Archives available at journals.mriindia.com

International Journal of Recent Advances in Engineering and Technology

ISSN: 2347-2812
Volume 14 Issue 1s, 2025

An Attribute-Based Access Control Mechanism for Cloud Storage using Blockchain Technology

Dumbre Sayali P[1]; Prof. Dere Kapil D.[2]

Computer Engineering, JCEI's Jaihind College of Engineering Kuran

Peer Review Information

Submission: 20 Jan 2025
Revision: 24 Feb 2025
Acceptance: 27 March 2025

Keywords

Attribute-Based Access Control
Blockchain Technology
Cloud Storage Security
Decentralized Access Control
Data Privacy in Cloud Computing

Abstract

Implementing Attribute-based Access Control for data sharing in order to generate knowledge is a complex area of research. This is because an application may need to access personal data that is stored in a different country from where the application is being accessed. This article presents a data sharing platform for Attribute-based Access Control. The platform consists of a global cloud that is constructed on top of various security gateways located in different countries. When an application seeks permission to access data from a specific country or region, the global cloud retrieves the data stored in local data hubs using the security gateway of that region. During the process of moving data to the global cloud, the security gateway logs this transfer information on a blockchain that is managed and maintained by the global cloud. This study introduces a method for sharing data in a cloud environment using reliable blockchain technology. The entire system operates on the blockchain within a decentralized peer-to-peer foundation.

Introduction

The suggested platform has the capability to manage any participant, such as a data sender, data receiver, or any other entity, that behaves inappropriately. We evaluate our technology through empirical analysis, presenting various graphs derived from multiple trials conducted in blockchain contexts. In addition, we explain the functionality of the multilayer signature, specifically the Elliptic Curve Digital Signature Algorithm, within our platform. Our project aims to create a cross-border data sharing system that utilizes blockchain technology to store and transport historical data in real-time on a display screen. The objective is to establish a hierarchical fog computing environment that enables parallel data processing for end-user applications. To develop and execute a proprietary SHA family block for the whole blockchain. Blockchain is a decentralized method of storing data for various transactional systems. Its purpose is to ensure the utmost data security during data transactions and prevent different network and data threats originating from fraudulent requests. The data is safeguarded in the cloud by additional cryptographic measures such as sophisticated signature and exclusive requirement encryptions, which will be further discussed. The primary advantages of an access control system include the capacity to tailor the access policy for encrypted data without the need for duplication among numerous participants, the ability to establish dynamic access policies, and the secure uploading and sharing of data with multiple groups. Verification of sender and receiver identities through the use of ECC signature verification. The blockchain ensures data security by enabling automatic recovery from any type of database attack.

Literature Survey

The limits of existing supply chain management systems are examined by the authors of [1], who also present a concise overview of how blockchain technology could potentially mitigate these shortcomings. The existing configuration of the supply chain has a centralized structure, hence engendering a multitude of challenges. The key issue at hand is to transparency, as the supplier possesses the capacity to unilaterally increase tax rates, subsequently burdening other parties within the supply chain as a result of self-demand.

In [2] the literature indicates that the utilization of blockchain smart contracts is recommended for the purpose of automating supply chain transactions. The execution of the transaction is contingent upon the satisfaction of the conditions outlined in the smart contract, rendering the presence of a third party superfluous and thereby eradicating any concerns pertaining to trust.

In [3] it encompasses a header that encompasses vital information. In edge devices, the data is saved in blocks that are organized in a chronological manner, and later transmitted to the cloud. The utilization of blockchain technology within a cloud-based infrastructure offers a very safe platform for data storage.

The literature in [4] the application of blockchain technology in the surveillance of counterfeit pharmaceuticals throughout the whole supply chain. Pharmaceutical manufacturers furnish comprehensive information for every pharmaceutical within this system, encompassing the drug's nomenclature, date, whereabouts, constituents, application, and adverse reactions. A smart contract is utilized to authorize this. If a person wishes to obtain additional information regarding a medicine, they have the option to furnish the maker with their public key. This key will then be utilized to encrypt the QR code and transmit it to the participant.

