International Journal of Scientific Research & Engineering Trends
Volume 7, Issue 4, July-Aug-2021, ISSN (Online): 2395-566X

A Review on Block Chain in Cloud Computing Healthcare Data Security

M.Tech. Student Atul Soni, Asst. Prof. Manoj Kumar Gupta
Department of Computer Science and Engineering
Sagar institute of research and Technology College,
Sage University, Indore,MP,India
atulsoni19101997@gmail.com, manoj.gupta.ietdavv@gmail.com

***Abstract*- Cloud service providers may maintain all patient records and provide users with access to data. Cloud service providers can view all documents uploaded and downloaded to the cloud. The CSP checks for authentication before the data user receives a document request and authorizes it. Next, the CSP executes the query and returns an encrypted document based on the search token. It also returns additional certifications along with your documents to confirm your search results. After creating the block, the healthcare provider uploads the record to the cloud. If you want to search for records in the cloud, first assume that your healthcare provider searches for records. Results are displayed based on the search. After obtaining approval and key from the cloud service provider, healthcare providers can download the data.**

***Keywords*- AES, Encryption, Descryption, Cloud Computing, Block Chain.**

I. INTRODUCTION

Cloud computing is a evolving cloud model that retains cloud information with new aspects and capabilities. In order to keep cloud server safe data, numerous techniques and approaches are available. Cloud computing is subject to numerous attacks and can be secured with security-related methods and techniques [12]. A standard network protocol accessible from every connected device (such as computers, mobile phones or tablets) provides cloud service all over the world.[13]

Cloud computing security is based on the authentication and testing of certain parameters that can help in the right data security measurements in the cloud server. Biometry technology provides identity checks and a delicate level of safety, while key management for key storage in cryptography is needed.Two phases of network analysis are the start and disappointment to detect the stream of network traffic; biometric data is secured using secret key sharing between encryption and decryption parties. The original biometric information is extracted by a key. The cryptography key is completely biometric independent.

Biometrics may more efficiently secure the pass code [9] and authenticate the individual unique in providing access by fingerprint scanner technology to the computer or system. An evolutionary internal protocol is essential for the Block chain. It is an asymmetric and distributed architecture for open source cryptography. Many aspects of technology can be found in the chain of blocks peer-to-peer technology, cryptography [10] distributed over a network. Block chain technology differs entirely from the traditional structure of databases. Peer to peer network that collectively has carried out the block chain by protocol to communicate inner node and to authenticate new nodes. Each block is distributed via a network with a valid transaction. This technology for block chains uses a script to deal with the system's sudden pattern transaction. Three technologies are composed of private, peer-to-peer, and block-chain protocol key cryptography. The block chain is merely an encrypted data list [11].

The main benefit of block chain technology is that data can be dispersed itself. The block chain is subject to many third-party attacks to access cloud-based files [14] and can be prevented through the use of technologies and the blocking of the security chain to protect data from theft. This paper discusses encryption key together with block chain technology to help secure biometric data in the cloud server. Bigger rblockchains user with more copies of a network cryptography key and block-chain technology have a less risk of being attacked by the hacker due to the large number of difficulty in breaking such a data secure on the cloud server.

II. RELATED WORK

Bio-cryptography ensures data through cloud server encryption and decryption. Since the security of encryption keys is weak in order to remember pass codes, there must be a method for more accurate data protection. Not secure for encryption keys. This process is concerned with many privacy issues, so a technique is needed to fully protect the cloud server.

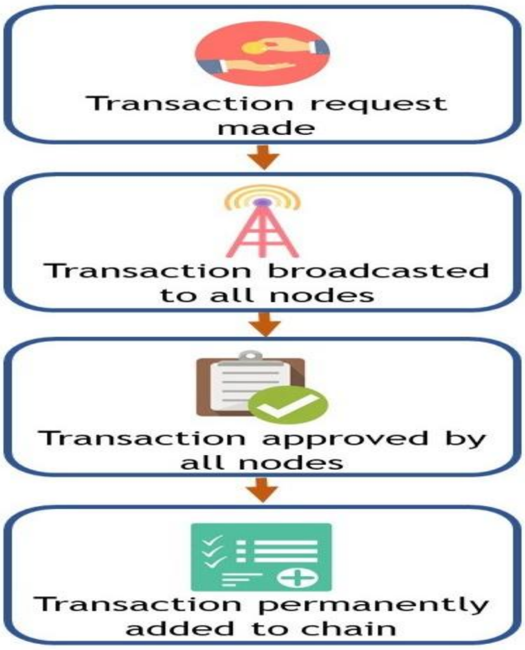
Transaction request made
Transaction broadcasted to all nodes
Transaction approved by all nodes
Transaction permanently added to chain

Fig 1. A generalized workflow of the block chain process.

