IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2320-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 6, June 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.512

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

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 10, Issue 6, June 2021 ||

| DOI:10.15680/IJIRSET.2021.1006431|

Blockchain Based Data Sharing Framework

Miss. Shete Kajal Bharat[1], Prof. Monika Rokade[2]

PG Student, Sharadchandra Pawar College of Engineering, Junnar Pune, India[1]

Assistant Professor, Sharadchandra Pawar College of Engineering, Junnar Pune, India [2]

ABSTRACT*:* Data is and will continue to be an important component of any modern application that we envision. Machine learning and Artificial Intelligence's potential will only increase as we move further into the future. Data sharing is fraught with issues such as data format and meaning, legal requirements, privacy, data security, and concerns about unintended repercussions of data sharing, to name a few. It's not an easy subject to tackle because it involves not just technical issues, but also social, financial, ethical, and regulatory ones. To retain consumer and community trust, it is necessary to design sharing frameworks that handle technical obstacles, include regulatory frameworks, and anticipate and address concerns about fairness and justice of outcomes. This study presents a paradigm for data sharing that includes several ecosystems, with blockchain technology serving as the system's backbone. Because blockchain addresses the major challenges of trust, data correctness, and reliability, it also offers a revolutionary data sharing option.

KEYWORDS: Blockchain, Public Key, Proof of Work, Distributed Ledger Technology

I. INTRODUCTION

This is a document. Medical/Healthcare, Banking, and IoT are data-intensive domains where vast amounts of data (we'll be talking about structure data throughout this study) are created, disseminated, stored, and retrieved on a daily basis. Data from numerous source systems was collected, retrieved, converted, and fed into Datawarehouse throughout the last decade (DWH). Data reconciliation is then performed between the source system and the DWH.
However, once this data is developed and it needs to be shared across the internet, we face a number of issues, as data exchanged with other parties will be different and not identical. This occurs because data synchronization is usually not immediate and occurs at the end of the day. There is a cost associated with this reconciliation process. Additionally, there is always the possibility of data tampering, and in the case of financial transactions, double spending is always a concern.

II. LITRATURE SURVEY

Smart Contracts [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 BC 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 BlockOn IOT with [2]. In its initial endeavor, he uses smart-home technology to understand how IOT can be blocked. Blockwheels 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 can not 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 feature-based encryption scheme, which has dynamic features. Using BlockChain based decentralized badgers; Our systems provide an irrevocable log for accessibility requests for all meaningful security incidents like large financing, access policy assignment, alteration

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

|| Volume 10, Issue 6, June 2021 ||

| DOI:10.15680/IJIRSET.2021.1006431|

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 siftertext is only transmitted by the blockcon laser. Our system has been tested on prototype smart contracts and tested on IteriumBlockchan platforms.

According to Huehuangenet. Al [4]they offer a blockchain and a MedRec-based approach by enabling encryption and attribute based authentication to enable 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) The authenticity of patients' EHR can be verified;3) Flexible and finer access control can be provided and 4) it is possible to maintain a clearedaudit 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, Cefhettext is 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 identification-based encryption (HIBE).

Hao Wang et Mate Al [6] They offer a secure electronic health record (EHR) system based on special-based crypt ococcurs and blockchan 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, we present a new cryptographic primitive, it 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, we use blockconne techniques to ensure the integrity and inspection of medical data. Finally, we offer a demonstration application for medical insurance business. According to Yan Michalevskyet. Al [7] system introduces the first practical decentralized ABE scheme with proof of policy-hiding. Our creation is based on the basic encryption of decentralized internal product, which is an encryption strategy launched in this paper. This ABB 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 [8]they successfully address these issues by offering a clearepolicy 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.

According to SarmadullahKhanet. 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 Ruuguet. 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 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 BillineDiffie-Hellman concept, we also formally demonstrate that, in relation to the specialty-

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

|| Volume 10, Issue 6, June 2021 ||

| DOI:10.15680/IJIRSET.2021.1006431|

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. RELATE WORK.

