International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 6, 2025
https://theaspd.com/index.php

Lightweight Cryptographic Protection of Sensitive Data Using ECDSA in a Blockchain-IPFS Architecture

Vandana V1, Dr.S Veni2
[1]Research Scholar Department of Computer Science, Karpagam Academy of Higher Education, Coimbatore, India, vandanavijayan7@gmail.com
[2]Professor Department of Computer Science, Karpagam Academy of Higher Education, Coimbatore, India, venikarthik04@gmail.com

ABSTRACT
Health-care is undergoing a considerable digital shift in the present state, which is driven by the rise of new technologies and the changes taking place globally. The movement is rebalancing the provision and availability of health care, at the same time that it highlights the importance of protecting confidential information about patients. Coupled with the cryptographic primitives, blockchain technology provides a formidable answer, as it promises to improve data integrity using decentralized processes.
In this paper, a hybrid blockchain-based EHR management and security solution to Electronic Health Records (EHRs) is described. Having considered the drawbacks of the blockchain in its ability to work with large files the system is connected with Ethereum blockchain through Ganache and program construction tools is equipped with the InterPlanetary File System (IPFS). In the hybrid model, one does store each row hash (unique identifier) of the patients records on the blockchain, but one does not store the actual data on the blockchain, instead on IPFS. A Decentralized Application (DApp) built on the programing language of Ethereum, Solidity, and the web3.js interface also allows secure data access via cryptocurrency wallets like MetaMask.
The use of smart contracts is deployed to process transactions to achieve transparency and verifiability. To enhance security the Elliptic Curve Digital Signature Algorithm (ECDSA) is adapted to provide unauthorised access. Results of simulation reveal that a suggested method is reliable in providing patient data security, maintain immutability, and secure exchange of data. The approach promotes transparency within the digital health-care systems and strengthens the stakeholder belief by allowing a decentralised structure of these systems.
Keywords: Blockchain, Etherum, InterPlanetary File System, Smart Contract, MetaMask,ECDSA

INTRODUCTION

The sheer advancement of technology has significantly changed the face of healthcare and homecare practice, mostly coinciding with the introduction of new-fangled solutions, which, besides securing the experience, enhance the level of user experience to a new degree. Among the most crucial areas of change relates to safe handling and storing of electronic health records (EHRs), which has been a complex issue long associated by inquiries regarding data integrity, confidentiality, and accessibility. The traditional systems, which included the use of paper or manual record keeping systems, had tendencies to fail because of errors, redundancy and inefficiency in organizations thus, undermining the accuracy and confidentiality of the patient data.

The blockchain technology provides a strong solution roadmap to deal with these challenges. Blockchain also offers security to sensitive medical data and its integrity and confidentiality by allowing distribution and storage of data that is not susceptible to changes and tampering. The capacity is most relevant particularly in homecare and hospital facilities where they work in an environment that requires sharing of data seamlessly over platforms and geography to deliver appropriate diagnosis and treatment.

Current EHR systems have all the abilities of scheduling appointments, quick access to test results, wearable EHR equipment, among other aspects, which are also installed with blockchain solutions. Such systems have been embraced by most health institutions across the globe due to their effectiveness in enhancing the quality of the data collected, reducing medical errors, and positively impacting patient outcomes. The combination of blockchain and the EHR systems is thus an important step towards the provision of secure, efficient and interoperable healthcare delivery.
The use of blockchain is one of the sources of securing personal medical records. Since it is decentralized,

it records and runs things over the network and does away with the use of intermediary parties. All data in the block chain are secured through modern cryptographic methods and stored in the blocks. In this cryptographic form of structure, it is through this that the blocks are connected to each other in such a form that changes are not possible. In case data in one block is changed then this will result in the consequences to all the succeeding blocks and thus re-compute the hash values of the blocks. Therefore, the attackers would find it necessary to execute the hash values of the block chain. This task would consume computational complexities that makes such manipulation out rightly impossible.

Available studies that have attempted to explore how block chain technology can be used in safeguarding medical records of patients, verify that it can guarantee integrity of the medical records, hence enhancing the overall information security. According to findings, medical records under lock and key of the blockchain network are secured, unchangeable, and accessible to only participants with the necessary access credentials.

LITERATURE REVIEW

The researchers, Andi et al. (2022, p. 1), have presented evidence-based approach to reinforcing the security of medical records of COVID-19 patients. It is also critically examined that there are limited facts obtained on blockchain applications in the health sector as the literature review unveils no significant research to test the security of medical record storage using blockchain (Andi et al., 2022, p. 2). The proposed model can fill this gap because it also uses ECDSA to provide access control issue pertinent to blockchain in preserving the integrity of data (Andi et al., 2022, p. 2). This is then followed by an elaborate introduction of DSA, ECDSA, and the elliptic curve cryptography and why ECDSA is better than RSA or ElGamal (Andi et al., 2022, p. 4). There is the discussion of the evolution of blockchain technology and various reactions to it, in the field of medical records security in particular (Andi et al., 2022, pp. 4 5). The simulation of the ECDSA proves that medical records encrypted with a public key could only be deciphered by authorized users with the adequate public key (Andi et al., 2022, pp. 6677). In the following blockchain simulation with a Proof-of-Work (PoW) algorithm, it is observed that modifying one of the blocks starts a long mining procedure that requires revalidation of the whole chain, thus discouraging data tempering (Andi et al., 2022, pp. 78. The results support the conclusion that the security standard of the model is high, which can be discussed in the context of both scholarly and practical research of secure storing of medical records with a small number of records 10,000 ones.

