IOSR Journal of Engineering (IOSRJEN) www.iosrjen.org
ISSN (e): 2250-3021, ISSN (p): 2278-8719 Special Issue || September 2021 || PP 44-49
7th National Conference On Advancements in Communication, Computing and Electronics Technology-ACCET 2021

A Document Verification System To Avoid Lazy Auditors Using Blockchain Technology

Dr. (Miss) Revati M. Wahul (MESCOE)
Amol Desai (MESCOE)
Siddhesh Joshi (MESCOE)
Vinayak Patil (MESCOE)
Mohd Danish(MESCOE)

Abstract: *Consumers can benefit significantly from the use of cloud computing service in terms of data management. However, it poses some security issues, one of which is data integrity. Established document verification systems are vulnerable to lazy auditors who may not execute on-time verification, while document verification strategies enable a consumer to hire a third-party auditor to verify data integrity on their sake. Furthermore, many public authentication schemes depend on public key infrastructure, and certificate management issues are a concern. We suggest using blockchain technology in this paper; Attribute Based Encryption (ABE) is a cryptographic practice that gives data owners direct control over their data stored in public cloud storage. The typical ABE structure requires a single expert to manage a collection of attributes, which can serve as a single-point bottleneck for both security and efficiency. In the cloud, we currently use the multi-authority verification protocol Role Base Access Control (RBAC). Threshold Multi-Authority Access Control System is what RBAC stands for. TPA has fair access to the entire attribute collection in RBAC, but no one has total control over any particular attribute. We are building an effective multi authority access management framework in public cloud storage that offers dramatic protection utilizing blockchain technology. TPA verifies the user's identity and provides access control according to roles. The framework can also defend against network attacks such as DDoS and SQL injection.*

Keywords: *Blockchain,Trusted Party Auditor (TPA), public key infrastructure (PKI), Cloud Storage, Role base Access Control (RBAC).*

I. Introduction :

Users' eligibility to use such programs is often differentiated using roles and names. A role-based access control (RBC) system, which defines access controls between users and facilities, serves as such a mechanism. Users are linked to roles, and roles are linked to position services in RBAC. A structure like this many people use it organizations and businesses to extend their internal access control standards to their computer systems. If a company's programmer has access to the backend and frontend source code, the quality assurance team only takes access to the source code listed above. This access control is widely used within an organization, but it's important to remember that RBAC is a flexible system, and functions are often used across organizations. Students, for example, are often authorized to buy books at reduced prices. Users' ability to use such programs is usually determined by their roles and names. The role-based access management (RBAC) system, which defines the access management relationship between users and facilities, has sculpted such a process. Users are linked to functions, and roles are linked to services in RBAC. Many businesses and companies use such a mechanism in their computer systems to meet their internal access control requirements. A programmer, for example, has access to both the backend and frontend supply codes in a business, while quality assurance staff only has access to the frontend supply codes. This access management is often used within a company, but it should be noted that RBAC is a flexible framework; that is, roles are often used across organizations. Students, for example, are often permitted to purchase books at a reduced price.

II. LITERATURE SURVEY

Smart Contracts [1]It is also known as crypto-contract, it is a program used to transfer / control the property or digital currents in particular parties. Not only does it define the terms and conditions but it can also implement the policy / agreement. Because of the complexity and protection, these smart contracts has been stored in the block chains and BitCoin is an ideal token to store those contracts. The smart contract specifies where the transaction should be transferred / returned or where the transaction is occurred when a transaction is considered.

Currently CSIRRO team has proposed a new approach to integrate Block on IOT with [2]in the beginning, he uses smart-home technology to find out how IoT can be disabled. Block wheels are particularly useful for providing an access control mechanism for Smart Device Transactions that take place in the Smart-Home. When it comes to incorporating BC technology into IoT, this quest offers some additional security features; however, any mainstream BC technology must have a definition that excludes the concept of comprehensive algorithms. Furthermore, in the case of IoT, this technology is unable to provide a generic type of block-chain solution.

