IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 3, March 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303260 |

Global Id Generation with Verification Based Medical Record Access

C. Ashwathi[1], K.Guneha[2], K.Rajammal , M.E (Ph.D)[3]

UG Student, Dept. of CSE., E.G.S Pillay Engineering College, Nagapattinam, India [1 2]

Assistant Professor, Dept. of CSE., E.G.S Pillay Engineering College, Nagapattinam, India [3]

ABSTRACT: the cloud securely stores patient health records, guaranteeing data availability, redundancy, and scalability. To protect sensitive medical data, cloud infrastructure providers frequently use industry-leading security measures. One of the biggest challenges facing modern healthcare is how to securely and quickly share patient health details in an emergency. In order to overcome this difficulty, a revolutionary system that uses the patient's biometric data and national identity to identify them has been developed, along with a special QR code. Medical records of patients, including their personal data, medical history, and prescription information, are kept in a highly secure database that uses blockchain technology and sophisticated security mechanisms. The solution offers distinct QR codes for each patient record, a safe database to store patient data, and national identity with biometric verification for patient identification. Authorized medical personnel have secure portal access to patients' vital information in the event of data sharing. This method enables third parties (data users) to access patient data in an emergency, guaranteeing prompt and life-saving treatments. Consent procedures, strong authentication standards, and data exchange based on verification guarantee privacy and adherence to pertinent healthcare laws. The project places a high priority on data security, scalability, and usability. It also includes upgrades and ongoing maintenance to keep up with changing security requirements and healthcare technologies. By enabling quick, safe, and accurate access to critical medical data, this system seeks to transform patient care and eventually enhance healthcare outcomes.

KEYWORDS: Health record management, National ID registration, Biometric data registration, Patient record storage, Blockchain creation, QR code creation, Record distribution.

I. INTRODUCTION

The digital revolution in the quickly changing healthcare industry has resulted in the creation of cloud-based solutions for sharing and storing patient health records, especially in an emergency. This creative method combines the strength of cloud computing, strong security protocols, and instant access to medical data to enable quick and knowledgeable decision-making when it counts most. A forward-thinking method of managing healthcare data is to store patient health records on cloud servers for effective data sharing in an emergency. This cutting-edge system makes the most of cloud computing by combining regulated access, real-time updates, and secure data storage to enable quick and well-informed decision-making in emergency medical situations. Patient data is safely kept on cloud servers, which provide scalability, redundancy, and data availability in addition to strong data security. Healthcare personnel can make prompt and accurate judgments during emergencies when they have access to the most up-to-date and accurate patient information thanks to real-time updates.

By using multi-factor authentication and encryption, access to patient records is strictly restricted, making sure that only individuals with the proper authorization may access and edit the data. The system also has emergency alert features that may be activated to alert pertinent healthcare providers about a patient's condition, location, and particular needs. This helps to expedite the response time and customize care for each patient. Additionally , this system's interoperability guarantees that patient data may be easily exchanged between various healthcare facilities and clinicians, improving the general standard of treatment in emergency situations.

QR Code Creation

Computer devices use quick response (QR) codes, which are square-shaped matrices of either light or dark pixels, to encode and quickly retrieve data. QR codes are a significantly more versatile form of barcoding than regular barcodes, with a multitude of uses ranging from supply chain management to bitcoin wallet addresses. There are currently numerous QR code variants and versions that are tailored for various uses or that have increased data storage capacity.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303260 |

The square form for a QR Code structure is far more significant than barcodes. Barcodes are only retained for convenience because using a QR Code has so many benefits. Learn the rationale behind the QR code structure's square form.

- **Higher data capacity:** QR Codes can scan data in two dimensions, such as vertical and horizontal, because to their square form. They are a particularly helpful tool due to the suggested wealth of information in their little code.
- **Customization features:** These codes can also be changed to fit the look of the website or the campaign. Furthermore, the square layout makes it easier to alter the QR Codes even after they have been shown.
- **Improved error correction:** Many companies are aware that QR Codes allow for a margin error of 7 to 30% and are more damage-resistant than other forms of codes. They are therefore essential to the inventory department.
- **Easy to read:** All you need to do is download the app to your smartphone, tablet, or desktop computer and start scanning QR codes on practically any device. Modern devices have incorporated a QR Scan feature with their cameras since QR codes are here to stay.