The authors in [5] The agricultural supply chain has numerous shortcomings, such as the existence of intermediaries and middlemen that use marketing channels for personal benefit while inadvertently transferring losses onto farmers. The application of blockchain technology has promise in addressing issues such as disinformation, misconceptions, and trust deficits across several domains by offering precise and reliable information pertaining to the supply chain. Production companies have the potential to enhance their decision-making process, resulting in heightened profitability and diminished overall losses.

The literature [6] This study undertakes an analysis of the many difficulties encountered throughout the whole supply chain and assesses their compatibility with blockchain technology. The primary aim of this essay is to offer a thorough examination of the various areas where blockchain technology intersects with supply chain management, in order to encourage further investigation and advancement.

According to [7], The researchers examine the possible application of blockchain technology in establishing a full log of theft occurrences in composite materials across the entirety of the production process, encompassing transportation, handling, and storage. The utilization of blockchain technology has been recognized in businesses characterized by rigorous requirements, such as the aerospace sector, where the ability to monitor components or inventories is of utmost importance.

The authors [8] This paper presents a proposed Supply Chain Management model aimed at improving the tracking and reliability of logistical operations. The proposed model exhibits the capacity to streamline market transactions and commercial interactions inside worldwide company networks, eliminating the need for intermediaries that are often involved in the conventional Supply Chain model. Hyperledger Fabric is utilized to implement this concept.

Literature [9] the eliminating intermediaries and promoting transparency among all participants in the supply chain network, blockchain technology offers a promising solution. However, the utilization of blockchain technology in certain scenarios may lead to an increase in processing costs. To overcome this obstacle, the authors of creative compositions.

In [10] an integrated system that combines elements of both blockchain and off-chain methodologies. The server facilitates the exchange of information between the blockchain and the supply chain by furnishing hashed data pertaining to all instances or records within the blockchain.

Table 1.1: Overview of existing systems

Ref. No	Methodology	Algorithm	Gap Analysis
[11]	The privacy and security of the proposed e-Government system are facilitated by the encryption, validation, and immutable techniques provided by Blockchain technology.	Node registration and user registration using blockchain	Implementation has done on e VIBES simulator no real implementation results has shown
[12]	The store use many methods, such as Zero Knowledge proof, Public-key cryptography, and IPFS, to recover and identify any efforts to alter copies. It produces far more effective solutions compared to the other systems. .	Blockchain using various database attack detection models	Cryptography , PoW, token
[13]	The hybrid blockchain is utilized to record all transactions related to land sales. The aforementioned transactions undergo verification by a miner, which operates on peers or nodes authorized by the government.	Blockchain for manufacturing supply chain and logistics	Proof of Work, Proof of stake, Byzantine Fault Tolerance
[14]	The objective is to enhance the land registration process by improving transparency, efficiency, cost-effectiveness, and minimizing occurrences of fraud. Tracking the hand-to-hand transfers of property using built-in Blockchain technology is possible.	Approaches toward blockchain innovation	Ethereum blockchain and custom smart contract
[15]	This study elucidates the potential of Blockchain technology in enhancing the transparency, trustworthiness, and efficiency of land ownership data.	Blockchain for transportation systems	Hash generation, smart contract, mining, PoW,

Proposed System Design

We provide a concise overview of a potential application of the algorithms mentioned in Figure 1.1. In order to enhance efficiency, it is recommended that data be encrypted using a symmetric cipher, specifically the PBE with MD5 and DES algorithm employed in this system. The encryption process involves the use of a fresh random number as the key, which is also encrypted. This encryption is performed using our specific scheme and is subsequently attached to the cipher text stored by the cloud service provider (CSP). The process of decryption can be achieved by users who have access to the symmetric key, or in other words, individuals who possess the requisite qualities and have not had their access revoked.

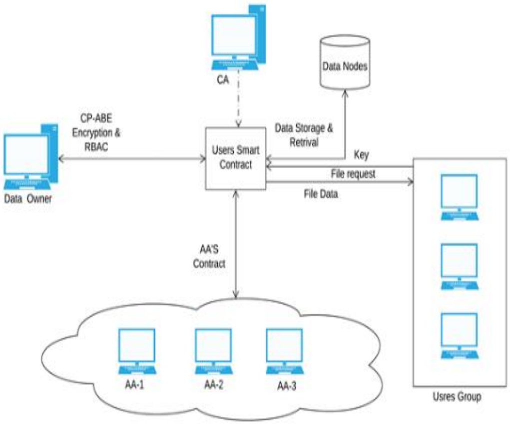

Figure 1: Proposed System Design

Implement Module

Data Owner (DO): A DO refers to any person, regardless of their rights, who possesses material that may be uploaded and shared. A Data Object (DO) establishes an access policy to regulate data access, ensuring that only authorized users with corresponding attribute sets are granted authorization to decrypt and gain access to the plaintext data.

