Shielding Electronic Health Record with Attribute-Based Encryption via QR-Code on Blockchain

Akshatha D[1], A M Chandrashekhar[2]
[1,2]*Sri Jayachamarajendra College of Engineering (SJCE), JSS S&TU Campus, Mysore, Karnataka, India*

Abstract **- It is desirable to use the digital data than traditional medical records, clinical establishments experience difficult issues, for example, electronic wellbeing record stockpiling and sharing. Patients and doctors invest impressive energy questioning the necessary information while getting to electronic wellbeing records, however they got information are not really right, and access is now and again limited. To overcome this problem, we proposed medical related information sharing using blockchains, which use ciphertext-based attribute encryption to guarantee information confidentiality and access control of clinical information. QR Codes are predominantly used to pass on or store messages in light of the fact that they have higher or enormous capacity limit than some other ordinary standardized tags. So, this encryption data is stored in this QR code is perfectly secured all the time, without the information getting leaked to outside world and to more secure blockchain technology is combined. Different data users for example, insurance policy, police investigation etc., can also use this electronic record for their purposes by getting the authorization.**

Index Terms **- Attribute-based encryption, Blockchain, Data sharing, Electronic health records, QR Code.**

I.INTRODUCTION

Electronic health records (EHRs) reduce cost of the traditional medical data storage. EHRs are designed for allow patients to manage their own medical data. Data users have limited access to EHRs.

Electronic health records using an encrypted retrieval of such records must be implemented. A searchable encryption scheme has been proposed to achieve retrieval on ciphertext [2]. Searchable encryption can be symmetric or asymmetric. Symmetric searchable encryption has the higher encryption efficiency compared with the asymmetric [3], [4]; however, its private key management is more complicated during the data sharing. To solve the key management problem, Boneh et al. [5] introduced public key encryption with keyword search. Public key searchable encryption is suitable for multi-user data sharing. To achieve multi-user data sharing, [6] proposed attribute-based encryption.

Quick Response Codes utilized in the field of Cryptography. QR Codes are mostly used to pass on or store messages since they have higher or huge capacity limit than some other ordinary standardized identifications. QR Codes can be utilized for scrambled information for the receiver. This technique will be appropriate in any business house, government areas, and correspondence system to send their encoded messages quicker to the objective. Or then again an individual can even utilize this strategy to keep his significant records, similar to passport number, pan-card id, and social security number, more secure made with him all the time, without the data getting spilled to outside world [7].

With the fast improvement of the electronic wellbeing record, dispersed capacity stages have gotten the broad consideration through a system of the various stockpiling gadgets. With the increasing popularity of these storage platforms, distributed platforms that store data have become a target of cyber-attacks. To reduce the risk of data leakage,[8]and [9] proposed data storage on blockchain.

A blockchain is resistant for modify the data. Blockchain is decentralized, so it eliminates the concentration of cloud storage servers and solves the security flaws caused by the network attacks. A blockchain is created by nodes of the mining block in system, and each block contains hash function value of the previous block header. This structure makes the blockchain more difficult to tamper the data.

The QR code data is stored in the folder and that path will be specified in the database based on the blockchain concept. For more security, the file can be stored in the cloud to make bit secure and also tracking also can be done for the file.

II.RELATED WORKS

Usually, people go to hospitals when they fall ill, and they may even get admitted to hospital when there is any severe health issue. The hospital in-charge collects the basic information from the patients and records it as a file summary in the system. This data is stored in the database. Whenever there is need of these files, they retrieve it from the database. These files can be accessed by any third party, hence there is no security for these files. There should be a solution adapted to increase the security of these patient's summary files.

As of late, blockchains have got broad consideration in the field of information stockpiling, information sharing, and security insurance. Blockchain are straightforward and not altered. Subsequently, information put away in the blockchain must be encoded. Accessible encryption takes care of the hunt issue on the ciphertext. [10] Constructed a safe file utilizing blossom filter, however the list items are mostly off base.

For the issue of symmetric searchable encryption key management, Bonehet al. [5] proposed an open key accessible encryption plot. By narrowing down the pursuit through watchwords, Golle et al. [11] proposed a multi-watchword search plot, and [12], [13] and [14] proposed other multi-catchphrase accessible encryption plans with exceptional capacities, which broadened multi-watchword recovery applications. With regards to data sharing, property encryption stretches out the application situation to a one-to-numerous circumstances. Qiu et al. [15] proposed a trait accessible encryption that could oppose the inward catchphrase speculating assault, however requires the information proprietor to be online continuously, to such an extent that another information client who joins the framework arranges the pursuit key with information proprietor, and the information proprietor is significantly troubled.