The use of centralized storage systems is the typical way to manage the archiving of sensitive patient data but the arrangement has a substantial privacy liability impact and places the data at the risk of single-point failure. Kumar and Tripathi of the National Institute of Technology, Raipur, analyse these weaknesses and underline the worth of keeping things safely and publicly and in a decentralised way (2020, p. 1).The authors suggest the solution to these drawbacks: a hybrid on-chain off-chain storage model (Kumar & Tripathi, 2020, pp. 1 2). The content-addressed hashes of diagnostic reports, prescriptions, and other data are stored in the form of a tamper-proof log on the blockchain, as the consortium-style network (Kumar & Tripathi, 2020, p. 2). At the same time, the real reports are located on IPFS distributed network. The solution reduces scalability challenges caused by putting huge data on a blockchain (Kumar & Tripathi, 2020, p. 2). In the consortium blockchain, the data can be accessed by authorized healthcare providers (peers), and a peer authorization procedure based on a proof-of-identity (PoI) is enabled (Kumar & Tripathi, 2020, pp. 2-3).

The paper of Saini et al. (2021) proposes a new access-control model of electronic medical records (EMRs) in a smart-healthcare layout consisting of cloud and fog. The authors start by reviewing the deficiencies of centralized systems, mentioning that single points of failures can be observed and the capacity of patients to work with their own data could be limited (Saini et al., 2021, p. 1). They are proposing a solution where smart contracts in a blockchain are used to monitor the access privileges in a decentralized and secure fashion (Saini et al., 2021, p. 1).Centralized EMR solutions have always demonstrated weaknesses, insufficient transparency, and datacontrol that is limited to the patient side (Saini et al., 2021, p. 1). Access-control frameworks that are popular in the mainstream, i.e. DAC, RBAC, ABAC, and CaBAC, rely on centralized authorities, which creates a unified point of failure (Saini et al., 2021, p. 1). Even though it has decentralized options, usually, this solution is based on cloud-based access policy rather than transparency, which in most cases harms security (Saini et al., 2021, p. 1). The described architecture includes patients, hospitals, smart-healthcare devices, medical-control units

(MCUs) and a cloud server (Saini et al., 2021, p. 3). EMRs are being encrypted with Elliptic Curve Cryptography (ECC) and are placed in the cloud, whereas their hashes and index numbers are stored in blockchain (Saini et al., 2021, p. 2). The given hybrid topography is the creation that aims at uniting harsh security requirements and scaling limits within a clearcut dimension (Saini et al., 2021, p. 2).

Particularly, Mishra et al. (2025), hereinafter referred to as Mishra 2025, suggests a resource framework of the secure and privacy-preserving management of Electronic Medical Records (EMRs) through integration of the blockchain technology with the InterPlanetary File System (IPFS). The discussion highlights the inadequacies of the existing centralized paradigms of storage of EMR excluding its vulnerability to security compromise, privacy infringement, and inability to be as transparent as possible. It is further argued that patients do not normally have any control over the organizations accredited with access of their EMRs or use to which the data is put. Responding to the same, Mishra 2025 provides the elaborate prototype architecture that incorporates blockchain and IPFS to infuse decentralized governance of EMR.Their system uses a hybrid approach: the data of patients are encrypted and stored to IPFS, but the respective cryptographic hashes are appended to the blockchain. This organization removes the burden of storage on the blockchain and at the same time provides integrity of the data.
In contrast, the study by Nishi et al. (2022) hereafter Nishi 2022 promotes the paradigm of blockchain-based Electronic Health Records (EHRs) protection. Focusing on the flaws that exist in the current centralized EHR frameworks, authors plan to support the security, privacy and data availability concerns by using the decentralized and tamper-proof approach. Applied in Ethereum, the framework offers smart contracts operating together with IPFS to store the data of EHR metadata and to execute granular access control, thus, balancing high robustness with scalability.
[Faroug and Demirci (2021)](https://doi.org/10.1145/3449914) examine the prospects of blockchain technology that can enhance the security and performance of Electronic Health Record (EHR) systems. Focused on the susceptibility of the centralised EHR infrastructures to information breaches and loss, the article claims that the security of blockchain and its immutability help to secure and share the sensitive medical data, including the vaccination records. Thereby, it describes two EHR applications based on blockchain and analyses them. The former, which is based on Hyperledger Fabric, must be used to manage EHR in general; the latter, which is coded on Ethereum, is supposed to track the records of vaccinations.
[Abouali et al. (2022)](https://doi.org/10.1145/3539028) seek to affect the issues of patient medical record transfer (PMRT) that are currently highlighted by the pandemic of the COVID-19. The pandemic exposed flaws in interoperability, increased cyberattacks and the vulnerability in such systems dealing with centralised data storage. In line with this, the authors introduce a blockchain-conceptualized framework that the authors believe gives control of the medical data of patients completely to them which further increases security and privacy. They are inspired by the need to have a safer, transparent and efficient PMRT system that is going to solve the existing loopholes of inefficiency of the system, maintain the privacy of patients and advance patient care by bringing together the various medical systems into a common system.
According to Riadi et al., (n.d., p. 1) explore vulnerabilities revealed by Electronic Health Record (EHR) systems over the long term of the COVID-19 pandemic, particularly that of data integrity and data security breach. The authors then put forward general outline with a combination of blockchain technology and the InterPlanetary File System (IPFS) should be used to increase data protection and give patients more control over their records. The article proposes an effective and thoroughly tested solution to enhancing security and integrity of EHR systems by implementing blockchain and IPFS covering the most dangerous holes in security highlighted by the pandemic. Despite the fact that the framework also has its limitations, it proposes an interesting potential of further development and application in terms of the healthcare facilities.
Muhaimin Aziz et al. (n.d) have published the current technical report in order to explore how IPFS (InterPlanetary File System) can be merged with Ethereum smart contracts in order to develop a more effective way to manage and store data. The authors mark the drawbacks of using blockchain networks as a large-scale data storage only high costs and lack of scale. They devise a hybrid system whereby the hash of the data can be stored on the Ethereum block chain but the complete data set on the decentralized IPFS block chain. The discussion will start with the identification of the disadvantages of

