iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** IV **Month of publication:** April 2021

DOI: https://doi.org/10.22214/ijraset.2021.33998

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue IV Apr 2021- Available at www.ijraset.com

Integrating Block Chain based Ensuring Security and Privacy of Electronic Health Record Systems using Machine Learning Techniques

M. Vengateshwaran[1], T. Kiruthika[2], M. Nandhini[3]
[1]*Assistant Professor,* [2, 3]*UG Student, Department of Information Technology, Sri Sai Ram Institute of Technology (Autonomous), Chennai, Tamilnadu*

Abstract: ***Nowadays, patients are come to know awareness about their secured medical data which are stored in the personal health record (PHR) system. Multi-party authorization (MPA) involves in multiple parties to access the shared datain cloud with granted permission of user. At this stage, almost standing PHR system are centralized and endangered to the single point failure problem. We provide security analysis and discuss the generalization aspects of our solution.Cryptographic schemes allow the patient to split and share a secret key with a set of trusted parties, such as the healthcare regulatory agency, guardians, and hospitals, in such a way that they can collectively decide on sharing medical data on behalf of patients.The patients can share their PHR with doctors securely. It hold on to track record in the form of Graph and tables so that it can be envisage by the doctor simply.***

Keywords: personal health record, Multi-party authorization, medical data etc.

.

I. INTRODUCTION

Considering how the patients can engage their medical data which tends tomore positive healthcare experience, most of the patients are becoming interested in taking controlover their medical data to be secured.For a PHR system to feasible, it requires to be patient centered, which called for the glad of the health records are no way access, scanned, or revised by any entity other than the patient. Using a deep learning-based architecture in a PHR system,providestransparency,security, andprovenance, andauditable features. In recent years, development of the attributed-based encryption and machine learning technology enables many patients easily to share their conditions with doctors by uploading their personal health record(PHR) files to the cloud servers in e- Medical System. Wildcat access or intentional violation has become one of the social warning that is presented due to the steamy implementation and maintenance of access control systems. The main goal of developing monitoring systems is to reduce health care costs by reducing physician office visits, hospitalizations, and diagnostic testing procedure. Checking the confidentiality of sensitive data is one of the primary requirements of nowadays systems. Access control policies play an animated role in terms of system security.Another study conducted that proposes an access control policy for an electronic health record (EHR) system.The information which requires to be shared is originally encrypted with symmetric keys. Implementation and maintenance systemsof access control policies must be secured enough because if they get compromised, then the internal and external defense systems are no longer be useful. Once the health issue has been increased dramatically to the critical stage and the life of the person is endangered, then they take medical assistance, which can cause an unnecessary waste of their earnings. This also comes into account especially when certain epidemic is spread in an area where the reach of doctors is impossible specifically, the MPA technology can be used to secure the most tactful features against insider attacks that are mostly carried out by the insider acting alone. On the other hand, most of the existing proxy re-encryption schemes used to give secure access to shared encrypted data are centralized and cannot be trusted.Specifically, the main focus of our proposal is to enable decentralized access control for their medical records between a patient and a doctor, along interacting with regulatory agency and guardians too.

II. SYSTEM REVIEW

This paper proposes a narrative access control scheme for personal health record (PHR) data in cloud computing. The scheme uses a attribute based encryption(ABE), hash function and symmetric encryption to realize a fine grained, access control over to PHR. The patients can share their PHR with medical departments. The practical results show the importance of our scheme in terms of storage. Personal health records (PHRs) are valuable assets to individuals because they enable them to integrate and manage their medical data.A PHR is an e- application through which patients can take over their health records. Giving patients control on their medical information offers a merit realignment of the doctor patient active one. However, today's PHR management systems fall short of giving securable patients control on their medical data, which poses serious threats to their metricsMoreover, most of the current approaches and systems leveraged for managing PHR are centralized that not only make medical data sharing difficult but also pose a risk of single point of failure problem.

In this paper, we propose Ethereum blockchain-based smart contracts to give patients control over their data in a manner that is decentralized, immutable, transparent, traceable, trustful, and secure. The proposed one engage decentralized storage of interplanetary file systems (IPFS) and believe in addition to reputation based reencryption oracles to securely fetch, store, and share patients' medical records. We present algorithm with their full implementation details. We evaluate the proposed smart contracts using two important perform calculatios, such as cost and correctness. Further, we provide security survey and discuss the generalization outlook of our solution. We outline the limitations of the proposed approach. We get the smart contract source code publicly on Github.