Li et al. [16] proposed property encryption dependent on a key technique to actualize a solitary catchphrase accessible encryption scheme. To retrieve files efficiently Sun et al. [17] proposed a characteristic based accessible encryption conspire that bolsters client renouncement, executing expanded fine-grained search authorization, which allows owners to encrypt and redistribute their information to the cloud worker freely. Sun et al. [18] utilized idle re-encryption innovation to actualize quality renouncement.

Health bank utilizes blockchain innovation to guarantee outright information stockpiling security. Mohler [19] gave an information stockpiling structure on a blockchain however did not give an efficient search strategy. Li et al. [20] executed information retrieval on a blockchain, but the search results were in accurate, and the hunt efficiency was low. Zhang [21] accomplished the verifiability of worker side information. Xia et al. [22] proposed a blockchain-based wellbeing information sharing model.

The framework for sharing EHRs in the blockchain utilizes the blockchain as a guide for information sharing rather than an essential device for information stockpiling, the board, and sharing. Likewise, the current blockchain clinical information recovery arrangement does not give complete solutions for information proprietors and information clients [24].

QR Codes are for the most part utilized for pass on or store the messages since they have higher or enormous capacity limit than some other ordinary standardized identifications. This paper portrays the connection of QR Code and the cryptography. Since QR Codes have quick response time and have enormous limit, QR Codes can be used consummately to store the encoded data (messages) [7].

III.METHODOLOGY

To improve medical information wellbeing, we proposed the scheme which builds the medical platform dependent on clinical organizations that share EHRs in a specific locale. Multiple hospitals patient data can collaborate so there is more flexible in accessing the patient data without any delay based on their authorization. Patient can easily switch from one hospital to another, here treatment data of the patient is always available they can easily start diagnosis the patient based on their previous prescription. The doctor provides the treatment summary of their patient and the system manager stores keywords of these records will manage the encrypted electronic health records stores in the QR code on the servers of the respective hospitals with the blockchain. The five entities are described in the below Figure 1 as follows:

System manager: The system manager who manages the entire system, each patient, doctor, and data user they need to do registration before use this entire system. Multiple hospitals data are controlled by the

manager. He will provide the authorization for the data users and access key will be generated for accessing the patient details.

Doctor: The doctor produces a patient's electronic health record encodes the health record utilizing the patient's entrance structure and transfers the encrypted electronic health record to EHR System.

EHR System: The EHR system offers medical services to a medical institution. Normally, every hospital has a server and different computer customers. Every computer customer records the patient's wellbeing data. The server administrator then broadcasts the keywords of the electronic health record to the blockchain. The server will register the data users and doctors in the system. At the point when the doctor transfers an electronic health record to the server, the server must check the authorization of doctor.

Patient: When patient visits a hospital, the person must enroll at the hospital first. During enrollment, the token will provide for the patient, which is utilized as a go for the patient to see the doctor. The approved doctor produces an electronic health record of the patient and stores the encoded electronic health on their server. The server manager stores hash key of the electronic health record on the blockchain.

Data user: At the point outsider associations or people exists other than the hospitals for example, insurance policy, research etc., and patients who need to get the patients information. Here acquiring secret entryways created by patients is important in looking the blockchain.

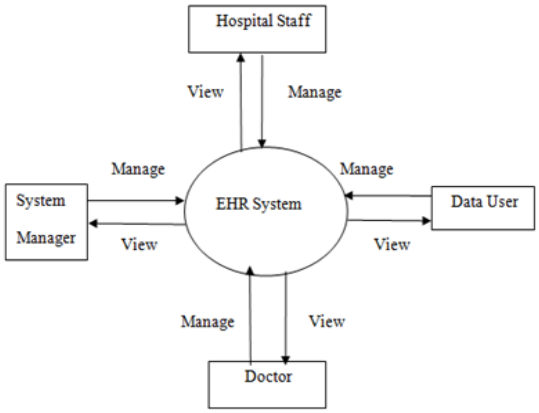

Figure 1: Actors of the Proposed system

IV.IMPLEMENTATION

Propose a system to develop a web application which focuses on the security of the patient's treatment summary recorded in the hospitals. When the patients get admitted to hospital, the system manager of the hospital collects basic details of the patient. Then, this data name, age, gender, log date is stored in the database as keywords. Hash values is generated based on these keywords using SHA algorithm which acts as key.

