International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.194 |

|| Volume 8, Issue 4, April 2020 ||

Secure Access Controlling Model for Blockchain-Based Electronic Health Records

S. Murali [1], R. Arun Kumar[2], K.G. Krishna Kumar[3], S. Selvaganesh[4], P. Aravind Kumar[5]

Assistant Professor, Dept. of CSE, Velammal College of Engineering and Technology, Madurai, Tamil Nadu, India[1]

[2,3,4,5] UG Students, Dept. of CSE, Velammal College of Engineering and Technology, Madurai, Tamil Nadu, India

ABSTRACT: Healthcare is one of the fields handling with most sensitive data of any individuals in the world. One particular trend observed in healthcare is the progressive shift of data and services to the cloud due to the availability of data and cost-effectiveness. Such centralization of data also brings threats to the information that has been stored in the cloud. In traditional electronic health records, medical-related information is usually separately controlled by different hospitals and thus it results in inconvenience in data sharing. Our solution for these sorts of problems is to use blockchain technology for secure storing of data. To provide secure access to the data i.e. access control, the data is encrypted before the outsourcing to the cloud through most secured encryption algorithms.

KEYWORDS: blockchain; cloud computing; cryptography; centralization; data security; electronic health records; healthcare

I. INTRODUCTION

Cloud computing offers a chance for reducing the burden of managing large amounts of information and performing computations. Due to the increasing popularity of cloud computing, an oversized number of information Owners store their data within the cloud and it reduces cost in data management.

In Cloud computing, data security is provided by following a layered approach that features data encryption, key management, strong access controls, and counter-intelligence. Healthcare is a data-intensive domain where an oversized amount of data is formed, analyzed, stored, and accessed daily. Cloud computing can play a vital role in improving the standard of look after patients.

Facilitating data sharing, there's a desire EMRs to formalize their structure and also the design of HIS. Electronic Health Records (EHRs), are designed to permit patient anamnesis to maneuver with the patient or be made available to multiple healthcare providers. EHRs have a richer data structure than EMRs. There have also been initiatives to develop HIS and infrastructures that can scale and support future needs, as evidenced by the assorted national and international ongoing project to standardize the sharing of EHRs. Blockchain is employed to record transaction data, which is comparatively small in size and linear.

II. METHODOLOGY

Electronic Medical Records (EMRs) contain medical data associated with a given patient and stored by the healthcare provider. This provides the access and analysis of healthcare data. Management of EMRs, early generations of Health Information Systems (HIS) is intended with the potential to create new EMR instances, store them, and retrieves stored EMRs of interest. Health System will be a relatively simple solution, which might be schematically described as a graphical user interface or a web service. These are generally the front-end with a database at the back-end, during a centralized or distributed implementation. Patient mobility being increasingly the norm in today's society, it became evident that multiple stand-alone EMR solution must facilitate the sharing of healthcare data among different providers, even across national borders, as needed.

To overcome the safety problems that are occurred within the existing system and effectively store the info over the cloud we introduce this technique. Each electronic health record is encrypted with a unique key. Information user outsources the encrypted documents to the cloud. Information user gets the result, the proof, and public verification key; others can verify the freshness, authenticity, and completeness of the search result even without decrypting.

Every Healthcare provider should have a unique cloud id. Then the Healthcare provider logins and loads the patient records. A 128 bit Key is generated for every record created using Advanced Encryption Standard (AES) algorithm.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.194 |

|| Volume 8, Issue 4, April 2020 ||

Then using the key generated the patient record is encrypted and the upload request is performed.

When the request is accepted then the block is created and the chain is built. Every block of data has some connectivity with the next block preceding one. Then the blockchain is uploaded to the cloud. If we want to download and view the record then Download request is performed. Then the request is verified whether it is a valid request by checking the requestor identities. Then the encrypted data along with key is sent. Using the key the data is decrypted and viewed securely.

