iJRASET
International Journal For Research in Applied Science and Engineering Technology

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 13 **Issue:** VIII **Month of publication:** August 2025

**DOI:** https://doi.org/10.22214/ijraset.2025.73735

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 13 Issue VIII Aug 2025- Available at www.ijraset.com*

# Secure Storage Layer Using Hybrid Technologies for Decentralized File Storage

Ms. Geeta N. Brijwani[1], Dr. Prafulla E. Ajmire[2]
[1]*Research Scholar, PGTD Computer Science & Engineering, SGBAU, Amravati & Assistant Professor, KC College, Churchgate, Mumbai*
[2]*Supervisor, PGTD Computer Science & Engineering, SGBUA, Amravati & Professor & Head, Dept. of Computer Science., GS College, Khamgaon*

***Abstract:*** ***Decentralized file storage systems are pivotal for secure and reliable data management in applications such as healthcare. This research proposes a novel hybrid technology integrating the InterPlanetary File System (IPFS) and Practical Byzantine Fault Tolerance (PBFT) to create a secure storage layer for a Blockchain-based Electronic Health Record (EHR) system. IPFS ensures decentralized data storage with high availability and redundancy, while PBFT provides fault-tolerant consensus to maintain data integrity and consistency across network nodes. The proposed architecture encrypts healthcare records using AES, splits them into chunks for storage on IPFS, and employs PBFT to validate transactions, ensuring resilience against faulty or malicious nodes. The hybrid approach achieves robust security, scalability, and fault tolerance, making it ideal for sensitive medical data management. Experimental outcomes demonstrate enhanced data integrity, availability, and reliability, positioning this solution as a significant advancement in decentralized storage for healthcare applications.***
***Keywords: secure, reliable, data storage, fault-tolerant, scalability, data integrity, availability***

## I. INTRODUCTION

Blockchain is a decentralized and distributed ledger technology that enables secure and transparent record-keeping of transactions across a network of computers [1]. It is a distributed system that stores time-ordered data in a continuously growing list of blocks. Each block contains information on transactions and business activities, and the network uses a consensus algorithm to agree on which block will be attached to the current recognized chain, hence the term “blockchain” [2]. Cryptocurrencies like Bitcoin and Ethereum have demonstrated the feasibility of decentralized digital currencies, offering alternatives to traditional payment systems and enabling peer-to-peer transactions with high transparency and efficiency [3].

This research proposes a hybrid technology for decentralized file storage using a secure storage layer. The hybrid approach combines the decentralized data storage capabilities of the InterPlanetary File System (IPFS) with the fault-tolerant consensus mechanism of Practical Byzantine Fault Tolerance (PBFT) to provide a robust and resilient storage solution. IPFS serves as the underlying storage layer, distributing and replicating data across multiple nodes in the network [4]. PBFT establishes consensus among nodes regarding the order and validity of data transactions, ensuring data consistency and integrity despite faulty or malicious nodes. By integrating these technologies, the hybrid approach achieves decentralized storage with built-in fault tolerance, making it suitable for applications requiring high availability, reliability, and security [5.6].

### *A. Outcome of Research*

The research on designing a novel Blockchain-based Electronic Health Record (EHR) system has yielded significant outcomes, positioning it as a superior solution for modern healthcare data management. The hybrid IPFS and PBFT storage solution enhances data integrity and availability while providing robust fault tolerance, ensuring the reliability of healthcare records even during network failures [7]. This approach addresses critical challenges in healthcare data management, offering a secure, scalable, and resilient platform for sensitive medical information.

## II. LITERATURE SURVEY

The literature review examines key works relevant to the proposed hybrid storage solution:

Li (2020) proposes a multi-layer PBFT consensus mechanism to address scalability challenges in blockchain systems. The study highlights limitations in traditional PBFT algorithms, which struggle to scale efficiently with growing transaction volumes. Li’s scalable solution maintains performance and security, offering insights into designing consensus mechanisms for large-scale networks (Li et al., 2020).

