International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 8, August 2020 ||

Blockchain-Based Public Integrity Verification for Cloud Storageagainst Procrastinating Auditors

Ankit Nipane[1], Akash Bathe[2], Rohit Yadav[3], Nandkumar Panchaware[4], Prof Sumit Dhotre [5]

UG Students, Indira College of Engineering and Management, Parandwadi, Maharashtra, India[1,2,3,4]

Asst. Professor, Indira College of Engineering and Management, Parandwadi, Maharashtra, India[5]

ABSTRACT: Deploying cloud storage services will offer significant benefits to data management for consumers. It also raises other security concerns, though, and one is data integrity. Public verification techniques can enable a user to employ a third-party auditor to verify data integrity on user'sbehalf, while existing public verification schemes are vulnerable to procrastinating auditors who may not conduct on-time verification.Additionally, many public verification schemes are built on public key infrastructure, and certificate management problems exist. In this paper we propose using blockchain technology;Attribute Based Encryption (ABE) is a cryptographic practice which offers data owner straight control concluded their data in public cloud storage. In the customary ABE structure consist of single expert to sustain attribute set which can carry a single-point bottleneck on equally security as well as performance. Currently we use multi authority verification protocol Role Base Access Control (RBAC) in cloud environment. RBAC is Threshold Multi-Authority Access Control System. In RBAC, TPA equally achieves the entire attribute set but no one takes full control of whichever precise attribute. TPA verifies the user's identity and provides the access control according the roles, we developing efficient multi authority access control system in public cloud storage which provide drastic security using blockchain technology. The system also able to eliminate various network attacks like DOS, SQL injection etc.

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

I.INTRODUCTION

The implementation of cloud computing systems has significant advantages in handling user data. This also creates other security concerns, however, and one of them is confidentiality of the data. Public verification techniques can enable a user to employ a third-party auditor to verify data integrity on their behalf, while existing public verification schemes are vulnerable to procrastinating auditors who may not conduct on-time verifications. In addition, most public authentication schemes are based on the Public Key Infrastructure (PKI), and thus suffer from certificate management issue.

- Decent data storage as well as large data collection needed for informationsystems
- Different problem of attack in centralized databasearchitecture.
- There is no automatic attack retrieval in the central dataarchitecture.
- The decentralized architecture provides automatic data recovery from variousattacks.

In the proposed research work to design and implement a public verification technique transaction data system where users can store all information in a single block chain in a distributed computing environment with any Trusted Third Party (TTP). The system also implemented data integrity, confidentiality and eliminated end-user.

II.LITERATURE SURVEY

Smart Contracts[1] Also referred to as crypto-contract, it is a computer 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 are stored on block chains and BC is an ideal technology to store those contracts. The smart-contract specifies where the transaction should be transferred / returned or where the transaction actually occurred when a transaction is considered.
A new approach to incorporate Block On IOT with [2] is currently being suggested by CSIRRO team. He incorporates smart-home technology in his initial effort to understand how IOT can be prevented. Block wheels are especially used to provide Smart-Devices Transactions access control system located on the Smart-Home. Introducing BC technology in IOT, this search again provides some additional security features, but every mainstream BC technology must have a concept that doesn't include the concept of comprehensive algorithms. Furthermore, in the case of IOT use this technology can not provide a general form of block-chain solution.

According to [3] framework, a multi-user system implementation for access control over data sets stored in awesome cloud environments is present. Cloud storage as with other insecure environments requires the ability to share information safely. The solution offers oversight of access to data stored in the cloud without an investment from the provider. Access Control Mechanism The main tool is the dynamic feature-based encryption scheme which has dynamic characteristics. Using decentralized badgers based on BlockChain; Our systems provide an irrevocable log for accessibility requests for all meaningful security incidents such as large financing, assignment of access policy, alteration or cancelation. We give a collection of cryptographic protocols that confidentthe hidden or secret key of cryptographic service. The sifter text hash code is only transmitted by laser blockchain. Our system was tested on prototype smart contracts and deployed on networks with Iterium Blockchain.

We offer a block chain and a MedRec-based approach according to [4] by allowing encryption and attribute-based authentication to allow secure sharing of healthcare data. By applying this approach: 1) The fragmented EHR fragment of all patients can be seen as a complete record and can be safely stored against tampering; 2) Patient EHR authenticity can be verified; 3) Flexible and fine-tuned access control can be provided and 4) a clear audit trail can be maintained.

