings. When submitting documents online, it is important to provide clarifications about their security, novelty, trustworthiness, and other relevant aspects. On the flip side, the user must ensure they have additional privacy measures in place when submitting documents online for further processing. The suggested system addresses the challenges of Security, Novelty, Integrity, Access Control, and Durability to find solutions to the mentioned problems and queries. Blockchain is a term that encompasses all industries today, whether government or non-government, as it extends its influence across various sectors to demonstrate its importance universally.

The banking industry also utilizes Blockchain to offer security to account holders. The suggested program utilizes Blockchain technology for document verification, offering the highest level of security for users to digitally submit documents to authorities. The authorities can verify the documents intelligently while adhering to security protocols. The Blockchain system generates necessary data as a Block, with the first block being called the Genisis Block, guiding subsequent blocks sequentially without interference. The Miner Verification process in Blockchain checks the records in a Block against incoming records to ensure uniqueness before allowing them to be added to the next block. In the current system, records are blocked by Miner Verification process if they are already in the block. However, in this new system, Miner Verification is a voluntary process where volunteers physically verify Blockchain Miner verification process. More details will be provided later on. Every block in the Blockchain has a unique identity represented in cipher form through the use of SHA, a strong one-way encryption algorithm with a 256-bit encryption process. The whole procedure of the suggested system guarantees a secure and smart document verification scheme using Blockchain technology with effective innovation.

Keywords: Blockchain, Crypto Hashing, Document Check, Integrity Analysis, Secure Hash Algorithm, Cloud Interface, Miner Verification Process, Volunteer, Genisis Block.

I. INTRODUCTION

Currently, users are interested in utilizing smart systems for their daily tasks and are also anticipating the integration of various intelligent systems into their everyday routine. Numerous intelligent devices and mobile phones are accessible in the market to meet people's needs, yet the demand for these systems and their importance is still not adequately met in the current scenario.

The digital document verification process offers total security to users who wish to keep their documents in a digital form. Numerous government departments are shifting from paper to digital formats in their operations, such as the Registration Office and Banking Sectors, among others. These activities and changes help maintain the digital environment and ensure the government operates flawlessly. The Blockchain process typically involves two key steps in processing, known as Miner Requisition and Verification, along with Genisis Block management.

The Genisis Block Management serves as the starting point and guides the following blocks in the process. The suggested document verification system enables users to submit digital documents to the authority even in the event of natural disasters like Tsunami, earthquake, and flood. The documents are inputted into the cloud server in a block-by-block manner, where each user request is treated as a separate block and stored in the server with its own distinct identity.

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.2024.11581

The unique identity established by the server cannot be compromised by any person or service providers, as the user's identification is securely encrypted using the Secure Hash Algorithm (SHA-256). This algorithm operates at a 256-bit frequency and ensures the accuracy of the encrypted result.

To prevent unauthorized access or identification of the password or distinct identity of the blocks by potential intruders or attackers.

II. PROBLEM DEFINITION

The current document verification system, which relies on physical checking, causes numerous challenges and difficulties for applicants, especially in cases of accidents or disasters. The individuals impacted are required to draft a letter to request for disaster recovery assistance, and the request for assistance must be sent to the appropriate authorities for validation. It is important to address these issues and ensure that they do not impact the individual's application for disaster recovery assistance. The system being proposed needs to focus on the verification process, which should be automated and unbiased, with every step being transparent and giving the applicant the opportunity to inquire about it. The applicant can report any misuses to the authority or file a complaint if necessary. The system design should be able to handle faults and be cloud-supported, enabling users to submit applications from anywhere at any time. With this method, applicants can also upload photos of the affected area, allowing authorities to respond quickly and accurately.

III. OBJECTIVES

1. Immutability : Make sure that once a document is stored on the blockchain, it is kept safe from any alterations and remains secure. This creates a dependable history of accuracy over the years, increasing confidence in the legitimacy of the document.
2. Security : Utilize cryptographic methods and decentralized storage to protect documents from unauthorized access, changes, or fraudulent activities. This enhances security protocols to safeguard confidential data.
3. Verification Efficiency : Simplify the verification process by allowing for fast, clear, and automated validation of documents. This decreases the amount of time and resources required for manual verification, improving overall efficiency.

IV. LITERATURE SURVEY

The authors proposed a document verification system that uses blockchain technology to ensure the authenticity and integrity of online documents in "An online document verification system using blockchain technology"
[1]. The proposed system makes use of a distributed ledger to store hashed documents and digital signatures. The authors also built a system prototype and tested its performance. The authors proposed a blockchain-based system for verifying academic certificates in "A blockchain-based online document verification system for academic certificates" The authors also built a system prototype and tested its performance.

V. FEATURES

1. **Decentralization :** Blockchain functions on a decentralized network of nodes, removing the necessity for a central entity. The decentralized structure creates challenges for any one organization to manipulate or control the information.
2. **Transparency :** All participants in the network can see transactions on a blockchain. This openness guarantees that authorized parties can track and confirm any modifications or revisions made to documents.
3. **Document Digitization:** Change physical documents into digital format or generate digital documents. Every document is given a distinct identification number or hash.

VI. DESIGN CONCEPT

The document verification system utilizes various software designs like Ethereum Blockchain, Truffle Suite, IPFS Cluster, AES encryption, and web application. The file uploaded to the system will be stored in IPFS Cluster, which has unique capabilities. The IPFS hash value, pointing to the file stored in the IPFS, will be stored on the Ethereum blockchain platform. Truffle Suite is the platform utilized for developing an application that utilizes the test Ethereum network without requiring computational power or resources. In conclusion, the web application will serve as the platform for the document verification system, allowing users to upload and authenticate documents.

