DYNAMIC HEALTH LEDGER

Dr. T Shyam Prasad, Shivaratri Aishwarya, Pathlavath Pavan Raj, Anumula Varun Chand K

1 IV-year Department of Computer Science and Engineering ,2 IV-year Department of Computer Science and Engineering ,3 IV-year Department of Computer Science and Engineering, 4 Assistant Professor - Department of Computer Science and Engineering

Anurag University, Ghatkesar, Hyderabad, India

1 [20eg105345@anurag.edu.in](mailto:20eg105345@anurag.edu.in), 2[20eg105339@anurag.edu.in](mailto:20eg105339@anurag.edu.in) 3[20eg105302@anurag.edu.in,](mailto:20eg105302@anurag.edu.in,) 4 [shyamprasadcse@anurag.edu.in](mailto:shyamprasadcse@anurag.edu.in)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Abstract** - This abstract introduces the Dynamic Health Ledger; it is a new way of managing healthcare data that keeps it safe and secure. It uses two main technologies: RSA encryption and blockchain. RSA encryption keeps communications and access to data secure, while blockchain ensures that all transactions with health records are recorded in a way that can't be changed. This system makes it easier for different parts of the healthcare system to work together and ensures that patients' information stays private and protected. Overall, it's a big step forward in how we handle healthcare information.

**Index Terms** –Dynamic Health Ledger (DHL), Rivest Shamir Adleman (RSA), Blockchain Technology, Distributed ledger, Electronic Health care Records (EHR).

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# **Introduction**

In our project, "Dynamic Health Ledger," we've combined RSA encryption and blockchain technology to make managing patient health records more secure and efficient. With healthcare data needing to be both safe and easy to share, we've created a system that does both. RSA encryption keeps the data secure, while blockchain ensures that it can't be tampered with. This means patient records can be shared safely across different healthcare providers. We've focused on making our system easy to understand and use, so healthcare institutions can implement it smoothly and improve the quality of care they provide.

**I.I.BACKGROUND**

Each method of sharing patient health records has its own advantages and considerations, and healthcare organizations may use a combination of these methods based on their specific needs, technological capabilities, and regulatory requirements.

Different Types of sharing patient health records:

* Electronic Health Record (EHR) Systems: EHR systems are digital repositories that store patient health information. Healthcare providers within the same institution or network can access and update patient records securely through these systems. EHRs facilitate real-time sharing of patient data, enabling coordinated care among multiple healthcare professionals involved in a patient's treatment.
* Secure Messaging Platforms: Secure messaging platforms, such as encrypted email or secure messaging apps, can be used to transmit patient health information between healthcare providers. These platforms employ encryption and other security measures to protect the confidentiality and integrity of the transmitted data.
* Telemedicine Platforms: Telemedicine platforms enable remote consultations and virtual visits between patients and healthcare providers. During these virtual encounters, patient health records can be shared securely between the patient and the healthcare provider through the platform's secure messaging.
* Patient Portals: Patient portals are secure online platforms that allow patients to access their own health records and communicate with their healthcare providers. Patients can view their medical history, test results, and treatment plans, as well as share this information with other healthcare professionals as needed.
* Faxing: While less common in modern healthcare settings, fax machines are still used in some healthcare organizations to transmit patient health records securely.

Each of these methods offers unique advantages and considerations, and healthcare organizations may employ a combination of these approaches based on their specific needs, technological infrastructure, and regulatory requirements.

Various Kinds of Storage Methods:

* Cloud-based Storage: Healthcare organizations often utilize cloud-based storage solutions to store and manage patient health records. Cloud storage offers scalability, accessibility, and cost-effectiveness, allowing healthcare providers to securely store large volumes of data while ensuring easy access from any location with an internet connection.
* On-premises Servers: Some healthcare organizations prefer to maintain on-premises servers to store patient health records. On-premises servers provide full control over data management and security, allowing organizations to implement customized security measures and comply with specific regulatory requirements.
* Electronic Health Record (EHR) Systems: EHR systems serve as centralized repositories for storing patient health records electronically. These systems allow healthcare providers to efficiently organize, access, and update patient information, facilitating coordinated care.
* Health Information Exchanges (HIEs): HIEs enable the secure exchange of patient health information between different healthcare organizations and systems. By connecting disparate healthcare entities, HIEs promote interoperability and facilitate the seamless sharing of patient data.
* Virtual Private Networks (VPNs): VPNs create encrypted connections over public networks, allowing healthcare organizations to securely transmit patient health records between remote locations or across different networks. VPNs help safeguard data privacy and security during transmission.

