# DYNAMIC SECURE ACCESS OFE-HEALTH CARE SYSTEM USING CLOUD COMPUTING AND BLOCKCHAIN

V.Punitha[1], U.Sundhar[2], D.Kanthasamy[3], P.Chitra Devi[4]

[1]P.G student, Department of CSE, Thiruvalluvar College of Engineering and Technology, Vandavasi.

[2]Head of the Department, Department of CSE, Thiruvalluvar College of Engineering and Technology, Vandavasi.

[3]Head of the Department, Department of CSE(AI&ML),Thiruvalluvar College of Engineering and Technology Vandavasi.

[4]Assistant Professor, Department of CSE, Thiruvalluvar College of Engineering and Technology Vandavasi

**ABSTRACT -** *Electronic health records contain details about a patient's medications and their medical history. These records are highly sought after by attackers due to the invaluable information they hold. The loss of electronic health records can result in incorrect medication or surgical procedures. Unfortunately, healthcare systems often implement inadequate security measures to protect these records. Blockchain technology, which is a decentralized and distributed ledger, plays a crucial role in safeguarding data and transactions. By integrating blockchain into healthcare systems, the protection of health records from attackers is significantly enhanced. Nevertheless, blockchain is still vulnerable to various attacks, including phishing, dictionary-based attacks, and threats to both cold and hot wallets. This paper suggests a multilevel authentication scheme to defend the blockchain against such attacks. Given that patients lack control over their data, the risk of misuse is considerable. Therefore, a patient-centered approach that is entirely decentralized is necessary to detect data theft, prevent data manipulation, and ensure that patients have rights over access control. Blockchain technology emerges as an optimal solution to tackle these issues and meet the requirements. As a decentralized and distributed ledger, blockchain is also poised to influence billing, record sharing, medical research, identity theft, and financial data crimes in the future. The implementation of smart contracts in healthcare can further streamline processes, where invoking, record creation, and validation will be managed through blockchain.*

**Key words: blockchain, Electronic health, healthcare systems, threats, attacks**

## 1. INTRODUCTION

The Blockchain is a secure, distributed database that maintains records of data; in other words, it serves as a digital ledger for transactions and contracts that require independent documentation.One of the primary characteristics of Blockchain is that this digital ledger is available across numerous computers, rather than being confined to a single location. The Blockchain technology has already begun to disrupt the financial services industry, serving as the foundation for digital currency transactions, such as Bitcoin. Participants can engage directly and conduct transactions over the internet without the involvement of a third party.

Transactions conducted via Blockchain do not disclose any personal information about the participants, and they generate a transaction record by encrypting identifying details. The most remarkable aspect of Blockchain is its significant reduction in the likelihood of data breaches. Unlike traditional methods, Blockchain maintains multiple shared copies of the same database, making it difficult to execute a data breach or cyber-attack.With its fraud-resistant features, Blockchain technology has the potential to transform various business sectors, rendering processes smarter, more secure, transparent, and efficient compared to conventional business practices. It provides a history of activities rather than merely a snapshot at a specific moment in time. While a standard database offers an up-to-date snapshot of data, Blockchain does this as well, but it also preserves a record of all prior information. It is essentially a database with historical context.

There is no singular, central point of vulnerability. The decentralized nature of Blockchain for storing and accessing data enhances the overall security of the system; unlike centralized databases, there is no single entry point for hackers. This feature makes it especially advantageous for securely recording transactions without a centralized authority.

Need For Study

Blockchain represents a form of digital ledger technology that enables secure, transparent, and direct transactions between parties without the need for intermediaries. It operates as a decentralized database that is spread across a network of computers, with each node in the network maintaining a copy of the ledger.

This article aims to explore the necessity of blockchain technology. For example, in the realm of supply chain management, blockchain can be utilized to ensure complete visibility and traceability, enabling consumers to track a product's journey from the manufacturer to the retailer. In the financial industry, blockchain technology can provide auditors and regulators with real-time access to financial transactions, thereby improving the effectiveness and efficiency of financial oversight. Additionally, crowdfunding is the practice of gathering financial support from a large number of individuals, typically via the internet. Conversely, the blockchain's decentralized and distributed ledger technology facilitates secure and transparent transactions without relying on intermediaries.

*Paper Objective*

*Enhanced Security*

Your information is sensitive and vital, and blockchain can profoundly alter your perspective on your essential data. By establishing a record that is immutable and encrypted from end to end, blockchain effectively mitigates fraud and unauthorized actions.

