International Journal Of Multidisciplinary Research In Science, Engineering and Technology (IJMRSET)

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 4.988

| Volume 4, Issue 4, April 2021 |

Secure Personal Health Record Management System with Blockchain

DR.W.Gracy Theresa M.E.Ph.d., Keerthika.G, Elakkiya.P, Ramadevi.M

Assistant professor, Department of CSE, Panimalar Institute of Technology, Chennai, India

Student, Department of CSE, Panimalar Institute of Technology, Chennai, India

ABSTRACT: Data security refers to the process of protecting data from unauthorized access and data corruption throughout its lifecycle. Data security includes data encryption, hashing, tokenization, and key management practices that protect data across all applications and platforms. The security system used nowadays uses data encryption software to effectively enhance data security by using an algorithm (called a cipher) and an encryption key to turn normal text into encrypted ciphertext. To an unauthorized person, the cipher data will be unreadable. That data can then be decrypted only by a user with an authorized key. Whereas with the improving data insecurity nowadays leads to loss of confidential data as the key is easily hackable because of a single algorithm usage. To overcome this problem this project presents a medical application that accepts and analyses a patient's medical data to give a diagnosis to check if he/she is diabetic with an efficient data security system where two security algorithms will be merged to secure the patient's medical data stored and accessed in cloud. In this project logistic regression algorithm, a regression machine learning algorithm is used to process the entered patient's medical data and to predict if the patient is diabetic or normal. A web application using react java script developed from which the patient's medical data which will be encrypted using the hybrid secure algorithms before being uploaded to the database. In addition, the emerging block chain technology with the wireless data transfer system, makes easy the interaction between the data and cloud. The medical data is analyzed and the result is stored securely in a cloud database such as Mongo DB as a highly secure encrypted key. The result is received from the database and decrypted in the frontend to view the test results. Thus, this project presents an effective end to end security for medical application.

I. INTRODUCTION

The main purpose of the project is to secure particular health related information such as medical prescription, progress notes, lab reports etc. Data security refers to the process of protecting data from unauthorized access and data corruption throughout its lifecycle. Data security includes data encryption, hashing, tokenization, and key management practices that protect data across all applications and platforms. Organizations around the globe are investing heavily in information technology (IT) cyber security capabilities to protect their critical assets. Whether an enterprise needs to protect a brand, intellectual capital, and customer information or provide controls for critical infrastructure, the means for incident detection and response to protecting. The medical history of a patient will be efficiently accessible to the consulting medical care provider whenever it is needed it cannot be accessed to unauthorized users. The data is locked and stored in cloud. The data stored in the cloud provided a URL where we can access the data whenever it is needed. To develop the web application, react java script is used react java script is an updated version of java script.it is used to develop web application because it is more interactive and it is light weighted and easily refreshed. The required data in the website will be a raw data to convert it as an online data format use JSON format. Then JSON is converted into java web token encryption is used here to secure the data. Crypto AES algorithm used to convert the token in to cipher text then cipher text to hash conversion using SHA-256 algorithm. Node API create the request and it is developed by using node JS it defines the interaction between multiple software intermediaries. whenever the medical data is requested, then the key is received from the database and decrypted using in the frontend to view the original medical data.

II.DISCUSSION

The working of the total model from the above diagram can be explained as follows. the medical data to be secured is given through a web application which is converted to the JSON format, that is to be secured and encrypted is first converted to a token using a HS-256 algorithm, with an inbuilt secret key. this token is then encrypted to a cipher text using a crypto AES algorithm, with an inbuilt secret key. These two secret keys from the JWT and crypto AES algorithm are converted to a hash key using a blockchain algorithm SHA-256 algorithm. the hash key is then embedded with the cipher text which is nothing but the end output of the encryption process. This medical data is sent from a react

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 4.988

| Volume 4, Issue 4, April 2021 |

java script web application to a MongoDB database through API which is developed using node java script. A machine learning algorithm logistic regression is used to predict if the patient is diabetic or normal based on the input medical data. The data secured through block chain can never be decrypted it can only be encrypted using the hash key of another number of a network.