Moving on from VipulGoyalet. Al[5] develops new cryptosystems for the proper sharing of encrypted data, which we call encryption based on key policy attributes (KPABE). In our cryptosystem, Cephet's text is labeled with a set of properties and controls that it connects to configurations for private key access which a user can decrypt. We view our product utility for sharing audit log information and for transmitting encryption. Our development supports private key providers who subscribe to classified identity based (HIBE) encryption.
Hao Wang et. al. [6] they offer a secure electronic health record (EHR) system based on special-based cryptocurrencies and blockchain technology. In our system, we use attribute-based encryption (ABE) and identity-based encryption (IBE) to encrypt medical data and to use identity-based signature (IBS) to apply digital signatures. In order to obtain various functions of ABI, IBE and IBS in crypto, they presented a new cryptographic primitive, which is called a joint feature-based / identity-based encryption and signature (C-AB / IB-ES). It simplifies system maintenance and does not require the installation of separate cryptographic system for various security requirements. In addition, they use blockchain techniques to ensure the integrity and inspection of medical data. Finally, offers a demonstration application for medical insurance business.
In [7] authors proposed an approach based on blockchain technology to represent the right to access a resource and to allow the transfer of such right among users. This paper proposes a new approach based on blockchain technology to publish the policies expressing the right to access a resource and to allow the distributed transfer of such right among users. Also the policies and the rights exchanges are publicly visible on the blockchain. Consequently any user can know at any time the policy paired with a resource and the subjects who currently have the rights to access the resource. The problem with this approach is that the standard policy language XACML is a verbose formalism and policies can be relatively big. So, in this approach the link to the policies and cryptographic hash of the policies are stored in the blockchain to make it tamper proof and policies are stored on cloud to avoid space occupation problem. Policy Create Transaction (PCT), Rights Transfer Transaction (RTT), Rights Update, Revoke are stored in blockchain.
According to Axin Wu et. al. [8] they successfully address the issues which are the search time in most searchable attribute-based encryption schemes increases with the number of attributes, which increases the burden on the server and reduces the

user experience and another problem of preventing the revoked users from decrypting the previous ciphertext by offering a clear policy feature-based data sharing plan with direct revocation of attributes and fast keyword search and hidden policy using AND gate access control in which When the ciphertext is uploaded, the access control structure does not need to be uploaded. In their scheme, the non-terminated user's private key is not required to be updated during the cancellation of direct revocation of features. In addition, a keyword search has been realized in their plan, and the search is stable with the increase in time features. Specifically, the policy is hidden in the plan, and therefore, the privacy of users is preserved. Their security and performance analysis show that their proposed plan can deal with security and efficiency concerns in cloud computing.

According to Sarmadullah Khan et. al. [9] embedded power transactions in blockchain are based on their defined characteristics through the signature of many manufacturers. These signatures have been verified and customers are satisfied with the features that do not open any information that meet those features. The public and private key manufacturers have been created for these customers and using this key ensures that the support process is authorized by customers. There is no central authority required in this perspective. To protest against collision attacks, the makers are given secret pseudo-functional work seeds. Comparative analysis shows the efficiency of the proposed approach to existing people.

According to RuiGuoet. al. [10] To guarantee the validity of the EHR surrounding the block channel, he has submitted a special-based signature scheme with multiple officials, in which the patient supports the message according to the specifications, but there is no evidence that he does not have any other information. In addition, there are many officers without generating a reliable individual or a central person in order to generate and deliver a public / private key, which avoids the escrow problem and adapt to the mode of data storage distributed in the block. By sharing the secrecy of the secret pseudo-festive festivals in the authorities, this protocol opposed the attack of N-1 affiliated with officials. Under the computational Diffie-Hellman concept, they also formally demonstrate that, in relation to the specialty-signatory's enforceability and complete privacy, this specialty-based signature scheme is safe in random decorative models. Comparison shows the efficiency and qualities among the proposed methods and methods in other studies.

III.PROJECTSCOPE

According to industry experts, Blockchain, a digital laser technology that can keep data records and ever-growing transaction lists secure, has the ability to potentially transform real estate. The way in which the real estate industry simplifies and accelerates data in areas such as revenue cycle management, interoperability of real estate data and supply chain verification, dramatically reducing blockchain back-office data input and maintenance costs, and data accuracy and security Has the power to improve.

