

# Medical Report Manager Blockchain: Patients Control Encrypted Health Records Across Providers

Komal<sup>1</sup>, Dr. Anupam Bhatia<sup>2</sup>, Dr. Sneha Punia<sup>3</sup>  
MCA Student<sup>1</sup>, Associate Professor<sup>2</sup>, Asst Prof.<sup>3</sup>

Deptt. of Comp. Sc. and Application, Ch. Ranbir Singh University, Jind, Haryana, India

**Abstract:** Medical records are among the most sensitive and valuable assets in the healthcare sector, containing prescriptions, laboratory reports, diagnostic images and treatment histories that are essential for diagnosis and treatment. Traditional healthcare systems store these records in centralized databases which are vulnerable to hacking, unauthorized access, data breaches and single-point failures. In addition patients often do not have full control over who can access their medical information. This study proposes a blockchain-based Medical Report Manager that enables patients to control encrypted health records across multiple healthcare providers. The proposed system uses Hyperledger and Smart Contract to provide secure and decentralized medical record management. Medical reports are encrypted and stored securely while their cryptographic hashes are recorded on the blockchain to ensure authenticity and integrity. Smart contracts automate access control allowing patients to grant or revoke permissions to doctors, hospitals, and laboratories. The proposed framework improves privacy, security, interoperability, and trust while enabling efficient verification and sharing of medical records across healthcare providers.

**Index Terms:** Healthcare, Blockchain Technology, Hyperledger Fabric, Smart Contracts, Patient-Centric Access Control

## 1. Introduction

The healthcare industry generates a vast amount of sensitive digital information every day including prescriptions, laboratory reports, diagnostic images, treatment histories and discharge summaries. These medical records are usually stored in centralized databases maintained by hospitals, clinics, laboratories and insurance providers[1]. While centralized systems simplify data storage and management but they also introduce serious concerns related to privacy, security and patient ownership. Cyberattacks, unauthorized access, data breaches and single points of failure can compromise highly confidential health information putting both patients and healthcare institutions at risk. Therefore, secure methods for managing, verifying and sharing medical records have become increasingly important. In healthcare verification involves confirming that medical records are authentic and have been issued by legitimate healthcare providers while validation ensures that the information is accurate, complete and has not been altered. Traditional methods of sharing health records often require patients to manually collect documents from different hospitals and provide them to new doctors when seeking treatment. Healthcare professionals may need to contact previous providers to verify a report which is a time-consuming and inefficient process[2]. This delay can affect the quality and speed of medical decision-making especially during emergencies or when patients consult multiple specialists. To address these challenges blockchain technology

offers a secure and decentralized approach for managing medical records. Blockchain is a distributed digital ledger that stores information across multiple node, making it extremely difficult to modify or tamper with stored data[3]. Its key features include cryptographic encryption, immutability, transparency and decentralized consensus which together ensure data integrity and trust. In this proposed Medical Report Manager patients maintain full control over their encrypted health records and can grant or revoke access to doctors, hospitals and laboratories as needed. Hyperledger is particularly suitable for this purpose because it provides a permissioned blockchain environment where only authorized participants can access the network and execute smart contract[4]. Consequently, a blockchain-based Medical Report Manager represents a promising solution that enhances the security, authenticity, accessibility and patient ownership of electronic health records across multiple healthcare providers.

### 1.1 Medical Record Fraud and Data Integrity: A Growing Problem

Medical records are among the most valuable and sensitive forms of personal information because they contain details about a patient's health conditions, diagnoses, medications, laboratory reports, treatment history and insurance information. Accurate medical records are essential for making correct clinical decisions, ensuring continuity of care and protecting patient safety. When medical data is incomplete, altered or falsified it can lead to incorrect diagnoses, inappropriate treatments, insurance fraud and serious risks to both patients and healthcare providers. Healthcare organizations around the world face increasing challenges related to medical record fraud, unauthorized modifications and data breaches.. In addition duplicate records, missing information and inconsistent data across hospitals create major obstacles when patients receive treatment from multiple healthcare providers. In some cases laboratory reports, prescriptions or insurance documents may be intentionally manipulated which can result in financial losses and compromise patient trust.

There are several common forms of medical record fraud and data tampering[5]:

1. *Fabricated Medical Reports* – Completely fake prescriptions, laboratory results or diagnostic reports created to misrepresent a patient's condition.
2. *Modified Medical Records* – Genuine records that have been altered by changing diagnoses, treatment details, dates or patient information.
3. *Unauthorized Access* – Sensitive health information viewed or downloaded by individuals without patient consent.
4. *Duplicate or Inconsistent Records* – Multiple versions of the same patient's history stored across different institutions leading to confusion and treatment errors.
5. *Insurance Fraud Documents* – Manipulated medical documents used to support false reimbursement claims.