III. EXISTINGSYSTEM

Individual authorizations to entities and public-key cryptography management help to preserve the privacy of the patient PHR while allowing multiple users to get full access to the data. However, the solution cannot provide partial access to some of the patient records, in addition to being dependent on cloud services for storing the PHR data. The cloud dependency makes the solution architecture centralized, and there- fore it is vulnerable to security attacks, such as the denial of service (DoS), thereby making the entire system unavailable.The owner combines the private key with the receiver's public key to create a re-encrypted key that is sent to the proxy.The proxy downloads the encrypted files and re-encrypts them with the new key and pushes the data to the receiver that is decrypted with the private keys. Through this approach, each new user always requires a new re-encryption key that makes it inefficient.Also, the re-encryption is performed using a centralized server that can-not be trusted in most of the cases.

A. *Demerits*

1) There is no security for multi-party the patient's details are easily retrieved.
2) On a server-side, there is a possibility of server attack where the third party will access the data easily.
3) There is less security in storage part where all the genomic sequence are stored in adatabase canbeeasily retrieved bythethirdparty.

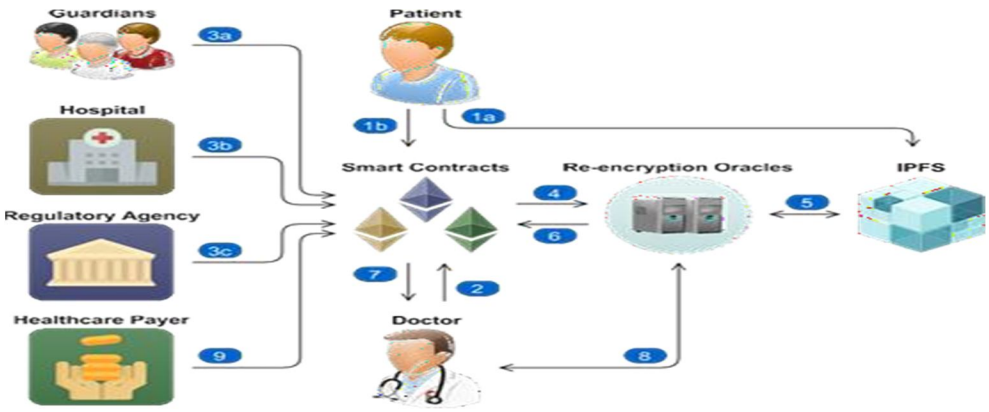
IV. PROPOSEDSYSTEM

In this proposed system where the Patientsrecords coming from several hospitals are encrypted and stored at a data storage site.In this patients data are stored securely in an encrypted format where the local server cannot attack the data.We use different techniques like trapdoor for cryptography, Block chain techniques, AES algorithm, Random forest Classifier in our proposed method.All these operations have to be performed securely. In our system it is easy to claim medical insurance for the patients without any struggle. Once the patient accept the doctor request and the doctor verifies the report and give the prescription according to it.

