|| Volume 5 || Issue 9 || September 2020 || ISSN (Online) 2456-0774
INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH
AND ENGINEERING TRENDS

A SECURE BLOCKCHAIN BASE INDIAN JURISDICTION SYSTEMS

Shubham Patil[1], Kajal Wani[2], Karnali Rode[3], Harshada Pisal[4], Prof.S.C.Chaudhari[5]

Student, Department of Computer Engineering, Padmadhushan Vasat Dada Patil Institute of Technology Bavdhan Pune[1,2,3,4]

Assistant Professor, Department of Computer Engineering, Padmadhushan Vasat Dada Patil Institute of Technology Bavdhan Pune[5]

Abstract: The blockchain is a distributed network that records digital transactions on a publicly accessible ledger. This paper explores whether blockchain technology is a suitable platform for the preservation of digital signatures and public/private key pairs. Conventional infrastructures use digital certificates, issued by certification authorities, to declare the authentication of key pairs and digital signatures. This paper suggests that the block chain's hash functions offer a better strategy for signature preservation than digital certificates for Indian Jurisdiction System using blockchain and Artificial Intelligence (AI). Compared to digital certificates, hashing provides better privacy and security. It is a form of authentication that does not require trust in a third party authority, and the distributed nature of the blockchain network removes the problem of a single point of failure.

Keywords*: Smart Contract, RSA, DSA, Hashing, Mining, Consensus algorithm*

I INTRODUCTION

Basically block chain is the technique which provides decentralized approach data storage for different transactional systems. Basically it is introduced to achieve the highest data security during the data transactions and eliminate various network as well as data attack from malicious requests. Crypto currency is the base framework for block chain technology, Bit coin is the master currency introduced in crypto currency market. There are various crypto currencies which is already introduced different crypto currency platforms like ethereum, ripple, cordono etc. Which platform provides different kind of security aspects during the performance of transactional data. The smart contract is another concept which is introduced by prospective block chain transaction. Hash generation and mining strategy is too much important to create a runtime block. Different consensus algorithm also provides the proof of validation for different page in peer to peer network. Basically this system proposed decentralized approach which provides automatic data recovery in a distributed environment. The system also carries out Automatic load rebalancing and data validation protocol in entire execution.

The document certificate and privacy is a very essential to provide security to private information, various platform already exist to store such a kind of large data in a secure manner. Some centralized cloud storage provides data encryption strategies for achieve highest security for a documentation. In real time large document verification is very tedious process which requires much resources as well as time also. Where manual systems are has been followed by different organization since couple of years, for employee verification, student document verification as well as any other government document verification by particular agencies. Sometime industrial organizations and colleges should be verifying the students and employees documentation. This research basically eliminate such time consuming process introduce the cost of traditional existing systems.

II.LITERATURE SURVEY

Smart Contracts A1 [1] also called crypto-contract, it is a computer program used for transferring / controlling the property or digital currents in specific parties. It does not only determine the terms and conditions but may also implement that policy / agreement. These smart contracts are stored on block-chain and it is an ideal technology to

store these contracts due to the ambiguity and security. Whenever a transaction is considered, the smart-contract determines where the transaction should be transferred / returned or since the transaction actually happened.

Currently CSIRRO team has proposed a new approach to integrate Block on Internet of things (IOT) A1 [2]. In its initial endeavor, they used smart-home technology to understand how IOT can be blocked. Block chains are especially used to provide access control system for Smart-Devices Transactions located on Smart-Home. Introducing BC technology in IOT, this search again provides some additional security features; however, every mainstream BC technology must have a concept that

Does not include the concept of comprehensive algorithms. Moreover, this technology cannot provide a general form of block-chain solution in case of IOT usage.

According to Ilya Sukhodolski. The Al [3] system presents a prototype of multi-user system for access control over datasets stored in incredible cloud environments. Like other unreliable environments, cloud storage requires the ability to share information securely. Our approach provides access control over data stored in the cloud without the provider's investment. Access Control Mechanism The main tool is the dynamic feature-based encryption scheme, which has dynamic features. Using Block chain based decentralized badgers; our systems provide an irrevocable log for accessibility requests for all meaningful security incidents like large financing, access policy assignment, alteration or cancellation. We offer a set of cryptographic protocols that make the secret or secret key of cryptographic operation confidential. The hash code of the sifter text is only transmitted by the block on laser. Our system has been tested on prototype smart contracts and tested on Ethereum Blockchain platforms.

According to Huehuangenet. Al [4] they offer a block chain and a MedRec-based approach by enabling encryption and attribute based authentication to enable secure sharing of healthcare data. By applying this approach: The fragmented electronic health record fragment of all patients can be seen as a complete record and can be safely stored against tampering; the authenticity of patients' electronic health record can be verified; Flexible and finer access control can be provided and it is possible to maintain a cleared audit trail.