Hegde et al. (2023) present a blockchain solution tailored for healthcare applications, focusing on PBFT consensus and lightweight blockchain architectures. The study explores cryptographic properties, practical implications, strengths, limitations, and future directions, providing a foundation for secure healthcare data management (Hegde et al., 2023).

Kebira et al. (2023) introduce BlockMedCare, a healthcare system integrating IoT, blockchain, and IPFS to address data management security challenges. By leveraging the synergies of these technologies, BlockMedCare establishes a secure and resilient platform for managing sensitive medical information, aligning closely with the proposed hybrid approach (Kebira et al., 2023).

These studies underscore the potential of combining IPFS and PBFT to enhance security, scalability, and fault tolerance in blockchain-based systems, particularly for healthcare applications.

## III. PROPOSED METHODOLOGY

The proposed system streamlines the process of storing and accessing electronic health records (EHRs) through its blockchain-based architecture. Leveraging IPFS for decentralized storage and PBFT consensus mechanism for efficient transaction processing, the system ensures rapid and secure access to patient data while maintaining data integrity and confidentiality [7,8]. The utilization of smart contracts on the Ethereum blockchain facilitates seamless interaction and interoperability among healthcare providers, patients, and other stakeholders, enabling real-time access to critical health information and improving care coordination and decision-making.

### *A. Secure Storage Technique (IPFS + PBFT)*

The proposed hybrid architecture combines the decentralized storage capabilities of IPFS with the consensus mechanism of PBFT to provide a secure and efficient storage solution for the Blockchain-based EHR system. The integration leverages the strengths of both technologies to ensure data integrity, availability, and reliability [8].

The below figure shows a "Hybrid of IPFS + PBFT," combining Interplanetary File System (IPFS) for decentralized storage and Practical Byzantine Fault Tolerance (PBFT) for secure consensus in a blockchain-based healthcare system. [9]

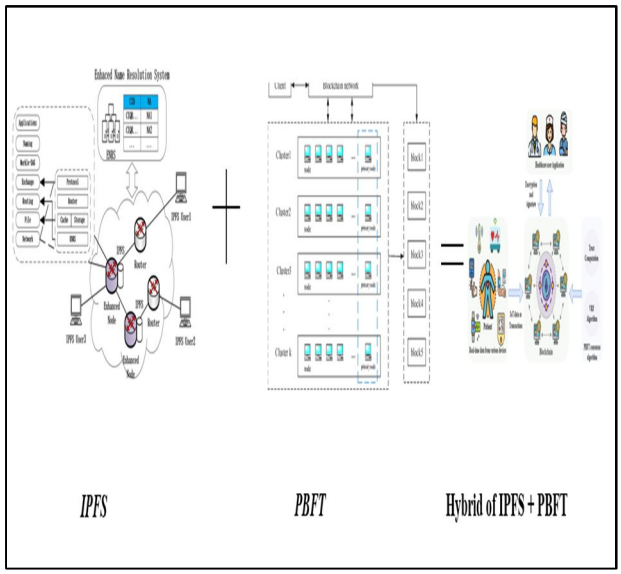



Figure 1: Integration of IPFS and PBFT

The process begins with encrypting healthcare records using the Advanced Encryption Standard (AES) [10]. The encrypted data is split into chunks and stored on the IPFS network, which ensures high availability and redundancy through its distributed nature. Cryptographic hashes guarantee data integrity. The PBFT consensus mechanism manages the state of records stored on IPFS, ensuring all nodes agree on changes to maintain consistency and reliability [11]. This hybrid approach provides a robust solution by combining IPFS's decentralized storage with PBFT's fault tolerance and security [12].

In summary, the hybrid IPFS and PBFT architecture enhances the proposed EHR system by delivering a secure, reliable, and efficient storage solution, ensuring the integrity, availability, and security of healthcare records [30].

