# SECURE CLOUD STORAGE USING BLOCKCHAIN FOR DECENTRALIZED SYSTEM WITH MERKLE TREE ALGORITHM

**1 Dr.Srinivas Dava, 2 Dr.Srinivas Konda, 3 Dr. Kavitha Rani Balmuri,**
**4 Viswaprakash Babu**
1 Associate professor, Department of CSE, Jyothishmathi institute of technology and science, Karimnagar, Telangana, India
2 Professor & Head, Department of CSE (Data Science), CMR Technical Campus, Hyderabad, India
3 Professor & Head, Department of Information Technology, CMR Technical Campus, Hyderabad, India
4 Associate professor, Department of EEE, Jyothishmathi Institute of Technology And Science, Karimnagar, Telangana, India
Email:srinivasdava84@gmail.com, Phdknr@gmail.com, phdknr1@gmail.com, vishwaprakash0078@gmail.com

## *ABSTRACT*

*In today's world, the simplest way to share data is through the internet. Cloud computing is a technology provided by the internet, which is dependent on large storage providers. These storage companies function as untrustworthy third parties, managing massive amounts of data saved in the cloud. This data may contain sensitive information that belongs to multiple individuals or organizations. Such types of models may involve security issues like privacy and integrity. Blockchain Technologies has gained widespread attention, with a surge of interest in applications varying from information storage to cyber security, IoT, healthcare, and financial services. Blockchain applications were used to carry safe and comfortable healthcare data, and there was a lot of interest in them. Additionally, blockchain is converting traditional medical care practices into a more dependable way of efficient diagnostics and treatments over safe and secure data sharing. In this paper, developed the decentralized system architecture with Merkle Tree structure, and preserving this health monitoring statistics in the cloud parallel processing in distributed environment.*

***Keywords:*** *Blockchain, Blockchain healthcare systems, Cloud Computing, decentralized system, Merkle Tree.*

## 1 INTRODUCTION

Several organizations are now dealing with the issue of keeping massive amounts of data. To resolve this problem, corporations have chosen cloud computing as a means of storing data. Cloud-based services have grown in popularity as a result in recent years. These services enable remote storing of user data in the cloud [1]. Businesses do not need to retain in-house storage since services are accessible across numerous platforms at any time and from any place. Notwithstanding the advantages indicated, there are a number of issues with cloud storage [2]. They preserve the security and reliability of data. Cloud storage may include sensitive information. But, copyright difficulties enter the image here. Anyone more than the owner may access the data since we are posting it to the open environment [3].

While storing information on the cloud, encryption is the foremost important factor to consider. Yet, loud services provider does not guarantee a high degree of security. The system presented in this paper [4] will help to overcome all the issues mentioned with the help of Blockchain-based Secure Data Storage and Access System. In this paper [5], Blockchain enhances the security of the data stored on the cloud by maintaining logs of operations performed by the user.

## 2 RELATED WORKS

It is possible for integrated personal health records (PHR) to have inadequate security, which might result in a single point of failure [6]. Combining Blockchain & IPFS, we suggest an infrastructure that attempts to deliver speedier rescue and continuous availability of PHR. The findings reveal that an ideal node is picked in each phase between all the possible nearby nodes [7]. The InterPlanetary File System (IPFS) is an unique decentralized architecture of storage that aims to offer decentralized cloud storage by expanding on the foundational ideas of P2P networking and resource addressing [8].

IPFS is also known as a distributed file system. Since IPFS is used by more than 230 thousand peers on a weekly basis and processes tens of millions of requests on a daily basis, it is a fascinating large-scale operational network to examine [9]. Blockchain is developing as a promising tool for handling confidential data in digitized healthcare system [10]. It is crucial to the healthcare, medical research, and insurance industries. IoT devices benefit from a high degree of security thanks to the consensus procedures employed in blockchain technology to choose a new block.

Data from the IoT is one of the most valuable assets that can be used into business models to facilitate the provision of a variety of dazzling and pervasive services [11]. The Internet of Things has the benefit of being vulnerable to hackers and other malevolent users. In spite of the fact that smart cities are supposed to increase production and efficiency, inhabitants and authorities still run the risk of putting themselves in danger when they ignore cyber security [12]. To enable the safe administration and analysis of the vast data from the smart city, traditional blockchain techniques were used.

