Voice Biometric Access Control in Blockchain-Enhanced Electronic Health Records

Prashnatita Pal * and Rituparna Bhattacharya

Posted Date: 8 May 2026

doi: 10.20944/preprints202510.1587.v2

Keywords: voice authentication; blockchain; electronic health records; wireless communication; data security

 doi:10.20944/preprints202510.1587.v2

Article

Voice Biometric Access Control in Blockchain-Enhanced Electronic Health Records

Prashnatita Pal [1,*] and Rituparna Bhattacharya [2]

[1] Department of Electronics & Communication Engineering, St. Thomas College of Engineering & Technology, Kolkata, India

[2] Department of Computer Science & Engineering, Techno India University, West Bengal, India

* Correspondence: prashnatitap@gmail.com

Abstract

Securing electronic health records (EHRs) is critical in the modern healthcare landscape, where digital transformation enhances connectivity and data-driven decision-making. This paper introduces a secure framework that integrates voice-based authentication, blockchain technology, and machine learning to protect EHRs, particularly in IoT-enabled, high-frequency wireless communication environments. The new distributed system utilizes blockchain technology to improve the security and integrity of medical records. Voice authentication, which incorporates a biometric element, facilitates user verification. A working model was designed to show the system's feasibility along with a case study on heart health monitoring. Simulated results demonstrated better block creation time, transaction latency, and validation accuracy.

Keywords: voice authentication; blockchain; electronic health records; wireless communication; data security

I. Introduction

Extensive electronic health or medical records (EH/MRs) facilitate the retrieval and management of patient documentation by healthcare providers. This modification is associated with the increased utilization of EHRs, which require the safeguarding of sensitive medical information. With greater dependence on computers to store sensitive medical information, an increase in information breaches, unauthorized access, identity theft, and the erosion of patient privacy become a concern. Advanced protection mechanisms are vital to secure EHRs in the contemporary face of danger to patients' privacy and trust in the healthcare system. In the past decade, standard username-password combination authentication systems impeded access to EHRs. These methods, however, do have some gaps, which include phishing, poor password choices, and the sharing of passwords, leading to increased vulnerability to unauthorized access and potential breaches of sensitive patient information. Eliminating the requirement of a physical token with a device that can capture biometric features such as fingerprints can improve the security of electronic health records while making it easier for the patients. Voice verification, a form of biometric authentication, could be invaluable in the medical field. In healthcare, specialists and patients may be identified using voice authentication, which utilizes different speaking characteristics and patterns, thereby enhancing security and streamlining access to medical information. Additionally, develop a decentralized blockchain technology for managing private health records in the healthcare field. Health records in the healthcare field. This study outlines a method for securing electronic healthcare records within the healthcare industry that relies on voice authentication, blockchain, and high-frequency wireless transmission. The work aims to accomplish several things, but its primary goals are to investigate the viability and efficacy of voice authentication as an extra safeguard for EHRs, to evaluate its influence on user processes and acceptability, and to handle any obstacles and legal concerns. AI-powered speech recognition through the Internet of Things is also used here. From the two options shown,

 doi:10.20944/preprints202510.1587.v2

choose one kind of voice authentication that best suits your needs. Our discussion of the voice enrollment process, authentication techniques, and security measures used to safeguard the voice biometric data and related EHRs will take us into the technical parts of voice authentication in the sections that follow. We will also provide the results of a thorough usability test that looked at how healthcare providers and patients felt about using the voice authentication system. Finally, the article analyzes the implications of using the fusion of voice identification and blockchain technology in healthcare and outlines the advantages of the proposed approach. Through this research, we aim to further the ongoing efforts to enhance the protection and privacy of health data by providing a detailed explanation of this new security framework. We analyze the execution of the prototype of our proposed approach under "Evaluation and Execution," assessing its security and effectiveness.

II. Related Works

The increasing adoption of electronic health and medical records (EHRS/EMRS) has revolutionized the way health service providers access and manage patient data. With this shift, protections have become sensitive medical information, considering the risk of unauthorized access, data leaks, and identity theft. Traditional security measures such as passwords have proven susceptible to threats such as phishing and weak registration management [1]. To correct these defects, the biometric method pays attention to its reliability and user-friendliness. Among them is language authentication as a user—a friendly and secure way to check your identity using your own vocal features [2]. At the same time, blockchain technology provides a decentralized and operational framework that improves data exchange and simultaneously maintains trust and security. It examines the practicality of integrating language authentication into medical work processes, examines user acceptance, and highlights potential regulatory considerations [3]. This approach also includes AI-driven speech recognition, which allows for flexible adaptation of authentication strategies. Usability analysis of health occupation members and patients assesses the effectiveness of the system [4]. Ultimately, we hope to contribute to further development of secure infrastructure for digital health by presenting the possibilities of this integrated approach. This research studies the benefits and challenges of blockchain implementation in healthcare systems [5]. A recurring problem is the fragmentation of patient files. This issue is because people are often sourced from multiple providers. This leads to distributed data storage and restricts access to patient history information [6]. As a rule, patients do not continue to control these records due to legal orders of certain jurisdictions or procedural standards, which can create barriers to accessing their own health information and understanding their medical history. According to HIPAA (Health Insurance Portability and Accountability), health service providers have a 60-day window to respond to patient inquiries regarding changes or deletion of records but are not obligated to comply with [7]. Establishing safe and consistent communication between agencies is complicated by including several stakeholders, such as hospitals, doctors, and insurance companies, which can lead to misunderstandings and delays in information sharing. Decentralization provides improved security and trust in data exchange but can be ignored if malicious insiders are using access, which highlights the need for robust monitoring and access controls to mitigate these risks. Memory limits also provide practical challenges. Medical files such as test results, images, and documents use critical storage space that makes efficient and scalable solutions essential. Despite growing global interest in blockchain, standardization is not sufficient [9]. Many health groups are reluctant to share patient files due to competition concerns, data protection risks, or economic motivations, which can hinder collaboration and the overall improvement of healthcare services, ultimately leading to fragmented care and missed opportunities for better patient outcomes. To facilitate data exchange, trust must be cultivated among all parties. This is vital to providing effective care. Without robust protection measures, these systems are susceptible to cyber threats [10]. Extended hacking tools can bypass traditional security protocols and put sensitive health data at risk, leading to potential breaches that can compromise patient privacy and safety. Therefore, reliable infrastructure and effective measures are essential [11]. There is also the technical acceptance of human factors in patients and members of

 doi:10.20944/preprints202510.1587.v2

health occupations. Some agencies continue to rely on paper-based records, while others strive to protect encryption and access protocols. Resistance is often based on uncertainty or complaints about digital systems, particularly regarding their reliability, user-friendliness, and the potential for data breaches. Ethical concerns, particularly concerns about data confidentiality, remain fundamental to patient provider relationships [12]. Ensuring secure access through encryption, user authentication, and regular data backups is important to maintaining trust. Nevertheless, concerns regarding data ownership, access control, and network scalability should be considered [13], as these factors can significantly impact the effectiveness of security measures and the overall integrity of patient data management. The integration of asymmetric encryption methods and AI-based monitoring can help improve security and, at the same time help to maintain system transparency [14].