conventional contracts and the benefits linked with the Ethereum smart contracts, especially their ability to enable secure and transparent transactions. The authors, however, denounce the problem of scalability as well as cost that emerges by trying to bring large volumes of data directly to the blockchain. They are therefore proponents of a mixed design, one that brings together the security assurances, provided by Ethereum, with the cost-effective storage of large volumes, provided by IPFS.
The following review part of the paper is a survey of the previous research on blockchain technology (Muhaimin Aziz et al., n.d., pp. 3) Ethereum smart contracts (Muhaimin Aziz et al., n.d., pp. 3), and IPFS (Muhaimin Aziz et al., n.d., pp. 46). All the technologies are discussed in detail covering blockchain consensus mechanisms, Ethereum virtual machine (EVM), and the distributed file system structure of IPFS. Along with this, it is seen that the authors have presented the CIA triad (Confidentiality, Integrity, Availability) to secure data (Muhaimin Aziz et al., n.d., pp. 6 7) and the Quality of Service (QoS) metrics namely throughput, packet loss and delay that will be used to evaluate the performance (Muhaimin Aziz et al., n.d., pp. 6 7).

According to the proposal given by Jahir Pasha et al. (2024), the system is a structure meant to manage electronic health records (EHRs) within home-care settings by embedding Ethereum blockchain into other elements that intern increase security and efficiency of operations. By stipulating that their discussion is limited to the drawbacks of the currently existing EHR models, the authors specifically mention shortcomings in the home-care models that fail to prioritize record security as the hospital-based IT systems by contrast (Jahir Pasha et al., 2024). Realistic protection measures on the integrity of data have not been found where clinicians have a tendency of sending sensitive data through email or other unencrypted media (Jahir Pasha et al., 2024). The primary goal of the proposed research is to enhance the security and accessibility of patient data, and this project attempts to meet the above purposes relying on a blockchain network. The main benefits, which are linked to this model, are, namely, transparency, immutability, and strong anti-tampering resistance (Jahir Pasha et al., 2024). To acknowledge the fact that it is simply too expensive to store all very large datasets in a fully on-chain storage, the authors suggest using IPFS (InterPlanetary File System) as a data storage repository, and only the data hashes to be written on the Ethereum blockchain (Jahir Pasha et al., 2024).

METHODS & MATERAILS

a) Elliptic Curve(EC)

Elliptic curve is a mathematical term that represents a curve the definition of which is determined by the equation

$$y^2 = x^3 + ax + b$$

Elliptic curves sit in the centre of cryptographic study and protocols based on elliptic curves include key exchange, digital signatures, and public-key encryption. Therefore, the choice of an elliptic curve has a conclusive impact on security of the system where it is being used.

b) Elliptic Curve Cryptography (ECC)

Backing the patient medical records is the Elliptic Curve Cryptography (ECC). Elliptic curve cryptography (ECC) is a type of public-key cryptography based on elliptic curves mathematics and serving as a contemporary, computationally-efficient substitute to old fashioned cryptography approached (e.g., RSA and DiffieHellman) giving the same level of protection as those old methods but with a much smaller key length. A user creates a pair of keys comprising a point on an elliptic curve and its corresponding point on the curve; the first one can be shared, whereas the second one should be kept secret. Security is based on the impracticality of an attempt to invert the public key and retrieve the private one. ECC finds use in secure communication schemes, digital signature algorithms and encryption schemes and its computational requirements, as well as its use of smaller key sizes compared to other systems, makes it particularly interesting in low resource environments.

c) Elliptic Curve Digital Signature Algorithm (ECDSA)

In 1992, Scott Vanstone proposed Elliptic Curve Digital Signature Algorithm (ECDSA) to resist the manipulation of data as well as maintain data integrity. Such a proposal was as a result of the National Institute of Standards and Technology, requesting the general public comment, regarding its DSS draft. Later in 1998 the scheme was formalized by the International Standards Organization (ISO) as ISO

14888-3, in 1999 as an American National Standards Institute (ANSI) standard as ANSI X9.62, and in 2000 as an Institute of Electrical and Electronics Engineers (IEEE) standard as IEEE 1363-2000 and a Federal Information Processing Standard (FIPS) as FIPS 186-2. The revision of the FIPS 186 of 2009 confirmed the FIPS status as the ECDSA. Both techniques rely on Discrete Logarithm (DPL) issues, and this one is an extension of DSA(Andi et al., 2022, p. 1). But the ECDSA method makes use of a collection of curve points, Moreover, the generating key is little. There are three steps in this method.

- **Key generation:**

1) Select a random or pseudorandom integer d in the interval [1, n–1].
2) Compute Q = dG
3) Public key is Q, private key is d.

- **Signature generation:**

1) Select a random or pseudorandom integer k, $1 \leq k \leq 1$.
2) Compute kG = (x1, y1) and convert x1 to an integer $\overline{x}$.
3) Compute r = x1 mod n. If r = 0, go to step 1.
4) Compute $k-1$ mod n.
5) Compute SHA-256(m) and convert this bit string to an integer e.
6) Compute $s = k-1(e+dr)$ mod n. If s = 0, go to step 1.
7) Signature for the message m is (r, s).

