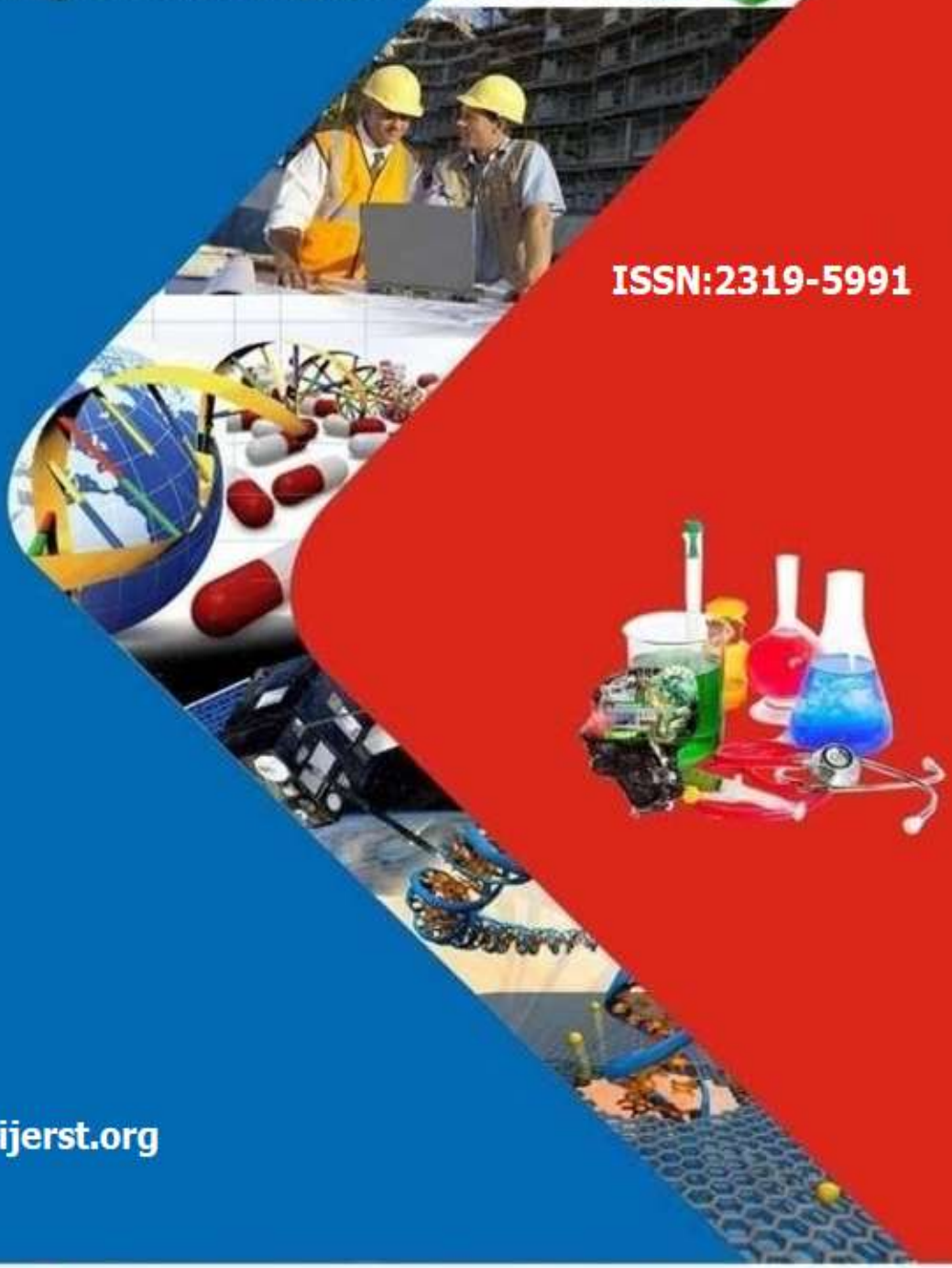
# International Journal of Engineering Research and Science & Technology

IJERST

ISSN:2319-5991



www.ijerst.org

E-mail: editor@ijerst.org or ijerst.editor@gmail.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
*Vol. 20, Issue 1, 2024*

# BLOCKCHAIN-ENABLED SYSTEM FOR CONFIDENTIAL AND TAMPER-PROOF EXAM PAPER DELIVERY

**[1]P.Veena Kumari**

[1]Assistant Professor, Brilliant Grammar School Educational Society Group Of Institutions Integrated Campus,
Near By Ramoji Filmcity, Hayathnagar, Abdullahpurmet, Hyderabad, Telangana 501505