## IV. EXPERIMENTAL ANALYSIS & RESULTS

In the context of Electronic Health Recording (EHR) systems, the choice of a storage solution is critical due to the need for high security, availability, and scalability [14,15]. This section compares the hybrid storage system combining IPFS (InterPlanetary File System) and PBFT (Practical Byzantine Fault Tolerance) with other decentralized storage solutions, namely Storj, Sia, Arweave, and Swarm and justifies why the IPFS + PBFT hybrid approach is the most secure and effective for managing healthcare records [16].

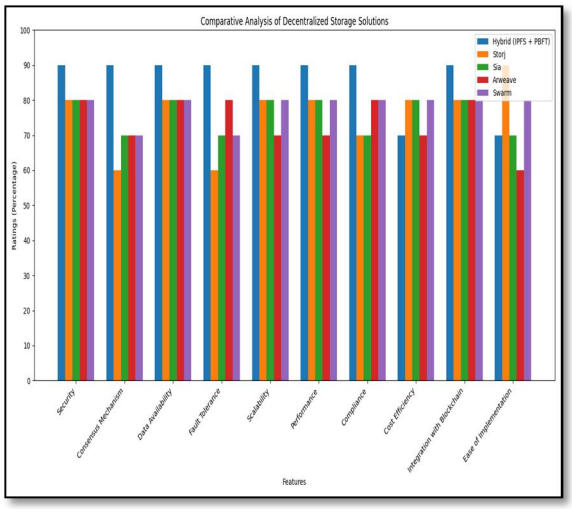



Figure 2: Hybrid (IPFS + PBFT)-Optimal Choice for Storing and Accessing Healthcare Records

Figure 2 titled "Comparative Analysis of Decentralized Storage Solutions for EHR Systems: Justifying Hybrid (IPFS + PBFT) as the Optimal Choice for Storing and Accessing Healthcare Records" presents a comprehensive evaluation of different decentralized storage solutions based on ten key features. The x-axis lists these features: Security, Consensus Mechanism, Data Availability, Fault Tolerance, Scalability, Performance, Compliance, Cost Efficiency, Integration with Blockchain, and Ease of Implementation. Each feature is crucial for the effective management of healthcare records in an EHR system. The y-axis represents the ratings of these features as percentages, ranging from 0% to 100%, allowing for a clear comparison of the performance of each storage solution. The ratings are presented as bars, with different colors representing the five technologies compared: Hybrid (IPFS + PBFT) in blue, Storj in orange, Sia in green, Arweave in red, and Swarm in purple.

Table 1: Comparative analysis table highlighting the key features of different consensus algorithm solutions, justifying the Hybrid (IPFS and PBFT) as the most secure and best option for storing and accessing healthcare records

| Criteria | Hybrid (IPFS + PBFT) | PoW | PoS | PoA | Tendermint | PoET |
|---|---|---|---|---|---|---|
| Security | Extremely High | Very High | High | High | High | Moderate |
| Scalability | High | Low | Moderate | High | High | High |
| Energy Efficiency | Very High | Very Low | High | Very High | High | Very High |
| Fault Tolerance | High | Moderate | High | Moderate | High | High |
| Latency | Low | High | Moderate | Low | Low | Low |
| Data Availability | High | High | High | High | High | High |
| Compliance and Regulatory | High | Moderate | High | High | High | Moderate |
| Ease of Implementation | Moderate | Low | Moderate | High | Moderate | Moderate |

Explanation for Hybrid (IPFS + PBFT): The Hybrid (IPFS + PBFT) solution stands out as the best choice for storing and accessing healthcare records in a blockchain environment. It combines the strengths of decentralized storage with efficient and secure consensus, offering a balance of high security, scalability, energy efficiency, fault tolerance, and regulatory compliance [17]. This makes it an optimal solution for the demanding requirements of Electronic Health Recording (EHR) systems. The combination of IPFS's decentralized storage with PBFT's robust consensus mechanism ensures that healthcare records are stored and accessed securely, reliably, and efficiently, aligning well with the specific needs of healthcare data management [18,19].