III. System Architecture for Electronics Healthcare System

The proposed device is designed to be up-to-date, providing a cozy and decentralized framework for dealing with electronic health information (EHRs) through a blockchain-enabled infrastructure. This structure helps a distributed ledger environment in which a couple of legal entities—along with hospitals, clinics, sufferers, and researchers—can take part in statistics management with defined right of entry and updated privileges. Depending on privacy requirements and operational goals, the device can be implemented as a private, public, or consortium blockchain network. Every model defines precise regulations for getting admission, updated control, information sharing, and governance among participating nodes. The center additives of the gadget are as follows: I. Consumer Registration and Authentication: This module manages consumer onboarding and identification verification. It creates and continues virtual identities for patients and scientific staff and is up-to-date. Every user undergoes a comfy, up-to-date registration method. Make certain that the simplest legal members can get admission updated and interact with the system. ii. Healthcare provider control This phase governs the registration and verification of service companies, inclusive of updated hospitals, laborious dairies, and clinics. The handiest tested entities can deliver services or up-to-date fitness records. This phase guarantees the integrity and trustworthiness of companies in the community. iii. Profile control machine This face update handles the advent, update, and tracking of user profiles. Patients can manage non-public data and set possibilities, while healthcare providers can list qualifications, specializations, and different credentials. iv. Smart Contracts Those contracts outline the terms of interplay between specific stakeholders—sufferers, companies, and establishments. They include permissions, information-sharing seeing eye-to-eye updated, treatment propanediols, and economic agreements. Smart contracts make sure that everyone's interactions comply with agreed-upon regulations and that execution is automatic and verifiable. v. Patient data up-to-date management This module enforces strict control over who can get entry updated, up-to-date patient information. Up-to-date is granted based on the consent recorded in clever contracts and affected person-defined settings. All transactions are logged on the blockchain for traceability and duty. vi. Continuous Enhancement and Remarks Loop The architecture supports modular improvements, allowing up-to-date development based on user remarks, rising threats, and advances in generation. Regular updates ensure the device stays comfy and efficient. vii. Integration and Interoperability Layer To facilitate collaboration among various entities, this residue guarantees seamless conversation and fact trade. It lets in exceptional system modules' updated features cohesively, bridging gaps among special technologies or structures. viii. Consumer-Centered Interfaces The device emphasizes intuitive and responsive interfaces for both sufferers and healthcare providers. Those interfaces help a extensive variety of obligations, up-to-date having access to updated clinical information, managing permissions, and interacting with providers, at the same time as administrative updates simplify operations for backend cuspidated.ix. Scalability and performance optimization The system is designed for scalability to accommodate expanding consumer bases and large volumes of clinical data. Load balancing, records caching, and optimized algorithms make certain that performance stays high as the network grows, ensuring that the system can handle increased user demand and data processing

 doi:10.20944/preprints202510.1587.v2

without degradation in speed or efficiency. The figures (which include architectural diagrams and system fashions referenced in Figures 1 and 2) may be retained from your authentic paper, but up-to-date ones should be redrawn or tailored if they came from a third-birthday party supply to avoid visual plagiarism.

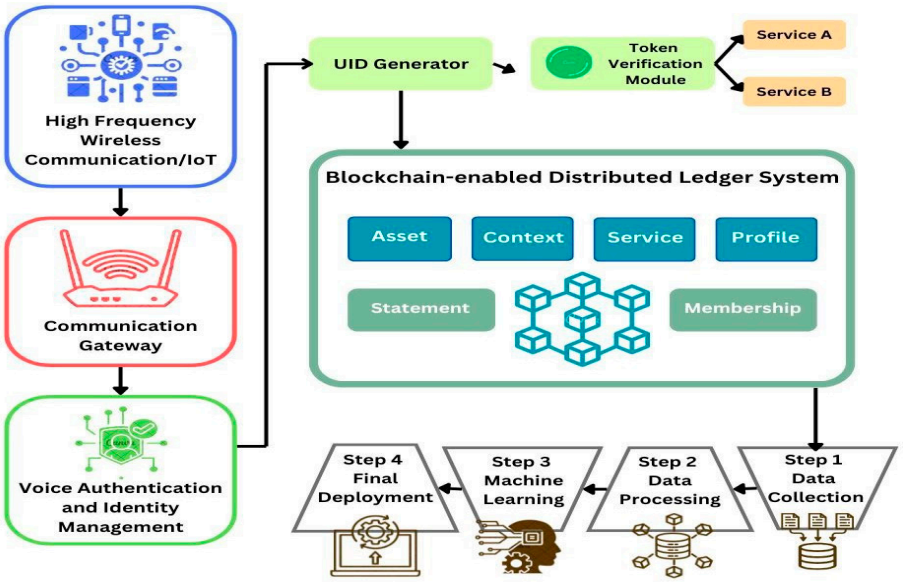

Figure 1. System architecture: Electronic Health Records System Based on Voice Authentication Management.

