IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

An Attribute-Based Access Control System For Cloud Storage With Blockchain

Abhale Amol Anil[1]
Department of Computer Engineering, Sharadchandra Pawar College of Engineering, Dumbarwadi, Otur, Pune, India

Prof. Dr. Monika Rokade[2]
Department of Computer Engineering, Sharadchandra Pawar College of Engineering, Dumbarwadi, Otur, Pune, India

Prof. Dr. Sunil Khatal[3]
HOD, Department of Computer Engineering, Sharadchandra Pawar College of Engineering, Dumbarwadi, Otur, Pune, India

Abstract:
Access control systems are employed within the realm of computer security to govern the authorization of individuals to access essential or valuable resources, including but not limited to data, services, computational systems, and storage space. Attribute-based Access Control (ABAC) policies are comprised of a collection of conditions that define the characteristics of the persons, resources, environment, etc., involved in the access request. This report presents a novel methodology utilizing blockchain technology to facilitate the dissemination of policies that delineate the entitlement to access data and resources. Additionally, it proposes the utilization of smart contracts to enable the decentralized transfer of these rights among users in cloud computing. The proposed approach aims to establish self-enforcing policies over Virtual Machines (VMs). The proposed model entails the public visibility of policies and rights exchanges on the blockchain, which are securely encrypted. Additionally, data is stored in the cloud. Consequently, any user has the ability to access the policy associated with a given data or resource, as well as the individuals who currently possess the rights to access said data or resource. The proposed system facilitates distributed auditability, hence mitigating the risk of a party engaging in fraudulent practices to deny the rights conferred by a policy that can be enforced.

I. INTRODUCTION

Blockchains possess several advantageous attributes, such as exceptional availability, unchangeability, transparency, and the dispersion of trust. Ten years after the introduction of Bitcoin, the Blockchain technology has experienced notable progress, evolving from a rudimentary cryptocurrency framework to a wide array of distributed ledger systems. These systems enable the development of trust in the precision of code execution and shared storage, hence obviating the need for a definitive central trusted entity. ABE is a new type of encryption algorithms that simplifies the process of encrypting data inside an access policy that includes attributes. In Cipher text-policy attribute-based encryption (CP-ABE) systems, the access policy is integrated into the cipher text during the data encryption process. Public key cryptography is a traditional method that entails the encryption of data for a specific receiver by utilizing their private key. Proficiency in this procedure requires familiarity with both the target recipient and their public key. The restricted scalability of these solutions becomes apparent when there are frequent changes in the number of participants. The need to encrypt the data set for every authorized user arises anytime a collaborator is added or removed. Hybrid systems offer a practical solution; yet, their administration becomes complex as the number of participants grows.

Block Chain work:

Decentralized Network: The blockchain technology is characterized by its decentralized nature, wherein a central authority is absent. In contrast, the system functions within a network of interconnected computers, referred to as nodes, which collaborate to authenticate and document transactions.

Transactions: Transactions serve as the foundational components of a blockchain environment. The data includes details regarding the sender, recipient, and the specific quantity of cryptocurrency being sent.

Blocks: Blocks are formed by grouping transactions together. Every block within the blockchain comprises a collection of transactions, a timestamp, and a reference to the preceding block, so establishing a sequential sequence of blocks.

Consensus Mechanism: To append a block to the blockchain, consensus must be reached within the network regarding the block's validity. Consensus is attained by means of a consensus mechanism, which encompasses a collection of regulations that dictate the manner in which nodes attain consensus over the legitimacy of transactions. Proof of Work and Proof of Stake are two examples of consensus techniques.

Security: The blockchain is securely connected to the preceding block using a cryptographic hash. Any effort to modify the data within a block would need modifying all following blocks, rendering it exceedingly difficult to manipulate the blockchain.

Smart Contracts: Smart contracts are contractual agreements that are capable of completing themselves, wherein the buyer and seller's terms are encoded directly into lines of code. The terms of the contract are automatically enforced and executed upon the satisfaction of specific criteria. Blockchain platforms incorporate smart contracts as a fundamental component.

II. 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,

III. 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.

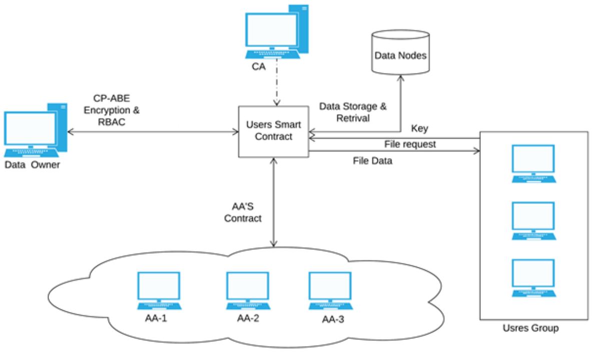

Figure 1: Proposed System Design

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.

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

[1]. 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.

[2]. 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.

[3]. 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.

[4]. 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.

[5]. 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.

[6]. 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.

[7]. 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.

[8]. 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.

[9]. 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.

[10]. 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.
[11] Elisa, Noe, et al. "A Secure and Privacy-Preserving E-Government Framework Using Blockchain and Artificial Immunity." IEEE Access 11 (2023): 8773-8789.

[12] 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.

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

[14] 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.

[15] 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.