Attribute Authority (AA): An Authentication Authority (AA) is tasked with assigning a specific group of users and a set of qualities, referred to as domains, to users and distributing keys to them. Each AA has the ability to register users within its domain and distribute the attribute keys associated with its domain to said users. The primary objective of an AA is not just to create users, but also to assign attributes. It has the ability to allocate characteristics to users who are not part of its own domain. For example, a user established by AA may acquire traits that are assigned by AA. In our approach, we make the assumption that each AA is semi-trusted. This means that while AA may have an interest in the value of a plaintext, it does not have any intention of interfering with it.

Data User: A data user refers to an individual who has been granted authorization to access encrypted data. The individual completes the registration process with an Attribute Authority and acquires one or many sets of attributes. When the attribute sets meet the access policy for a cipher text, the end user can access the cipher data. By inputting the correct key, they can decrypt the cipher text and gain access to the plaintext.

Distributed Blockchain: The Blockchain serves as a decentralized ledger that is employed to depict the present condition of delegated access privileges within the system. The Root Authority and the Attribute Authorities are responsible for managing permissions to engage with the Blockchain.

Algorithms 1: SHA-256 Values Generation

```
Input: The original block, previous-hash, and data d,
Output: The hash H was generated based on the provided data's.
Step-1:  The record is inputted as d.
Step-2: Utilize SHA-256 from the hash values range.
Step-3: C_Hash= SHA-256(d)
Step-4: Retrun C_Hash
```

Algorithms 2: Peer-to-peer (P2P) verification protocols

```
Input: The user receives an IP address and a User Transaction TID.
Output: Activate the IP address or current query to determine the validity of any connection.
Step 1: The user generates a mysql query using DDL, DML, or DCL.
Step 2: Retrieve the present IP address.
For each (read IP into IP address)
If(Assuming that the connection (IP) is true)
Flag-true
Else
Flag-false
End for-each
Step 4 : if (Flag.equals(valid))
Peer-to-peer (P2P) verification valid
Else
Peer-to-peer (P2P) verification Invalid
End if
End for
```

Mathematical Model

The system is comprised of five distinct phases, each of which operates with its own set of dependencies.

System Sys = (S1, I2, T3, I4, O5) where –

- S1: represents a limited collection of states.
- I2: represents a finite collection of symbols known as the alphabet.
- T3: The transition function is denoted as T3.
- I4: represents the beginning state from which any input undergoes processing.
- O5: denotes a collection of final state/states.

When all data nodes share the similar blockchain, they will completely return a value of 1.

S1 = the encryption and decryption and genesis block contains the initial transactional data

S2= {PBEwithMD5 and DES, SHA-256, Mining, Validation and Majority, Recovery}

S3 = Validate all database server (DB1 ⊆ DB 2⊆ DB 3⊆ DB 4) all database server data validation process

S4 = The initial transaction denoted as T[0],

S5 = {Commit Transaction,
Get_Show_Data}

State =>

1: Whether all chains are valid or identical.

0: If any server with a length of t(n) contains an incorrect chain.

CONCLUSION

The primary outcome of this study is the development of a software system prototype that effectively incorporates the access control model applicable to data kept in contexts lacking trust. The system algorithms have been chosen based on their reasonable complexity, functionality, and implementation complexity. The access control system offers several significant advantages. Firstly, it allows for the customization of access policies for encrypted data without the need for duplication across a large number of participants. Secondly, it enables the definition of dynamic access policies. Thirdly, access policy changes do not necessitate any additional actions from other system members, thereby eliminating the need for frequent modifications to user keys. Lastly, the system ensures the integrity of transaction information, encompassing the granting and alteration of access, the acquisition of file access, the rejection of access, and the inability to modify such data. This is achieved through the utilization of blockchain technology and smart contracts.