# **Literature survey**

# **II.I  Concerns and Security for Storing Health care records**

**Authors,** M. Misbhauddin, A. Alabdulatheam, M. Aloufi, H. Al-Hajji, and A. AlGhuwainem, ‘‘MedAccess:.

The aim of the paper is to reduce the concerns regarding security in storing healthcare records are effectively addressed through a combination of blockchain technology, encryption techniques, and secure authentication mechanisms. Blockchain ensures data integrity and immutability, making healthcare records resistant to tampering and unauthorized access. Encryption techniques, such as RSA, safeguard sensitive data during transmission and storage, while digital signatures authenticate user identity and access requests. Robust user authentication mechanisms and compliance with regulatory standards, such as HIPAA and GDPR, further enhance security and privacy. Continuous monitoring, updates, and adherence to best practices ensure that the system remains resilient to evolving threats and compliant with industry regulations, providing a secure platform for managing electronic healthcare records.

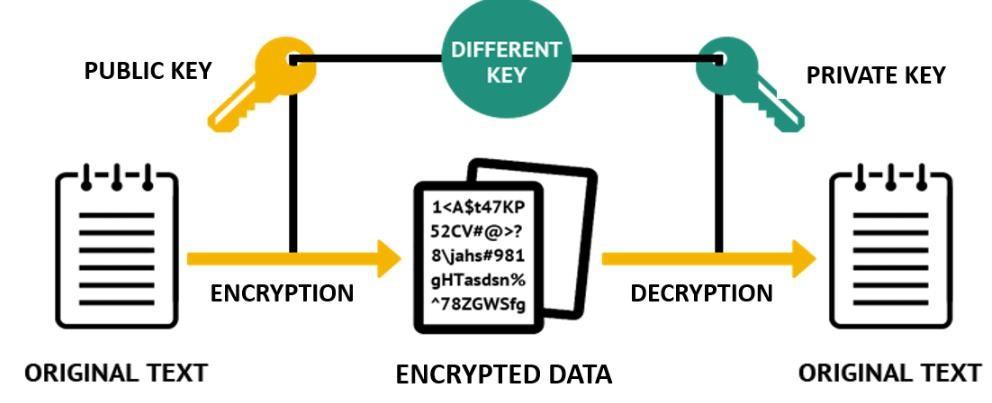
**II.II. Security and Privacy Issues with health care technology**

**Authors:** M Meingast, T Roosta and S Sastry

The main goal of this paper is to address security and privacy concerns in healthcare technology through a multi-faceted approach. Firstly, by leveraging blockchain technology, we established a decentralized platform that ensures data integrity and immutability, mitigating the risk of unauthorized access and tampering. Additionally, encryption techniques, such as RSA encryption, were implemented to secure data transmission and access control, safeguarding sensitive patient information from interception or unauthorized viewing. User authentication mechanisms, including digital signatures and public key verification, were employed to ensure that only authorized individuals can access patient health records. Moreover, compliance with regulatory standards, such as HIPAA and GDPR, was prioritized to protect patient privacy and confidentiality. Continuous monitoring and updates to security protocols were implemented to stay ahead of emerging threats and vulnerabilities, ensuring a proactive approach to cybersecurity. Through these measures, we established a robust framework that addresses security and privacy issues in healthcare technology, fostering trust and confidence among patients, healthcare providers, and administrators alike.