The data stored at each healthcare facility is maintained in silos, and due to technical and physical restrictions, these silos prevent the data from being readily shared with other institutions [13]. To secure the security of IIoT data, blockchain technology may be deployed. The proof size for confirming the data's integrity and accuracy is huge in the classic blockchain system since it stores data using Merkle trees [14]. In the IoT, the information of users is often gathered through a variety of different sorts of smart gadgets [15]. Since the received user data is stored in the cloud, there is a risk of data leakage. A procedure known as the verification of retrievability scheme will be carried out on a regular basis by both the user and the cloud provider in order to ensure the confidentiality and integrity of the user's personal information [16].

Blockchain technology is here to remain and has considered the next revolution, much like the Internet. Some real-world use examples of blockchain technology [17]. These have been efforts made to create digital currency, but none of them have been successful owing to the difficulties associated with maintaining trust and security. The data access control mechanism in cloud data sharing systems provides an effective means of ensuring the security of the data. Intruders and malevolent cloud servers make it more difficult to manage data access [18].

The vast majority of conventional methods do not take into account the challenges involved in managing user access to cloud-based data storage & sharing. Some of the most successful methods for providing security data access control for confidential data that is stored in the cloud is ciphertext policy attribute-based encryption [19]. Merkle Hash-Trees are used as Authenticated Data Structures in this cutting-edge Decentralized Digital Currency System (DDCS). A distributed, peer-to-peer architecture without a ledger is used by DDCS [20]. The planned currency is called E-Money. E-Money is designed to take the place of traditional forms of payment and comes equipped with security protocols on par with those of crypto-currencies.

## 3 PROPOSED METHODOLOGY

A blockchain-powered security mechanism for protecting sensitive patient healthcare data. In a fog computing environment, this study proposes a solution for health care data that allows users to store all information in a single blockchain without using any Trusted Authentication Services (TAS). The system also ensured data integrity and confidentiality, as well as eliminating inconsistencies for end users.

Decentralized data storage and information systems both demand large amounts of data storage. The many vulnerabilities that centralized database designs face when it comes to attacks. With central data architectures, there is no provision for the automated recovery of attacks. The decentralized design allows for the automated recovery of data after a variety of assaults. After doing an investigation of this system, we designed a decentralized system architecture with a Merkle Tree structure as shown in fig 1. This architecture, together with fog computing, enables parallel processing in a distributed environment.

