Grenze International Journal of Engineering and Technology, June Issue

A Thorough Study on Revoking Key Agreement Protocol on Cloud using Blockchains

Nishant Gajanan Deshmukh[1] and Prashant B. Kumbharkar[2]
[1-2]JSPM's Rajarshi Shahu College of Engineering, Pune-411033
Email: nishant44deshmukh@gmail.com, deanpnd@jspmrscoe.edu.in

***Abstract*—It can be noticed that there has been a considerable improvement in the realizations of the health care sector in the recent years with consistent and remarkable additions. The medical improvements can be highly useful in improving the lives of the others as well as enhancing the quality of life in general by a large margin. These advancements are necessary to facilitate the growth and maintain the optimum performance of the individuals that can allow for a much better realization of the long term goals. But there has been an increased concern over the data or information being utilized for the purpose of sharing the electronic health records of the patients. These are valuable records that can help mitigate a lot of problems and streamline the jobs of the doctors that are being over-burdened with the large amount of work loads. These concerns over the privacy and security of the medical need to be addressed to improve the confidence of the users in sharing their vital health records to other institutions. Therefore, an effective and useful mechanism for achieving key agreement protocol has been proposed that utilizes the blockchain platform to achieve its goals on the EHR data stored on the cloud through the Amazon RDS service. The approach will be elaborated in detail in the upcoming editions of this research.**

***Index Terms*— Electronic Health records, Public Cloud, Medical Health Records, Cryptography, and Blockchain.**

I. INTRODUCTION

Conventional paper health records typically contain the patient's individual health information, medications, vaccinations, examination findings, medical photos, and genetic predisposition of hereditary disorders. Unfortunately, because to the characteristics of the research, transferring paper-based medical records between two or even more healthcare centers was time-consuming and complicated. One potential answer to this problem is the electronic sharing of patients' medical information. When doctors have access to digitized versions of patients' medical records, they can make increasingly precise assessments. Medical records may be stored in this manner indefinitely and retrieved whenever needed. Notwithstanding this, a costly improvement in storage capability is required to accommodate the ever-increasing amount of medical data. Data integrity is easily breached when sensitive patient information is sent electronically from one medical facility to another via an unsecured network.

Cloud computing allows for the low-cost and convenient long-term preservation of massive amounts of electronic medical information, as well as access to computationally intensive tools. More and more people and healthcare institutions are relying upon that cloud to store and share their medical data. The expense of storing

Grenze ID: 01.GIJET.9.2.531_1

medical records locally may be reduced by having users save their data centrally and accessing it remotely. Several potential cloud-based methods for the secure exchange of medical information have already been proposed.

Such procedures are very dependent upon that provider of cloud services (CSP). If the CSP wants to create place for the information of these other users and generate more money, it might choose to delete data that clients have hardly or never accessed at all. The data stored in the cloud, however, is vulnerable to corruption due to cloud server failure, management blunders, or malicious attacks; nonetheless, the CSP may opt to conceal the reality that information was corrupted on intentionally to preserve its reputation. Because of this, one may draw the following consequences: storing data in the cloud facilitates the ability for healthcare centers to communicate electronic health information among one another, but data saved there are vulnerable to manipulation, falsification, and access by those who are not allowed to see them.

In terms of database management systems, blockchain is evolving and may be accessed on the web. Its unique selling points are its decentralization, openness, and resistance to data tampering. With blockchain technology, users don't have to depend on other parties to securely store our data for us, nor do we have to fret about losing access to that data if they fail to do so. Because of this, the cloud's traditionally problematic security may be avoided. A great number of scholars have recently studied the application of blockchain innovation in the field of medicine.

Xiaodong Yang et. al. [1] presents a novel system for the exchange of medical data that takes use of both the benefits of using the cloud to store information as well as blockchain solutions. The cloud service is used in this scheme to preserve classified health information, as well as the blockchain technology is used to maintain the identity of matching medical data ciphertext as well as other details connected to medical matters. As a result, the prerequisites for irreversibility as well as enforceability are satisfied by the system that was presented. When an attribute-based cryptosystem is used, not only is it possible to guarantee the secrecy of medical information stored on the cloud, but it is also possible to validate the credibility of the medical source of data. In addition, by using the ODABE technique, consumers of medical information may lessen the load of computing work that is placed on their shoulders.

