e-ISSN:2582 - 7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 4, Issue 7, July 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 5.928

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 5.928|

| Volume 4, Issue 7, July 2021 |

|DOI:10.15680/IJMRSET.2021.0407020|

Secure Data Sharing Based on Blockchain Technology

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: This article discusses how to protect data on the 5G network in an effective and secure manner. It also considers a strategy based on blockchain technology to address privacy concerns in 5G networks. It is also demonstrated how the usage of blockchain in data sharing builds mutual trust between content providers and user communities.

KEYWORDS: Blockchain; Smart Contract; Solidity; Truffle; Security; Cloud

I. INTRODUCTION

With recent improvements and successful installations around the world, 5G networks represent the future phase of telecommunication. Ultra low latency, increased mobile broadband, and huge machine-to-machine communication are the three main characteristics of 5G networks. The most serious problem with 5G networks is security. The approaches utilised in 2G, 3G, and 4G are insufficient for 5G since they are incapable of dealing with data tampering, as well as security and privacy beyond data integrity protection. There are a slew of new 5G technologies on the horizon, like SDN and D2D communications, which will exacerbate security and privacy concerns. 5G wireless networks will be decentralised, which is important for security and privacy considerations. Decentralization, immutability, and openness are key aspects of 5G that help us solve security challenges.

As a result of the security and privacy concerns in 5G networks, data sharing has become a big worry. Because present techniques are incapable of dealing with the concerns in 5G, we must go a step farther to meet the challenges. The introduction of blockchain technology could be a watershed moment for 5G and beyond networks. The blockchain is a database that is decentralised, unchangeable, and transparent. Blockchain offers a solution to the problems that 5G networks face. Unlike a centralised authority, blockchain is based on a peer-to-peer network design in which all participants in the ledger govern the information. Because of its decentralisation and immutability, blockchain fosters trust and security.
We strive to combine blockchain and data sharing to tackle the challenges in data sharing since blockchain can solve security and privacy issues.

Blockchain
The cryptocurrency Bitcoin transactions are the most well-known aspect of Blockchain. The technology is based on the concept of decentralisation. Rather than storing the data in a single area, it is replicated and spread across the ledger's participants. Every time a new transaction occurs or a new block is added, it is reflected on all of the computers. The fundamental benefit of blockchain is that it does not have a single point of failure. The blockchain is open to everyone, yet it is not under the jurisdiction of any network body. Private and public chains are the two types of chains.

Data block:
A blockchain is a series of blocks that form a linear structure. The genesis block is the initial block in the chain. Each block contains a certain amount of transactions and is hashed to the preceding block. The preceding block's hash can be found in the current block. Each block has a block header, which includes a collection of transactions, a block hash for validation, a nonce value, and a time stamp.

Distributed ledger:
This is a networked database that is duplicated and shared among the users. The block information is accessible to everyone on the network.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 5.928|

| Volume 4, Issue 7, July 2021 |

|DOI:10.15680/IJMRSET.2021.0407020|

Consensus algorithm

Because there is no centralised party to monitor transactions, we must assess the block trustworthiness in order to manage transaction rules and protect data from attacks. Consensus algorithms are used to meet these requirements. The Proof of Work algorithm is a security-enforcing consensus mechanism run by miners in Bitcoin.

Smart Contract

On a blockchain network, a smart contract is a software that runs. Any changes to the contract must be made after it has been deployed. It is intelligent due to its self-executing nature. Consider transferring monies; these funds are automatically transferred over the network. This will be recorded as a transaction and stored on the immutable blockchain.

II. LITERATURE SURVEY

A.G. Said et. al. [1] proposed a system authentication System Using BlockchainIn short, the program's purpose is: a valid registry with electronic certificates, i.e. an electronic credential is generated at the applicant's request. At the same time, that student's record is preserved by using hash values in blockchain blocks. The customer is also presented with a particular QR code or serial number, in accordance with the E-certificate. And instead the demand unit (e.g. company to which the applicant has applied for a job) must verify the authenticity of the electronic file using the QR code or the relevant serial number based on the reported details in the blockchain

Jiin-Chiou Cheng et. al. [2] proposed a system Blockchain and smart contract for digital certificate, Then build an electronic paper document file that follows those related details into the database and thus decides the hash value of the electronic file. Finally, the hash value within the ring is stored in the chain process. To be affixed to the paper credential, the software will produce a related QR code and question string data. It will involve the demand device for paper certificate validity verification via mobile phone scanning or web site inquiries. Since of the blockchain's unchangeable property, the network not only increases the credibility of unique paper-based certificates but also the authentication risks of various types of certificates electronically types of certificates

Marco Baldi et. al. [3] Certificate Validation The program solves the problem through Shared Ledgers and Blockchains by introducing a mechanism in which several CAs share a transparent, shared and stable database where CRLs are received. To this end, we find the concept of blockchain-based shared ledgers implemented for use of cryptocurrencies, which is becoming a common solution for many web applications of high protection and reliability requirements.