- **Signature verification:**

1) Verify that r and s are integers in the interval $[1, n - 1]$.
2) Compute SHA-256(m) and convert this bit string to an integer e.
3) Compute $w = s-1$ mod n.
4) Compute u1 = ew mod n and u2 = rw mod n.
5) Compute X = u1G + u2Q.
6) If X = Θ, reject the signature. Otherwise, convert the x-coordinate, x1 of X, to an integer $\overline{x}1$, and compute $v = \overline{x}1$ mod n.

d) IPFS

Peer-to-peer distributed file systems like IPFS enable all computing devices to share a single file system. It is currently difficult to store significant quantities of data on the blockchain since each block only contains around 1MB of data. A public key is used to encrypt the symmetric key that is used to encrypt the data that is uploaded to IPFS. Peer-to-peer file sharing is just one use for IPFS; it may be used for other purposes as well. The InterPlanetary Name Server (IPNS), a distributed substitute for a centralized DNS system, is one example. The IPFS network returns hash codes that a user can use to view a webpage stored on IPFS. The Ethereum blockchain natively supports IPFS, a decentralized massive data storage system that is compatible with smart contracts. CIDs, or content identifiers, are labels used to identify material on IPFS. It creates an address based on the content itself, even if it doesn't display the location of the content's storage. Although it supports alternative hash algorithm types, IPFS defaults to using the SHA-256 method. The SHA-256 technique is still used in this study for IPFS data uploads.

e) Smart Contract

A smart contract encompasses executable code that facilitates, implements, and enforces the stipulations embedded in the agreement for parties that may be deemed untrustworthy. A smart contract possesses the capability to execute autonomously upon the fulfillment of the conditions delineated within the contract. A smart contract mandates rigorous regulations among the parties engaged in the Ethereum blockchain network without any form of external intervention. Smart contracts expand the functionality of blockchain technology to establish protocols for peer-to-peer collaboration [30]. Each smart contract is equipped with a public interface that can manage pertinent events. This interface is activated by transactions containing the appropriate payload data, and all legitimate transactions are meticulously documented within the block chain.

f) Ethereum

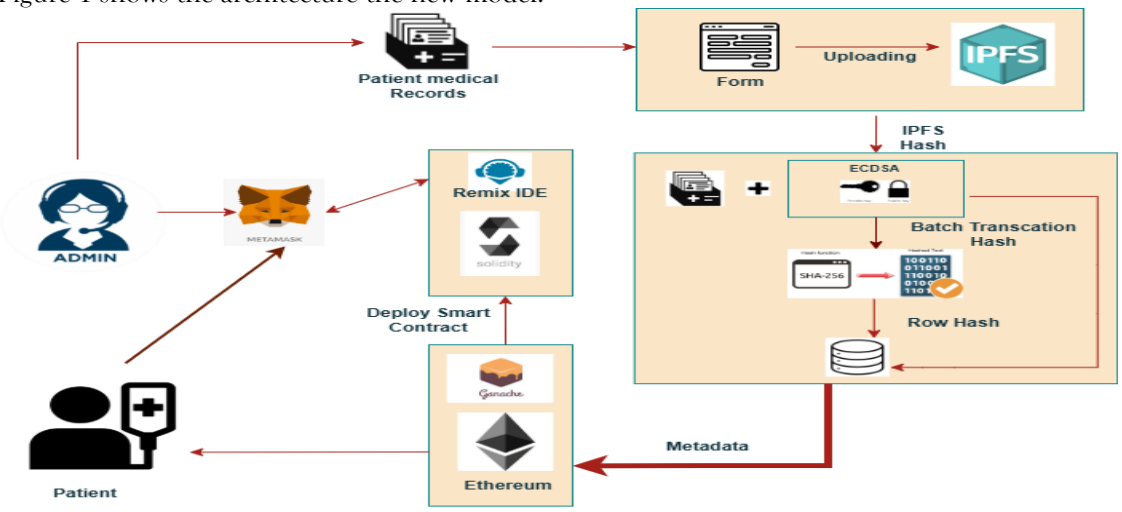
Ethereum represents a singular network that employs a decentralized blockchain technology characterized by the utilization of smart contracts, which is both open-source and programmable in nature. It operates as a global consortium of computational units collaborating to construct a supercomputer capable of creating, managing, and executing decentralized digital applications, commonly referred to as “dapps”.

Smart contracts facilitate the members of the Ethereum blockchain network to engage in agreements and conduct transactions directly, thereby eliminating the necessity for intermediary third parties. The network is associated with its own cryptocurrency, designated as Ethers. This cryptocurrency serves the purpose of enabling transactions between accounts that are interconnected within the Ethereum blockchain network.Ethereum possesses a distinct programming language specifically tailored for the creation and deployment of smart contracts, known as Solidity. This programming language is classified as a high-level language with a contract-oriented feature. Solidity draws its influences from the paradigms of C++, Python, and Javascript, and is meticulously designed for optimal use within the Ethereum blockchain.

IMPLEMENTATION

The study introduces an innovative framework that integrates blockchain technology alongside the ECDSA algorithm to enhance the security of medical records. This proposed model represents a significant advancement over the methodologies and frameworks put forth by prior scholars. The dataset used in the research is taken from https://synthea.mitre.org/downloads . The proposed model

Figure 1 shows the architecture the new model.



of

Fig 1: Proposed Model Architecture

Ethereum is a platform that functions as a contemporary blockchain. The cryptocurrency known as Ether (ETH) is based on this community-driven technology, which also offers a wide range of instantaneous applications. Ethereum is a leading platform for Web3 development because of its innovative smart contract technology, sizable developer community, well-established ecosystem, robust security and decentralization, interoperability standards, ongoing development initiatives, and broad enterprise adoption. Through the use of Ethereum and IPFS, we were able to make data sharing safer, more effective, and patient- focused.

IPFS makes sure that the real data is saved effectively and securely, while Ethereum's smart contracts may control consent and permissions. Medical data may be distributed across several nodes for decentralized storage using IPFS.Because of this, the system is extremely scalable and can manage massive data volumes without the need for centralized servers. The Ethereum platform is used in the system's design. A Solidity smart contract is created to communicate with a PyCharm application using web3.js in order to test the system. We use Ganache to operate a local blockchain network, the Ethereum Remix IDE to debug the smart contract, and the MetaMask wallet to log in.