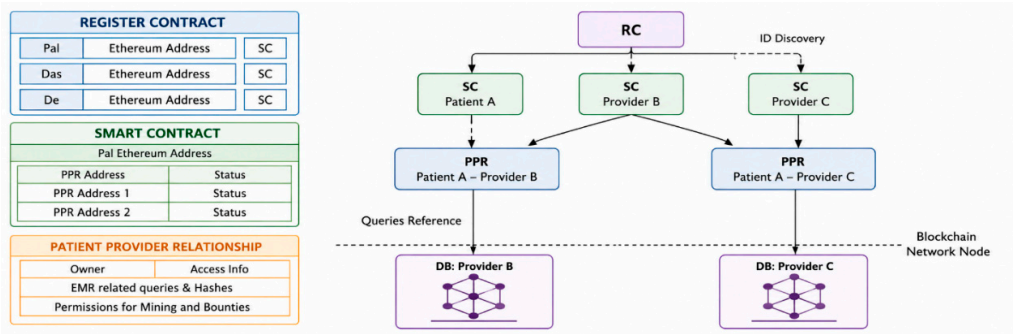

Figure 2. Modelling how blockchain works as a structure for EHR.

IV. Voice Authentication-Based Identity Management Is Integrated with Blockchain Technology

Voice authentication, also referred to as voice biometrics, uses unique characteristics of an individual's speech to confirm their identity. Unlike traditional credentials such as passwords or PINs—which are prone to theft, sharing, or forgetting—voice authentication provides a more natural and secure verification method. This approach is especially relevant in scenarios where users need hands-free, secure access, such as in healthcare or high-risk environments.

Advancements in artificial intelligence (AI) and signal processing have significantly improved the accuracy of speech recognition systems. These technologies can now detect, process, and verify voice patterns with high reliability. Within the proposed framework, two types of voice authentication mechanisms are considered:

 doi:10.20944/preprints202510.1587.v2

1. **High-frequency wireless voice authentication**—which uses advanced transmission techniques but may be costlier and slower to deploy.

2. **AI-powered voice recognition**—which integrates directly with IoT and blockchain systems, offering scalability and real-time analysis, though it requires robust integration efforts for secure deployment.

A. Benefits and Integration with Blockchain

Integrating voice authentication with blockchain enhances security and trust. While voice serves as the biometric layer, blockchain ensures data immutability, decentralized access control, and auditability. The parameters in Figure 3 include SC for Summary Contact, RC for Registered Contact Administration, and PPR for Patient Service Provider Administration, which address various challenges in healthcare security, such as unauthorized access, identity fraud, and data tampering. Secure infrastructures increasingly utilize AI-enhanced voice systems. When paired with blockchain, these systems verify identity and maintain a tamper-proof record of authentication events. For instance, only a successful voice match can grant access to sensitive health data, and all access attempts are logged immutably. Moreover, blockchain's decentralized structure allows the system to operate without a single point of failure, significantly reducing the risk of insider threats or external attacks.

B. Key Components of the Integrated System

The system successfully meets its requirements according to a specific workflow:

i. The voice enrollment stage deals with capturing voice samples, reception, and producing the necessary biometric templates, or voiceprints. These templates are generated and safeguarded either on the blockchain or through secure off-chain storage that is encrypted and associated with the blockchain.

ii. Voice sample authentication. Standard authentication procedures verify whether users utter a certain phrase. Incoming samples are matched against the voiceprint and the system outputs an authentication confirmation event on the blockchain.

iv. Restriction of access via smart contracts: Access management policies are implemented by way of smart contracts. They set up the rules, including who and under which authentication is allowed to access certain data. Voice recognition systems can be used to trigger specific operations and authorize certain information exchanges.

v. The immutable audit trail is enhanced regardless of whether the authentication is successful or not. In addition, it serves compliance to scrutinize regulations for forensic investigation (actor disputes).

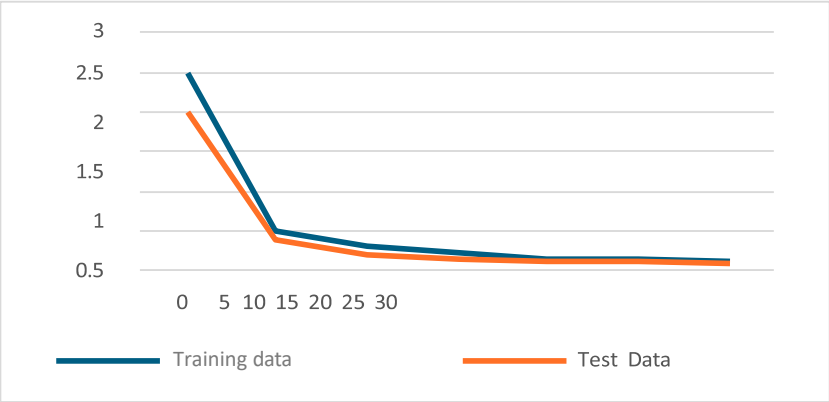

Figure 4. Epoch losses between train data and test data.

 doi:10.20944/preprints202510.1587.v2

C. Security Implications and Use Cases

In healthcare environments, especially those transitioning into smart city infrastructures, digital access points must be rigorously protected. Voice authentication, combined with blockchain, allows for secure gateways to systems such as patient portals, diagnostic data, and remote monitoring tools.

Potential use cases include:

· Hospital record access control

· Secure transmission of sensitive diagnostics

· Voice-activated emergency alert systems

· Access control for wearable or mobile health devices

With the ability to detect anomalies (e.g., voice spoofing attempts or abnormal access patterns), AI-enhanced voice systems can further fortify system integrity. This approach also reduces reliance on vulnerable systems like passwords or smart cards. Voice samples collected include phonation of vowels, noises, breathing noises, and counting numbers quickly and slowly. Further details included in the metadata include the following: gender, age, location, present health state, and comorbidities, if any. Figure 4 demonstrates that the epoch loss of the test data is less than that of the training data. The model is successfully generalizing to the testing data when the test and train lines converge toward the end of the graph [20]. The model's ability to adapt to new, unknown data and produce correct predictions is shown by this convergence. The fact that the test and train lines are in perfect alignment shows how reliable the model is and how useful it may be in the real world. We evaluated the performance of the speech recognition system using a specific test dataset of one hundred audio files. In this dataset, there were ten audio files total, one for each of the ten speakers included in the training set. We evaluated the system's performance on this test dataset and found it to be 87% accurate. The system correctly identified 100 out of 103 audio files.

V. Performance Evaluation and Experimental Findings

A. Accuracy in Testing

Testing specificity, accuracy, and sensitivity are the three metrics used to assess the performance. The developed voice authentication model undergoes assessment using three metrics: testing specificity, accuracy, and sensitivity. They employ an optimization algorithm created by Jaya.