JWT generation, JWT to cipher generation, Merging of Cipher and SHA-256, Node API Generation, Database integration, Web development JSON Web Token is an Internet standard for creating data with optional signature and/or optional encryption whose payload holds JSON that asserts some number of claims. The tokens are signed either using a private secret or a public/private key. The tokens can be signed by one party's private key (usually the server's) so that party can subsequently verify the token is legitimate. If the other party, by some suitable and trustworthy means, is in possession of the corresponding public key, they too are able to verify the token's legitimacy. The tokens are designed to be compact, URL-safe, and usable especially in a web browser single-sign-on (SSO) context. JWT claims can typically be used to pass identity of authenticated users between an identity provider and a service provider, or any other type of claims as required by business processes. JWT relies on other JSON-based standards: JSON Web Signature and JSON Web Encryption.

The Advanced Encryption Standard (AES) is a symmetric block cipher chosen by the U.S. government to protect classified information. AES is implemented in software and hardware throughout the world to encrypt sensitive data. It is essential for government computer security, cybersecurity and electronic data protection. AES includes three block ciphers: AES-128, AES-192 and AES-256.AES-128 uses a 128-bit key length to encrypt and decrypt a block of messages, while AES-192 uses a 192-bit key length and AES- 256 a 256-bit key length to encrypt and decrypt messages. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128, 192 and 256 bits, respectively. AES is used widely for protecting data at rest.

Merging of cipher and SHA 256: The SHA-256 algorithm is one favor of SHA-2 (Secure Hash Algorithm 2), which was created by the National Security Agency in 2001 as a successor to SHA-1. SHA-256 is a patented cryptographic hash function that outputs a value that is 256 bits long. What is hashing? In encryption, data is transformed into a secure format that is unreadable unless the recipient has a key. In its encrypted form, the data may be of unlimited size, often just as long as when unencrypted. For example, a 512- bit string of data would be transformed into a 256- bit string through SHA-256 hashing. In cryptographic hashing, the hashed data is modified in a way that makes it completely unreadable. It would be virtually impossible to convert the 256-bit hash mentioned above back to its original 512-bit form. So why would you want to create a scrambled message that can't be recovered? The most common reason is to verify the content of data that must be kept secret. For example, hashing is used to verify the integrity of secure messages and files.

Node API generation: In this project node java script is used for API generation. An application programming interface (API) is a computing interface which defines interactions between multiple software intermediaries. It defines the kinds of calls or requests that can be made, how to make them, the data formats that should be used, the conventions to follow, etc. An application programming interface (API) is a computing interface which defines interactions between multiple software intermediaries. It defines the kinds of calls or requests that can be made, how to make them, the data formats that should be used, the conventions to follow, etc.

NodeJS is an open-source, cross-platform, back-end, JavaScript runtime environment that executes JavaScript code outside a web browser. NodeJS lets developers use JavaScript to write command line tools and for server-side scripting—running scripts server-side to produce dynamic web page content before the page is sent to the user's web browser. Consequently, NodeJS represents a "JavaScript everywhere" paradigm, unifying web-application development around a single programming language, rather than different languages for server- and client-side scripts. NodeJS allows the creation of Web servers and networking tools using JavaScript and a collection of "modules" that handle various core functionalities. Modules are provided for file system I/O, networking (DNS, HTTP, TCP, TLS or UDP), binary data (buffers), cryptography functions, data streams, and other core functions. NodeJS modules use an API designed to reduce the complexity of writing server applications.

Database integration: In this project MongoDB is used for database integration. MongoDB is a cross- platform, document-oriented database that provides, high performance, high availability, and easy scalability. MongoDB works on concept of collection and document. Database is a physical container for collections. Each database gets its own set of files on the file system. A single MongoDB server typically has multiple databases. Collection is a group of MongoDB documents. It is the equivalent of an RDBMS table. A collection exists within a single database. Collections

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 4.988

| Volume 4, Issue 4, April 2021 |

do not enforce a schema. Documents within a collection can have different fields. Typically, all documents in a collection are of similar or related purpose. Document A document is a set of key-value pairs. Documents have dynamic schema. Dynamic schema means that documents in the same collection do not need to have the same set of fields or structure, and common fields in a collection's documents may hold different types of data.