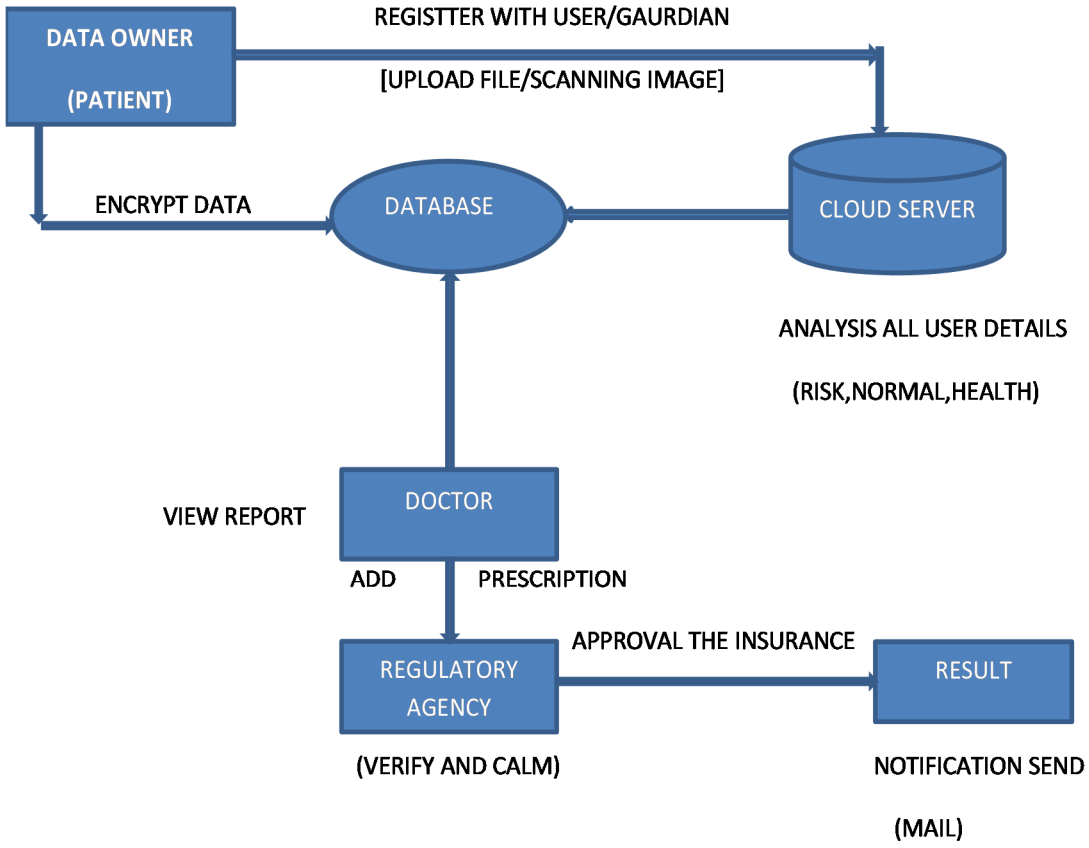
A. *Merits*

1) It is more secure from the local users, where all the patients' genomic sequence arestoredinan encryptedmanner.
2) Highly secured because of cryptographic technique.
3) Time consuming.
4) Best accuracy Model helps in better treatment as early.

V. SYSTEM ARCHITECHTURE



ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue IV Apr 2021- Available at www.ijraset.com



Patients upload encrypted medical document bundle to decentralized storage and submits he bundle hash to the smart connect. Doctor requests medical document through smart contract. Guardians, hospital and regulatory agency generate the re-encryption key and spend the smartcontract. Smart contract emits the medical document bundle and re-encryption key to re-encryptionoracles. Re-encryption oracles request and retrieve the medical document bundle from thedecentralized storage. Smart contract picks a re-encryption oracle and notifies the doctor of the choice.The chosen oracle re-encrypts the bundle from the patient key to the doctor key and sends it to the doctor. The doctor decrypts the bundle, making the medical document viewable.

A. Application

1) Patients don't need to carry their report every time when he/she goes to hospital.
2) It is used to claim medical insurance.
3) Doctor gives the prescription online, so no need to go the hospital.

B. Algorithm

1) *Support Vector Machine:* SVMs are specific linear classifiers which are based on the edge maximization postulate**.** They perform structural risk minimization, which improves the complexity of the classifier with the aim of achieving excellent generalization performance.
2) *Random forest Classifier:* Random forest is a supervised learning algorithm. The "forest" it builds, is an ensemble of decision trees, usually trained with the "capturing" method. The established plan of the capturing method is that union of learning models enlarge the overall result.
3) *Clustering:* Clustering is a Machine Learning technique that implies the assemble of data points. Specified a set of data points, we can use a clustering algorithm to analyzing every data point into a peculiar group.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue IV Apr 2021- Available at www.ijraset.com

VI. SYSTEM MODULE

A. Doctor

1) Register with their own details
2) Login with correct username and password
3) View all patient detail after accept by the patient
4) Scanning image view and give prescription by the doctor
5) Level wise approval to insurance.
6) Logout

B. Patient

1) Register(name, password, email, guardian, personal doctor name,location,specialist,.etc)
2) Login after authorized by the cloud server
3) Upload the file with scanning image
4) View all prescription send by doctor (level-wise)
5) View insurance details
6) Logout.