You can tackle privacy concerns on the blockchain by anonymizing personal information and utilizing permissions to restrict access. Information is stored across a network of computers instead of a single server, making it challenging for hackers to access data.

*Increased Transparency*

In the absence of blockchain, each organization must maintain its own separate database. Blockchain employs a distributed ledger, which records transactions and data uniformly across multiple locations.

All network participants with authorized access view the same information simultaneously, ensuring complete transparency. Every transaction is permanently recorded and is marked with a time and date stamp. This feature allows members to examine the full history of a transaction, virtually eliminating any chance of fraud.

*Immediate Traceability*

Blockchain establishes an audit trail that tracks the origin of an asset at every stage of its journey. In sectors where consumers are concerned about environmental or human rights issues related to a product—or in industries plagued by counterfeiting and fraud—this provides essential proof.With blockchain, sharing provenance data directly with customers becomes feasible. Traceability information can also reveal vulnerabilities in any supply chain, such as where goods may be delayed on a loading dock awaiting shipment.

*Enhanced efficiency and speed*

Conventional paper-based processes are labor-intensive, susceptible to human mistakes, and frequently necessitate third-party involvement. By optimizing these processes through blockchain technology, transactions can be executed more swiftly and effectively.

Documentation can be securely stored on the blockchain alongside transaction information, removing the necessity for paper exchanges. This eliminates the need to reconcile various ledgers, allowing for significantly quicker clearing and settlement.

*Automation*

"Smart contracts" can facilitate the automation of transactions, further enhancing your efficiency and accelerating the overall process. Once the predetermined conditions are satisfied, it automatically initiates the subsequent step in the transaction or process.

Smart contracts minimize human involvement and decrease dependence on third parties to confirm the fulfillment of contract stipulations. For instance, in the insurance sector, once a customer submits all required documentation to process a claim, the system autonomously settles and disburses the claim.

## 2.LITERATURE REVIEW

The paper titled" Third party public auditing on cloud storageusing the cryptographic Algorithm" B. L. Adokshaja ; S. J. Saritha ( 2017) A data auditing mechanism will be implemented in cloud computing to ensure secure data storage. Auditing involves verifying user data, which can be performed by either the data owner or a Third Party Auditor (TPA). This process is essential for maintaining the integrity of data stored in the cloud. The responsibilities of the TPA are categorized into two types:The first is private auditability, which enables both the data owner and the user to verify the integrity of the data. In this case, no one has the authority to question the server about the data, although this may increase the verification burden on the user. The second is public auditability, where only the TPA is authorized to assess the confidentiality of the data.

The TPA is an organization that operates on behalf of the client. It possesses all the essential expertise, capabilities, knowledge, and professional skills necessary for conducting integrity verification tasks, thereby alleviating the client's concerns. It is crucial for the TPA to conduct regular audits of the cloud data storage without needing to request a local copy of the data. Cloud computing faces numerous challenges, particularly regarding integrity and privacy. Therefore, additional security measures and efficient mechanisms are required to ensure the integrity and privacy of data stored in the cloud.

The proposed scheme includes three fundamental entities:

- Data owner,
- Cloud server storage, and
- TPA.

The data owner, or user, is tasked with dividing the file into blocks, encrypting these blocks using the AES algorithm, and generating a hash value for each block to verify whether the file has been corrupted. The cloud server's role is solely to store the encrypted blocks of files, thus relieving it of the additional responsibility of computing the verification proof. In this context, verification proof refers to the generation of hashes for the encrypted

blocks.

*Efficiency*

- Secure and Highly efficient
- Less Encryption Time
- Support dynamic operation
- Privacy Preserving
- Batch Auditing

*Drawbacks*

- Less Secure, High Embedding extractiontime.
- Poor Application Performance
- Reduce the Modality gap by synthesizing

In the paper titled" Enhancing data storage security in Cloud using Certificate less public auditing" R. Swathi, T. Subha(2017) Cloud computing represents a groundbreaking model that offers beneficial, on-demand access to configurable processing resources. In this paradigm, IT-related capabilities are delivered as services, accessible without requiring in-depth knowledge of the underlying technologies, and with minimal management effort. However, the significant cost savings promised by cloud computing are often offset by the perceived security risks that users fear. The stored data on an unreliable server raises concerns about the cloud server's ability to protect the data without retrieving it. The system generates probabilistic proofs of ownership by checking random sets of pieces from the cloud server, which has significantly reduced input/output costs. Users maintain a consistent amount of data to verify data integrity. The challenge/response protocol transmits a small, consistent amount of data, which minimizes network communication.