According to Ilya Sukhodolski. The Al [3]system shows a multiple user system prototype for controlling access to databases housed in amazing cloud environments. Cloud storage, like other insecure settings, necessitates the ability to securely exchange information. Without the provider's expenditure, our solution offers access control over the data stored in the cloud. Mechanism for Controlling Access The dynamic feature-based encryption scheme, which has dynamic features, is the key method. Our systems have an irreversible log for accessibility requests for all the meaningful security events such as broad funding, access policy assignment, modification, or cancellation using Blockchain-based decentralized badgers. We provide a collection of cryptographic protocols that guarantee the security of the secret or secret key used in cryptographic operations. Only the block on laser transmits the hash code of the sifter text. Our framework has been tested on IteriumBlockchan platforms and prototype smart contracts.

According to [4] a basic IoT based Blockchain fusion model having four layers containing different types of IoT devices. IOT data in huge amount is considered to be stored in Distributed systems. Then, a case study for blockchain based IOT application, a Machine-to-Machine(M2M) trading system, is proposed on the Ethereum blockchain. Smart contracts for device registration are also build , data storage, service providers and genuine payment, and the proof-of-concept is implemented using 2 Raspberry Pis to work with smart contracts. Blockchain will improve IOT applications in transparency, traceability and security is verified in proposed system.

According to [5] Edgence (EDGe + intelligENCE, is proposed to serve as ablockchain-enabled edge-computing platform in IoT usecases to intellectually handle huge decentralized applications. To extend the range of blockchain to IOT based dApps, Edgence adopts master node technology for connecting to a closed blockchain based system to the real world. A master node containing a full node of the blockchain along with collateral, and is deployed on an edge cloud of mobile edge computing, which somehow is convenient for master node for using resources of the edge cloud and running IOT dApps

According to [6]introducing HCloud, a secure JointCloud platform for IoT systems that operate without a server. HCloud enables an IoT server to be deployed with many servers but fewer functions, and it schedules these functions on separate clouds according to a scheduling policy. The client defines the policy, which includes the requisite functionalities, execution tools, latency, and price, among other things. HCloud gathers each cloud's status and, based on the schedule policy, dispatches serverless functions to the most appropriate cloud. We will also ensure that our device cannot deceive the cloud status or incorrectly dispatch the target functions by using blockchain technology.

According to [7] introducing the concept of a decentralized gasified service exchange platform where we can find the solution providers who can offer and request services in an peer- to-peer(P2P) algorithm. Costing as well as decision to exchange services has been set during operation time based on gasification policies according to the business goals. In this proposedsystem we project blockchain technology whichwill provide a tokenized platform where the IOT solution providers can implement gasification techniques using the smart contracts to maximize profits during service offerings as well asrequesting.

According to Vipul Goyalet. Al [8]develops key-policy attribute-based encryption, which is a modern cryptosystem for properly sharing encrypted data (KPABE). Cephet text is labeled with a collection of properties and controls in our cryptosystem, which bind to private key access configurations from which a user can decrypt the encryption. We demonstrate how our product can be used to share audit log information and broadcast encryption. Our design is compatible with private key providers that use categorized identification-based encryption (HIBE).

Hao Wang et Mate Al [9]They have a secure electronic health record (EHR) system based on blockchain technology and special-based crypt co-occurs. In our scheme, we encrypt medical data with attribute-based encryption (ABE) and identity-based encryption (IBE), and we apply digital signatures with identity-based signature (IBS). We present a new cryptographic platform called a joint feature-based / identity-based encryption and signature (C-AB / IB-ES) to obtain various functions of ABI, IBE, and IBS in cryptography. It simplifies system maintenance and eliminates the need for several cryptographic systems to acquire different security requirements. In addition, to ensure the accuracy and examination of medical records, we employ blockconne techniques. Finally, we have a medical insurance company demonstration application.

According to [10] a scheme for generatinga seed which is needed for key generation and a scheme for managingthe public key using blockchain. First will be a random seed generation scheme required for key

generation? For preventing the risk of a man-in-the-middle attack and reverse engineering, seeds will be generated using out-of-band communication and hardware variation. Secondly for thekey management system for IOT device using blockchain? We propose a scheme to distribute the public key on the blockchain network. Forencrypting a session key whichwill be used for communication between devices the public key will be used.