## ABSTRACT

In a traditional examination management system, the processes of requesting and setting question papers, along with the circulation of finalized papers from the Controller of Examination (COE) to teachers and examination superintendents, are predominantly carried out physically. These manual processes raise significant concerns regarding security, confidentiality, and efficiency. Moreover, the physical circulation of question papers involves additional costs and delays. To address these challenges, a Blockchain-based decentralized system is proposed. This system leverages Blockchain and the Interplanetary File System (IPFS) to securely manage the creation, distribution, and storage of examination papers while ensuring tamper-proof and immutable records. By eliminating physical circulation, the proposed system reduces costs, enhances security, and expedites the examination management process. The solution is implemented using Django for the web framework, Ganache for Blockchain development, and IPFS for decentralized file storage.

**Index Terms:** Blockchain, IPFS, Examination Management System, Security, Decentralization, Django, Ganache, Question Paper Management, Smart Contracts, Data Integrity.

## 1 INTRODUCTION

In today's era, every individual's data is available on the internet, which can be retrieved from anywhere in the world, increasing various challenges in the aspects of data security, trust, and transparency over the internet. A number of universities have been adapting to conducting the examination in online mode, and many more have been motivated to do the same in the wake of the conditions rendered because of COVID-19. The primary constraint of online examination is trust and security. Several

ISSN 2319-5991 www.ijerst.com
*Vol. 20, Issue 1, 2024*

service providers offer their users One-Time Passwords, private network lockers, passwords, and strong security passwords, etc. Security of the data is more important in the existing system as it involves third parties. Blockchain is an evolving technology that provides data privatization. In this, a third party will not be involved in any kind of service. It creates a chain of data blocks and maintains data integrity by validating data using cryptographic algorithms. Each data block in the blockchain is associated with a hash code. These codes are validated by validators. Blockchain uses smart contracts, which is an agreement process without involving any third party. Applications of blockchain spread across a wide domain including healthcare, finance, business, and many more. The proposed system makes use of the blockchain concept for the transmission of the examination paper.

### 1.1 BLOCKCHAIN

It is a decentralized, distributed ledger that can be used for asset tracking in business. An asset can be tangible or intangible. Implementation of blockchain technology was initially done for Bitcoin. Bitcoin is a digital cryptocurrency. The main idea behind Bitcoin is to offer a decentralized banking system. Users exchange their assets and trust the transaction results, which are recorded on the distributed shared ledger. Every user in a blockchain network acts as a node, who is responsible for initiating and validating the transaction. Above, Figure 1 depicts the architecture of blockchain. Nodes in a blockchain network are connected in a decentralized manner. Every node maintains a copy of the blockchain ledger, which is updated on a regular basis with each transaction. The term “blockchain” means the chain of blocks. In this, any block can initiate a transaction and broadcast it to other nodes in the network. Network nodes validate this transaction. All transactions that occur at a particular moment of time are grouped together, which forms the block. This block is then added to the blockchain. Each block is composed of two parts, namely the block header and the block body.

### 1.2 HYPERLEDGER BLOCKCHAIN

Hyperledger is a developing modular, extensible framework with common building blocks that can be reused. It is interoperable. It provides services like consensus and membership. One of the

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
*Vol. 20, Issue 1, 2024*

attractive features that Hyperledger fabric provides is its design to facilitate various pluggable components. It facilitates the running of distributed applications and supports a number of consensus protocols. Distributed applications, which are in general-purpose programming languages, can also be run on it.

### 1.3 INTER-PLANETARY FILE SYSTEM (IPFS)

IPFS is designed to link every computing device with the same file system. IPFS is designed to be used in several ways; it provides various features to decrease the complexity of the produced data blocks, reduce data redundancy, and provide security.

### 1.4 SMART CONTRACTS

It is the most important element in the blockchain system as it provides a mechanism to configure the behavior of it. These are scripts that fire when a particular event occurs. It can be written in a native language or a general-purpose programmable language.

