

# A Secure Medical History Card Powered by Blockchain Technology

Samiha Fairouz<sup>1</sup>, Shakila Yeasmin Miti<sup>2</sup>, Zihadul Islam<sup>2</sup>, Meem Tasfia Zaman<sup>\*,2</sup>

<sup>1</sup>University of Adelaide, Faculty of Sciences, Engineering and Technology, Adelaide, South Australia

<sup>2</sup>North South University, Department of Electrical and Computer Engineering, Dhaka, Bangladesh

## ARTICLE INFO

Article history:

Received: 29 September, 2023

Accepted: 26 November, 2023

Online: 30 December, 2023

Keywords:

Medical history card

Web application

Blockchain

Decentralized database

Electronic medical records

Healthcare

## ABSTRACT

A reliable healthcare system ensures that the population has access to top-notch medical services, ultimately enhancing their overall health most efficiently. At times, data are not secured or handled appropriately. Addressing these concerns, blockchain technology is projected to bring about a substantial revolution in the medical industry by assuring the confidentiality of electronic health information. This research not only seeks to rectify the shortcomings in Bangladesh's existing health system but also explores the potential of blockchain technology's decentralized database to fortify the entire healthcare framework. More importantly, it showcases a web-based application, particularly a medical history card that displays a patient's details, diagnoses, vaccines, medication records, investigation background, familial information, blood donation history, and many additional information starting from birth. Alongside, the paper emphasizes the transformative impact of implementing blockchain technology in the healthcare sector, paving the way for a more secure and efficient healthcare ecosystem. All in all, the array of medical information captured within the pack face of a single card could hasten medical decisions and ensure the effectiveness of any treatment.

## 1 Introduction

The health sector holds an exceedingly central position in safeguarding an overall sustainable socio-economic advancement. The health world is immensely diversified with the presence of several technical and biomedical analyses. The previous concepts of medical management are now found substituted over time. Currently, people are more focused on constituting a community of healthiness in which disease prevention outweighs the importance of the cure, unlike in the past. Notwithstanding that, the healthcare management system confronts the most critical challenges and barriers. Although technological and medicinal advancements are now quite prominent, no steps have yet been taken to incorporate the patient's medical history in a decentralized manner. The patients of private and public Healthcare Centers (HCs) are still found carrying the baggage of reports, diagnoses, and prescriptions while visiting a physician. Reports or prescriptions are either lost or misplaced, resulting in harassment and stress during emergencies. Medical health records are irreplaceable not only to patients but also to the hospital authorities themselves. A detailed history can put additional value to the current treatment by the medical consultants and physicians. The continuing development of the Internet of Medical Things (IoMT) could accelerate the maintenance of digital documents while offer-

ing greater convenient services to clients. Despite these precautions, healthcare frequently encounters virtual hacking incidents that end up resulting in the deletion and disclosure of personally identifiable information. Software vulnerabilities, security collapse, and human error are ordinarily the reasons behind this catastrophe. Amid such a situation, the data breach discloses many loopholes in the healthcare database system that can be encapsulated under three keynotes: 1) centralized aggregation of essential data, 2) unauthorized access to the public, and 3) disclosing confidential data purposely due to inadequate information security. Notable, health records need to be breach-proof as any data tampering can cause critical medical emergencies, including the death of patients. With the significance of medical history in mind, we are introducing a medical history card that would contain all a person's medical records under a platform. To explain, the patients will be emancipated from the burden of bearing all their medical history before visiting a physician. Furthermore, the likelihood of doctors encountering incorrect and deceptive information will decrease. The utilization of blockchain technology in the card ensures the decentralized accuracy of medical information, eliminating the need for third-party electronic storage. Blockchains are often referred to as distributed ledger technology (DLT) as blockchain records are immutable and cannot be modified, changed, or deleted.

\*Corresponding Author: Meem Tasfia Zaman, North South University, Email: [zaman.tasfia@northsouth.edu](mailto:zaman.tasfia@northsouth.edu)

## 2 Literature Review

Conventionally, the idea of digitally archiving medical information has traditionally been in development for a significant period of time. The current paper is dedicated to extending the paper entitled "A medical history card utilizing the Blockchain technology" which was published in the 2023 5th International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA) [1]. In the past in 1973, The Regenstrief Medical Record System (RMR), a type of paper-based electronic record system has been utilized in outpatient healthcare facilities. The RMR obtained information about patients from a wide range of sources including physician chambers, forensic lab data, pharmacies, and others. It generated a summary report, surveillance report, and the Patient Encounter Form (PEF) to deliver protocol-based feedback to doctors about critical clinical conditions. It was extensively believed that the widespread use of EMRs had decreased surgical errors, boosted health, and decreased expenditures on healthcare. Likewise, the organizational processes have ensured excellent quality, effectiveness, and transparency through EHRs [2]. In order to create an integrated medical record between patients and medical professionals, the author of [3] (2008) established a patient portal called CONNECT (Care Online: Novel Networks to Enhance Communication and Treatment). The patients could easily access it from home, hospital, or doctor's office using the heterogeneous networks. CONNECT application was committed to improving patient-provider communication and assisting patients in understanding and managing their illnesses. In 2010, author of the paper [4] described that the use of EMRs in long-term care institutions at the time was neither widespread nor successful. The hospitals implementing EMRs were working on techniques to evaluate effectiveness; no statistical information was available on the efficacy of EMRs in the long-term care context. They opposed the widespread use of EMRs. Conversely, it was evident that when most patients carry their EHR, many chances were created for the industries. For instance, a "health record bank," proposed in [5], was a starting point for the enterprise's additional "value-added" services. An EHRs facilitates clinicians to view patients' data from numerous sources across a period for extensiveness and continuity of care. Research showed that the appropriate application of the EHRs could minimize medical errors, assist in diagnosing detrimental health events, facilitate the more appropriate use of healthcare services, and potentially reduce healthcare expenses [6]. An e-prescription system that assists mother and children with medicine data recording, retrieving, and reporting techniques have been developed by the author of [7]. Moreover, the possible medication errors were reduced by upgrading the prescribing process. In [8], the author claimed that the Implantable Device Cardiac Observation (IDCO) profile had been constructed at the Leiden University Medical Centre (LUMC) to integrate data from the external databases maintained by two device providers into the departmental Cardiology Information System. They continued by saying that the growing use of ICDs and remote monitoring at treatment stations will improve patient outcomes by lessening the burden of follow-up on clinics and personnel. From the patient's point of view, it was appealing due to better security and prevention of lengthy and time-consuming visits to the hospital. In particular, readmissions were minimized