The process begins by hashing the entire CSV file using a cryptographically secure algorithm like SHA-256, generating a file-level hash. This hash is then signed using the Elliptic Curve Digital Signature Algorithm (ECDSA) with a private key, creating a digital signature verifiable using the corresponding public key. Both the hash and signature, along with the public key, are stored on the Ethereum blockchain. This provides a tamper-evident record of the file's existence and integrity at a specific point in time. Furthermore, each row within the CSV undergoes a similar process: individual SHA-256 hashing, ECDSA signing, and storage of the hash, signature, and public key on the Ethereum blockchain that appears in the Fig 5. This granular approach allows for verification of individual row integrity, enhancing the overall security and auditability of the data. The CSV file itself is uploaded to the InterPlanetary File System (IPFS), a decentralized storage network as shown in Fig 2, providing a persistent and readily accessible copy. Optionally, metadata including the IPFS hash and a timestamp can be stored, providing further context and traceability that is shown in Fig 3. This multi-layered approach leverages the strengths of blockchain technology for immutability and cryptographic techniques for data integrity, offering a high level of security and transparency for the CSV data. Tests are conducted to determine how the quantity of blocks and security difficulty targets relate to one another level, which is shown by mining time in the event that the block changes. We call this testing procedure Proof of Work (POW) as shown in Fig 14.

Fig 2:Uploading File to IPFS

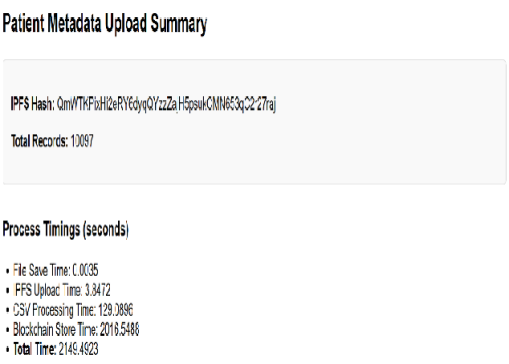


Fig 3:Hash generated from IPFS

When a CSV file is uploaded, it is stored, uploaded to IPFS using Pinata for decentralized storage, and its IPFS hash is obtained. After that, an Ethereum private key is used to hash and cryptographically sign each row of the CSV file as appears in Fig 5. The public key and signature are produced.In order to enable on-chain data authenticity verification, these signed data records are then batched that is shown in Fig 4 and committed as transactions to a deployed smart contract on a local Ganache blockchain. The program provides a transparent and verifiable data management system by carefully monitoring and displaying performance parameters, such as the time required for file operations, IPFS upload, CSV processing, and blockchain transactions as shown in Fig 3, in addition to the transaction hashes and gas use.

Fig 4:Batch Transaction Hashes

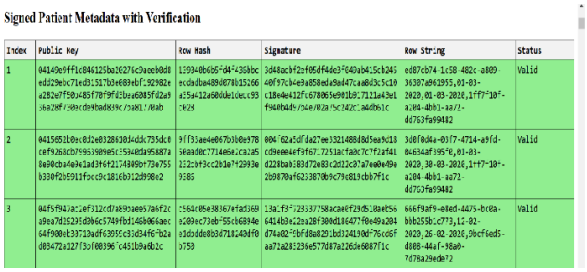


Fig 5: Each row in the file is hashed

Individual patients can authenticate their data by submitting a specific row hash using the "patient" gateway as shown in Fig 7. The program searches the blockchain for a matching record, extracts its important information (public key, row hash, signature, and verification status), and compares it with

the IPFS-hosted CSV to display the pertinent patient data.
Auxiliary functions allow consistent data normalization (e.g., converting hexadecimal characters to lowercase without the '0x' prefix) so that user input, on-chain data, and IPFS data may be precisely compared. This framework provides an open, verifiable process for confirming the validity and integrity of medical records

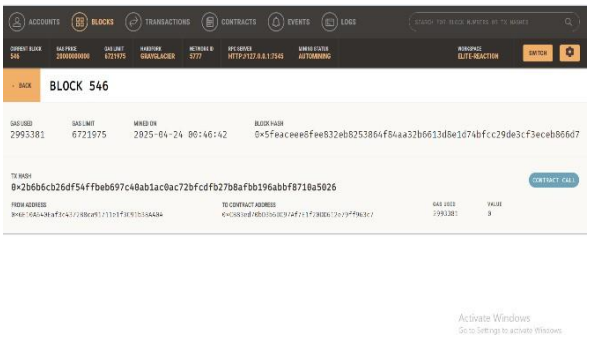


Fig 6:Contract Call

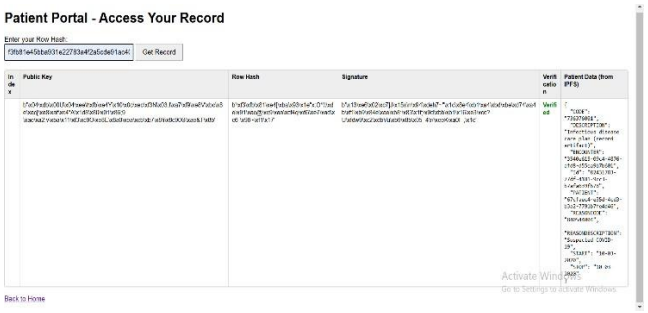


Fig 7:Patient Record

Utilizing a local Ethereum blockchain (Ganache) and a CSV file hosted on IPFS, the application serves as a data validation gateway, enabling the review and verification of patient records. It connects to a pre-configured smart contract, whose Application Binary Interface (ABI) is retrieved from a JSON file, and uses it to obtain digital signatures, row hashes, and public keys that have been saved. Additionally, using IPFS hash, simulation can accesses and parses a particular CSV file from an IPFS gateway to obtain the original patient data. In addition to displaying the verification status of each record's signature, the site displays all blockchain records and integrates them with the matching patient data obtained from the IPFS CSV as appears in Fig 8.