Table 2: Data for the comparative analysis of various consensus mechanisms and it's accuracy

| Consensus Mechanisms | Accuracy (Percentage) |
|---|---|
| Hybrid (IPFS + PBFT) | 87.50% |
| PoW | 51.25% |
| PoS | 77.50% |
| PoA | 85.50% |
| Tendermint | 86.50% |
| PoET | 83.75% |

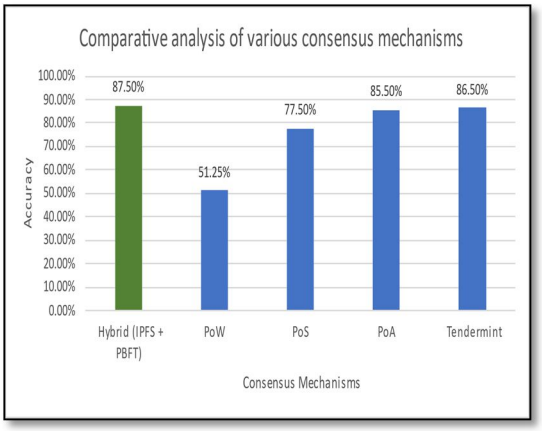



Figure 3: Comparative analysis of various consensus mechanisms

Figure 3 showcasing the overall accuracy of each mechanism and emphasizing the superiority of the Hybrid (IPFS + PBFT) solution for storing and accessing healthcare records in blockchain-based Electronic Health Recording (EHR) systems. Figure 3 titled "Comparative Analysis of Consensus Mechanisms with Overall Accuracy" presents the overall accuracy of various consensus mechanisms for storing and accessing healthcare records on a blockchain. The x-axis lists the different consensus mechanisms: Hybrid (IPFS + PBFT), Proof of Work (PoW), Proof of Stake (PoS), Proof of Authority (PoA), Tendermint, and Proof of Elapsed Time (PoET). The y-axis represents the overall accuracy as a percentage.

*B. Overall Accuracy Calculation*

The overall accuracy for each consensus mechanism is calculated by averaging the ratings of eight key criteria: Security, Scalability, Energy Efficiency, Fault Tolerance, Latency, Data Availability, Compliance and Regulatory Adherence, and Ease of Implementation [20].

*C. Ratings*

*1)* Hybrid (IPFS + PBFT): Achieved an overall accuracy of 87.50%, reflecting its high performance across all criteria, especially in security, scalability, energy efficiency, fault tolerance, latency, and compliance.

*2)* PoW: Scored the lowest with 51.25% due to its high computational requirements, low energy efficiency, and low ease of implementation.