Patients frequently need to present their medical history when consulting specialists, changing hospitals, applying for insurance or seeking treatment abroad. In traditional systems, healthcare providers may spend significant time contacting previous hospitals or laboratories to verify the authenticity of reports. This manual verification process can take hours or days that delays diagnosis and increases administrative costs. During emergencies such delays can directly affect patient outcomes. Blockchain technology offers a powerful solution to these challenges by providing a secure and tamper-resistant platform for managing health records. In a Medical Report Manager based on Hyperledger patients retain ownership of their encrypted health records and can grant or revoke access to hospitals, doctors, laboratories and insurance providers[6]. Each medical document is cryptographically secured and recorded on the blockchain ensuring that reports are authentic, traceable and cannot be altered without authorization. This approach improves trust, reduces fraud and enables faster and safer sharing of medical information across healthcare providers.

## 1.2 Limitations of Traditional Medical Record Management Systems

Traditional methods for managing and verifying medical records have several important limitations. Most healthcare organizations store patient information in centralized databases or paper documents which are vulnerable to unauthorized access, data loss and tampering. These systems also provide limited control to patients over their own health records. The main limitations are described below:

- **Ownership:** Although medical records contain personal health information, they are usually controlled by hospitals and clinics rather than by patients. Patients often cannot directly manage or share their records.
- **Availability:** Paper records may be lost or damaged and digital records can become inaccessible due to system failures or institutional closure.
- **Dependence on Third Parties:** Sharing or verifying records often requires assistance from hospital staff, laboratories or other intermediaries.
- **Time Consumption:** Collecting and verifying medical reports from multiple healthcare providers can take several hours or days which delays treatment.

These limitations highlight the need for a secure and decentralized solution in which patients can control their encrypted health records and share them efficiently across healthcare providers using blockchain technology.

## 2. Need of Blockchain Technology

Blockchain technology provides a secure and transparent way to store and share medical records. Once a medical report is recorded on the blockchain it cannot be altered without authorization which ensures data integrity and authenticity[7]. Each transaction is digitally signed and time-stamped which creates a permanent audit trail of all access and updates. In a blockchain-

based Medical Report Manager patients control their encrypted health records and can grant or revoke access to doctors, hospitals and laboratories as needed. Smart contracts automate access permissions, reduces manual work and improving data sharing across healthcare providers. Thus blockchain enhances security, privacy, trust and efficiency in managing electronic health records.

### 2.1 Potential of Blockchain Technology

Blockchain technology has the potential to replace traditional paper-based and centralized methods of storing and sharing medical records. In a blockchain-based Medical Report Manager patients can securely store their encrypted health records and share them digitally with doctors, hospitals, laboratories and insurance providers. Because each record is linked to the blockchain and its authenticity can be verified instantly and any unauthorized modification becomes nearly impossible. The decentralized nature of blockchain eliminates the need for a single central authority to manage all patient data. Instead copies of the ledger are maintained across multiple authorized nodes, increasing reliability and preventing data loss. Cryptographic signatures and time-stamping ensure that every medical report is traceable, verifiable and permanently recorded. This is particularly important in healthcare where accurate and untampered information is essential for diagnosis and treatment. Using a permissioned platform such as Hyperledger access to medical records can be controlled through smart contracts which allow patients to grant or revoke permissions securely. Blockchain also supports all types of healthcare documents, including prescriptions, laboratory reports, diagnostic images and discharge summaries, regardless of their file format. Overall blockchain offers a powerful framework for securing, sharing, and verifying medical records while giving

patients full ownership and control over their health information.

### 3. Related Work

The healthcare industry is rapidly transitioning toward digital systems creating significant challenges in the secure management of electronic health records (EHRs). One of the major concerns is the unauthorized access, modification and misuse of sensitive patient information. Medical reports are commonly stored and shared through centralized databases and cloud platforms where data may be altered, duplicated or accessed without the patient's consent.