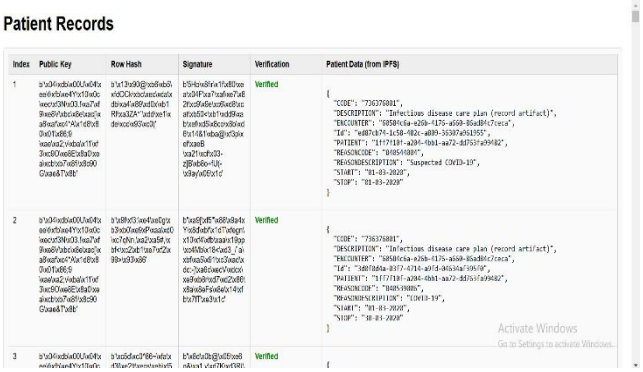


Fig 8:Patient Record View by Verifying ECDSA

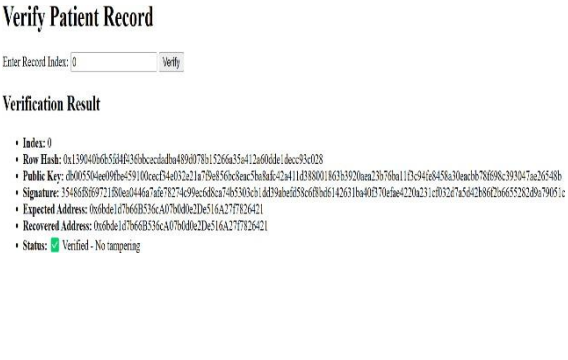


Fig 9:Verifying the patient records

RESULT & DISCUSSION

The temporal durations associated with batch processing tend to consistently oscillate within the range of approximately 19 to 20 seconds show in fig: 10, which serves to indicate a performance that remains remarkably stable and uniform across the vast majority of the 101 batches that were examined during this analysis. Although it is evident that the preponderance of the batches resides comfortably within this relatively narrow temporal spectrum, there do exist certain anomalies, notably exemplified by Batch 1 and Batch 35 that have recorded processing times that are conspicuously elevated in comparison to the rest of the data set. The processing demonstrates a propensity to uphold a processing speed that is relatively constant for each individual batch processed. In summary, the overall performance metrics reveal a commendable degree of consistency throughout the execution of the

batches, with only sporadic deviations observed, which are indicative of minor fluctuations in the execution times associated with the batches in question.

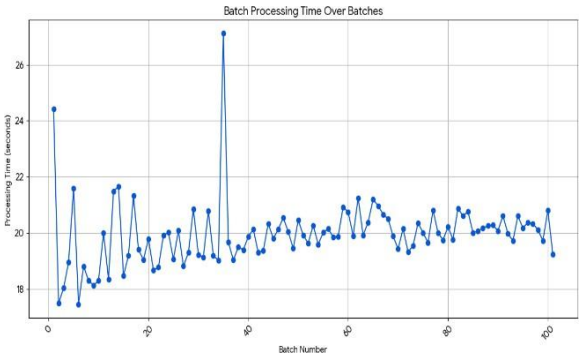


Fig 10:Batch Processing Time

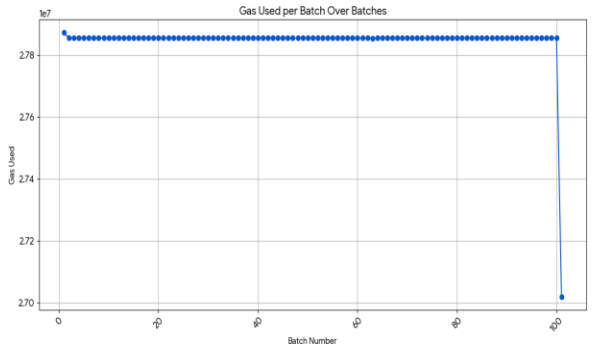


Fig11:Gas used for each batch

The fig:11 illustrates the remarkably consistent levels of gas consumption exhibited across the majority of the batches, while simultaneously highlighting a particularly striking and abrupt decline in gas usage that occurs specifically at Batch 101. Throughout the initial batches ranging from 1 to 100, the gas consumption remains astonishingly stable and consistent, maintaining a level that hovers just slightly above 2.78 x 10^7 units, which strongly suggests that there exists a predictable and uniform computational cost associated with these operations that can be anticipated with a high degree of reliability. In stark contrast, the pronounced decrease observed at the concluding batch, which dips to a value that approaches 2.70 x 10^7 units, signifies a noteworthy alteration in the pattern of resource consumption, a phenomenon that may potentially be attributable to a variety of factors, including but not limited to the execution of a different type of operational process, the implementation of an optimization strategy, or the possibility that the final batch was either left incomplete or managed in a manner that diverges from the established norms of handling the preceding batches.

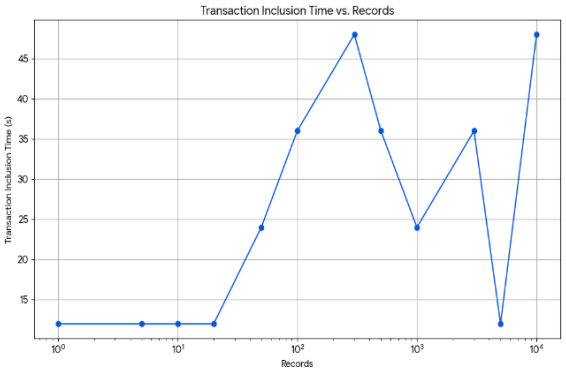


Fig 12:Transcation Inclusion Time

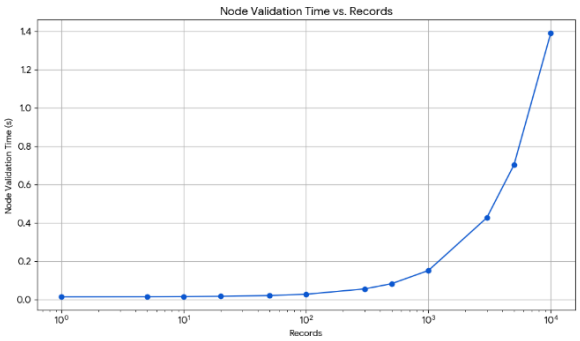


Fig 13:Node Validation Time

In the field of distributed transaction processing, achieving efficient Node Validation Time and predictable Transaction Inclusion Time is crucial for system reliability and user confidence. The rate of validation nodes processing the transaction data is among the criteria commonly referred by the name of Node Validation Time, which is addressed in the proposed architecture. The speed by which it is measured is at least ten times faster through the introduction of new computation methods as shown in Fig. 13. This decreased Node Validation Time will reduce the computational bottleneck hence increasing its scalability as well as maintaining data integrity under highly congested environments - a behavior that outperforms the performance of traditional distributed ledger systems.