According to VipulGoyalet. Al [5] develops new cryptosystems to share encrypted data properly, which we call key-policy attribute-based encryption (KPABE). In our cryptosystem, cipher labeled with a set of properties and controls that it connects to private key access configurations that a user can decrypt the encryption. We display the utility of our product to share audit log information and broadcast encryption. Our creation supports private key providers, which subscribe to categorized hierarchical identification-based encryption (HIBE).

According to Ruuguet Al [6] To guarantee the validity of the electronic health record 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 prepares 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 Billine Diffie-Hellman concept, we 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.

Hao Wang et Mate Al [7] They offer a secure electronic health record (EHR) system based on special-based Cryptococcus and block chain technology. This system carried out the Auto Bitcoin (BTC) Builder as well as Id-Based encryption to encrypt medical data and to use Institute of blockchain to apply digital signatures. . In order to obtain various functions of Application binary interface, Id-Based Interface and Institute of blockchain in crypto, we present a new cryptographic original; it is called a joint identity-based encryption as well as signature. It simplifies system maintenance and don't require the installation of separate cryptographic system for various security requirements. In addition, we use

blockchain techniques to ensure the integrity and inspection of medical data. Finally, we offer a demonstration application for medical insurance business.

According to Sarmadullah Khanet. Al [8] 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 Yan Michalevskyet. Al [9] system introduces the first practical decentralized Attribute base encryption (ABE) scheme with proof of policyhiding. Our creation is based on the basic encryption of decentralized internal product, which is an encryption strategy launched in this paper. This Auto BTC Builder scheme supports results, disputes, and threshold policies, which protect the access policies of those parties that are not authorized to decrypt content. In addition, we handle the receiver's privacy issue.

Using our plan with Vector Commitment, we hide a complete set of attributes presented by the individual with the recipient; just disclose the feature that regulates the authority. Finally, we propose random-polynomial encoding that immerses this scheme in the presence of corrupt officials. Al [10] they successfully address these issues by offering a cleared policy feature-based data sharing plan with direct cancellation and keyword search. In the proposed scheme, the non-terminated users' 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 our plan, and the search is stable with the increase in time features. Specifically, the policy is hidden in our plan, and therefore, the privacy of users is preserved. Our security and performance analysis show that the proposed plan can deal with security and efficiency concerns in cloud computing.

III.PROPOSED SYSTEM DESIGN

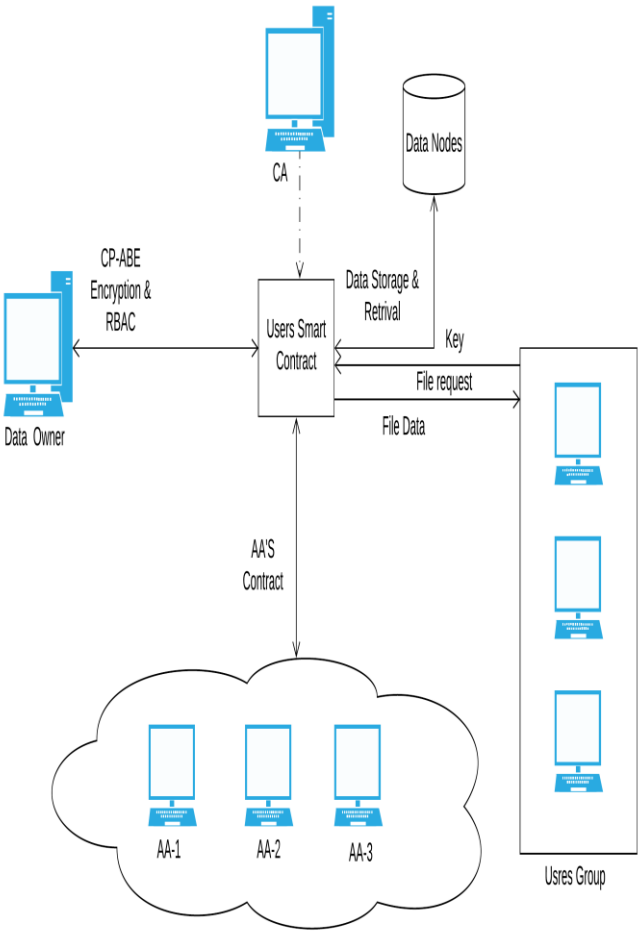

Figure 1 : Proposed system architecture

Admin: The administrator generate the transactional information and add it into the master

block, admin also can view the whole transactional information.

Data Owner (DO): A DO is an authorized user of the system, who owns data to be uploaded and shared. A DO defines an access policy for accessing the data, so that only the desired users with matching attribute sets are granted permission to decrypt and get access to the plaintext data.

Cloud Service Provider (CSP): CSP is a semi-trusted environment responsible for data storage. Attribute Authority (AA): An AA is responsible for granting a set of users and a set of attribute which we will call as domain to users and key distribution to them. Each AA may register users in its domain and hand out the

attribute keys of its domain to users. Besides creating users, attribute assignment is the main purpose of an AA. It may assign attributes to users outside its own domain, i.e. a user created by AA may receive attributes given out by AA. We assume that each AA is semi-trusted in our system, i.e. it might be curious about the value of a plaintext in the system, but has no intention of tampering with it.