Project Scope :

Blockchain, a digital laser technology that can safely maintain data records and ever-growing lists of transactions, has the power to potentially transform real estate, according to industry experts. The way the procrastinating auditors industry simplifies and accelerates data in areas such as revenue cycle management, real estate data operation and supply chain verification, dramatically reducing back-office data input and maintenance costs in the blockchain, and data accuracy and security has the power to improve.

III. METHODOLOGY

- System must validate the previous block before commit block.
- User can access the data over the internet 24*7.
- If any block has changed by third party attacker or unauthorized user, it must show during transaction current blockchain is invalid.
- It can recover the invalid blockchain using other data nodes, with the help of majority of trustiness.
- The data is broadcasttowards the network when a node or the user want to make a transaction.
- The node or the user who will receive the data will verify the authenticity of the data received in the network. Then the verified data is stored into the block.
- The proof of work algorithm or the proof of stake algorithm is used for validation for a certain transaction made by all the nodes or users.
- The storage of the data to the block which is further added to blockchain is done by Consensus algorithm. And all users or the nodes in the network accept the respective block and extend the chain based on the block

5.1 System Architecture:

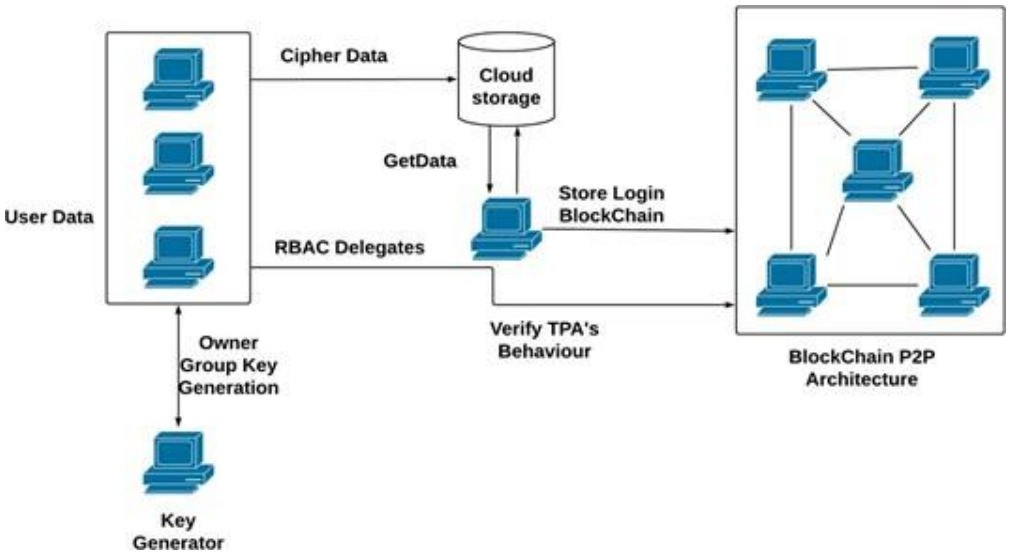

Figure 1 : Proposed Systemarchitecture

Algorithm Design

Algorithm 1: Hash Algorithm

Input: First block, previous hash, data d
Output: Generated hash key H according to the given information
Step 1: Input data as d
Step 2: Apply SHA 256 from SHA family
Step 3: Current Hash= SHA256 (d)
Step 4: Return Current Hash

Algorithm 2: Protocol for Peer to Peer Verification

Input: User Transaction request, Present Node Chain CNode [chain], AddedResidual Nodes blockchain NodesChain [Node_id] [chain]
Output: If some of the chain is invalid, boost it; otherwise, run the current query.
Step 1: User create any transaction like DDL, DML or DCL query
Step 2: Get current server blockchain
Cchain←Cnode[Chain]
Step 3: For each

$$NodesChain\ [Nodeid, Chain] \sum_{i=1}^{n} (GetChain)$$

End For
Step 4: For each (read I into the NodeChain)
If (!equalsNodeChain[i] with (Cchain))
Flag 1
Else Continue Commit query
Step 5: If (Flag == 1)
Count = SimilarNodesBlockchain()
Step 6: Calculating the majority of the server Recovery invalid blockchain from specific node
Step 7: End If
End If
End For

