IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 6, June 2022

DOI: 10.17148/IJARCCE.2022.11627

Block Chain based Health-Care System

Bhavana Ramdas Pendor[1], Ashish B. Deharkar[2], Neehal B. Jiwane[3]

Student, Computer Science & Engineering, Shri Sai College of Engineering & Technology, Bhadrawati, India[1]

Asst.Prof, Computer Science & Engineering, Shri Sai College of Engineering & Technology, Bhadrawati, India[2]

Asst.Prof, Computer Science & Engineering, Shri Sai College of Engineering & Technology, Bhadrawati, India[3]

Abstract: As we can see in today's generation the hospital records and data are stored more in the cloud. As well as the data of the patient needs to saved more securely. The security of the data and the information security is the basic important in most of the organization , even in the home computer user, client data, data of payment, documents and account details. This data are difficult to change, or it may be difficult to replace, and it becomes danger, if it goes to the wrong hand. The gathered information which are lost due to the flood, fire is a type of crushing but loosing of data by the hacker can have significantly more net worth result. In other word we can say that when the block is completed , It creates a secure code ,In this system the data will be of the health care system, and it needs to secure this work is being designed by the help of blockchain concept key based cryptographic technique it works on the storing data of the health care, and it is stored on the web that stored data of the health care should be in the secure mode.

Keywords: Block-chain technology, ledger, cryptography, hashing, healthcare system storage data.

I. INTRODUCTION

A block is defined as the distributed system in which the records and transaction are being stored , it is specifically defined as " a shared immutable record of peer to per transaction", that is built from the linked transaction blocks and are stored in a digital ledger. It is similar to database which store the information the main difference is that the data is stored in the network of the personal computer called nodes, Where there is no central authority as government rest all the data is shared publicly, and the data is only accessible from there permission. In the figure below it illustrate that how the information is stored in the distributed network as compare to centralized and decentralized network. Each of the participant is basically connected to the blockchain, and they have a secret and private key and also the public key that acts as the visible identifier. The pair of cryptography is linked in such a way that the identity is possible in the one direction only by using the private key , In order to unlock the participant identity to uncover what is the information in the blockchain is relevant to their profile. As now the world has come to know about the blockchain concept before nine year back Satoshi Nakamoto conceptualized it in 2008 it got developed in a year using the Bitcoin , a crypto, currency and digital payment system .This concept discoursing to distributed ledger the blockchain to verify and share transactions without cryptocurrency. The term blockchain is used to represent descriptive technology for the industries and the health to finance. Blockchain is divided of the database of records of public ledger events or transaction which has got executed and shared among the involving , blockchain is a public ledger residing of order it also a path of recording data and transaction digitally. The record are connected to an individually blocks that is connected to chronologically in a chain.

II. MOTIVATION

The blockchain is the emerging technology for the transaction and the distributed system which share data across a large network of untrusted participant. As today the health care data is increasing rapidly. The individual patient is more important, so it should in a secure mode and can be accessible form anywhere. The need is to store the data very securely by the blockchain , As the database is more tangible thing consisting of bits and bytes. If we try to store any content in the database of the physical memory in a particular system any of them who has access to the system could corrupt the data. With the help of blockchain there is no need of the central authority eliminated by the cryptography. Since the health care system deals with the confidential patient information, and it requires quick access to the information and because of the blockchain the medical records enables their sharing securely. It may be a global journey where blockchain is being implemented step by step.

III. REVIEW OF LITERATURE

R.Alvaro-Hermana, J. Fraile-Ardanuy, P. J. Zufiria, L. Knapen, and D. Janssens they proposed the concept of the two electrical vehicles which diminish the charging procedure on the power framework and business hours. This approach is also beneficially for all the economical users involved in this process. The activity approach is used to predict the daily

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 6, June 2022

DOI: 10.17148/IJARCCE.2022.11627

trips of the population for Flanders(Belgium)[1]

Y. Xiao, D. Niyato, P. Wang, and Z. They provide a study of the possible functional factors that enables DET in communication network. Their are various design issue how to implement DET in practice are discussed. An approach is created to delay tolerant remote controlled to the correspondence organizes in which the remote device can masterminded its information and transmit the energy exchange activites[2].