Data Sharing on DLT

After reviewing a number of studies (mentioned in the references section) and the different basic components and functionalities of Distributed Ledger Technology (DLT) systems, which are characterised by a secure, decentralised, and distributed network, I came to this conclusion. This study presents a paradigm for data sharing that includes several ecosystems, with blockchain technology serving as the system's backbone. Blockchain addresses the major challenges of trust, data accuracy, and reliability, as well as providing a revolutionary data sharing method.

Data Sharing Challenges

In terms of security, energy consumption, and processing overhead, traditional data sharing methods are often prohibitively expensive for current applications. Most apps today choose to run on the cloud, owing to the convenience of high availability and cost savings. However, in an increasingly cloud-based environment, utilising traditional cryptographic primitives and access control methods to handle security and privacy concerns has limitations. Furthermore, many state-of-the-art frameworks are excessively centralised and, as a result, are not well-suited for current applications data sharing due to scaling issues, security, lack of consensus mechanisms, single point of failure, and user privacy and permission. As a result, these contemporary Applications necessitate consensus-based data sharing, tamper-proof data storage, and distributed security and privacy protection. Following the literature review, we have included the work that has been done on data sharing frameworks in several domains.

- Provides an useable blockchain-based architecture for a collection of researchers' data, including access accountability, complete and up-to-date information, and a verifiable record of the provenance, which includes all data accesses, sharing, and usages.
- On the Hyperledger Fabric blockchain technology, describe the design and execution of a smart contract for consent-driven and double-blind data sharing.
- Look into the possibility of using Blockchain technology to protect cloud-based healthcare data. Describe the practical difficulties of such a notion as well as the need for additional investigation.
- Provides an overview of DLT and considers its potential for overcoming current KYC process difficulties and lowering KYC expenses. Demonstrated how design science research was used to solve the issue. Also, include recommendations for how the solution might be implemented.
- Propose a decentralised storage using blockchain on a common cloud-based platform that is applicable to all types of Meta Products and assures trust and privacy while exchanging user data across different manufacturers' applications.

Blockchain

In general, blockchain is a technology that allows for the creation of an open and distributed online database consisting of a list of data structures (also known as blocks) that are linked to one another (i.e. a block points to the following one, hence the name blockchain). These blocks are dispersed across many infrastructure nodes and are not stored centrally. Each block has a timestamp for when it was created, a hash for the previous block, and transaction data. [6]

Blockchain has been proposed as a data structure for creating a public distributed digital transaction ledger that is shared among a dispersed network of computers rather than relying on a single provider. Blockchain is analogous to cloud computing in that all nodes are connected via the internet and all of them perform the same computing activity for which they are rewarded. [9]

To summarise, the blockchain offers features such as immutable distributed ledgers and synchronised ledgers across networks, consensus mechanisms for parties/participants in networks to agree unanimously, uniqueness of data that cannot be copied or replicated, data that is time stamped with fully connected chronological blocks with audit trail, data that is digitally sealed with cryptography, and data that is digitally sealed with cryptography.

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

|| Volume 10, Issue 6, June 2021 ||

| DOI:10.15680/IJIRSET.2021.1006431|

Monika Rokade and Yogesh Patil [11] proposed a system deep learning classification using nomaly detection from network dataset. The Recurrent Neural Network (RNN) has classification algorithm has used for detection and classifying the abnormal activities. The major benefit of system it can works on structured as well as unstructured imbalance dataset.

The MLIDS A Machine Learning Approach for Intrusion Detection for Real Time Network Dataset has proposed by Monika Rokade and Dr. Yogesh Patil in [12]. The numerous soft computing and machine learning classification algorithms have been used for detection the malicious activity from network dataset. The system depicts around 95% accuracy ok KDDCUP and NSLKDD dataset.

Monika D. Rokade and Yogesh Kumar Sharma [13] proposed a system to identification of Malicious Activity for Network Packet using Deep Learning. 6 standard dataset has sued for detection of malicious attacks with minimum three machine learning algorithms.

Sunil S. Khatal and Yogesh kumar Sharma [14] proposed a system Health Care Patient Monitoring using IoT and Machine Learning for detection of heart and chronic diseases of human body. The IoT environment has used for collection of real data while machine learning technique has used for classification those data, as it normal or abnormal.