# **RSA KEY GENERATION:**

In the "Dynamic Health Ledger," the RSA key exchange algorithm is employed to establish secure communication channels between users, ensuring the confidentiality and integrity of health records. When two parties, such as a healthcare provider and a patient, need to communicate securely, the system generates a pair of RSA keys for each party: a public key and a private key. The public keys are exchanged, while the private keys are kept securely by the respective parties. Messages sent by one party are encrypted with the recipient's public key, ensuring that only the recipient, holding the corresponding private key, can decrypt and access the information. This asymmetric encryption scheme provides a strong level of security, allowing for confidential and authenticated communication while mitigating the risk of eavesdropping and data tampering. The RSA key exchange algorithm is a fundamental component of the system's security infrastructure, safeguarding sensitive health data during transmission.



#### RSA KEY GENERATION

**Encryption with Public Key:** The sender encrypts the session key using the recipient's

public key. This encrypted session key is then transmitted securely to the recipient.

**Decryption with Private Key:** The recipient uses their private key to decrypt the session key sent by the sender. This action ensures that only the recipient can access the session key.

**Secure Communication:** With the session key established, both parties can securely encrypt and decrypt messages using symmetric encryption algorithms, such as AES. This guarantees the confidentiality and integrity of their communication.

**III.I. Modules and their Description**

The system comprises 1 major module with their sub-modules as follows:

**Module:**

1. **Registration:**

* The user will have to enter their Email ID.
* They can enter a password.
* If they are entering for the first time then they have to generate a new password.
* If the user is a patient, then he has to upload the HER.
* Whereas if the user is a doctor, then he has to request for the access of the patient’s data.

**2. Sharing of Data:**

* Once after the doctor logs into his account, he will check out whether there are any patients

They have to request for the HER records.

* After requesting the patient sends the digital signature via email
* Digital signature is nothing but the block hash number and the public key of the patient
* The doctor validates the details.
* And treats the patients.

**Concept Tree:**

Secure Healthcare Records Platform

└── Workflow:

├── Patient:

│ ├── Creates an account

│ ├── Uploads Electronic Health Records (EHR) to the blockchain

│ ├── Uploads encrypted disease text file

│ └── Generates a digital signature

├── Doctor:

│ ├── Creates an account

│ └── Requests access to patient's EHR

├── Patient (Continued):

│ ├── Approves doctor's request

│ ├── Sends digital signature

│ └── Shares public key via messages or phone calls

└── Doctor (Continued):

├── Receives digital signature and public key

├── Verifies both keys

├── Decrypts disease text file

└── Diagnoses patient

**III.II Parameter Formulas:**

**Mathematical Formulae:**

**RSA Key Generation Formulas:**

**1.Select Two Large Prime Numbers (p and q):**

* Choose two distinct prime numbers, p and q.

**2.Calculate the Modulus (n):**

* Compute the modulus (n) as the product of p and q: n = p \* q

**3. Calculate Euler's Totient Function (φ(n)):**

• Calculate φ(n), the totient function of n, as follows:

φ(n) = (p - 1) \* (q - 1)

**1. Select an Encryption Exponent (e):**

• Choose an encryption exponent (e) such that 1 < e < φ(n) and e is relatively prime to φ(n). Common choices for e include 3 or 65537.

**2. Calculate the Decryption Exponent (d):**

* Calculate the modular multiplicative inverse of e modulo φ(n). This is often done using the Extended Euclidean Algorithm. The formula is:

d ≡ e⁻¹ (mod φ(n))

The public key consists of (n, e), and the private key consists of (n, d).

Here are some key variables:

* n: The modulus, used in both the public and private keys.
* e: The public exponent, used for encryption.
* d: The private exponent, used for decryption.
* p and q: The prime factors of the modulus n.
* φ(n): Euler's totient function of n.

**III.III. Features/Advantages Blockchain combined with RSA:**

The major advantages of the proposed system in this paper are as mentioned below:

Enhanced Security: By leveraging blockchain technology and encryption techniques, the system ensures robust security measures to protect sensitive patient health records. The decentralized nature of blockchain and the use of encryption mechanisms safeguard against unauthorized access, tampering, and data breaches, thereby enhancing the overall security posture of the healthcare data ecosystem.