Oliver et. al. [4] illustrates Using blockchain as a Government degree tracking and assessment tool: a business analysis based on two financial factors comparing the service price as the main players between the customer and the employer. Students need a low-cost and easy-to-check evidence of competence, and employers also need swift and accurate documentation of their degree before recruiting. All models are built for growing regional markets and shares to discover ways of extending this sector in the European Union.

Because of the The arbitrary existence of hashing is never a guarantee of producing an appropriate object. Thus, Bitcoin mining is a competitive enterprise where miners are effectively hashed and admitted into the blockchain by awarding new Bitcoin for each block[5]. Miners, a collaborative consumer network, verify and check transactions and set up specialized computation equipment called "hashes." They vote with their CPU strength, demonstrating their approval of legitimate blocks by working to expand them and by declining to operate on invalid blocks[6]. These record strings (hashes) that keep track of any Bitcoin transaction and are repeated on any device in the Bitcoin network.

Blockchain is a decentralized LEDGER used for safe trading of digital currencies, deals and transactions[7], and peer-to-peer network management. All nodes adopt the same internode contact protocol, and verify new objects. If the data is validated in every block no block will change it. To modify individual block data, all corresponding block data will be modified, resulting in network cooperation and denial of the transaction by all nodes. The The power used to "farm" the cryptocurrency is a key aspect since its costs are rising. According to the Bitcoin statistics site Digiconomist, citizens worldwide use more than 30 terawatts-hours of electricity are mining the crypto-currency. This is greater than, at least, the human energy use 159 countries like Hungary, Oman, Ireland, and Lebanon [8].

Bitcoin mining is a Creation of new Bitcoin process by verifying Bitcoin Network transactions. That transaction is stored in a shared ledger, and all of the machines involved in the Bitcoin network check and manage the ledger. This "net" of transactions is known as the ledger, and. transaction is basically a timestamp for the database that may involve

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 5.928|

| Volume 4, Issue 7, July 2021 |

|DOI:10.15680/IJMRSET.2021.0407020|

data [9]. Narayanan et al. [10] Describe a block string as a data structure composed of a related array of hash pointers. Every entity in the list is a block containing some previous block data and hash. This renders it a tamper-evident file, implying the data can only be applied to the list and the prior data can not be changed without detection.

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.

III. PROPOSED METHODOLOGY

When it came to the original implementation, I looked into how phone calls function in 4G networks, which is analogous to data sharing. The study of 4G voice conversations aids in the understanding of network design. A blockchain-based architecture can be created to address the problem statement using system architectural expertise. Figure 1 depicts the architecture on which we will build the previously stated solution. Following the above offered solution locally and testing it is one technique to fixing the problem. Using Truffle and Remix, we may deploy contracts for testing purposes.Always test your code before deploying it. We must ensure that content providers, user communities, and cloud storage are all connected via a smart contract in which a miner is invoked and a block is added (only when content provider uploads a data to cloud). Hashing is blockchain's most valuable asset. When the hash of data in the block and the hash of data in the cloud match, the data integrity is confirmed. Keccak256 and Sha256 are the two most common hashing algorithms. The most crucial distinction to make is that Sha256 and Keccak256 are not the same thing. For the same data, we obtain various hashes.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 5.928|