Dividing data integrity into components allows for the identification of entity aspects that may impose limitations on data integrity and the issues that are mapped to the critical dimensions of data integrity they affect, identifying factors that could threaten the integrity of data for essential data dependencies. To design and implement efficient data storage in the cloud, the following objectives are established and accomplished.

- Data security: Ensures the protection of data stored in the cloud. Examples of data security measures include software/hardware disk encryption and backups.
- Cloud storage: Cloud storage providers are responsible for keeping the data accessible, ensuring the physical environment is secure and operational.
- Integrity: To ensure the trustworthiness and availability of data in the cloud and to uphold the quality of cloud storage services, it is crucial for users.

*Efficiency*

- Increases the opaqueness of the user data from the auditor
- Support scalable and efficient public auditing in the cloudcomputing
- Provides a privacy preserving auditing process
- Secure and Highly efficient

*Drawbacks*

- Narrowly specialized knowledge
- Heavyweight
- Big payloads

In the paper titled" S-Audit: Efficient Data Integrity Verification for Cloud Storage" Filipe Apolinário, Miguel Pardal, Miguel Correia(2018) This paper introduces S-AUDIT, a

service designed for the integrity verification of data stored in commercial cloud environments. S-AUDIT employs homomorphic authentication alongside digital signatures to eliminate the need to retrieve protected data from the cloud. The service has been integrated with a cloud-based file system known as SCFS to demonstrate its practical application. Our experimental analysis indicates that utilizing S-AUDIT is 7.1% more cost-effective than employing RSA signatures for monthly data integrity verification, and 34.9% more economical for weekly verification in a typical scenario. Currently, data owners implement integrity control mechanisms that rely on cryptographic hashes to safeguard their outsourced storage. Digital signatures are utilized for collaborative storage when data is shared among multiple cloud users, while MACs (Message Authentication Codes) are employed for private storage when data is accessed by a single cloud user. To conduct integrity control, users must possess a personal key: either an asymmetric private/public key pair for digital signatures or a symmetric key for MACs. User data is stored along with either a signature or a MAC, generated using the user's private key or symmetric key, respectively.

In S-AUDIT, there is interaction among three types of entities:

- clouds,
- users and
- auditors

These papers propose the below cryptographic techniques:

- Multiplicative Cyclic Group
- Pairing-based cryptography
- BLS Signature Scheme

*Efficiency*

- Secure and Highly efficient
- Stateless verification
- Maintains Integrity of Data
- Maintains Confidentiality of Data

*Drawbacks*

- Scalability is an issue for those designs as the number ofusers and the amount of data grow
- Complexity of its Real Time Implementation
- Prohibitively Expensive in terms of Time and Memory Usage

## 3.IMPLEMENTATION

*Doctor Information*

This system is designed to enhance the capabilities of hospitals, multi-specialty clinics, doctors, and medical practitioners by automating the process of recording patient information. The prevalent programming paradigm utilized here is procedural programming, which organizes a program similarly to a recipe by providing a sequence of steps, represented as functions and code blocks, that flow in order to accomplish a task. We employ a standard naming convention to ensure immediate recognition by the reader.

*Login Screen & Dashboard*

To access the Identity-Based Integrity auditing application, you must first enter a username and password. Authentication involves identifying a user and confirming that this user has permission to access the application. To reach your Identity-Based Integrity Auditing Application, please enter the following URL in your web browser's address bar:
http://127.0.0.1:9091

Before you can utilize the site application tools, you will need to log in. The login screen for the Identity-Based Integrity Auditing Application requires an admin to enter a username and password. Your application user will provide you with these credentials. Please note that login information is case-sensitive. After a successful login, you will be welcomed by the Identity-Based Integrity Auditing Application Dashboard within the Admin area. The following objectives are upheld and accomplished.