III. SYSTEM ARCHITECTURE

The below block diagrams explains the architecture of the proposed system (Fig 3.1 Architecture Diagram and Fig 3.2 Flow Diagram):

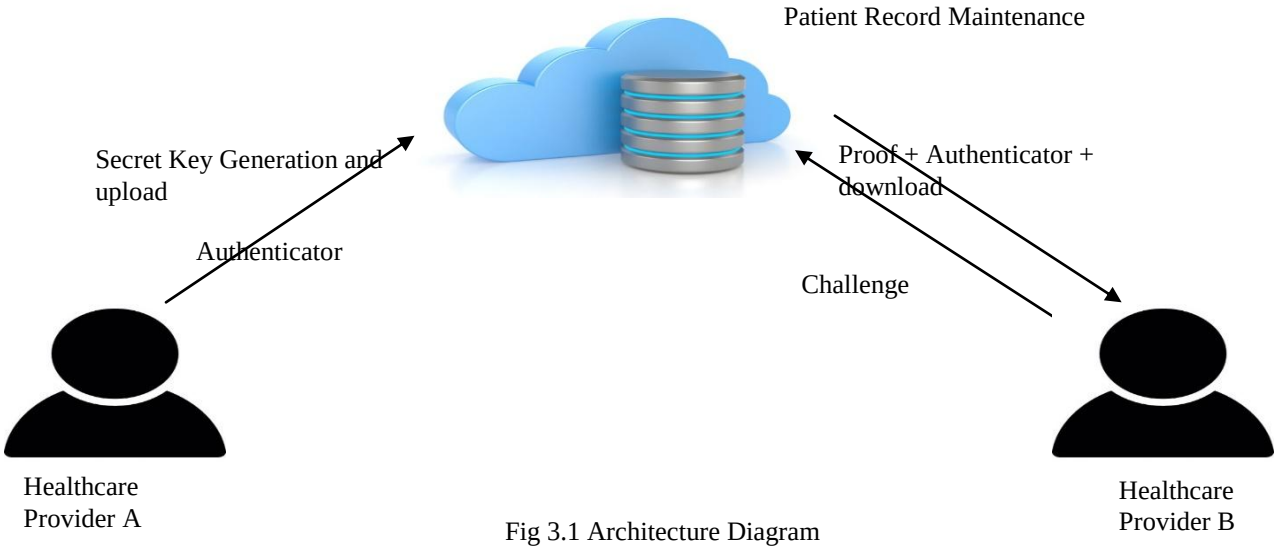

Fig 3.1 Architecture Diagram

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.194 |

|| Volume 8, Issue 4, April 2020 ||

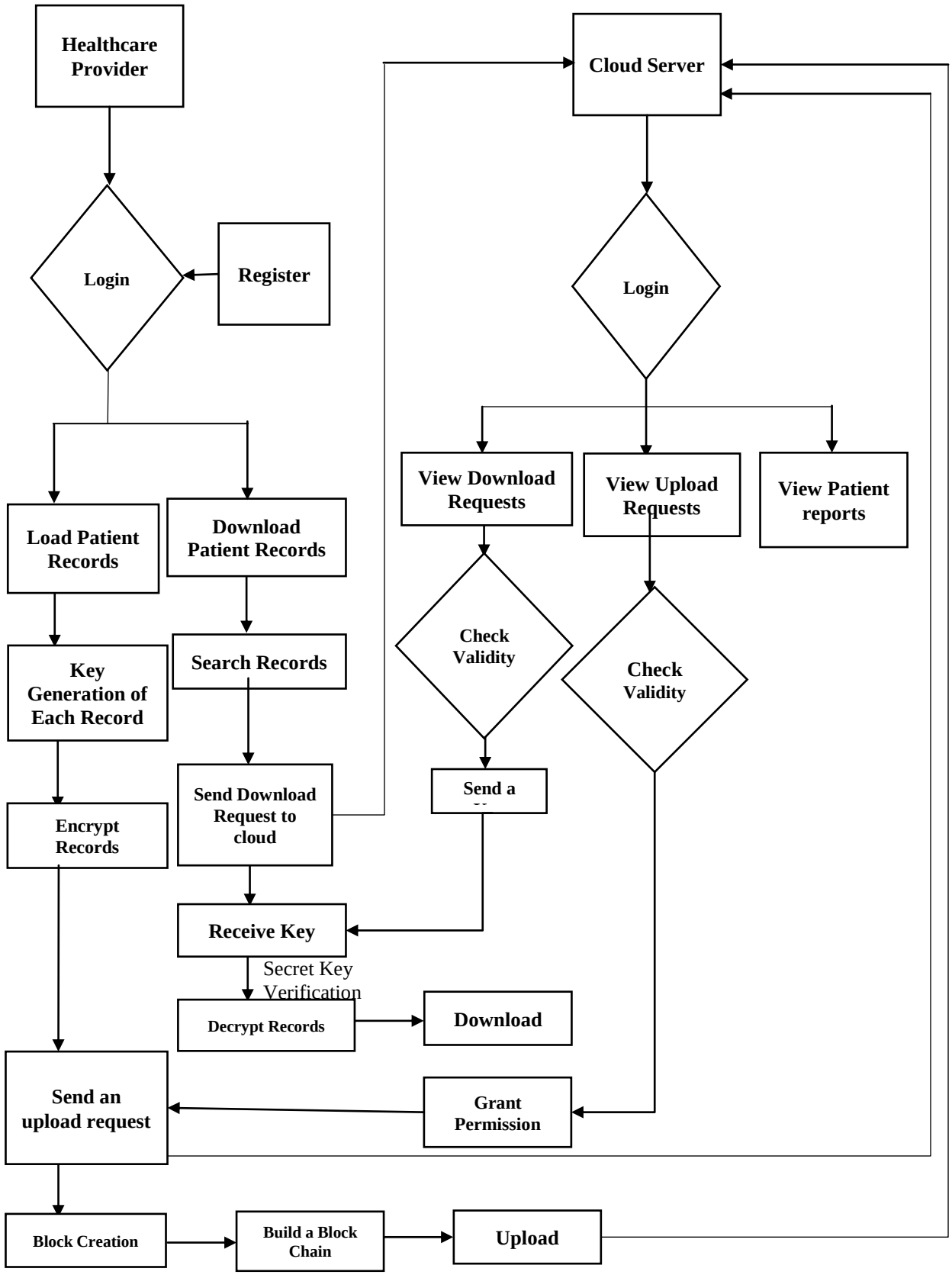

Fig 3.2 Flow Diagram

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.194 |

|| Volume 8, Issue 4, April 2020 ||

IV.RESULT