Fog Computing

Fog computing is a distributed computing infrastructure that resides between the data source and the cloud, storing, processing, and data. Similar to edge computing, fog computing puts the power and advantages of the cloud closer to the data creation and action point. Many people mix up the phrases edge computing and fog computing since they both refer to bringing processing and intelligence closer to the site of data production. The primary reason for this is efficiency enhancement, while security and compliance concerns may also be taken into consideration. The fog metaphor comes from the meteorological term meaning a cloud close to the ground, just as fog concentrates around the edge of the network. The expression is often associated with Cisco; Ginny Nichols, the company's product line manager, is credited with coining it. The general public can access fog computing, which is registered under the name Cisco Fog Computing.

1.2.2 Components of Fog Computing

The following are some of the essential elements of cloud fog computing:

- **Edge devices:** These are the units that are located at the edge of the network and closest to the data source. Examples of edge devices include sensors, gateway routers, and programmable logic controllers, or PLCs.
- **Data processing:** Data processing is done locally on edge devices rather than being sent to a central location. This results in improved performance and reduced latency.
- **Data storage:** Edge devices can store data locally rather than sending it to a central location for storage. This improves security and privacy while reducing latency.
- **Connectivity:** Fast connectivity between edge devices and the rest of the network is necessary for fog computing to function. To do this, wired or wireless techniques are applied.

1.2.3 Types of Fog Computing

Fog computing is the term for technology that extends cloud computing and services to the edge of an enterprise's network. It enables the placement of resources, such as data and apps, nearer to or even above final users.

The following lists the four primary categories of fog computing.

- Device-level fog computing makes use of low-powered hardware such as switches, routers, sensors, and other devices. Data can be gathered with these devices and then uploaded to the cloud for analysis.
- Servers or appliances located at a network's edge are responsible for fog computing. These devices allow for the processing of data before it is sent to the cloud.
- Hardware acting as a bridge between the cloud and the edge powers fog computing at the gateway level. These devices allow for the regulation of traffic and ensure that only relevant data is sent to the cloud.
- Cloud-based servers or appliances power cloud-level fog computing. These devices may be used to process data before it is provided to end users.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303260 |

There are several reasons why fog computing is used:

- **To improve latency and performance:** Because fog nodes are typically positioned at the network edge, closer to the IoT devices themselves, they can dramatically reduce processing times and improve performance for applications that require low latency.
- **To improve decision-making:** Fog computing helps to improve decision-making in the moment since it allows real-time data collection and analysis from IoT devices.
- **To reduce costs:** The cost of data analysis and storage can also be reduced with the help of fog computing. This is because, by relocating computation and data storage closer to the network edge, fog computing reduces the amount of data that needs to be transported back to a central point for processing.

II. RELATED WORK

Mayer, et.al,…[1] created the Fog Chain design paradigm for the healthcare sector, integrating blockchain, fog computing, and IoT technologies. The Fog Chain architecture and its idea of using a differential method to overcome IoT constraints—adding an intermediary Fog layer close to the edge to enhance its capabilities and resources—are the primary contributions. Given that the patient's medical records are to be locally accessible under a Fog computing layer, Fog Chain enables nearly real-time data processing, which enhances medical professionals' reaction times and decision-making. Here, a JavaScript model prototype was created, and the hyper ledger Fabric distribution was used at the Blockchain level of the model. FogChain allows for real-time data processing, storing, and decision making when the requirements of smart contracts are met. The response time is important and needs to be considered if handling sensitive or critical information. Reducing the physical gap between components by approximating the Blockchain peer to the IoHT devices by hosting a peer inside the fog. When considering FogChain's potential uses in the healthcare industry, hospital wards and departments could use it to manage internal demands inside their infrastructure. Additionally, a FogChain that manages its sensors and ambient data gathered from devices may be installed inside patient rooms. The model is based on the idea of utilizing fog computing architecture to enhance the integration of Blockchain and IoHT, with the goal of decreasing latency in networks and increasing the amount of resources that are available at the edge.