Each treatment summary is encrypted by using AES Rijndael algorithm and is stored as blocks in the database. When the doctor, patient, data user has to view the summary of specific patient they need to request, and access key will be provided. Once granted, they can request for view treatment. Then hash value is generated based on keywords and compared with the stored hash value which is stored in the Blockchain. If it matches, then the patient's treatment summary is decrypted which is stored in the QR code the data will viewed by the requested person. This enables privacy and security and prevents from third- party access. Flow of implementation is shown in the Figure 2

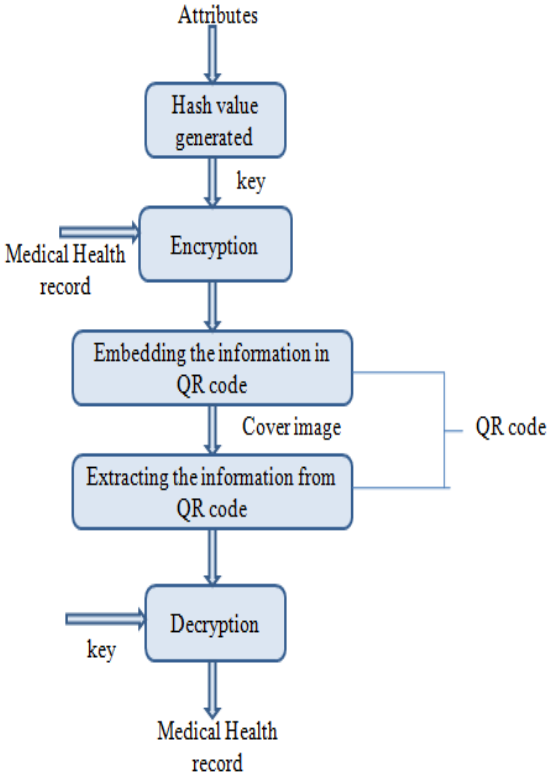

Figure 2: Flow of Encryption and Decryption process

The different stages undergone during implementation:

1. Data collection

The different hospital information data are collected. Who, need to secure the treatment summary of the patient for the efficiency of their hospital. The doctors and patient's information data are taken with respect to their hospital.

2. Key generation

Keygen(attr): The attributes attr are considered for generating the key. Here, generates the hash value based on the attributes. For hash value generation we use the SHA algorithm which will be unique, and it is irreversible. The hash value is stored in the blockchain concept for the comparison during accessing the data. It takes input as attr then, outputs the hash value. We take the some of the bits of hash value and do some changes then this will be the key for encryption.

3. Encryption

Encrypt (ts, key): The treatment summary ts of the patient will be encrypted. The encryption algorithm is run for the treatment summary. We used Rijndael AES algorithm for encrypting the treatment data to safeguard from the unauthorized user. The doctor should provide the treatment summary of the patient. Then, this encryption process is executed. It takes input as treatment data and also the key for encrypting the data, then outputs the encrypted data.

4. Embedding to the QR code

Embed (edata): The encryption data edata of the treatment summary of the patient will be write into the QR code for safer purpose. The QR code file should be kept in the secured way without losing the QRcode file. We need to provide some privileges from being accessing. If, anybody try to access the QR code they will not be able to decrypt the data because they need the key for decrypting the encrypted data. It takes input as encrypted data and output the QR code file path where it is stored. The path will be stored in the blockchain concept.

5. Decryption

Decrypt (qread, key): The decrypt the patient treatment data stored in the QR code. The same steps followed for generating the key by considering the attributes. The hash value generated based on the attribute and comparing with the stored hash value in-turn stored in the block chain concept. If it matches, then decryption process will be done. So, from this we come to know if anybody tampered the attributes or not. It takes input as QR code read and same key for decryption, then outputs the treatment summary of the patient.

Members in the blockchain comprise of medical organizations and the searchers involving members specified by the blockchain concept. Members confirm the transaction records communicated by every server to the blockchain and execute the information search work on the blockchain. In the blockchain concept, hash value will be stored, the file paths were encrypted data stored in the QR code, everyday diagnosis data of the patient are stored. Implemented the blockchain concept in the cloud database for more secure and get to know when anybody tamper the data when they are viewing the treatment summary. The overall implementation shown in the below Figure 3, of EHR system model with QR code in the blockchain concept.