when patient history was viewed [9]. In the publication with reference [10], the author covered, The Internet of Things (IoT) and the digitization of medical records topics in a number of their presentations. They made portable web servers out of smart gadgets like smart discs and cards, making remote diagnostics record-keeping easier. The functional requirements call for a device-enabled system that could obtain and capture all the records with a backup on a few cloud-based platforms so that data is not lost, even though the device was lost. The system claimed to eliminate paper from patient transactions completely. Besides, storing patient reports, histories, visits, prescriptions, results, pharmacy bills, and emergency contact information was more straightforward. The patient had exclusive access to the gadget, and adequate verification was required for updating any information on the device. Additionally, in the same year, an advanced decentralized system, MedRec for managing Electronic Health Records (EHRs) through Blockchain technology was proposed. Their solution offered patients a comprehensive, tamper-proof log and easy access to their data [11]. In 2008, the basic concept of a distributed secure ledger was introduced. Blockchain technology is the approach to creating an immutable, secure, distributed database of transactions. Blockchains were trained to deliver a distributed ledger of financial transactions, not relying upon a central bank, credit company, or other financial institution. Additionally, it confirms a secure and permanent record of transactions. The significant progress in EMRs was the generation of a distributed ledger to productively transfer patients' records from the healthcare organization to the individual. One of the key features of blockchain technology is that it is way too transparent: transactions are processed by the network without requiring a single computer, database, or institution. Besides, the paper [12] offered insights into the use of blockchain in healthcare data management, with a specific focus on sharing EMRs among healthcare providers. Collaborating with Stony Brook University Hospital, a framework was developed for managing and sharing Electronic Medical Records (EMRs) of cancer patients. This framework involved connecting to the hospital's local database management system, which was specifically designed for storing oncology-related data. Patient data was then encrypted using each patient's unique key and stored on a cloud-based platform known as Varian Cloud. Additionally, a blockchain-based data-sharing system was proposed as part of this initiative. This system aimed to leverage the immutability and autonomy characteristics of blockchain technology to effectively address various medical challenges related to data security and sharing [13], [14]. In 2018, a blockchain-based data-sharing system called BPDS (Blockchain-based Privacy-Preserving Data Sharing) was introduced with the primary goal of safeguarding user privacy. By implementing BPDS, patients gained control over their Electronic Medical Records (EMRs), and both users and institutions could access this data without concerns about compromising patient privacy. In BPDS, the original EMRs were securely stored in the cloud-based BPDS system, while the indexes were maintained within a consortium that had stringent tamper-proof measures. This approach significantly reduced the risk of medical data leakage. During the same year, a novel method involving attribute-based signatures, with multiple authorities, was developed to ensure the authenticity of Electronic Health Records (EHRs) embedded within the blockchain. In this method, a patient could sign a message based on certain

attributes without revealing any additional personal information, thus providing proof of their attestation [15] [16]. To enhance privacy within the system, a method involving Personalized Radio Frequency Identification (RFID) cards was implemented. These RFID cards assigned unique IDs to different users, and modifications to these IDs could only be made by the relevant doctors using the medical database. This approach ensured the authentication of medical information, as only authorized personnel could manage and update the data. Furthermore, another blockchain-based approach was suggested to secure Electronic Medical Records (EMRs) for healthcare applications. In this approach, access control was patient-centric, meaning that patients would share the decryption key only with trusted doctors. These trusted doctors would then store the patient's encrypted electronic medical information securely on a blockchain, adding an additional layer of security to the handling of medical data. By utilizing the encryption technology, the authors of the publication [17] proposed a Sensitive and Energetic Access Control (SE-AC) mechanism for certifying fine-grained confidentiality of the patient's Electronic Health Record (EHR), wherein people given authorization could update or examine certain EHR. The authors emphasized that the security of EHRs seriously threatens the patient's privacy, and most third-party hosting platforms have some issues with data security and user privacy. Individuals having drug or alcohol addiction histories and HIV could request primary care physicians to access certain documents in the hospital [18] [19] [20]. The concept of remote healthcare was introduced with a focus on securing electronic records through encryption before they are transmitted to medical Blockchain networks. In this approach, the medical team members established a session key for authorized groups in a way that allowed authorized participants to decrypt and access patient information. Importantly, the content could only be deciphered using either the patient's private key or a group member's session key, and no personal identification password was involved in the entire process. In [21], the authors discussed the use of 'The InterPlanetary File System (IPFS)' for storing Electronic Medical Records (EMRs) and the Ethereum platform for replicating the blockchain. This proposed method enhanced the confidentiality of uploaded data, reduced the risk of errors due to data manipulation, and facilitated the secure digitization of medical records. The public key served as a universal identifier to segregate and maintain the complete medical record history for each patient [22]. In 2021, a comprehensive healthcare system was developed, encompassing an Android app, an iOS app, and a website, all designed to grant patients easy access to their medical records and history. Additionally, a novel feature was introduced: a health passport designed to compile and display patients' medical data from various healthcare providers. This encompassed a wide range of information, including medical images, clinical reports, lab results, dental records, and more. Users had the convenience of utilizing their smartphones to consolidate their medical history from diverse sources, including healthcare providers, imaging CDs, PDF notes, fitness trackers like Fitbit and Apple Watch, wellness forms, CDA Files, JPEG documents, and self-reported health records. Furthermore, they could maintain and update their health vitals such as Blood Pressure, Heart rate, height, weight, BMI, Body Temperature, Oxygen saturation, allergies, and BSA. Additionally, the application provided a user-friendly feature that enabled individuals to easily

locate their nearest healthcare center and schedule appointments, making healthcare management more accessible and efficient [23]. A new architecture termed as Internet-of-Health-Care-Systems (IoHCS) was launched to supervise the EHRs accumulated from all partaking hospitals in a network; through Blockchain Technology developed on the Ethereum platform. Software agents via Message Queueing Telemetry Transport (MQTT) protocol were used to network the Health Information Systems (HIS) of all linked hospitals. A mobile app for accessing patient records using a Key Management System (KMS) and an Application Programming Interface (API) for reading and writing data for each hospital on the blockchain was also generated. Studies show that the prevailing HIS of 350 partaking hospitals was incorporated into the app. The EHRs of the patient have been formulated in 6 parts — personal information, visit information, laboratory test information, drug order information, and a hash value created by the encryption module. Amazon Key Management System and Amazon S3 (Simple Storage Service) guarantee data and process security. In 2022, a new web-based project was proposed with the aim of creating a centralized database to store patients' medical histories. The paper provided details about the software and technological architecture employed for this purpose. The project focused on enabling remote control and management of the integrity and documentation of medical histories, reports, and prescriptions. For the backend of the online application, PHP, AJAX, and jQuery were utilized, with MySQL serving as the database. On the frontend, HTML5, CSS, Bootstrap, and JavaScript were employed. Researchers developed a prototype platform that aimed to digitalize the healthcare system by offering digital appointments, artificial intelligence-driven recommendations, and a health-tracking blood bank. One notable challenge addressed in the context of the technological revolution was the storage of segmented Electronic Health Records (EHRs) in Healthcare Centers (HCs). To tackle this issue, a platform was introduced to establish a distributed electronic health record (EHR) ecosystem. This ecosystem aimed to integrate electronic medical reports securely within a private and permissioned blockchain, addressing the fragmentation of EHR data. The notable advantages of implementing the distributed network regarded clinical outcomes such as improved quality, and reduced medical errors; organizational outcomes like financial, and operational benefits; managerial outcomes, e.g., improved ability to conduct research, improved population health, and lower costs [24], [25]. To highlight, Blockchain is an emerging decentralized technology to validate and secure a patient's medical record efficiently. Several attempts were proposed to use Blockchain technology to address healthcare data privacy, security, and ownership issues. Blockchain-based digital platforms empower patients to communicate with their data providers, including healthcare providers, in a faultless, secure, and efficient approach [26], [27].