IV. METHODOLOGY

- System must validate the previous block before commitblock.
- User can access the data over the internet24*7.
- If any block has changed by third party attacker or unauthorized user, it must show during transaction current blockchain isinvalid.
- It can recover the invalid blockchain using other data nodes, with the help of majority of trustiness.
- The node or user who wants to initiate a transaction would record and broadcasts the data to the network.
- The node or user who receives the data verifies the authenticity of the data received in thenetwork. Then the verified data is stored to a block.
- All nodes or users in the network validate the transaction by executing either the proof of work algorithm or the proof of stake algorithm to the block that needsvalidation.
- Consensus algorithm used by the network will store the data to the block that is addedto blockchain. And all nodes in the network admit the respectiveblock and extend the chain base on the block.

5.1 System Architecture:

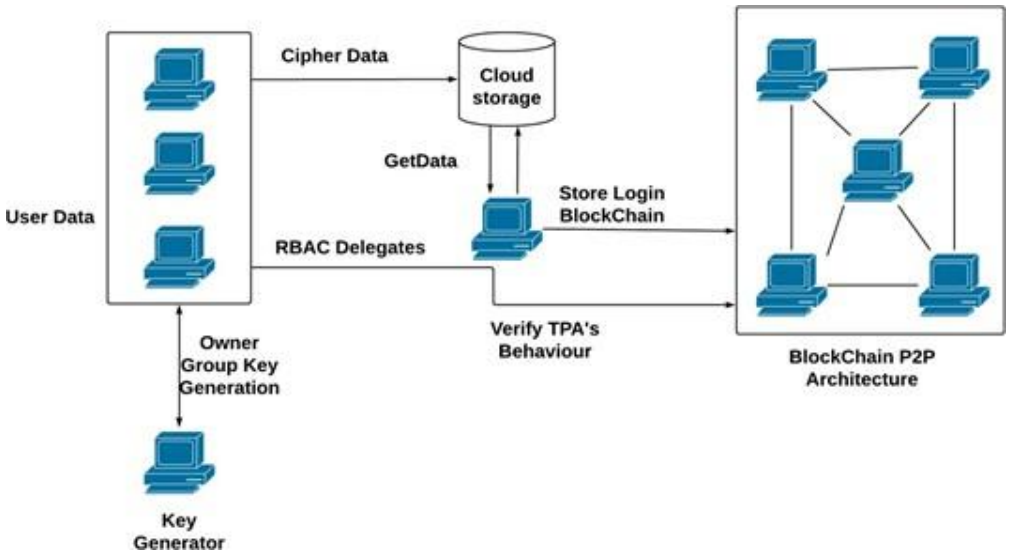

Figure 1 : Proposed Systemarchitecture

Algorithm Design

Algorithm 1: Hash Generation
Input: Genesis block, Previous hash, data d
Output: Generated hash H according to 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

Pseudocode: Protocol for Peer Verification
Input: User Transaction query, Current Node Chain CNode[chain], Other Remaining Nodes blockchain NodesChain[Nodeid] [chain]
Output: Recover if any chain is invalid else execute current query
Step 1: User generate the any transaction 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 NodeChain)
If (!equalsNodeChain[i] with (Cchain))
Flag 1
Else Continue Commit query
Step 5: If (Flag == 1)
Count = SimilarNodesBlockchain()
Step 6: Calculate the majority of server Recover invalid blockchain from specific node
Step 7: End If
End If

End For

Mining Pseudocode for valid hash creation
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 defines the first module in which user 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[])
Role base access control for each ith user has been defined using below formula

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

User revocation has done using below formula
U[i] ←Revoke(F) : DataOwner

V.RESULTS AND DISCUSSIONS

For results we here show the transactions recorded as Blocks to form blockchain as Transaction Hash of block 1 will be Previous Hash in block 2 and for block 1 Previous Hash will be 0 as it is first block which is also called as genesis block.

Lable	Values
ID	2
Transcation Hash	0x00000a327782b1af9ae034ab79cf4c69c6e814ac1045de67172fc89a9ffc9657
From Owner	0x1f76581a05a6dde25df7e53149c4cced333275ea
To User	0x9b7248e3245cb391227e23db747c0b6880d4fe61
File Name	Amazon S3.txt
Action	FileShare
Timestamp	Fri Jul 12 14:54:04 IST 2019
Time Duration	30#Day
Owner Cost	55
Transfer Cost	0.003
Nonce	2763823
Previous Hash	0x0000001df555d21de053af9abf80ab3097b7b5af65f02cb72183e69405a60cef

