IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Enriching Security of Medical IOT Data in Cloudthrough Blockchain

[1] Shruti Chaudhari, [2]Piyush Rawool, [3]Shreyas Gawade, [4]Shreya Aralimar, [5]Snehal Thorave

[1]Student, [2] Student, [3]Student, [4]Student, [5]Guide,
[1]Computer Department,
[1]Dhole Patil College of Engineering, Pune, India.

Abstract — **The rapid pace of advancement in the perspective of healthcare phenomenon has been accelerated with the recent pandemic. There has been a greater focus over the medical aspects of the environment and diagnostics that has made people and other healthcare professionals more aware about their wellbeing. It has been noticed that a large assortment of devices have been developed in the last decade that facilitate the monitoring of the patients. These devices have been getting smaller and increasingly accessible to the larger audience and has stepped out of expensive equipment that a large number of regular users can afford these devices. This allows for the larger implementation of such Internet of Medical Things sensors allows for remote diagnosis and consultation which is widely believed to be an efficient form of development. But such devices due to their footprint can become increasingly insecure and this is reason this approach defines an effective mechanism for increasing its security. The proposed approach implements, RCC encryption and Amazon RDS along with bit mapping and forensic report generation to achieve increased security for the IoMT data which has been quantified through rigorous experimentations.**

Index Terms* - *Internet of Medical Things, Public Cloud, Medical Health Records, Cryptography, Search over encrypted data.

I. INTRODUCTION

Human health requirements are met through medical systems, and that as the aging of the population, those needs become ever more critical. Humans may also see the importance of real-time knowledge in situations like the most current epidemic. In terms of epidemics, information on a patient's condition, which including warmth or discomfort, is very helpful. The elderly workforce and the prevalence of chronic conditions have increased health awareness and the demand for superior patient care. Nowadays, the trend is for consumers to prefer patient-centered healthcare than traditional healthcare. Increasingly, patient- and hospital-centered treatment has lost in favor of electronic and mobile-based medicine that has developed towards national coverage. Considering current technological advancements like that of the Internet of Medical Things, it is now feasible to reliably and quickly obtain practically all types of marketing knowledge. Whereas more cost-effective and cost-effective procedures have been made possible by mobile and ubiquity equipment, new challenges have been brought forth by portable and web-enabled IoMT equipment.

Ensuring the integrity of all internet-enabled equipment is the biggest problem in the technological and all-pervasive medical industry. Many networks today are built for using smart phones to offer customers services that are mobile-centric. A staggering quantity of healthcare data is created and transferred every day, every week, and so forth as a result of the significant expansion of Internet-based medical equipment and apps. The existing health care infrastructure may have specific strengths, but it also has some drawbacks. The majority of these drawbacks are related to costs, technology, standardization, psychological attitudes, and organizational restraints.

The contemporary decentralization methodology Blockchain offers reliable answers to the security and dependability problems in the healthcare sector. The absence of middlemen seems to be another compelling feature of blockchain technology. In current history, blockchain has been utilized to create different techniques and routes outside of cryptocurrencies. This represents a revolutionary frequency of distribution that eliminates the need for middlemen, and it may be the entrance to health care. Assimilation of blockchain technology into smart healthcare, taking into account all privacy-related issues, the reliability of wellbeing, and customer and IoMT internet connectivity.

The present state of blockchain acceptance and interoperability, particularly in the healthcare industry, is demonstrated by Sabita Khatri [1]. Additionally, there is little doubt that Blockchain has great promise for something like the creation of safe, more decentralized physician systems with exceptional amounts of data handling and administration. This report's main goal is to enlighten contemporary blockchain-based advances in medicine. With a predetermined process, many performance indicators were examined and assessed in accordance with the study objectives. The study's findings demonstrate the expanding tendency in blockchain healthcare. Healthcare institutions look for novel and improved ways to protect confidentiality and trustworthiness.

The goal of Emeka Chukwu [2]'s investigation into the condition of blockchain technology as it relates to medical studies is to identify any latest innovations. They displayed the variety of public blockchains used by the publications that assessed. This report has shown that, despite an increase in awareness in blockchain in medicine and academia, the majority of submitted research are indeed theoretical, frameworks propositions, and exploratory designs with little actual execution or piloting. This article summarizes the state-of-the-art for blockchain technology in healthcare and outlines practical application cases. This investigation demonstrates that high costs, poor overall functionality, and poor durability continue to be significant barriers to adopting a sustainable blockchain in the medical industry, as well as in several other industries.