### 3 Features

Since the inception of the paper, the goal has been to deploy the history card for the comprehensive collection of an individual's crucial medical records to facilitate appropriate treatment

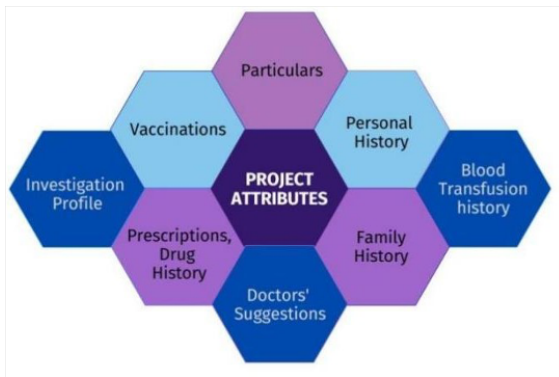


Figure 1: Features Diagram

To ensure the card's effective and optimized application, various features have been integrated, in Figure 1. Initially, 'Particulars' will contain the Name, Date of birth, blood group, parent's name and details, weight, height, classification of gender, address, and contact number. The 'Personal History' section provides comprehensive information concerning past allergies, sinusitis, any congenital anomalies, diabetes, Claustrophobia, thyroid conditions (hypothyroidism or hyperthyroidism), etc. Another vital segment is the 'Investigation Profile,' which grants access to all diagnostic reports, including cellular and chemical analyses (such as blood analysis, glucose tolerance test, serological test, enzyme analysis, kidney and liver function, protein-bound iodine test, gastric fluid analysis, and more); diagnostic imaging (such as mammography, ultrasonogram, brain scanning, and so forth); health examinations (like biopsy, laparoscopy, and others). Following that, the 'Vaccinations' section will contain a record of all vaccinations administered from birth onwards. Subsequently, the 'Drug History' segment provides a catalog of medication names, dosages, and the timing of each medication taken. In the 'Blood Transfusion History,' the record includes details about the quantity and blood type of blood donations made by the patient. Similarly, in the 'Prescriptions' section, all prescriptions provided by doctors are organized chronologically. Another essential component is the 'Family History,' which encompasses the genetic diseases present in the patient's family, such as Congenital deafness, Cancer, thyroid concerns, and so on. Finally, 'Doctors Suggestions' will outline the healthcare recommendations given by doctors regarding the patient's medical conditions.

## 4 Proposed Strategical Plan

The paper initially intends to use the health card to collect necessary information in order to eliminate the need for patients to repeatedly visit the history room next to the doctor's office. In summary, there are four sorts of users in this article's web application: patients, doctors, vaccine staff, and report staff. The priority of patient's health history has been analyzed as per the priority list of records in the card.

Following that, the attributes of the website such as Patients (Name, age, blood group, gender, etc.), Vaccination History, Personal History (Diabetics, High / Low blood pressure, thyroid, history of surgery, blood transfusion, allergy, congenital anomaly, Covid-19, etc.), Diagnosis Report, Prescriptions, Drug History, Family History

(Kidney, Heart Disease, Cancer, Skin disease, etc.) and Doctors' Suggestions schemed.

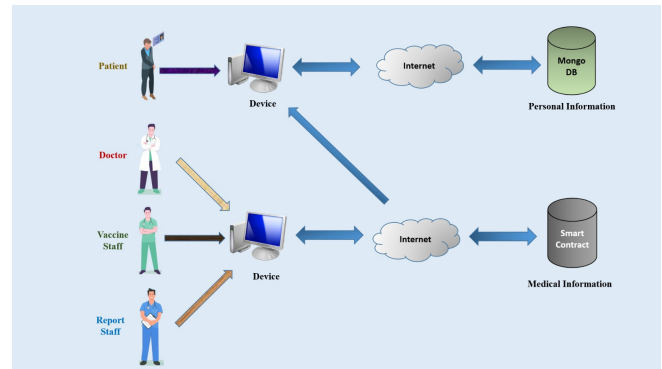


Figure 2: Network Diagram

The Network diagram depicts the fundamental work processes of the users for circumstances where accessibility to health records is prohibited for security reasons. (Figure 2). All of the patient's information can be read by both patients and doctors, but only they have the ability to make specific changes. The two more users, the vaccine and report staff are only permitted to look at the patient's personal background and relevant fields. Moreover, patients might view the automated EMR snapshots and update their personal information. Furthermore, MongoDB, a NoSQL database, was used to save the users' other traditional information, such as personal narratives, via the Internet, and the blockchain Smart Contract was chosen to store the medical data because there is always the risk of vital medical information being lost.

Smart Contract has been deployed as Blockchain Database to accommodate the patient's medical health history. To add, Smart Contract is a form of Ethereum account capable of sending transactions over the network. The agreement enables the execution of a contract between two parties through blockchain, without the involvement of any legal system.

## 5 Implementation

In this section, the web application's tools, frameworks and databases as well as the benefits of using these methods over more conventional methods. In addition, we shed light on the robust security measures and policies that have been put in place to safeguard the system.

### 5.1 Framework and Structural Design

The web application has been constructed using the MERN stack, which seamlessly combines four core technologies: React, and Node, MongoDB and Express. Furthermore, the application adheres to an architecture model that is built with 3-tier and it is characterized by three distinct layers: the front-end tier, represented by the web interface; the middle tier, composed of servers; and the back-end tier, covering the databases.

## 5.2 Approach to User Interface Development

To begin, the front-end infrastructure was constructed with HTML, CSS, React and JavaScript (JS). React is preferred for the project as it provides a front-end build pipeline making it useable with any back-end. Secondly, in order to develop dynamic HTML sites for taking user input into account and preserving permanent data using specialized objects, files, and relational databases, JS was utilized. Thirdly using CSS, the website's appearance and layout were updated.

## 5.3 Approach to Server-Side Development

The back-end server was developed with Node JS. In order to establish a connection between the front-end and the back-end, the Web3 application programming interface has been seamlessly integrated into the system.

During authentication, JSON Web Token (JWT) has been implemented for security purpose. JWT has been attached as "bearer" header on each login request to server. After that, it will be parsed by the server from header and the client identity will be verified. The JWT has been implemented because this authentication system is helpful to use for different type of users. To generate the JWT during every login HS256 signing algorithm has been used in the header that has been given below:

```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

And the payload part of the JWT contains the claims of the particular users. The claims includes statements about the user and additional data which looks like this:

```
{
  "hid": "123456789",
  "exp": "5th June, 2023"
  "iat": "2023-12:12 12:20:00"
}
```

Similarly, the refresh JWT is also being set as cookie so that, while the login access JWT will be invalidated the server could take set cookie of the refresh JWT and can generate a new refresh token for the logged in user. In the whole process, the expiration time of the access JWT has been set for 15 minutes and the refresh JWT has been set for 60 days.

In Figure 3, the displayed code snippet from our web application represents the implementation of the login process using JWT. As well as, specific validations has been incorporated to enhance security measures. Furthermore, to mitigate the risk of database injection, the use of the 'sanitize-html' package has been implemented.

## 5.4 Decentralized and Prominent Databases

The information will be stored in two separate databases. MongoDB will handle the orthodox data, while Smart Contract will store significant EMRs to enhance long-term protection. Additionally, MetaMask has been incorporated into the system as a wallet for overseeing and managing expenses related to ether.

```
23 // Login route to generate and return access and refresh tokens
24 app.post('/clientLogin',
25   handler: (req: Request, ResBody: ResBody, ReqQuery: LocalizedObj, res: Response: ResBody.LocalizedObj) => {
26     const { hid, password } = req.body;
27
28     // Find the user based on the provided health ID and password
29     const user = users.find((u) => u.hid === hid && u.password === password);
30
31     if (!user) {
32       return res.status(401).json({ message: 'Authentication failed' });
33     }
34
35     // Generate an access token with user information, exp, iat, and a secret key using HS256 algorithm
36     const accessToken = jwt.sign(payload: {
37       hid: user.hid,
38       exp: Math.floor(Date.now() / 1000) + (15 * 60), // 15 minutes from now
39       iat: Math.floor(Date.now() / 1000), // Issued at the current time
40     }, secretKey,
41     options: { algorithm: 'HS256' },
42     callback: function(err, accessToken) { console.log(accessToken); });
43
44     // Generate a refresh token with user information and a refresh secret key using HS256 algorithm
45     const refreshToken = jwt.sign(payload: {
46       hid: user.hid,
47       exp: Math.floor(Date.now() / 1000) + (60 * 24 * 60 * 60), // 60 days from now
48       iat: Math.floor(Date.now() / 1000),
49     }, refreshSecretKey,
50     options: { expiresIn: '60d', algorithm: 'HS256' },
51     callback: function(err, refreshToken) { console.log(refreshToken); });
52
53     // Set the refresh token in a cookie with a secure flag and HttpOnly to make it more secure
54     res.cookie({ name: 'refreshToken', refreshToken, options: {
55       maxAge: 60 * 24 * 60 * 60 * 1000, // 60 days
56       httpOnly: true,
57       secure: true,
58       sameSite: 'none',
59     }});
60
61     // Return the access token to the client
62     res.json({ body: { message: "Successfully Logged In", access_token: accessToken } });
63   });
```

Figure 3: Code Snippet Illustrating User Authentication

```
ClientInfo.sol 1 x {} ClientInfo.json
contracts > ClientInfo.sol
1 // SPDX-License-Identifier: MIT
2 pragma solidity >=0.4.22 <0.9.0;
3
4 contract ClientInfo {
5   // Prescription Contract Start here.
6   uint256 public prescriptionCount = 0;
7
8   struct prescriptionStruct {
9     uint256 id;
10    string Dfirstname;
11    string Dlastname;
12    string Docregid;
13    string hospitalname;
14    string src;
15    string Time;
16    string hid;
17  }
18 }
```

Figure 4: Medical Information's Data Structure

Patient's medical data is kept in an Ethereum Smart Contract Database. Each specific category of medical information has its own data structure (Figure 3).

The patient's whole medical history was then entered into the smart contract using the set method. The data was lastly acquired using the get method (Figure 5). The EMRs are securely stored within a decentralized Blockchain database. The decision to implement blockchain technology was primarily driven by two key objectives: transparency and data integrity. Specifically, blockchain was chosen to ensure that both patients and doctors cannot conceal information and to prevent the falsification of critical medical data. The blockchain architecture operates as a decentralized digital ledger, recording distinct data or transactions across a network of computers in blocks. Each node within this network possesses a complete copy of the blockchain, ensuring security and transparency without reliance on a central authority. Characterized by decentralization

and distribution, blockchain networks facilitate secure peer-to-peer transactions. Blocks, comprised of validated transactions, contain a cryptographic hash of the preceding block. The database's security is enhanced through decentralization, immutability, consensus mechanisms, cryptographic security, transparency, redundancy, and controlled access.

server has the capability to alter, amend, or delete any previously recorded information from the medical records. This combination of transparency and data immutability establishes a robust and secure foundation for the management and protection of sensitive medical information within the system.

```

33 function setPrescriptionData()
34     string memory _Dfirstname,
35     string memory _Dlastname,
36     string memory _Docregid,
37     string memory _hospitalname,
38     string memory _src,
39     string memory _Time,
40     string memory _hid
41     public {
42     }
43     prescriptionCount++;
44     newPrescriptionStruct[prescriptionCount] = prescriptionStruct(
45     prescriptionCount,
46     _Dfirstname,
47     _Dlastname,
48     _Docregid,
49     _hospitalname,
50     _src,
51     _Time,
52     _hid
53     );
54 }

function getPrescriptionDataCount() public view returns (uint256) {
    return (prescriptionCount);
}

function getPrescriptionData(uint256 dataNum)
    public
    view
    returns (
        uint256,
        string memory,
        string memory,
        string memory,
        string memory,
        string memory,
        string memory,
        string memory
    )
    {
        prescriptionStruct memory s = newPrescriptionStruct[dataNum];

        return (
            s.id,
            s.Dfirstname,
            s.Dlastname,
            s.Docregid,
            s.hospitalname,
            s.src,
            s.Time,
            s.hid
        );
    }
    
```

Figure 5: Set and Get Method of Medical Information

An object-oriented, high-level Solidity language was used for implementing Smart Contracts. This language is designed to target the Ethereum Virtual Machine (EVM). Truffle, the development environment, asset pipeline, and testing framework for smart contracts was used for the framework. Smart contracts, functioning within these networks, execute agreements or transactions without intermediaries, using platform-specific languages like Solidity for Ethereum. Once deployed on the blockchain, Smart Contracts become immutable code, and decentralized verification prevents any single entity from controlling their execution. This technology holds transformative potential for revolutionizing medical history management by securely storing records, providing patient-controlled access, and triggering actions based on predefined conditions. The project utilized MetaMask as a wallet to purchase ether. To add, MetaMask is a free web crypto wallet that allows users to store and connect with the Ethereum blockchain ecosystem. Lastly, to host the Blockchain server locally Ganache was deployed to set up a local Ethereum blockchain to test the decentralized application in a safe environment. Additionally, the Blockchain design eliminates the risk of data loss through its distributed architecture, where each server on the network maintains a copy of the data, and no

## 6 Outcome and Prospects

In this section, the output of the web application has been demonstrated in order to get a clearer web experience. More especially, with the use of screenshots from the web application, the actions of the four different user types— doctors, patients, the vaccine team, and the reporting team—are elucidated.

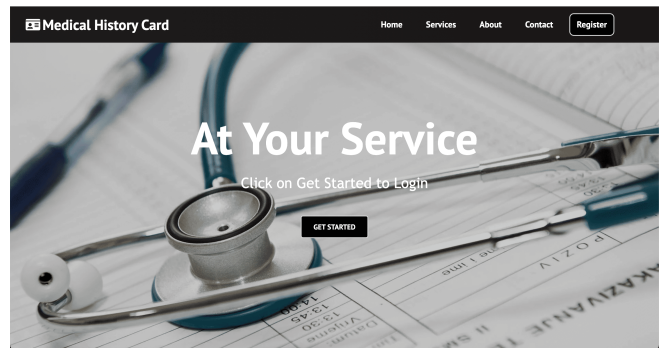


Figure 6: Home Page of the Website

The MHC starts with a Home page. This on boarding page will help the users learn how to get started and derive value from it (Figure 6). The home page contains a Navigation bar at the top to direct to a particular sector as per the user's requirements.

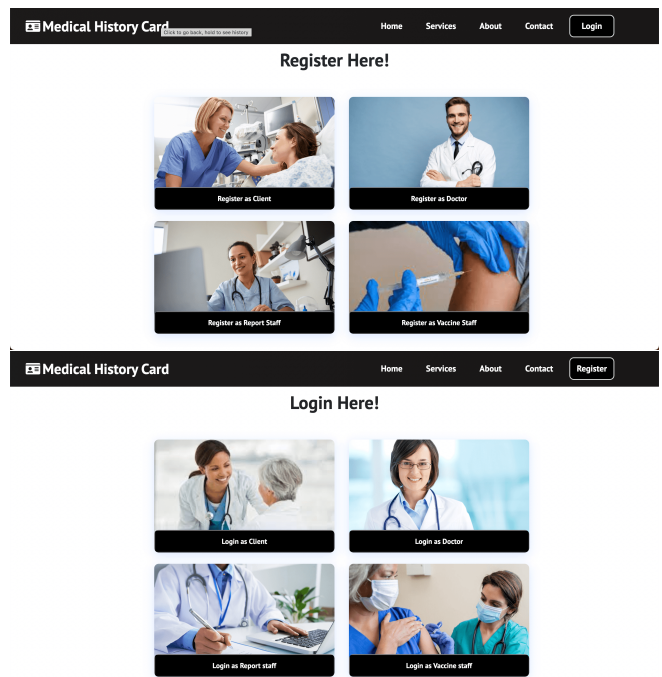


Figure 7: Registration and Login Dashboard

The registration and login pages contain four individual cards designed for each of our four users (Fig. 7). In the registration process, both the birth identity (BID) and national identification (NID) are collected as input, as the web application allows patients under the age of 18 to create accounts. In such cases, the BID becomes a mandatory requirement. After that, a success message will be received as well as the client could see the automatically generated HID in the message. Likewise, users can log in with the help of the login page after registration.

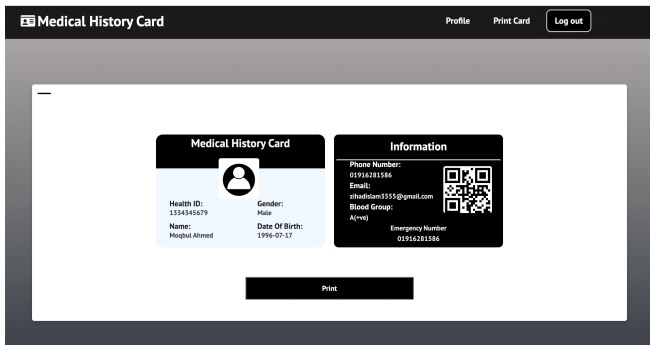


Figure 8: A Demo of the Medical History Card

The inclusion of a unique HID and QR code for each patient card adds an extra layer of convenience and security to the web application for both doctors and patients. It also adds an extra layer of security by ensuring that only authorized personnel (doctors and the respective patients) can access and view the associated medical records. Additionally, patients have the option to download and print their cards by clicking the "Print" button within the website's application, as illustrated in Figure 8.

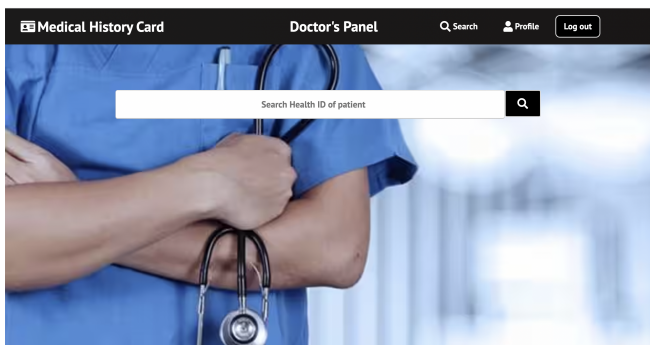


Figure 9: Doctor's Searching Panel

The doctor can then search for a patient in the doctor searching panel by entering the patient's HID and will be able to view his medical information (Figure 9). In a similar manner, the staff members who work with vaccines and reports have access to search. However, the patient's medical information has been limited in accordance with the roles.

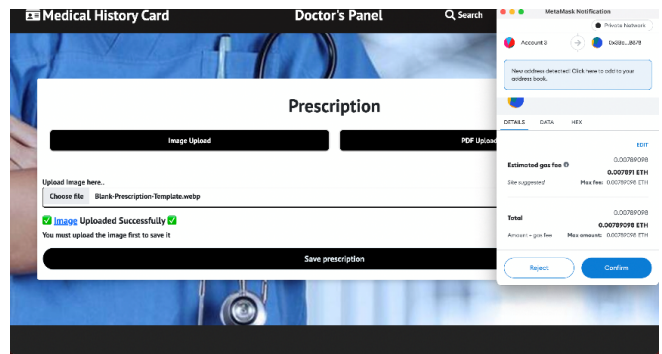


Figure 10: A Doctor Uploading a Patient's Prescription

Doctors have the flexibility to upload patient prescriptions which prompts them to select the prescription file they want to upload. They can choose either an image file (e.g., JPG, PNG) or a PDF document, as shown in Figure 10.

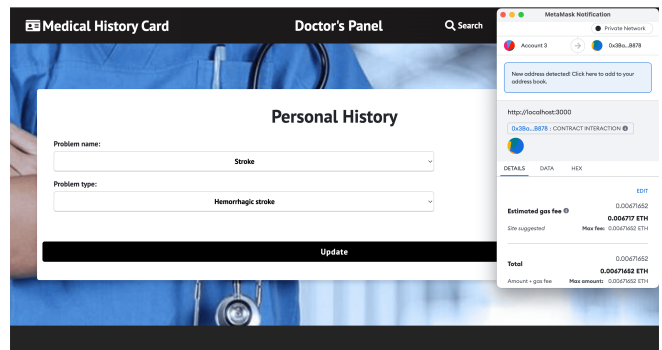


Figure 11: A Doctor Submitting Personal Health History of Patient

Moreover, they have the option to upload a patient's personal medical background by picking the issue's name and category from a drop-down menu, input familial medical histories by selecting the disease name and the family member's relationship from a separate drop-down menu, and offer recommendations by entering information into a designated text field (Figure 11).

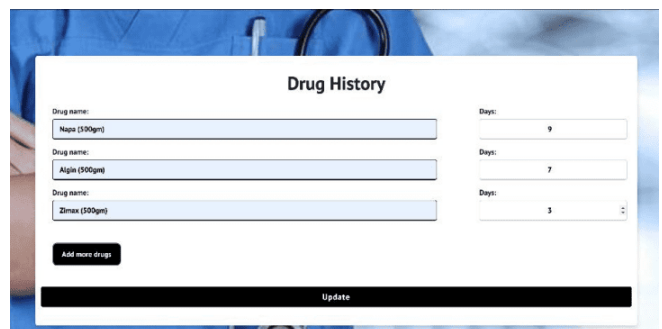


Figure 12: A Doctor Submitting a Patient's Medication History

In the web application's 'Drug History' section, physicians can make updates to a patient's prior medication record. To accomplish this, they need to enter the medication's name manually into the text area and specify the duration of consumption by using the increment counter located on the right, as depicted in Figure 12.

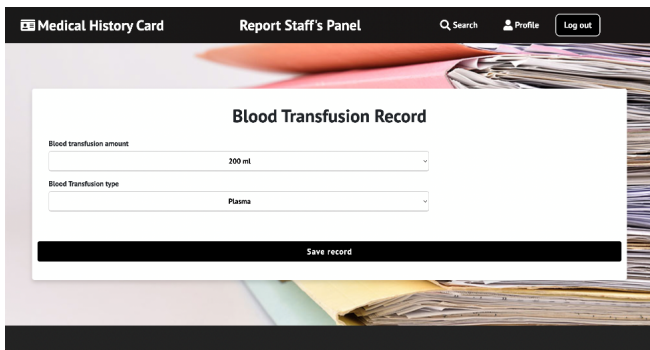


Figure 13: A Report Staff Uploading Blood Transfusion Record

On the other hand, the personnel responsible for managing vaccines and reports have the capability to not just review personal histories but also to make updates to vaccination histories and reports as needed. The "Blood Transfusion Record" might also be synced by the report staff, as shown in Figure 13. In this case, the drop-down boxes are utilized to choose the quantity and type of transfused blood.

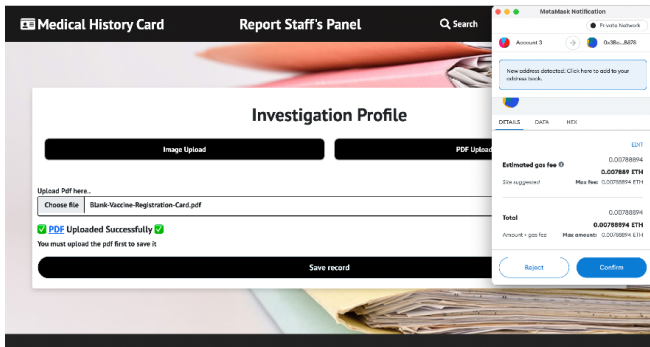


Figure 14: A Report Staff Uploading Patient's Investigation Profile

The report staff is also authorized to update a patient's "Investigation Profile," and the functionality for this task is similar to that of the prescription page. They have the ability to upload reports in both image and PDF file formats, providing flexibility in how medical information is recorded and shared.

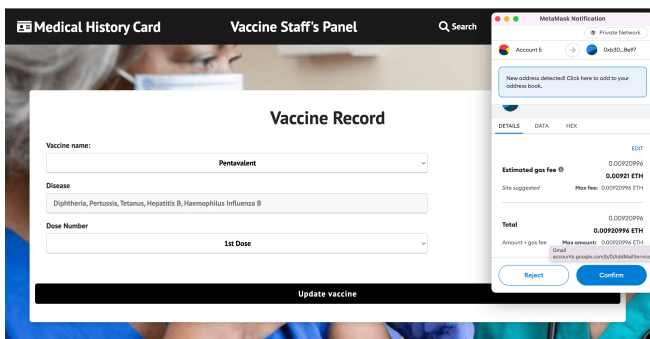


Figure 15: A Vaccine Staff Uploading Vaccination Record

It's also notable that, when updating vaccination histories, the vaccine staff will automatically see the name of the disease for which the vaccine is administered after selecting the vaccine's name from

the drop-down box. Afterward, they must also select the quantity of vaccine doses (Figure 14).

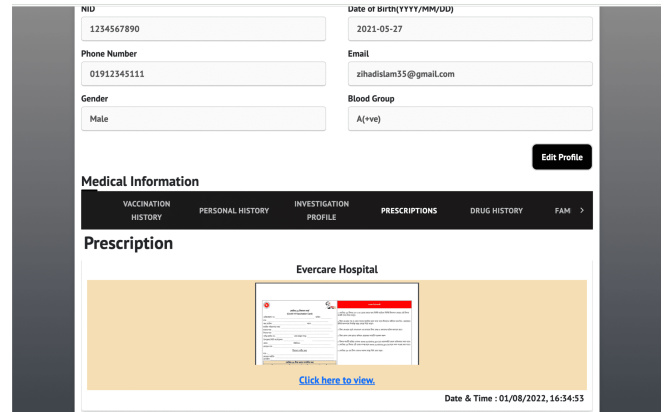


Figure 16: A Patient Viewing His Medical Information

Subsequently, patients are unable to upload their own data, but they can readily access their health-related information through the central navigation bar (as shown in Figure 15). Moreover, for enhanced monitoring, individuals have the option to download or print the medical reports and prescriptions, as well as capture screenshots of their medication history, personal health history, and vaccine history.

## 7 Contribution

The aforementioned card plays a crucial role in enhancing the security of patients' important medical data and preventing unauthorized access and manipulation of information. Along with preserving the authenticity of those high-priority data, this card can assist users during life-threatening conditions. The details enlisted in Personal History are of immense importance in the medical world. People with diabetes, high blood pressure, allergies, sinusitis, or asthma cannot afford every treatment or medicine. For this reason, doctors always ask these notable queries during consulting patients. If the patients are unaware of these facts, they are asked to undergo tests immediately. Besides, surgery history and thyroid (either hypothyroid or hyperthyroid) are also essential health indicators. During emergencies, the particulars provide essential information about a person. Specifically, the blood group and emergency contact number can significantly help during critical accidents. Concurrently, the investigation profile will remove the burden of carrying out reports, making diagnosis analysis easier for the doctors. They can glance through the reports to check whether the patient has any significant problems. To add, they can also check the severity of the disorder at that moment, which would instantly give them a more advanced view of the patient's present condition. They would understand if the present illness is somehow related to the previous history or not. Furthermore, people at a time tend to forget their vaccinations and the number of doses taken. This might create confusion in adulthood. Hence, this card can remove the hassle of memorizing all the vaccines. Drug history and prescriptions are the only ways to know about past treatments for any disease. With this card, the patients will no longer lose these valuable records while getting



treated. Consequently, they will get proper treatment on time. Congenital anomalies or birth defects develop prenatally or may be diagnosed later in life. These records help assess whether a disease is by birth. Afterward, the card will assist doctors in becoming familiar with the genetic disorders of a patient in such a way that they can recommend effective ways to reduce the risks. In the same way, blood transfusion history makes the task of knowing about the transfusion date and amount easier. So, patients can refrain from confirming any hypothetical dates to the medical officers.

It is worth mentioning that, Blockchain technology addresses healthcare security challenges in a broader range through its decentralized and tamper-resistant nature. Advanced encryption techniques and hash functions contribute to securing data within each block. The decentralized structure, distributed across a network of nodes, minimizes the risk of unauthorized manipulation. Smart contracts automate and enforce security protocols, reducing reliance on centralized databases and enhancing overall data protection. Above all, Blockchain presents a comprehensive solution to healthcare security by combining transparency, integrity, and patient-centric control in the management of sensitive health data.

Finally, advice given by doctors will be enlisted in this card. Suppose any patient has consulted two doctors for any particular disease over a time interval, and the former doctor has suggested something. Viewing the records allows the latter to analyze if it worked for the patient. Besides, he can also add his suggestions for future reference.

## 8 Observation

Between 1973 and 2023, there has been a significant evolution in the field of medical records. In the past, people relied on paper-based records, which were susceptible to data loss and damage, including the risk of being destroyed by fire or other accidents. As in [28] (2011) the authors have pointed out, EMRs have the potential to reduce diagnostic errors through various mechanisms. In a similar vein, we have structured our EMR system by categorizing information, aiming to create a more allocated, reliable, and information-rich system while maintaining brevity and efficiency. Furthermore, our web application is designed to alleviate the workload of hospital medical professionals and support staff.

Later, in 2016, the authors of the paper as referred [10] shed light on different aspects concerning the IoT and the digitalization of healthcare data. They emphasized that IoT mobile devices faced numerous challenges, including problems with integrating data, ensuring security and privacy, handling large volumes of data, maintaining performance, offering flexibility, dealing with the abundance of applications, and managing device diversity and interoperability. On the other hand, Blockchain databases were recognized for their flexibility and security. Additionally, our web application based on card technology was considered more convenient than relying on a device-oriented server.

Subsequently, we encountered web software which is stored information within a central database. However, in today's digital landscape, privacy issues have become prevalent, and concerns regarding hacking and data tampering with centralized databases have grown. Consequently, to enhance safety and visibility, we

made the decision to adopt a decentralized database, specifically utilizing Blockchain technology. Moreover, we came across numerous applications that allowed patients to input their reports and other healthcare records. Nevertheless, on MHC, this information is automatically kept up to date by healthcare professionals and other affiliated staff members.

Following that, in [12] the authors provided valuable insights into the management of healthcare data utilizing blockchain technology, with a particular emphasis on sharing EMRs among medical providers. These researchers developed a prototype framework that aimed to guarantee privacy, security, availability, and precise access control over EMR data. It should be noted, however, that their framework had limitations, as it was designed exclusively for managing data related to cancer patients. In contrast, our paper extends this concept to encompass all patients, providing a more comprehensive approach to healthcare data management.

Next, in 2018, the researchers in [15] introduced an innovative attribute-based signature system that involved the participation of multiple authorities to authenticate the validity of EMRs integrated into the Blockchain. In this method, a patient signs a message using a specific attribute, revealing no extra information except for the verification that they have indeed endorsed it. It's important to emphasize that this signature method is rather complex and involves a higher associated cost. Conversely, our project is designed to be cost-effective, ensuring that it remains affordable for every citizen of a nation.

In summary, the Blockchain-based MHC system offers a solution where neither patients nor doctors can conceal or manipulate information, as records cannot be removed or altered. This innovative approach ensures the immutability of data, effectively putting an end to unreliable and erroneous information. The decentralized and distributed nature of Blockchain introduces a substantial level of complexity when it comes to any efforts to manipulate stored data, although it is not entirely impervious to such attempts. Moreover, the risk of data loss is eradicated because the servers of the network preserve a copy of the data.

Blockchain-based medical records systems in live healthcare environments face challenges such as user adoption, infrastructure integration, and regulatory compliance. These include complexity, resistance to change, compatibility with legacy systems, scalability, and compliance with data standards. Healthcare systems are highly regulated, and adhering to these regulations is crucial for patient data security. Additionally, ensuring interoperability and compliance with data standards across different healthcare providers' systems is essential. Initial investment in infrastructure, development, and training can be challenging, and resource allocation can be ongoing. To address these challenges, collaboration and education, pilot projects, interoperability standards, partnerships, and continuous evaluation and improvement are essential. A strategic approach, collaboration between stakeholders, and a clear understanding of technical and regulatory landscapes are necessary for successful implementation in a live healthcare environment.

The MHC system is not only cost-free but also more optimized than relying on any gadget-based server. Moreover, it is readily accessible to every citizen which makes it a valuable addition to the tech improvements of the medical field.

## 9 Upcoming Work

The medical history card is dedicated to advancing healthcare technology through the utilization of Blockchain technology. Its ultimate objective is to guarantee the safety and credibility of medical data. To enhance its use during emergencies, microchips will be incorporated in the future. This electronic, intelligent microchip-based card will store all patient data, enabling doctors to quickly access medical histories by scanning the card. Additionally, the implementation of biometric fingerprints will further enhance user authentication, providing significant benefits even for unconscious patients who may not have a physical card. Furthermore, MHC could serve as evidence of health insurance by storing records within a decentralized database. Medical history is essential in medical insurance, guiding risk assessment, underwriting, and claim validation. It informs insurers about health risks, aids policy customization, and verifies the legitimacy of treatments. Customizing policies based on health profiles and using medical history in actuarial analysis enhances overall insurance efficiency, ensuring tailored coverage and effective resource management. In essence, MHC is a cornerstone in shaping informed decisions throughout the insurance process.

In terms of family history, it would automatically establish a family history by cross-referencing an individual's HID with that of their parents. That said, the card that collects a patient's thorough history from birth will become inundated with a substantial amount of information, posing challenges and requiring a significant amount of time for doctors to navigate through. Therefore, several AI recommendations for assisting doctors would be added. When a patient visits a doctor, the system will prioritize displaying relevant information about the doctor's field of specialization. As an example, a cardiologist will be able to go through the patient's analysis reports, prescribed medicines, and diagnosis results of other consulted cardiologists first. This will not only optimize time and energy but also help in identifying the underlying causes more efficiently. The website will incorporate a search bar to simplify the process of searching for specific patient medical information by entering relevant keywords. In addition to this, it will introduce a filtering feature that allows doctors to search a patient's EMRs based on the year. The website will utilize AI to examine all the vital criteria provided by the client. If any potential risk factors are identified, the site will display a warning message and offer recommendations for the appropriate specialists. The integration of automated recommendation represents a paradigm shift in healthcare, employing AI, ML, and data analytics to offer personalized guidance to healthcare professionals and patients. These systems analyze patient data, create personalized treatment plans, predict health risks, monitor health remotely, prescribe medications, optimize resource allocation, and contribute to clinical trials. By leveraging extensive datasets, these automated recommendations enhance patient outcomes and streamline healthcare delivery, showcasing a substantial leap in utilizing data for improved medical practices. It also aspires to utilize AI to analyze user-provided information about their current health issues and provide recommendations for appropriate first-aid measures and relevant specialists. Besides, the users will be able to submit their urgent needs and preferred location for blood through a new section on the website. Anyone in the vicinity who is willing to donate blood will be promptly notified by the application.

## 10 Conclusion

The current paper implements a multi-functional history card system to be the best companion in one's healthcare world. In other words, it terminates the conventional papered system of preserving patients' medical history by introducing a portable card; that accumulates every tiny detail such as personal narrative, prescriptions, reports, drugs, vaccine history, etc. The card serves the dual purpose of consolidating Electronic Medical Records (EMRs) into a unified system and ensuring that users have controlled access to protect their privacy. Crucially, a brief review of the history card provides doctors with a more concise overview of the patient's medical background. Moreover, it makes it easy for the users to search for and get an auto-update of their required medical information within a trouble-free go. Besides, the understandable user interface can assist people in avoiding any last-minute stress while visiting doctors. Conversely, doctors and medical officers can also track patients' diagnoses properly. They can view, read, and update medical data as per their need and avoid the hassles of handling lots of reports and papers, eventually protecting their goodwill in the long run. Hence, the medical history card comes into the picture in every scenario of contributing to the flourishing of the healthcare world. All in all, Blockchain technology can revolutionize healthcare with secure, interoperable, and patient-centric data management. Research priorities include improving security, ensuring interoperability, implementing consent management, addressing legal challenges, and enhancing user experience and adoption. Continued research and development efforts have the potential to significantly elevate the capabilities and reliability of blockchain-based systems for medical records, transforming the healthcare industry.

## References

- [1] S. Fairouz, S. Y. Miti, Z. Islam, M. T. Zaman, "A medical history card utilizing the Blockchain technology," in 2023 5th International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), 1-6, 2023, doi:10.1109/HORA58378.2023.10156689.