Data Hiding In Audio-Video Using Anti Forensics Technique For Authentication has proposed by Sunil S.Khatal and Yogesh kumar Sharma [15]. This is a secure data hiding approach for hide the text data into video as well as image. Once sender hide data into specific objects while receivers does same operation for authentication. The major benefit of this system can eliminate zero day attacks in untrusted environments.

Sunil S.Khatal and Yogesh Kumar Sharma [16] proposed a system to analyzing the role of Heart Disease Prediction System using IoT and Machine Learning. This is the analytical based system to detection and prediction of heart disease from IoT dataset. This system can able to detect the disease and predict accordingly.

IV. PROPOSED METHODOLOGY

On the basis of block chain technology, we offer a data sharing architecture. There are several parties engaged here, including the issuer and the verifier. These are the users who would contribute, update, or retrieve data from the system. They could be individuals or organisations. The user's intention is to upload the most recent documents or artefacts to a blockchain-based system.

The data to be updated is referred to as records or documents, and it is fresh or existing data that is saved on cloud storage. The user might request this information for the purpose of studying and validating it. The system accepts this information and generates the document's hash. This hash, along with the document, is saved on the cloud. This document's details, as well as its hash, are changed in the block, which is only sent to approved peers. The authorization update module in the system can be used to update this authorization. The data is entered in the chain and connected to the preceding block once the block has been checked and accepted by the application.

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

|| Volume 10, Issue 6, June 2021 ||

| DOI:10.15680/IJIRSET.2021.1006431|

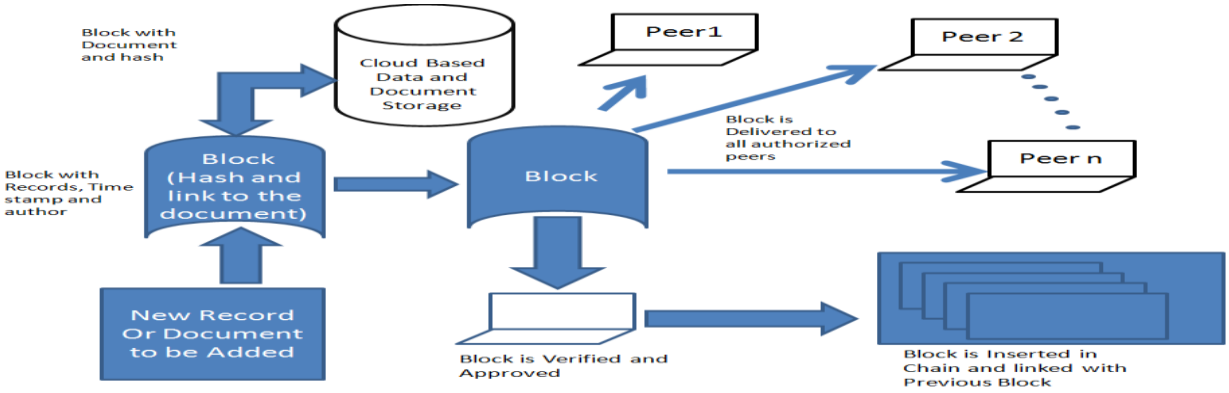

Figure 1 : Proposed System Architecture

Depending on the use case, different responsibilities would be assigned to the system. For example, in a VISA application for a specific nation, one role might be for the country's embassy, another for the visa applicant, and so on, depending on the usecase. The data format is next, and we recommend using structured data that can be used with any related database.

It's possible that the programme will be portable. All system access rights will be governed through the application, which will be based on roles, which can be allocated to users.

Most notably, blockchain aids in the management of security's CI (Confidentiality and Integrity) element. Redundancy can be employed at the application architecture level for availability, however this is not covered in this work.

The next stages are to implement this framework and investigate its metrics in terms of additional optimization and scalability.

V. RESULTS AND DISCUSSION

Basically, this experiment has done to evaluate the proposed hash string is valid or not according to a given mining policy. In many times when the system generates Hash values for given transaction data it never fulfills the mining policy. To fulfill the proposed mining policy according to given scenario mining to generate the multiple variations on a given string. The below figure 2 shows numbers of time taken in milliseconds to generate the valid Hash string for a specific transaction.