In the future, the block chain can be a technology that can potentially contribute to personalized, reliable and secure healthcare, by combining the whole clinical data on a patient's health in a given real time and presenting it in the future as a secure and current health system. Background information and related healthcare work using block chain as a tool a short overview.

Describes various applications of the emerging health and medical blockchain technology. Presents health care and medical challenges when using block chains. Highlights the blockchain technology's future perspectives in the health field. Section 6 describes the conclusion, followed by the sections.

1. Blockchain Technology:
Blockchain offers a dispersed, complete user-wide information warehouse. It is a distributed database that promotes an ever-increasing roster of business data records that are cryptographically shielded from interference and review. The transaction data is stored in the loop of the bank. The block chain comprises of three first components for data storage, the second one as a hash value that operates as a fingerprint and is always special in identifying the block. The method of incorporating fresh block by hash checking operation to block the loop is called mining. The fresh block inserted is connected to the earlier block. The final component is preceding block hash is block chain to render blockchain safer.

The primary drawback of the block chain is the elevated consumption of equipment, power and moment needed for the mining process. Blockchain has emerged from a technology with small digital currency-related apps. To safeguard against attackers, the safety in blockchain is essential. The details were protected and

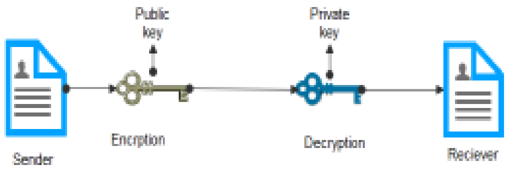

Fig 2. Block Chain Process.

2. Block:
The block in the block chain is the blockchain's main core. A request record registered over a specified moment in a survey. The occurrence of magnitude and application is distinct from blockchain indefinitely. The block chain regulates their token's motion. The block header contains the last hash, transaction, time, target and version of the blockchain that describes the data structure. When a block is finished, a unique safe file is created, which is linked to the next block kept in the cloud server by blockchain.

The information is placed in the block forming circuits. The information is handled to suit into a row and each unit is represented by using generally recognized as digital fingerprint cryptographic hash. The feeling of the block chain is analyzed when fundamental cryptographic algorithms are breached. Below is the blockchain framework.

The blockchain is the cryptographic protocol comprising it; every block chain technology is a variable in meeting the demands. For the security of the block chain, the security of cryptographic hash functions is essential and its nature should be secure for a very long time. The block chain technology used information pieces to hold the information in it and by chaining them.

III. LITERATURE SURVEY

Christian Esposito One trend noticed in healthcare is that data and services are progressively shifted into the cloud partly because of comfort (e.g. the availability in real-time of a complete patient history) and savings (e.g. healthcare management economic data). There are, however, restrictions on the use of standard cryptographic primitives and access control designs to tackle safety and privacy issues in an increasingly cloud-based setting. This article explores the possibilities of using Block Chain technology to safeguard health information stored in the cloud. We also outline the practical difficulties of such a proposal and further study that is needed.

Healthcare is a data-intensive sector that produces large amounts of data, distributes, saves and accesses every day. For instance, when patients are tested (e.g. computer tomography or axial tomography scans), the data are produced and the data is distributed to the radiation system and the medicineThe visit results will be stored in a hospital, which may be accessible at a future date by a Doctor in another hospital in the network. It is clear that technology can contribute greatly to improved patient care performance (i.e. leveraging data analytics to generate educated medical decisions) and may reduce expenditure by allocating more resources in respect of employees, equipment, etc.