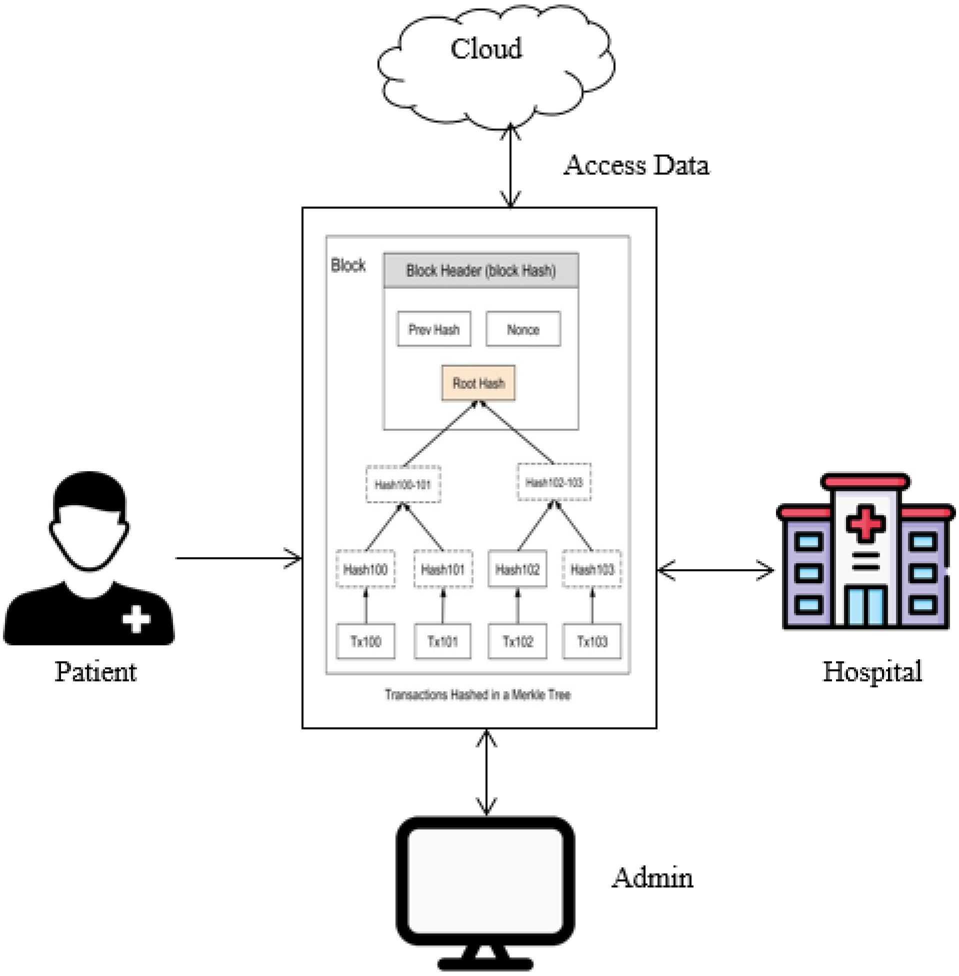


Figure 1: Architecture Diagram of Proposed System

**Algorithm**

*Step 1: Upload patient details.*  
*Step 2: Validate admin*  
*Step 3: If the data is valid, then upload in cloud*  
*Step 4: Create block for every transactions with Merkle tree hashing function.*  
*Step 5: If the date request by patient is valid chain, then show original data and access by using hashing key.*  
*Step 6: Create timestamp with Blockchain to access data in particular time.*

The demand for innovation is constant in the realm of Healthcare data. The method in which patient health records are maintained and protected today does not demonstrate the technical improvement that has occurred in this field over the previous decade, and hospitals continue to employ data management systems that are decades old for patient data. This is in part because of the stringent restrictions that surround the privacy and security of medical data. These regulations have prevented the adoption of the most recent technology, which would have made medical data management more open and helpful for both patients and physicians.