In terms of transaction confirmation, our system performs better too. In particular, the recorded Transaction Inclusion Time, i.e., the time duration between a transaction submission and its availability in a published block decreased steadily as it can be observed in Fig. 12. More traditional networks would have a degree of randomness in these confirmation intervals; our solution by contrast would give these systems a stable and computed route toward transaction finality. This kind of Transaction Inclusion Time stability optimizes the user experience and minimizes the confirmation lag and provides a good base of the reliability needed in firm applications in the real world, ensuring predictable data immutability. Such results combined with the increased speed of validation offer a new level of performance in distributed ledger technologies.

Number of Blocks	Minning Time in Seconds					
	DT Level 1 (Seconds)	DT Level 2 (Seconds)	DT Level 3	DT Level 4 (Seconds)	DT Level 5 (Seconds)	DT Level 6 (Seconds)
1	0.05	0.5	5	60	32832	86400
5	0.25	2.5	25	300	164160	432000
10	0.5	5	50	600	328320	864000
20	1.00	10.00	100.00	1200.00	656640.00	1728000.00
50	2.50	25.00	250.00	3000.00	1641600.00	4320000.00
100	5.00	50.00	500.00	6000.00	3283200.00	86400000.00
300	15.00	150.00	1500.00	18000.00	9849600.00	25920000.00
500	25.00	250.00	2500.00	300000.00	16416000.00	43200000.00
1000	50.00	500.00	5000.00	60000.00	32832000.00	86400000.00
3000	150.00	1500.00	15000.00	180000.00	98496000.00	2592000000.00
5000	250.00	2500.00	25000.00	300000.00	164160000.00	432000000.00
10000	500.00	5000.00	50000.00	600000.00	328320000.00	864000000.00
10100	505.00	5050.00	50500.00	6060000.00	331603200.00	872640000.00

Fig 14:Mining Time

The table labeled Mining Time in Seconds is an illustration of the resource (a unit of time) needed to extract one of the blocks in six available types of difficulty levels labeled as levels of difficulty tiers. The same applies to mining times that will always be higher with the increase in the number of blocks on all the levels. The most visible trend, however, is the exponentially increasing mining time on the one hand possible to move from Tier 1 to Tier 6 in this system; the extraction of 10,100 blocks has a mining time of 505 s at Tier 1 and a mind-flabbergasting 87,264,000,000 s at Tier 6 and this shows the overwhelming effects of a more difficult environment on processing time in this profile. Tier 6 (Seconds): That is the final level of the Tiers proposed and it would give the longest mining times. Once taken a single block, it takes 86,400 s (About one day) and 10,100 blocks will take 87,264,000,000 s (About 2,767 years).

CONCULSION

The system demonstrates the **robust and efficient and secure performance** of the proposed system across key metrics. Batch processing consistently achieves remarkable stability, with durations largely confined to a narrow **19-20 second window**, underscoring the system's dependable operational consistency. While minor deviations, such as those observed in Batches
1 and 35, indicate sporadic fluctuations, the overall trend reflects a highly predictable computational cost. This stability is further corroborated by the consistent gas consumption, maintaining a near-constant **2.78×107 units** for the initial 100 batches, indicative of uniform resource utilization. The considerable decrease in the amount of prepared gas at Batch 101 (in contrast to **2.78×107 units** at the time) is also to be examined in more detail as potential indication of optimization, a change in the operating processes, or some shift in the way the batches are worked with. Specifically, it is important to notice that the new techniques that have been introduced allow decreasing Node Validation Time by quite significant values, which helps eliminate the computational constraints and scale to a greater extent, as well as maintain data integrity even in case of heavy network traffic. At the same time, the new architecture will have faster and more stable Transaction Inclusion Times, which will allow setting a new standard of reliable finality in transaction processing, and, therefore, enhancing user experience in the distributed ledger technology. Overall, these results show a significant level of consistency, effectiveness and predictability in the operation of Batch 101 which can be considered as an evidence of its appropriateness as a reliable mechanism of distributed transaction processing.

The analysis further notes that high Difficulty Tiers have tangible effect in mining blocks. In particular, lower levels imply processing time that can be handled, which has an acceptable alignment to block quantity, but Tier 6 has a severe bottleneck, given large-scale conditions. These results open the way to better algorithms and scalable architectures that minimize temporal burden when dealing with high-challenge tasks, to actually play it within a reasonable time and make it a long-term performance solution. Last but not least, the analysis demonstrated clearly that a higher computational hardness in a

Proof of Work (PoW) introduces an adverse impact on block mining efficiency: on the one hand, low-complexity enjoys an easy processing time, on the other hand, at high-complexity, massive restraints are added. These findings highlight the need of PoW architectures to democratically balance the security needs with finality of transactions and use high-level algorithms, as well as scalable network stack to address the temporal limitation of high difficulty distributed ledgers.