Our proposed system helps to store and maintain a large volume of patient records and easy to process and retrieve the records securely. It provides more accurate search results. By building a blockchain, it prevents data integrity attacks in SSE. It is suitable for large scale data and easily accessible by any healthcare provider.

The signing cost per time is compared between the existing system and the proposed system in the fig.4.1

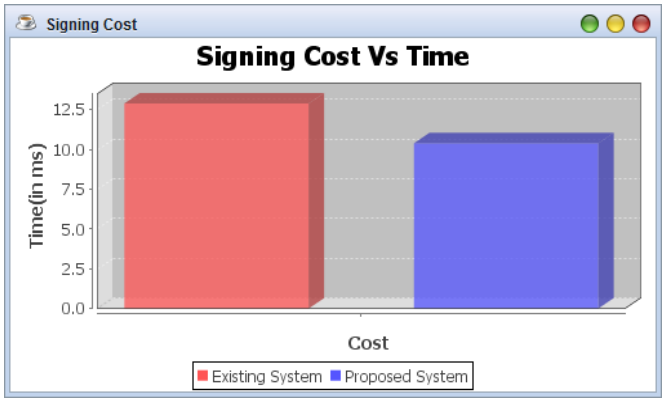

Fig 4.1 signing cost vs time

Both the systems are compared on the given parameter and the results are represented graphically in the following figure 4.2.