| Volume 4, Issue 7, July 2021 |

|DOI:10.15680/IJMRSET.2021.0407020|

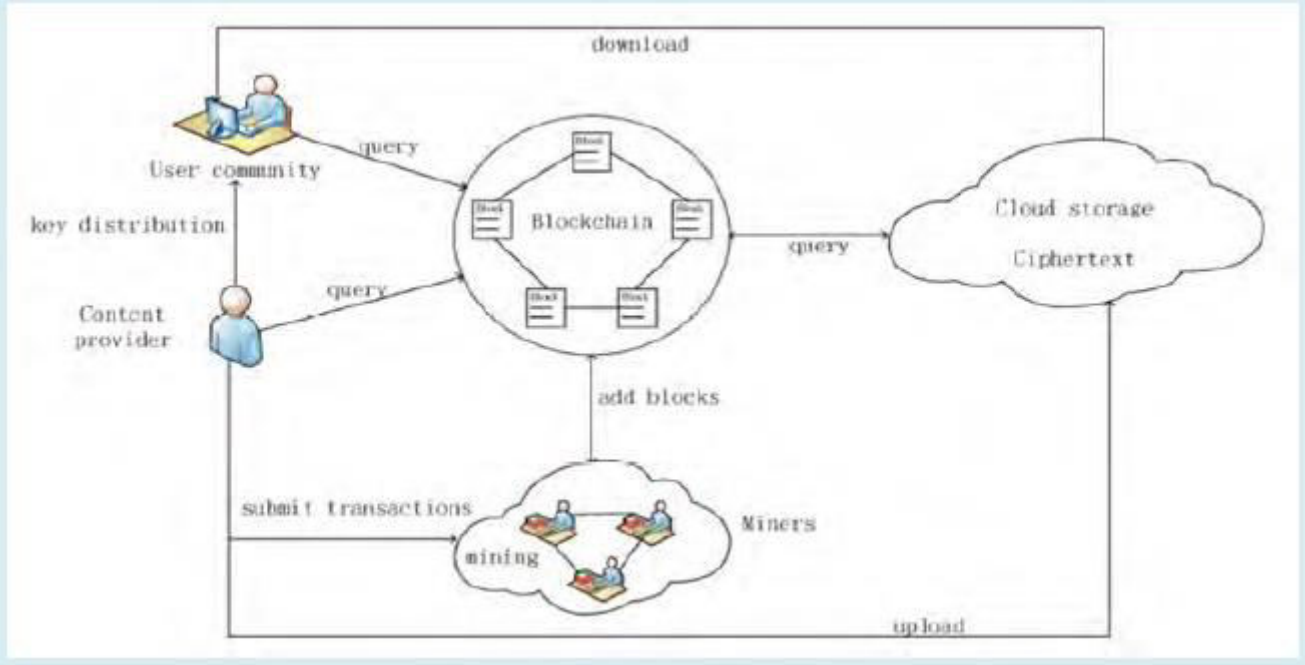

Figure 1: System Architecture

IV. SYSTEM ANALYSIS

Software Requirements

1. System interfaces: Windows Operating System

2. User interfaces: User interface using Jsp and Servlet

3. Hardware interfaces

Processor :- Intel R-Core i3 2.7 or above

Memory :- 4GB or above

Hard Disk :- 500 GB

4. Software interfaces:

Front End: Jdk 1.7.0, Eclipse

IE 7.0/above

Back-End: Mysql 5.1.

V. RESULTS AND DISCUSSION

The proposed solution above proved effective in maintaining data integrity. For the sake of simplicity, one content source and two users were evaluated, and the aforesaid solution for data integrity issues was successfully implemented. As previously stated, the user can only download data that has not been altered. To demonstrate this locally, we change data in cloud storage and check whether or not the data is being downloaded. Instead of an empty string, the user downloads a message 'ERROR' to see if the updated data was downloaded.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 5.928|

| Volume 4, Issue 7, July 2021 |

|DOI:10.15680/IJMRSET.2021.0407020|

Attack to Cloud Storage: If a malevolent user wishes to access data stored in cloud storage, he must first decode the data, which is encrypted using the content provider's private key. He needs the decryption key to access it, and without it, the data is useless to the attacker**.**

VI. CONCLUSION

The majority of security and privacy issues are addressed with blockchain. We addressed our key challenges of data sharing in 5G networks using blockchain and smart contracts. Blockchain has the potential to significantly contribute to security, privacy, and data integrity in next generation networks. In comparison to other existing technologies, blockchain offers a lot more to offer networks. Blockchain, like new technology, has the potential to exceed existing security and privacy methods.

REFERENCES

[1] A.G. Said, R.P. Ashtaputre, B. Bisht, S.S. Bandal, P.N. Dhamale, “E-Certificate Authentication System Using Blockchain,” International Journal of Computer Sciences and Engineering, Vol.7, Issue.4, pp.191-195, 2019.
[2] Cheng JC, Lee NY, Chi C, Chen YH. Blockchain and smart contract for digital certificate. In2018 IEEE international conference on applied system invention (ICASI) 2018 Apr 13 (pp. 1046-1051). IEEE.
[3] Baldi M, Chiaraluce F, Frontoni E, Gottardi G, Sciarroni D, Spalazzi L. Certificate Validation Through Public Ledgers and Blockchains. InITASEC 2017 (pp. 156-165).
[4] Oliver M, Moreno J, Prieto G, Benítez D. Using blockchain as a tool for tracking and verification of official degrees: business model.
[5] George F. Hurlburt and Irena Bojanova, "Bitcoin: Benefit or Curse?," in IEEE, 2014
[6] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, White Paper.
[7] Nirmala Singh and Sachchidanand Singh, "Blockchain: Future of financial and cyber security," in IEEE, Noida, 2016.
[8] Henrique Rocha ,Marcus Denker and Stephane Ducasse Santiago Bragagnolo, "SmartInspect: solidity smart contract inspector," in IEEE, Itly, p. 2018.
[9] GWYN D'MELLO. (2017,Dec.) https://www.indiatimes.com/technology/news. [Online].
https://www.indiatimes.com/technology/news/bitcoin-miners-are-using-more-electricity-than-irelandother-159-countries-no-kidding-335114.html
[10] Narayanan A., Bonneau J., Felten E., Miller A. & Goldfeder S. (2016) Bitcoin andCryptocurrency Technologies: A Comprehensive Introduction. Princeton: Princeton University Press
[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: 5.928

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

9710 583 466 9710 583 466 ijmrset@gmail.com

www.ijmrset.com