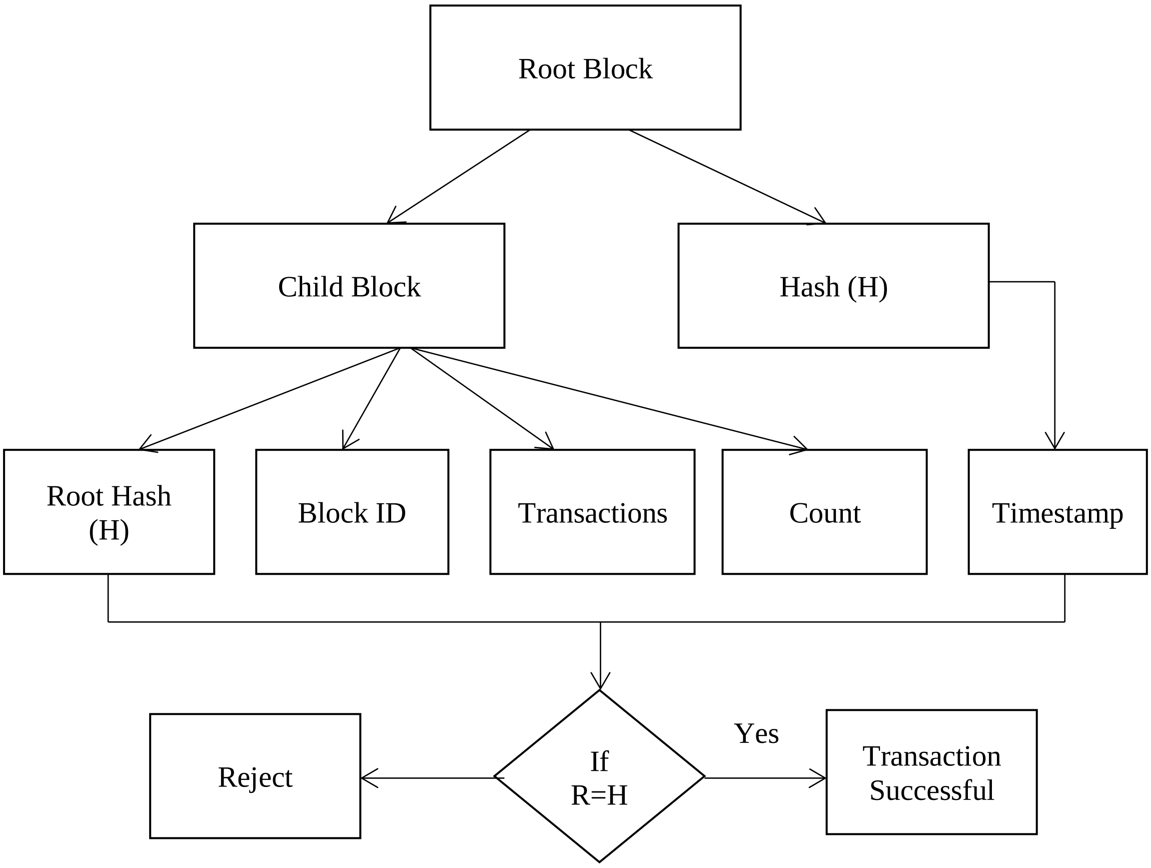


Figure 2: Blockchain Process using Merkle Tree and Timestamp

This demonstrates a blockchain-based framework for managing medical data/access as shown in fig 2. The app depicts the system from the perspectives of four stakeholders.

i. The results of admin are the administrator of a group of hospitals and hold the highest access level in the hierarchy. In their dashboard, they may add a new group (hospital) to the conglomerates and assign/de-assign hospital administrators.

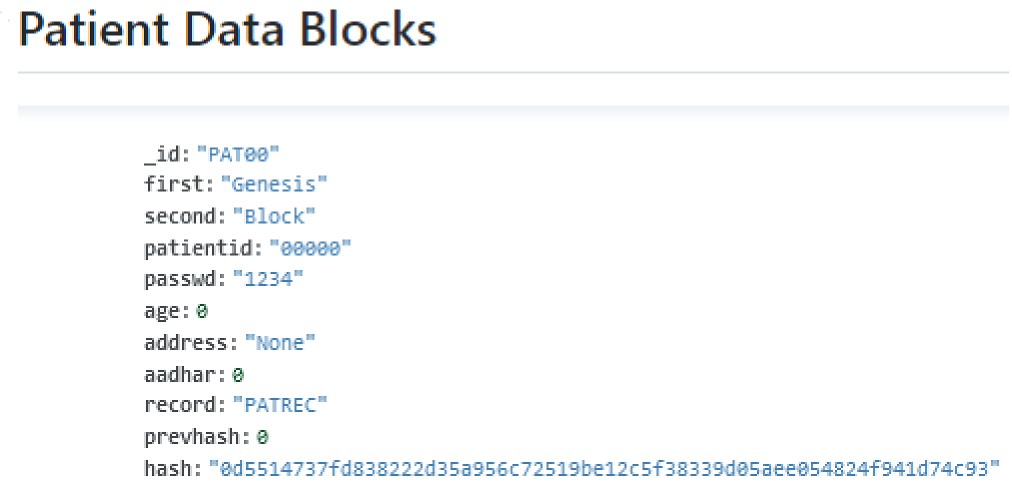
ii. The organizational (hospital) administrator is in charge of a specific hospital that is a member of the conglomerate/solution. They may add new people with the roles of doctor or patient, as well as delete members.

iii. The doctor is an organizational user having the proper role who may post records for their patients as well as download/view papers for their patient to whom they have been authorized access.

iv. The patient is an organizational user with the proper position who may contribute files on their own, examine them, check document access records, and control access to their docs through their dashboard.