EHR sharing plans, according to Zhen Pang [3], are crucial for ensuring that patients receive thorough and correct care. EHR sharing programs can compel communication process between institutions and advance the field of medicine. Since the EHR comprises a wealth of details, organizations must safeguard private information while exchanging data. The suggested technique can guarantee the veracity and safety of the shared information since it maintains data together on and off-chain. The multi-keyword privacy preserving method used in this study can increase the cipher text’s effectiveness and precision.

The Section 2 of this paper is all about the past works named as related works whereas on the other hand Section 3 Discuss the detailing about the current deployment of the Idea with the name proposed methodology. Obtained results are evaluated in section 4 as Results and Discussions. This Research paper is terminated with the section 5 Conclusion and future scope.

II. RELATED WORKS

According to Alaa Haddad [4], Blockchain technology is generating a significant amount of awareness from individuals and businesses of all different sizes. It really can change the traditional sector with its qualities, which would include decentralization, confidentiality, permanence, and verifiability. Technologies for blockchain are anticipated to leverage artificial intelligence to transform the medical industry. The method would indeed be transparent and secure, but it likely also increase patient outcomes while lowering costs. In the proposed methodology, they discussed several internet technologies used in the healthcare sector and listed the most significant ongoing and future research initiatives.

Information privacy is a significant concern for most source systems, according to Vikas Jaiman [5]. Data tenderers must adhere to GDPR including data suppliers' authorization in the aspects of data transfer. Researchers discovered that efforts to make data exchange without user permission easier are still in the early stages. In this paper, researchers presented a methodology for information sharing with data suppliers' express permission. They incorporate a standardized metaphysical authorization and information access paradigm using the DUO as well as ADA-M models. To establish a general permission framework, they created a smart contract, which was then implemented and validated on LUCE, the permissioned service.

The subject of the present current state of the science in blockchain-based EHR administration development and potential possibilities is addressed by Abdullah Al Mamun [6]. Researchers displayed the proportion of public blockchains and kinds employed by the publications under examination. Whereas the significant benefits of using blockchain for administer EHRs have exceeded expectations of stakeholders inside the medical fields, they also discovered that a number of problems still need to be thoroughly investigated. For example, different and sometimes contradictory laws may make it difficult to share Electronic health records internationally. Additionally, regulations differ according to the precise government policy. Therefore, more research on EHR legislation, standardization, and international availability is essential.

In perspective of EHR custodianship, EHR collaboration, and EHR architecture, Rahul Ganpatrao Sonkamble [7] discusses the significance of EHR interconnectivity for integrated medical care. This study includes a thorough analysis of huge data repositories for EHR modelling, accessible protocols for EHR understanding, and medical semantics for representation of knowledge in EHRs. This aids in the analysis of the way the varied architecture of EHRs and the difficulties of non-uniform interpretations have been handled in the literary works for data integration. Employing measurement systems and consistent criteria, a comparison of data warehouses is made to reflect the heterogeneity EHR architecture.

According to Bandar Alamri [8], the key benefit of employing BC is the removal of dependence on a particular reliable third - party provider. The outcomes demonstrate that all investigations that suggested authentication mechanism preferred the decentralized trustworthy implemented sustainable, despite the fact that BC may offer 2 identity and access management frameworks and decentralized trustworthy identification. There seem to be two crucial factors in the review process that should be noted. The possible improvements were often contrasted with other strategies based on some other BC alternatives, even if a handful of research studies revealed positive outcomes according to the performance reviews completed in the research. It is accurate that something might indicate how well the program is doing, but that would not imply that the application fulfils the safety criteria.

A blockchain-based HIE platform called MEXchange, introduced by Deoksang Lee [9], uses the ring verification and stealthy addresses to solve the reasoning challenge. They put the suggested framework into practice as a concept and assessed it both quantitatively and qualitatively. Researchers also looked at potential risks to the suggested strategy. In conclusion, this seems to have strengths in terms of dependability, secrecy, consistency, anonymity, and visibility, but downsides in terms of higher transactional delay and reduced TPS when comparable to the current blockchain-based HIE. The strategy excels in the confidentiality area in especially by avoiding the assumption issue.