Zulqarnain Rashid Now the health sector is growing tremendously in a day as the elderly population is growing and the childbirth rate is falling. The absence of medical doctors has made health care a major problem. Due to these problems, a paradigm change is being made from need-based health surveillance to preventive health surveillance. With this in mind, we have created a Ubiquitous Health System that enables consumers preserve their wellness and protects customers from becoming ill. Web services communicate with different parts of the scheme. Web facilities help users to keep their health records remotely and have access to health parameters worldwide. Feedback and advice are also given through the use of a web service. These services are designed to be supplied by the cloud service as well as the main database which is also available on the cloud service.

Unnati Dhanaliya Enhanced health care systems are needed for any country's economic, technological and social development. The development of the health care system requires no workforce, particularly if a patient requires continuous monitoring. The power of ICT has given an efficient and efficient healthcare system alternative person can be remotely supervised and controlled using the Internet of Things (IoT) system. In this document, we introduce e-health care through cloud computation and web-based facilities. Remote monitoring and control is created feasible with cloud computing. It provides automatic update of measured parameter of patient as well as it sends alert mail by using SMTP (Simple Mail Transfer Protocol).

Nimmy John The health care sector has gone a long way since the introduction in health care of IT since computerized operations and virtual patient service, from more than just Hospital Information Systems (HIS), the Electronic Medical Records (EMR). Increased digitality, collaboration, patient-centricity and data-driven health care in all types of economies is gone with improvements in information technology. It seeks to access data everywhere, everytime. This huge quantity of information produced and the different health care facilities to be provided for clients will no longer be possible thanks to conventional technologies infrastructure in the health industry.

Cloud computing is a rapidly expanding trend, with several facilities provided in a pay-as-you-go system on demand on the web. It vows to speed up the deployment of apps and reduce expenses. In handling the present pattern of digital data development and the accessibility of medical facilities every time, cloud computing can play a crucial part. Cloud computing can help substantially contain healthcare inclusion expenses, optimize funds and launch a fresh period of healthcare innovation. In brief, this paper analyzes some of the digital information challenges facing the health sector. The article defines a scheme that can offer multiple cloud-based health-care facilities. The document also introduces one of the services provided in the mentioned scheme.

S. R. Satheesh Cloud computing is a main resource sharing platform that involves IaaS, Saas, PaaS and company processes. This offers numerous advantages for customers to build and store cloud information using fewer customer systems funds. The scheme suggested relies primarily on the safety of health information. Researchers are constructing intelligent healthcare atmosphere in which medical information are continually tracked by health professionals in order to decrease the expense of hospitalization.

Some of the most important imports that still need to be debated before such systems are widely accepted include medical data security and privacy gathered by these instruments. Enhanced RSA is a method used as an added method in traditional RSA by random integer. The improved RSA storage safety approach utilizes distant data encryption and decryption technology to improve current RSA encryption and decryption.

The encrypted information is placed in the cloud using proven information ownership. The primary protection method is used to secure health care information to enhance privacy and safety. Better safety is achieved by the technique proposed. This technique ensures that the information from medical care are correct and that the file block is identified in the cloud. This approach also promotes information entry, change and removal and attempts to decrease server calculation time. The assaults are produced using encrypted information and the findings show that the suggested system exceeds the current techniques by improving safety in information storage to provide data security.

Cryptography is the key to the privacy of blockchain where transactions need to be confidential. Block chain's manufacturing advantages are to enhance discovery, decrease expenses and difficulty, and can be believed in maintaining record headquarters. Blockchain improves accessibility and business network effectiveness. The Block chain system was shown in Fig.

Block- The block in the block chain is the blockchain's main core. A request record registered over a specified moment in a survey. The occurrence of magnitude and application is distinct from blockchain indefinitely. The block chain regulates their token's motion. The block header contains the last hash, transaction, time, target and version of the blockchain that describes the data structure. When a block is finished, a unique safe file is created, which is linked to the next block.

IV. PROPOSED APPROCH

The information consumer outsources the encrypted files to the cloud to solve the safety issues that occur in the current scheme and efficiently distribute the information over the cloud. The data user receives every result, proof and public verification key and can check the freshness, authenticity and completeness of the results of the search without decrypting them. Provide security of cloud server data with block chain technology that allows crypto applications to perform secure data.