J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain present the work to request the reaction giving the motivating forces to releasing PHEVs adjust the nearby power request for their own self interests. Since exchange of security and security insurance show genuine difficulties they investigate a promising consortium block chain innovation to exchange the security without dependence on a confided in outsider. Trading framework with consortium block chain strategy has proposed to represent detailed activity [3].

N. Z. Aitzhan and D. Svetinovic present a work which address the issue of providing security of the transaction in decentralized smart grid energy trading without confident over the third parties. The proof of the decentralized energy trading system using the block chain technology multi signatures, encrypted flows of message, securely perform trading transcation [4].

I. Alqassem et al present a work that Bit-Coins is constantly improved by open source network and different BIT- coinslibraries, APIs, are being created [5].

IV. PROPOSED WORK

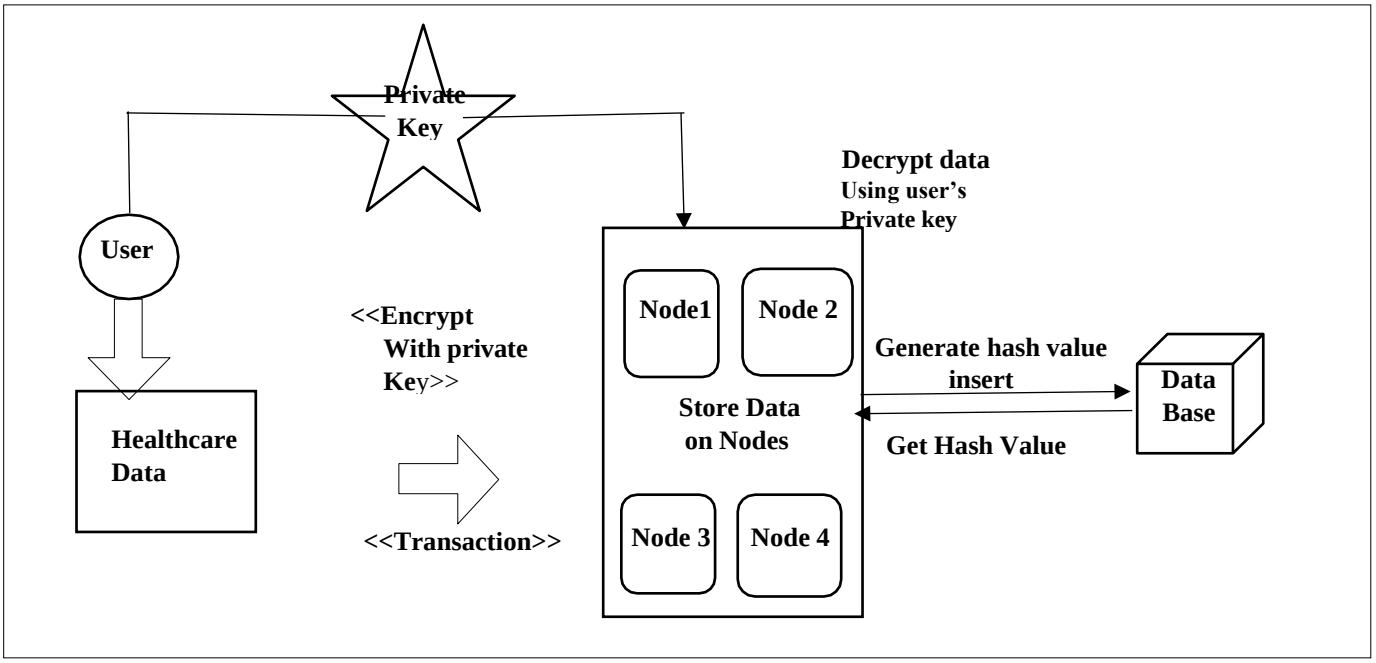

Fig. 1. Proposed system architecture

V. SYSTEM OVERVIEW

Data forms foundation of the application system, Its integrity is the key to the data value it aims the data security technology prevention. According to the approach of the cryptography , digital signature generate the set of data information representing the identity. The user validate the digital signature through the public key of the user for verification of the authenticity and integrity of the data information. The main motive of the using the private key based cryptography technique is for users to verify the origin of the data information.