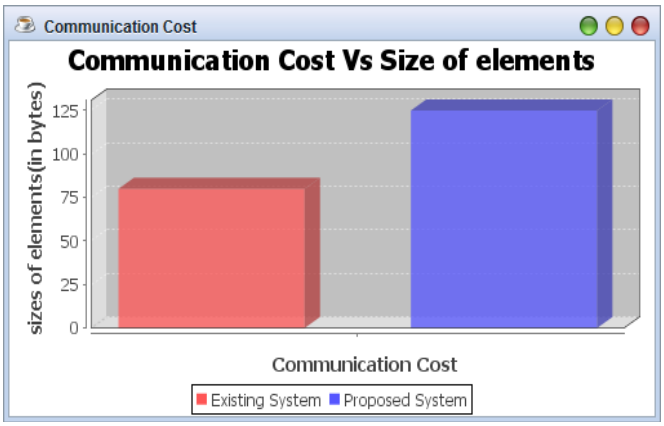

Fig.4.2. communication cost vs size of elements

V.CONCLUSION & FUTURE WORK

Our application can be built as an android and iOS application so that health care providers can use the application easily wherever they are, using their mobile phones or any of their handhelds and it will be more than a user-friendly application. Building as a mobile app has a lot of benefits like faster download speed, Instant Online, and Offline access and Push Notifications and instant updates. It can be build using Edge Computing technology so we can bring computation and data storage closer to the location where it is needed, to improve response times and save bandwidth. The most important benefit of edge computing is its ability to increase network performance by reducing latency since it processes data locally or in the nearby edge data center.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.194 |

|| Volume 8, Issue 4, April 2020 ||

REFERENCES

[1] Yunru Zhang, Debiao He, and Kim-Kwang Raymond Choo, "BaDS: Blockchain-Based Architecture for Data Sharing with ABS and CP-ABE in IoT," Wireless Commu. and Mobile Comput., 2018.

[2] Jiawen Kang, Rong Yu, Xumin Huang, Maoqiang Wu, SabitaMaharjan, ShengliXie, and Yan Zhang "Blockchain for Secure and Efficient Data Sharing in Vehicular Edge Computing and Networks," IEEE Internet of Things J., 2018.

[3] Oscar Novo, "Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT," IEEE Internet of Things J., vol. 5, pp. 1184-1195, 2018.

[4] Kuo TT, Kim HE, and Ohno-Machado L, "Blockchain distributed ledger technologies for biomedical and health care applications," Ame. Medi.Infor. Assoc. J., vol. 6, pp. 1211-1220, 2017.

[5] Nabil Rifi, ElieRachkidi, NazimAgoulmine, and Nada ChendebTaher, "Towards Using Blockchain Technology for eHealth Data Access Management," in Proc. IEEE on Advances in Bio.Engineering., Oct. 2017.

[6] S.H. Han et al., "Implementation of Medical Information Exchange System Based on EHR Standard" 2010.

[7] D. He et al., "A Provably-Secure Cross-Domain Handshake Scheme with Symptoms-Matching for Mobile Healthcare Social Network," IEEE Transactions on Dependable and Secure Computing, 2016

[8] F.Y. Leu et al., "A Smartphone-Based Wearable Sensors for Monitoring Real-Time Physiological Data," Computers and Electrical Engineering, 2017.

[9] M. Memon et al., "Ambient Assisted Living Healthcare Frameworks, Platforms, Standards, and Quality Attributes", 2014.

[10] P.C. Tang et al., "Personal Health Records: Definitions, Benefits, and Strategies for Overcoming Barriers to Adoption" 2006.

[11] S. Marceglia et al., "A Standards-Based Architecture Proposal for Integrating PatientHealth Apps to Electronic Health Record Systems" Applied Clinical Informatics, 2015.

[12] A. Mu-HsingKuo, "Opportunities and Challenges of Cloud Computing to Improve Health Care Services" Journal of Medical Internet Research, 2011.

[13] V. Casola et al., "Healthcare-Related Data in the Cloud: Challenges and Opportunities" IEEE Cloud Computing, 2016.

[14] S. Nepal et al., "Trustworthy Processing of Healthcare Big Data in Hybrid Clouds" IEEE Cloud Computing, 2015.

[15] G.S. Poh et al., "Searchable Symmetric Encryption: Designs and Challenges" 2017.