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.2024.11581

The diagram of the entire system design is illustrated in Figure 1. The goal of a document verification system is to confirm the presence and integrity of the file. Prior to verification, the file needs to be uploaded onto the system to confirm that it is the original submission, and it will then be validated against the original file's presence and content. The conditions for uploading a file to the system include it being in pdf format and encrypted with the AES algorithm, requiring a password to access the system. Encrypting data can be achieved via Microsoft software and file explorer, with a prerequisite of having Microsoft version 2007 or a more recent one.

A. **VETRIFICATION PROCESS:** The file must be uploaded before verification. The required elements for verification include the file to be verified, the password for the encrypted file, and the transaction hash of the file. adding information to the system. The application requires all three components to be entered for the verification process to take place. Once these three elements are inputted into the system, verification begins by fetching the transaction hash. Blockchain transaction that contains the identical transaction hash. Next, the system will extract the metadata from the transaction block in order to retrieve the IPFS hash value and the file's password. Following this, the submitted file will undergo hashing, and the file's verification involves comparing the hash value of the submitted file with the stored hash value that has been obtained from the transaction block within the blockchain. Next, the password entered will be checked against the stored password in the blockchain. The system requires three distinct components to authenticate. In the file, there will be four different scenarios in which each component entered into the system is either incorrect or verified.

B. **WRONG TRANSACTION HASH VALUE:** The initial situation occurs when the transaction hash presented does not correspond to any of the transaction hashes in the blockchain. Submitting the transaction serves the purpose of retrieving the designated IPFS hash and the password for the encrypted file stored in the transaction block. If the transaction hash provided does not correspond to any transaction hash in the blockchain, no metadata can be retrieved from the transaction block, leading to the verification process being halted. The data is being compared to other submitted components, but the transaction hash does not correspond to any transaction hash in the blockchain.

C. **WRONG PASSWORD OF THE ENCRYPTED FILE:** Once the transaction hash has been confirmed, the next step is to verify the password for the encrypted file. The second situation occurs when the password provided for the encrypted file does not match the password in the transaction block.

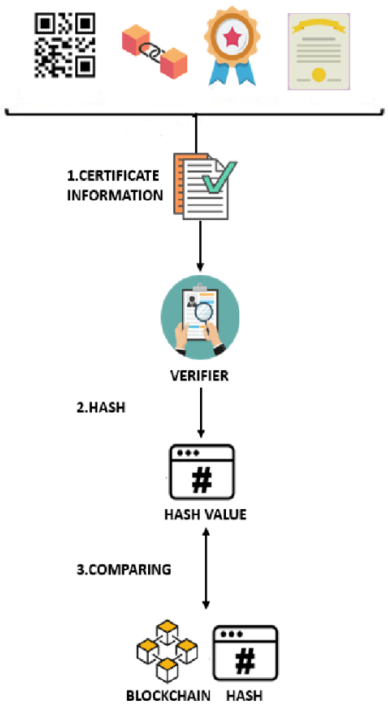

Fig: System Architecture Diagram

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.2024.11581

VII. CONCLUSION

Blockchain is a highly intriguing and sophisticated concept, with numerous organizations now harnessing its advantages to offer secure and reliable data services to their clients. This new system combines the advantages of Blockchain technology and implements a novel document verification approach that receives the document from the user, processes it without any errors, and prevents document duplicates on the server by employing block management principles. The support offered by the web application allows users to access the system globally, but users must upload a photo of the affected area in order for volunteers to assist. The results ratio in the relevant section clearly demonstrates the volunteer adjustment ratio and document occupancy on the server. The whole system functions effectively within the cloud-based document management setup, with security improvements achieved through the use of a one-way data hashing algorithm known as SHA operating at 256 bits. All of these theories have been verified through experiments, and the outcomes are clearly detailed with visual aids in the results and discussion section.

REFERENCES

[1]. A. Singh ‘‘Blockchain Based Verification of Educational and Professional Certificates’’ *Interact. Technol. Smart Educ.*, vol. 18, no. 1, pp. 1–17, May 2023.

[2]. H. Gaikwad, N. D’Souza, R. Gupta, and A. K. Tripathy, ‘‘A blockchain based verification system for academic certificates,’’ in *Proc. Int. Conf. Syst., Comput., Autom. Netw. (ICSCAN)*, Puducherry, India, Jul. 2021, pp.1–6,doi: 10.1109/ICSCAN53069.2021.9526377.

[3]. U. Rahardja, M. A. Ngad, S. Millah, E. P. Harahap, and Q. Aini, ‘‘Blockchain application in educational certificates and verification compliant with general data protection regulations,’’ in *Proc. 10th Int. Conf. Cyber IT Service Manage. (CITSM)*, Sep. 2022, pp. 1–7, doi:10.1109/CITSM56380.2022.9935909.

[4]. V. Senthilkumar‘‘Certificate Storage and Verification using Blockchain,’’ in *Proc.3rd Int. Conf. Intell. Comput. Instrum. Control Technol. (ICICICT)*, Aug. 2023, pp. 1201–1204,

[5]. C. Lakmal, S. Dangalla, C. Herath, C. Wickramarathna, G. Dias, and S. Fernando, “IDStack -The common protocol for document verification built on digital signatures,” 2017 Natl. Inf.Technol. Conf. NITC 2017, vol. 2017–Septe, no. September, pp. 96–99, 2018.