Nguyen, et.al,…[2] suggested a unique hybrid strategy that uses edge cloud and blockchain to share and offload data for the healthcare industry. IoT health data can first be offloaded to nearby edge servers for private data processing thanks to an efficient data offloading strategy. Subsequently, software for data sharing is integrated, enabling healthcare users to share data via blockchain. Specifically, a robust access control mechanism is developed using smart contracts for access authentication in order to enable secure EHRs exchange. IoT layer is made up of numerous smart hospitals that use mobile gateways from sensor IoT devices to monitor patients in various locations, overseen by physicians. The edge layer consists of a collection of edge cloud nodes, each of which oversees a collection of adjacent IoT devices to offer distributed computing services for the healthcare industry. To provide immediate healthcare services, all computations, including data processing and analysis, are carried out at the edge layer. cloud layer that shares processed health data with end users and stores it from edge nodes. We develop four essential cloud components—admin, EHRs manager, distributed cloud storage, and smart contracts with miners and policy storage—in order to construct a cloud blockchain network. They will be covered in more detail in the section that follows. The end user layer is the network of healthcare users—patients, caregivers, and healthcare providers—who are interested in using cloud healthcare services. For example, individuals can view their medical record history, or doctors can employ cloud-based health data analysis to diagnose diseases.

Costa, et.al,…[3] created and put into use a prototype of the healthcare software Fog-Care. Performance metrics such as latency, throughput, and send rate were evaluated in a hypothetical scenario where a global integrated vaccination campaign using a blockchain, unique identity, and fog computing approach was adopted in widely dispersed locations (Brazil, USA, and United Kingdom). Three components make up the primary technology components: the adoption of the GS1 Standards, a worldwide name system, to reduce the traffic of shared healthcare data, a blockchain network for scalability and privacy support, and a fog network. Every company has a single fog node. Patients are unique individuals who have visited a hospital, clinic, or other medical facility for medical treatment. A worldwide identification number is assigned to each patient. Since the main objectives of healthcare are to prevent illness, extend life, and enhance quality of life, patients play a crucial role in the concept. A patient may possess a gadget, such a tablet or smartphone that they can use to write down and review pertinent information about them. Health data refers to past information discovered in patient medical records, including electronic health records. Generally, a mobile app allows the patient to view their health data. Typically, the hospital stores this data, and the

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303260 |

doctor uses software to retrieve it. All information located outside of the local and necessary data is included in the global data. This information includes medical records from other clinics, hospitals, etc., to which access is subject to patient authorization. The information may be kept on a blockchain that is shared with every affiliated medical facility.

T. de Oliveira, et.al,…[4] created a procedure that enables all treatment teams involved in the emergency care to safely decrypt relevant data from the patient's electronic medical record and update new information about the patient's status. The method safely allows many treatment teams to share EMRs via a cloud platform. The proposed system combines emergency protocols with the attribute-based encryption (ABE) technique. Token authentication is also used to provide and restrict access throughout the acute stroke treatment timeline. Here, we illustrate the security of our method by creating a simulator that is computationally equivalent to the real protocol. Furthermore, illustrate below how resistant the recommended approach is to the various attacks specified in the threat model. When the patient arrives at the first hospital, the ambulance teams and call center leave the emergency department. Revocation of τe should be possible right away by the call center. The ambulance personnel is allowed extra time to enter their reports into the patient's medical file once they get to the hospital, though. Generally speaking, τh needs to be canceled after a patient leaves hospital emergency care. If the patient needs to be transferred for medical attention, their token from the first hospital will be revoked as soon as they arrive at the second. The moment the MA learns of the patient's arrival or departure from hospital emergency care, it tells the CSP of the revocation of the access token Therefore, even if a token is still valid according to the predetermined expiration date, the CSP will not provide any form of access to the data after the revocation. The suggested method enables medical professionals to decrypt encrypted patient data by using time-based tokens given during an emergency. When the tokens expire, the users' access to the patient's data is blocked. We show the security of our solution using both simulation-based security and direct attacks on the protocol.