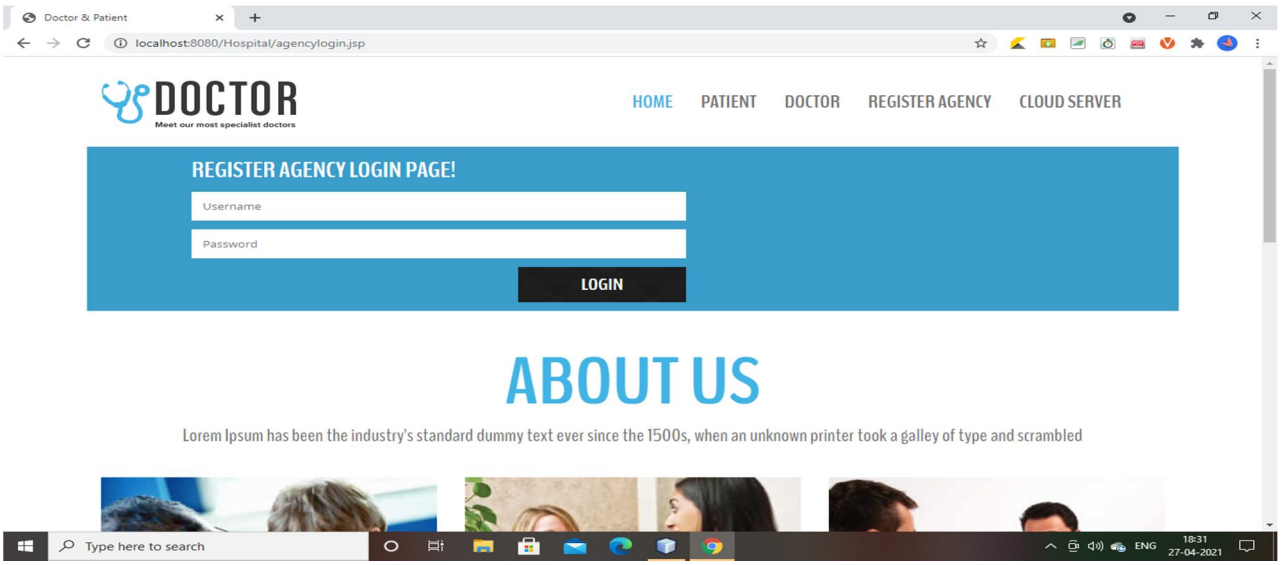
C. Regulatory Agency

1) Login with correct username and password
2) View doctor assigned insurance detail and then, approval the insurance
3) view details of the patient to claim insurance
4) Logout