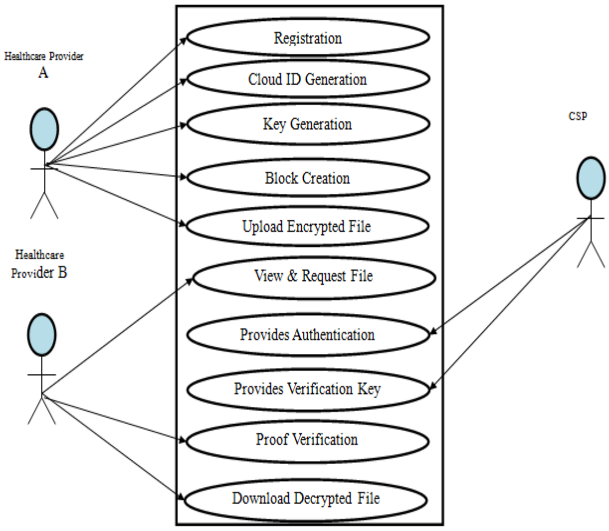

Fig 3. Proposed flow chart.

Block Chain is also an online distributed database method based on undistributed architecture, a cryptographic asymmetric component. Block chain method used advanced as data block component which holds data in the form of a text file of a paper. There are three components in the block chain, one for data storage, another for hash value, which operates like fingerprint. Cryptography is the primary component of the block chain where it is necessary to keep the operation confidential.

V. CONCLUSION

A data center for cloud computing can house information from different customers. Data evaluation can be performed to provide the amount of safety depending on the significance of information. This classification scheme should take into account different elements such as frequency of entry, frequency of updates and entry by different organizations, etc. depending on data type. Once the data is classified and tagged, it is possible to apply the level of security associated with this particular tagged data element. Security level involves confidentiality, encryption, integrity, memory, etc. chosen depending on data type.

REFERENCES

[1] Esposito ,Alfredo De Santis ,Salerno Henry Chang Kwang Raymond Choo IEEE Cloud Computing Co published by the IEEE CS and IEEE ComSoc 2325-6095/18/$33.00 ©2018 IEEE.

[2] Ahmed Adem Ms. Roshni Pradhans Fekadu Workneh; Understanding Cloud Based Health Care Service with Its Benefit2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT).

[3] Health Records Privacy Issues in Cloud Computing Mahmoud Said Elsayed Marianne A. Azer 2018 1st International Conference on Computer Applications & Information Security (ICCAIS) Year: 2018 |

[4] F.Y. Leu et al., "A Smartphone-Based Wearable Sensors for Monitoring Real-Time Physiological Data," Computers and Electrical Engineering, 2017

[5] G.S. Poh et al., "Searchable Symmetric Encryption: Designs and Challenges," ACM Computing Surveys, vol. 50, no. 3, 2017.

[6] Q. Alam et al., "A Cross Tenant Access Control (CTAC) Model for Cloud Computing: Formal Specification and Verification," IEEE Transactions on Information Forensics and Security, vol. 12, no. 6, 2017, pp. 1259–1268.

[7] January Implementation of E-health care system using web services and cloud computing Unnati Dhanaliya ; Anupam Devani 2016 International Conference on Communication and Signal Processing (ICCSP) Year: 2016 | Conference Paper | Publisher: IEEE.

[8] M. Li et al., "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption," IEEE Transactions on Parallel and Distributed Systems, vol. 8, no. 3, 2016, pp. 2084–2123.

[9] A novel cloud based hospital health care service network framework with delay sensitive handoff guarantee Xiaodan Zheng Tigang Jiang 2016 13th International Conference on Service Systems and Service Management (ICSSSM)Year: 2016 | Conference Paper | Publisher: IEEE

[10] F. Tschorsch and B. Scheuermann, "Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies," IEEE Communications Surveys & Tutorials, vol. 18, no. 3, 2016, pp. 2084–2123.

[11] A. Azaria et al., "MedRec: Using Blockchain for Medical Data Access and Permission Management,"

Proceedings of the 2nd Int'l Conference on Open and Big Data (OBD 16), 2016, pp. 25–30.

[12] J. Zhang, N. Xue, and X. Huang, "A Secure System for Pervasive Social Network Based Healthcare," IEEE Access, vol. 4, 2016, pp. 9239–9250.

[13] V. Casola et al., "Healthcare-Related Data in the Cloud: Challenges and Opportunities," IEEE Cloud Computing, vol. 3, no. 6, 2016, pp. 10–1.

[14] 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.

[15] 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.