Ganiga, et.al,…[5] provides a framework for EHR security that addresses the availability, confidentiality, and integrity of medical records. The EHR system's hazards are represented by the STRIDE modeling tool, and the degree of risk is assessed using DREAD. The security of the EHR system is the main concern at every level of the healthcare system. A security paradigm for cloud-based electronic health record systems is proposed by this study. The EHR system's hazards are represented by the STRIDE modeling tool, and the degree of risk is assessed using DREAD. Mitigation strategies have been studied and numerous exploits and vulnerabilities have been uncovered. The suggested approach safeguards the medical data entered, kept, and updated in the cloud-based EHR database. It gives healthcare application developers an organized security approach, allowing them to assess security risks and determine the best countermeasures. The framework also includes security guidelines that guarantee the confidentiality, integrity, and security of the EHR system, such as technical, administrative, and physical measures. By linking all tiers of the public health system, regardless of geographic borders, the Electronic Health Record (EHR) holds the potential to deliver real-time patient and demographic data. When sharing health information at different levels of healthcare, the main concern is the security of the electronic health record. The client is the initial component of an EHR system that is visible. It is necessary in order to enter, retrieve, and modify health data. It follows that this component is expected to be the target of the biggest attack. The second most visible part of the system is the server. The compromised server is completely under the attacker's control. Server assaults can completely damage the system and reveal, alter, or erase health information. A network compromise during data transmission allows for eavesdropping, altering, and other activities. The attacker's main goal is to target the system's visible components, like the client, server, and networks.

III. BACKGROUND OF THE WORK

The current manual method of storing health records, which depends on tangible formats like paper records or hard copies, has many drawbacks, particularly in an emergency. The main challenge is the restricted accessibility. Usually kept in filing rooms or cabinets, these paper records can make it difficult to quickly and easily retrieve them in an emergency. There may be dire repercussions if vital patient data is not retrieved quickly. Additionally, data inconsistencies and out-of-date information can be found in paper records, which could mislead medical professionals in an emergency. Retrieval inefficiency is yet another important problem. It takes a lot of time and stress to sift through a lot of papers in order to locate specific medical records when under pressure. Paper records' restricted mobility can also make it difficult to use them in emergency situations that happen outside of healthcare facilities or during patient transfers between facilities. Moreover, there is always a chance that paper records would be lost, damaged, or destroyed as a result of natural disasters like fires or floods, which could cause the irreversible loss of crucial patient data. In a manual system, security and privacy are jeopardized since it may be simpler for unauthorized individuals to obtain private patient information. Physical security is a never-ending task. Furthermore, in a manual system, getting patient consent and authorization for exchanging records—a requirement mandated by privacy laws—is frequently a laborious procedure. Decision-making and emergency care may be delayed as a result. Ultimately, the manual system is a resource-intensive and less sustainable strategy because it requires a large amount of administrative staff, physical

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303260 |

space, and record maintenance. Due to these difficulties, switching to more effective, safe, and easily available electronic health record systems is becoming more and more necessary, especially in times of dire need.

IV. SECURE HEALTH RECORD SHARING WITH UNIQUE IDENTIFICATION BASED VERIFICATION

Patient information management will be completely transformed by the Patient Record Register with National Identity Integration, Blockchain-Based Data Storage, Global ID Generation, and QR Code Data Transfer system. The system creates a safe connection to reliable identification sources by incorporating national identity verification into the patient record registration procedure, guaranteeing the authenticity and correctness of patient data. A further degree of security and immutability is added when biometric data is stored on a blockchain, protecting patient records from unwanted changes. By combining national identity and biometric data, the global ID generation process generates a single, standardized identifier that cuts through traditional silos and encourages interoperability amongst healthcare systems worldwide.