## 2 LITERATURE SURVEY

Technologies like Blockchain and Hyperledger Fabric have been around for quite some time. They still have a lot of potential for usage in various sectors. Some newer technologies like IPFS can be combined with blockchain to make the decentralization more secure and applicable for distributed file-sharing systems. The conduct and evaluation of academic tests requires a trusted and transparent authority. Blockchain can be used to develop systems that would eliminate the necessity for a central trusted entity for obtaining certificates. In [6] Exam Record Management using Blockchain is discussed. It proposes a methodology to use blockchain for conducting decentralized examination and for better evaluation of the examination records. It is based on delegated proof of stake which provides transparency and creditability to the examination process. IPFS is a suitable match for Blockchain since both technologies use Merkle tree data structures for the generation of unique hash identifiers. Despite having the same nature as blockchain, IPFS pairs quite inefficiently with it. To solve this problem, the authors proposed a secure file sharing system that

ISSN 2319-5991 www.ijerst.com
*Vol. 20, Issue 1, 2024*

includes a distributed access control and group key management through the adoption of the IPFS proxy [7]. In [8], the authors discover the use of secure multiparty computation (MPC) for supporting private data on Fabric. In the literature [9], the significance of a blockchain network in the education system is discussed. The use of public blockchains in the modern education system is described in this research. They use consensus algorithm to secure every block and reduce the amount of computation power required. The solidity language was used to create and manage the contract. They were able to create a smart-contract based online examination system and successfully compare it against a cloud-based examination system [9]. In paper [10], a solution is proposed for the implementation of a smart contract built on permission Blockchain Hyperledger Fabric. In [11], secured data sharing using IPFS and blockchain is proposed. It provides data authenticity and quality of data to customers. It also provides a stable business platform for owner. In [12], secure bank transactions are done using visual cryptography and steganography. Here this hybrid mechanism is used to transfer the transaction key securely. In Paper [13], the identity of the source, destination and route is secured using the ALERT routing protocol. In [14], secure authorized deduplication is achieved using a token generation algorithm. This [15], [16] patent discusses the use of blockchain technology for transferring digital evidence or data. In patent [17], data storage system in blockchain is discussed. In [18], an in-depth survey on blockchain's security and privacy issues has been conducted. This survey is based on publications in five well-known databases like IEEE, WoS, ACM digital library, Inder science, etc. In [19], authors propose an IoT and fog computing based smart healthcare system. To ensure better security concept of blockchain is used in the proposed system. In [20], hybrid blockchain with cloud integration model is developed for preowned vehicle application to track its details. This system provides transparency in preowned car purchases. In [21], in-depth study is done regarding use of blockchain technology in education domain. This paper also discusses some case studies which reflects how the use of blockchain technology is helpful in achieving educational outcomes. In [22], blockchain based model to preserve privacy of patients health record is developed. Using this decentralized model patient can give

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
*Vol. 20, Issue 1, 2024*

access rights of their medical record. The major motivation for doing this research is to enhance the process of the existing examination system, in particular to provide secure transmission of examination papers.

### 3.1 EXISTING SYSTEM

The existing examination management system is largely dependent on manual operations for the formulation, distribution, and handling of question papers. In this traditional setup, the Controller of Examination (COE) initiates the process by physically sending requests to teachers for setting question papers. Once the papers are prepared, teachers manually submit them to the COE. This approach raises several critical concerns. Firstly, physical handling and transportation of question papers increase the risk of unauthorized access, tampering, and even leaks, compromising the integrity of the examination process. Secondly, this manual procedure is time-consuming and incurs significant administrative and logistical costs, leading to inefficiencies and delays. Moreover, the reliance on centralized repositories for record-keeping presents a major vulnerability; a single point of failure could result in the loss, corruption, or unauthorized alteration of sensitive data, thereby undermining the security and trustworthiness of the entire system.

#### 3.1.1 DISADVANTAGES

- Manual handling of question papers leads to high risk of tampering, data leaks, and security breaches.
- The process is time-consuming, costly, and prone to inefficiencies due to centralized and physical operations.

### 3.2 PROPOSED SYSTEM

To overcome the limitations of the existing system, a Blockchain-based decentralized examination management system is proposed, integrating cutting-edge technologies to enhance security, efficiency, and transparency. The system is built on a decentralized architecture using Blockchain, which provides an immutable and transparent ledger for tracking all activities related to question paper management. This ensures tamper-proof record-keeping and eliminates the risks associated with centralized data storage. Question papers are securely stored using the Interplanetary File System (IPFS), which distributes data across