According to Rui P. Pinto [10], the major goal was to understand the viability of putting into practice a platform combining m-health with distributed ledger technology with techniques for healthcare information accountability while maintaining confidentiality and making it possible to promote healthcare information proprietorship. The processes and techniques that integrate distributed ledgers with m systems or make an endeavor to enhance EHR systems utilizing blockchain were analyzed in order to achieve the specified criteria. This assessment made it sufficiently transparent that now the suggested organization needed to include a database constituent to stockpile off-chain information that is impractical to purchase in the blockchain as a whole, a blockchain constituent to take opportunity of unchanging transaction control's beneficial features, and an implementation to facilitate interaction among both the system and the user.

The privacy needs of a decentralized, multilateral verification strategy for blockchain-based platforms were taken into consideration when Manjunath Hegde [11] introduced the DDMIA identification technique. The person can start a treatment after registering with an online health care professional. The patient may be referred by the e-health practitioner to any e-health providers for the necessary care. The individual is mutually authenticated and is not necessary to subscribe continuously. A blockchain-based e-health network's privacy criteria have been established, and the DDMIA mechanism was theoretically and crypt analytically validated.

A blockchain-based infrastructure for exchanging healthcare information relying on HL7 FHIR Specifications is proposed by Ye Seul Bae [12]. By addressing issues with confidentiality, transparency, and confidence, the implementation of distributed ledger technology could boost consumers' confidence in the transmission of information. This Health Pocket framework may recycle information for a number of solutions with ubiquitous and standardized elements by utilizing the suggested strategy. The poor ratings for observed usability and simplicity of being used are among the study's limitations.

The blockchain connector configuration to share information with blockchain, procedure the transmitting medical record, offer additional user interfaces with graphics for consumers to get a visual presentation of the communication with the blockchain network, and 2 layers of protection configurations to guarantee that now the hospital HIE is achieved, according to Yan Zhuang [13].

III. PROPOSED METHODOLOGY

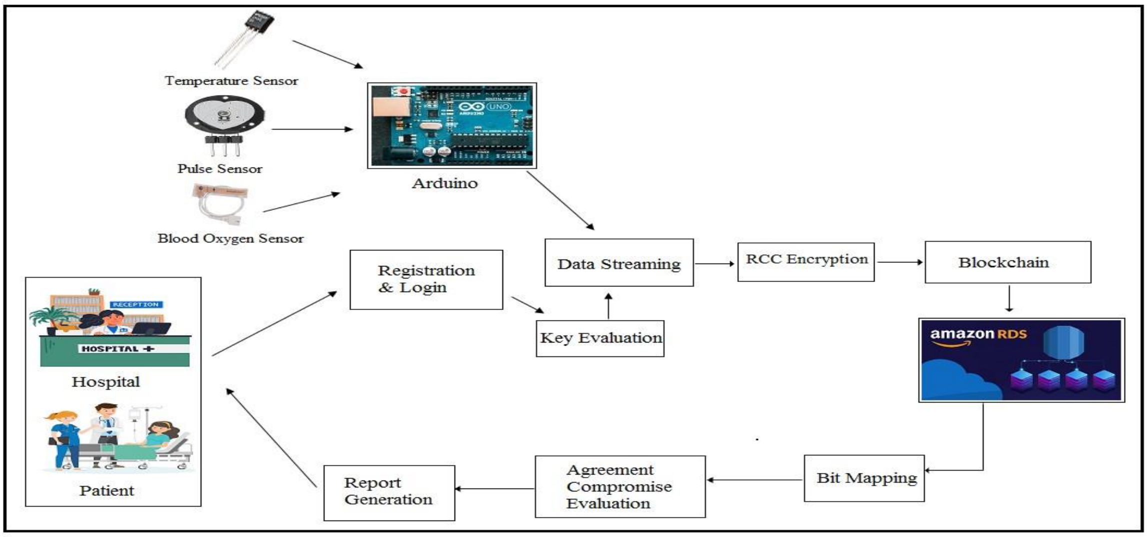


Figure 1: System Overview

The Proposed approach for the purpose of securing the Medical IoT data on the cloud platform has been illustrated in the figure 1 given above. There are a number of different steps that are being utilized for the purpose of achieving this system which are discussed below.