The method takes one step further in the field of data transfer by creating QR codes linked to the global ID. Because they are simple to scan, these QR codes provide a quick and safe way to send patient data. This QR code-based data transfer technique simplifies access to vital health information in many situations, for emergency responders, healthcare providers, and patients alike. The blockchain's decentralized structure guarantees data privacy and integrity, and the system complies with strict security guidelines to protect patient data. Furthermore, the QR code function improves patient involvement by giving people direct choice over the sharing and distribution of their medical records. In addition to addressing the difficulties associated with patient identification and data sharing, this all-encompassing strategy puts healthcare organizations in a strong position to prosper in the age of digital transformation. It establishes the framework for a healthcare ecosystem that is more patient-centered and networked, encouraging cooperation among various healthcare providers while placing a premium on security, privacy, and the smooth transfer of patient data across international borders.

The integration of national identity, biometric data, blockchain technology, and QR codes in the global patient ID generation system poses a number of possible issues that need to be resolved to assure the system's success and efficacy. First of all, there are serious worries about the security and privacy of the private patient data that is gathered, including biometric and national identity information, which calls for strong safeguards against illegal access and data breaches. Furthermore, the attainment of interoperability with current healthcare systems is a multifaceted challenge because different locations and providers utilize different protocols and technology. Because differences in biometric characteristics and technological constraints may affect identification accuracy, the accuracy and dependability of biometric authentication techniques also need to be carefully considered. Furthermore, even while blockchain technology has advantages like data immutability and decentralization, as the system grows, scalability and performance problems could occur, requiring careful design and optimization. Regulatory compliance, which necessitates adherence to various legal standards across jurisdictions, adds another degree of complexity. This is especially true with regard to healthcare regulations and data protection legislation. Concerns regarding privacy, security, and usability may also make it difficult for users to use the system, which emphasizes the significance of establishing credibility and proving the system's dependability. It's also crucial to put strong verification procedures in place for QR codes to stop fraud and illegal access. Lastly, infrastructure and resource limitations may make it difficult to carry out a project; therefore, funds and resources must be carefully allocated in order to install and maintain the essential infrastructure. To ensure the effective deployment and long-term viability of the global patient ID system, addressing these issues calls for concerted effort, stakeholder participation, and a proactive risk management strategy.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303260 |

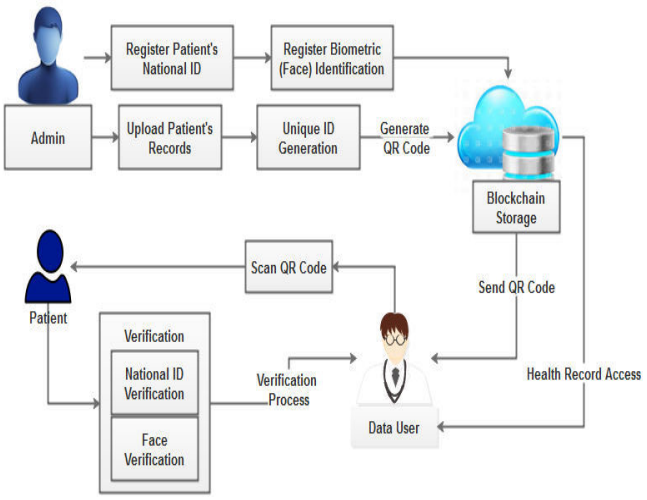

Fig 1: Proposed Framework

The proposed health record sharing using unique ID generation and verification process has the following modules,

Data Sharing Framework

Create a framework that combines national identity systems, biometric data, and global ID generation; a multifaceted strategy is used. Real-time patient information validation and synchronization are ensured by the framework's secure API interfaces with national identity databases. Using cutting-edge encryption methods, biometric information—such as fingerprints or facial recognition—is safely collected and connected to the patient's global ID. A blockchain-based infrastructure's smart contracts ensure the smooth integration of these parts and enforce stringent permission management and access constraints. By cross-referencing patient identities with reputable national databases, this framework not only ensures patient identity correctness but also improves security via biometric verification. The final product builds a stable and compatible framework that supports patient data privacy and dependability while complying with legal requirements for identity management in the healthcare industry.