Lable	Values
ID	3
Transcation Hash	0x0000094f4913c8dea91e6d1568126e0850d4758cd3928c54ce090f15727b2eb9
From Owner	0x1f76581a05a6dde25df7e53149c4cced333275ea
To User	0x9b7248e3245cb391227e23db747c0b6880d4fe61
File Name	Test.txt
Action	FileRevoke
Time	Fri Jul 12 15:55:30 IST 2019
Time Duration	0
Owner Cost	0
Transfer Cost	0
Nonce	3658019
Previous Hash	0x00000a327782b1af9ae034ab79cf4c69c6e814ac1045de67172fc89a9ffc9657

Figure 2: Transactions recorded in blocks to form Blockchain

As shown in Figure 3 two blocks are shown in that Transaction Hash in block 2 is Previous Hash in block 3. In block transaction is recorded in which From Owner is sender address and To User is the receiver address, then File Name, Action performed which will be File Share or Revoke, Timestamp is time at which transaction is performed, Time Duration for what time period access to file is given and according to that Owner Cost, Transfer Cost paid to get access is recorded and for Revoke transaction Time Duration, Owner Cost, Transfer Cost value will be not be there, and Nonce of the transaction is also calculated. And in this work Proof of Authority will be used as in our System Authorities are present which will be there to grant or reject the request so we used Proof of Authority in our work.

For the system performance evaluation, calculate the matrices for accuracy. The system is executed on java 3-tier architecture framework with INTEL 2.4 GHz i3 processor and 4 GB RAM with distributed environment. The below figure 3 shows the time required for consensus algorithm to validate the blockchain in 4 nodes. X axis shows the size of blockchain and Y shows the time required in milliseconds with respective 4 nodes.

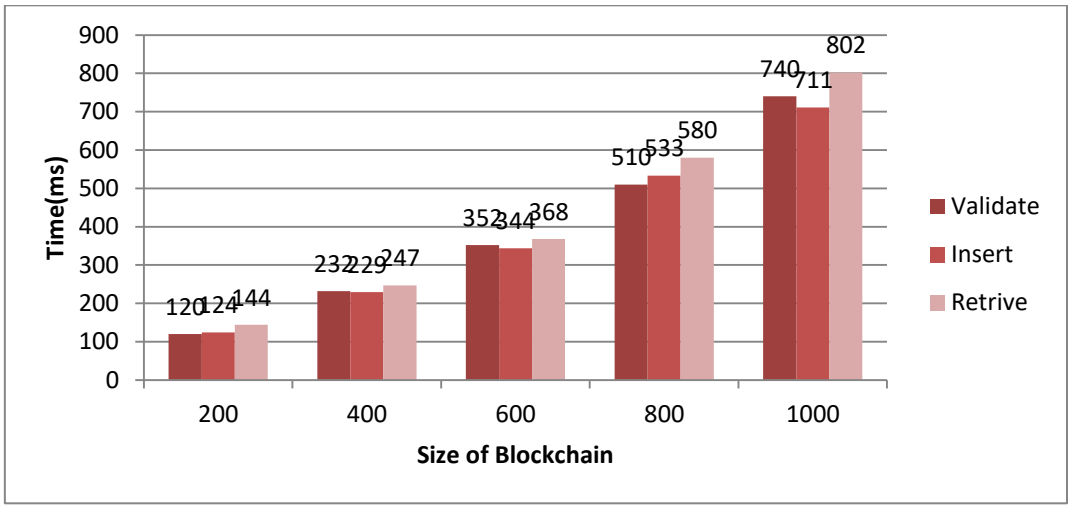

Figure 3: Time required (in milliseconds) for complete transaction with different records blockchain using 4 data nodes in P2P Network

In the second experiment we evaluate the proposed system with smart contract validation by consensus algorithm in different number of peer to peer nodes.

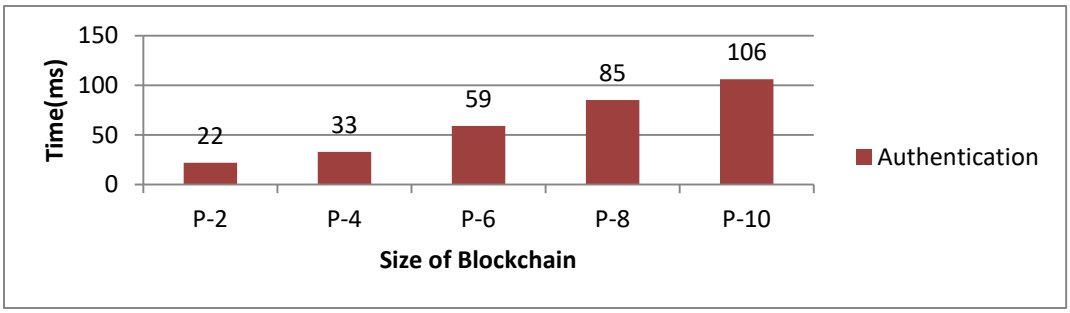

Figure 4: Time required for smart contract validation with different no. of P2P network in blockchain.