Data User: Data user is an authorized user who intends to access encrypted data. The user registers with an Attribute Authority and obtains one or more attribute sets. If the attribute sets satisfies an access policy associated with a cipher text, the end user will be able to get access to cipher data and by entering the valid key it can decrypt cipher text and get access to the plaintext.

Distributed Blockchain: The Blockchain is the distributed ledger used to represent the current state of delegated access rights in the system. Permissions to interact with the Blockchain are handled by the Root Authority and the Attribute Authorities.

IV ALGORITHM DESIGN

Algorithm 1 : Hash Generation

Input : Genesis block, Previous hash, data d,

Output : Generated hash H according to given data

Step 1 : Input data as d

Step 2 : Apply SHA 256 from SHA family

Step 3 : CurrentHash= SHA256(d)

Step 4 : Return CurrentHash

Algorithm 2 : Mining Algorithm 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

V RESULTS AND DISCUSSION

For the system performance evaluation, calculate the matrices for accuracy. The below figure 2 shows the time required for consensus algorithm to validate the blockchain in 4 nodes, with different number of tractions.

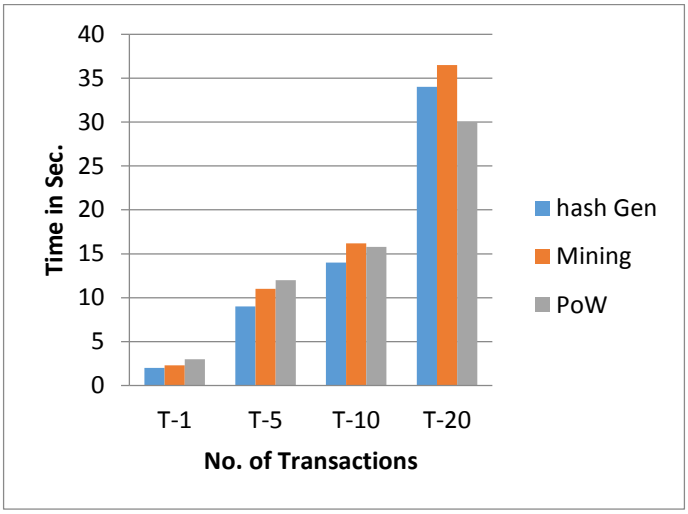

Figure 2 : Time base experiment of proposed system with various number of transactions

VI CONCLUSION AND FUTURE WORK

In this work we applied blockchain to keep record of file share or revoke transaction between users. But in cloud many applications, data files, services and resources are shared among user's group having multiple users instead of single user and in such cases it's difficult to know which user made what changes and this needs to be tracked to know if one of the user from group is acting as malicious user. So, The functionality of this prototype can be expanded further to ensure the security of data or shared resources hosted in the cloud among shared user's groups who are using shared data or resources and working on them and this prototype can be applied to track the changes made by each and every individual user in the user's group on shared application, data, services and resources. Further work can be done to study how to effectively integrate an access control system in blockchain technology.

REFERENCES

[1] "Smart Contracts," http://searchcompliance .techtarget.com/definition/ smart- contract, 2017, [Online; accessed 4-Dec- 2017]

[2] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchainin internet of things: Challenges and Solutions,"arXiv:1608.05187 [cs], 2016. [Online].Available:http://arxiv.org/abs/1608.05187%5Cn http://www.arxiv.org/pdf/1608.05187.pd

[3] Sukhodolskiy, Ilya, and Sergey Zapechnikov. "A blockchain-based access control system for cloud storage." Young Researchers in Electrical and Electronic Engineering (EIConRus), 2018 IEEE Conference of Russian.IEEE, 2018.

[4] Yang, Huihui, and Bian Yang. "A Block chain-based Approach to the Secure Sharing of Healthcare Data."Proceedings of the Norwegian Information Security Conference. 2017.

[5] Goyal, Vipul, et al. "Attribute-based encryption for fine- grained access control of encrypted data." Proceedings of the 13th ACM conference on Computer and communications security. Acm, 2006.

[6] Guo, Rui, et al. "Secure attribute-based signature scheme with multiple authorities for Block chain in electronic health records systems." IEEE Access 776.99 (2018): 1-12.

[7] Wang, Hao, and Yujiao Song. "Secure cloud-based EHRsystem using attribute-based cryptosystem and blockchain.Journal of medical systems 42.8 (2018): 152.

[8] Khan S, Khan R. Multiple authority's attribute-based verification mechanism for Block chain mircogrid transactions. Energies. 2018 May; 11(5):1154.

[9] Michalevsky Y, Joye M. Decentralized Policy-Hiding Attribute-Based Encryption with Receiver Privacy.

[10] Wu, Axin, et al. "Hidden policy attribute-based data sharing with direct revocation and keyword search in cloud computing." Sensors 18.7 (2018): 2158.