ReactJS is JavaScript library used for building reusable UI components. According to React official documentation, following is the definition − React is a library for building composable user interfaces. It encourages the creation of reusable UI components, which present data that changes over time. Lots of people use React as the V in MVC. React abstracts away the DOM from you, offering a simpler programming model and better performance. React can also render on the server using Node, and it can power native apps using React Native. React implements one-way reactive data flow, which reduces the boilerplate and is easier to reason about than traditional data binding. JSX stands for JavaScript XML. JSX allows us to write HTML in React. JSX makes it easier to write and add HTML in React. It is faster than normal JavaScript as it performs optimizations while translating to regular JavaScript.

It makes easier for us to create templates. Instead of separating the marks up and logic in separated files, react uses components for this purpose. We will learn about components in details in further articles. Components are independent and reusable bits of code. They serve the same purpose as JavaScript functions, but work in isolation and returns HTML via a render function. Components come in two types, Class components and Function components, in this tutorial we will concentrate on Class components. Unidirectional data flow and Flux React implements one-way data flow which makes it easy to reason about your app. Flux is a pattern that helps keeping your data unidirectional.

III.CONCLUTION

This project is used to provide a solution to perform securely transmit data through a wireless communication medium using a web application developed using a java script framework react JS. By this project, we can protect data from unauthorized access. Thus, this project provides an affordable and efficient means to protect and preserve data.
In the coming future, we review the application of the project to determine technology in the fields that require data security and privacy. In the banking and medical field, they are more chance to develop or convert this project in many ways. Thus, this project has an efficient scope in coming future where data can be transmitted securely over a wireless communication.

REFERENCES

1. Jun Shang, Maoyin Chen, Member, IEEE, and Tongwen Chen, Fellow, IEEE,“Optimal Linear Encryption Against Stealthy Attacks on Remote State Estimation” ,[2020]
2. Novel Hybrid CMOS/Memristor Implementation of the AES Algorithm Robust against Differential Power Analysis Attack, Massoud Masoumi,[2019]
3. An Enhancement of Data Encryption Standards Algorithm (DES), Nadia Mustafa Mohammed Alhag University of Gezira Faculty of Mathematical Sciences and Computer Medani,[2018]
4. Ensuring Data Security in Databases Using Format Preserving Encryption, Shikha Gupta1 , Satbir Jain3 Computer Engineering NSIT New Delhi, India,[2017]
5. Enabling Authorized Encrypted Search for Multi-Authority Medical Databases,Lei Xu, Shifeng Sun, Xingliang Yuan, Joseph K. Liu, Cong Zuo, Chungen Xu*[2016]
6. Chained Compressed Sensing: A Block-Chain- inspired Approach for Low-cost Security in IoT Sensing, Mauro Mangia, Alex Marchioni, Fabio Pareschi, \Riccardo Rovatti, Fellow, IEEE,Gianluca Setti, Fellow, IEEE, 2019
7. J. S. Ancker, M. Silver, and R. Kaushal, ‘‘Rapid growth in use of personal health records in new york, 2012–2013,’’ *J. Gen. Internal Med.*, vol. 29, no. 6, pp. 850–854, Jun. 2014.
8. Health Records—Apple. Accessed: Mar. 16, 2020]. [Online]. (Available:https://www.apple.com/healthcare/health-records/
9. Bhardwaj, S. B. H. Shah, A. Shankar, M. Alazab, M. Kumar, and T. R. Gadekallu, ‘‘Penetration testing framework for smart contract blockchain,’’ Peer-to-Peer Netw. Appl., pp. 1–16, Sep. 2020, doi: 10.1007/s12083- 020-00991-6.
10. Y. Sharma and B. Balamurugan, ‘‘Preserving the privacy of electronic health records using blockchain,’’ Procedia Comput. Sci., vol. 173, pp. 171–180, Jan. 2020.
11. M. Qazi, D. Kulkarni, and M. Nagori, ‘‘Proof of authenticity-based electronic medical records storage on blockchain,’’ in Smart Trends in Computing and Communications. Singapore: Springer, 2019, pp. 297–306
12. T.McGhin, K.-K.R.Choo,C.Z.Liu,andD.He,‘‘Blockchain in healthcare applications: Research challenges and opportunities,’’ *J.Netw. Comput. Appl.*, vol. 135, pp. 62–75, Jun. 2019. [Online].
13. Available: http://www. sciencedirect.com/science/article/pii/S108480451930 0864