National Id Registration

Connects and validates patient records with formal identity documentation by integrating with national identity systems. The seamless integration of a patient's official national identification information into the healthcare data ecosystem is known as national identity integration, and it occurs within the framework of the patient record management system. To confirm the veracity of the patient's identity, the module communicates with official or government identity verification services. This integration aligns with government-issued identity documents and improves the standardization, legitimacy, and correctness of patient records.

Bio-metric Data Registration

The biometric data registration process for patients entails the acquisition and retention of distinct facial features for the purpose of identification. Following feature extraction, distinguishing traits including the separation between the eyes, nose shape, and face contours are found in the collected facial photos. These features are analyzed by the Haar Cascade algorithm, which generates a distinct biometric template that depicts the patient's facial traits. The face traits that are retrieved are transformed into a biometric template, which is an individually unique mathematical representation. In order to preserve patient privacy and guarantee data security, the template is safely kept in a database and frequently encrypted. The process of biometric registration in healthcare systems improves security, precision, and effectiveness.

Upload Patient Record

An essential component of healthcare systems is the Patient Data Upload for Global ID Generation module, which makes it possible to safely transfer patient data to a central server in order to create distinct global identifiers. Through strong encryption mechanisms, access controls, and adherence to data protection laws, this module guarantees the integrity and privacy of patient information. It includes features like server-side validation, error management, and data standardization to ensure the correctness and quality of the provided data. The upload process is made accountable and transparent by the module by enforcing strict authentication procedures and keeping thorough records. After data transmission is successful, the module starts generating global identifiers using secure methods, which promotes a standardized and interoperable method of patient identification in a variety of healthcare settings. The system

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303260 |

contributes to a smooth and effective worldwide healthcare information exchange system by giving data security, privacy, and regulatory compliance first priority.

Blockchain Creation

To ensure a complete and accurate depiction of the patient's identity, integrate the national identity systems and biometric data with the global ID generation process. Securing, interoperable, and globally unique identification of uploaded patient data requires a methodical process that is carried out while creating a unique global ID and storing it on a blockchain. In order to improve the integrity, privacy, and accessibility of medical records, a blockchain for uploaded patient data storage must be created. This can be done by taking advantage of the decentralized and secure characteristics of blockchain technology. To improve security, create unique identifiers (hashes) for every piece of data using a cryptographic hashing technique like SHA-256. Establish a uniform data format for medical records so that the blockchain is consistent. Provide the information that is required while protecting patient privacy and adhering to data protection laws.

QR Code Creation

A critical component in the modernization of patient data management systems is the creation of a QR code based on a globally unique ID. Through the process, a scannable QR code with the unique identification linked to a patient's records is created, allowing for quick and secure access to relevant health information. To guarantee dependability, the encoding incorporates error correction features through the use of recognized QR code standards. Simplified identification procedures are made possible by the effective linkage to patient data made possible by the QR code's integration with pertinent healthcare applications. Patient education programs make sure that people are aware of the value of QR codes and how they can improve privacy and accessibility when retrieving medical records using a unique global identifier.

Record Distribution

Encoding crucial health data into a scannable QR code format, such as a distinct global ID or a link to the patient's records, is the first step in distributing a patient's data via a QR code. A safe and effective way to share patient data is using this QR code. Using a mobile device or specialized scanner, healthcare providers or authorized workers can scan the QR code to gain access to the patient's information. Only those with permission can access and examine the patient's records thanks to a secure authentication mechanism that is triggered by the scanning procedure. In healthcare settings, this approach improves data delivery speed and accuracy while upholding essential security and privacy protocols to facilitate simplified workflows. Furthermore, the distribution method respects patient permission and privacy preferences, in line with regulatory requirements and encouraging a patient-centric approach to healthcare data management.