## 4 Experimental Results

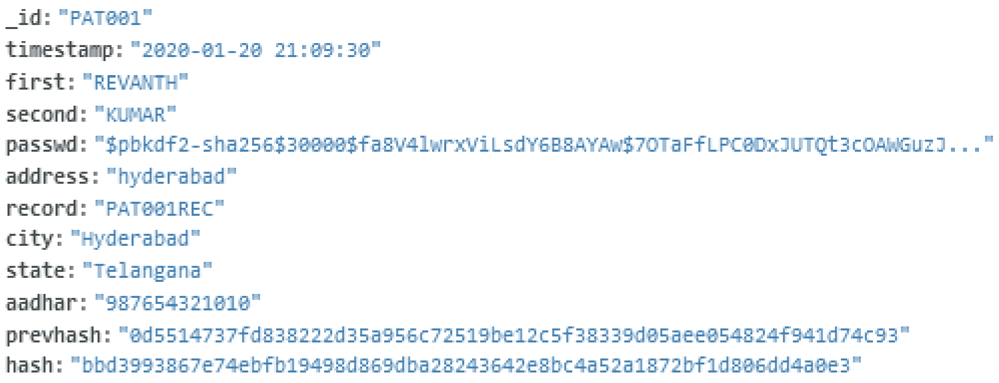
Utilizing the hashes of the document on the blockchain as opposed to the file blocks is one technique to improve the effectiveness of file storage/retrieval. It also gives auditable responsibility for precisely what material has been allowed by whomever for exchange and transmission through the file transferring guard.



Patient Data Blocks

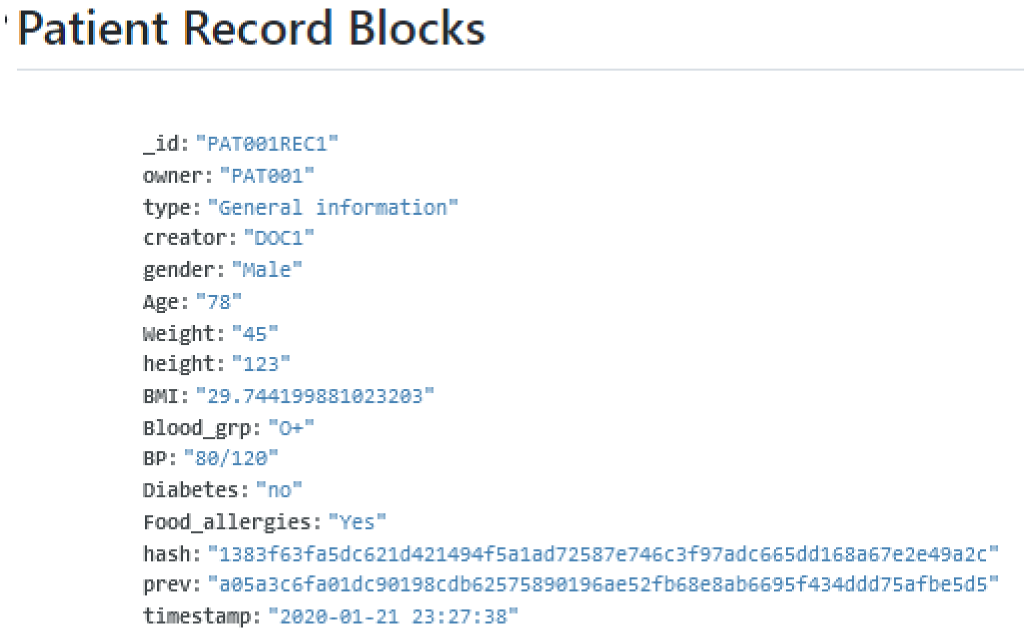
```
_id: "PAT00"
first: "Genesis"
second: "Block"
patientid: "00000"
passwd: "1234"
age: 0
address: "None"
aadhar: 0
record: "PATREC"
prevhash: 0
hash: "0d5514737fd838222d35a956c72519be12c5f38339d05aee054824f941d74c93"
```

