IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 3, March 2020

A Panacea for Healthcare Data Security and Privacy

M.Swetha[1], S. Subalakshmi[2], Mr. A.S.Balaji[3]

Student, B.E Computer Science and Engineering, Anand Institute of Higher Technology, Chennai, India[1,2]

Assistant Professor, CSE, Anand Institute of Higher Technology, Chennai, India[3]

Abstract: In many parts of the city, there are several hospitals with many patients with different disease and several different treatments. Every hospital has different approach in treatment and procedures. Whereas other hospitals do not have much facility compared to big hospitals. In this project, details about a particular treatment ,patient details,disease information all are transferred between other hospitals in a secured manner using blockchain technology in a cryptographic approach by requesting and downloading files between the hospitals by using keys by advance encryption standard algorithm which is a fast and secure form of encryption which is a symmetric block cipher. The project gives a quick and easy access of medical data through the website.

Keywords: Data security and privacy, Advance Encryption Standard Technique (AES), Blockchain Technology

I. INTRODUCTION

Electronic Medical Records (EMRs) contain helpful and clinical data related to a given patient and away by the careful social protection supplier. They support the recuperation and examination of social protection data. To all the more promptly reinforce the organization of EMRs, early periods of Wellbeing Information Systems are arranged with the ability to make new EMR models, store them, and request and recoup set away EMRs of intrigue. To empower data sharing or even patient data adaptability, there is a fundamental for EMRs to formalize their data structure and the approach of HIS. Electronic Health Records (EHRs), for example, are proposed to empower understanding recuperating history to move with the patient or be made open to different human associations providers (for instance from a trademark helpful concentration to a crisis office in the capital city of the country, before the patient outputs for medicinal thought at another restorative concentration in a substitute country).3 EHRs have a more uncommon data structure than EMRs. With patient transportability (both inside and remotely to a given country) being continuously the standard in the present society, it ended up obvious that various free EMR courses of action must be made interoperable to energize sharing of social protection data among different providers, even over national edges, as required. Blockchain technology now produces a very good data security and privacy,which holds all data together in blocks where each block contain data, value and hash value of previous block.

II. EXISTING SYSTEM

In existing system, now a days in particular city lot of hospitals are there and in that every hospitals are joining with different disease.mainly in some of the big hospital only have all the equipment for treatment. And some of the doctors only know everything about all treatments. Some of the hospital they don't have any idea about that treatment. In this system blockchain technology was not used earlier.To overcome all those problem we are going to implement one method .how to share the information about the treatment about new disease to other hospitals.

III. SYSTEM ARCHITECTURE

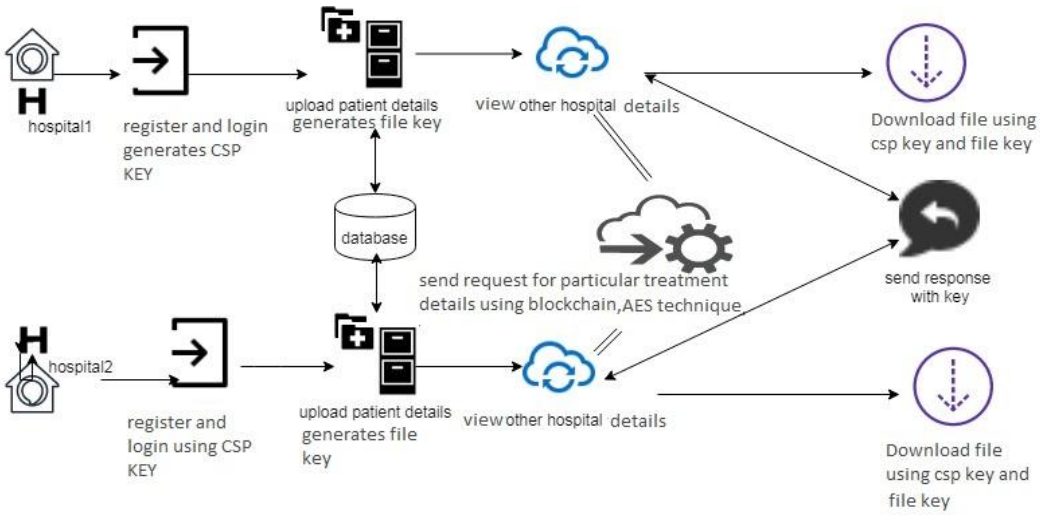
Proposed System: In existing system to overcome that problem, server will maintain a common database.So as a hospital management first they have to register with the details. while registering time for each and every user they will generate CSP key for each and every user after that they can login with user credentials they can upload all data related to treatment and disease and how to solve that problem everything will be uploaded while uploading time server will provide a security for that file by using of AES algorithm so file be stored in database. So the same content can view each and every user if the person is related to that account server.So if they need the solution about that disease they can select that disease and send the request for that explanation file, then that file request will go to the concern hospital. If the hospital accept that request then only that user can get that file and file key ,if that hospital need to access that file they have to enter that user CSP key ,it will authenticate if it was correct or not. If it was confirm then they will ask the file key if two keys was correct then file as a user they can download.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 3, March 2020