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
*Vol. 20, Issue 1, 2024*

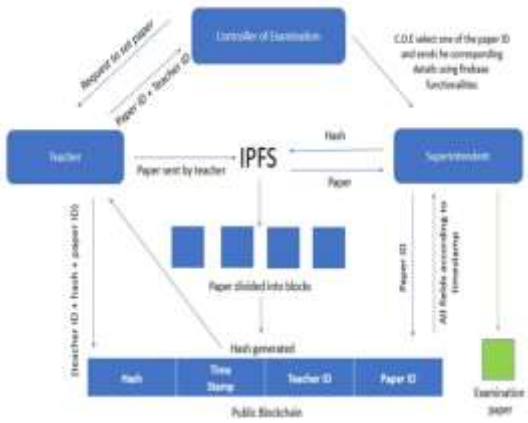
multiple nodes, making it immutable and accessible only to authorized users.

Role-based access control mechanisms are implemented to regulate interactions among the COE, teachers, and examination superintendents, ensuring that sensitive information is accessible only by designated personnel. Furthermore, the system automates the processes of request generation and paper distribution, effectively eliminating the need for physical handling and reducing time delays. Security is significantly enhanced through the combination of Blockchain's data integrity and IPFS's secure, decentralized storage, which together mitigate risks of data breaches and unauthorized modifications. The proposed solution is developed using Django as the web framework, Ganache for simulating the Blockchain environment, and IPFS for decentralized file storage, forming a comprehensive and secure platform for managing examinations in a modern academic environment.

### 3.2.1 ADVANTAGES

- Blockchain and IPFS ensure secure, tamper-proof, and decentralized storage and distribution of question papers.
- The system improves efficiency, reduces costs, and ensures role-based access to maintain confidentiality and integrity.

## 4. SYSTEM ARCHITECTURE




The process begins with a teacher initiating the creation of an exam paper by sending a request to the Controller of Examination. Subsequently, the teacher prepares the exam paper and uploads it to the InterPlanetary File System (IPFS), a decentralized storage network. Upon upload, IPFS generates a unique cryptographic hash representing the paper's content, which serves as its permanent, content-based address. Along with this hash, the teacher's identification and a paper identifier are then recorded onto the public blockchain, ensuring an

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
*Vol. 20, Issue 1, 2024*

immutable and transparent record of the paper's submission. The InterPlanetary File System plays a dual role by providing decentralized storage for the exam paper itself and generating the crucial cryptographic hash that anchors the paper's integrity on the blockchain. While the diagram conceptually shows the paper divided into blocks within IPFS, the blockchain primarily stores the metadata associated with the entire file. This metadata includes the IPFS-generated hash, a timestamp of the recording, the submitting teacher's ID, and the unique Paper ID, creating a verifiable and auditable trail of the exam paper's journey. The Controller of Examination acts as a central coordinator, receiving the initial paper setting request from the teacher. From the submitted papers, the C.o.E. selects a specific Paper ID. Utilizing Firebase, a platform for real-time data synchronization, the C.o.E. securely transmits the selected Paper ID and potentially other relevant instructions to the Superintendent, initiating the paper retrieval process for examination administration. Finally, the Superintendent receives the Paper ID and associated details from the Controller of Examination via Firebase. Leveraging the Paper ID, which is linked to the immutable hash recorded on the blockchain, the Superintendent can securely retrieve the authentic and untampered encrypted exam paper from IPFS using this hash. The system ensures that the Superintendent has access to all relevant details recorded on the blockchain, including the timestamp, providing a verifiable history of the exam paper's lifecycle and guaranteeing its integrity.