Step 1: Admin Registration and Login– The presented technique has been designed in the form of an attractive Graphical user interface that is developed using the swings framework for java. This interactive interface can be utilized by the admin to gain access into the system to perform the various different activities of this methodology. If the admin is accessing the page for the first time, the sign up page can be utilized to create an account. The sign up form takes information such as name, email id, mobile number, qualification, registration number, specialty, and years of experience, username and password. Once these details are verified, only then the account is created and the admin can use the login credentials to gain access into the system.

For the purpose of logging in, the admin provides the relevant username and the password for the authentication. Once the admin has been authenticated, the operation frame is displayed. There are a number of different operations that can be performed by the admin in this operation frame.

In the operation frame, the admin can manage their profile which allows for an option to change the current password. As the database for the storage of the login information is on the cloud provider, which in this case is AWS or the amazon public cloud. The verification of the admin and the storage of the username and password credentials is performed on the cloud. Therefore, the manage profile option to change the attributes of the user profile is also performed on the cloud database.

The admin also has the capability to initiate the data streaming from the IoT sensors by accessing the data storage menu. The data storage menu has a sub menu named as data streaming, which will be used for the purpose of collection of the data from the sensors. Once the data streaming option has been selected by the user, they are greeted with another page that has two buttons, start data streaming and the stop data streaming buttons. The start streaming option button once clicked will initiate the data collection process from the sensors, whereas the stop data streaming option will stop the data streaming. The data streaming from the sensors will be discusses in the next step of the approach.

Step 2: Sensor Data Streaming – Starting a data stream is the first step in beginning sensor data gathering. The sensor values will be gathered when the user presses the start data streaming button. Step one in the process involves hooking up the Arduino UNO microcontroller to the computer acting as the development platform. For the purpose of integrating the sensors and collecting data, an Arduino UNO microcontroller is being used. This set-up employs a number of sensors, including those that measure heart rate and skin temperature. The very same sensors are connected to an Arduino microcontroller and then programmed to gather and transmit data to a laptop computer.

The sensor values from the microcontroller are gathered and the java code is started. With this goal in mind, an easy-to-use graphical user interface (GUI) has been developed to kick off the sensor data collection mechanism. When this option is activated, a thread is launched that waits for sensor values to be delivered over the COM4 port. The heart rate sensor, and temperature sensor readings are all collected by the thread and entered into a database with the present date and time. It will continue indefinitely so long as the thread is open. To temporarily halt the collection of sensor data, the user may hit the stop button upon that interface, which immediately terminates the thread.

Step 3: Sensor Data Encryption and Cloud Storage – The sensor data transmitted in the preceding phase is used as an input in this stage, including the time and date to be encrypted. For this reason, the Reverse circle Cipher Encryption protocol is used, and the encryption keys are created.

A symmetric encryption key is included in code for security purposes. When this key is provided to the RCC method, new keys can be generated and used to conceal the sensors' identities. The sensor values are effectively collected and transferred to the

Reverse Circle Cipher – One of the many extremely effective cryptographic methods that may be utilized with a cloud service is the Reverse Circle Cipher. The RCC method involves first rotating the incoming characters exactly anti-clockwise or clockwise, then substituting the appropriate characters. The presented method does this by segmenting sensor data and then rotating each segment to encode content. The encryption is carried out correctly by the Reverse Circle Cipher, and the encrypted data is then uploaded to a remote server. When it comes to encrypting sensitive information and keeping it private, the Reverse Circle Cipher is a top contender. It is all laid out in Algorithm 1 underneath for Reverse Circle Cipher Encryption.