For the security of the data , the proposed work is designed using the block chain concept and key based digital signature technology. In this proposed work we store the hash table of raw data and also the file on the blockchain, It validates other copies by running a hashing technique, than checks the data has been stored in blockchain if there is any interface with the data it will be quickly found because the original hash tables are stored in the millions of the nodes. In this system admin head will store user data securely by applying encryption and then the doctors can get the data.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 6, June 2022

DOI: 10.17148/IJARCCE.2022.11627

VI. ALGORITHM

Algorithm1 : Advance Encryption Standard.Encryption:
step 1:128 bit data blockstep 2-key expansion step3: add round key
step4:sub byte ,shift row,mix columns ,add round key
step5:sub byte ,shift rows, add round keystep6-128 but encrypted block Decryption:
step1-128 but encrypted blockstep2-key expansion
step3-add round keys ,shift rows,subbytes
step4-add round keys ,mix columns, shift rows ,sub bytesstep5-add round key
step6-128 bit block
Algorihtm2 : SHA-1(Secure Hash Algorithm1).
In cryptography, SHA-1 (Secure Hash Algorithm 1) could be a cryptographic hash function which takes an input and produces a 160-bit (20-byte) hash value called a message digest – typically rendered as a hexadecimal number, 40 digits long. Secure Hashing Algorithms, also called SHA, are a family of cryptographic functions designed to stay data secured. It works by transforming the info employing a hash function: an algorithm that consists of bitwise operations, modular additions, and compression functions The hash function then produces a hard and fast size string that appears just like the original size. These algorithms are designed to be one-way functions, meaning that when they're transformed into their respective hash values, its virtually impossible to rework them into the first data. a standard application of SHA is to encrypting passwords, because the server side only must keep track of specific users hash value, instead of the particular password.

VII. CONCLUSION

In work is meant using block chain concept and key-based cryptographic technique which estimate the protection of block-chains specifically using hashing. Proposed system work to security on healthcare data. Block-chain technology isn't just an application technology for new-generation transactions. It creates trust, responsibility and transparency while simplifying business processes. This approach allows users to authenticate the information access through the general public and personal key of user sources, while improving network access performance by locally authenticating keys supported block-chain copies and its hash values this work is intended using block chain concept and key-based cryptographic technology to supply the protection to healthcare data of patient.

VIII. REFERENCE

[1]. Lowlesh Nandkishor Yadav “Predictive Acknowledgement using TRE System to reduce cost and Bandwidth” Factor 7.39 Vol. 11, Issue 3, March 2022.
[2]. Ashish B Deharkar “An Approach To Reducing Cloud Cost And Bandwidth Using Tre System”.
[3]. 1.R. Alvaro-Hermana, J. Fraile-Ardanuy, P. J. Zufiria, L. Knapen, and D. Janssens, “Peer to peer energy trading with electric vehicles,” IEEEIntell. Transp. Syst. Mag., vol. 8, no., pp. 33–44, Fall 2016.
[4]. Y. Xiao, D. Niyato, P. Wang, and Z. Han, “Dynamic energy trading for wireless powered communication networks,” IEEE Commun. Mag., vol. 54, no. 11, pp. 158–164, Nov. 2016.
[5]. S. Barber et al, “Bitter to better-how to make bitcoin a better currency,” in Proc. Int. Conf. Financial Cryptography Data Security, 2012, pp. 399–414.