To address these issues blockchain technology provides a secure and tamper-resistant solution for verifying and managing medical records. Similar to certificate verification systems blockchain enables validation of the originality and integrity of healthcare data through cryptographic hashing and distributed consensus[12]. Studies by Tanzila Nargis demonstrate how blockchain can overcome limitations of traditional verification methods including ownership disputes, availability issues, high verification costs and delays. In the healthcare context this approach empowers patients to control encrypted medical reports to grant or revoke access to doctors and hospitals and ensure that all transactions are transparent, auditable and secure. As a result a blockchain-based Medical Report Manager offers a patient-centered framework for protecting privacy, improving interoperability and enabling trusted sharing of health records across multiple healthcare providers.

**TABLE 1.** A Thorough Analysis Of Previous Studies Based On A Blockchain Technology Parameter {R1:Smart Contracts R2:Hyperledger Fabric R3:Privacyand Security R4:SHA-256/Encryption R5:Patient-CentricAccess Control R6:Consensus Mechanism,--- Denotes Null

| citations | Key contribution                                                                                 | R1 | R2  | R3 | R4  | R5 | R6 |
|-----------|--------------------------------------------------------------------------------------------------|----|-----|----|-----|----|----|
| [1]       | Patient-centric blockchain framework for secure EHR sharing using IPFS and hybrid encryption.    | R1 | --- | R3 | R4  | R5 | R6 |
| [8]       | PREHEALTH framework using Hyperledger Fabric for privacy-preserving EHR management.              | R1 | R2  | R3 | --- | R5 | R6 |
| [9]       | Blockchain and edge-node architecture with AES encryption and access control for health records. | R1 | R2  | R3 | R4  | R5 | R6 |
| [10]      | Patient-owned EHR system for secure and interoperable data sharing across providers.             | R1 | --- | R3 | --- | R5 | R6 |
| [11]      | Hyperledger Fabric-based framework with usage control and time-limited access to health records. | R1 | R2  | R3 | R4  | R5 | R6 |
| [6]       | Generic patient-centered EHR management system with full patient control over record access.     | R1 | --- | R3 | R4  | R5 | R6 |

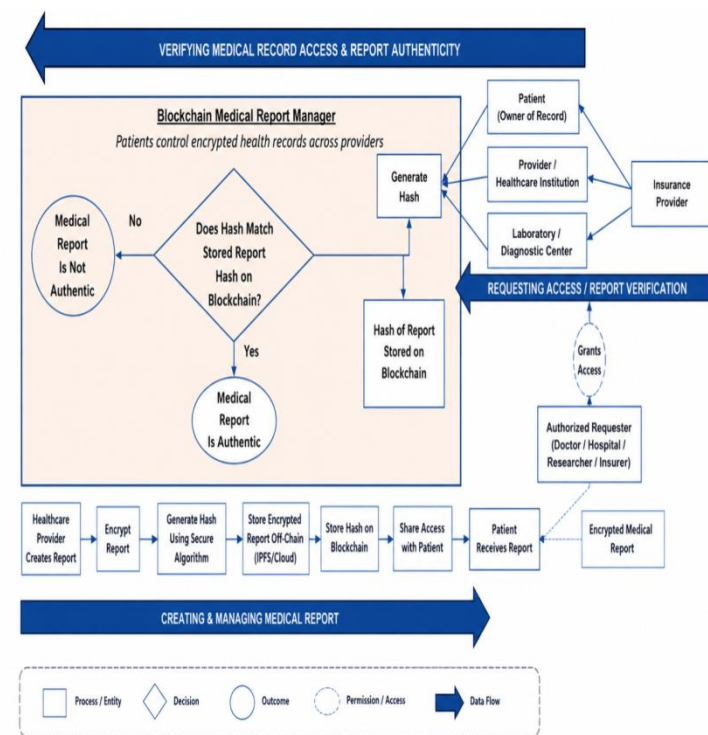
conversations}

Blockchain technology possesses several important characteristics including privacy, integrity, auditability, public verifiability, persistence, anonymity and trust anchoring. These properties make it highly suitable for managing sensitive healthcare information where data confidentiality and integrity are critical. In traditional Electronic Health Record (EHR) systems patient data are commonly stored in centralized databases making them vulnerable to unauthorized access, tampering and misuse. Blockchain addresses these concerns through decentralization, immutability and cryptographic techniques such as hashing and encryption ensuring that medical records remain secure and verifiable while giving patients greater control over their health information. Despite its advantages blockchain technology faces challenges such as high implementation costs, scalability issues, system complexity, privacy concerns and the need for continuous validation and consensus[13]. However many researchers have demonstrated its effectiveness in healthcare applications.. These studies demonstrate that blockchain-based smart contracts, encryption and consensus mechanisms that provide a secure and trustworthy foundation for healthcare data management. Table 1 presents a comparative analysis of these previous studies based on key blockchain technology parameters.