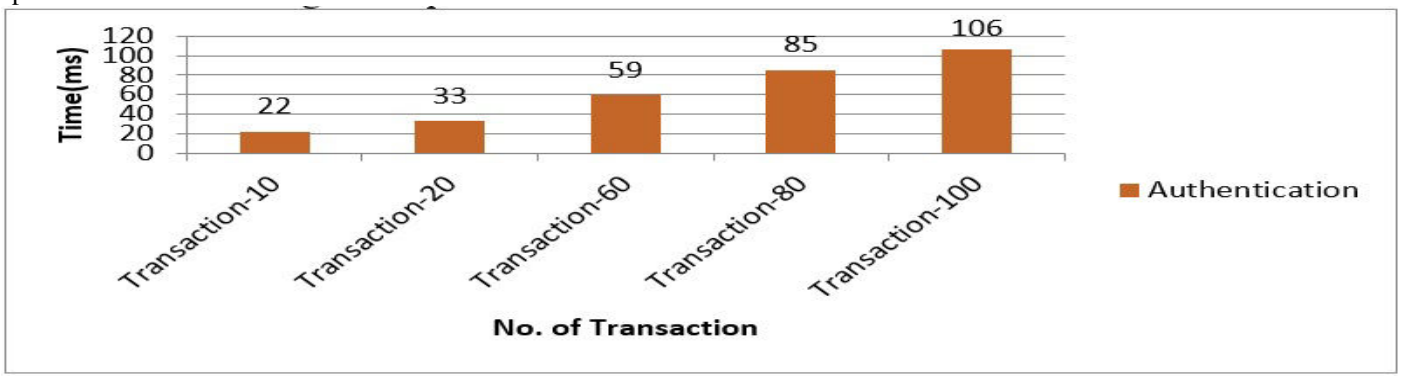

Figure 2: Data Sharing Transaction Time required for block chain

VI. CONCLUSION

We suggested a block chain-based data sharing framework in this research, which is very flexible and may be applied to any domain where sensitive data sharing between numerous parties is an issue. Data is shared in a secure manner, and data privacy is preserved, thanks to this framework. The communication and authentication procedures should be examined further, and this research should be expanded. We will continue to construct the system based on this framework in the future and perform a study to obtain better optimization and empirical data that can be used for further research and studies.

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

|| Volume 10, Issue 6, June 2021 ||

| DOI:10.15680/IJIRSET.2021.1006431|

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%5Cnhttp://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 Blockchain-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] 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] Michalevsky Y, Joye M. Decentralized Policy-Hiding Attribute-Based Encryption with Receiver Privacy.

[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.

[11] Monika D.Rokade ,Dr.Yogesh kumar Sharma,"Deep and machine learning approaches for anomaly-based intrusion detection of imbalanced network traffic."IOSR Journal of Engineering (IOSR JEN),ISSN (e): 2250-3021, ISSN (p): 2278-8719

[12] Monika D.Rokade ,Dr.Yogesh kumar Sharma"MLIDS: A Machine Learning Approach for Intrusion Detection for Real Time Network Dataset", 2021 International Conference on Emerging Smart Computing and Informatics (ESCI), IEEE

[13]Monika D.Rokade, Dr. Yogesh Kumar Sharma. (2020). Identification of Malicious Activity for Network Packet using Deep Learning. *International Journal of Advanced Science and Technology*, *29*(9s), 2324 - 2331.

[14] Sunil S.Khatal ,Dr.Yogesh kumar Sharma, "Health Care Patient Monitoring using IoT and Machine Learning.", **IOSR Journal of Engineering (IOSR JEN),** ISSN (e): 2250-3021, ISSN (p): 2278-8719

[15]Sunil S.Khatal ,Dr.Yogesh kumar Sharma, "Data Hiding In Audio-Video Using Anti Forensics Technique ForAuthentication ", IJSRDV4I50349, Volume : 4, Issue : 5

[16]Sunil S.Khatal Dr. Yogesh Kumar Sharma. (2020). Analyzing the role of Heart Disease Prediction System using IoT and Machine Learning. *International Journal of Advanced Science and Technology*, *29*(9s), 2340 - 2346.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.512

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details