Table 1. Performance across Iterations (JHBO-based DNFN).

Iteration	Accuracy	Sensitivity	Specificity
25	0.915	0.915	0.914
45	0.936	0.9273	0.925
65	0.945	0.9305	0.938
85	0.944	0.9307	0.967
115	0.957	0.9515	0.970

Table 2. Comparative Performance with Other Methods.

Metric	MFCC	HMM	GMM	Proposed (JHBO-DNFN)
Accuracy	0.8956	0.8910	0.8910	0.8979
Sensitivity	0.885	0.8831	0.8813	0.9107
Specificity	0.9164	0.8963	0.9031	0.9221

In a **k-fold analysis**, the proposed method continued to show superior performance:

 doi:10.20944/preprints202510.1587.v2

Metric	MFCC	HMM	GMM	Proposed
Accuracy	0.9176	0.9005	0.8806	0.9394
Sensitivity	0.8982	0.8816	0.8938	0.9307
Specificity	0.9125	0.8926	0.9014	0.9312

The honey badger optimization algorithm is used during the training process of deep neural networks and for enhancing reasoning aptitude through fuzzy inference systems (DNFN). The DNFN is trained using a newly introduced optimization technique called the hybrid Honey Badger Optimization (JHBO) model, which aims to improve detection performance in the near future through the JHBO-based DNFN [21,22].

The true positive and negative fractions of all audio samples, which are denoted as

$$Ac = (\varrho_t+\varrho_f) / (\varrho t+\varrho_t+\sigma_t+\sigma_f)\text{……...(1)}$$

ii) Sensitivity: The accurate categorization of voice authentication is assessed by sensitivity. which is defined by

$$Se = \varrho_f / (\varrho_f + \sigma_t)\text{……... (2)}$$

iii) Specificity: The formula for predicting the exact categorization of voice authentication, indicated as

$$S_p=\varrho_t/(\varrho_t+ \sigma_f)\text{ ……..(3)}$$

We have ϱt, which represents a true positive; ϱf, which is a true negative; σf, which stands for a false negative; and σt, which is a false positive.

B. Machine Learning Optimization and Accuracy

The voice authentication system was enhanced using a hybrid optimization method—Jaya Honey Badger Optimization (JHBO)—applied to a Deep Neuro-Fuzzy Network (DNFN). The JHBO algorithm improves the learning performance by fine-tuning the network's parameters for more accurate predictions. Test results using a dataset of 100 audio files (10 per speaker) showed that the system achieved an accuracy rate of 87%, correctly identifying 100 out of 103 audio samples. Experimental results from various iterations using JHBO-based DNFN are presented in Table 1

C. Evaluation of Performance

The performance study of the proposed method with the help of JHBO-based DNFN is detailed in Table 1 and Figure 5, using a variety of performance indicators and different training data. [23] The figure displays the results of analyzing the accuracy of the JHBO-based DNFN, developed using various iterations [24]. The creation of the JHBO-based DNFN technique achieves testing accuracy of 0.915, 0.936, 0.945, 0.944, and 0.957 with iterations 25, 45, 65, 85, and 115, respectively, compared to 85% training data. Figure 5 also shows the results of an investigation of the sensitivity of many iterations of a JHBO-based DNFN that was developed. JHBO-based DNFN introduces the sensitivity of the proposed method through iterations 25, 45, 65, 85, and 115. The values are 0.915, 0.936, 0.945, 0.944, and 0.957, respectively. Figure 5 shows the results of an investigation to develop the JHBO-based DNFN method across several iterations with respect to specificity. For iterations 25, 45, 65, 85, and 110, the specificity of the developed JHBO-based DNFN is 0.915, 0.9273, 0.9305, 0.9307, and 0.9515, respectively, when the training data is 85%.

D. Comparative Analysis with Existing Techniques

To assess the proposed approach's performance, the current voice authentication approaches are taken into consideration, including MFCC (Mel-frequency cepstral coefficients) [25], HMM (Hidden Markov model) [26], and Gaussian Mixture Model (GMM) [27]. In this part, we can see how different performance metrics were used to compare the designed JHBO-driven DNFN with data (training) and k-fold values shown in tables 2 and 3. Predicted from another method, a proposed method using a DCNN kernel and a DNFN K-fold fusion protein based on JHBO verifies precision at 0.9176, 0.9005, 0.8806, and 0.8894. A sensitivity of 0.8982, 0.8816, and 0.8938 and an alpha of 0.9307 Findings with a

 doi:10.20944/preprints202510.1587.v2

high degree of certainty (0.9125, 0.8926, 0.9014, 0.9219) Information used for Training accuracy of testing: 0.8959, 0.8910, 0.8901, 0.9151 In terms of specificity, we have 0.902 and 0.8896. 0.8932 and 0.9182 and a sensitivity of 0.9123, 0.8868, 0.9001, and 0.9218. The performance measures and the designed proposed method using JHBO-based DNFN are compared in Table 2. The results of a comparison study of the JHBO-driven DNFN, which was introduced to assess accuracy with different k-fold values, are presented. In terms of k-fold value, MFCC, HMM, and GMM all achieve testing accuracy of 0.8925, with MFCC coming in at 0.887 and the proposed JHBO-based DNFN reaching 0.9054. A comparison of the sensitivity of JHBO-based DNFN with different k-fold values for k-fold value, MFCC, HMM, and GMM has sensitivity values of 0.8912, 0.8780, and 0.8816, respectively; in contrast, the created proposed method using JHBO-based DNFN has a sensitivity of 0.9085.

VI. The Provider Adds a New Patient's Record Through System Administration Using the Proposed Method

It makes sure that the system nodes can connect to pre-existing EMR systems. It interprets it as meaning that many nodes, mainly healthcare providers, already reliably operate databases on servers connected to the internet. The backend library, database gatekeeper, Ethereum client, and EMR manager are the four components that our architecture presents.

It can run these components on servers and combine them to form a distributed type of system that functions. An online user interface and integration with the use of an SQLite database are the hallmarks of prototype implementation of these components. The modular protocol is defined by proposed blockchain contracts to allow any provider's backend. The user interface is implemented to participate in the system.

In this system, both providers and patient nodes contain the same fundamental components. Any desktop, laptop, or even a cell phone can run these components. They may use their local database, which is only one of several small database implementations. All the databases need to do is act as a temporary repository for the patients' medical records. If you follow the steps in the node's summary contract, you can get missing data back from the network whenever you need it. The first is the backend library, which is built to help the system run. It's a collection of tools that are put together. The library hides the details of blockchain interactions by exposing a functional API. So, the record management apps and their user interfaces won't have to deal with the blockchain's complexities. Making sure the network confidently accepts every transaction is one such challenge. When it comes to mining and discarding transactions, the library takes care of the uncertainty automatically. When using an Ethereum client, the backend library may practice the protocol's low-level formatting and parsing. Details discuss how new patent records are added, explained in [28].

The proposed architecture integrates voiceprint-based access control and blockchain technology to manage Electronic Health Records (EHRs) securely and transparently. The system utilizes provider nodes, Ethereum smart contracts (via the MedRec framework), and a distributed ledger to facilitate secure interactions. The end-to-end process is outlined as follows:

a. **Record Initialization**: A new patient record is created and updated within the local database by the **EHR manager** at the provider node. This event triggers the initialization of a blockchain transaction.
b. **Smart Contract Association**: The system resolves the appropriate blockchain address and identifies the corresponding smart contract (SC). A new **patient-provider relationship (PPR)** is posted to the blockchain. The smart contract is then linked to the newly created PPR.
c. **Mining and Validation**: The transaction is broadcast to the blockchain network, where it is processed and validated by a **miner**. Upon successful mining, the miner receives an incentive or bounty for contributing to the consensus mechanism.
d. **Smart Contract Update**: Post-validation, the smart contract is updated to reflect the new record association and access permissions, as specified in the PPR metadata.

 doi:10.20944/preprints202510.1587.v2

e. **Notification Dispatch**: A notification is sent to relevant stakeholders or subsystems indicating the successful update of the EHR and its associated permissions on the blockchain.

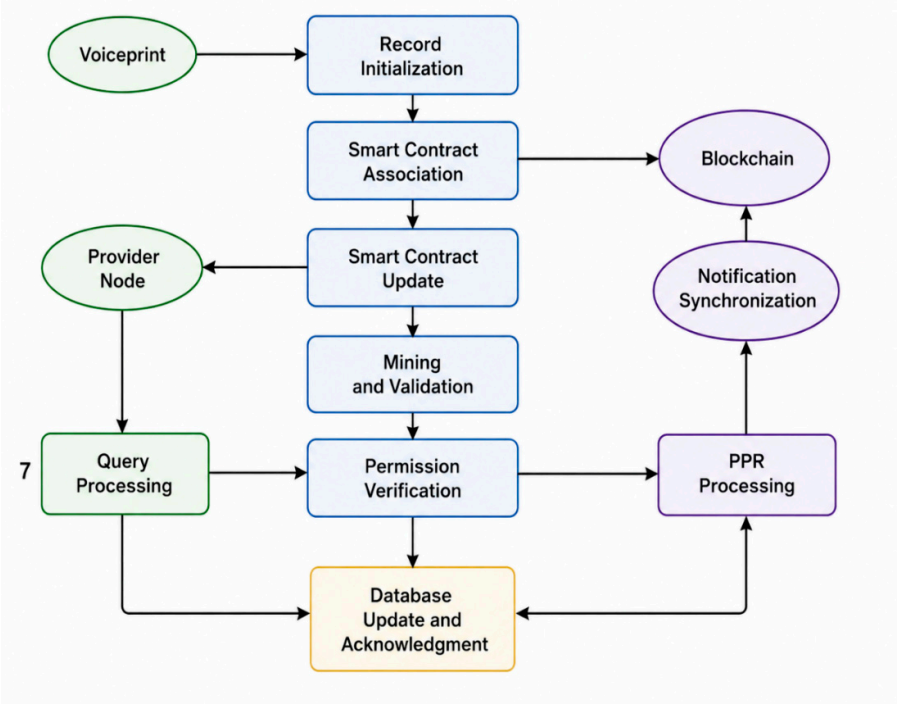

Figure 6. Blockchain-Enabled EHR Management Process Flow.

f. **PPR Status Synchronization**: The status of the PPR is updated within the smart contract to reflect its current state (e.g.,pending, approved, or completed), ensuring consistent access control enforcement.

g. **Query Processing**: When a provider node requires access to a patient's health record, it initiates a **query request**. This request is sent to the blockchain network for verification.

h. **Permission Verification**: The **MedRec service** within the Ethereum client evaluates the query by verifying access permissions embedded in the smart contract. If access is authorized, the requested EHR data is retrieved and returned to the provider node.

i. **Database Update and Acknowledgment**: Based on the query response, the EHR manager updates the local database accordingly. The system then provides a final acknowledgment or rejection, depending on the outcome of the access verification and data retrieval process.

This process uses blockchain technology to create a decentralized, auditable, and secure way to manage EHR access. It also uses biometric voiceprint authentication to improve identity verification and privacy control.

VII. System Prototype Implementation with Blockchain and Voice Authentication

To demonstrate the practical viability of the proposed model, a prototype was implemented and evaluated using a case study focused on heart health monitoring. The implementation integrates voice-based user authentication, high-frequency wireless data transmission, and blockchain-backed data integrity.

The developed system architecture comprises several essential components:

 doi:10.20944/preprints202510.1587.v2

- **Backend Library** – Provides abstraction over blockchain interactions.
- **Database Gateway** – Manages temporary patient data storage.
- **Ethereum Client** – Facilitates blockchain transactions.
- **EMR Manager** – Connects the system with existing Electronic Medical Record (EMR) databases.

Each node—whether a healthcare provider or a patient—hosts a local version of these components. They can run on lightweight devices like laptops or smartphones, using SQLite or similar embedded databases to temporarily store records. The blockchain acts as the central ledger to verify and synchronize data across all nodes. Smart contracts are employed to enforce access policies and automate permissions. The system interface is web-based, developed using Flask and JWT (JSON Web Token) libraries for secure user authentication and session control. This modular design allows seamless integration with any healthcare provider's digital infrastructure.

1. *Environment for Experiments*

We evaluated our approach by simulating the use case scenario for waste management from the prior section. As an example, each business in the simulated group of three companies collaborating on distinct services was able to register genuine hardware as assets and create JSON tokens that complied with the access control specifications. The results of our study are based on two distinct types of locally stored (offline) data; for the second, we use the huge chain-DB online test node stores, and for the initial, Docker technology is used. The experiment's multiple components use RESTful APIs to communicate data. We created our prototype employing the programming language Python, the FLASK micro-online structure, and the JWT crypto libraries to evaluate the performance of our proposed access control strategy. The execution environment is a virtual computer operating Ubuntu with 8 GB of memory and a single Intel Core i5-4510U 2.00 GHz CPU. Additionally, parallel registration and authentication requests were modeled using Apache JMeter.

VIII. Results and Discussion

To evaluate the practical performance of the proposed voice-authenticated blockchain healthcare system, a simulation environment was developed using **Network Simulator 3 (NS-3)**. This platform was chosen due to its flexibility and the availability of libraries tailored for blockchain-based network configurations. The simulation replicated a vehicular communication network context, adapted for healthcare data transmission scenarios.

Throughput and latency data for the two blockchain systems (existing system and and thegested technique) are compared. The estimated throughput for the existing and suggested systems was 17.6756 and 16.4736, respectively, based on Equation (4). These two findings demonstrated that the suggested system increased overhead by 3.806%. The latency values of the two systems—the proposed system and the existing system—were 0.00191 and 0.00471, respectively, based on Equation (5). The latency of the baseline and suggested systems was too low for comparison.

1. **Throughput Analysis:** As illustrated in the simulation (Figure 6.14), the proposed system achieved higher throughput compared to PoW, DTC, and VBCA. This performance gain is attributed to the optimized consensus selection process and the use of stationary "leader" nodes that minimize wait times for block confirmation. While PBFT demonstrated competitive throughput due to its private network nature, it lacks the scalability and flexibility offered by the proposed hybrid system.
2.
3. **Transaction Delay Analysis:** Figure 6.15 shows that the proposed model also significantly reduces transaction latency compared to PoW and DTC. This is because, unlike traditional blockchain approaches that require network-wide agreement for every transaction, the system uses smart contracts and delegated verification to expedite processing. PBFT recorded the lowest delay among the comparison set, as expected from a permissioned network. However, our model balances lower latency with a broader, more scalable architecture.

 doi:10.20944/preprints202510.1587.v2

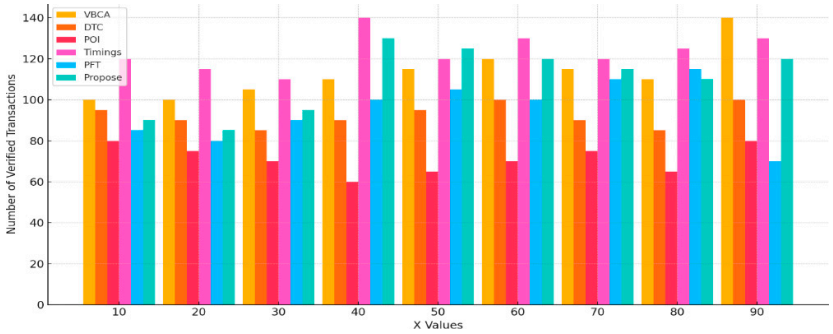

Figure 7. Throughput Analysis of Proposed EHR.

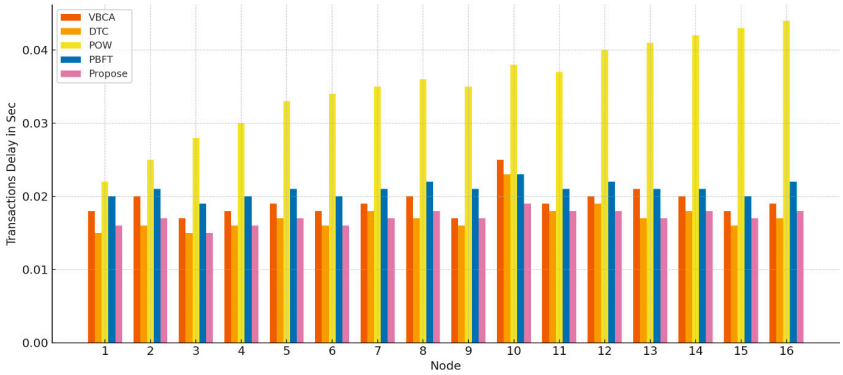

Figure 8. Delay in transactions (transaction delay) in the proposed EHR.

System Implementation and Case Study: Heart Monitoring with Blockchain and Voice Authentication

To display the practical feasibility of the proposed model, a prototype was applied and evaluated using a case study centered on cardiac health monitoring. The implementation integrates voice-based user authentication, high-existing wireless data transmission, and blockchain-supported data integrity.

1. *Prototype Implementation*

The developed system architecture comprises several essential components:

- **Backend Library** – Provides abstraction over blockchain interactions.
- **Database Gateway** – Manages temporary patient data storage.
- **Ethereum Client** – Facilitates blockchain transactions.
- **EMR Manager** – Connects the system with existing Electronic Medical Record (EMR) databases.

Each node—whether a healthcare provider or a patient—hosts a local version of these components. They can run on lightweight devices like laptops or smartphones, using SQLite or similar embedded databases to temporarily store records. The blockchain acts as the central ledger to verify and synchronize data across all nodes. Smart contracts are employed to enforce access policies and automate permissions. The system interface is web-based, developed using Flask and JWT (JSON Web Token) libraries for secure user authentication and session control. This modular design allows seamless integration with any healthcare provider's digital infrastructure.

In case study scenarios, the system is used to develop a secure real-time cardiac monitoring solution. The goal is to continuously collect and transmit cardiac data while simultaneously using voice recognition to ensure data protection and patient authentication. To prevent unauthorized access, check your identity regularly.

 doi:10.20944/preprints202510.1587.v2

Key System Components:

- **High-Frequency Wireless Communication:** Supports rapid, encrypted transmission of sensor data over IoT networks.
- **Heart Monitoring Device:** A wearable sensor collects real-time metrics such as heart rate and rhythm.
- **Voice Authentication Module:** Verifies the identity of the user periodically or at login to prevent unauthorized access.
- **Blockchain Network:** Stores encrypted health data in a decentralized manner, ensuring tamper resistance.
- **Data Analysis Engine:** Detects abnormalities and triggers alerts for critical conditions.
- **User Interface (UI):** Provides access to health records for patients and medical professionals with role-based controls.

1. *System Workflow*

The operational flow of the heart monitoring system is as follows:

- **User Enrollments:** A user registers via a mobile app and provides a voice sample, which is encrypted and stored on the blockchain.
- **Device Pairing:** The wearable heart monitoring device is connected to a user's smartphone using wireless protocols like Bluetooth.
- **Data Collection:** The device gathers and transmits vital signs at defined intervals.
- **Voice Authentication Checkpoint:** At predefined intervals or during sensitive operations, users must authenticate through voice input.
- **Secure Data Logging:** Authenticated health data is encrypted and appended to the blockchain ledger, maintaining an immutable audit trail.
- **Health Data Analysis:** AI-driven analysis tools evaluate the collected data to identify irregularities and suggest interventions if necessary.
- **User Interaction:** Patients and clinicians access historical data, live metrics, and alerts through the application dashboard.

This case study validates the effectiveness of integrating modern technologies such as blockchain and voice authentication in a healthcare setting. It highlights not only the feasibility of real-time health monitoring but also the importance of maintaining trust, security, and usability in sensitive digital health ecosystems.

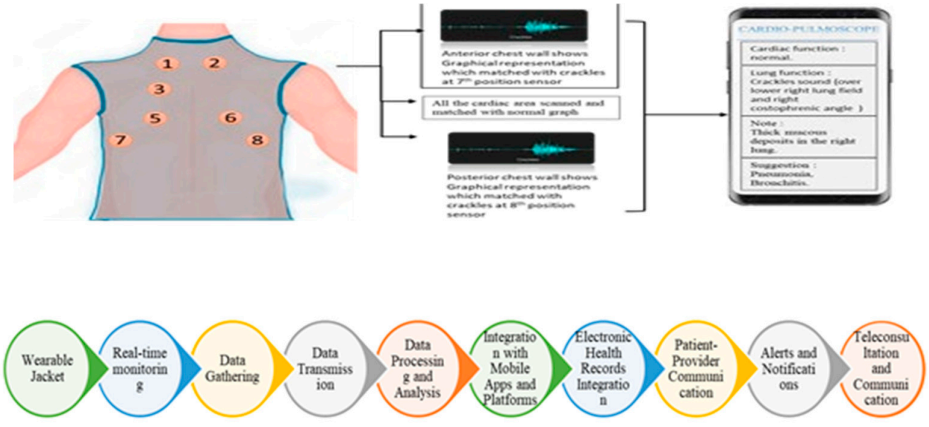

Figure 5. (a) Proposed model and working principle of a heart monitoring system (a lightweight jacket with attached sensor). (b) Block representation of heart monitoring system.

 doi:10.20944/preprints202510.1587.v2

Conclusion

In this article, a voice authentication-based patient health information system linked with a blockchain-based secured healthcare system has been proposed. Voice authentication has several benefits over conventional forms of authentication like passwords or biometrics. It enhances security, user-friendly experience, non-intrusiveness, and strong authentication, which are some of the main advantages of using voice authentication to secure electronic health records. Finally, the voice authentication-based blockchain network shows enormous potential to secure and efficiently handle the healthcare ecosystem. The proposed combination provides robust security, user-friendliness, and regulatory compliance. Expanded use of high-frequency wireless communication-based voice authentication of the healthcare records will be possible with continued investment in the health care sector and continuous advancements in blockchain technology. In the ever-changing healthcare business, voice authentication with blockchain has great potential to be an essential tool for protecting patient information and maintaining the trust and privacy that are fundamental to the contemporary healthcare system.

References

1. Ratta, P.; Kaur, A.; Sharma, S.; Shabaz, M.; Dhiman, G. (2021). "Application of blockchain and internet of things in healthcare and medical sector: Applications, challenges, and future perspectives." *In Journal of Food Qual*. **2021(7608296).** https://doi.org/10.1155/2021/7608296
2. Reegu, F.A.; Al-Khateeb, M.O.; Zogaan, W.A.; Al-Mousa, M.R.; Alam, S.; Al-Shourbaji, I. (2021). "Blockchain-based framework for interoperable electronic health record." Ann. Rom. Soc. Cell Biol**. 30:** 6486–6495.
3. Nazir, S.; Ali, Y.; Ullah, N.; García-Magariño, I. (2019). "Internet of things for healthcare using effects of mobile computing: A systematic literature review." Wirel. Commun. Mob. Comput. **2019 (5931315).**
4. Bamakan, S.M.H.; Moghaddam, S.G.; Manshadi, S.D. (2021) "Blockchain-enabled pharmaceutical cold chain: Applications, key challenges, and future trends." J. Clean. Prod. **302 (127021).**
5. Makridakis, S.; Polemitis, A.; Giaglis, G.; Louca, S. (2018) "Blockchain: The next breakthrough in the rapid progress of AI. Artif. Intell.-Emerg." Trends Appl. **27(10).**
6. Abunadi, I.; Kumar, R.L. (2021). "Blockchain and business process management in health care, especially for COVID-19 cases." Secur. Commun. Netw: **2021 (2245808).**
7. Bindlish, S.; Chhabra, S.; Mehta, K.; Sapra, P. (2022) "Blockchain in Health Care: A Review." Cyber Security. Digit. Forensics. **122:** 423–430.
8. Attaran, M. (2022) "Blockchain technology in healthcare: Challenges and opportunities." International Journal of Health Care Management :**15:** 70–83.
9. Mackey TK, Kuo T, Gummadi B, et al. (2019) "Fit-for-purpose?" - challenges and opportunities for applications of blockchain technology in the future of healthcare." BMC Med. Mar **27;17(1)**:68.
10. Hoy MB. (2017) "An introduction to the blockchain and its implications for libraries and medicine." Med Ref Serv Q; 36(3):273–279
11. Yaeger K, Martini M, Rasouli J, et al. (2019) "Emerging blockchain technology solutions for modern healthcare infrastructure." J Sci Innov Med. **9(9):**2–7.
12. Roehrs A, da Costa CA, da Rosa Righi R. (2017) "OmniPHR: a distributed architecture model to integrate personal health records." J Biomed Inform.; **71**:70–81.
13. Peterson K, Deeduvanu R, Kanjamala P, et al. (2020). "A blockchain-based approach to health information exchange networks." Mayo Clinic.
14. Ichikawa D, Kashiyama M, Ueno T. (2023) "Tamper-resistant mobile health using blockchain technology." JMIR MhealthUhealth. 5(7):134–144.
15. [11] Zheng, Y., and Zhao, S. (2016). A Usable Authentication System Based on Personal Voice Challenge. 2016 International Conference on Advanced Cloud and Big Data (CBD), IEEE, Chengdu, 13-16 August 2016, 194-199.