In the third experiment evaluate number of variation taken by algorithm from propose SHA value. Basically this experiment has done for to evaluate the propose hash string is valid or not according to given mining policy. In many times when system generates SHA code for given transactional data it's never fulfill the mining policy. To fulfill the propose mining policy according to given scenario mining to generate the multiple variation on given string. The below figure 5 shows numbers of time taken in milliseconds to generate the valid SHA string for specific transaction.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 8, August 2020 ||

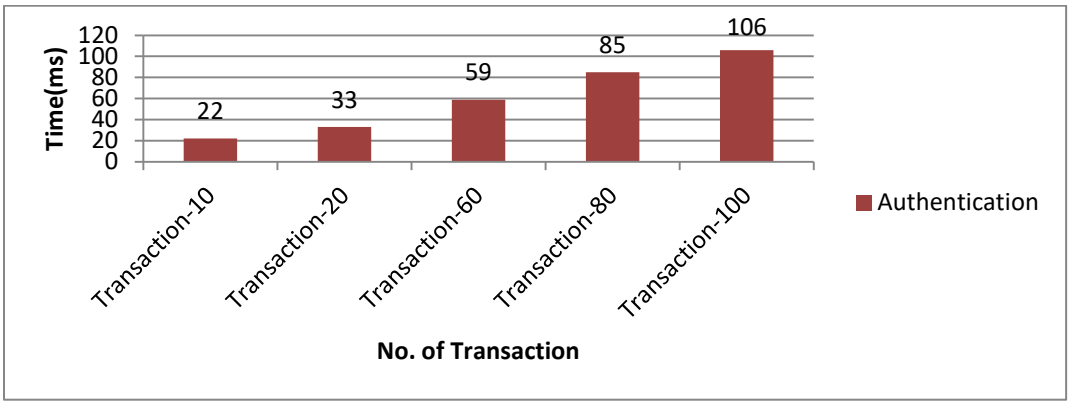

Figure 5: Time required for mining

VI.CONCLUSION

The main result of this work is the implementation of a software system prototype that implements the access control model of the system to data stored in untrusted environments. To implement the system algorithms have been selected acceptable complexity, functionality, and complexity of implementation. Key benefits of access control system are: the ability to customize the access policy for the encrypted data without duplicating them to a large number of participants; the ability to define dynamic access policies; access policy change does not require any additional action from other members of the system, which avoids the need for regular changes to user keys; the integrity of information about all transactions, including the granting and changing access, facts gain access to file, rejection of the fact and the inability to edit these data is guaranteed through the use of the blockchain and smart contracts.

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 outsourcingof differentially private data publication," in Proc. ESORICS, 2019, pp. 187–206.
[4] L. Zhong, Q. Wu, J. Xie, J. Li, and B. Qin, "A secure versatile light payment system basedon blockchain," Future Generation Computer Systems, vol. 93, pp. 327–337, 2019.
[5] G. Xu, H. Li, Y. Dai, K. Yang, and X. Lin, "Enabling efficient and geometric range querywith access control over encrypted spatial data," IEEE Trans. Information Forensics and Security,vol. 14, no. 4, pp. 870–885, 2019.
[6] Wang, Hao, and Yujiao Song. "Secure cloud-based EHR system using attribute-based cryptosystem and blockchain." Journal of medical systems 42.8 (2018): 152.
[7] Damiano Di Francesco Maesa, Paolo Mori, and Laura Ricci. "Blockchain Based Access Control." In International Federation for Information Processing 2017 by Springer International Publishing AG 2017.
[8] Wu, Axin, et al. "Hidden policy attribute-based data sharing with direct revocation and keyword search in cloud computing." Sensors 18.7 (2018): 2158.
[9] Khan S, Khan R. "Multiple authorities' attribute-based verification mechanism for Blockchain mircogrid transactions." Energies.2018 May; 11(5):1154.
[10] Guo, Rui, et al. "Secure attribute-based signature scheme with multiple authorities for Blockchain in electronic health records systems." IEEE Access 776.99 (2018): 1-12.