Figure 3: Patient 1 Data Blocks



```
_id: "PAT001"
timestamp: "2020-01-20 21:09:30"
first: "REVANTH"
second: "KUMAR"
passwd: "$pbkdf2-sha256$30000$fa8V4lwrxViLsdY6B8AYAw$7OTaFfLPC0DxJUTQt3cOAWGuzJ..."
address: "hyderabad"
record: "PAT001REC"
city: "Hyderabad"
state: "Telangana"
aadhar: "987654321010"
prevhash: "0d5514737fd838222d35a956c72519be12c5f38339d05aee054824f941d74c93"
hash: "bbd3993867e74ebfb19498d869dba28243642e8bc4a52a1872bf1d806dd4a0e3"
```

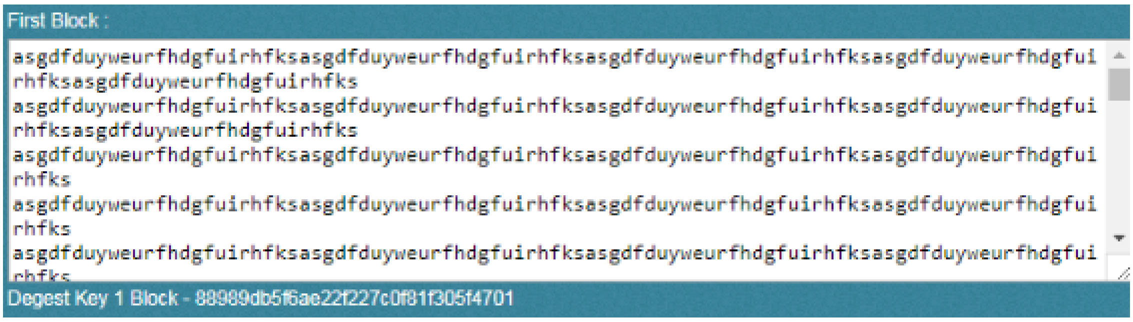
Figure 4: Patient 2 Data Blocks



Patient Record Blocks

```
_id: "PAT001REC1"
owner: "PAT001"
type: "General information"
creator: "DOC1"
gender: "Male"
Age: "78"
Weight: "45"
height: "123"
BMI: "29.744199881023203"
Blood_grp: "O+"
BP: "80/120"
Diabetes: "no"
Food_allergies: "Yes"
hash: "1383f63fa5dc621d421494f5a1ad72587e746c3f97adc665dd168a67e2e49a2c"
prev: "a05a3c6fa01dc90198cdb62575890196ae52fb68e8ab6695f434ddd75afbe5d5"
timestamp: "2020-01-21 23:27:38"
```