Data Integrity and Immunity to Tampering: The utilization of blockchain technology ensures the immutability of health records stored on the platform. Each transaction recorded on the blockchain is cryptographically linked to previous transactions, creating a tamper-proof audit trail. This ensures the integrity and authenticity of patient health records, mitigating the risk of data manipulation or unauthorized alterations.

Efficient Access and Exchange of Health Records: The system facilitates efficient access and exchange of electronic healthcare records (EHRs) among patients, doctors, and administrators. Through secure digital signatures and encryption techniques, authorized users can seamlessly access and share patient health information, enabling timely diagnosis, treatment, and decision-making.

Patient Empowerment and Control: Patients are empowered to take control of their own health data and participate actively in the management of their healthcare information. By securely uploading their EHRs onto the blockchain and granting access to healthcare providers on a need-to-know basis, patients maintain autonomy over their health records while ensuring privacy and confidentiality.

Improved Care Coordination and Continuity: The secure exchange of health records facilitates improved care coordination and continuity across different healthcare providers and settings. Doctors can access comprehensive patient information, including medical history, diagnoses, and treatment plans, enabling informed decision-making and personalized care delivery.

Compliance with Regulatory Standards: The proposed system adheres to prevailing regulatory standards and requirements governing healthcare data management, such as HIPAA (Health Insurance Portability and Accountability Act) in the United States or GDPR (General Data Protection Regulation) in the European Union. By incorporating robust security measures and privacy-enhancing technologies, the system ensures compliance with regulatory mandates, thereby reducing legal and regulatory risks for healthcare organizations.

Transparency and Auditability: The use of blockchain technology provides transparency and auditability to the system. Every transaction recorded on the blockchain is visible to all authorized participants, creating a transparent and auditable record of data access and transactions. This transparency enhances trust among stakeholders and facilitates accountability in the management of healthcare data.

Reduction of Administrative Burden: By streamlining data access and exchange processes, the system reduces the administrative burden associated with managing healthcare records. Automated verification mechanisms and secure digital signatures minimize the need for manual intervention, freeing up administrative resources for more value-added tasks.

Cost-Efficiency: The system offers cost-efficiency benefits by reducing overhead costs associated with traditional paper-based record-keeping systems. By digitizing and automating processes, healthcare organizations can lower operational expenses related to storage, retrieval, and maintenance of paper records, resulting in significant cost savings over time.

Faster Diagnosis and Treatment: With seamless access to comprehensive patient health records, doctors can expedite the diagnosis and treatment process. Timely access to relevant medical information enables healthcare providers to make informed decisions and implement appropriate interventions promptly, leading to improved patient outcomes and satisfaction.

Facilitation of Research and Analytics: The system's secure and centralized repository of healthcare data facilitates research and analytics initiatives aimed at improving healthcare delivery and outcomes. Researchers and analysts can access anonymized patient data for population health studies, clinical trials, and outcome analyses, driving innovation and advancements in healthcare.

Resilience to System Failures: The decentralized nature of blockchain technology enhances the system's resilience to system failures and cyberattacks. With data distributed across multiple nodes in the network, the system remains operational even in the event of a localized failure or malicious attack, ensuring continuous availability and accessibility of healthcare records.

Empowerment of Healthcare Providers: Healthcare providers are empowered with access to comprehensive patient information, enabling them to deliver more personalized and patient-centered care. By having a holistic view of a patient's health history, healthcare providers can tailor treatment plans to meet individual patient needs and preferences, fostering better patient-provider relationships.