#### 4. Proposed Model For Medical Record Management

Healthcare organizations have grown significantly over time to manage the increasing number of patients, doctors, laboratories, pharmacies and insurance providers. Serving a large patient population and handling vast amounts of medical data have become challenging tasks for hospitals and clinics which creates operational difficulties for healthcare administrators and staff. This has gradually affected the efficiency and quality of healthcare services offered to patients. Several factors contribute to the reduced effectiveness of existing healthcare systems. One of the most important issues is the secure storage, sharing and verification of medical records and related documents. In traditional healthcare systems patient information is stored in centralized databases which are vulnerable to hacking, unauthorized

access and data loss. To address these challenges the proposed methodology shown in Figure 1 uses blockchain technology for secure medical report management. Blockchain is an advanced technology that can simplify the process of storing, verifying and sharing encrypted health records. The proposed system enables patients and healthcare providers to securely manage and verify medical reports across multiple institutions while ensuring privacy, integrity, and patient-centric control over healthcare data.



**FIGURE 1:** Block chain-based model for medical record management

#### 4.1 Discussion

Without accurate medical records doctors cannot provide effective diagnosis and treatment. Healthcare providers require authenticated patient information such as prescriptions, laboratory reports, and treatment histories. Hospitals and clinics are responsible for maintaining and validating these records for patients who require ongoing or emergency care. The verification and collection of medical reports from different healthcare institutions often takes a significant amount of time sometimes several hours or even days. Doctors and hospitals invest considerable effort in coordinating with laboratories, diagnostic centers and other institutions to obtain reliable patient information and deliver appropriate treatment. Verifying medical documents is a laborious but essential process to determine the authenticity and integrity of patient records. Blockchain is an emerging technology that can simplify medical record verification for both patients and healthcare providers. Cryptographically signed and encrypted digital documents such as prescriptions, test reports and discharge summaries can be securely stored and managed using blockchain technology[12]. These digital records improve file sharing, transparency and trust among hospitals, laboratories and medical authorities. Healthcare institutions can upload medical reports to a private blockchain network where only their one-way cryptographic hash is stored. Authorized doctors and hospitals can securely retrieve and verify these records when the patient grants permission through their digital credentials. This approach reduces verification time, prevents data manipulation and gives patients complete ownership and control over their encrypted health records across multiple healthcare providers.

#### 4.2 Analysis Of The Proposed Solution

Blockchain technology is a secure and decentralized system that combines important features such as hashing, encryption, peer-to-peer networking, timestamping and distributed storage. These technologies work together to provide a reliable platform for managing sensitive healthcare data. In the proposed Medical Report Manager using Blockchain these components are

used to securely store, manage and verify encrypted medical records across multiple healthcare providers. The theoretical model shown in Figure 1 explains the working of the proposed system.

- **Generating Encrypted Medical Reports**

In the proposed system, hospitals, laboratories, and diagnostic centers generate digital medical records such as prescriptions, laboratory reports, diagnostic images, discharge summaries, and treatment histories. Before storage, the medical records are encrypted to ensure that sensitive patient information remains confidential and protected from unauthorized access[14].

- **Hashing**

The system uses the SHA-256 hashing algorithm to generate a unique hash value for every medical report. The generated hash acts as a digital fingerprint of the file. Even a small modification in the report produces a completely different hash value, making it possible to detect any unauthorized changes in the data[12].

- **Timestamping**

Each uploaded medical report is assigned a timestamp that records the exact date and time of creation or modification. Timestamping helps maintain a chronological history of all medical records and improves transparency and traceability in the healthcare system.

- **Storage of Medical Records**

The encrypted medical reports are stored in decentralized storage such as IPFS (InterPlanetary File System). Instead of storing the complete file on the blockchain, only the cryptographic hash of the medical report and the IPFS reference are stored on the private blockchain. This approach reduces storage overhead while maintaining data integrity and security.

- **Verification of Medical Reports**

When a doctor, hospital, or laboratory needs access to a patient's medical history, the patient can authorize the request. The healthcare provider retrieves the encrypted report and verifies its authenticity by comparing the current hash value with the hash stored on the blockchain. If both values match, the report is confirmed to be original and unaltered.

- **Secure Sharing Across Healthcare Providers**

The proposed system allows secure and efficient sharing of medical records among multiple healthcare providers. Since the blockchain network is decentralized and tamper-resistant, it ensures that only authorized participants can access patient information while maintaining privacy, transparency, and trust throughout the healthcare ecosystem.

