isrjournals

International Journal of Advanced Research in Computer Science Engineering and Information Technology

Volume: 6, Issue: 3,Special Issue: 3 ,Apr,2024 ,ISSN_NO: 2321-3337

LEARNING A DIAGNOSTIC AND MEDICAL DATA WITH DEEP REINFORCEMENT LEARNING

Jaya Shalini J[1], Savya Sri K[2], Preetha G[3], Edith Esther E[4*]

[123]UG Scholar-Dept.CSE, GRT Institute of Engineering & Technology, Tiruttani, India.

[4*]Assistant Professor-Dept.CSE, GRT Institute of Engineering & Technology, Tiruttani,India.

jayashalini203@gmail.com,savyasriroyal@gmail.com,preetharaj23012003@gmail.com

[*]Corresponding Author: edithesther@gmail.com

Abstract

The intersection of machine learning and healthcare has shown promising results, particularly in diagnostic tasks. Deep reinforcement learning (DRL) has emerged as a powerful technique for learning complex decision-making policies from raw data in medical field, refers to medical conditions in patients. However, such features are not always readily available due to the high cost of time and money associating with medical tests. To address this, this study identifies the diagnostic strategy learning problem and proposes a novel framework consisting of three components to learn a diagnostic strategy with limited features. It involves medical history, test results, and other relevant information to reach a diagnosis. The vast amount of information collected from patients, including medical records, lab tests, scans, X-rays or MRIs and genetic data etc. And also utilize secure storage mechanisms such as encrypted databases and secure file systems to store medical data.

***Keywords**: Machine Learning, Deep Reinforcement Learning*

1. Introduction

Deep Reinforcement Learning (DRL), a subset of artificial intelligence. By training an agent to interact with the diagnostic environment, we aim to learn policies that optimize diagnostic accuracy, efficiency, and patient outcomes. Furthermore, we investigate the interpretability of the learned diagnostic policies, providing insights into the decision-making process and facilitating collaboration between AI systems and healthcare professionals. By harnessing the power of deep reinforcement learning, we strive to advance the state-of-the-art in medical diagnostics, ultimately improving patient care and clinical outcomes.

2. Related Work

Healthcare blockchains offer an innovative approach to securely store and manage healthcare information and transactions in a decentralized network. Despite significant interest from various sectors, concerns over security and privacy persist when utilizing blockchain for healthcare data sharing. This paper delves into these concerns, focusing on security and privacy requirements for medical data sharing via blockchain technology. It presents a thorough analysis of associated risks, requirements, and technical solutions. Specifically, it discusses necessary security and privacy attributes for medical data sharing using blockchain and examines existing efforts across three reference usage scenarios. The paper also explores technologies like anonymous signatures, attribute-based encryption, zero-knowledge proofs, and smart contract verification techniques to address security and privacy challenges in healthcare blockchain applications. Ultimately, this survey aims to equip healthcare professionals, decision-makers, and developers with comprehensive insights into blockchain's role in ensuring the security and privacy of healthcare data.[1]

Electronic Health Records (EHRs) are digital health records containing information about an individual's health. These records are shared among healthcare stakeholders but face challenges such as power failures, data misuse, and privacy issues. Blockchain technology, however, offers a decentralized and secure environment where network nodes can connect without a central authority. It has the potential to address EHR management limitations by providing a secure and decentralized platform for data exchange. Blockchain stores data securely using distributed ledger technology that ensures data integrity and immutability. Smart contracts facilitate secure decision-making and analytics, especially when combined with machine learning algorithms.[2]

Smart healthcare systems have improved patients' lives by allowing their records to be analyzed remotely by different people. But this involves sending a lot of data over the Internet to predict diseases, which can put patient privacy at risk and affect how models are trained on centralized servers. To solve this, federated learning (FL) has come into play. FL trains models on individual devices (like phones or computers) and then combines the results to create an overall model. This way, patient data stays private and secure. FL has many benefits for healthcare, but its full potential hasn't been fully explored yet. We need more detailed studies specifically focusing on FL in healthcare informatics (HI). Our survey introduces an FL-based system for healthcare informatics and discusses its benefits and challenges. This review will be useful for researchers and healthcare professionals looking to use FL to improve data privacy and patients' lives.[3]

Electronic Health Records (EHRs) are digital records of health information that are shared among healthcare providers but face challenges like power failures, data misuse, and privacy concerns. Blockchain is a modern technology that allows decentralized communication among computers without a central authority. It can address EHRs' limitations by offering a secure and decentralized way to exchange health data.

Researchers have proposed three types of blockchain solutions for managing EHRs: conceptual ideas, prototype systems, and fully implemented solutions. A recent study reviewed 99 papers to understand how blockchain can manage EHRs. They analyzed these papers based on privacy, security, scalability, accessibility, cost, consensus algorithms, and types of blockchain used.[4]

Electronic Health Records (EHRs) are digital records of health information that are shared among healthcare providers but face challenges like power failures, data misuse, and privacy concerns. Block chain is a modern technology that allows decentralized communication among computers without a central authority. It can address EHRs' limitations by offering a secure and decentralized way to exchange health data.
Researchers have proposed three types of blockchain solutions for managing EHRs: conceptual ideas, prototype systems, and fully implemented solutions. The study found that blockchain technology could improve EHR management by providing decentralization, security, and privacy that traditional systems lack. The findings can guide future researchers in choosing the right blockchain approach for managing EHRs effectively. This study also suggests future research directions to explore new blockchain-based systems for EHR management.[5]

3. Objective

The primary objective of this project is to develop and evaluate a diagnostic strategy for medical data using deep reinforcement learning (DRL). Our ultimate goal is to improve patient care, clinical outcomes, and healthcare efficiency through the integration of deep reinforcement learning techniques into medical diagnostics. Address privacy and security concerns related to handling sensitive medical data. Implement robust data anonymization, encryption, access controls, and audit trails to protect patient privacy

4. Proposed System

The proposed system would likely entail creating a state representation of patient data, defining actions (diagnostic tests or treatments), and training. First, as we often encounter incomplete medical records of the patients, a sequence encoder is designed to encode any set of information in various sizes into fixed-length vectors. Second, taking the output of the encoder as the input, a feature selector based on reinforcement learning techniques is proposed to learn the best feature sequence for diagnosis. Finally, with the best feature sequence, an oracle classifier is used to give the final diagnosis. The results suggest that the proposed method is effective for providing personalized diagnostic strategies and makes better diagnoses with fewer features compared with existing methods.

5. Architecture Diagram

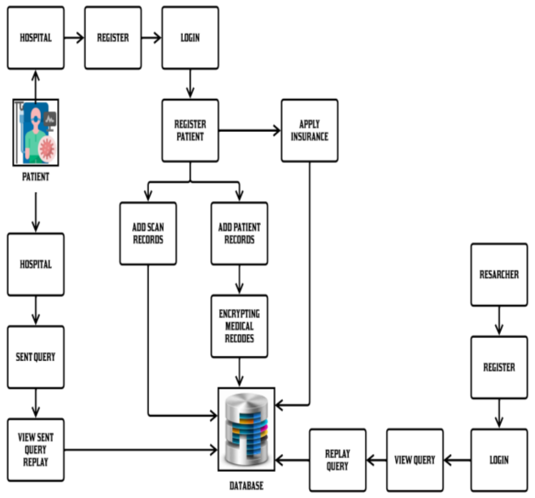


Fig 5.1 Architecture Diagram

6.Algorithm

6.1 Deep Reinforcement Learning

Deep reinforcement learning (deep RL) is a subfield of Machine Learning that combines ReinforcementLearning (RL)and deep learning. RL considers the problem of a computational agent learning to make decisions by trial and error. Deep RL incorporates deep learning into the solution, allowing agents to make decisions from unstructured input data without manual engineering of the state space. Deep RL algorithms are able to take in very large inputs (e.g. every pixel rendered to the screen in a video game) and decide what actions to perform to optimize an objective (e.g. maximizing the game score). Deep reinforcement learning has been used for a diverse set of applications including but not limited robotics, Video games, transportation, finance and healthcare.

6.2 AES Algorithm

AES (acronym of Advanced Encryption Standard) is a symmetric encryption algorithm. The algorithm was developed by two Belgian cryptographers Joan Daemen and Vincent Rijmen. AES was designed to be efficient in both hardware and software, and supports a block length of 128 bits and key lengths of 128, 192, and 256 bits

7. Implementation

7.1 Admin Dataset

In this Module, a User must Authorised in 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.

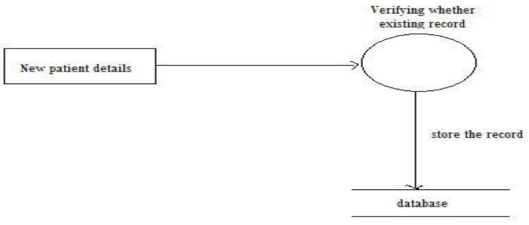


Fig 7.1 Admin Dataset

7.2 Unique Id and Key Verification

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

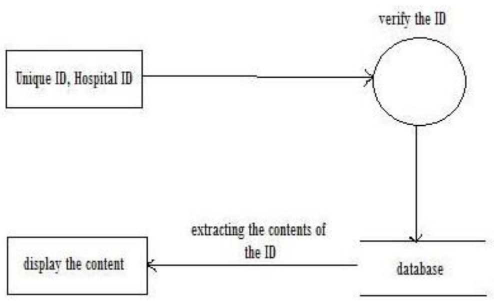


Fig 7.2 Unique Id and Key Verification

7.3 Reports Upload

In this module, when a User booked his Provider along with Hospitality Functions and Doctor Specialist in an application...Once a User come back for further process. They made an counselling to Particular Doctor

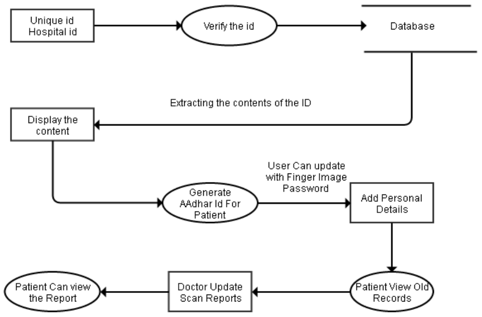

Unique id Hospital id
Verify the id
Database
Extracting the contents of the ID
Display the content
User Can update with Finger Image Password
Generate AAdhar Id For Patient
Add Personal Details
Patient Can view the Report
Doctor Update Scan Reports
Patient View Old Records

Fig.7.3. Reports Upload

7.4 Doctor Counselling

We 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. For example, a pharmacy may want to obtain the prescriptions of patients for marketing and boosting its profits.

7.5 User Entry Checking

In this Module, we had implemented main goal of the Project it denotes security for viewing our personal information to all roles in an application…To prevent that we had proposed to use Attribute Based Encryption Algorithm for the access to encrypt the Selected Details to Restrict to view by others.

7.6 Data base 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

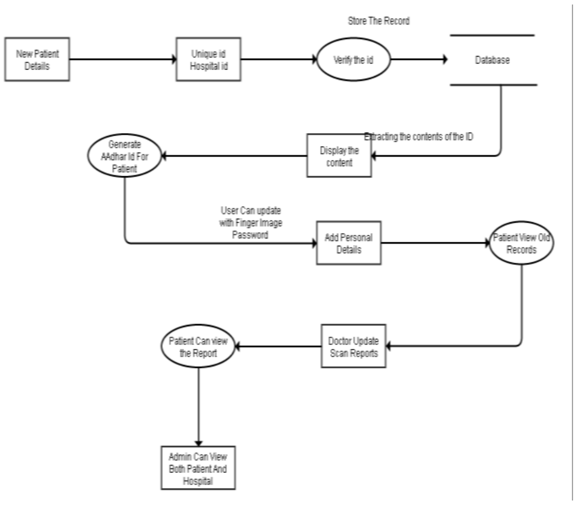
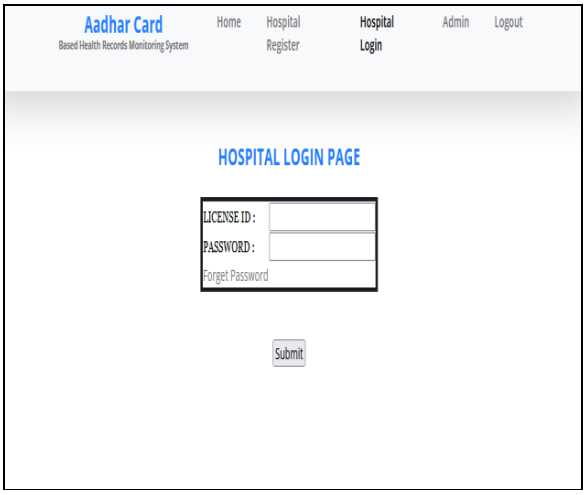

Store The Record
New Patient Details
Unique id Hospital id
Verify the id
Database
Extracting the contents of the ID
Display the content
Generate AAdhar Id For Patient
User Can update with Finger Image Password
Add Personal Details
Patient View Old Records
Doctor Update Scan Reports
Patient Can view the Report
Admin Can View Both Patient And Hospital

Fig 7.6 Database Report Search

8. Experimental Results

This result discusses about the implementation of the Policy based security for various cases are identified and the below Fig 8.1, Fig 8.2, Fig 8.3, Fig 8.4, Fig 8.5, Fig 8.6 shows the implementation of admin policy based on the proposed methodology.



HOSPITAL LOGIN PAGE

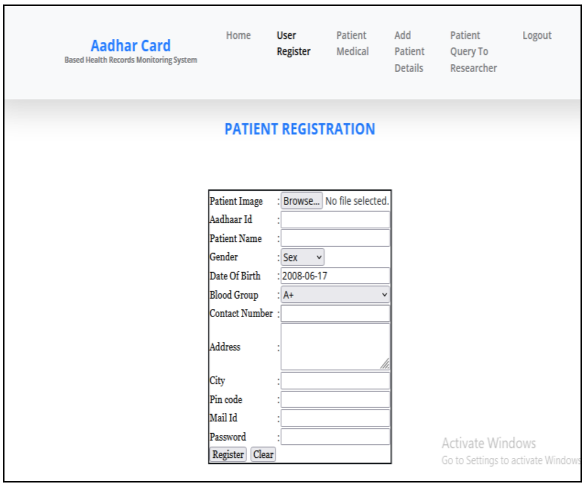
LICENSE ID :

PASSWORD :

Forget Password

Submit

Fig 8.1 Hospital Login



PATIENT REGISTRATION

Patient Image : Browse... No file selected.

Aadhaar Id :

Patient Name :

Gender : Sex

Date Of Birth : 2008-06-17

Blood Group : A+

Contact Number :

Address :

City :

Pin code :

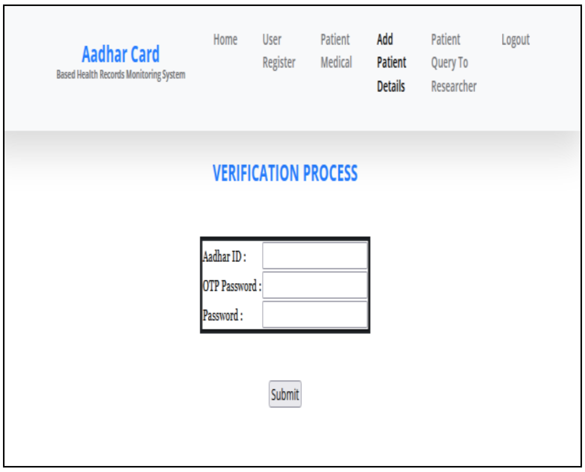
Mail Id :

Password :

Register Clear

Activate Windows
Go to Settings to activate Windows

Fig 8.2 User Registration



VERIFICATION PROCESS

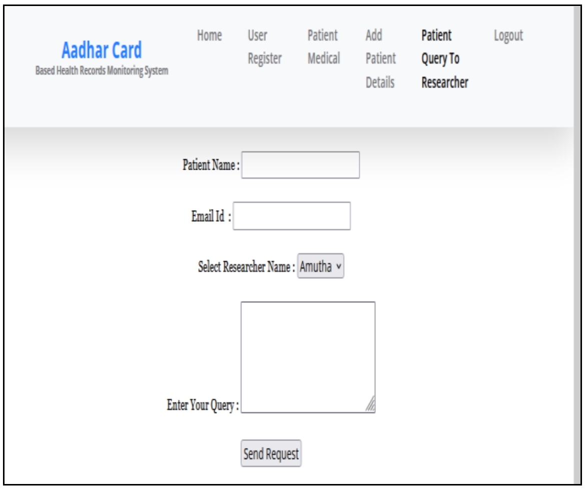
Aadhar ID :

OTP Password :

Password :

Submit

Fig 8.3 Verification process



Patient Name :

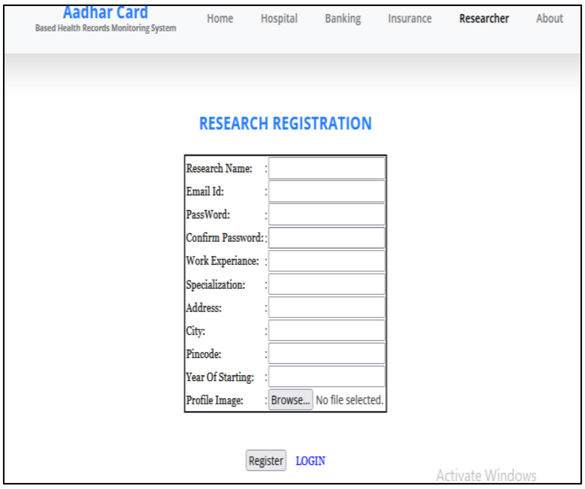
Email Id :

Select Researcher Name : Amutha

Enter Your Query :

Send Request

8.4 Patient Query to Researcher



RESEARCH REGISTRATION

Research Name: :

Email Id: :

PassWord: :

Confirm Password: :

Work Experiance: :

Specialization: :

Address: :

City: :

Pincode: :

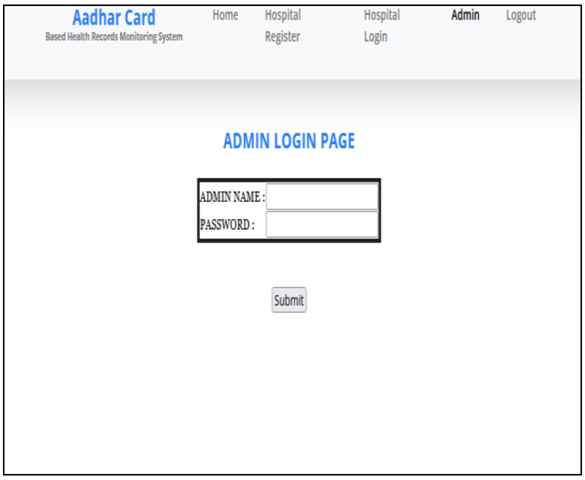
Year Of Starting: :

Profile Image: : Browse... No file selected.

Register LOGIN

Activate Windows

Fig 8.5 Researcher Page



ADMIN LOGIN PAGE

ADMIN NAME :

PASSWORD :

Submit

Fig 8.6 Admin Login Page

9. Conclusion & Future Work

Employing the deep reinforcement learning (DRL) for developing diagnostic strategies on medical data shows promise in enhancing accuracy and efficiency. However, challenges such as data privacy, interpretability, and generalizability need to be addressed for wider adoption in clinical settings. Further research and collaboration between medical professionals and AI experts are essential to realize the full potential of DRL in medical diagnostics.

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.

10.Reference

[1] Rui Zhang, RuiXue, and Ling Liu, "Security and Privacy for Healthcare Blockchains," 1939-1374 July 01,2021.

[2] Alaa Haddad, Mohamed HadiHabaebi, Md. Rafiqul Islam, NurulFadzlinHasbullah, And Suriza Ahmad Zabidi, "Systematic Review on AI-Blockchain Based E-Healthcare Records Management Systems," Volume 10, 2022

[3] VishwaAmitkumar Patel, Pronaya Bhattacharya, SudeepTanwar, Rajesh Gupta , Gulshan Sharma, Pitshou N. Bokoro , Ravi Sharma, "Adoption of Federated Learning for Healthcare Informatics: Emerging Applications and Future Directions," Volume 10, 2022.

[4] Abdullah Al Mamun, Sami Azam, Clementine Gritti. "Blockchain-Based Electronic Health Records Management: A Comprehensive Review and Future Research Direction,"Volume 10, 2022.

[5] HuaShen, "Enhancing Diagnosis Prediction in Healthcare with Knowledge Based Recurrent Neural Networks," Volume 11, 2023.

[6] H. Malik, N. Fatema, and J. A. Alzubi, AI and Machine Learning Paradigms for Health Monitoring System: Intelligent Data Analytics. Berlin, Germany: Springer, 2021.

[7] J. G. D. Ochoa and F. E. Mustafa, ''Graph neural network modelling as a potentially effective method for predicting and analyzing procedures based on patients' diagnoses,'' Artif. Intell.Med., vol. 131, Sep. 2022, Art.no. 102359.

[8] A. AwadAbdellatif, L. Samara, A. Mohamed, A. Erbad, C. F. Chiasserini, M. Guizani, M. D. O'Connor, and J. Laughton, ''MEdge-chain: Leveraging edge computing and blockchain for efficient medical data exchange,'' IEEE Internet Things J., vol. 8, no. 21, pp. 15762–15775, Nov. 2021.

[9] P. Bhattacharya, S. Tanwar, U. Bodkhe, S. Tyagi, and N. Kumar, ''BinDaaS: Blockchain-based deep-learning as-a-service in health- care 4.0 applications,'' IEEE Trans. Netw. Sci. Eng., vol. 8, no. 2, pp. 1242–1255, Apr. 2021.

[10] C. Hou, K. K. Thekumparampil, G. Fanti, and S. Oh, ''Reducing the communication cost of federated learning through multistage optimization,'' in Proc. Int. Conf. Learn. Represent., 2022, pp. 1–49.

[11] J. Zhu and J. Ma, "A new authentication scheme with anonymity for wireless environments," IEEE Transactions on Consumer Elec-tronics, vol. 50, no. 1, pp. 231–235, Feb 2004.

[12] P. Gope and T. Hwang, "Lightweight and energy-efficient mutual authentication and key agreement scheme with user anonymity

for secure communication in global mobility networks," IEEE Systems Journal, vol. 10, no. 4, pp. 1370–1379, Dec 2016.

[13] J. Ni, K. Zhang, X. Lin, H. Yang, and X. S. Shen, "Ama: Anonymous mutual authentication with traceability in carpooling systems," in ICC 2016, May 2016, pp. 1–6.

[14] G. Yang, Q. Huang, D. S. Wong, and X. Deng, "Universal authentication protocols for anonymous wireless communications," IEEE Transactions on Wireless Communications, vol. 9, no. 1, pp. 168–174, January 2010.

[15] Q. Yang, K. Xue, J. Xu, J. Wang, F. Li, and N. Yu, "Anfra: Anonymous and fast roaming authentication for space information network," IEEE Transactions on Information Forensics and Security, vol. 14, no. 2, pp. 486–497, Feb 2019.