# **COMPARISONS**

**IV.I.** Comparison of Existing Strategies for Problem solving:

|  |  |  |  |
| --- | --- | --- | --- |
| Sl.No | Strategies | Advantages | Disadvantages |
| 1. | Centralized Storage | Streamlined Management  Controlled Access  Familiarity  Cost-Effectiveness | Single Point of Failure  Limited Scalability  Data Silos  Regulatory Compliance Challenges |
| 2. | Patient Empowerment | Enhanced Control.  Improved Engagement | Privacy Concerns  Potential for Misinterpretation |
| 3. | Access Control | Enhanced Security  Granular Permissions | Administrative Overhead  Complexity |
| 4. | Data Immutability | Enhanced Data Integrity:  Auditability and Transparency: | Inflexibility,  Data Deletion Challenges. |
| 5. | Interoperability | Enhanced Coordination of Care:  Improved Patient Outcomes | Data Security and Privacy Risks  Complexity and Implementation Challenges: |
| 6. | Security and Privacy | Enhanced security, Strong User verification, Reduced risk of unauthorized access | Complexity, Usability, Cost of Implementation, Dependency on device, Integration challenges. |

**IV.II.** Comparison of Existing Method from selected Methods (Dynamic Health Ledger methods) :

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Sl.No | Author | Methods | Advantages | Disadvantages |
| 1. | M. Meingast, T. Roosta and S. Sastry | Security and privacy issues with healthcare information technology | Efficiency and Accuracy,  Remote Healthcare. | Complexity,  Learning Curve,  Dependency on Technology. |
| 2. | L. Lamport, R. Shostak and M. Pease | The Byzantine Generals Problem | Flexibility,  Decentralization. | Performance Impact,  Resource Consumption. |
| 3. | M. Castro and B. Liskov | Practical Byzantine Fault Tolerance | Trustless and Non-Permissioned Network. | Message Overhead,  Complexity. |
| 4. | D. Ongaro and J. K. Ousterhout, | understandable consensus algorithm | Security,  Decentralization,  Immutability,  Efficiency. | Centralization Risk,  High Energy Consumption,  Vulnerabilities to Attacks,  Scalability Limitations. |
| 5. | M. Misbhauddin, A. Alabdulatheam, M. Aloufi, H. Al-Hajji, and A. AlGhuwainem, ‘‘MedAccess: | A scalable architecture for blockchain based health record management | Enhanced Security,  Improved Data, Integrity,  Decentralization,  Interoperability,  Disadvantages. | Network Congestion,  Increased Complexity,  Cost,  Regulatory Compliance,  Energy Consumption. |

# **CONCLUSION**

In conclusion, the project strives to establish a secure and decentralized platform for managing electronic healthcare records (EHRs) with efficiency and confidentiality. By leveraging blockchain technology and encryption techniques, the platform ensures the security, integrity, and accessibility of patient data for individuals, healthcare professionals, and administrators alike. Patients are empowered to securely upload their EHRs onto the blockchain, including encrypted disease text files and digital signatures. When healthcare providers request access to a patient's EHR, a secure process ensues where the patient grants approval, providing necessary digital signatures and public keys for verification. Subsequently, doctors can decrypt the disease text file, conduct diagnosis, and deliver appropriate medical interventions. Trust and transparency are prioritized through blockchain's immutable ledger, while patient empowerment is emphasized by granting control over their health records. Scalability, continuous improvement, and collaboration with stakeholders are pivotal for the project's success, ultimately aiming to revolutionize healthcare delivery and improve patient outcomes globally.

This project signifies a groundbreaking advancement by harnessing the capabilities of blockchain and encryption technologies to tackle pervasive obstacles in healthcare data management. Through decentralizing data storage and bolstering the system with robust encryption measures, the platform offers a comprehensive solution to pressing issues regarding data privacy and integrity within healthcare systems. By dispersing data storage across a decentralized network rather than a centralized repository, the platform minimizes the risk of data breaches and unauthorized access, ensuring patient confidentiality and privacy.

Moreover, the incorporation of strong encryption mechanisms further fortifies the security of patient health records, making them resistant to tampering or manipulation. This not only safeguards sensitive medical information but also fosters trust between patients and healthcare providers, reinforcing the foundation of the doctor-patient relationship.

By establishing a secure channel for information exchange between patients and healthcare providers, the platform streamlines the diagnosis and treatment processes. Healthcare professionals gain expedited access to comprehensive patient health records, enabling them to make well-informed decisions and deliver personalized care tailored to individual patient needs. This seamless flow of information facilitates timely interventions, reducing the likelihood of medical errors and optimizing patient outcomes.

In essence, the project signifies a pivotal leap forward in revolutionizing healthcare delivery by leveraging cutting-edge technologies to address longstanding challenges. By enhancing data privacy, integrity, and accessibility within healthcare systems, the platform lays the groundwork for a more efficient, transparent, and patient-centric approach to healthcare information management. Ultimately, this initiative aims to elevate overall patient outcomes, ushering in a new era of healthcare innovation and excellence..

However, the journey towards achieving comprehensive security and efficiency in healthcare data management is an ongoing endeavor. Continuous vigilance and proactive measures are imperative to adapt to evolving security threats and regulatory requirements prevalent in the healthcare sector. Therefore, key recommendations for the sustained success of the project include:

* Continuous Security Enhancements: Regular updates and enhancements to encryption algorithms and security protocols are indispensable to stay abreast of emerging threats and vulnerabilities in the healthcare landscape.
* User Education: Provision of comprehensive training and educational resources to users, encompassing patients, doctors, and administrators, is essential to instill best practices for securely accessing and managing electronic healthcare records.
* Scalability Planning: Anticipation of future growth and scalability requirements is crucial to ensure that the platform can seamlessly accommodate the burgeoning volume of healthcare data and users. Proactive planning ensures that the platform remains responsive and efficient in catering to evolving needs and demands in the healthcare ecosystem.
* Regular Audits and Compliance Checks: Implementing a regimen of regular audits and compliance checks ensures that the platform adheres to prevailing regulatory standards and industry best practices. These audits help identify and rectify any potential vulnerabilities or non-compliance issues, thereby fortifying the platform's integrity and trustworthiness.
* Community Engagement and Feedback Mechanisms: Foster a culture of community engagement by soliciting feedback from users, stakeholders, and industry experts. Incorporating user feedback and insights into the platform's development roadmap ensures that it remains aligned with the evolving needs and expectations of its user base, ultimately driving continuous improvement and innovation.

1. **REFERENCES**
2. Rui Lebre, Carlos Costa, "An Efficient and Reliable Architecture for Distributing Medical Imaging Data", *2021 International Conference on e-Health and Bioengineering (EHB)*, pp.1-4, 2021.
3. K. Swetha, C.Ishaq Shareef, G. Sreenivasulu, K. K. Baseer, M. Jahir Pasha, "Study on Implementation of Electronic Health Records using Blockchain Technology", *2023 4th International Conference on Electronics and Sustainable Communication Systems (ICESC)*, pp.607-611, 2023.
4. K. K. Baseer, B. Jaya Naga Varma, B. Harish, E. Sravani, K. Yashvanth Kumar, K. Varshitha, "Design and Implementation of Electronic Health Records using Ethereum Blockchain", *2023 Second International Conference on Electronics and Renewable Systems (ICEARS)*, pp.784-791, 2023.
5. Caspar Von Lengerke, Alexander Hefele, Juan A. Cabrera, Oliver Kosut, Martin Reisslein, Frank H. P. Fitzek, "Identification Codes: A Topical Review With Design Guidelines for Practical Systems", *IEEE Access*, vol.11, pp.14961-14982, 2023.
6. Narendra Kumar Rout, Debabrata Dansana, Nirjharinee Parida, Ranjeet Kumar Rout, "Improving Performance of Electronic Healthcare Record Management Systems (EHRMS) using Low Complexity Blockchain", *2022 Second International Conference on Computer Science, Engineering and Applications (ICCSEA)*, pp.1-5, 2022.
7. D. Ongaro and J. K. Ousterhout, ‘‘In search of an understandable consensus algorithm,’’ in USENIX Annu. Tech. Conf., 2014, pp. 305–319.
8. M. Misbhauddin, A. Alabdulatheam, M. Aloufi, H. Al-Hajji, and A. AlGhuwainem, ‘‘MedAccess: A scalable architecture for blockchainbased health record management,’’ in Proc. 2nd Int. Conf. Comput. Inf. Sci. (ICCIS), Oct. 2020, pp. 1–5.