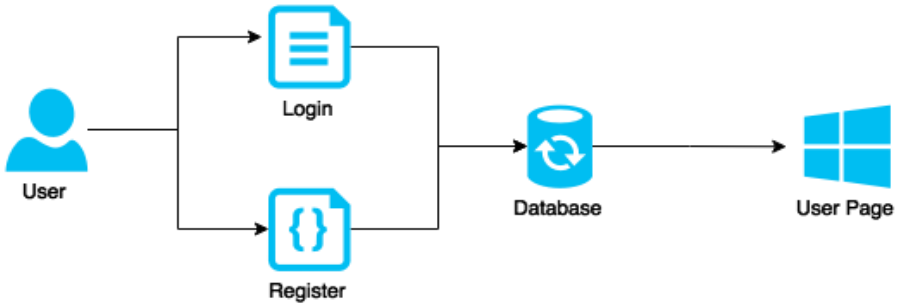


IV. MODULES

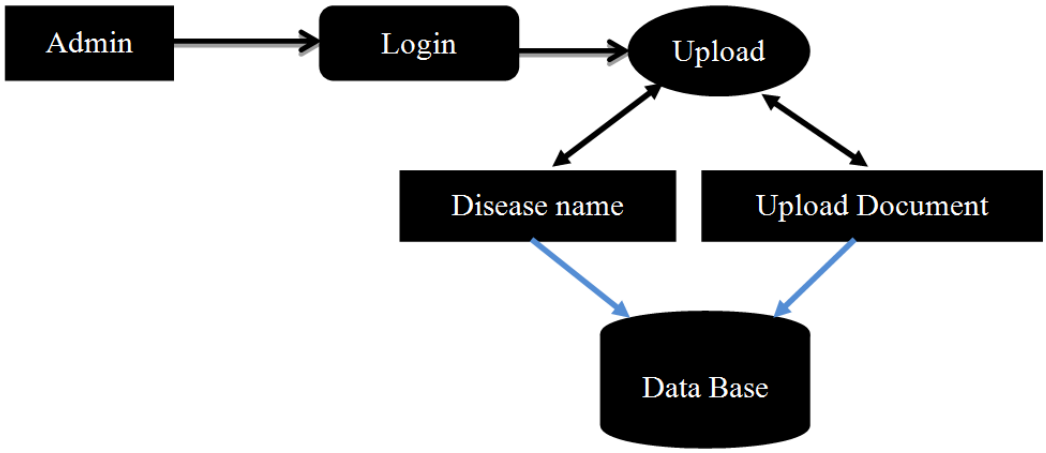
1. Register and login.
2. Treatment upload.
3.Search new treatment.
4. Blockchain document request.
5. Blockchain document download

1. Register and login

Here a as hospital management they have to register in one account under the database concord while registering time it self automatically for each and every user they can get one private key automatically it will generate. That Csp for each and every user they have a separate Csp key will generate automatically by using random key generation.