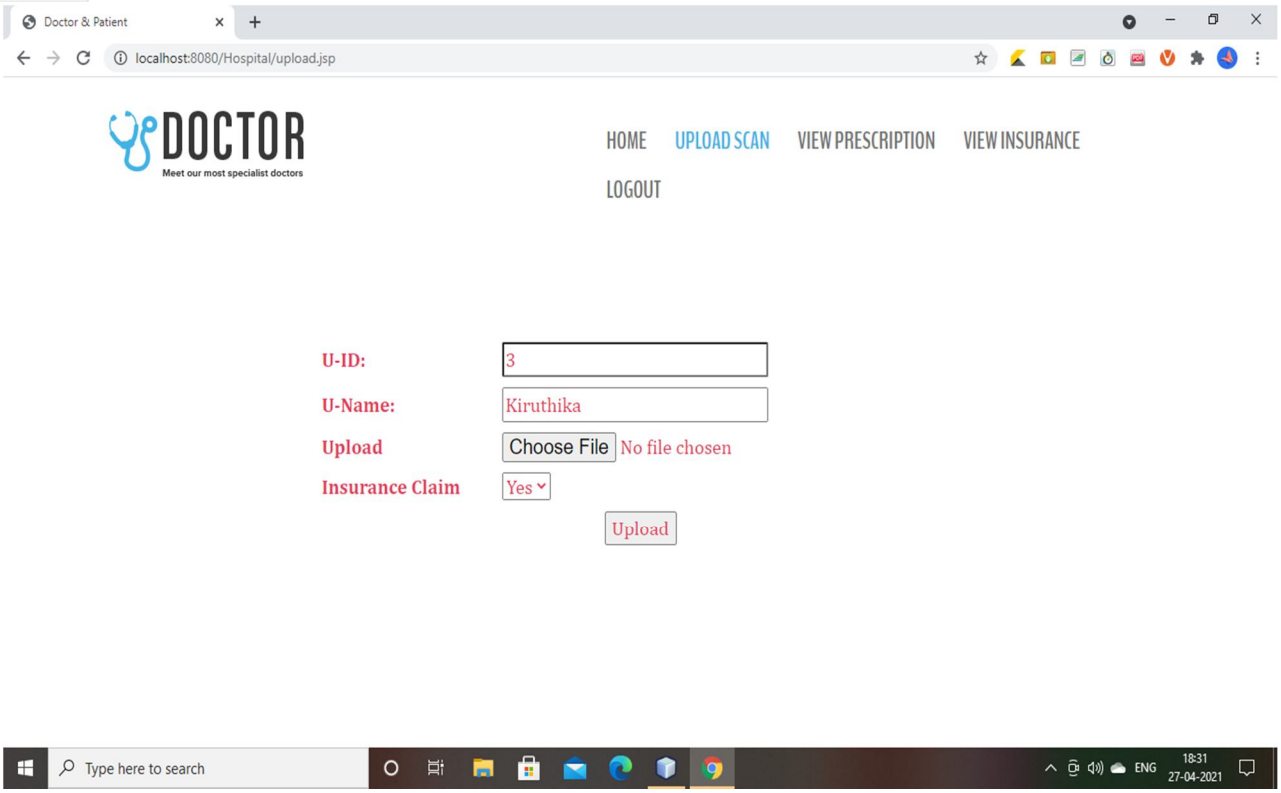
D. Cloud Server

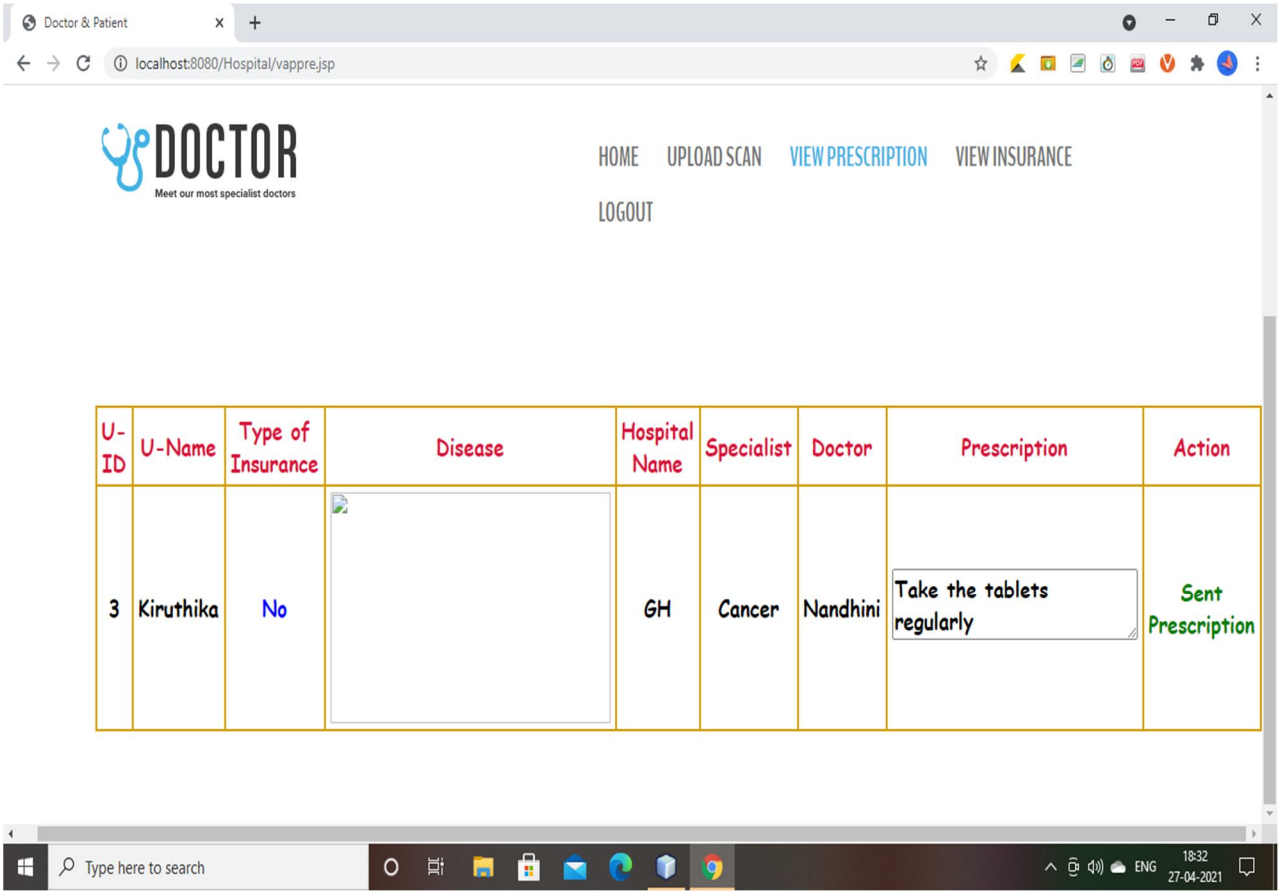
1) Login with cloud username and password
2) View all new patient key generation the mail
3) View all doctor details
4) View all insurance details
5) View all report upload by patient
6) Result
7) Logout.