REFRENCES

[1]Walonoski J, Klaus S, Granger E, Hall D, Gregorowicz A, Neyarapally G, Watson A, Eastman J. Synthea™ Novel coronavirus (COVID-19) model and synthetic data set. Intelligence-Based Medicine. 2020 Nov;1:100007. https://doi.org/10.1016/j.ibmed.2020.100007

[2]Sonkamble, R.G., Bongale, A.M., Phansalkar, S., Sharma, A., Rajput, S., 2023. Secure Data Transmission of Electronic Health Records Using Blockchain Technology. Electronics 12, 1015. https://doi.org/10.3390/electronics12041015

[3]Kumar, S., Bharti, A.K., Amin, R., 2021. Decentralized secure storage of medical records using Blockchain and <scp>IPFS</scp>: A comparative analysis with future directions. Security and Privacy 4. https://doi.org/10.1002/spy2.162

[4]Arya Raditya Prawira Putra, D., Purwanto, Y., Paryasto, M., 2022. The IMPLEMENTATION OF BLOCKCHAIN AS COVID-19 TEST AND VACCINE CERTIFICATE STORAGE SYSTEM. CEPAT 1, 7. https://doi.org/10.25124/cepat.v1i02.5189

[5]Mohanapriya, M.D., Suresh Kumar, S., Shanker, P.J.V., Mukesh, M., Sathish, M., Assistany Professor -Computer Science and Engineering, Nandha College of Technology, Erode, Tamil Nadu UG -Computer Science and Engineering, Tamil Nadu UG -Computer Science and Engineering Assistany Professor -Computer Science and Engineering Nandha College of Technology Erode, Nandha College of Technology, Erode, Tamil Nadu Nandha College of Technology Erode Tamil Nadu, 2024. Med-block: Secure Health Record Management System Using Blockchain with Ipfs.

[6]Abouali, M., Sharma, K., Saadawi, T., 2022. Patient Full Control over Secured Medical Records Transfer Framework Based on Blockchain, in: 2022 International Conference on Electrical Engineering and Informatics (ICELTICs). Presented at the 2022 International Conference on Electrical Engineering and Informatics (ICELTICs), IEEE, pp. 43–48. https://doi.org/10.1109/iceltics56128.2022.9932113

[7]Kabashi, F., Snopçe, H., Luma, A., Aliu, A., Shkurti, L., 2023. Implementation of Elliptic Curve Digital Signatures in Blockchain for Management of Certificates in Higher Education.

[8]Nishi, F.K., Shams-E-Mofiz, M., Khan, M.M., Alsufyani, A., Bourouis, S., Gupta, P., Saini, D.K., 2022. Electronic Healthcare Data Record Security Using Blockchain and Smart Contract.

[9]Jahir Pasha, M., Baseer, K.K., Vasavi, N., Sreenivasulu, K., Mohammed Nadeem, S., Obula Reddy, A.C., 2024. Ethereum Blockchain-Based Design and Implementation of Electronic Records for Home Care, in: 2024 2nd International Conference on Networking and Communications (ICNWC). Presented at the 2024 2nd International Conference on Networking and Communications (ICNWC), IEEE, pp. 1–8. https://doi.org/10.1109/icnwc60771.2024.10537339

[10]Mishra, D.P., Rajeev, B., Mallick, S.R., Lenka, R.K., Salkuti, S.R., 2025. Efficient blockchain based solution for secure medical record management. IJ-ICT 14, 59. https://doi.org/10.11591/ijict.v14i1.pp59-67

[11]Riadi, I., Ahmad, T., Sarno, R., Purwono, P., Ma, A., n.d.Faroug, Al., Demirci, M., 2021. Blockchain-Based Solutions for Effective and Secure Management of Electronic Health Records, in: 2021 International Conference on Information Security and Cryptology (ISCTURKEY). Presented at the 2021 International Conference on Information Security and Cryptology (ISCTURKEY), IEEE, pp. 132–137. https://doi.org/10.1109/iscturkey53027.2021.9654325

[12]Muhaimin Aziz, A., Widjajarto, A., Budiyono, A., n.d. Analysis and Implementation of Nodes Communication Between InterPlanetary File System (IPFS) in Smart Contract Ethereum.

[13]Capraz, S., Ozsoy, A., 2024. A Secure Medical Data Sharing Framework for Fight Against Pandemics Like Covid-19 by Using Public Blockchain. IEEE Access 12, 93593–93605. https://doi.org/10.1109/access.2024.3423714

[14]Saini, A., Zhu, Q., Singh, N., Xiang, Y., Gao, L., Zhang, Y., 2021. A Smart-Contract-Based Access Control Framework for Cloud Smart Healthcare System. IEEE Internet Things J. 8, 5914–5925. https://doi.org/10.1109/jiot.2020.3032997

[15]Kumar, R., Tripathi, R., 2020. A Secure and Distributed Framework for sharing COVID-19 patient Reports using Consortium Blockchain and IPFS, in: 2020 Sixth International Conference on Parallel, Distributed and Grid Computing (PDGC). Presented at the 2020 Sixth International Conference on Parallel, Distributed and Grid Computing (PDGC), IEEE, pp. 231–236. https://doi.org/10.1109/pdgc50313.2020.9315755

[16]Guo, R., Shi, H., Zhao, Q., Zheng, D., Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, under Grant SKLNST-2016-2-11. Key Laboratory of Networking and Switching Technology under Grant SKLNST Beijing University of Posts and Telecommunications 2016-2-11, n.d. SPECIAL SECTION ON RESEARCH CHALLENGES AND OPPORTUNITIES IN SECURITY AND PRIVACY OF BLOCKCHAIN TECHNOLOGIES.

[17]Mahajan, R., Dey, R., Khan, M., Shelke, P., Kumbhar, V., Shendage, J., 2025. Blockchain-Enabled Tamper-Proof Vaccine Distribution Records.

[18]Andi, A., Juliandy, C., Robet, R., Pribadi, O., 2022. Securing Medical Records of COVID-19 Patients Using Elliptic Curve Digital Signature Algorithm (ECDSA) in Blockchain. CommIT (Communication and Information Technology) Journal 16, 87–96. https://doi.org/10.21512/commit.v16i1.7958