Algorithm 3:Mining the blockchain for valid hash generation

Input: Hash Validation Policy P[], Current Hash Values hash_Val
Output: Valid hash
Step 1: System generate the hash_Val for ith transaction using Algorithm 1
Step 2: If (hash_Val.valid with P[])
Valid hash
Flag =1
Else
Flag=0
Mine again randomly
Step 3: Return valid hash when flag=1

Mathematical Model

First, we consider a
A= {A1, A2, A3……..An} each set holds the specific module activity of system.
A1= {file uploading phase or file sending phase}
A2= {data encryption and re-encryption phase}
A3= {Share and Access control for delegates}
A4= {Revocation and proxy key re-generation}
A1 will define the first module in which user will upload the multiple documents

$$\text{Data}[d] = d[k] + \sum_{k=0}^{n} (\text{a1}, \text{a2} \ldots \ldots \text{an})$$

d[k] ← {Att1, Att2……Attn} each document contains the set of attributes
keys[] ← Keygen(RandomText)
Enc[c1] [c2] ← encryption(Data, keys[])
DecData← decryption ([c1] [c2], keys[])
Using the below formula we can define the role based access control for each of the ith user

$$\text{U[i]}\leftarrow\text{file(x)} = \sum_{\text{n}=1}^{\text{m}} \left(\text{u}_{[\text{n}]}[\text{read}, \text{write}, \text{update}, \text{delete}]\right)$$

Using the below formula the revocation has been done
U[i] ← Revoke(F) : DataOwner

IV.Results and Discussions

Evaluate the algorithm's deviations from the proposed SHA value. Essentially, this is done to assess the proposed hash string in order to decide if the mining policy is correct. When the system produces SHA codes for given transaction data, it often fails to meet the mining policy. To enforce the proposed mining policy in unity with the provided scenario mining in order to generate multi variations on a given string. The graph below shows how long it took to generate a correct SHA, mining, and consensus string for a specific transaction in milliseconds.

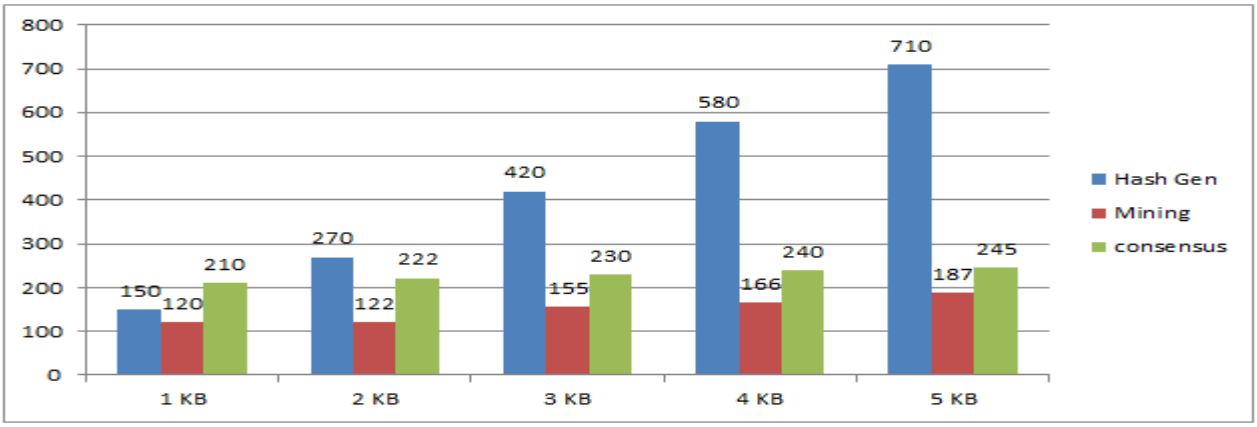

Figure 2: Transactions recorded in blocks to form Blockchain(Estimated)

In the second experiment, determine how many variations the algorithm takes from the proposed SHA value. Basically, the aim of this experiment was to see whether the proposed hash string was correct or not according to the mining policy. When a system produces a SHA code for a given transaction data, it often fails to meet the mining policy. To enforce the proposed mining policy in accordance with the given scenario mining in order to produce multiple variations on a given string. Figure 3 shows the time it took to produce a correct SHA string for a particular transaction in milliseconds.