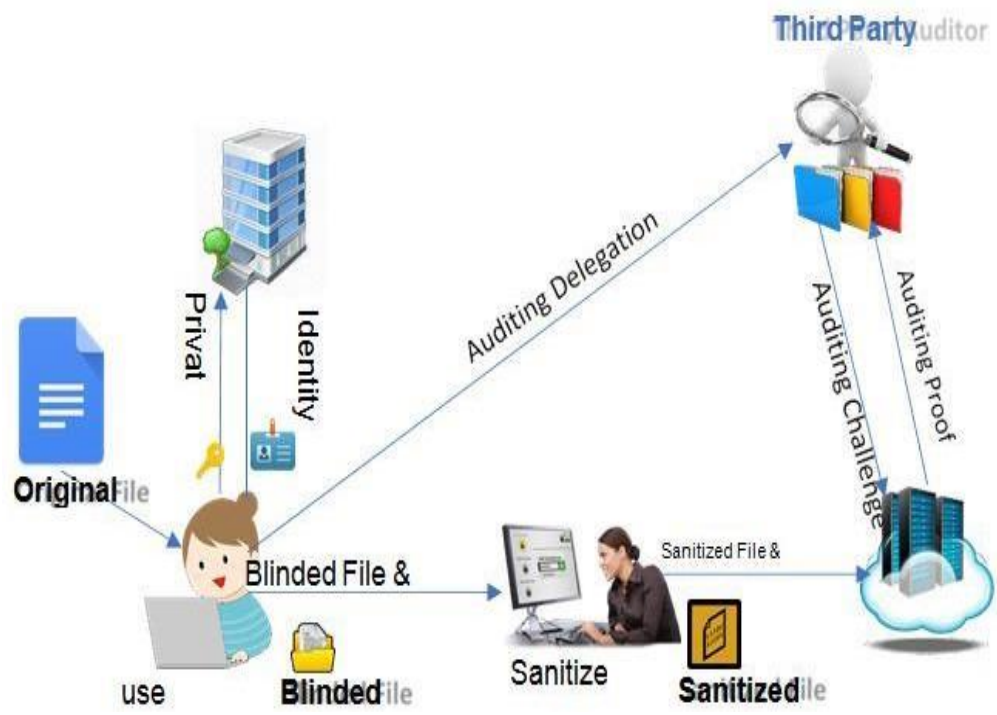


**Fig 3.1: System Architecture**

*Data security*: Ensures the protection of data stored in the cloud. Examples of data security measures include software and hardware disk encryption, as well as backups.

*Cloud storage*: Cloud storage providers are responsible for keeping the data accessible, ensuring an open environment, and maintaining the physical infrastructure securely and operational.

*Integrity:* The primary goal is to ensure the reliability and availability of data in the cloud while upholding the quality of the cloud storage service, which is crucial for users. Electronic IoT data systems have the capability to enhance health outcomes by providing healthcare professionals with better information regarding their IoT devices. They can also elevate the quality of healthcare and assist in cost management through increased efficiency. The literature review focuses on health information systems, particularly on the management of IoT data, and will aid in contextualizing the survey findings. Specifically, it addresses the challenges associated with transitioning IoT data from paper-based records to digital formats.

*Patient &EHR*

This module manages all patient demographic information. A unique registration number, serving as a patient identifier, is assigned here. The registration number assigned to the patient will track the number of visits to the outpatient department (O.P.D.) as well as the

number of hospital admissions. Distributed health data networks enhance the capacity to gather and analyze data, thereby improving the effectiveness, safety, and quality of care.

*EHR RECORD*

Electronic Health Records (EHRs) can incorporate multimedia elements, such as images, which aid in delivering comprehensive patient information. Translation services are a prime example—healthcare providers and insurers are legally obligated to ensure language access in service delivery while safeguarding sensitive patient data. Health care data encryption is a method of securing data, ensuring that electronic medical records (EHR) are obscured from unauthorized access.

*IoT Data and IoT Information*

This module oversees all IoT demographic details. A unique registration number, functioning as an IoT identifier, is assigned here. The registration number allocated to the IoT will store relevant details. Individual IoT data is frequently aggregated for monitoring, evaluation, or reporting to higher management levels. However, this aggregated data is also beneficial locally, as it can foster a 'culture of improvement'—measuring service quality and outcomes to implement necessary changes. The aim of collecting and storing IoT data is to facilitate decision-making at the point of care or for management and policy analysis and action. It is crucial to understand that most individual IoTs have multiple points of care and may transition between various locations, including across countries. It is essential that their individual IoT information be available at all points of care and all sites for analysis. In order for this to work, there must be standards for representing the data and for communication. Distributed IoT data networks have been proposed to improve the ability to collect and analyse data across institutions leading to improved effectiveness, safety, and quality of data.