Figure 5: Patient Record Blocks

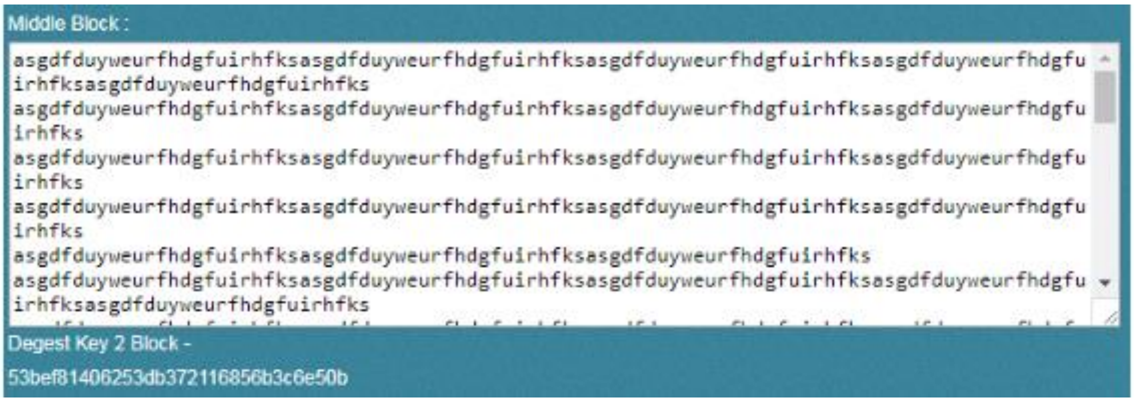


First Block :

```
asgdfduyweurfhdgfuirhfksasgdfduyweurfhdgfuirhfksasgdfduyweurfhdgfuirhfksasgdfduyweurfhdgfui
rhfksasgdfduyweurfhdgfuirhfks
asgdfduyweurfhdgfuirhfksasgdfduyweurfhdgfuirhfksasgdfduyweurfhdgfuirhfksasgdfduyweurfhdgfui
rhfksasgdfduyweurfhdgfuirhfks
asgdfduyweurfhdgfuirhfksasgdfduyweurfhdgfuirhfksasgdfduyweurfhdgfuirhfksasgdfduyweurfhdgfui
rhfks
asgdfduyweurfhdgfuirhfksasgdfduyweurfhdgfuirhfksasgdfduyweurfhdgfuirhfksasgdfduyweurfhdgfui
rhfks
asgdfduyweurfhdgfuirhfksasgdfduyweurfhdgfuirhfksasgdfduyweurfhdgfuirhfksasgdfduyweurfhdgfui
rhfks
```

Degest Key 1 Block - 88989db5f6ae22f227c0f81f305f4701

Figure 6: First Block of Transaction with Encryption Key



Middle Block :

```
asgdfduyweurfhdgfuirhfksasgdfduyweurfhdgfuirhfksasgdfduyweurfhdgfuirhfksasgdfduyweurfhdgfu
irhfksasgdfduyweurfhdgfuirhfks
asgdfduyweurfhdgfuirhfksasgdfduyweurfhdgfuirhfksasgdfduyweurfhdgfuirhfksasgdfduyweurfhdgfu
irhfks
asgdfduyweurfhdgfuirhfksasgdfduyweurfhdgfuirhfksasgdfduyweurfhdgfuirhfksasgdfduyweurfhdgfu
irhfks
asgdfduyweurfhdgfuirhfksasgdfduyweurfhdgfuirhfksasgdfduyweurfhdgfuirhfksasgdfduyweurfhdgfu
irhfks
asgdfduyweurfhdgfuirhfksasgdfduyweurfhdgfuirhfksasgdfduyweurfhdgfuirhfks
asgdfduyweurfhdgfuirhfksasgdfduyweurfhdgfuirhfksasgdfduyweurfhdgfuirhfksasgdfduyweurfhdgfu
irhfksasgdfduyweurfhdgfuirhfks
```

Degest Key 2 Block -
53bef81406253db372116856b3c6e50b

Figure 7: Middle Block of Transaction with Encryption Key

Continuously upgrading the ledger for each file transfer creates an irreversible record of the file's complete life cycle. The system incorporates a WebApp based interface for the concerned parties involved in the transaction to communicate in an effective manner thereby providing a base for decentralized approach with Merkle Tree system as given in fig 3-7.

## 5 CONCLUSIONS

The proposed system secures the data which is stored in untrusted environments. The implementation of blockchain with cloud will be very efficient to solve various problems in cloud based data storage like data privacy, data breaches, data leakage, data loss, system vulnerabilities etc. Blockchain technologies has the potential to tackle a wide range of issues afflicting the healthcare business today. Just providing the facts is insufficient. The suggested method, which employs personal Blockchain technology, may play an essential role in making data immutable, safe, and shareable inside a decentralized network. The blocks in this study are defined as high-level 3-scenarios, and their regulations are critical for implementing this new technology in the health-care system. Ultimately, the total efficiency of imperceptibility and durability values on each distributed ledger block is evaluated. Every concept includes some information as well as the reasoning behind the technological approach. It is anticipated that this report will spark more research and development to benefit both patients and the whole health-care system.