Vangelis Malamas et. al. [2] proposed an effective system for regulating granularity access to health-relevant data. The solution was built on an innovative multilayer multi blockchain infrastructure with sophisticated functionality. A collection of completely functioning smart contracts, security methods utilized for encryption technology, a fine-grained access management system, and a powerful forensics-by-design methodology with very resilient audit logs as well as substantial integrity assurances all lend their assistance to the framework. They have created a proof-of-concept application in order to show that their architecture may be used to a variety of situations. According to the findings of these experiments, the proposed framework is flexible enough to encompass multiple use case circumstances together within health care environment. These use case circumstances involve the management of health-related information and the enforcement of multi-entity, fine-grained policies for access control.

Mohammad Moussa Madine et. al. [3] presented a system that utilized blockchain technology that would offer patients authority to control their own medical information in a way that was decentralized, transparent, dependable, trustworthy, and confidential. Researchers have constructed two smart contracts that are predicated on Ethereum in order to streamline the operation of the activities that have been established. They were able to safely retrieve, preserve, and exchange patients' medical data by integrating the recommended alternative with a variety of other technologies and services, like as IPFS, proxy re-encryption, verified oracles, and perception systems. The authors gave methods as well as the application and testing information for those algorithms. The researchers conducted an analysis of the suggested agreements within the context of a patient health record (PHR) system in order to validate their accuracy. The cost as well as security study that was provided aimed to demonstrate the practicability, resistance to assaults, and overall acceptability of the solution that was being suggested.

This literature review paper divides section 2 into an assessment of prior work in the form of a review of literature, and section 3 concludes with recommendations for future research.

II. Related Works

Haya R. Hasan et. al. [4] developed a telemedicine system that is based on a private blockchain. The suggested solution assures the accountability, consistency, and usability of all telehealth transactions and data connected to the provision of medical treatment, investigations, including surveillance for patients who are located remotely or who are caring for themselves at home. The solution that was offered made use of the essential properties that

are inherent to private blockchains in order to guarantee confidence, transparency, authenticity, accessibility, and confidentiality. This study helps pave the road toward providing better medical treatment for persons living in remote and unreachable places by contributing to the method in which the path is paved. It also makes it easier for doctors to treat patients who are located in distant areas. The authors were successful in protecting the patient's privacy as well as their medical information by employing a blockchain network that required permission to access. The researchers demonstrated how the system may be connected with cloud as well as IPFS storage platforms to improve the portability as well as accountability of immutable digital material that is huge in size.

Diana Hawashin et. al. [5] offered a blockchain-based technology as a means of reducing the waste of essential medicines that is brought forward by their excess production including underutilization in a way that is decentralized, responsible, traceability, accessible, protected, and reliable. [5] The authors created four different types of smart contracts, each of which dynamically records occurrences, keeps track of the provenance of data, and ensures integrity. The researcher identified five techniques that illustrate the reasoning underlying the smart contracts that we designed. The intricacies of each stage of the suggested resolution are covered in depth, encompassing the evaluation and validation procedures, as well as the deployment specifics. In addition, the mechanism by which the approach protects data confidentiality and authenticity, as well as scalability, responsibility, and resilience to assaults by middlemen, is described.

Ganesan Subramanian et. al. [6] proposes the use of the NEM symbolic blockchain as a reliable medium for the storage of medical information pertaining to diabetes patients. The blockchain agreement was developed for the purpose of storing medical records. Medical facilities, a vaccine facility, a government, and numerous other participants are located inside the collaboration network. The ABE algorithm ensures the confidentiality of patients' medical information. A number of XYM may be allotted to a stakeholder on the NEM blockchain so that they can participate in operations amongst consortium servers. It has been shown that the NEM symbol blockchain may serve as either a proof-of-concept prototype. An investigation on the integrity of the currently operational blockchain as well as the QR code included into the fingerprint is carried out. In consequence of this, nodes within the consortium are able to communicate with one another despite needing to be aware of the identities of the different nodes.

