

A Novel Approach Revoking Key Agreement Protocol on Cloud using Blockchain

Nishant Gajanan Deshmukh¹ and Prashant B. Kumbharkar²

^{1,2} JSPM's Rajarshi Shahu College of Engineering, Pune-411033

Email: nishant44deshmukh@gmail.com, pbk.rscoc@gmail.com

Abstract—It is unmistakable that, throughout the course of the past couple of decades, the profits of the medical service business have expanded dramatically, exhibiting both consistent and exceptional growth. The evolution of medical technology has an opportunity to have a significant positive impact on the well-being of individuals as well as improve the standard for human development worldwide. It is vital to make these adjustments in order to stimulate growth in individuals and maintain outstanding performance, which could result in more successful long-term goal accomplishment. In spite of this, there has been an increase over the last few years in the number of worries regarding the data or knowledge that is utilized to accomplish the exchange of electronic health records of individuals. These are essential papers that, by simplifying the procedures that doctors currently have to go through and eliminating extraneous complexities, may help relieve some of the stress that they are already under. It is necessary to find solutions to problems relating to privacy and safety before individuals would feel at ease disclosing sensitive information about their medical histories to other parties. As a consequence of this, a method for getting key agreement protocol had been developed. This method takes advantage of the blockchain technology in order to accomplish its goals on the electronic health record (EHR) information that is stored in the cloud by means of the Amazon RDS service. The methodology has been subjected to exhaustive testing for its effectiveness measurements, which has culminated in satisfactory results.

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

I. INTRODUCTION

Over the course of the last several years, there exists a discernible trend toward an increase in the conclusions of the healthcare sector, which has been accompanied by amazing and constant increases. This may be seen. The advances in medical technology have the potential to be of tremendous assistance in bettering the lives of others and, more generally, in elevating the standard of living across the board. These innovations are important to enable the development and sustain the optimal performance of the people, which could make it possible for an improved accomplishment of the long term objectives. They are also essential for promoting the expansion of the organization as a whole. However, there has been a rise in the level of worry throughout the information and data that is being employed for the purpose of reaching the goal of sharing the patients' electronic health records. These important records have the potential to alleviate a significant number of issues and make the work of the overworked physicians more manageable by streamlining the processes involved in their duties. The users' worries about the privacy and safety of their medical information ought to be resolved in order to boost their

trust in the practice of sharing their important health data with other organizations.

The patient's specific information regarding health, prescriptions, immunizations, test outcomes, diagnostic pictures, and biological propensity of inherited ailments are often included in conventional printed medical records. Regrettably, due to the nature of the study, moving paper-based medical information across two or even more medical centers was both time consuming and complex. This was because of the peculiarities of the research. The electronic dissemination of patients' medical information is one possible solution to this issue that might be considered. When medical professionals have access to digital copies of their patients' medical information, they are better able to provide accurate diagnoses and treatment recommendations. In this approach, medical records may be preserved for an endless amount of time and accessed anytime they are required. In spite of this, a pricey upgrade in storage capacity is necessary to meet the ever-increasing volume of medical data. This improvement is required immediately. When sensitive patient information is electronically transferred from one medical institution to another across an unprotected network, there is a high risk that the data integrity may be compromised.

The use of cloud computing enables not only the access to computationally expensive tools but also the long-term storage of large volumes of electronic medical data at a cheap cost and in a manner that is both practical and easy. When it comes to storing and sharing personal medical data, an increasing number of individuals and healthcare organizations are turning to the cloud. It is possible to save costs associated with maintaining medical information locally by requiring users to store their data in a central location and then retrieving it remotely. There have already been many suggestions made for possible cloud-based solutions that may be used to communicate medical information in a safe manner.