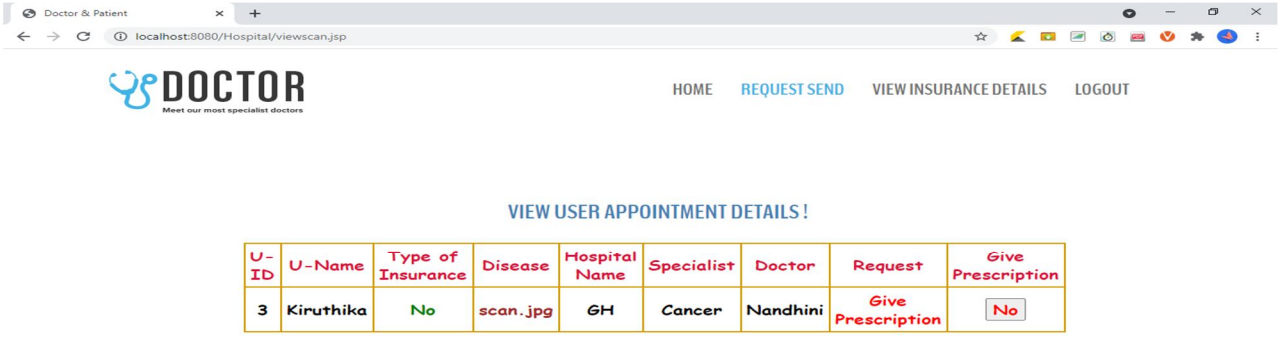
VII. SAMPLE OUTPUT

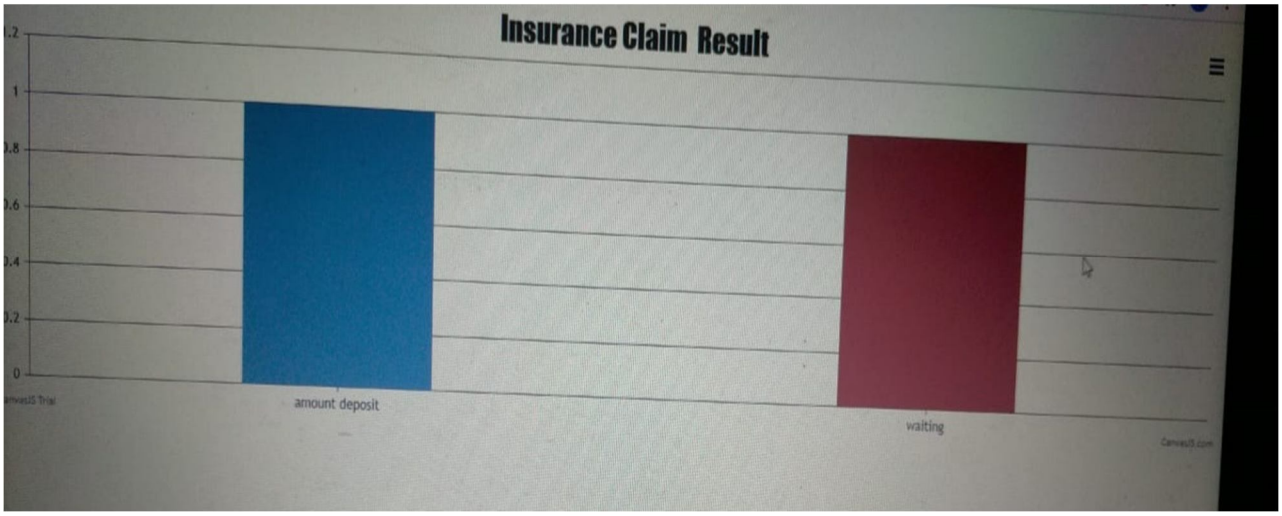


ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue IV Apr 2021- Available at www.ijraset.com









VIII. CONCLUSION

We have proposed a fully decentralized multi-party consent management solution for sharing and granting access to encrypted medical documents in a manner that is secure and trustworthy. Our approach maintains complete action traceability while providing an architecture for patients to authorize trusted entities to make access permission decisions on their behalf in case of emergencies. We implemented multi-party authorization and threshold cryptographic to allow the patients to securely share and grant access to their medical documents along with sharing their secret keys. We integrated decentralized IPFS storage with our system architecture and introduced reputation-governed trusted oracles to mitigate the data and computation related limitations.

REERENCES

[1] S. S. Woods, E. Schwartz, A. Tuepker, N. A. Press, K.M. Nazi, C. L. Turvey, and W. P. Nichol, ‘‘Patient experiences with full electronic access to health records and clinical notes through the my HealtheVet personal health record pilot: Qualitative study,’’ J. Med. Internet Res., vol. 15, no. 3, p. e65, Mar. 2013.

[2] J. S. Ancker, M. Silver, and R. Kaushal, ‘‘Rapid growth in use of personal health records in New York, 2012– 2013,’’ J. Gen. Internal Med., vol. 29, no. 6, pp. 850–854, Jun. 2014.

[3] Health Records–Apple. Accessed: Mar. 16, 2020.

[4] L. J. Kish and E. J. Topol, ‘‘Unpatients—Why patients should own their medical data,’’ Nature Biotechnol., vol. 33, no. 9, p. 921, 2015.

[5] Y. Al-Hammadi, S. Pesic, and S. Ellahham, ‘‘Blockchain for giving patients control over their medical records,’’ IEEE Access, vol.8, pp. 193102–193115, 2020.

[6] T.-S. Chen, C.-H. Liu, T.-L. Chen, C.-S. Chen, J.-G. Bau, and T.-C.Lin, ‘‘Secure dynamic access control scheme of PHR in cloud computing,’’ J. Med. Syst., vol. 36, no. 6, pp. 4005–4020, Dec. 2012.

[7] A. G. M. Alzahrani, A. Alenezi, A. Mershed, H. Atlam, F. Mousa, and G. Wills, ‘‘A framework for data sharing between healthcare providers using blockchain,’’ Tech. Rep., 2020.

[8] X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, ‘‘Integrating blockchain for data sharing and collaboration in mobile healthcare applications,’’ in Proc. IEEE 28th Annu. Int. Symp. Pers., Indoor,Mobile Radio Commun. (PIMRC), Montreal, QC, Canada, Oct.2017, pp. 1–5.

[9] H. S. G. Pussewalage and V. A. Oleshchuk, ‘‘An attribute based access control scheme for secure sharing of electronic health records,’’ in Proc. IEEE 18th Int. Conf. E-Health Netw., Appl. Services (Healthcom), Munich, Germany, Sep. 2016, pp. 1–6.