According to Jiyu Tao et. al. [7], progress in the area of medical informatics will continue to be made in the future. The exchange of medical records is an essential component. Patients may be able to avoid having to undergo the same exams several times, while researchers may get useful information. In this work, we present a system for the practical exchange of medical files that is based on blockchain technology and decentralized ABE. Under this system, patients maintain full control on personal medical records, thus there is no requirement for them to be concerned about the disclosure of private information to unauthorized parties. The associative structure of multi-person collaboration, participatory decision, and flexibility for dynamic transformations in individuals bring the concept closer to representing the way things really work in the real world. Not only does the decentralized model correspond to the concept of decentralization that underpins the blockchain, in addition it sidesteps the organizational challenges that are brought on by centralized organizations.

Haya R. Hasan et. al. [8] outlines the conception, implementation, and testing of a blockchain-based system that can produce healthcare technology passports complete with immunization credentials. The suggested approach contributes to the reduction of the transmission of transmissible illnesses in overall, as well as the disease COVID-19 in specific. The study offered several smart contracts that make use of on-chain occurrences and alerts, in addition to relying on little on-chain data storage. In this method, researchers added related biometrics, self-sovereign identities, and re-encryption intermediates to the one-of-a-kind Ethereum identities of the organizations that were taking part. The authors conducted an evaluation of the procedures for the proposed approach by first doing a comprehensive cost assessment inspection, and then utilizing the smart check program to confirm for any security vulnerabilities. The technique, according to the authors, opens up the possibility towards efficient approaches that may aid in halting the spread of illnesses by accurately capturing occurrences in a reasonable timeframe that cannot be tampered with.

Neha Garg et. al. [9] developed a unique identification key agreement technique for the Internet of Medical Things environment using blockchain technology (BAKMP-IoMT). BAKMP-IoMT ensures the confidentiality of key management amongst all of the various communication organizations. The data pertaining to healthcare may also be accessed in a safe manner from either the cloud servers by the individuals who are authorized to do so. The whole of the data pertaining to medicine is kept on a blockchain that is managed by the cloud storage. Comprehensive safety evaluation of BAKMP-IoMT is indeed undertaken to establish its persistence to a variety sorts of probable assaults using the widely-recognized AVISPA tool as well as via formal and non-formal security research. This is done to show that BAKMP-IoMT can withstand these attacks. When compared to other

relevant current schemes, BAKMP-IoMT not only works better but also operates more effectively in aspects of security as well as functionality characteristics, less connectivity, and lower communication overhead throughout the key authentication along with key management period.

Abdullah Ayub Khan et. al. [10] asserts BIoMT, a blockchain hyperledger fabric-enabled Internet of medical things distributed architecture, with the goal of lowering the amount of resources that are used, such as data processing, network, as well as storage, and increasing the ecosystem's level of dependability within the IoMT atmosphere. Sustaining an integrated subsystem for health information supply chain transparency and decency without blockchain hyperledger fabric-enabled denunciation is essential to this suggested BIoMT, which has correctly arranged the entire design to be secure, guarded, and resource convenient without distressing the originator of the constructed ecosystem. To automating the execution of the networks of medical operations in a distributed environment, the researchers created and executed a total of three distinct smart contracts in this particular piece of research. These smart contracts were combined with adjusted agreement procedures (PoW).

Samiulla Itoo et. al. [11] presented a novel and efficient strong authentication methodology for electronic healthcare platforms that is dependent on blockchain technology and the cloud. The CKMIB security solution that has been presented ensures user confidentiality and anonymity while also being resistant to several types of assaults. As a result of the fast growth of technology, so each record in the electronic healthcare delivery system is now being substituted by an electronic file. Because these electronic medical records include patients' personally identifiable information, it is imperative that they be protected. The authors of this research developed a robust CKMIB methodology that makes use of blockchain technology in conjunction with cloud computing. Underneath the assumptions of the random oracle model, the suggested protocol is safe. In particular, AVISPA's High-Level Public-Key Cryptography Standard (HLPSL) was used in order to carry out comprehensive security assessment and validation.

Jin Sun et. al. [12] present a new encryption method for the safe storage and efficient exchange of electronic medical information. This new encryption system relies on the attribute-based encryption method, distributed ledger technology, and indeed the Inter Planetary File System (IPFS) hardware architecture. [12] A strong access control is provided for the electronic health care records by the arrangement, which makes use of attribute-based encrypted communications. As a result, third parties who aren't associated to the patient will not be able to view the patient's private information unless they have been given permission to do so. During the same period, the IPFS storage framework was established to remove the semi-honest and even though inquiring cloud server in order to guarantee the secure environment of the medical information. Additionally, the cryptographic protocols must have been implemented to document the memory and search procedures, guaranteeing the uniqueness and auditability of the information while also resolving the issue of a lack of security provided by a centralized authority.

Chun-Ta Li et. al. [13] asserts that as a result of the fast advances in scientific and engineering as well as the internet, paper-based papers are gradually being phased out in favor of digital documents. Not only are digital papers better for the environment than their paper-based counterparts, but digital data can also be exchanged and distributed in instantaneously. Whereas electronic health data can introduce a great deal of accessibility, which would include telemedicine, data extraction, healthcare information gathering and statistical data, and evaluation of outbreak phenomenon in current history, it is important to note that privacy concerns must be addressed when using electronic health information. In this context, the patients' very private medical data include all three main categories of medical records: electronic health records (EHR), electronic medical records (EMR), and personal health records (PHR). In the event that they are sent across the system, the confidentiality of the data may be called into question.

Zhen Pang et. al. [14] The electronic health record (EHR) sharing plan is particularly significant, since it can guarantee that patients get complete and correct care. A system for exchanging electronic health records may facilitate the sharing of information across various hospitals, which in turn can help the field of medicine advance. Because the EHR includes a significant amount of information, it is essential that the authors preserve the confidentiality of data throughout the data exchange process. The data will be stored upon both chain including off chain that will also assure the shared data's validity and integrity. The proposed technique store information in each of these locations. This article makes use of a multi-keywords searchable encryption system, which is a method that has the potential to increase both the effectiveness and the precision of cypher text.

Ye Seul Bae et. al. [15] propose a health information sharing network that uses blockchain technology and is based on the HL7 FHIR Standards. It is possible that the use of blockchain technology would mitigate issues relating to trustworthiness, privacy, and confidentiality, hence boosting consumers' faith in the information that is being traded. The Health Pocket framework is able to reuse information for a wide range of applications since it makes advantage of these standards and incorporates standardized elements wherever possible. The

researchers designed and tested a framework that permits individuals to make proactive use of and distribute their health information with other people. For the purpose of achieving data standardization, each component of PGHD was transformed through into HL7 FHIR format. In relation, the uploading of the responsible for sharing to a blockchain network makes it more difficult to falsify or fabricate data, which helps to maintain the confidentiality of the information.

A. Limitations

The analysis of the previous approaches has led to the identification of the limitations that have been crucial in the implementation of the revoking key agreement protocol. The blockchain platform is subjected to certain limitations in terms of scalability. The blockchain scaling is complex process that leads to the increase in the computational complexities and introduction of delay. This needs to be effectively overcome to reduce the time and space complexities.

B. Challenges

The majority of the approaches have been utilizing the common and widely used platforms for open source implementations of the Blockchain such as Ethereum, Hyperledger Fabric, etc. These implementations are very useful and highly modular to attain the desired distributed platform goals, but these approaches are difficult to control. The open source framework is also less scalable and provides less performance, this is the reason why we will be implementing a private blockchain and will not be using the public offerings. It is going to be challenging to achieve the private blockchain in this methodology.

III. PROPOSED MODEL

Through deep analysis of the current methodologies for the purpose of achieving the methodology that can be depicted through the flowchart given below in the Figure.1. The approach is initiated through the registration of the patient and the doctor, once the login credentials are created the E-health record is provided to the system that encrypts it with AES Encryption. These encrypted records are then transformed into a blockchain framework. This blockchain is stored on an online cloud storage for easier access and storage for sharing. The bitmapping is being used for the realization of the analysis of the integrity of the data. If the agreement has been compromised then the system generates a report and revokes the key agreement protocol.

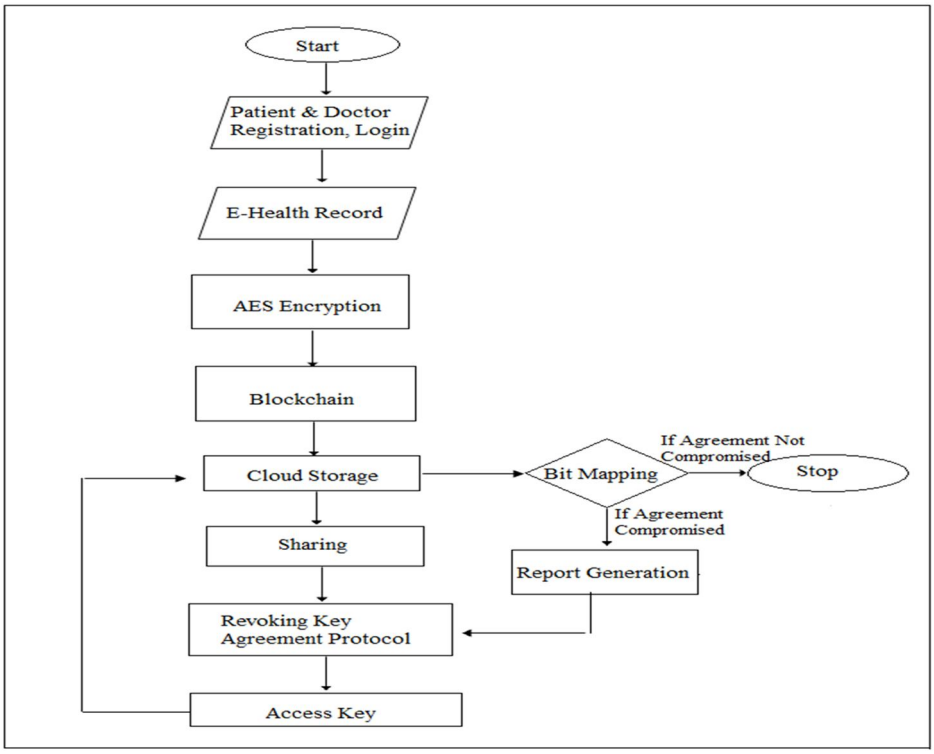

Figure 1. Proposed model

IV. CONCLUSIONS

It is clear that the health care industry's earnings have increased significantly over the last several years, with steady and spectacular gains. Medical advancements have the potential to greatly benefit the lives of others and raise the bar for human flourishing everywhere. In order to foster development and sustain peak performance in people, which may lead to more effective long-term goal attainment, these improvements are essential. Concerns about the data or information used to achieve the sharing of patient's Electronic health records have, nevertheless, grown in recent years. These are important documents that may ease the pressure on already overworked physicians by streamlining their processes and reducing unnecessary complications. For people to feel more comfortable giving their sensitive medical information to other organizations, issues related to privacy and security must be resolved. As a result, a technique for obtaining key agreement protocol has been devised, which makes use of the blockchain platform to realize its aims on the EHR data saved in the cloud through the Amazon RDS service. Future iterations of this study will provide further clarification on the methodology used.

REFERENCES

[1] X. Yang, T. Li, X. Pei, L. Wen and C. Wang, "Medical Data Sharing Scheme Based on Attribute Cryptosystem and Blockchain Technology," in IEEE Access, vol. 8, pp. 45468-45476, 2020, doi: 10.1109/ACCESS.2020.2976894.

[2] V. Malamas, P. Kotzanikolaou, T. K. Dasaklis and M. Burmester, "A Hierarchical Multi Blockchain for Fine Grained Access to Medical Data," in IEEE Access, vol. 8, pp. 134393-134412, 2020, doi: 10.1109/ACCESS.2020.3011201.

[3] M. M. Madine et al., "Blockchain for Giving Patients Control Over Their Medical Records," in IEEE Access, vol. 8, pp. 193102-193115, 2020, doi: 10.1109/ACCESS.2020.3032553.

[4] H. R. Hasan, K. Salah, R. Jayaraman, I. Yaqoob, M. Omar and S. Ellahham, "Blockchain-Enabled Telehealth Services Using Smart Contracts," in IEEE Access, vol. 9, pp. 151944-151959, 2021, doi: 10.1109/ACCESS.2021.3126025.

[5] D. Hawashin, K. Salah, R. Jayaraman, I. Yaqoob and A. Musamih, "A Blockchain-Based Solution for Mitigating Overproduction and Underconsumption of Medical Supplies," in IEEE Access, vol. 10, pp. 71669-71682, 2022, doi: 10.1109/ACCESS.2022.3188778.

[6] G. Subramanian and A. Sreekantan Thampy, "Implementation of Blockchain Consortium to Prioritize Diabetes Patients' Healthcare in Pandemic Situations," in IEEE Access, vol. 9, pp. 162459-162475, 2021, doi: 10.1109/ACCESS.2021.3132302.

[7] J. Tao and L. Ling, "Practical Medical Files Sharing Scheme Based on Blockchain and Decentralized Attribute-Based Encryption," in IEEE Access, vol. 9, pp. 118771-118781, 2021, doi: 10.1109/ACCESS.2021.3107591.

[8] H. R. Hasan et al., "Blockchain-Based Solution for COVID-19 Digital Medical Passports and Immunity Certificates," in IEEE Access, vol. 8, pp. 222093-222108, 2020, doi: 10.1109/ACCESS.2020.3043350.

[9] N. Garg, M. Wazid, A. K. Das, D. P. Singh, J. J. P. C. Rodrigues and Y. Park, "BAKMP-IoMT: Design of Blockchain Enabled Authenticated Key Management Protocol for Internet of Medical Things Deployment," in IEEE Access, vol. 8, pp. 95956-95977, 2020, doi: 10.1109/ACCESS.2020.2995917.

[10] A. Ayub Khan, A. A. Wagan, A. A. Laghari, A. R. Gilal, I. A. Aziz and B. A. Talpur, "BIoMT: A State-of-the-Art Consortium Serverless Network Architecture for Healthcare System Using Blockchain Smart Contracts," in IEEE Access, vol. 10, pp. 78887-78898, 2022, doi: 10.1109/ACCESS.2022.3194195.

[11] S. Itoo, A. A. Khan, V. Kumar, A. Alkhayyat, M. Ahmad and J. Srinivas, "CKMIB: Construction of Key Agreement Protocol for Cloud Medical Infrastructure Using Blockchain," in IEEE Access, vol. 10, pp. 67787-67801, 2022, doi: 10.1109/ACCESS.2022.3185016.

[12] J. Sun, X. Yao, S. Wang and Y. Wu, "Blockchain-Based Secure Storage and Access Scheme For Electronic Medical Records in IPFS," in IEEE Access, vol. 8, pp. 59389-59401, 2020, doi: 10.1109/ACCESS.2020.2982964.

[13] C. -T. Li, D. -H. Shih, C. -C. Wang, C. -L. Chen and C. -C. Lee, "A Blockchain Based Data Aggregation and Group Authentication Scheme for Electronic Medical System," in IEEE Access, vol. 8, pp. 173904-173917, 2020, doi: 10.1109/ACCESS.2020.3025898.

[14] Z. Pang, Y. Yao, Q. Li, X. Zhang and J. Zhang, "Electronic Health Records Sharing Model Based on Blockchain With Checkable State PBFT Consensus Algorithm," in IEEE Access, vol. 10, pp. 87803-87815, 2022, doi: 10.1109/ACCESS.2022.3186682.

[15] Y. S. Bae et al., "Development of Blockchain-Based Health Information Exchange Platform Using HL7 FHIR Standards: Usability Test," in IEEE Access, vol. 10, pp. 79264-79271, 2022, doi: 10.1109/ACCESS.2022.3194159.