## 5.OUTPUT SCREEN


**Fig 5.1 : Home page of Blockchain-based Examination Paper Transmission**


**Fig 5.2 : Admin Portal of Controller of Examination (COE)**

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
*Vol. 20, Issue 1, 2024*

**Fig 5.3 : COE Creating Paper Request**

**Fig 5.4 : View Exam Paper Requests**


**Fig 5.5 : Superintendent Portal Teachers Details**

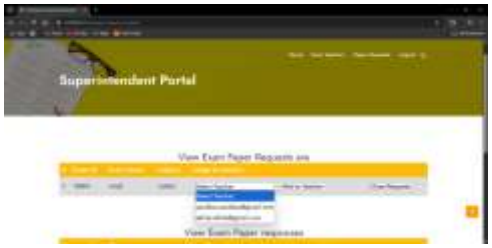



**Fig 5.6 : Superintendent Allocating Paper Request**

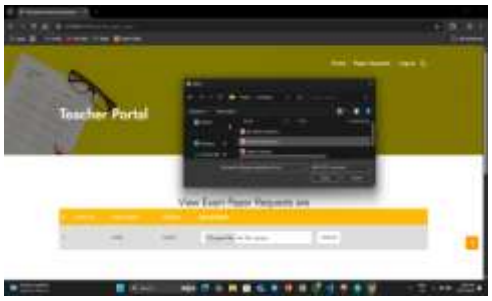



**Fig 5.7 : Teacher Uploading the Requested Exam Paper**

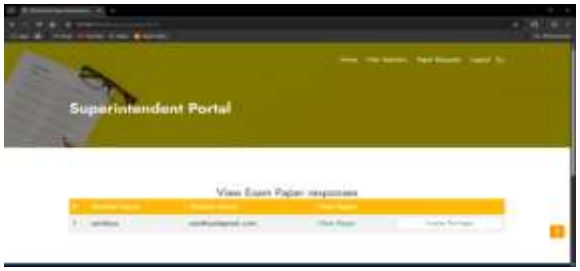



**Fig 5.8 : Superintendent Finalize the Exam Paper Responses**


**Fig 5.9 : Paper Uploaded IPFS server and Data Stored in Block Chain**

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
*Vol. 20, Issue 1, 2024*

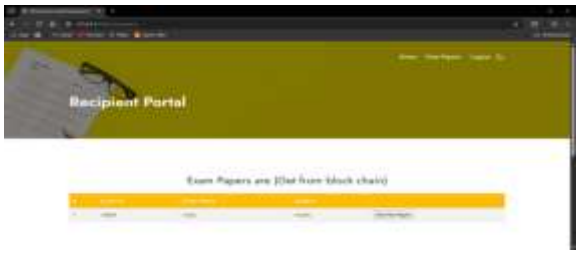



**Fig 5.10 : List of Papers Uploaded in Block Chain**


**Fig 5.11 : IPFS Server**

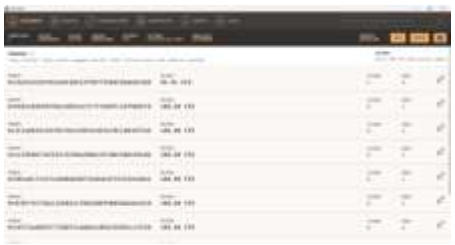


**Fig 5.12 : Ganachi Block Chain**

## 6.CONCLUSION

In conclusion, the blockchain and IPFS-based system presented in this paper offers a compelling solution to the inherent vulnerabilities associated with traditional physical examination paper transmission and distribution. By employing IPFS for decentralized file sharing and Hyperledger for a tamper-proof and transparent record of paper metadata, the system effectively addresses issues such as the exposure of paper setter identities, susceptibility to bribery and threats, and the risk of pre-exam paper leaks through strong encryption of IPFS file hashes. The inherent immutability of the blockchain further fortifies the system against unauthorized modifications. This innovative approach not only enhances the security and integrity of the examination process but also paves the way for future advancements in securing other critical educational documents, ultimately contributing to a more trustworthy and efficient academic ecosystem.

## 7.FUTURE SCOPE

The proposed secure examination paper transmission system, leveraging Hyperledgerblockchain and IPFS, lays a robust foundation for future enhancements and broader applications within the educational domain. One significant avenue for expansion involves integrating the system with the secure management and verification of student credentials, such as result certificates. By extending the blockchain's immutability and transparency

ISSN 2319-5991 www.ijerst.com
*Vol. 20, Issue 1, 2024*

to these vital documents, the system could facilitate paperless verification processes, reduce the risk of forgery, and streamline the sharing of academic achievements with educational institutions and potential employers. Furthermore, exploring the integration of advanced access control mechanisms, such as attribute-based access control (ABAC), could provide more granular control over paper access and enhance security. Investigating the use of zero-knowledge proofs could also offer a way to verify the integrity of exam papers without revealing their content to unauthorized parties.

## 8. REFERENCES

[1] RavindharVadapalli, Blockchain Fundamentals Textbook Suitable for all. Edition: 1.1, Publisher: Blockchainprep,Editor: Blockchainprep. UAE ISBN: 301.345.908.

[2] Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, 2009. [online]. Available: https://bitcoin.org/bitcoin.pdf

[3] Elli Androulaki, Artem Barger, Vita Bortnikov, et al., “Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains”, EuroSys '18: Proceedings of the Thirteenth EuroSys Conference, Art. no. 30, pp. 1-18, 2018.