 doi:10.20944/preprints202510.1587.v2

16. Aizat, K., Mohamed, O., Orken, M., Ainur, A., and Zhumazhanov, B. (2020). Identification and Authentication of User Voice Using DNN Features and i-Vector. Co-gent Engineering, 7, Article ID: 1751557
17. Pal, P., Sahana, B.C., Ghosh, S., Poray, J., Mallick, A.K. (2021). Voice Password-Based Secured Communication Using RSA and ElGamal Algorithms. In: Panigrahi, C.R., Pati, B., Pattanayak, B.K., Amic, S., Li, KC. (eds) Progress in Advanced Computing and Intelligent Engineering. Advances in Intelligent Systems and Computing, vol. 1299. Springer, Singapore. https://doi.org/10.1007/978-981-33-4299-6_32.
18. Lv, Z., Qiao, L., Kumar Singh, A., and Wang, Q. (2021). AI-Empowered IoT Security for Smart Cities. ACM Transactions on Internet Technology, 21, 1-21. https://doi.org/10.1145/3406115
19. Rashid, J., Teh, Y.W., Memon, N.A., Mujtaba, G., Zareei, M., Ishtiaq, U., Akhtar, M.Z., and Ali, I. (2020). Text-Independent Speaker Identification through Feature Fusion and Deep Neural Network. IEEE Access, 8, 32187-32202. https
20. Dibaei, M., Xia, Y., Xu, X., Jolfaei, A., Bashir, A.K., Tariq, U., Yu, D., and Vasilakos, A.V. (2022). Investigating the Prospect of Leveraging Blockchain and Machine Learning to Secure Vehicular Networks: A Survey. IEEE Transactions on Intelligent Transportation Systems, 23, 683-700.https://doi.org/10.1109/TITS.2020.3019101
21. Jawad Ahmad Dar, Kamal Kr. Srivastava, Sajaad Ahmed Lone, Spectral features and optimal hierarchical attention networks for pulmonary abnormality detection from the respiratory sound signals, Biomedical Signal Processing and Control, Volume 78, 2022, 103905, ISSN 1746-8094, https://doi.org/10.1016/j.bspc.2022.103905.
22. Jawad Ahmad Dar, Kamal Kr Srivastava, Sajaad Ahmed Lone, Design and development of hybrid optimization-enabled deep learning model for COVID-19 detection with comparative analysis with DCNN, BIAT-GRU, and XGBoost, Computers in Biology and Medicine, Volume 150, 2022, 106123, ISSN 0010-4825, https://doi.org/10.1016/j.compbiomed.2022.106123.
23. Dar, J.A., Srivastava, K.K. & Lone, S.A. Fr-WCSO- DRN: Fractional Water Cycle Swarm Optimizer-Based Deep Residual Network for Pulmonary Abnormality Detection from Respiratory Sound Signals. *SN COMPUT. SCI.* **3**, 378 (2022). https://doi.org/10.1007/s42979-022-01264-0
24. Ponnupilla Omana S, Dar JA, Rajesh Kumar T, Sampath AK, Sharma S. Henry gas bird swarm optimization algorithm-based deep learning for brain tumor classification using magnetic resonance imaging. *Concurrency Computat Pract Exper*. 2023; 35(4):e7541. doi:10.1002/cpe.7541
25. Song, Z., Ma, L. (2024). Speech Command Recognition Algorithm Based on Improved MFCC Features. In: Wang, W., Liu, X., Na, Z., Zhang, B. (eds) Communications, Signal Processing, and Systems. CSPS 2023. Lecture Notes in Electrical Engineering, Vol. 1032. Springer, Singapore. https://doi.org/10.1007/978-981-99-7505-1_61
26. Chen, Yinchun. "A hidden Markov optimization model for processing and recognition of English speech feature signals." *Journal of Intelligent Systems*, vol. 31, no. 1, 2022, pp. 716-725. https://doi.org/10.1515/jisys-2022-0057
27. Ankur Maurya, Divya Kumar, and R.K. Agarwal, Speaker Recognition for Hindi Speech Signal using MFCC-GMM Approach, Procedia Computer Science, Volume 125, 2018, Pages 880-887, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2017.12.112.
28. Pal P, Sahana B C, and Poray J (2023) "Secured Information Transfer Power by Modified and Optimized RSA Cryptosystem," Easy Chair Preprint no. 10318.
29. Sehar, N.U., Khalid, O., Khan, I.A., et al. (2023). "Blockchain-enabled data security in vehicular networks." Sci Rep 13(4412). .https://doi.org/10.1038/s41598-023-31442-w
30. Shrestha, R., Bajracharya, R., & Shrestha, A. P. (2020). "A new type of blockchain for secure message exchange in VANET." Digit. Commun. Netw. 6(2), 177–186.
31. Chai, H., Leng, S., Zeng, M., and & Liang, H. (2019). "A Hierarchical blockchain-aided proactive caching scheme for the internet of vehicles." In IEEE International Conf. on Communications (ICC).
32. Dorri, A., Kanhere, S. S., Jurdak, R., & Gaurava, P. (2019). "LSB: A lightweight scalable blockchain for IoT security and anonymity." Journal of Parallel and Distributed Computing. 134(7), 180–197.

 doi:10.20944/preprints202510.1587.v2

33. F.A. Hashim, E.H. Houssein, K. Hussain, M.S. Mabrouk, W. Al-Atabany, Honey Badger Algorithm: new metaheuristic algorithm for solving optimization problems, Math. Comput. Simulat. 192 (2022) 84–110.
34. S. Javaid, M. Abdullah, N. Javaid, T. Sultana, J. Ahmed, N.A. Sattar, Towards Buildings Energy Management: Using Seasonal Schedules Under Time of Use Pricing Tariff Via Deep Neuro-Fuzzy Optimizer, in: Proceedings of IEEE 15th International Wireless Communications & Mobile Computing Conference (IWCMC), June 2019, pp. 1594–1599.