*Blinded File & Sanitized File Generation*

Why is Encryption Important?

- To ensure the security of financial and other R&D data alongside various internal information that must be protected from unauthorized access.
- Employees and organizations prefer that their financial or private information remains confidential.
- To facilitate swift transactions, ensuring that private information is not exposed. Encryption transforms text into an unreadable format for anyone without the appropriate keys to decode it, making it increasingly essential rather than optional in any security framework due to its effectiveness in slowing down and potentially deterring hackers from accessing sensitive data. Healthcare organizations must encrypt their IoT data, and they also need to understand what data they are encrypting and where it is located Infrastructure. Encrypting data at rest is clearly distinct from encrypting data. Algorithm for Blinded File:
- Python takes the file input and encrypts it utilizing the Pycrypto module.
- The filename is provided as an input parameter along with the password.
- Encryption is accomplished with the aid of a key generated according to algorithmic standards. The encrypted file is stored in the same directory with a prefix of (encrypted) added to its name.
- A cryptographic hash function produces keys that help maintain the security of files used for symmetric encryption.

- The files are fundamentally secured with passwords.
- Decryption follows a reverse process where the password and the encrypted file are taken as input parameters. Encryption algorithms modify their input data (referred to as plaintext) in a manner dependent on a variable key, resulting in ciphertext; this transformation can be easily reversed, if (and, hopefully, only if) one possesses the key. The key can be adjusted by the user or application, selected from a vast range of potential keys. AES, or Advanced Encryption Standards, is among the most commonly employed methods for encrypting and decrypting sensitive data. The key size utilized for this cipher determines the number of repetitions or "rounds" necessary to process the plaintext through the cipher and convert it into ciphertext.

Here's how the cycles are distributed.

- ❖ 10 rounds are necessary for a 128-bit key.
- ❖ 12 rounds are necessary for a 192-bit key.
- ❖ 14 rounds are necessary for a 256-bit key.

While longer keys offer users stronger encryption, this strength comes at the expense of performance, meaning that they will require more time to encrypt. The Advanced Encryption Standard is constructed from three block ciphers: AES-128, AES-192, and AES-256. Each of these encrypts and decrypts data in segments of 128 bits using cryptographic keys of 128, 192, or 256 bits. The initial step in the AES encryption process involves substituting the information using a substitution table; thesecond transmutation changes data rows and the third shifts columns. The lasttransformation is a basic exclusive XOR process done on each column using a different part of the encryption key. The longer the encryption key, the more rounds are needed. Although hashing isn't an encryption method, it is sometimes incorrectly referred to as one. Instead, hashes are a one-way function for providing authentication. The hash function takes a larger file as input, processes it, and returns a smaller output that is almost guaranteed to be a unique ―fingerprint‖ of the file. This makes it easy to compare two files to see if they are different from each other. Even changing one character will result in a different hash output. Hashing is often used in collaboration with encryption.

*Third Party Auditor*

For public verification, clients can engage an independent third party auditor (TPA) to confirm the accuracy of data storage in the cloud on their behalf through public verification. The system supports dynamic operations, allowing users to not only access but also update the outsourced data. The TPA is capable of managing multiple tasks from various clients simultaneously. By employing these techniques, we can effectively implement a verification scheme to ensure data accuracy in the cloud, although we cannot guarantee that the scheme is highly efficient. Taking into account the diverse range of devices used for access, such as mobile devices, clients are not required to expend excessive computational resources during both the initialization and verification phases of the auditing protocol. After the verification process, a report is generated and sent to the users. To ensure data reliability throughout the auditing process, the server produces proof and randomly selects data blocks. The TPA then verifies this proof against the cloud server, and the results of the audit are communicated to the user. A comprehensive execution analysis has shown that the proposed method outperforms existing solutions. The signed proof is forwarded to the trusted third party auditor (TTPA) for validation. The auditor first checks the signature and then validates the proof. The auditor has the authority to challenge the server at any time regarding data integrity. Subsequently, it verifies and confirms that the server's response is valid.

Our scheme is comprised of two critical phases in the second stage.