[4] Juan Benet, “IPFS - Content Addressed, Versioned, P2P File System”, 2014. [online]. Available: https://arxiv.org/pdf/1407.3561.pdf.

[5] Y. N. Patil, A. W. Kiwelekar, L. D. Netak et. al., “ A Decentralized and Autonomous Model to Administer University Examinations”, In: Lee SW., Singh I., Mohammadian M. (eds) Blockchain Technology for IoT Applications. Blockchain Technologies. Springer, Singapore, pp.1-18, 2021.

[6] R. Acharya and S. Binu, “Blockchain based examination system for effective evaluation and maintenance of examination records”, International Journal of Engineering and Technology, vol 7, No.2.6 , pp. 269-274, 2018.

[7] H. S. Huang, T. S. Chang, and J. Y. Wu., “A secure file sharing system based on IPFS and blockchain”, in ACM International Conference Proceeding Series, pp. 96–100, 2020.

ISSN 2319-5991 www.ijerst.com
*Vol. 20, Issue 1, 2024*

[8] F. Benhamouda, S. Halevi, and T. Halevi, “Supporting private data on Hyperledger Fabric with secure multiparty computation”, IBM Journal of Research and Development, vol. 63, no. 2, pp. 3:1 - 3:8, 2019.

[9] A. Jain, A. Kumar Tripathi, N. Chandra, and P. Chinnasamy, “Smart Contract enabled Online Examination System Based in Blockchain Network”, International Conference on Computer Communication and Informatics, India, 2021.

[10] V. Aleksieva, H. Valchanov, and A. Huliyan, “Implementation of Smart-Contract, Based on Hyperledger Fabric Blockchain”, In 21st International Symposium on Electrical Apparatus Technologies, pp. 1–4, 2020

[11] M. Naz et al., “A Secure Data Sharing Platform Using Blockchain and Interplanetary File System”, Sustainability (Switzerland), vol. 11, no. 24 , 2019.

[12] Prachi D. Rathod and Smita R. Kapse, “Secure bank transaction using data hiding mechanisms”, International Conference on Innovations in Information, Embedded and Communication Systems, IEEE, 2017.

[13] AniketKhasnikar and SmitaKapse, “Secured Routing Using ALERT in MANET's”, International Journal of Science and Research (IJSR), Vol. 4, issue 1, pp.1987-1989, 2015.

[14] V. Waghmare and S. Kapse, “Authorized deduplication: an approach for secure cloud environment”, Procedia Computer. Sci. 78, pp. 815–823, 2016

[15] Justin Fisher, Maxwell Henry Sanchez, “Authentication and Verification of Digital Data Utilizing Blockchain Technology”, Patent: US 2016/0283920 A1, 2016.

[16] Thomas Fay and Dominick Paniscotti, “Systems and methods of blockchain transaction recordation”, Patent:US20160292672A1, 2016.

[17] II Robert Allan Segar, “Data storage system with blockchain technology”, Patent:US20170264428A1, 2017.

[18] Mohanta, B.K., Jena, D., Panda, S.S. and Sobhanayak, S., 2019. Blockchain technology: A survey on applications and security privacy challenges”,Science Direct, Internet of Things, vol 8, Dec, pp.100-107, 2019.

ISSN 2319-5991 www.ijerst.com
*Vol. 20, Issue 1, 2024*

[19] Banerjee, A., Mohanta, B.K., Panda, S.S., Jena, D. and Sobhanayak, S., "A secure IoT-fog enabled smart decision making system using machine learning for intensive care unit." In 2020 International Conference on Artificial Intelligence and Signal Processing (AISP),pp. 1-6, 2020.

[20] Ganesan Subramanian, AnandSreekantanThampy, "Implementation of Hybrid Blockchain in a Pre-Owned Electric Vehicle Supply Chain", IEEE Access, Vol. 9, pp. 82435-82454, 2021.

[21] Patrick Ocheja, Friday Joseph Agbo, Solomon Sunday Oyelere, , Brendan Flanagan and Hiroaki Ogata , "Blockchain in Education: A Systematic Review and Practical Case Studies", IEEE Access, , Vol. 10, pp. 99525-99540, 2022.

[22] HafidaSaidi, Nabila Labraoui , Ado Adamou Abba Ari, et. al., "DSMAC: Privacy-Aware Decentralized Self-Management of Data Access Control Based on Blockchain for Health Data",IEEE Access, Vol. 10, pp. 101011-101028, 2022.