**References:**

1. Escobar, C. C., Roy, S., Kreidl, O. P., Dutta, A., & Bölöni, L. (2022). Toward a Green Blockchain: Engineering Merkle Tree and Proof of Work for Energy Optimization. *IEEE Transactions on Network and Service Management*, *19*(4), 3847-3857.
2. Peng, Z., Xu, J., Hu, H., Chen, L., & Kong, H. (2022). BlockShare: A Blockchain empowered system for privacy-preserving verifiable data sharing. *Bull. IEEE Comput. Soc. Tech. Comm. Data Eng*, *1*, 14-24.
3. Gong, J., & Navimipour, N. J. (2022). An in-depth and systematic literature review on the blockchain-based approaches for cloud computing. *Cluster Computing*, *25*(1), 383-400.
4. Miao, Y., Huang, Q., Xiao, M., & Susilo, W. (2022). Blockchain assisted multi-copy provable data possession with faults localization in multi-cloud storage. *IEEE Transactions on Information Forensics and Security*, *17*, 3663-3676.
5. Alvi, S. T., Uddin, M. N., Islam, L., & Ahamed, S. (2022). DVTChain: A blockchain-based decentralized mechanism to ensure the security of digital voting system voting system. *Journal of King Saud University-Computer and Information Sciences*, *34*(9), 6855-6871.
6. Kumar, P., Suresh, A., Anbarasu, V., Anandaraj, S. P., & Udayakumar, S. (2022). A decentralized secured grid integration system using APEBC technique with multi access AI framework. *Sustainable Computing: Informatics and Systems*, *35*, 100777.
7. Chen, L., Fu, Q., Mu, Y., Zeng, L., Rezaeibagha, F., & Hwang, M. S. (2022). Blockchain-based random auditor committee for integrity verification. *Future Generation Computer Systems*, *131*, 183-193.
8. Yao, Q., & Zhang, H. (2022). Improving Agricultural Product Traceability Using Blockchain. *Sensors*, *22*(9), 3388.
9. Itnal, S., Kannan, K. S., Suma, K. G., & Neelakandan, S. (2022, May). A secured healthcare medical system using blockchain technology. In *ICCCE 2021: Proceedings of the 4th International Conference on Communications and Cyber Physical Engineering* (pp. 169-176). Singapore: Springer Nature Singapore.
10. Qu, J. (2022). Blockchain in medical informatics. *Journal of Industrial Information Integration*, *25*, 100258.
11. Mubashar, A., Asghar, K., Javed, A. R., Rizwan, M., Srivastava, G., Gadekallu, T. R., ... & Shabbir, M. (2022). Storage and proximity management for centralized personal health records using an ipfs-based optimization algorithm. *Journal of Circuits, Systems and Computers*, *31*(01), 2250010.
12. Doan, T. V., Bajpai, V., Psaras, Y., & Ott, J. (2022). Towards decentralised cloud storage with IPFS: Opportunities, challenges, and future directions. *arXiv preprint arXiv:2202.06315*.
13. Prabha, P., & Chatterjee, K. (2022). Design and implementation of hybrid consensus mechanism for IoT based healthcare system security. *International Journal of Information Technology*, *14*(3), 1381-1396.
14. Patan, R., Manikandan, R., Parameshwaran, R., Perumal, S., Daneshmand, M., & Gandomi, A. H. (2022). Blockchain Security Using Merkle Hash Zero Correlation Distinguisher for the IoT in Smart Cities. *IEEE Internet of Things Journal*, *9*(19), 19296-19306.

15. Jayabalan, J., & Jeyanthi, N. (2022). Scalable blockchain model using off-chain IPFS storage for healthcare data security and privacy. *Journal of Parallel and Distributed Computing*, *164*, 152-167.
16. Wang, J., Chen, J., Ren, Y., Sharma, P. K., Alfarraj, O., & Tolba, A. (2022). Data security storage mechanism based on blockchain industrial Internet of Things. *Computers & Industrial Engineering*, *164*, 107903.
17. Ren, Y., Guan, H., Zhao, Q., & Yi, Z. (2022). Blockchain-based proof of retrievability scheme. *Security and Communication Networks*, *2022*.
18. Habib, G., Sharma, S., Ibrahim, S., Ahmad, I., Qureshi, S., & Ishfaq, M. (2022). Blockchain Technology: Benefits, Challenges, Applications, and Integration of Blockchain Technology with Cloud Computing. *Future Internet*, *14*(11), 341.
19. Ezhil Arasi, V., Indra Gandhi, K., & Kulothungan, K. (2022). Auditable attribute-based data access control using blockchain in cloud storage. *The Journal of Supercomputing*, *78*(8), 10772-10798.
20. Prabhu, S. M., Subramanyam, N., Krishnan, M., Shreya, P., & Sachidananda, M. (2022). Decentralized Digital Currency System using Merkle Hash Trees. *arXiv preprint arXiv:2205.03259*.