These processes are very reliant on the cloud service provider that they are used with a CSP. If the cloud service provider (CSP) wishes to make room for the knowledge of additional users and earn more revenue, it may decide to erase data that its customers have scarcely or never viewed at all. This might be a risky move. The data that is kept in the cloud, on the other hand, is susceptible to corruption as a result of cloud server breakdown, operational mistakes, or hostile assaults; nevertheless, the CSP may choose to hide the fact that information was purposely compromised on in order to retain its reputation. It is possible to draw the following conclusions as a result of this fact: storing data in the cloud makes it easier for healthcare facilities to share electronic health information with one another; on the other hand, data saved there are susceptible to being manipulated, falsified, and accessed by individuals who are not authorized to view them.

The blockchain is a decentralized ledger that is still undergoing development and can be accessed over the internet. The fact that it is decentralized, open, and resistant to having its data altered are the primary selling factors for it. Users no longer need to rely on third parties to safely keep their data for them or worry about lacking accessibility to that information if the third parties fail to do so. This is because blockchain technology eliminates the need for users to depend on third parties. As a result of this, it may be possible to circumvent the cloud's notoriously inadequate security. Recent research conducted in the area of medicine by a significant number of academics has focused on exploring the potential applications of blockchain technology. As a result, an efficient and helpful method for obtaining key agreement protocol is being provided. This mechanism makes use of the distributed ledger technology to accomplish its objectives on the EHR data hosted on cloud servers by means of the Amazon RDS service. The methodology will be broken down into its component parts in more depth in the next sections of this research article..

II. RELATED WORKS

Digital healthcare identities with vaccination certificates are described in detail by Haya R. Hasan et al. [1], who detail the development, deployment, and validation of a blockchain-based framework to accomplish this goal. The proposed method aids in the fight against the spread of infectious diseases generally and COVID-19 in particular. The research presented a number of smart contracts that not only make advantage of on-chain events and notifications, but also need not much in the way of on-chain information storage. Using this approach, researchers supplemented the unique Ethereum credentials of the participating companies with fingerprints, self-sovereign identifiers, and re-encryption composites. The authors inspected the processes for the suggested solution using a full cost evaluation examination, and then they used the smart check tool to validate for any security flaws. The scientists argue that the method may pave the way to effective strategies that might help curb the disease epidemic by collecting events in a timely manner which can't be altered.

Using blockchain and the data center, Samiulla Itoo et al. [2] introduced a new and effective robust identification mechanism for cloud-based electronic healthcare applications. This paper presents the CKMIB security program, which protects user anonymity and confidentiality and is resilient to a wide range of attacks. Each paper record

in the system that provides healthcare is being replaced by an electronic document as a consequence of the rapid development of technology. Protecting these digital health records is crucial because they contain patients' private information. In this study, the authors created a secure CKMIB approach that employs blockchain and cloud computing. Assertions made by the random oracle framework ensure that the proposed protocol is secure. Comprehensive security examination and verification was performed using AVISPA's High-Level Public-Key Cryptography Standard (HLPSL).

An efficient solution for controlling shared data precision in the health care sector was presented by Vangelis Malamas et al. [3]. The approach relies on a cutting-edge, multi-blockchain architecture that features complex operations. The architecture is supported by a set of fully operational smart contracts, privacy techniques used for encrypted communications, a granular access control system, and an effective forensics-by-design approach with extremely robust audit trails and strong reliability guarantees. To demonstrate the adaptability of their design, they have built a proof-of-concept application. The results of these tests suggest that the suggested framework is adaptable enough to accommodate a wide variety of scenarios that may arise in a healthcare setting. In these scenarios, for example, multi-entity, granular access controls must be enforced in order to handle health-related data.

Blockchain technology was used by Neha Garg, et al. [4] to create a one-of-a-kind identifying key establishment method for the IoMT setting (BAKMP-IoMT). With BAKMP-IoMT, all parties involved in a conversation may be certain that their access control practices will remain secret. Those who are permitted to use them can also safely retrieve health information either from the cloud servers. The entirety of the healthcare industry's data is stored in the cloud, and its blockchain serves as the central database. BAKMP-security IoMT's is thoroughly evaluated utilizing the well-known AVISPA tool in addition to official and informal security investigations to assess the protocol's resilience to a broad range of possible attacks. This is carried out to demonstrate that BAKMP-IoMT is resilient against such assaults. BAKMP-IoMT is superior to other comparable contemporary schemes in terms of performance, reliability, usefulness, connection, and network bandwidth throughout the entirety of the key authorization and key management process.

According to Chun-Ta Li et al. [5], the proliferation of computers and networks has led to the gradual phase-out of paper records. Electronic data can be exchanged and distributed in instantaneously, and it also has the added benefit of being far more environmentally beneficial than paper-based records. Ehealth, retrieval of data, health data gathering, analytics, and study of disease patterns in current history are all areas where digital health data may be a great help. In which the three categories of commonly seen medical records are all part of the patients' highly confidential medical files. Concerns concerning data protection may arise when it is sent via the network. So, numerous scholars have recommended several strategies for data security management to safeguard the confidentiality of patients' medical data from unauthorized access.

As stated by Jiyu Tao et al. [6], the field of medical intelligence will remain to see growth in the years to come. Specifically, it is crucial that patients and healthcare providers share their medical information. Researchers may learn something helpful, and patients could prevent repeat examinations. In this paper, we provide a blockchain-based and decentralized ABE-powered system for the efficient transfer of medical records. Individuals should not worry that their private health details would be shared without their knowledge or consent since they will have complete authority over their data. The notion draws nearer to replicating the manner things truly function in the real world because to its correlative structure, which allows for multi-person cooperation, collective decision, and the adaptability for adaptive alterations in persons. The decentralized approach not only avoids the operational problems that are driven on by hierarchical organizations, but it also corresponds to the notion of decentralization that supports the blockchain.

Diabetic individual medical records might be securely stored on the NEM conceptual blockchain, as proposed by Ganesan Subramanian et al. [7]. The blockchain protocol was originally conceived as a means of safely archiving patient information. The cooperation network is a large, interconnected system that includes medical centers, a vaccine production plant, a government, and many other organizations and individuals. A patient's medical records will remain private thanks to the ABE engine. Every NEM blockchain participant that wants to take part in server-to-server consortium activities may request and receive XYM tokens. As has been demonstrated, the NEM symbolic blockchain has the potential to act either as an empty proof-of-concept sample or a fully functional production system. Verification is performed on both the live blockchain and the QR code contained in the fingerprint itself to ensure its authenticity. As a result, members of the consortia may interact among themselves without having to learn the identification of each other's members.

To combat the overproduction and underdevelopment that lead to unnecessary drug wastage, Diana Hawashin et al. [8] proposed using blockchain technology. Their system would be transparent, accountable, transparent, approachable, secured, and dependable. Over all, the authors developed four distinct varieties of smart contracts,

which all proactively log events, trace strong authentication, and guarantee information integrity. The study's author singled out five methods that effectively portray the logic behind our conceived smart contracts. Assessment and verification methods, as well as implementation details, are all discussed in length. Furthermore discussed are the means by which the strategy may scale, take ownership of its behaviors, and resist attacks from intermediaries while maintaining data privacy and legitimacy.

With the objective of decreasing the number of resources utilised, including information processing, communications system, and retrieval, and ramping up the ecosystem's consistence inside the IoMT setting, Abdullah Ayub Khan et al. [9] propose BIoMT, a blockchain hyperledger fabric-enabled distributed architecture for IoMT medical devices. This proposed BIoMT has appropriately ordered the complete system to be safe, protected, and economically accessible without bothering the ecosystem's creator, which is vital for maintaining supply chain openness and dignity while dealing with sensitive patient data. In this study, the researchers developed and deployed three separate smart contracts to automate the implementation of networking of medical procedures in a dispersed setting. To complement these digital agreements, we revised our standard operating procedures (PoW).

Autonomous, accessible, reliable, reputable, and private, the solution proposed by Mohammad Moussa Madine et al. [10] uses blockchain technology in order to provide patients power to manage their own medical records. In the interest of standardizing the functioning of the specified operations, researchers have built two Ethereum-based smart contracts. By combining the suggested replacement with some other products and services like as IPFS, proxy re-encryption, certified oracles, and observation systems, they were capable of safely recover, store, and communicate patients' health information. The authors provided not just algorithms but also details on how to use and evaluate them. In order to verify the reliability of the proposed arrangements, researchers examined them in the framework of a patient health record (PHR) system. The price and safety analysis offered was meant to prove the method's viability, robustness against attacks, and general appeal.

In order to ensure the confidentiality of electronic medical records, Jin Sun et al. [11] provide a novel encryption approach. Attribute-based encryption, distributed ledgers, and the IPFS underlying hardware structure are the foundation on which this novel encryption algorithm rests. Since the setup employs attribute-based secure communications, it is able to deliver electronic health records with a high level of security in terms of who may access them. Hence, unrelated individuals will be denied access to the patient's personal information without specifically granted access. Concurrently, the IPFS information system was developed to get rid of the dishonest and despite questioning cloud server and ensure the safe keeping of medical records. Furthermore, cryptographic mechanisms have to have been put in place to record storage and retrieval processes; this will ensure the information is both distinctive and auditable and will address the problem of insufficient security from a centralized government.

In a new system for sharing medical records, Xiaodong Yang et al. [12] capitalize on the advantages of cloud computing and the decentralized nature of blockchain technology. With this system, sensitive health data is stored in the cloud, and the blockchain is employed to verify the authenticity of any ciphertext that matches encrypted health records or other data. In this way, the described system satisfies the requirements for irrevocability and accountability. Medical information saved in the cloud may be kept private and the reliability of the data's healthcare origin verified by employing an attribute-based cryptosystem. In particular, the ODABE method may help those who rely on medical data to reduce the amount of time spent on computer tasks.

III. PROPOSED METHODOLOGY

The diagram presented in Figure 1 illustrates the suggested methodology for safeguarding Electronic Health Records within a medical infrastructure by utilizing the blockchain framework and cloud storage. The procedures undertaken to accomplish this system are expounded upon below.

Step 1: Registration and Login – The method presented exhibits a streamlined graphical user interface that was developed utilizing the Java swings framework. The healthcare facility has the option to utilize this interactive interface for authentication purposes and to execute the various procedures mandated by this methodology. In the event that the hospital is accessing the system for the first time, it is possible for an individual to initiate the registration process for an account. The registration form necessitates the provision of personal information such as full name, email address, mobile phone number, gender, date of birth, username, and password. Verification of this information is necessary prior to the establishment of an account and the provision of hospital access.

The hospital is allocated a distinct user identification and password to ensure authentication. Upon verification, the hospital operation frame will be loaded. The hospital has the ability to perform a range of tasks during this operational period.

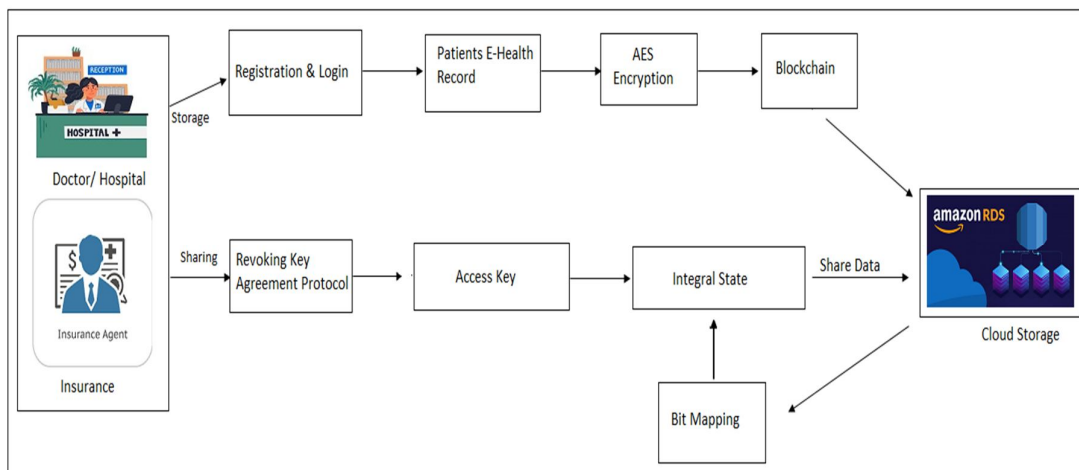


Figure 1: System Overview Diagram

Likewise, the physician has the ability to enroll in the system through the sign-up feature. The registration credentials provided by the doctor exhibit a high degree of similarity with those of the hospital, albeit with some minor variations. The physician is required to complete the necessary information, including but not limited to the individual's name, email address, phone number, educational background, registration identification, and area of expertise. The specialty field presents a selection menu featuring various medical disciplines, including but not limited to Allergy and Immunology, Anesthesiology, Cardiology, Dermatology, Endocrinology, Nephrology, Neurology, Obstetrics and Gynecology, Pathology, Pediatrics, Radiology, and Urology. Upon completion of filling in the necessary details, the physician may proceed to finalize the registration process by selecting the "sign up" option.

The individual may also register by utilizing the appropriate sign-up feature and supplying the necessary information, including their email address, full name, mobile phone number, date of birth, and gender. Upon selecting the sign-up button and creating login credentials, the patient's particulars are subsequently gathered. The system can be accessed by the actors through the sign-in screen by providing valid credentials.

The act of managing one's profile within the operational framework encompasses the ability to modify the current password. The database responsible for managing login credentials is maintained by the cloud service provider, specifically AWS or Amazon Web Services as illustrated in this instance. The utilization of cloud technology is employed for the purpose of hospital authentication and storage of login credentials, including usernames and passwords. As a result, the cloud-based database is utilized for the management of profile functionality, facilitating the modification of user profile attributes.

Access to the Doctor/Hospital operation frame is contingent upon satisfactory verification and authentication of the information provided on the sign-in page. The operational framework utilized by the hospital, doctor, and patient is characterized by a comparable menu. The available options on the menu comprise of three distinct functionalities, namely managing, uploading, and downloading. The "manage" function enables the user to oversee their profile and associated credentials. The remaining operations, namely "upload" and "download," will be addressed in subsequent stages of the approach.

Step 2: EHR Upload – The Electronic health records of the person being treated can be submitted and retrieved by the healthcare facility, the medical professional and the patient. During the first stage, the physician is permitted to upload the Electronic Health Records (EHRs) of the patient. This phenomenon can be attributed to the patient's initial encounter with the physician, which subsequently leads to the generation of medical records. The document encompasses a range of parameters pertaining to the patient's visit, including symptoms, diagnosis, and prescribed medication provided by the physician.

Upon generating the electronic health record (EHR) file of the patient, the physician will proceed to employ the upload option in the menu to transfer the file. The upload functionality initiates a new frame containing the browse file option, which enables the utilization of the `jfilepicker` class by the java code to browse and choose the relevant file. Upon selecting the file, it may be uploaded by clicking the designated "upload file" button. This

action will initiate the transfer of the document to the cloud via a specialized s3 bucket provided by Amazon Web Services.

Step 3: Blockchain Formation and Cloud Storage – The file submitted by the doctor needs to be safeguarded before it is uploaded to the cloud. The initial encryption of the file employs the AES encryption standard for the purpose of ensuring the security of its contents. However, this measure alone does not suffice to discourage potential attackers. Consequently, the integration of a distributed platform based on Blockchain technology provides an additional layer of security. The electronic health record (EHR) file that has been encrypted undergoes a hashing process utilizing the SHA256 algorithm in order to obtain the key. In order to produce a less lengthy key, the modulus operation eliminates a random selection of the initial seven characters from the long key that has been generated through this process. The Head Key is commonly referred to as such owing to its notable significance. Algorithm 1 outlines the process for generating a key.

Algorithm 1: Block Head Key Generation

// Input: Electronic health records E_R

// Output: Head Key H_{KY}

Function: headKeyGenerator (E_R)

0: Start

1: $H_{KY} = \emptyset$

2: $S_{KEY} = \text{SHA256}(E_R)$

3: $X = S_{KEY} \text{ MOD } 7$

4: **If** $X < 7$, **then**

5: $Q = X + 1$

6: **for** $i = 0$ **to** $H_{KY} \text{ length} < 7$

7: $i = i + Q$

8: **if** $i < H_K \text{ length}$, **then**

9: $H_{KY} = H_{KY} + S_K[i]$

10: $S_K = \text{rotate}(S_K)$

11: **end if**

12: **else**

13: $i = 0$

14: **end for**

15: **end if**

16: **return** H_{KY}

17: Stop

The head keys utilized for successive file uploads are produced through the application of SHA256, with indistinguishable parameters calculated and affixed to the head key of the previous transaction during every repetition of the uploading of files process. The aforementioned process is executed on every occasion when a novel Electronic Health Record (EHR) is transferred to the cloud. The ultimate phase of this procedure is fortified by a master key, which is securely preserved in a designated location. The database maintains a comprehensive log of files, including file identification numbers, file names, usernames, user types, date and time stamps, and block header keys.

Upon the completion of the data recording process on the blockchain, the information is subsequently transferred to Amazon's s3 bucket, which is accessed through the user interface of Amazon Web Services. The file that has been uploaded is deemed trustworthy and can be efficiently shared with the insurance agent.

Step 5: EHR Sharing with Insurance Agent – It is imperative to ensure the safeguarding of the file uploaded by the medical practitioner prior to its transmission to the cloud. The blockchain approach was employed in the preceding stage to accomplish this task. The insurance agent needs to register into the system before being able to effectively utilize the secure sharing of the EHR approach. The Insurance agent provides the basic information for the purpose of achieving the effective realization of the registration process. Once the details provided by the insurance agent are validated, they are stored on the database on the cloud.

The insurance agent can now utilize these credentials that will be authenticated and the insurance agent will be given access to the stored EHR files. The access key for the files will be provided. The files that have been uploaded can be accessed through the download menu located within the operation frame. Upon the appearance of the Download Frame, the files that have been uploaded to the s3 bucket are retrieved and presented to the user in a tabular format. The table presents data pertaining to the file title, as well as the time and date of upload,

specifically for the patient in question. To obtain the file, one must choose the respective file from the table and initiate the download process by selecting the designated button. The electronic health record (EHR) document is retrieved from the Amazon S3 storage service and subsequently decrypted to enable insurance agent access and viewing.

The files are continually being verified using the bitmapping protocol for the integral state of the files. The integral state is confirmed through the evaluation of the avalanche effect. Once the avalanche effect is identified through the bitmaps, the key agreement protocol utilized for providing the access to the insurance agent is revoked. This causes the malicious insurance agent to lose the access to the files, preventing any further manipulation. Therefore, the EHR shared with the insurance agents is secured through the revocation of the key agreement protocol.

IV. RESULTS AND DISCUSSIONS

The programming language Java was utilized in conjunction with the NetBeans IDE to implement an idea for a system that enables secure sharing of Electronic Health Records (EHR) on the cloud via a key agreement protocol. The employed system utilized a laptop equipped with an Intel i5 processor, 4 GB of RAM, and 500 GB of hard drive space. The MySQL database server has effectively performed its obligations related to managing the database along with storage capacity.

The study evaluated the operational efficiency of a cloud-based electronic health record (EHR) sharing system that employs a key agreement protocol. This was accomplished by conducting a series of comprehensive experiments. The following section elucidates the outcomes of the review and the characteristics employed for the assessment.

A. Character assignment for Encryption Comparison

The effectiveness of the Introduced approach has been evaluated through a series of experiments designed to assess the efficacy of the AES encryption algorithm employed in the suggested technique for encryption and decryption.

The AES algorithm for encryption is widely utilized in diverse networks and data platforms as an established encryption method. The AES is commonly referred to as an asymmetrical encryption technique due to its utilization of distinct key sets for the decryption and encryption procedures. The public key is employed for encryption while the secret key is employed for decryption. The computation of a combination of significant numbers is utilized to derive both the public and private keys. The utilization of a set of number sequences to derive keys for the implementation of the AES cryptographic protocol is a well-established practice.

The evaluation of the encryption efficiency of the suggested model, which relies on the AES algorithm, is conducted via comprehensive experimentation. In each experimental trial, a predetermined quantity of characters is encrypted utilizing a specific technique. The characters have been augmented to comprehend the effect on the implementation of the encryption. By utilizing this particular technique for examination and subsequent accumulation of outcomes, a comparative analysis is conducted between the encryption performance of the present approach and the technique that has been employed in a previous study [13]. Table 1, presented below, displays the outcomes of the exploration and the comparison between encryption methods.

TABLE I: NUMBER OF CHARACTERS UTILIZED FOR ENCRYPTION (AES v/s RCC)

Experiment No.	No of Characters	No of Different Characters (AES)	No of Different Characters (RCC)
1	0	0	0
2	1000	52	40
3	2000	56	53
4	3000	59	52
5	4000	57	56
6	5000	61	55

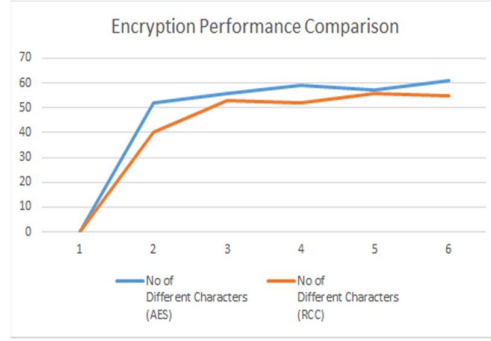


Figure 2 : Plot of the number of characters utilized for encryption in AES v/s RCC encryption techniques

The findings provided demonstrate that the AES encryption method utilizes a notably greater quantity of characters in the encryption process, in comparison to the RCC encryption approach outlined in reference [13]. Figure 2 represents a graphical representation of the tabulated outcomes.

The graphical representation depicted in Figure 2 accentuates the advantages of utilizing the RSA encryption technique expounded in the recommended approach as opposed to the RCC encryption technique delineated in reference [13]. The AES encryption algorithm utilizes a greater number of characters for encryption, thereby increasing the level of sophistication of the procedure and ultimately improving the security measures by a significant degree. The increased complexity of encryption techniques enhances the level of resistance against potential attacks, thereby leading to a substantial boost in security.

B. Scalability Analysis of Blockchain Transaction

The demonstrated technique of sharing EHR through the usage of key agreement protocol is evaluated for the scalability of blockchain operations. In order to achieve this goal, an experiment is run where various EHRs are used to create the blockchain numerous times. Every time a new EHR is uploaded to the cloud storage, the blockchain is updated. After which, the number of blockchain transactions is calculated every second. The results are tabulated in table 2 and a corresponding plot is shown in figure 3.

The acquired result is contrasted with the findings of [14], in which blockchain technology was used to preserve the accuracy of vote data. This is comparable to the way we went about creating the blockchain—we used several EHR files rather than multiple votes to do this. The votes in [14] are comparable to the EHR files used in our key agreement protocol for sharing with the insurance agent, incurring the same computational cost when blockchain transactions are performed.

The outcome in [14] offers a transaction rate of 23.01 transactions per second for a single client. As seen in Table 2, the proposed strategy results in a blockchain transaction rate of about 12.28. The comparison of the approaches is depicted in table 3 and illustrated in the figure 4. The implementation of the key agreement protocol, which enables a secure implementation while preserving the performance of the blockchain, accounts for a large portion of the difference between our approach and the technique of [14], making the suggested model superior to that of [14].

TABLE II: BLOCKCHAIN TRANSACTION TIME ESTIMATION TABLE

S no.	Number of EHR files	Blockchain Transaction time	Transaction per second
1	100	1122	11.22
2	200	2365	11.825
3	300	3891	12.97
4	400	4937	12.3425
5	500	6543	13.086

TABLE III: COMPARISON OF BLOCKCHAIN TRANSACTION PERFORMANCE

Methodology	Transaction time (in seconds)
Our Approach (Key agreement based EHR Blockchain)	12.28
Evoting Blockchain approach in [14]	23.01

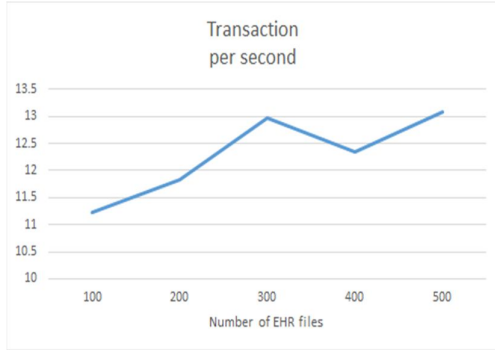


Figure 3: Transaction per Second

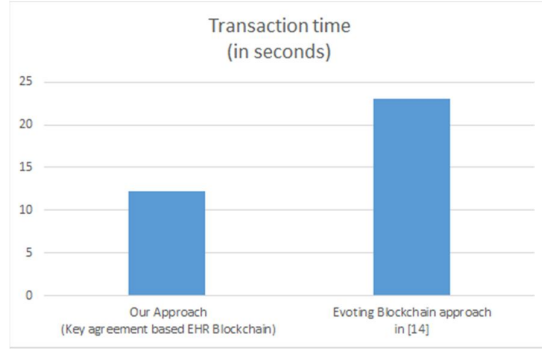


Figure 4: Comparison of Blockchain transaction performance

V. CONCLUSION AND FUTURE SCOPE

The presented approach for the purpose of achieving the revoking of key agreement protocol for the sharing of the patients E-health records have been presented in this research article. The presented approach initiates with the realization of the user registration and login that is performed for the doctor as well as the hospital. The registration is performed for the doctors by taking in their various attributes such as name, DOB, email mobile number etc. The user attributes are validated and then the respective username and password provided at the time of registration can be utilized for the purpose of achieving the access into the system. The hospital itself can perform the registration too and login into the system. The doctor as well as the hospital are tasked with the uploading of the relevant E Health Records of the patient. Once the records are uploaded into the system, the system encrypts these records and converts it into a blockchain before storing the blockchain on the cloud using the Amazon RDS service. The EHR can be shared with the insurance agent on the time of audit where the access key is provided and can be used to access these files. But if the insurance agent performs any modification or tampering on the EHR data, the bit mapping protocol in charge of maintaining the integral state is triggered and the key agreement protocol is revoked. The approach has been tested for its effective realization and implementations which has been proven to be effective with satisfactory results.

REFERENCES

- [1] 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.
- [2] 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.
- [3] 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.134393134412,2020,doi:10.1109/ACCESS.2020.3011201.
- [4] 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.
- [5] 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.

- [6] 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.
- [7] 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.
- [8] 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.
- [9] 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.
- [10] 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.
- [11] 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.
- [12] 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.
- [13] E. R. H. P. Isaac, J. H. R. Isaac and J. Visumathi, "Reverse Circle Cipher for personal and network security," 2013 International Conference on Information Communication and Embedded Systems (ICICES), Chennai, India, 2019, pp. 346-351, doi: 10.1109/ICICES.2013.6508354.
- [14] Kashif Mehboob Khan, Junaid Arshad, Muhammad Mubashir Khan " Investigating Performance Constraints for Blockchain Based Secure e-Voting System", Published by Elsevier B.V, 2019.