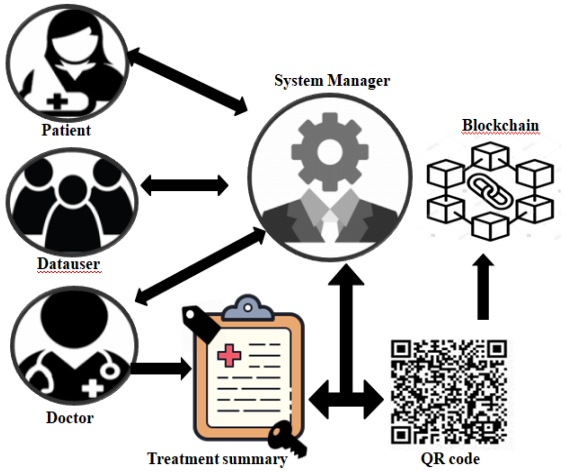

Figure 3: Electronic Health record system model with QR code in blockchain

V. CONCLUSION AND FUTURE ENHAUNCEMENT

We proposed an approach that will receive the treatment summary of the requested patient. We have experimented with the one feature that is QR code where the attribute-based encryption on block chain data is stored which will provide more secure for the patient data. Encrypted QR codes are QR codes that not everyone can scan and access. They are not very common where regularly used in the marketing, for UPI-based payment etc., everybody can access the QR code. The full use of medical information enables doctors to make quick and accurate diagnosis plans for patients and improve the efficiency of hospital work.

In future we can use this data for the different data users where there will be no loss and it can be efficient use the data. Like multiple hospital, multiple insurance policy company, multiple police station can be included there will more efficiency and secure.

REFERENCES

[1] Shufen Niu, Lixia Chen, Jinfeng Wang, and Fei Yu, "Electronic health record sharing scheme with searchable attribute-based encryption on Blockchain", in IEEE TRANSACTIONS and JOURNALS,2019.

[2] D.X.Song, D.Wagner, A. Perrig, "Practical techniques for searches on encrypted data", in S&P 2000, IEEE Computer Society, 2000, pp. 44–55.

[3] D.Cash, S.Jarecki, C.S.Jutla,et al. "Highly scalable searchable symmetric encryption with support for boolean queries", in: LNCS, vol.8042, Springer, 2013, pp: 353–373.

[4] S.Jarecki, C.S.Jutla, H.Krawczyk, M.Rosu, M.Steiner, "Outsourced symmetric private information retrieval", in: CCS 2013, ACM, pp: 875–888.

[5] Boneh D, Crescenzo G, Ostrovsky R, et al. "Public key encryption with keyword search", in Proceedings of EUROCRYPT 2004, Interlaken, Switzerland, 2004, pp:506–522.

[6] Puneeth L Sankadal, Prashanth Chillabatte, A M Chandrashekhar, “Network Security situation awareness system”, Volume 3, Issue 5, May 2015.

[7] Rahul kumar Gupta, A M Chandrashekhar, Shivaraj H. P, “Role of information security awareness in success of an organization”, Volume 2, Issue 6, May 2015.

[8] Sandhya Koti, A. M. Chandrashekhar, Chitra K V, “Security Fundamentals of Internet of Things”, Volume 3, Issue no1, JAN-2016.

[9] Syed Tahseen Ahmed, A.M.Chandrashekhar, Rahul N, “Analysis of Security Threats to Database Storage Systems” International Journal of Advanced Research in data mining and Cloud computing(IJARDC), Volume 3, Issue 5, May 2015.

[10] Curtmola R,Garay J, Kamara S, et al. "Searchable symmetric encryption: improved definitions and efficient constructions", ACM Conference on Computer and Communications Security. ACM, 2006, pp:79–88.

[11] Golle P, Staddon J, Waters B, "Secure Conjunctive Keyword Search over Encrypted Data", in Proceedings of the 2nd International Conference on Applied Cryptography and Network Security, Huangshan, 2004, pp:31– 45.

[12] Sowmyashree K K, A M Chandrashekhar, Sheethal R.S, “Pyramidal aggregation on Communication security”, Volume 3, Issue 5, May 2015.

[13] A. M Chandrashekhar and K. Raghuveer, “Hard Clustering Vs. Soft Clustering: A Close Contest for Attaining Supremacy in Hybrid NIDS Development”, 2014.