The current healthcare information ecosystem can be significantly improved by using blockchain technology to store and verify medical records without relying on a centralized intermediary. Medical reports such as prescriptions, laboratory results and discharge summaries can be encrypted and securely recorded on a private blockchain. Once stored, these records can be automatically verified and accessed by authorized healthcare providers across hospitals, laboratories and clinics. During the sharing process only approved information is revealed while patient privacy and confidentiality are preserved. Blockchain-based medical record management provides a

practical solution to problems such as data breaches, unauthorized access, repeated tests and manipulation of medical records. For a medical record to be useful, it must be authentic and maintain its integrity. The content must exactly match the original report issued by the hospital or laboratory and no unauthorized changes should be made. By ensuring authenticity, integrity and patient-controlled access blockchain enables secure and trustworthy sharing of encrypted health records across multiple healthcare providers.

#### 4.3 Benefit Of Proposed Model

The advantages of the suggested method for the patients, healthcare providers and hospitals are covered in this section. The following illustrates how the suggested model would specifically benefit patients and healthcare organizations:

##### *Granting Benefits to Healthcare Authorities*

- Only encrypted and tamper-proof medical data is shared through the blockchain.
- All medical reports are securely stored and can be easily retrieved when required.
- Hospitals and laboratories do not need to spend extra time sending records manually to different providers.
- Healthcare institutions can securely issue, store and share authenticated medical records.
- Since all transactions are recorded on the blockchain records cannot be lost or altered.
- Authorized healthcare providers can access and verify records at any time with patient permission.
- There is no need to maintain multiple copies of the same report in different systems.

##### *Advantages for Patients and Healthcare Providers*

- Patients own and share encrypted medical records securely.
- All prescriptions, test reports and treatment histories can be managed in a single digital wallet or application.
- Doctors, hospitals, and laboratories can securely participate in the online verification process.
- Blockchain transactions ensure that records are permanently available and cannot be lost.
- Medical reports can be accessed and shared at any time from authorized devices.
- The system can be easily integrated to verify and retrieve the most recent version of any medical record.

## 5. Implication Of The Findings

Based on the provided context, here's a table outlining the implications for the work on aBlockchain-based medical report management framework, followed by the challenges and future directions:

**TABLE 2:** Implications of findings in blockchain technology for document verification in education sector

| Implications | Explanation                                                                                                                                             |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| Security     | Medical records can be securely stored and verified on blockchain, reducing the risk of hacking, data breaches and unauthorized modifications.          |
| Efficiency   | Blockchain streamlines the sharing and verification process, making access to medical reports faster and less labor-intensive than traditional methods. |

|                  |                                                                                                                                                     |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| Decentralization | The decentralized storage of medical records reduces dependency on a central authority and increases trust among patients and healthcare providers. |
| Transparency     | Blockchain ensures that all transactions and access activities are visible and traceable, improving accountability and auditability.                |
| Verification     | Medical reports can be instantly verified to confirm their authenticity and integrity before being used for diagnosis and treatment.                |
| Interoperability | Blockchain enables secure sharing of patient records across hospitals, laboratories, clinics, and insurance providers.                              |
| Patient Control  | Patients gain full ownership of their encrypted health records and can grant or revoke access to authorized healthcare providers.                   |

## 6. Conclusion And Future Work

To improve the management and verification of medical records this study proposes a blockchain-based Medical Report Manager that enables patients to control encrypted health records across multiple healthcare providers. The proposed system reduces the risk of data breaches, unauthorized modifications and misuse of sensitive health information while providing enhanced security, authenticity, privacy and patient-centric access control. One of the main advantages of the suggested model is that all information required for validating and verifying medical reports is securely maintained on the blockchain along with encrypted off-chain storage. Doctors and hospitals do not need to repeatedly contact the issuing laboratory or hospital to confirm the authenticity of a report they only need to verify that the current hash of the medical record matches the hash stored on the blockchain.

If both values match the report is considered original and unaltered. The proposed model can initially be implemented in selected hospitals and diagnostic centers and later expanded to larger healthcare networks. In future the system can be enhanced with smart contract-based automation to further improve access control, interoperability and secure sharing of medical records across multiple healthcare providers.