METHODOLOGY

HAAR CASCADE ALGORITHM

A crucial phase in the Haar Cascade technique is feature classification, in which a classifier that can differentiate between positive and negative samples is trained using the chosen features. Here are the steps involved in feature classification using Haar Cascade:

Prepare training data: The first step is to prepare the training data, which consists of both positive and negative samples. Positive samples are images that include the object of interest; negative samples are images that do not include the object.

Extract Haar-like features: Haar-like features are extracted from each image using the steps outlined in the previous answer.

Train the classifier: Using the retrieved features, a classifier is trained in the following phase. The Viola-Jones technique, which use Adaboost to choose the best features that can correctly categorize the images, is the most widely used classifier in Haar Cascade. The algorithm gives each sample a weight during training, and then iteratively chooses the best features to reduce the classification error.

Create a cascade classifier: After training, the classifier is split up into various phases, with a number of weak classifiers in each stage. By swiftly rejecting non-object parts of the image, the cascade classifier minimizes the amount of computing required.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303260 |

Test the classifier: Testing the classifier on a fresh image or video stream is the last stage. A sliding window is used to scan the image at various scales, and the Haar-like features are computed at each point. Each window is then subjected to the cascade classifier, and if the object is found, a bounding box is formed around it.

BLOCKCHAIN TECHNOLOGY

Blockchain is a decentralized, reliable, publicly accessible ledger of transactions over which no single person has total control. An rising amount of encrypted transaction data records are managed by this distributed database, which keeps them apart from other records to prevent alteration and manipulation. Consortium, private, and public blockchains are the three types that exist. The blockchain's cornerstone is the block. Each block has a header and a body that contains the transactions that are being written to the system. The timestamps for the block and the transactions are contained in the block's header, together with information about the block such as its prior hash, nonce value, and difficulty. It is estimated that the block's length varied from 1 to 8 MB. The header of the block to be inserted is the only thing that identifies it.

Each block in a blockchain is made up of the following headers.

Previous Hash:

This hash address identifies the preceding block.

Transaction Details:

Details about each transaction that needs to happen.

Nonce:

A random number assigned by cryptography to distinguish the block's hash address is known as a once.

Hash Address of the Block:

The transaction data, the nonce, and the previous hash are sent via hashing. This method yields a unique output known as the "hash address," which is a 256-bit value with 64 characters in length. As a result, it is referred to as the block hash. Many people use computer methods that satisfy predetermined criteria in an attempt to determine the correct hash value. Once the predefined condition is satisfied, the transaction is finished. To put it simply, blockchain miners attempt to solve a challenging mathematical challenge known as the proof of work problem.

Block and Hash Generation

1. A Block that includes details on current transactions.
2. Each piece of data produces a hash.
3. A hash is a combination of letters and integers.
4. Transactions are recorded in the chronological order that they took place.
5. The hash is based on both the hash of the most recent transaction and the hash of the one before it.
6. The hash is completely altered by each change made to a transaction.
7. To check that a transaction has not been altered, the nodes look at the hash.
8. If the majority of nodes approve a transaction, the transaction is included to the block.
9. The Blockchain is composed of separate blocks, each of which has a connection to the one before it.
10. A blockchain functions because copies of it exist on several computers, each with a copy of it.

V. CONCLUSION

In summary, a major development in healthcare technology is represented by the project of implementing a national identity and face verification system with a QR code-based patient health record storage and sharing system. It uses biometric data verification and national identity verification to provide patient identification. The combination of vital health information sharing, real-time health data updates, and QR code-based data exchange, which eventually improves patient outcomes and care. The system ensures the greatest level of patient data security through strict security measures and compliance with data protection rules. The healthcare industry is always changing, and this project's creative solutions will not only improve emergency response times but also pave the way for a future where healthcare is more patient-centered and technologically sophisticated.