- ❖ Challenge Response Phase
- ❖ Proof Verification Phase

Step 1: The auditor initiates a challenge request for the randomly chosen blocks. The auditor also indicates the specific block positions that the server should verify. The challenge message includes the count of the queried blocks. It randomly selects an element from the subset S = { S1 < ….< Sc} of the set that belongs to [1,n]. The auditor transmits the challenge message to the cloud server. Challenge message = {(i,mi)} where S1 < i < Sc

Step 2: Upon receiving the challenge request generated by TTPA, the server processes an input file F, the challenge request query, and the Signature set S. The server then sends the proof back as a response to the auditor.

Step 3: The auditor (TTPA) verifies integrity after receiving the response by executing the algorithm. The next step involves comparing the newly computed signature with the previously stored signature. Upon receiving the signature, TTPA first verifies the Certificate using its verification algorithm. If the verification is successful, the response is validated using its public key (PK). If not, the integrity verification process is halted. In the second step, the proof response is decrypted using the public key (PK) after the certificate has been verified to ensure authenticity. Subsequently, the signature is validated to confirm the server's authentication. Our scheme is designed to detect corrupted data caused by an active adversary. Our auditing protocol employs a digital signature algorithm in conjunction with certificates. This certificate is utilized to verify the server's authenticity. Certificates link identity information such as user name, IP address, and social security number (SSN) to a public key through digital signatures. Therefore, unauthorized access to the data is prevented.

In Fig.3.1, the architecture diagram serves as a visual representation of various concepts that constitute an architecture, encompassing its principles, elements, and components. System developers require these diagrams to comprehend, elucidate, and convey ideas regarding the system's structure and the user requirements that must be met. This fundamental framework can be utilized during the system planning phase, aiding stakeholders in grasping the architecture, discussing modifications, and clearly communicating intentions.