## 7. References

- [1] M. A. Rahman, M. Shamim Hossain, M. S. Islam, N. A. Alrajeh, and G. Muhammad, "Secure and provenance enhanced internet of health things framework: A blockchain managed federated learning approach," *IEEE Access*, vol. 8, pp. 205071 – 205087, 2020, doi: 10.1109/ACCESS.2020.3037474.
- [2] M. George and A. M. Chacko, "Health Passport: A blockchain-based PHR-integrated self-sovereign identity system," *Front. Blockchain*, vol. 6, 2023, doi: 10.3389/fbloc.2023.1075083.
- [3] A. Sahoo, R. K. Lenka, S. R. Mallick, and P. K. Tripathy, "Blockchain Applications in IoT-based Healthcare System- A Review," in *OCIT 2023 - 21st International Conference on Information Technology, Proceedings*, R. L., R. N.K., S. D.S., and R. J.K., Eds., Institute of Electrical and Electronics Engineers Inc., 2023, pp. 303 – 308. doi: 10.1109/OCIT59427.2023.10430704.
- [4] K. K. Hiran, R. Doshi, and M. Patel, *Modern technology in healthcare and medical education: Blockchain, IoT, AR, and VR*. IGI Global, 2024. doi: 10.4018/979-8-3693-5493-3.
- [5] Suman and A. Bhatia, "Blockchain based graduation certificate verification framework: Ensuring security and authenticity in educational documents," *AIP Conf. Proc.*, vol. 3325, no. 1, p. 30045, Oct. 2025, doi: 10.1063/5.0291763.
- [6] S. K. Verma, M. Nadeem, V. Verma, M. A. Sayeed, A. Agrawal, and R. A. Khan, "Blockchain Application in Healthcare Domain: Industry 5.0 Perspective," in *Proceedings of International Conference on Contemporary Computing and Informatics, IC3I 2023*, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 208 – 215. doi: 10.1109/IC3I59117.2023.10397614.
- [7] Suman and A. Bhatia, "Unleashing the Potential: A Bibliometric Analysis of Blockchain Applications in Education (2016-2024)," *2024 4th Int. Conf. Adv. Electron. Commun. Eng. AECE 2024*, no. November 2024, pp. 887–892, 2024, doi: 10.1109/AECE62803.2024.10911681.
- [8] X. Tang, B. Zhuang, Y. Yao, and X. Dong, "Research on high-reliability intelligent-sensing health service support platform and key technologies based on biometrics and blockchain security technology," in *ACM International Conference Proceeding Series*, Association for Computing Machinery, 2021, pp. 2514 – 2518. doi: 10.1145/3482632.3487461.
- [9] J. Gambril, C. Boyd, and J. Egbaria, "Application of Nonfungible Tokens to Health Care. Comment on 'Blockchain Technology Projects to Provide Telemedical Services: Systematic Review,'" *J. Med. Internet Res.*, vol. 24, no. 5, 2022, doi: 10.2196/34276.
- [10] H. K. Bella and S. Vasundra, "Healthcare Intrusion Detection using Hybrid Correlation-based Feature Selection-Bat Optimization Algorithm with Convolutional Neural Network A Hybrid Correlation-based Feature Selection for Intrusion Detection Systems," *Int. J. Adv. Comput. Sci. Appl.*, vol. 15, no. 1, pp. 671 – 679, 2024, doi: 10.14569/IJACSA.2024.0150166.
- [11] S. S. Rath and M. P. P. Jagadeesh, "Enhancing data security in SAP-enabled healthcare systems with cryptography and digital signatures using blockchain technology," *Int. J. Syst. Innov.*, vol. 8, no. 1, pp. 36 – 48, 2024, doi: 10.6977/IJoSI.202403\_8(1).0004.
- [12] Suman and A. Bhatia, "A Blockchain-Based Framework for Securing Digital Documents Using Off-chain Attribute-Based Encryption," *2024 2nd Int. Conf. Comput. Charact. Tech. Eng. Sci. IC3TES 2024*, no. November 2024, pp. 1–6, 2024, doi: 10.1109/IC3TES62412.2024.10877427.
- [13] A. L. Michala, H. Attar, and I. Vourganas, *Secure Data Transfer and Provenance for Distributed Healthcare*. Springer Nature, 2022. doi: 10.1007/978-981-16-8150-9\_11.
- [14] P. Narsimhulu and R. Sahay, "Federated Learning-based Techniques for Healthcare IoV: Challenges and Future Directions -A Knowledge Review," in *2024 IEEE 9th International Conference for Convergence in Technology, I2CT 2024*, Institute of Electrical and Electronics Engineers Inc., 2024. doi: 10.1109/I2CT61223.2024.10544256.