2. Treatment Upload:



IJARCCE

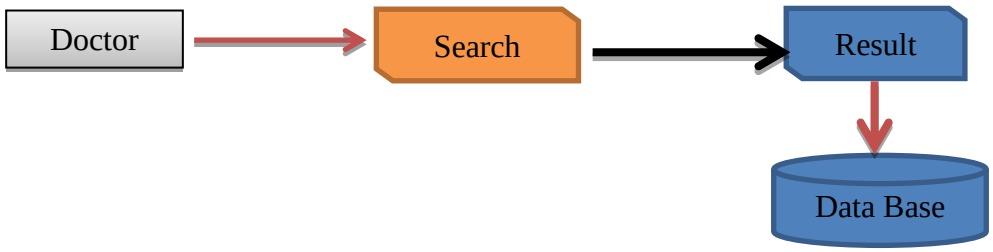
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

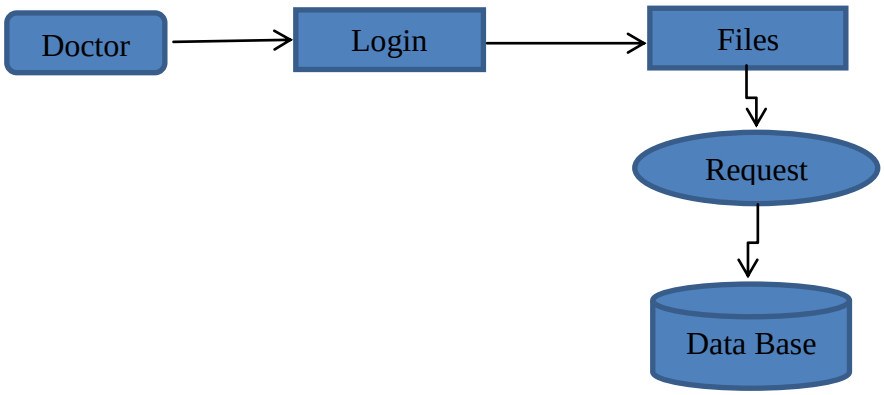
Vol. 9, Issue 3, March 2020

After register that account as a doctor they have to login with that user credentials. after login that in that particular hospital they have some of the expert senior doctors will be there so they have an idea so depends on new decease they will make that all process how to solve that problem they will make that all process in one document and they will upload that date while uploading time that content will encrypt and for that private will generate. All these in formation will stores in database.

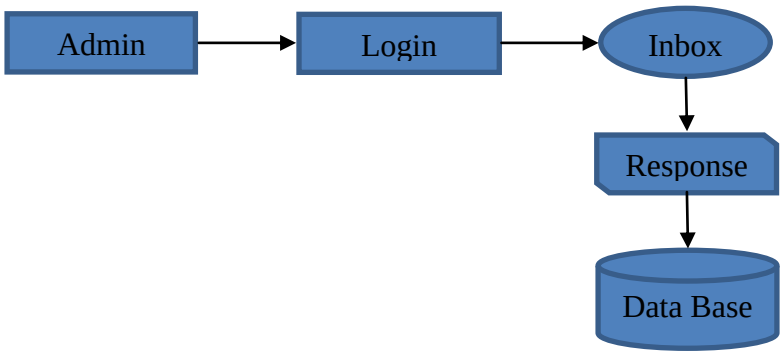
3. Search new treatment: As a doctor they can login and if they need any treatment document they can able to view that disease about all hospital data.



4. Blockchain document request: After searching the doctor result if they need that document to view they have to send that request that request will pass related to file owner.



5. Blockchain document download: After getting that file view request depends on hospital if they accept that request they can get that file and public key to that user those who send that file view request. If they need to access that file first they have to enter that user CSP key if it was authenticated correctly then it will ask enter your file view key if both was correct then only they can able to view that document.



V. SYSTEM TECHNIQUE

AES ALGORITHM:

AES is an iterative rather than feistily cipher. It is based on 'substitution–permutation network'. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations). Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix − Unlike DES, the number of rounds in AES is variable and depends on the length of the key.