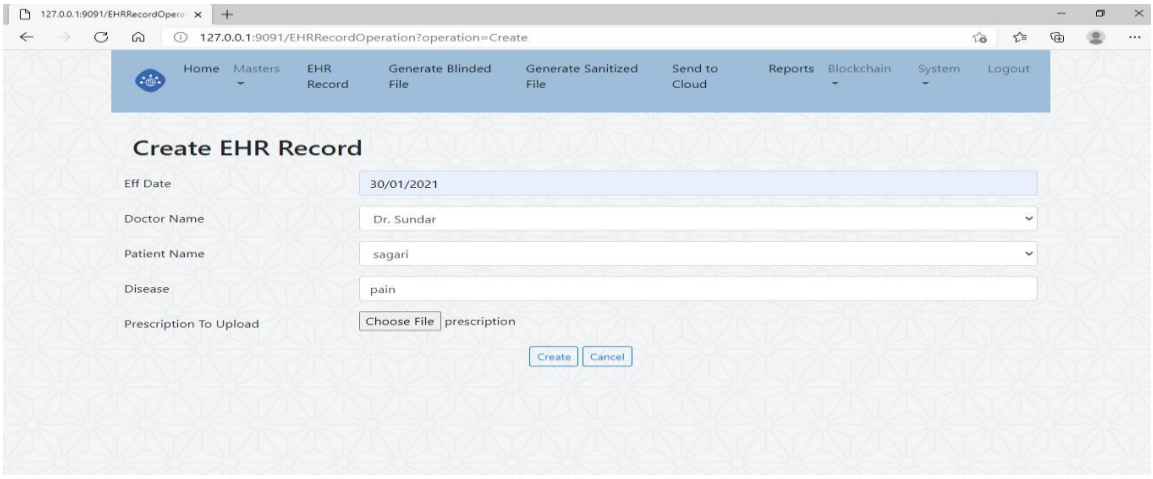


**Fig 3.2: Create EHR record**

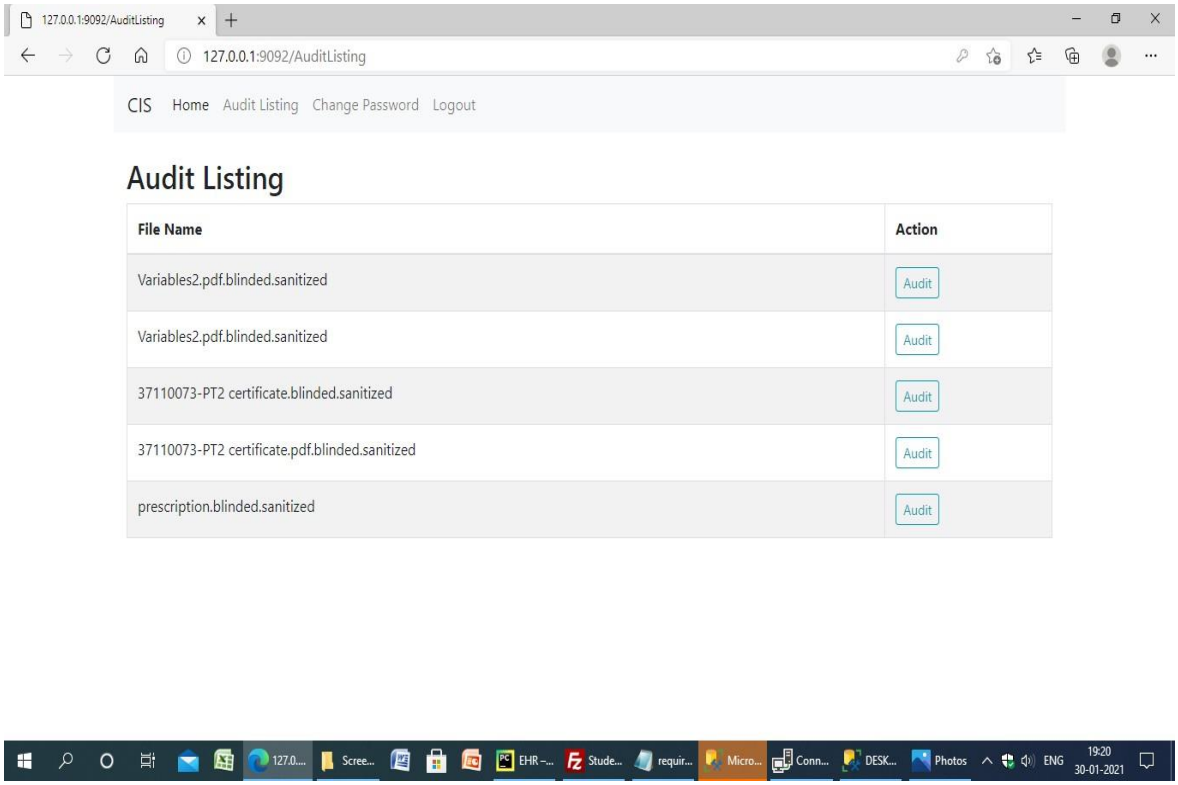


**Fig 3.3:Audit Listing**

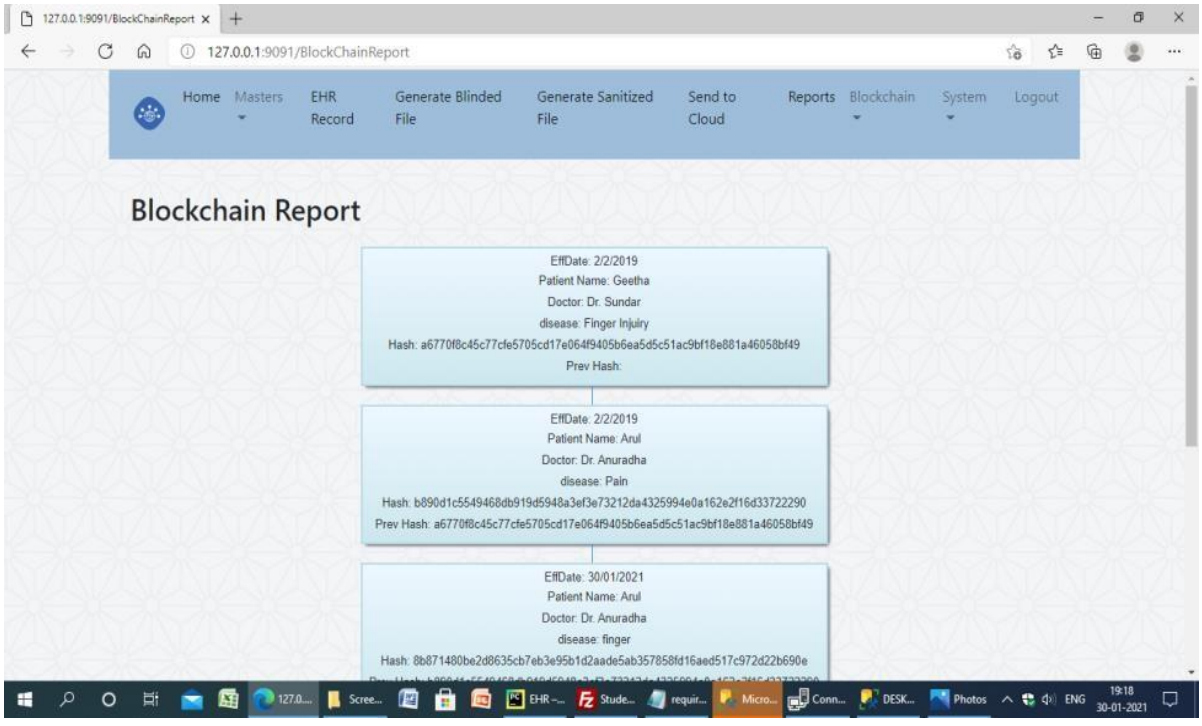


**Fig 3.4: Blockchain report is created**

.

## CONCLUSION

Ensuring the privacy and security of patient health information is our highest priority, and we have implemented blockchain technology to safeguard this information. We utilize data encryption, a form of data security, to protect it from unauthorized access. By employing distributed health data networks, we enhance our capacity to collect and analyze data, which in turn improves the effectiveness and quality of care.

## REFERENCES


[1]. Awasthi and K. Singh, ‖A Key Agreement Algorithm Based on ECDSA forWireless Sensor Network,‖ in 3rd International Conference on Advanced Computing Networking and Informatics, 2015.

[2]. Arabat Rashmi Vinod, Bhalke Sumit Sunidatta, Kumari Uma Rani, and Pillai Preethy Sasidharan. Hindering Data Theft Attacks Through Fog Computing. International Journal of Research in Engineering and Technology 2014, Volume 3, pp. 427-429.

[3]. Dnyanesh Patil, Suyash Patil, Deepak Pote, and Nilesh Koli. Secured CloudComputing With Decoy Documents. International Journal of Advances in Computer Science and Cloud Computing 2014, Volume 2, pp. 43-45.

[4]. H. liu, Y. huang, and J. K. Liu, ‗Secure sharing of Personal Health Records in cloud computing: Ciphertext-Policy Attribute-Based Signcryption,‘‘ Future Gener. Comput. Syst., vol. 52, pp. 67–76, Nov. 2015.

[5]. J. Shao, R. Lu, and X. Lin, ‗‗Fine-grained data sharing in cloud computing for mobile devices,‘‘ in Proc. IEEE Conf. Comput. Commun. (INFOCOM), Apr./May 2015, pp. 2677–2685.