References

S. Madumidha, P. S. Ranjani, S. S. Varsinee and P. S. Sundari, "Transparency and Traceability: In Food Supply Chain System using Blockchain Technology with Internet of Things," 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), 2019, pp. 983-987, doi: 10.1109/ICOEI.2019.8862726.

M. A. Habib, M. B. Sardar, S. Jabbar, C. M. N. Faisal, N. Mahmood and M. Ahmad, "Blockchain-based Supply Chain for the Automation of Transaction Process: Case Study based Validation," 2020 International Conference on Engineering and Emerging Technologies (ICEET), 2020, pp. 1-7, doi: 10.1109/ICEET48479.2020.9048213.

K. M. Botcha, V. V. Chakravarthy and Anurag, "Enhancing Traceability in Pharmaceutical Supply Chain using Internet of Things (IoT) and Blockchain," 2019 IEEE International Conference on Intelligent Systems and Green Technology (ICISGT), 2019, pp. 45- 453, doi: 10.1109/ICISGT44072.2019.00025.

R. Kumar and R. Tripathi, "Traceability of counterfeit medicine supply chain through Blockchain," 2019 11th International Conference on Communication Systems & Networks (COMSNETS), 2019, pp. 568-570, doi: 10.1109/COMSNETS.2019.8711418.

B. Hegde, B. Ravishankar and M. Appaiah, "Agricultural Supply Chain Management Using Blockchain Technology," 2020 International Conference on Mainstreaming Block Chain Implementation (ICOMBI), 2020, pp. 1-4, doi: 10.23919/ICOMBI48604.2020.9203259.

S. Yousuf and D. Svetinovic, "Blockchain Technology in Supply Chain Management: Preliminary Study," 2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS), 2019, pp. 537-538, doi: 10.1109/IOTSMS48152.2019.8939222.

A. E. C. Mondragon, C. E. C. Mondragon and E. S. Coronado, "Exploring the applicability of blockchain technology to enhance manufacturing supply chains in the composite materials industry," 2018 IEEE International Conference on Applied System Invention (ICASI), 2018, pp. 1300-1303, doi: 10.1109/ICASI.2018.8394531.

R. G.S. and M. Dakshayini, "Block-chain Implementation of Letter of Credit based Trading system in Supply Chain Domain," 2020 International Conference on Mainstreaming Block Chain Implementation (ICOMBI), 2020, pp. 1-5, doi: 10.23919/ICOMBI48604.2020.9203485.

S. NASIH, S. AREZKI and T. GADI, "Enhancement of supply chain management by integrating Blockchain technology," 2019 1st International Conference on Smart Systems and Data Science (ICSSD), 2019, pp. 1-2, doi: 10.1109/ICSSD47982.2019.9002771.

J. C. López-Pimentel, O. Rojas and R. Monroy, "Blockchain and off-chain: A Solution for Audit Issues in Supply Chain Systems," 2020 IEEE International Conference on Blockchain (Blockchain), 2020, pp. 126-133, doi: 10.1109/Blockchain50366.2020.00023.

Elisa, Noe, et al. "A Secure and Privacy-Preserving E-Government Framework Using Blockchain and Artificial Immunity." IEEE Access 11 (2023): 8773-8789.

Hasan, MM Rakibul, Md Mahinur Alam, and Kanita Jerin Tanha. "Decentralized Blockchain Based Land Deed Verification and Reservation System in Bangladesh." 2022 25th International Conference on Computer and Information Technology (ICCIT). IEEE, 2022.

Kadam, Rishikesh, et al. "Land Records System Using Hybrid Blockchain." 2020 International Conference on Convergence to Digital World-Quo Vadis (ICCDW). IEEE, 2020.

Kusuma, G., et al. "Secure Storage of Land Records and Implementation of Land Registration using Ethereum Blockchain." 2023 Third International Conference on Artificial Intelligence and Smart Energy (ICAIS). IEEE, 2023.

Manocha, Prabhat, Subhranil Som, and Kanjam Manocha. "Blockchain as an instrument for land ownership and authorization of services." 2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO). IEEE, 2021.