REFERENCES

[1] Mayer, André Henrique, Vinicius Facco Rodrigues, Cristiano André da Costa, Rodrigo da Rosa Righi, Alex Roehrs, and Rodolfo Stoffel Antunes. "Fogchain: a fog computing architecture integrating blockchain and internet of things for personal health records." IEEE Access 9 (2021): 122723-122737.

[2] Nguyen, Dinh C., Pubudu N. Pathirana, Ming Ding, and Aruna Seneviratne. "A cooperative architecture of data offloading and sharing for smart healthcare with blockchain." In 2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), pp. 1-8. IEEE, 2021.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303260 |

[3] Costa, Humberto Jorge De Moura, Cristiano Andre Da Costa, Rodrigo Da Rosa Righi, Rodolfo Stoffel Antunes, Juan Francisco De Paz Santana, and Valderi Reis Quietinho Leithardt. "A fog and blockchain software architecture for a global scale vaccination strategy." IEEE Access 10 (2022): 44290-44304.
[4] T. de Oliveira, Marcela, Alexandros Bakas, Eugene Frimpong, Adrien ED Groot, Henk A. Marquering, Antonis Michalas, and Silvia D. Olabarriaga. "A break-glass protocol based on ciphertext-policy attribute-based encryption to access medical records in the cloud." Annals of Telecommunications 75 (2020): 103-119.
[5] Ganiga, Raghavendra, Radhika M. Pai, and Rajesh Kumar Sinha. "Security framework for cloud based electronic health record (EHR) system." International Journal of Electrical and Computer Engineering 10, no. 1 (2020): 455.
[6] Masud, Mehedi, Gurjot Singh Gaba, Karanjeet Choudhary, Roobaea Alroobaea, and M. Shamim Hossain. "A robust and lightweight secure access scheme for cloud based E-healthcare services." Peer-to-peer Networking and Applications 14, no. 5 (2021): 3043-3057.
[7] Kumar, Mahender, and Satish Chand. "A secure and efficient cloud-centric internet-of-medical-things-enabled smart healthcare system with public verifiability." IEEE Internet of Things Journal 7, no. 10 (2020): 10650-10659.
[8] Abunadi, Ibrahim, and Ramasamy Lakshmana Kumar. "BSF-EHR: blockchain security framework for electronic health records of patients." Sensors 21, no. 8 (2021): 2865.
[9] Zhuang, Yan, Lincoln R. Sheets, Yin-Wu Chen, Zon-Yin Shae, Jeffrey JP Tsai, and Chi-Ren Shyu. "A patient-centric health information exchange framework using blockchain technology." IEEE journal of biomedical and health informatics 24, no. 8 (2020): 2169-2176.
[10] Zghaibeh, Manaf, Umer Farooq, Najam Ul Hasan, and Imran Baig. "Shealth: A blockchain-based health system with smart contracts capabilities." IEEE Access 8 (2020): 70030-70043.
[11] Li, Jiaxing, Jigang Wu, Guiyuan Jiang, and Thambipillai Srikanthan. "Blockchain-based public auditing for big data in cloud storage." Information Processing & Management 57, no. 6 (2020): 102382.
[12] Rajput, Ahmed Raza, Qianmu Li, and Milad Taleby Ahvanooey. "A blockchain-based secret-data sharing framework for personal health records in emergency condition." In Healthcare, vol. 9, no. 2, p. 206. MDPI, 2021.
[13] Al-Jaroodi, Jameela, Nader Mohamed, and Eman Abukhousa. "Health 4.0: on the way to realizing the healthcare of the future." Ieee Access 8 (2020): 211189-211210.
[14] Qiu, Han, Meikang Qiu, Meiqin Liu, and Gerard Memmi. "Secure health data sharing for medical cyber-physical systems for the healthcare 4.0." IEEE journal of biomedical and health informatics 24, no. 9 (2020): 2499-2505.
[15] da Costa, Leonardo, Billy Pinheiro, Roberto Araújo, and Antônio Abelém. "A decentralized protocol for securely storing and sharing health records." In 2019 IEEE International Conference on E-health Networking, Application & Services (HealthCom), pp. 1-6. IEEE, 2019.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details