[14] Yadunandan Huded, A M Chandrashekhar, Sachin Kumar H S, “Advances in Information security risk practices”, Volume 3, Issue 5 May 2015.

[15] Qiu S, Liu J, Shi Y, et al."Hidden Policy Ciphertext-Policy Attribute Based Encryption with Keyword Search Against Keyword Guessing Attack", Science China Information Sciences, 2017, 60(5): 052105.

[16] Li S, Xi M Z "Attribute-based public encryption with keyword search", Chinese Journal of Computers, 2014, vol.37, pp: 1017–1024.

[17] Song Yan, Han Wei, Chen Dong, et al. "Attribute encryption scheme supporting keyword arbitrary connection search", Journal on Communications, 2016, 37(8): 77-85.

[18] Sun Wenhai, Yu Shucheng, Lou Wenjing, et al. "Protecting your right: Verifiable attribute-based keyword search with fine-grained owner-enforced authorization in the cloud", IEEE Transactions on Parallel and Distributed Systems, 2016, vol.27, pp:1187–1198.

[19] Dagher G, Mohler J, et al. "Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology”. Sustainable Cities and Society,2018, vol.39, pp:283–297.

[20] LiHuige, TianHaibo, ZhangFangguo, et al. "Blockchain based searchable symmetric encryption scheme", Computers and Electrical Engineering, 2018, vol.73, 2018, pp:32–45.

[21] Zhang Yinghui,Shu Jiangang,et al. "TKSE: Trustworthy Keyword Search over Encrypted

Data with Two-side", IEEE Access, 2018,vol.6, pp:31077 –31087.

[22] Xia Q, Sifah E, Smahi A, et al." BBDS: Blockchain-Based data sharing for electronic medical records in cloud environments", Information, 2017, vol.8, pp:1–16, 2017.

[23] A. M. Chandrashekhar, Sahana K, Yashaswini K," Securing Cloud Environment using Firewall and VPN", "International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), Volume 6, Issue-1, January-2016.

[24] Prashanth G M, A.M.Chandrashekhar, Anjaneya Bulla, "Secured infrastructure for multiple group communication" International Journal of Advanced Research in Information and Communication Engineering (IJARICE), Volume 3, Issue 5, May 2015.

[25] Arpitha, Nidhishree G, A. M. Chandrashekhar, "Efficient data accessibility in cloud with privacy and authenticity using key aggregation cryptosystem", International Journal for Technological research in Engineering (IJTRE), Volume 3, Issue 5, JAN-2016.

[26] Koushik P, Jagadeesh Takkalakaki, A.M.Chandrashekhar, "Information security threats, awareness and coginizance" International Journal for Technicle research in Engineering, Volume 2, Issue 9, May 2015.

[27] A. M. Chandrasekhar, Jagadish Revapgol, Vinayaka Pattanashetti, "Security Issues of Big Data in Networking", International Journal of Scientific Research in Science, Engineering and Technology, Volume 2, Issue 1, JAN-2016.

[28] Nagaveni Bhavi, A. M. Chandrasekhar, Pushpanjali M K, "Hierarchical Group Communication Security", International journal of Advanced research in Computer science and Applications, Volume 4, Issue 1, Feb-2016.

[29] A M Chandrashekhar, Monika M R, Sushma J, Navya Nagaraj "Accident detection and alert – an android app", International journal for Technological Research in Engineering (IJTRE), Volume 7, Issue 10, June-2020.

[30] Huda Mirza Saifuddin, A.M.Chandrashekhar, Spoorthi B.S, "Exploration of the ingredients of original security" International Journal of Advanced Research in Computer Science and Applications, Volume 3, Issue 5, May 2015.

[31] A.M.Chandrashekar, Tejaswini S, "Comparative analysis of Indoor Positioning System Using Bluetooth and Wi-Fi", International Journal for Innovative Research in Science & Technology (IJIRST),Volume 4,Issue 1,June 2017.

[32] A.M. chandrashekhar, Meghana B.Ramesh, "Green computing: Recycling the E-Waste Using VDI Blaster Technique", International Journal of Scientific Research in Computer science, engineering and information technology, (IJSRCSEIT), volume 2, issue 3 , June 2017.

[33] A.M. Chandrashekhar, Adarsh L, Bhavana S, Varsha G "Comparison of the performance of Memory Augmented Neural Network Model with Long-Short Term Memory Model" International Journal of Engineering and Techniques, Volume 4 Issue 3, May - June 2018.