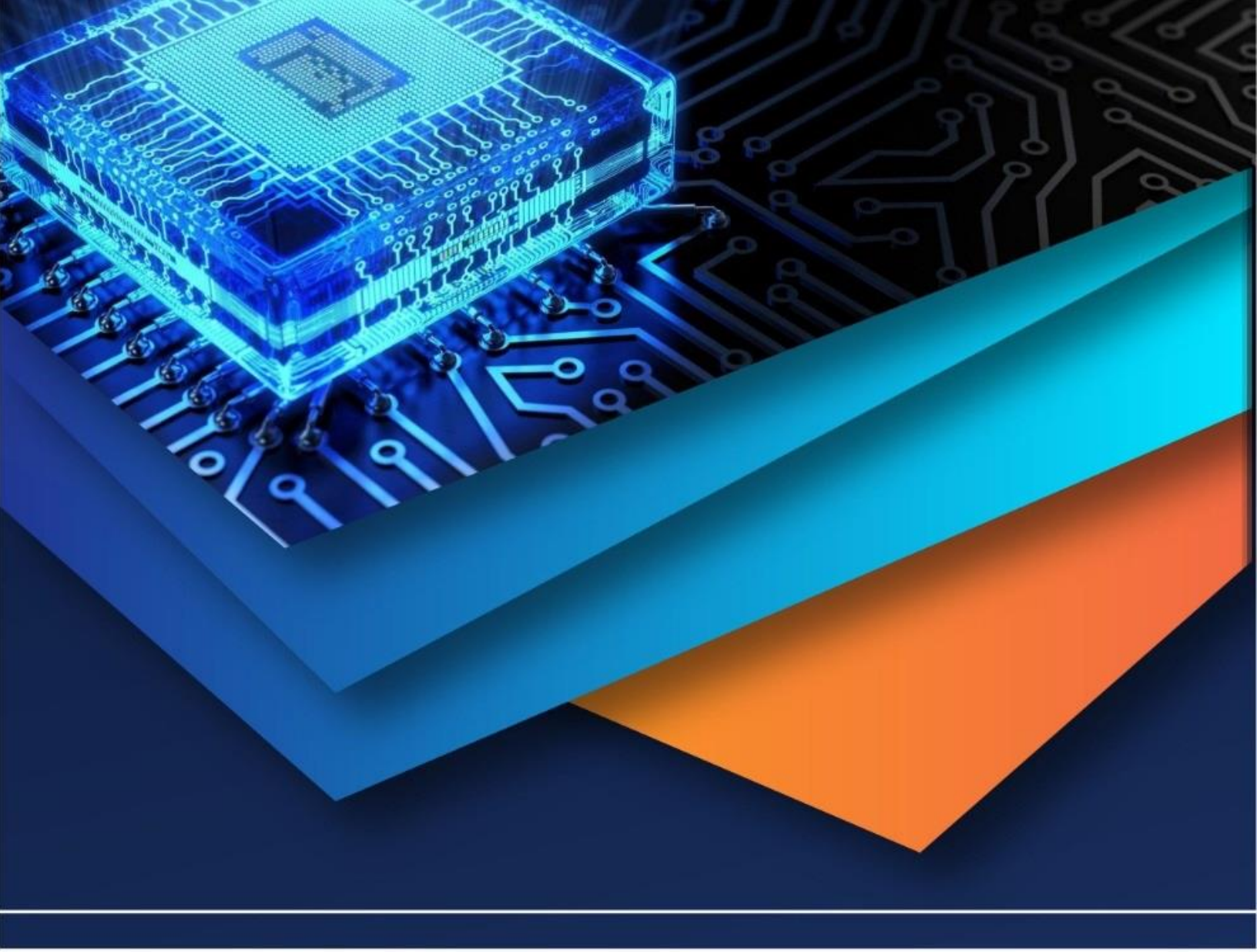
*3)* PoS: Achieved 77.50%, demonstrating good performance in security, energy efficiency, and fault tolerance, but moderate scalability and ease of implementation.
*4)* PoA: Scored 85.50%, performing well in scalability, energy efficiency, and ease of implementation, but with potential centralization risks.
*5)* Tendermint: Also scored 86.50%, indicating strong performance in security, fault tolerance, and latency.
*6)* PoET: Achieved 83.75%, showing high scalability, energy efficiency, and low latency, but moderate security due to reliance on trusted execution environments.

## V. CONCLUSION

This study demonstrates the hybrid approach of combining IPFS with PBFT that stands out as the most secure and effective for storing and accessing healthcare records in an EHR system. The combination leverages the strengths of both technologies, providing enhanced security, high availability, fault tolerance, performance, scalability, regulatory compliance, and flexibility. This hybrid system addresses the specific needs of healthcare data management, ensuring that sensitive patient information is stored and accessed securely, reliably, and efficiently. In conclusion, the Hybrid (IPFS + PBFT) solution is one of the best choices for managing healthcare records on a blockchain, balancing high security, scalability, energy efficiency, and fault tolerance. This makes it an ideal solution for the stringent requirements of Electronic Health Recording (EHR) systems.