[6]. J. Zhou et al., ‗Securing outsourced data in the multi-authority cloud with fine- grained access control and efficient attribute revocation,‘‘ Comput. J., vol. 60, no. 8, pp. 1210– 1222, Aug. 2017.

[7]. K. Huang et al., ‗PKE-AET: Public key encryption with authorized equality test,‘‘ Comput. J., vol. 58, no. 10, pp. 2686–2697, Oct. 2015.

[8]. L. Wu, Y. Zhang, K.-K. R. Choo, and D. He, ‗Efficient and secure identitybased encryption scheme with equality test in cloud computing,‘‘Future Gener. Comput. Syst., vol. 73, pp. 22–31, Aug. 2017

[9]. M. Sriram, V. Patel, D. Harishma, and N Lakshmanan. A Hybrid Protocol toSecure the Cloud from Insider Threats. In Cloud Computing in Emerging Markets (CCEM), IEEE International Conference, Bangalore, 2014.

[10]. R. Ahuja, S. K. Mohanty, and K. Sakurai, ‗‗A scalable attribute-set-based access control with both sharing and full-fledged delegation of access privileges in cloud computing,‘‘ Comput. Elect. Eng., vol. 57, pp. 241–256,Jan. 2017.

[11]. Sonali Khairnar and Dhanashree Borkar. Fog Computing: A New Concept to Minimize the Attacks and to Provide Security in Cloud Computing environment. International Journal of Research in Engineering and Technology 2014, Volume 3, pp. 124-127.

[12]. S. Jin-Shu, C. Dan, W. Xiao-Feng, and S. Yi-Pin, ‗‗Attributed-based encryption schemes,‘‘ J. Softw., vol. 22, no. 6, pp. 1299–1315, 2011.

[13]. Y. S. Rao, ‗A secure and efficient ciphertext-policy attribute-based signcryption for personal health records sharing in cloud computing,‘‘ Future Gener. Comput. Syst., vol. 67, pp. 133–151 Feb. 2017.