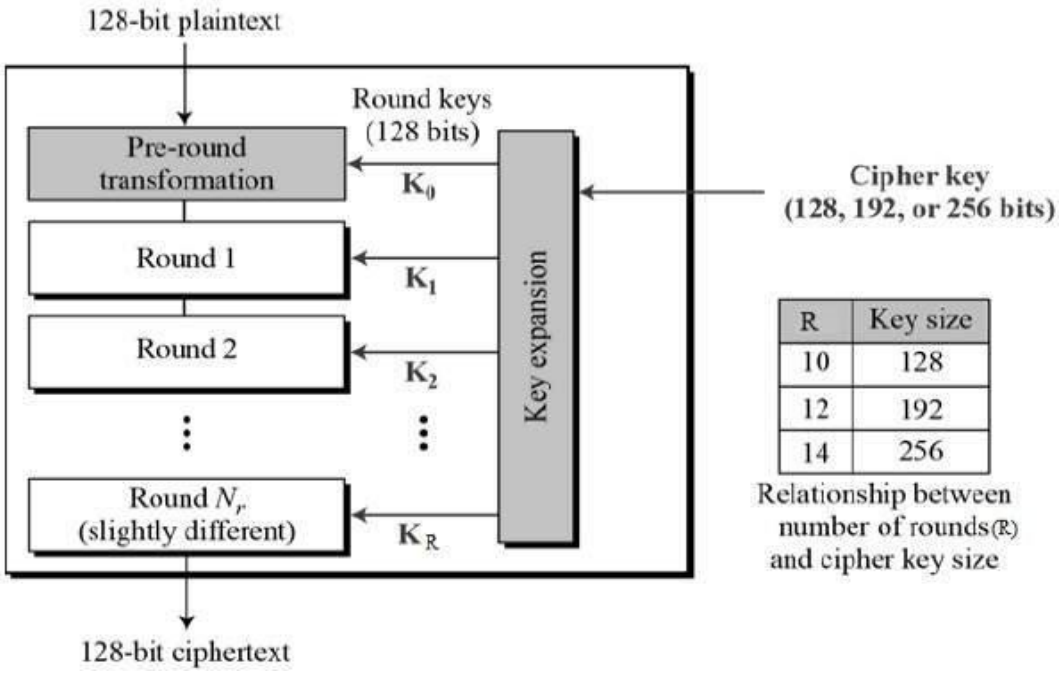
IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 3, March 2020

AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.



R	Key size
10	128
12	192
14	256

Relationship between number of rounds(R) and cipher key size

VI. APPLICATIONS

This method is used in the fields of
1. Hospitals
2. Industries and companies
3. Bank transaction
4. Educational universities for transferring of secured data.

VII. CONLUSION

From the process, the data is transferred between the hospitals, the treatment details and all data in a secured manner using the keys in a cryptographic way using the blockchain.

REFERENCES

[1]. M. Steward, "Electronic Medical Records," *Journal of Legal Medicine*, vol. 26, no. 4, 2005, pp. 491–506.
[2]. R. Hauxe, "Health Information Systems—Past, Present, Future," *Int'l Journal of Medical Informatics*, vol. 75, no. 3–4, 2006, pp. 268–281.
[3]. K. Häyrinena et al., "Definition, Structure, Content, Use and Impacts of Electronic Health Records: A Review of the Research Literature," *Int'l Journal of Medical Informatics*, vol. 77, no. 5, 2008, pp. 291–304.
[4]. M. Ciampi et al., "A Federated Interoperability Architecture for Health Information Systems," *Int'l Journal of Internet Protocol Technology*, vol. 7, no. 4, 2013, pp. 189–202.
[5]. M. Moharra et al., "Implementation of a Cross-Border Health Service: Physician and Pharmacists' Opinions from the epSOS Project," *Family Practice*, vol. 32, no. 5, 2015, pp. 564–567.
[6]. S.H. Han et al., "Implementation of Medical Information Exchange System Based on EHR Standard," *Healthcare Informatics Research*, vol. 16, no. 4, 2010, pp. 281–289.
[7]. D. He et al., "A Provably-Secure Cross-Domain Handshake Scheme with Symptoms- Matching for Mobile Healthcare Social Network," *IEEE Transactions on Dependable and Secure Computing*, vol. PP, no. 99, 2016; doi.org/DOI: 10.1109/TDSC.2016.2596286.
[8]. F.Y. Leu et al., "A Smartphone-Based Wearable Sensors for Monitoring Real-Time Physiological Data," *Computers and Electrical Engineering*, 2017.
[9]. M. Memon et al., "Ambient Assisted Living Healthcare Frameworks, Platforms, Standards, and Quality Attributes," *Sensors*, vol. 14, no. 3, 2014, pp. 4312–4341.
[10]. P.C. Tang et al., "Personal Health Records: Definitions, Benefits, and Strategies for Overcoming Barriers to Adoption," *Journal of the American Medical Informatics Assoc.*, vol. 13, no. 2, 2006, pp. 121–126.
[11]. S. Marceglia et al., "A Standards-Based Architecture Proposal for Integrating Patient Health Apps to Electronic Health Record Systems," *Applied Clinical Informatics*, vol. 6, no. 3, 2015, pp. 488–505