## REFERENCES

[1] Keccak specifications Guido Bertoni1, Joan Daemen1, Micha¨el Peeters2 and Gilles Van Assche1, (2018)
[2] A Scalable Multi-Layer PBFT Consensus for Blockchain Wenyu Li; Chenglin Feng; Lei Zhang; Hao Xu; Bin Cao; Muhammad Ali Imran, (2020).
[3] IoT data privacy via blockchains and IPFS Authors- Muhammad Salek Ali, Koustabh Dolui, Fabio Antonelli, (2017).
[4] A survey on the security of blockchain systemspanelXiaoqi Li a, Peng Jiang a, Ting Chen b, Xiapu Luo a, Qiaoyan Wen c- In their comprehensive survey (2020)
[5] Study and Survey on Blockchain Privacy and Security Issues Sourav Banerjee, Debashis Das, Manju Biswas, Utpal Biswas
[6] Blockchain Technology in Electronic Healthcare Systems Sujatha Alla, Leili Soltanisehat, Unal Tatar, and Omer Keskin Engineering Management & Systems Engineering Department
[7] Blockchain security enhancement: an approach towards hybrid consensus algorithms and machine learning techniques K. Venkatesan & Syarifah Bahiyah Rahayu- In their pioneering research (2024)
[8] Secure PBFT Consensus-Based Lightweight Blockchain for Healthcare Application Pawan HegdeandPraveen Kumar ReddyMaddikunta, (2023).
[9] Electronic Healthcare Data Record Security Using Blockchain and Smart Contract Farjana Khanam Nishi, Mahizebin Shams-E-, (2021)
[10] Blockchain in government: Benefits and implications of distributed ledger technology for information sharing Author links open overlay panelSvein Ølnes a, Jolien Ubacht b, Marijn Janssen, (2017).
[11] Mohsin, J.; Han, L.; Hammoudeh, M.; Hegarty, R. Two Factor vs. Multi-factor, an Authentication Battle in Mobile Cloud Computing Environments. In Proceedings of the International Conference on Future Networks and Distributed Systems, Cambridge, UK, 19–20 July 2017; ACM: New York, NY, USA, 2017; p. 39. [Google Scholar]
[12] Systematic approach to analyzing security and vulnerabilities of blockchain systems Thesis: S.M. in Engineering and Management, Massachusetts Institute of Technology, System Design and Management Program, 2019
[13] Blockchain-Assisted Secure Fine-Grained Searchable Encryption for a Cloud-Based Healthcare Cyber-Physical System IEEE/CAA J Autom Sin, 8 (12) (2021)
[14] Dorri A, Kanhere SS, Jurdak R. Towards an Optimized BlockChain for IoT. In: Proceedings of the Second International Conference on Internet-of-Things Design and Implementation – IoTDI '17. ACM Press: Pittsburgh, PA, USA; (2017).
[15] BlockMedCare: A healthcare system based on IoT, Blockchain and IPFS for data management security Author- Kebira Azbeg, Ouail Ouchetto, Said Jai Andaloussi, (2022).
[16] [Retracted] Blockchain in Secure Healthcare Systems: State of the Art, Limitations, and Future Directions Vahiny Sharma,Ankur Gupta,Najam Ul Hasan,Mohammad Shabaz,and Isaac Ofori, (2022).
[17] Exploring Potentials and Challenges of Blockchain-based Public Key Infrastructures, Thomas Hepp; Fabian Spaeh; Alexander Schoenhals; Philip Ehret; Bela Gipp, (2019).
[18] Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends Shuai Wang; Liwei Ouyang; Yong Yuan; Xiaochun Ni; Xuan Han; Fei-Yue Wang, (2019).
[19] Tracing manufacturing processes using blockchain-based token compositions Author links open overlay panelMartin Westerkamp, Friedhelm Victor, Axel Küpper, (2020).
[20] C. C. Agbo, Q. H. Mahmoud, and J. M. Eklund, "Blockchain technology in healthcare: a systematic review," Multidisciplinary Digital Publishing Institute, In Healthcare, vol. 7, no. 2,p. 56, 2019.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY