

# Block-Chain Based Unified Identity Authentication System in Medical Report for Health-Cares

Dr. Mohammed Abdul Waheed <sup>1</sup>, Najma Shaheen Ansari <sup>2</sup>, Zohara Begum <sup>3</sup>

<sup>1</sup> Department of Computer Science, VTU, CPGS, Kalaburagi, Karnataka, India.  
[prof.mawaheed@gmail.com](mailto:prof.mawaheed@gmail.com)

<sup>2</sup> Department of Computer Science, VTU, CPGS, Kalaburagi, Karnataka, India.  
[najmashaheen8899@gmail.com](mailto:najmashaheen8899@gmail.com)

<sup>3</sup> Assistant Professor Dept. of E&CE, FENT, KBN University, Kalaburagi. [zohra1@kbn.university](mailto:zohra1@kbn.university)

**Abstract:** Organisations and individuals can efficiently manage their identity management operations with the help of identity management software. 'Identity Management' (IdM) software assists the administrators of an organisation in clearly defining and modifying a person's role in the organisation and authorising the relevant access to them. An identity management process is designed to identify, authenticate, and authorise individuals to access organisational software resources. Using this programme, administrators are also able to monitor user login and activity on the corporate computer network. Thus, operational security is improved. The healthcare industry has grown at the quickest rate in terms of revenue and data. Security is now more crucial than ever because electronic medical records are so common. The security of each patient's medical records is a top priority in current medical systems. Furthermore, there are efforts to increase safety of this confidential data by encrypting it. Therefore, we advocated for implementation of block chain systems as decentralized approach to protecting patients' health information. It has three parts: data retrieval, encryption, and authentication using block chain technology. While assuring patient protection, the suggested framework might also keep the healthcare system's security and legitimacy.

Keywords: Identity Management (IdM), Block chain, encryption, security, electronic.

## 1. INTRODUCTION

The fastest-growing technology, block chains are used in a variety of secure applications. The different implementations among stakeholders leverage this block chain technology. Blockchain technology primarily has a big impact on the medical and healthcare sectors. owing to dispersed and decentralised technology. There is a high risk of data leak & accessibility delays due to present health care system's centralized architecture, that affects all of medical services. In this case, the patient might not be informed that their medical records are being archived. The key problem with the existing health care keeping system is retrieving information in highly secure method within network. Present online healthcare systems, known as Electronic Health Records (EHR/EMR), are crucial for keeping and storing data but have a serious problem with patient information leaking. This turns into the main driver behind the advancement of block chain technology. Block chain technology chases privacy, respectability, and verification in addition to security and ease of access. It also supplies additional production aspects in the administrations. Blockchain, or distributed secured database technological advances, was first used in 2008 to facilitate peer-to-peer electronic monetary transactions using bitcoin currency. Open ledgers, encryption, & chronological sequence of data blocks make up blockchain technology. [26]. The widespread cyber security capabilities of the blockchain technology have drawn attention. These capabilities can be applied to a variety of industries, including global finance, trade administrations, and healthcare. The blockchain's prospective services exceed its existing applications, and it appears that academia is really benefiting from it. There are areas within the academic community that could be advanced by using this innovation, and this sector may be just as important as healthcare and finance. The following are some of Blockchain's most distinguishing features:

1. Decentralization. Decentralization may be broken down into the three categories of architecture, politics, and logic.
2. Persistency. No data in network may be changed, & any attempt to do so would be quickly discovered.
3. Anonymity. A person might make up a bunch of fake email addresses to protect their privacy. It ensures that financial dealings remain private.
4. Auditability. It makes data on blockchain more transparent & traceable.

## 2. RELATED WORK

**G.Wood[13]**, Bitcoin is only one of several initiatives that have shown how useful blockchain paradigm can be when combined with cryptographically protected transactions. Every of these initiatives resembles a basic program running on a shared but isolated computing cluster. This model may be described as transactional singleton machine that uses shared state. Ethereum is a generalized implementation of this concept. Additionally, it offers a number of these assets, all of which has its own state and operation code but may communicate with one another via a message-passing architecture. We talk about how it was made, potential problems with execution, advantages, & potential problems in future.

**M. Wohrer and U. Zdun [14]**, Since they enable unauthorized parties to express contractual conditions in computer code and therefore remove requirement for trusted 3rd party, smart contracts which rely on blockchain technology are attracting a lot of interest in new applications for businesses & scientific fields. Ethereum is now the most popular smart contract platform, however it may be challenging to write contracts that function effectively and are safe. Only lately has business & science begun doing studies on this problem. We construct numerous prevalent security characteristics and explain them in depth upon framework of Solidity, dominant programming language for Ethereum, following study of gathered data using Grounded Theory methodologies. Developers working with Solidity may employ described patterns to help prevent common security breaches.

**P. Zhang, et.al [15]**, This paper aims at addressing existing gap in knowledge by presenting: (1) an examination of characteristics and difficulties encountered in achieving connectivity in medical field, (2) a comprehensive analysis of healthcare application based on blockchain technology that is currently under development, and (3) an exploration of potential benefits of employing fundamental software sequences to overcome prevalent problems with interoperability encountered by blockchain-based healthcare applications.

**Christo, et.al [16]**, IFBR-AODV routing system has been presented as a novel secure routing protocol for efficient network communications. In this study, we employ machine learning & fuzzy rules to the task of user decision making in network monitoring. Administrator keeps tabs on all of users & their actions inside health care program.

## 3. PROPOSED SYSTEM

Aim of our research is using block chain technology to control medical records access in a secure manner by individually identifying data security. The fundamental patient information and laboratory test results are encrypted using the Block Chain Crypto System Algorithm. An information system called the clinical dataset provides users with knowledge and personalised information in order to improve their health and healthcare outcomes. UIn the Crypto System, the practise of encrypting digital currency protects each patient's data. For locating the most pertinent patient data across several data sources, a unique paradigm is provided.

## 4. METHODOLOGY

Create an account by supplying the usual user information (name, surname, email address, password, etc.). First step in using registry is for patient to register their information, at which point a fresh user identification will be generated. If patient has previously existed, person may go ahead to view his or her medical records by entering unique identifier. With the aid of patient ID, a unique private key is created for every patient. Login operation can be done Using User Name and Password. Hence registration is finished.

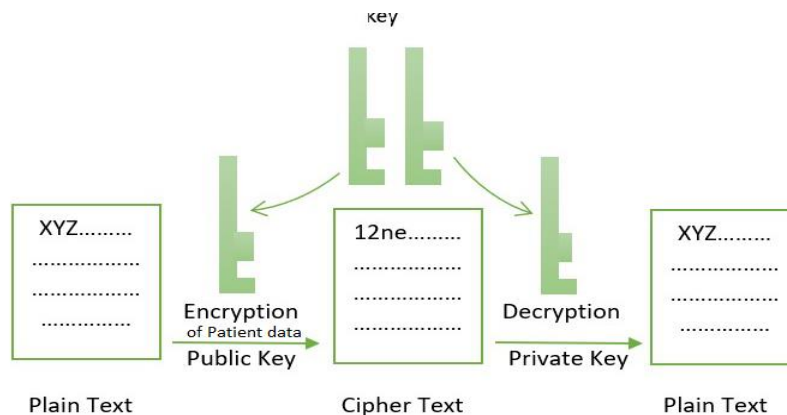
```

A. Generate New ID for Patient
if (patient == new user) then
Register with personal information
create unique ID (idp),
public key (Pkp),
private key (Skp)
login (idp, Skp, Pkd)
else
directly login using ID (idp)
    
```

**B. Authenticating doctor:** The hospital management must maintain track of doctor's medical records while creating a public key for physician. To complete authentication, the doctor's public key is utilized. Make a valid ID card for doctor, and if he or she wants to add anything to it, have patient sign off on it. After passing this Step, only patient's approved doctors will be able to access and edit their medical records. No physician without the patient's written consent shall be able to see his or her medical records. This will ensure confidentiality of patient's medical record.

**C. Health Care Data** The patient's medical history, including the patient's height, weight, blood pressure, climate, pulse, and indications for disease. Taking into account possible issues caused by a patient's co-existing health issues, we propose a Crypto system algorithm for multi-label learning, making use of correlations within labels database & expecting additional possible diseases of a patient.

**Block Chain Crypto System Algorithm** Every patient's records shall be secured utilizing the block chain algorithm and secure cryptographic method. The database's encrypted information is decrypted & presented to the correct patient and their doctor.



**Encrypt medical report** The AES algorithm may be used to accomplish the necessary encoding. The Advanced Encryption Standard, or AES, is a symmetric encryption algorithm with a defined use case for protecting digital information. The AES engine requires both the plain text to be encrypted & secret key in order to decode it. Patient information is encrypted using patient's private key,  $E_k(PR, k)$ . The medical record is encrypted using patient's private key. As a result, PC is where the encrypted data  $E_k(PR, k)$  accompanied by timestamp(T) &  $PC(PR, T)$  resides. Addresses of encrypted data kept in private clouds are recorded in a distributed ledger called a block chain (BC).

The term "Advanced Encryption Standard" (AES) refers to a set of guidelines for secure transmission of digital information. Although more difficult to install than its predecessors DES & triple DES, AES is now commonly utilized because to its superior strength.

Block ciphers are what AES is.

A 128-bit, 192-bit, or 256-bit key may be used.

Uses 128-bit key to encrypt data.

The Cipher's Internal Workings

When processing data, AES uses bytes instead of bits. Since 128-bit blocks are used in this encryption, 16 bytes of input data are processed at a time.

Key length determines how many times process is repeated.

128 bit key – 10 rounds

192 bit key – 12 rounds

256 bit key – 14 rounds

Creating Round keys:

Each round key may be computed by key using Key Schedule technique. Therefore, the primary key is implemented to generate a large number of secondary keys, each of them is utilized in subsequent encryption cycle.

Encryption :

Each block is represented in AES as 128, or 16-byte, column-major grid (4 bytes x 4 bytes).

```
[ b0 | b4 | b8 | b12 |
 | b1 | b5 | b9 | b13 |
 | b2 | b6 | b10 | b14 |
 | b3 | b7 | b11 | b15 ]
```

Every round has 4 phase:

Sub Bytes

Shift Rows

Mix Columns

Add Round Key

Mix Columns round did not occur in final round.

Algorithm's Sub Bytes function executes replacement, while Shift Rows & Mix Columns rearrange data.

SubBytes :

The replacement is put into effect at this point.

Here, we swap out one byte for another. A lookup table, sometimes referred to as an S-box, is used to do this. Bytes are swapped out in such a manner as same byte is never used twice, and neither is a byte that is the complement of current byte used. This process yields a 16-byte (4-by-4) matrix, the same size as previously.

The following two actions carry out permutation.

ShiftRows :

This is actual first step. A certain number of rows are moved around.

1st row remains unchanged.

2nd row moves to left by one position.

3rd row moves to left twice.

4th row moves to left by three spaces.

```
[ b0 | b1 | b2 | b3 ]   [ b0 | b1 | b2 | b3 ]
 | b4 | b5 | b6 | b7 | -> | b5 | b6 | b7 | b4 |
 | b8 | b9 | b10 | b11 |   | b10 | b11 | b8 | b9 |
 [ b12 | b13 | b14 | b1 ]   [ b15 | b12 | b13 | b14 ]
```

MixColumns :

In essence, what you're doing here is multiplying matrices. By multiplying every column by a unique matrix, can be shifted bytes inside that column around.

In final iteration, this process is bypassed.

$$\begin{bmatrix} c0 \\ c1 \\ c2 \\ c3 \end{bmatrix} = \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} b0 \\ b1 \\ b2 \\ b3 \end{bmatrix}$$

Add Round Keys :

Here, the preceding stage's output is XORed with its associated elliptic key. In this case, we treat the 16 bytes not as grid but as 128 individual bits of information.

The final result of these iterations is 128 bits of encrypted data. This procedure is continued until all of the target data has been encrypted.

Decryption :

Each step in cycles has an inverse that, when carried out, undoes the corresponding change. Depending on the size of key, every 128-bit block runs through 10, 12, or 14 iterations.

Every stage of decryption consists of the following steps:

Add round key

Mixed-Columns Inverse

ShiftRows

SubByte inversion

I'll discuss the procedures involved in decryption, which are essentially the same as those involved in encryption but with a few key distinctions.

Inverse MixColumns :

This process is analogous to MixColumns phase of encryption, with key difference being matrix utilized.

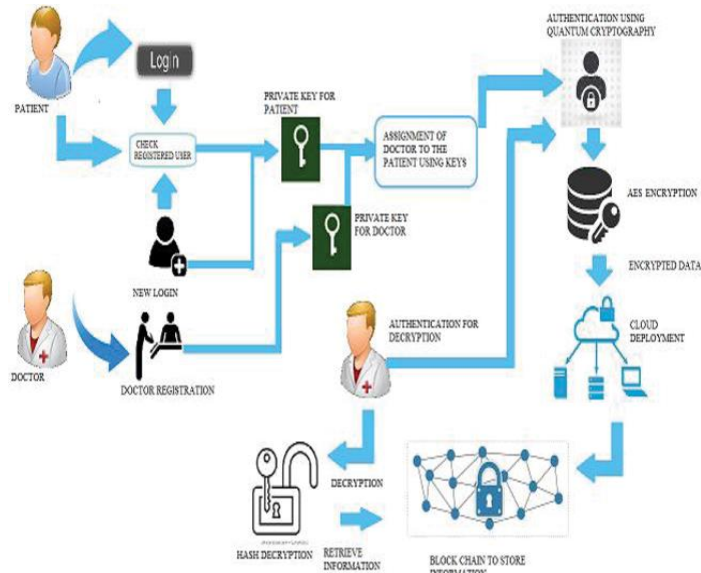
$$\begin{bmatrix} b0 \\ b1 \\ b2 \\ b3 \end{bmatrix} = \begin{bmatrix} 14 & 11 & 13 & 9 \\ 9 & 14 & 11 & 13 \\ 13 & 9 & 14 & 11 \\ 11 & 13 & 9 & 14 \end{bmatrix} \begin{bmatrix} c0 \\ c1 \\ c2 \\ c3 \end{bmatrix}$$

Inverse SubBytes :

When decryption, inverted S-box is employed as lookup table against that encrypted bytes may be replaced.

**D. Retrieving Medical Report** Only approved medical professionals will be able to access data. Data recovery through SHA method is now possible for verified physician.

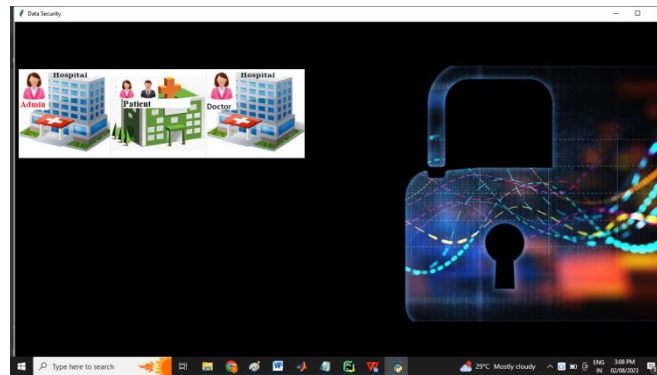
### 5. SYSTEM ARCHITECTURE



**Figure 1:** System Architecture

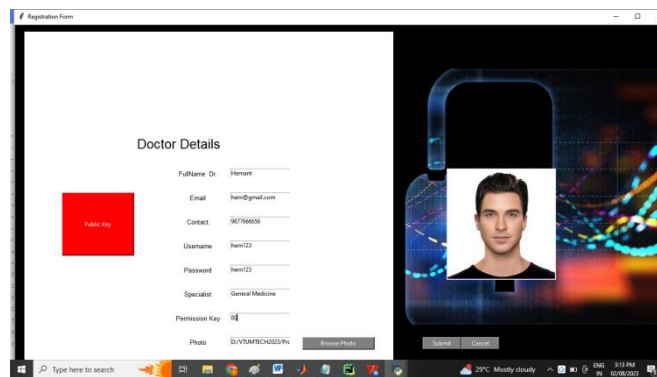
Patient is uploading the data using private key and doctor is downloading the patient data by decrypting the data using AES and DES algorithm.

### 6. IMPLEMENTATION



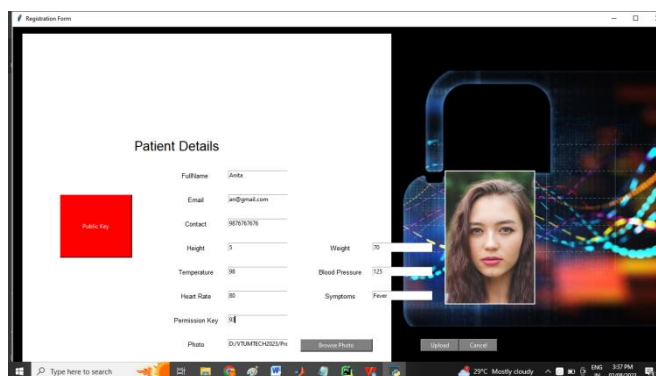
**Figure 2:** Menu

Using this Patient registration, Doctor registration, and patient data can access by the doctor



**Figure 3:** Doctor Details

Doctor’s medical history should be maintained by the administration of the hospital and public key for the doctor is generated. Then doctor’s public key is used as a key for the authentication using this module  
2117



**Figure 4:** Patient Details

Patient health care data like height, weight, blood pressure, temperature, heart beat rate, Diseases Symptoms will be given as input.

## 7. CONCLUSION

Many people and businesses of all sizes and types are starting to take an interest in blockchain. With properties like decentralization, anonymity, persistence, and auditability, it has the potential to revolutionize the conventional business sector. It is anticipated that blockchain technology would significantly alter healthcare sector. Not only will everything be open and safe, but quality of treatment will rise dramatically as costs drop dramatically. In this article, we covered a wide range of healthcare blockchain applications, highlighting both current and potential areas of study. In this talk, we discussed current state of study in medical data management as well as how use of block chain technology may improve patient agency and the efficiency with which health data can be shared. We discovered that academics agree on blockchain technology will finally put people in charge of their own health records. After entering the distributed ledger, health data are time-stamped by block chain to prevent any tampering. Patients should be able to choose who has access to their information and why. Nonetheless, there's number of questions which require answering.

## 8. REFERENCES

- [1] M. Iansiti and K. R. Lakhani. (2017). The Truth About Blockchain. [Online]. Available: <https://hbr.org/2017/01/the-truth-about-blockchain>
- [2] O. Ahumada and J. R. Villalobos, "Application of planning models in the agri-food supply chain: A review," *Eur. J. Oper. Res.*, vol. 196, no. 1, pp. 1–20, Jul. 2009. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0377221708001987>
- [3] P. Dutta, T.-M. Choi, S. Somani, and R. Butala, "Blockchain technology in supply chain operations: Applications, challenges and research opportunities," *Transp. Res. E, Logistics Transp. Rev.*, vol. 142, Oct. 2020, Art. no. 102067.
- [4] H. Feng, X. Wang, Y. Duan, J. Zhang, and X. Zhang, "Applying blockchain technology to improve Agri-food traceability: A review of development methods, benefits and challenges," *J. Cleaner Prod.*, vol. 260, Jul. 2020, Art. no. 121031.
- [5] K. Demestichas, N. Peppes, T. Alexakis, and E. Adamopoulou, "Blockchain in agriculture traceability systems: A review," *Appl. Sci.*, vol. 10, no. 12, pp. 1–22, 2020.
- [6] A. Kamilaris, A. Fonts, and F. X. Prenafeta-Boldú, "The rise of blockchain technology in agriculture and food supply chains," *Trends Food Sci. Technol.*, vol. 91, pp. 640–652, Sep. 2019.
- [7] G. Zhao, S. Liu, C. Lopez, H. Lu, S. Elgueta, H. Chen, and B. M. Boshkoska, "Blockchain technology in Agri-food value chain management: A synthesis of applications, challenges and future research directions," *Comput. Ind.*, vol. 109, pp. 83–99, Aug. 2019.
- [8] J. F. Galvez, J. C. Mejuto, and J. Simal-Gandara, "Future challenges on the use of blockchain for food traceability analysis," *TrAC Trends Anal. Chem.*, vol. 107, pp. 222–232, Oct. 2018.
- [9] J. Duan, C. Zhang, Y. Gong, S. Brown, and Z. Li, "A content-analysis based literature review in blockchain adoption within food supply chain," *Int. J. Environ. Res. Public Health*, vol. 17, no. 5, p. 1784, Mar. 2020.

- [10] C. Elsdén, A. Manohar, J. Briggs, M. Harding, C. Speed, and J. Vines, "Making sense of blockchain applications: A typology for HCI," in Proc. CHI Conf. Hum. Factors Comput. Syst., Apr. 2018, pp. 1–14, doi: 10.1145/3173574.3174032.
- [11] M. Foth, "The promise of blockchain technology for interaction design," in Proc. 29th Austral. Conf. Comput.-Hum. Interact., Nov. 2017, pp. 513–517, doi: 10.1145/3152771.3156168.
- [12] C. S. Wright. (2019). Bitcoin: A Peer-to-Peer Electronic Cash System. [Online]. Available: <https://bitcoin.org/bitcoin.pdf>
- [13] M. Torky and A. E. Hassanein, "Integrating blockchain and the Internet of Things in precision agriculture: Analysis, opportunities, and challenges," Comput. Electron. Agricult., vol. 178, Nov. 2020, Art. no. 105476.
- [14] I. Mistry, S. Tanwar, S. Tyagi, and N. Kumar, "Blockchain for 5Genabled IoT for industrial automation: A systematic review, solutions, and challenges," Mech. Syst. Signal Process., vol. 135, Jan. 2020, Art. no. 106382.
- [15] M. Singh, A. Singh, and S. Kim, "Blockchain: A game changer for securing IoT data," in Proc. IEEE 4th World Forum Internet Things (WFIoT), Feb. 2018, pp. 51–55.
- [16] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, "Blockchain and IoT integration: A systematic survey," Sensors, vol. 18, no. 8, p. 2575, Aug. 2018.

DOI: <https://doi.org/10.15379/ijmst.v10i4.2367>

This is an open access article licensed under the terms of the Creative Commons Attribution Non-Commercial License (<http://creativecommons.org/licenses/by-nc/3.0/>), which permits unrestricted, non-commercial use, distribution and reproduction in any medium, provided the work is properly cited.