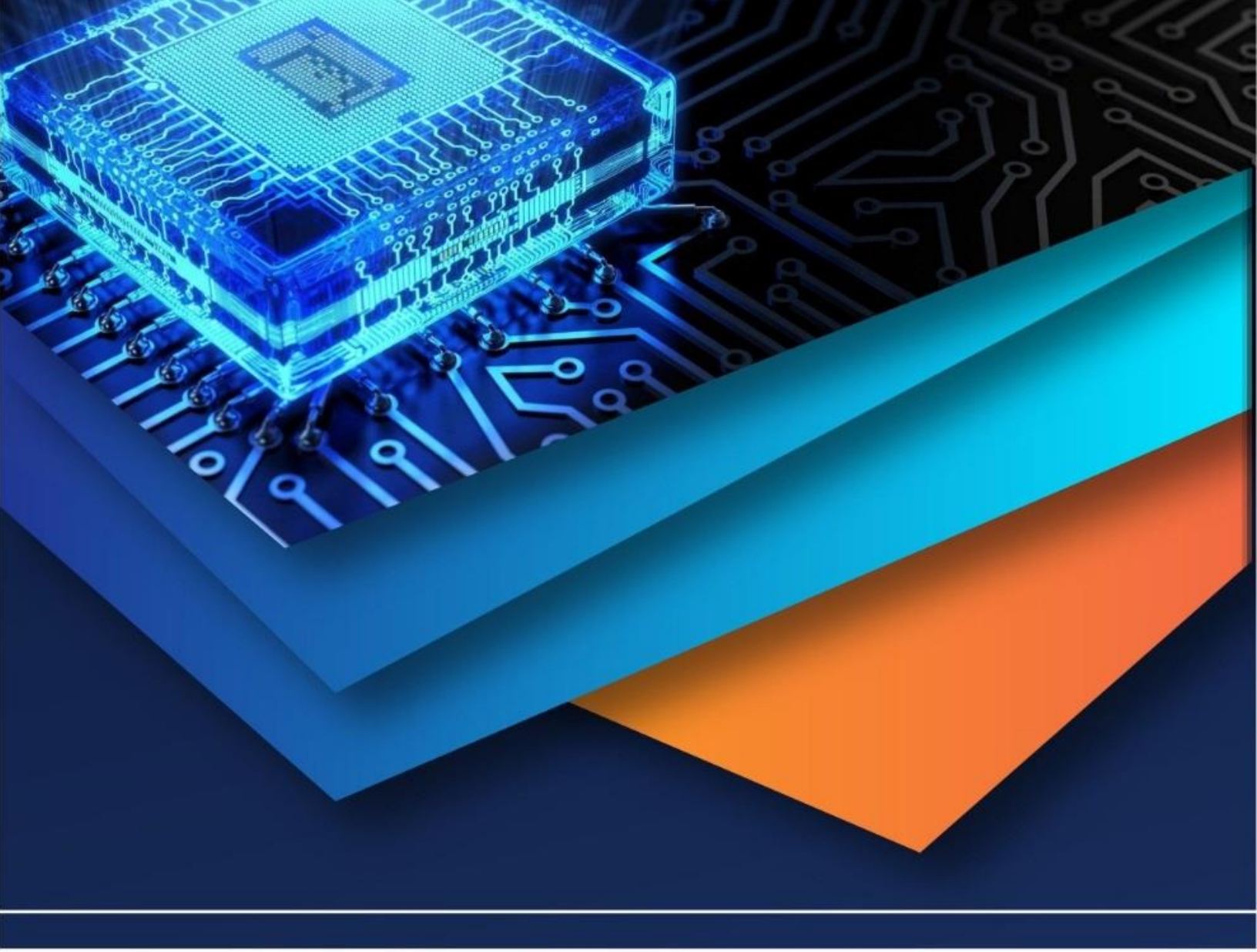
[10] X. Zhang and S. Poslad, ‘‘Blockchain support for flexible queries with granular access control to electronic medical records (EMR),’’ in Proc. IEEE Int. Conf. Commun. (ICC), Kansas City, MO, USA, May 2018, pp. 1–6.

Authors Profile

M.VENGATESHWARAN M.E.,
Assistant Professor
Sri Sai Ram Institute of Technology
Chennai

T.Kiruthika
UG Scholar
Sri Sai Ram Institute of Technology
Chennai

M.Nandhini
UG Scholar
Sri Sai Ram Institute of Technology
Chennai



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY