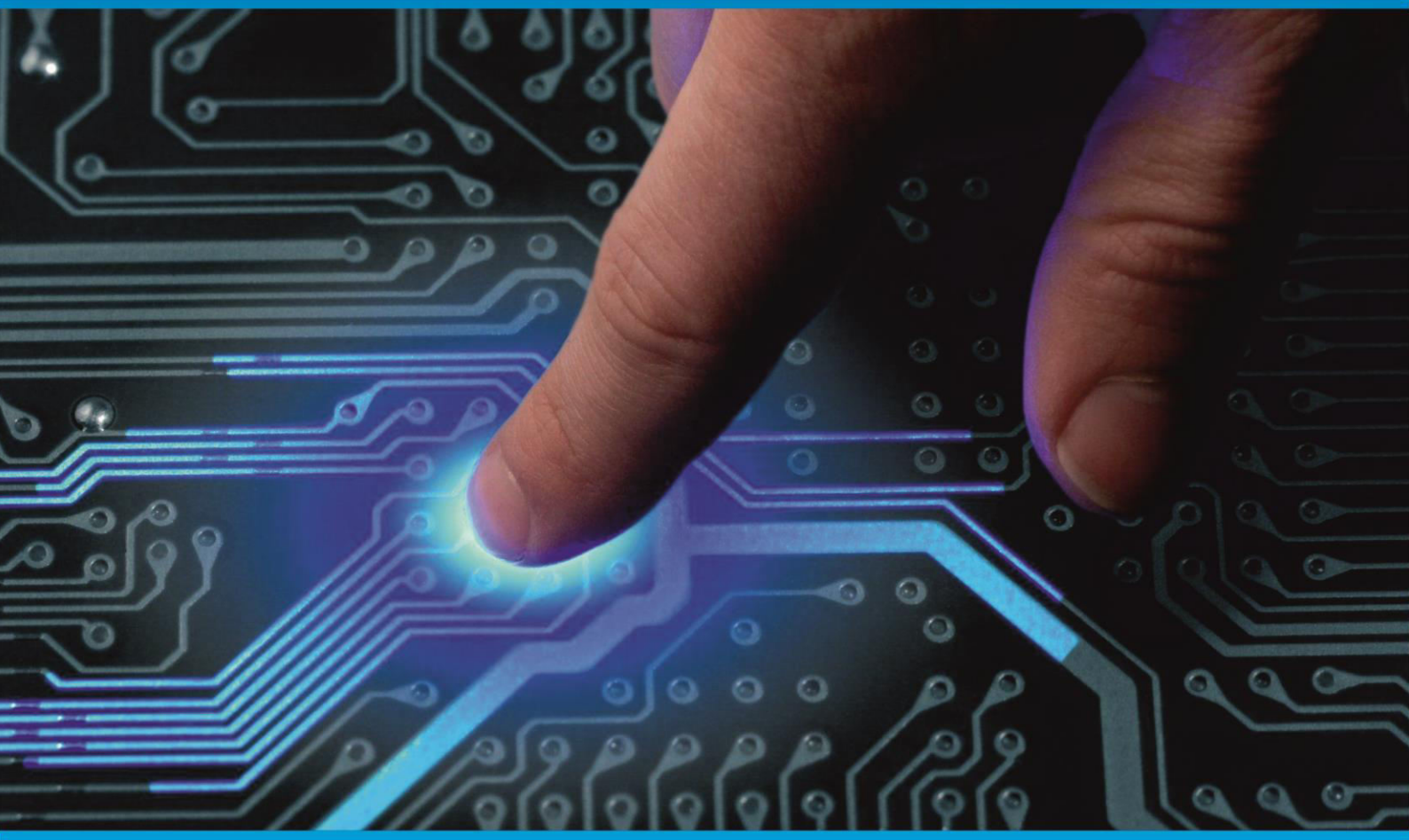
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 3, March 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

9940 572 462 | 6381 907 438 | ijircce@gmail.com | www.ijircce.com

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 3, March 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0903161 |

A Blockchain Based Data Aggregation and Group Authentication Scheme for Electronic Medical System

S. K.Kaneeshgar, T.Kavin Kumar, D. Shantanu Joshi, Mr.V.Manickavasagan,

UG Student, Department of Computer Science and Engineering, Velammal Institute of Technology, Chennai, Tamil Nadu, India

Assistant Professor, Department of Computer Science and Engineering, Velammal Institute of Technology, Chennai, Tamil Nadu, India

ABSTRACT: Cloud computing is emerging as a promising paradigm for computing and is drawing the attention from both academia and industry. The cloud-computing model shifts the computing infrastructure to third-party service providers that manage the hardware and software resources with significant cost reductions and data secured using machine learning. It is emerging as a new computing paradigm in the medical sector besides other business domains. Large numbers of health organizations have started shifting the electronic health information to the cloud environment in machine learning. Introducing the cloud services in the health sector not only facilitates the exchange of electronic medical records among the hospitals and clinics, but also enables the cloud to act as a medical record storage center. Moreover, shifting to the cloud environment relieves the healthcare organizations of the tedious tasks of infrastructure management and also minimizes development and maintenance costs. Storing the medical data in cloud makes the treatment efficient by retrieving patient's medical history from the server using machine learning before going for the treatment and get to know about thehealth issues of the patient.

KEYWORDS: Data sharing mechanism, attribute based encryption, secure outsourced computation,cloud computing, Electronic Medical Record.

I. INTRODUCTION

A system which handles the medical history of each individual of the country and provides access to all registered hospitals to read or update the data. The hospital which accesses the database must be registered and must have got a license. The license number is used as a unique code to access the database secured by machine learning. The details of the patients will be stored and an identification number will be generated when their data are stored into the database for the first time after the implementation of the system.

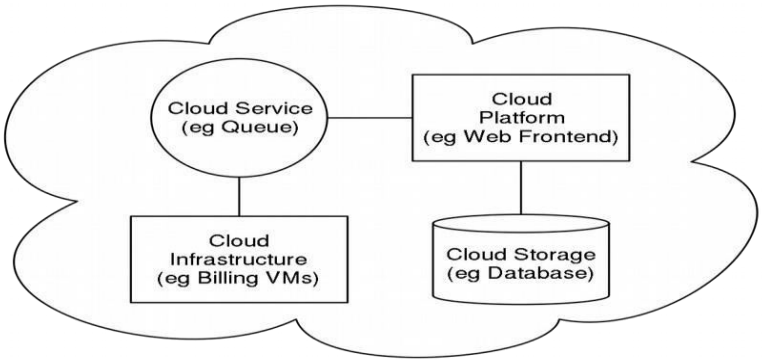


Figure 1

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 3, March 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0903161 |

II. LITERATURE SURVEY

In the year 2012 M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou. Proposed a system Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption, The objective personal health record (PHR) is an emerging patient-centric model of health information exchange, which is often outsourced to be stored at a third party, such as cloud providers. In this paper, we propose a novel patient- centric framework and a suite of mechanisms for data access control to PHRs stored in semi trusted servers. To achieve fine-grained and scalable data access control for PHRs, we leverage attribute-based encryption (ABE) techniques to encrypt each patient's PHR file. A high degree of patient privacy is guaranteed simultaneously by exploiting multiauthority ABE. Our scheme also enables dynamic modification of access policies or fileattributes, supports efficient on-demand user/attribute revocation and break-glass access under emergency scenarios. Extensive analytical and experimental results are presented which show the security, scalability, and efficiency of our proposed scheme.

In another study in the year project 2012 C. Wang, K. Ren, S. Yu, and K. M. R. Urs ,Proposed system for Achieving Usable and Privacy-assured Similarity Search over Outsourced Cloud Data, It investigates theproblem of secure and efficient similarity search over outsourced cloud data. Similarity search is a fundamental and powerful tool widely used in plaintext information retrieval, but has not been quite explored in the encrypted data domain. We formally prove the privacy-preserving guarantee of the proposed mechanism under rigorous security treatment. The extensive experiments on Amazon cloud platform with real data set further demonstrate the validity and practicality of the proposed mechanism.

In the year 2012,H. Liang, L. X. Cai, D. Huang, X. Shen, and D. Peng The objective of Mobile cloud computing is a promising technique that shifts the data and computing service modules from individual devices to geographically distributed cloud service architecture.The propose a service decision making system for interdomain service transfer to balance the computation loads among multiple cloud domains. To this end, we formulate the service request decision making process as a semi-Markov decision process. The optimal service transfer decisions are obtained by jointly considering the system incomes and expenses. Extensive simulation results show that the proposed decision making system can significantly improve the system rewards and decrease service disruptions compared with the greedy approach.

For instance in the year2014, Y. Yang, H. Li, L. Wenchao, H. Yang, and W. Mi proposed a system for Secure Dynamic Searchable Symmetric Encryption with Constant Document Update Cost, the development of cloud computing, data sharing has a new effective method, i.e., outsourced to cloud platform. In this case, since the outsourced data may contain privacy, they only allow to be accessed by the authorized users. In this paper, we leverage the secure k-nearest neighbor to propose a secure dynamic searchable symmetric encryption scheme. Our scheme can achieve two important security features, i.e., forward privacy and backward privacy which are very challenging in Dynamic Searchable Symmetric Encryption (DSSE) area. In addition, we evaluate the performance of our proposed scheme compared with other DSSE schemes. The comparison results demonstrate the efficiency of our proposed scheme in terms of the storage, search and update complexity.

III. PROPOSED METHODOLOGY AND DISCUSSION EXISTING SYSTEM

Cloud based health system's main focus is the patient's data collection, storage, access, analysis, and presentation etc. The current patient data collection techniques are time consuming, inefficient, laborious. It is also obvious that currents technique is violating the real time data access for monitoring the patients.It also brings about a series of challenges, especially how to ensure the security and privacy of the patients personal health information from various attacks in the wireless communication channel such as eavesdropping and tampering.

PROPOSED SYSTEM

Cloud based health system solution is based on the concept of "Cloud Computing" a distributed computing system where a pool of virtualized, dynamically-salable, managed computing power, storage, platforms, and services are delivered. This system provides an environment where patient's records are stored using machine learning and it will be referenced by the doctors to improve the efficiency of the treatment. This handles the medical history of each individual of the country and provides access to all registered hospitals to read or updatethe data. The hospital which accesses the database must be registered and must have got a license. The license number is used as a unique code to access the database. The details of the patients will be stored and an identification number will be generated when their data are stored into the database for the first time after the implementation of the system. Whenever they go for a

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 3, March 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0903161 |

treatment, their medical data will be stored into the database using their identification number and retrieved data used by machine learning. For security reasons, any person who wants to view their data will be allowed only to read the data. They will not be given access to update the database. For hospitals to update the database they require the license number along with the identification number of the person whose record has to be stored

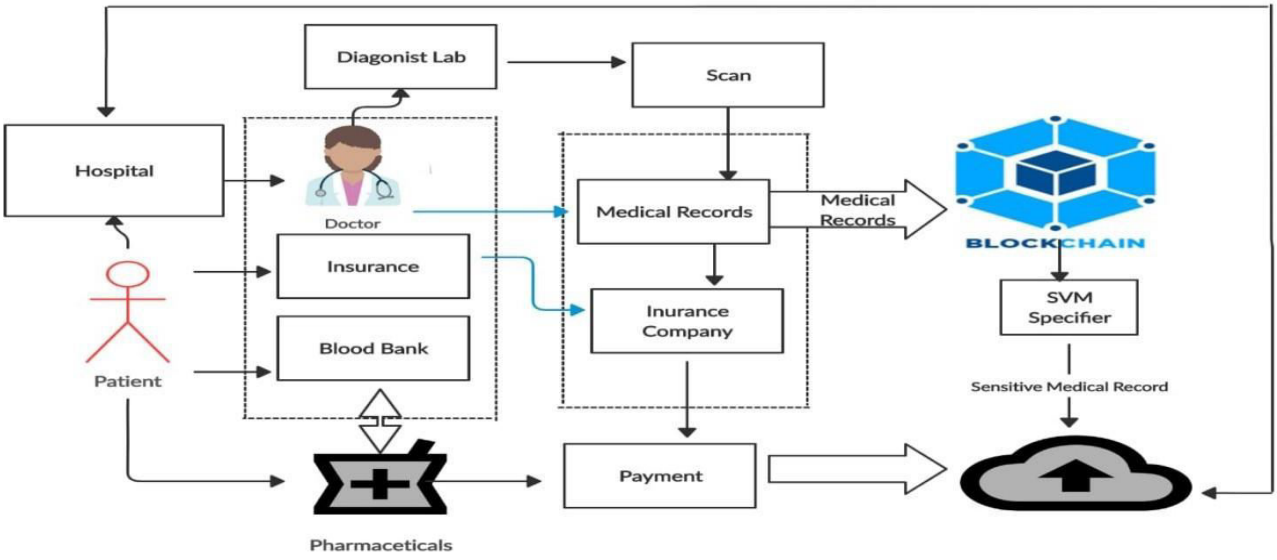


Fig 2: Architecture of the proposed system

Admin Module

In this Module, an User must Authorised in an our application and there is a provider side must add the doctors and hospitals for the further counselling for Patients or Users. Even Doctor Profile, Doctors only able to known the Password for their view of Counselling Information.

Unique Id And Key verification

In this module, when an every provider must have an unique hospital details and doctor list. When an Usercomes under in an application and accepts the Provider for further Proceeding Comes under in the booked Provider alone.

In this module, When an User booked his Provider along with Hospitality Functions and Doctor Specalist in an application.Once an User come back for further Process They made an counselling to Particular Doctor.A User must Authorized in an application and there is a provider side must add the doctors and hospitals for the further counselling for Patients or Users. Even Doctor Profile, Doctors only able to known the Password for their view of Counselling Information.

Doctor Counseling and User Entry Checking

Consider the server to be semi-trusted, That means the server will try to find out as much secret information in the stored PHR files as possible, but they will honestly follow the protocol in general. On the other hand, some users will also try to access the files beyond their privileges.It gives security for viewing ourpersonal information to all roles in an application.The proposed system uses Attribute Based Encryption Algorithm for the access to encrypt the Selected Details to Restrict to view By others.

Database Report Search

In this module, admin can able to view overall users report, Users personal Records and User Counselling Records In Such Case, user had made encrypted their information it will visualization in cipher text format and age display in the K-Anatomy Format.

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 3, March 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0903161 |

III. EXPERIMENTAL RESULTS

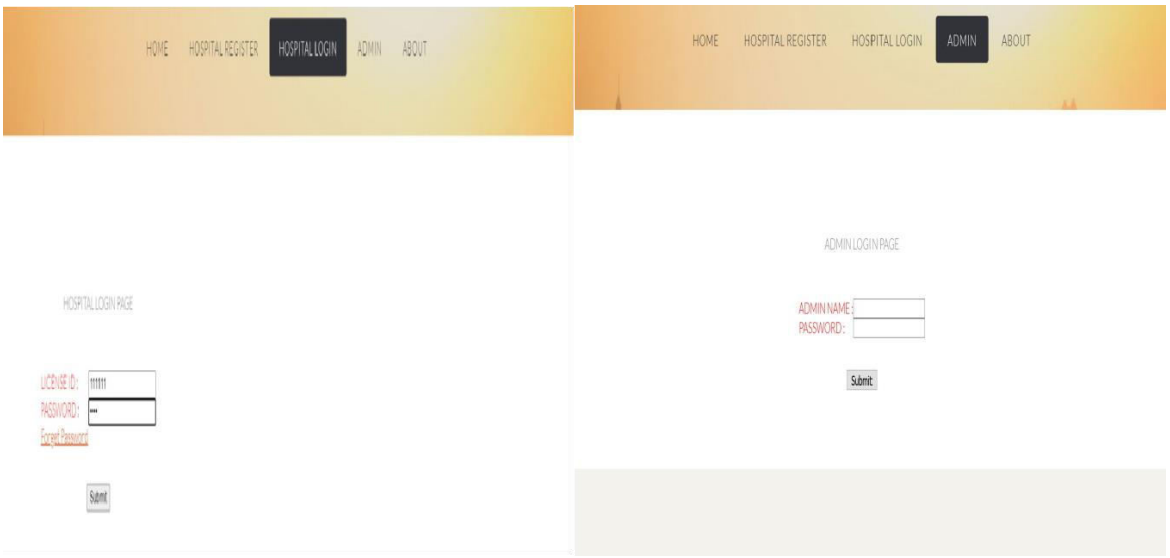


Figure 3 Login page

Figure.3 Add Personal Health Record Information

IV. CONCLUSION AND FUTURE ENHANCEMENT

In this project, proposed a system which monitors the health care details of each individual of the country. It comprises of modules like generating the unique ID and store and retrieve data of a person. The cloudcomputing is an emerging computing mode. It promises to increase the velocity with which applications are deployed, increase innovation, and lower costs, all while increasing business agility. The nature of cloud computing is useful for constructing the data center. To the new generation of cloud based health system, cloudcomputing is better approach in the future.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 3, March 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0903161 |

In future work, The authenticity of such information can be guaranteed by a proper authorization mechanism from users to their employees. We designed an identity-based signature scheme with multiple authorities for the block chain-based EHRs system. The scheme has efficient signing and patient data by Svm Specifier.

REFERENCES

[1] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," IEEE Transactions on Parallel and Distributed Systems, vol.24, no. 1, pp. 131–143, 2013.

[2] H. Liang, L. X. Cai, D. Huang, X. Shen, and D. Peng, "An smdpbased service model for interdomain resource allocation in mobile cloud networks," IEEE Transactions on Vehicular Technology, vol. 61, no. 5, pp. 2222–2232, 2012.

[3] Q. Shen, X. Liang, X. Shen, X. Lin, and H. Luo, "Exploiting geodistributed clouds for e-health monitoring system with minimum service delay and privacy preservation," IEEE Journal of Biomedical and Health Informatics, vol. 18, no. 2, pp. 430–439, 2014.

[4] Y. Yang, H. Li, L. Wenchao, H. Yang, and W. Mi, "Secure dynamic searchable symmetric encryption with constant document update cost," in Proceedings of GLOBECOM. IEEE, 2014, pp. 775–780.

[5] C. Wang, K. Ren, S. Yu, and K. M. R. Urs, "Achieving usable and privacy-assured similarity search over outsourced cloud data," in Proceedings of IEEE INFOCOM, 2012, pp. 451–459.

[6] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Advances in Cryptology–Eurocrypt. Springer, 2004, pp. 506–522.

[7] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," in Proceedings o ACM CCS, 2006, pp. 79—88.

[8] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," IEEE Internet Computing, vol.16, no. 1, pp. 69–73, Jan 2012.

[9] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in IEEE Symposium on Security and Privacy, 2000, pp. 44–55.

[10] F. Hahn and F. Kerschbaum, "Searchable encryption with secure and efficient updates," in Proceedings ofCCS. ACM, 2014, pp. 310–320.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.488

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details