- [2] R. Hillestad, J. Bigelow, A. Bower, F. Girosi, R. Meili, R. Scoville, R. Taylor, "Can Electronic Medical Record Systems Transform Health Care? potential health benefits, savings, and costs," *Health Affairs*, **24**(5), 1103-1117, 2005, doi:10.1377/hlthaff.24.5.1103.
- [3] C. M. Ruland, H. Bryhni, R. Andersen, T. Bryhni, "Developing a Shared Electronic Health Record for Patients and Clinicians," *Studies in health technology and informatics*, **136**, 57-62, 2008.
- [4] K. Phillips, C. Wheeler, J. Campbell, A. Coustasse, "Electronic medical records in long-term care," *J. Hosp. Mark. Public Relations*, **20**(2), 131-142, 2010.
- [5] M. Gomi, Y. Nakayama, Y. Sakurai, R. Oyama, K. Iwasaki, M. Doi, Y. Liu, M. Hori, H. Watanabe, K. Hashimoto, H. Tanaka, K. Tange, Y. Nakai, H. Akita, "Tolerogenic lipid nanoparticles for delivering self-antigen mRNA for the treatment of experimental autoimmune encephalomyelitis," *Pharmaceuticals (Basel)*, **16**(9), 1270, 2023.
- [6] Y. C. Li, P. S. Lee, W. S. Jian, C. H. Kuo, "Electronic health record goes personal world-wide," *Yearb. Med. Inform.*, **18**(01), 40-43, 2009.
- [7] S. Soegijoko, I. Puspitasari, A. Aridarma, I. Jani, "e-health for improving community healthcare: Encouraging clinical experience of simple e-prescription system and m-health system development for mother and childcare," in 2011 IEEE 13th International Conference on e-Health Networking, Applications and Services, 102-105, 2011, doi:10.1109/HEALTH.2011.6026722.

- [8] E. T. van der Velde, H. Foeken, T. A. Witteman, L. van Erven, M. J. Schalijs, "Integration of data from remote monitoring systems and programmers into the hospital electronic health record system based on international standards," *Neth. Heart J.*, **20**(2), 66–70, 2012.
- [9] O. Ben-Assuli, I. Shabtai, M. Leshno, "Using electronic health record systems to optimize admission decisions: the Creatinine case study," *Health Informatics J.*, **21**(1), 73–88, 2015.
- [10] A. Chhatlani, A. Dadlani, M. Gidwani, M. Keswani, P. Kanade, "Portable Medical Records Using Internet of Things for Medical Devices," in 2016 8th International Conference on Computational Intelligence and Communication Networks (CICN), 446–451, 2016, doi:10.1109/CICN.2016.93.
- [11] A. Ekblaw, A. Azaria, J. Halamka, A. Lippman, "A case study for blockchain in healthcare: "MedRec" prototype for electronic health records and medical research data. White Paper," Retrieved from <https://static1.squarespace.com/static/59aae5e9a803bb10bedeb03e/5/1517278000381/2016>.
- [12] A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, F. Wang, "Secure and trustable electronic medical records sharing using blockchain," in AMIA annual symposium proceedings, volume 2017, 650, American Medical Informatics Association, 2017.
- [13] "Why Blockchain Technology Is Important for Healthcare Professionals — Mendeley," <https://www.mendeley.com/search/?page=1&query=Why%20Blockchain%20Technology%20Is%20Important%20for%20Healthcare%20Professionals&sortBy=relevance>, (Accessed on 11/30/2023).
- [14] A. F. Hussein, N. ArunKumar, G. Ramirez-Gonzalez, E. Abdulhay, J. M. R. Tavares, V. H. C. de Albuquerque, "A medical records managing and securing blockchain based system supported by a Genetic Algorithm and Discrete Wavelet Transform," *Cognitive Systems Research*, **52**, 1–11, 2018, doi: <https://doi.org/10.1016/j.cogsys.2018.05.004>.
- [15] R. Guo, H. Shi, Q. Zhao, D. Zheng, "Secure Attribute-Based Signature Scheme With Multiple Authorities for Blockchain in Electronic Health Records Systems," *IEEE Access*, **6**, 11676–11686, 2018, doi:10.1109/ACCESS.2018.2801266.
- [16] J. Liu, X. Li, L. Ye, H. Zhang, X. Du, M. Guizani, "BPDS: A Blockchain Based Privacy-Preserving Data Sharing for Electronic Medical Records," in 2018 IEEE Global Communications Conference (GLOBECOM), 1–6, 2018, doi:10.1109/GLOCOM.2018.8647713.
- [17] K. Riad, R. Hamza, H. Yan, "Sensitive and Energetic IoT Access Control for Managing Cloud Electronic Health Records," *IEEE Access*, **7**, 86384–86393, 2019, doi:10.1109/ACCESS.2019.2926354.
- [18] Y. Zhao, M. Cui, L. Zheng, R. Zhang, L. Meng, D. Gao, Y. Zhang, "Research on electronic medical record access control based on blockchain," *International Journal of Distributed Sensor Networks*, **15**(11), 1550147719889330, 2019.
- [19] V. Mehra, P. Sarvari, N. Ruban, "RFID Based Secured, Remotely Accessible Personal Medical Data Base Including the Medicinal History," in 2018 4th International Conference on Computing Communication and Automation (ICCCA), 1–4, 2018, doi:10.1109/CCAA.2018.8777617.
- [20] M. T. de Oliveira, L. H. A. Reis, R. C. Carrano, F. L. Seixas, D. C. M. Saade, C. V. Albuquerque, N. C. Fernandes, S. D. Olabarriga, D. S. V. Medeiros, D. M. F. Mattos, "Towards a Blockchain-Based Secure Electronic Medical Record for Healthcare Applications," in ICC 2019 - 2019 IEEE International Conference on Communications (ICC), 1–6, 2019, doi:10.1109/ICC.2019.8761307.
- [21] S. Siva Rama Krishnan, M. Manoj, T. R. Gadekallu, N. Kumar, P. K. R. Maddikunta, S. Bhattacharya, D. Y. Suh, M. J. Piran, "A Blockchain-Based Credibility Scoring Framework for Electronic Medical Records," in 2020 IEEE Globecom Workshops (GC Wkshps), 1–6, 2020, doi:10.1109/GCWkshps50303.2020.9367459.
- [22] C.-T. Li, D.-H. Shih, C.-C. Wang, C.-L. Chen, C.-C. Lee, "A Blockchain Based Data Aggregation and Group Authentication Scheme for Electronic Medical System," *IEEE Access*, **8**, 173904–173917, 2020, doi:10.1109/ACCESS.2020.3025898.
- [23] M. T. Mahmud, F. Soroni, M. M. Khan, "Development of a Mobile Application for Patient's Medical Record and History," in 2021 IEEE World AI IoT Congress (AIIoT), 0081–0085, 2021, doi:10.1109/AIIoT52608.2021.9454227.
- [24] M. Nasim, S. Abdullah-Al-Noman, A. Ragib Hasan, A. Sattar, "Digitalization and Centralization of Medical Information and Patient History in Bangladesh," in 2022 6th International Conference on Computing Methodologies and Communication (ICCMC), 153–158, 2022, doi:10.1109/ICCMC53470.2022.9753690.
- [25] R. Cerchione, P. Centobelli, E. Riccio, S. Abbate, E. Oropallo, "Blockchain's coming to hospital to digitalize healthcare services: Designing a distributed electronic health record ecosystem," *Technovation*, **120**, 102480, 2023, doi: <https://doi.org/10.1016/j.technovation.2022.102480>.
- [26] S. Singh, S. Kumar Sharma, P. Mehrotra, P. Bhatt, M. Kaurav, "Blockchain technology for efficient data management in healthcare system: Opportunity, challenges and future perspectives," *Materials Today: Proceedings*, **62**, 5042–5046, 2022, doi: <https://doi.org/10.1016/j.matpr.2022.04.998>, international Conference on Innovative Technology for Sustainable Development.
- [27] M. Haidar, S. Kumar, "Smart Healthcare System for Biomedical and Health Care Applications using Aadhaar and Blockchain," in 2021 5th International Conference on Information Systems and Computer Networks (ISCON), 1–5, 2021, doi:10.1109/ISCON52037.2021.9702306.
- [28] N. Malhotra, M. Lassiter, et al., "The coming age of electronic medical records: From paper to electronic," *International Journal of Management & Information Systems (IJMIS)*, **18**(2), 117–122, 2014.