ALGORITHM 1: Reverse Circle Cipher

```
// Input: Sensor Data $S_D$
// Output: Sensor Cipher Data $S_{CD}$
Function reverseCircleCipher ($S_D$, KEY)
Start
Initialize list Block $LST_{BLK}$ =∅, $DIV_{STR}$=””, addupval=0
    for i = 0 to size of KEY
        addupval= addupval+ASCII ($KEY_{[i]}$)
    end for
    addupval= addupval MOD 20
    for i = 0 to size of $S_D$
        char ch= $S_{D\,[i]}$
        $D_{STR}$ = $D_{STR}$ +ch
        if ($D_{STR}$ size =10), then
            $LST_{BLK}$ = $LST_{BLK}$ + $D_{STR}$
            $D_{STR}$ =””
        end if
    end for
    $LST_{BLK}$ = $LST_{BLK}$ + $D_{STR}$

    For i = 0 to size of $LST_{BLK}$
        STR= $LST_{BLK\,[i]}$
```

```
            STR=rotate (STR, i)
                For j = 0 to size of STR
                    char ch= $STR_{[j]}$
                    newchar=ASCII(ch) + addupval
                    $S_{CD} = S_{CD} +$newchar
                end for
        end for
return $S_{CD}$
STOP
```

Step 4: Blockchain Formation – The Sensor readings must be secured before being transmitted to the cloud server. Thus, the Blockchain was built to accommodate this requirement. The SHA256 hashing method is used to produce the key using the sensor values and the current date and time. The mod operation takes the lengthy key obtained in this way and randomly removes the first seven characters to get a shorter key. Because of this, the Head Key is the name often given to this particular key. In algorithm 1 we see how the keys are generated.

Algorithm 1: Block Head Key Generation

```
// Input:  Sensor Readings with Date and Time $SR_{DT}$
// Output: Head Key $H_K$
Function: headKeyGenerator ($SR_{DT}$)
Start
$H_K$ =Ø
 $SH_{KEY}$=SHA256 ($SR_{DT}$)
        N=$SH_{KEY}$ MOD 7
    If N<7, then
    P=N+1
            for i=0 to $H_K$ length < 7
                i=i+P
                if i < $H_K$ length, then
                    $H_K = H_K + SH_K$ [i]
                    $SH_K$ = rotate ($SH_K$)
                end if
        else
                i=0
            end for
        end if
return $H_K$
Stop
```

Every time the sensor data streaming is performed, the very same parameters are calculated and added to the previous transaction's head key, and the whole hash key creation procedure is performed using SHA256 to produce the following transaction's head key. This is repeated for every instance of the sensor data collection and cloud streaming, and the final operation is secured by the master key, which is stored in a separate database for confidentiality

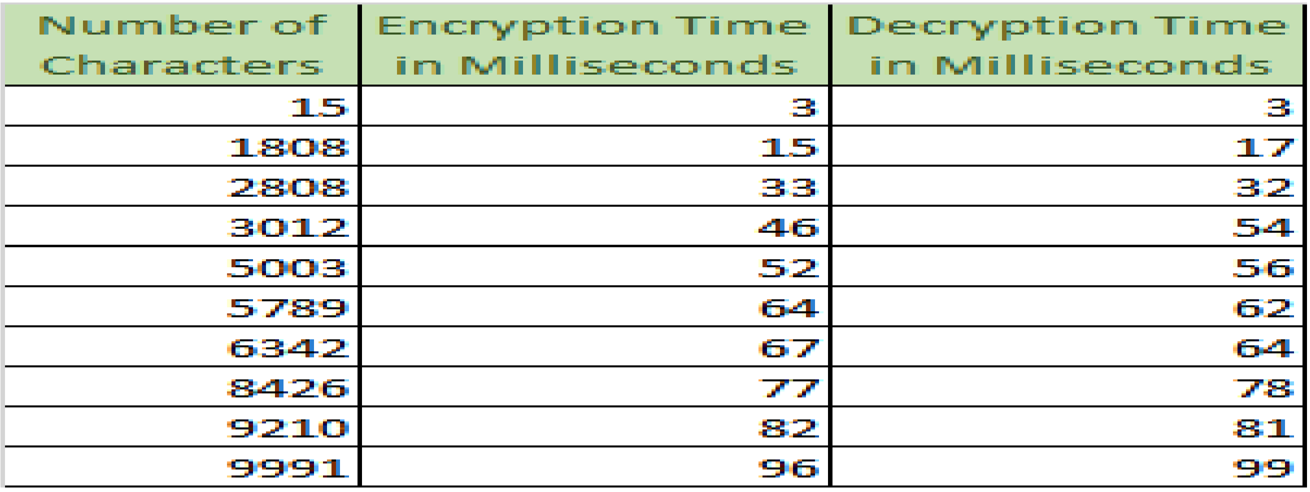
After the data is converted in to a blockchain, it is transmitted to the Amazon cloud via the AWS or Amazon Web Services interface. To accomplish this, click the "create table in cloud" button, and a new table will be created in your MySQL database on the Amazon app. The encoded sensor readings are stored in this table and may be viewed via the view history submenu of the data storage interface. Following the following procedures, the user will be able to decrypt and see the sensor values.

IV. RESULT AND DISCUSSIONS

The proposed technique for Securing medical IOT data in the public cloud is built in Java through using NetBeans Integrated Development Environment. A Windows laptop with an Intel Core i5 processor and 8 GB of RAM and 1 terabyte of storage space is perfect for employing this method. The data from the different sensors is being transmitted into the Arduino UNO microcontroller. The sensor readings are being uploaded to an Amazon S3 cloud database.

Encryption and Decryption Time performance

The proposed method uses encryption and decryption methods to ensure the sensor values remain private throughout their journey to the cloud database. This strategy's effectiveness may be assessed by following the steps provided in this section. The amount of time spent on encryption and decryption can be seen in Table 1, which is broken down by character count.



Number of Characters	Encryption Time in Milliseconds	Decryption Time in Milliseconds
15	3	3
1808	15	17
2808	33	32
3012	46	54
5003	52	56
5789	64	62
6342	67	64
8426	77	78
9210	82	81
9991	96	99

Table 1: Encryption and Decryption time performance

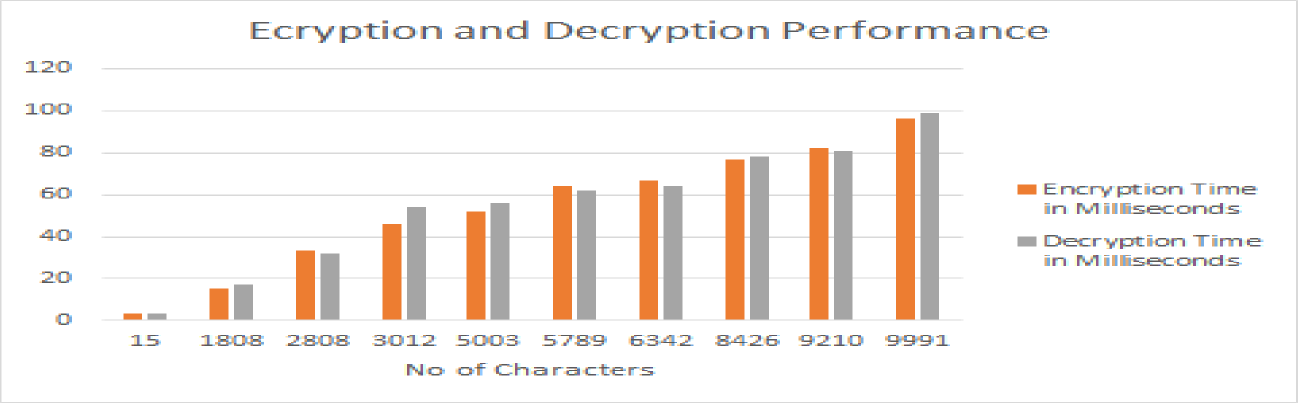


Figure 2: Encryption and Decryption Time

Figure 2 above is an acceptable bar graph retrieval for visual inspection of the data presented. Clearly, the time required to encrypt and decode is not proportional to the amount of input characters. This is due to the extensive research and practical use of the encryption method employed for this approach, the reverse circle cipher. This is the reason why the efficiency statistics indicates that the plan is being implemented quite well.

V. CONCLUSION AND FUTURE SCOPE

The latest epidemic has hastened the already quick pace of innovation in the field of medicine. Individuals as well as other medical practitioners are now more conscious of their wellness as a result of a stronger emphasis on the medical elements of the environmental and examinations. It has recently been noted that a wide range of gadgets that make patient surveillance easier have indeed been produced in the past ten years. Since these gadgets are no longer pricey pieces of hardware, a bigger population may now afford them thanks to their decreasing size and increased accessibility. This makes it possible for the Internet of Medical Things sensors to be used more broadly, enabling remote diagnosis and consultation, which is widely regarded as an effective method of development. However, these devices can become more and more insecure due to their footprint, which is why this approach defines an efficient mechanism for enhancing its security. In order to provide enhanced security for the IoMT data, which has been measured through rigorous experimentation, the suggested strategy utilizes RCC encryption and Amazon RDS coupled with bit mapping and forensic report production.

The future work can be done in the direction of enabling this approach in mobile application for effective and robust security of the medical IoT data in villages or other remote locations.

REFERENCES

[1] S. Khatri, F. A. Alzahrani, M. T. J. Ansari, A. Agrawal, R. Kumar and R. A. Khan, "A Systematic Analysis on Blockchain Integration With Healthcare Domain: Scope and Challenges," in IEEE Access, vol. 9, pp. 84666-84687, 2021, doi: 10.1109/ACCESS.2021.3087608.

[2] E. Chukwu and L. Garg, "A Systematic Review of Blockchain in Healthcare: Frameworks, Prototypes, and Implementations," in IEEE Access, vol. 8, pp. 21196-21214, 2020, doi: 10.1109/ACCESS.2020.2969881.

[3] 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.

[4] A. Haddad, M. H. Habaebi, M. R. Islam, N. F. Hasbullah and S. A. Zabidi, "Systematic Review on AI-Blockchain Based E-Healthcare Records Management Systems," in IEEE Access, vol. 10, pp. 94583-94615, 2022, doi: 10.1109/ACCESS.2022.3201878.

[5] V. Jaiman and V. Urovi, "A Consent Model for Blockchain-Based Health Data Sharing Platforms," in IEEE Access, vol. 8, pp. 143734-143745, 2020, doi: 10.1109/ACCESS.2020.3014565.

[6] A. A. Mamun, S. Azam and C. Gritti, "Blockchain-Based Electronic Health Records Management: A Comprehensive Review and Future Research Direction," in IEEE Access, vol. 10, pp. 5768-5789, 2022, doi: 10.1109/ACCESS.2022.3141079.

[7] R. G. Sonkamble, S. P. Phansalkar, V. M. Potdar and A. M. Bongale, "Survey of Interoperability in Electronic Health Records Management and Proposed Blockchain Based Framework: MyBlockEHR," in IEEE Access, vol. 9, pp. 158367-158401, 2021, doi: 10.1109/ACCESS.2021.3129284.

[8] B. Alamri, K. Crowley and I. Richardson, "Blockchain-Based Identity Management Systems in Health IoT: A Systematic Review," in IEEE Access, vol. 10, pp. 59612-59629, 2022, doi: 10.1109/ACCESS.2022.3180367.

[9] D. Lee and M. Song, "MEXchange: A Privacy-Preserving Blockchain-Based Framework for Health Information Exchange Using Ring Signature and Stealth Address," in IEEE Access, vol. 9, pp. 158122-158139, 2021, doi: 10.1109/ACCESS.2021.3130552.

[10] R. P. Pinto, B. M. C. Silva and P. R. M. Inácio, "A System for the Promotion of Traceability and Ownership of Health Data Using Blockchain," in IEEE Access, vol. 10, pp. 92760-92773, 2022, doi: 10.1109/ACCESS.2022.3203193.

[11] M. Hegde, R. R. Rao and B. M. Nikhil, "DDMIA: Distributed Dynamic Mutual Identity Authentication for Referrals in Blockchain-Based Health Care Networks," in IEEE Access, vol. 10, pp. 78557-78575, 2022, doi: 10.1109/ACCESS.2022.3193238.

[12] 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.

[13] Y. Zhuang, L. R. Sheets, Y. -W. Chen, Z. -Y. Shae, J. J. P. Tsai and C. -R. Shyu, "A Patient-Centric Health Information Exchange Framework Using Blockchain Technology," in IEEE Journal of Biomedical and Health Informatics, vol. 24, no. 8, pp. 2169-2176, Aug. 2020, doi: 10.1109/JBHI.2020.2993072.