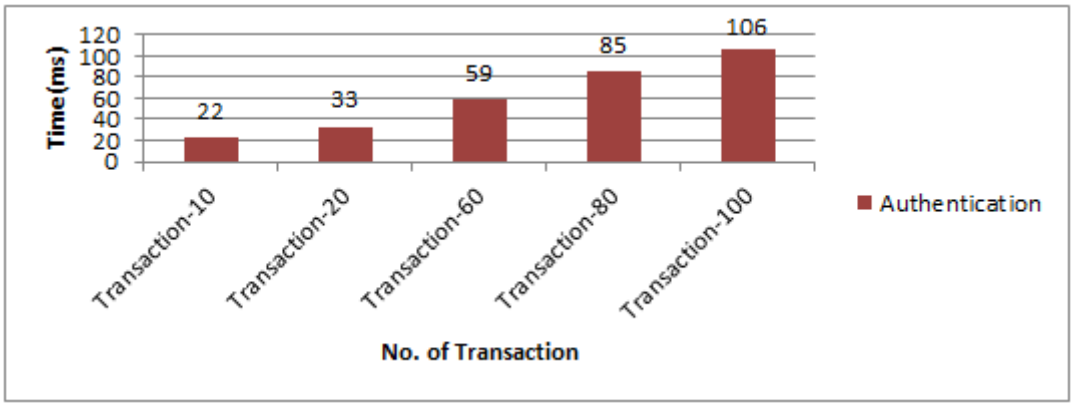

Figure 3: Time required for mining(Estimated)

V. CONCLUSION

The implementation of the software system prototype that applies the system's access control model to data stored in nontrusted environments is the main result of this work. Acceptable complexity, functionality, and implementation complexity have been chosen to implement the system algorithms. The ability to configure the access policy of the encrypted data without duplicating them to a large number of participants; the ability to establish dynamic access policies; access policy adjustment does not entail any additional intervention by other members of the system, eliminating the need for frequent updates to user keys; the integrity of information about the system.

REFERENCES

[1]. J. Yu, K. Wang, D. Zeng, C. Zhu, and S. Guo, "Privacy-preserving data aggregation computingin cyber-physical social systems," ACM Transactions on Cyber-Physical Systems, vol.3, no. 1, p. 8, 2019.

[2]. H. Ren, H. Li, Y. Dai, K. Yang, and X. Lin, \Querying in internet of things with privacy preserving: Challenges, solutions and opportunities," IEEE Network, vol. 32, no. 6, pp. 144{151, 2019.

[3]. J. Li, H. Ye,W.Wang,W. Lou, Y. T. Hou, J. Liu, and R. Lu, Efficient and secure outsourcing of differentially private data publication," in Proc. ESORICS, 2019, pp. 187 206.
[4]. Gong, Xinglin, Erwu Liu, and Rui Wang. Blockchain-Based IoT Application Using Smart Contracts: Case Study of M2M Autonomous Trading.2020 5th International Conference on Computer and Communication Systems (ICCCS). IEEE, 2020.
[5]. Xu, Jinliang, et alEdgence: A blockchain-enabled edge-computing platform for intelligent IoT-based dApps.& China Communications 17.4 (2020): 78-87.
[6]. Huang, Zheng, Zeyu Mi, and Zhichao Hua. & HCloud: A trusted JointCloud serverless platform for IoT systems with blockchain. & China Communications 17.9 (2020): 1-10.
[7]. Gheitanchi, Shahin. & Gamified service exchange platform on blockchain for IoT business agility& 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). IEEE,2020.
[8]. G. Xu, H. Li, Y. Dai, K. Yang, and X. Lin, \Enabling efficient and geometricrange query with access control over encrypted spatial data," IEEE Trans. Information Forensics and Security, vol. 14, no. 4, pp. 870{885, 2019.
[9]. K. Yang, K. Zhang, X. Jia, M. A. Hasan, and X. Shen, Privacy preserving attribute-keyword based data publish-subscribe service on cloud platforms," Information Sciences, vol. 387, pp. 116{ 131, 2017.
[10]. Choi, Jungyong, et al. "Random Seed Generation For IoT Key Generation and Key Management System Using Blockchain." 2020 International Conference on Information Networking (ICOIN). IEEE, 2020