



International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 4, April 2025

⊕ www.ijirset.com 🖂 ijirset@gmail.com 🖄 +91-9940572462 🕓 +91 63819 07438



International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)



Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404351|

Bio-Hash Secured Hardware E-Health Record System

P.Abirami, B.Arun Kumar, Yashwanth Reddy, A.Akash Kumar

Asst Professor, Department of CSE, Bharath Institute of Higher Education and Research, Selaiyur, Chennai,

Tamil Nadu, India

B. Tech Students, Department of CSE, Bharath Institute of Higher Education and Research, Selaiyur, Chennai,

Tamil Nadu, India

ABSTRACT: In e-healthcare system, an increasing number of patients enjoy high-quality medical services by sharing encrypted personal healthcare records (PHRs) with doctors or medical research institutions. However, one of the important issues is that the encrypted PHRs prevent effective search of information, resulting in the decrease of data usage. Another issue is that medical treatment process requires the doctor to be online all the time, which may be unaffordable for all doctors (e.g., to be absent under certain circumstances). In this paper, we design a new secure and practical proxy searchable re-encryption scheme, allowing medical service providers to achieve remote PHRs monitoring and research safely and efficiently. Through our scheme DSAS, (1) patients' healthcare records collected by the devices are encrypted before uploading to the cloud server ensuring privacy and confidentiality of PHRs; (2) only authorized doctors or research institutions have access to the PHRs; (3) Alice (doctor-in-charge) is able to delegate medical research and utilization to Bob (doctor- in-agent) or certain research institution through the cloud server, supporting minimizing information exposure to the cloud server. We formalize the security definition and prove the security of our scheme. Finally, performance evaluation shows the efficiency of our scheme.



Fig-1: system Architecture



International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)



www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404351| I. INTRODUCTION

With the rapid digitization of healthcare, Personal Healthcare Records (PHRs) have become essential for continuous patient monitoring and medical research. However, ensuring the privacy and secure access of sensitive medical data stored on cloud servers remains a significant challenge. This project aims to develop a secure and practical system using advanced cryptographic techniques like searchable encryption and proxy re-encryption, enabling authorized medical professionals and researchers to access and search encrypted PHRs efficiently. The motivation behind this project is to overcome two major limitations in current e-healthcare systems: the inability to perform keyword searches over encrypted data and the requirement for doctors to be constantly online to manage or monitor patient data. By introducing DSAS (Delegated Secure Access Scheme), our system allows doctors to delegate access rights securely without compromising patient privacy, ensuring uninterrupted medical service even when the primary doctor is unavailable Through this intelligent and privacy- preserving framework, healthcare providers can remotely monitor patient data, conduct research, and deliver quality care efficiently.

II. LITERATURE REVIEW

Machine learning-based method for personalized and cost-effective detection of Alzheimer's disease Diagnosis of Alzheimer's disease is often difficult, especially early in the disease process at the stage of mild cognitive impairment.Yet, it is at this stage that treatment is most likely to be effective, so there would be great advantages in improving the diagnosis process. We describe and test a machine learning approach for personalized and cost-effective diagnosis of AD. It uses locally weighted learning to tailor a classifier model to each patient and computes the sequence of biomarkers most informative or cost-effective to diagnose patients. Using ADNI data, we classified AD versus controls and MCI patients who progressed to AD within a year, against those who did not. The approach performed similarly to considering all data at once, while significantly reducing the number (and cost) of the biomarkers needed to achieve a confident diagnosis for each patient. Thus, it may contribute to a personalized and effective detection of AD, and may prove useful in clinical settings.

III. METHODOLOGY

Existing System:

Machines can predict diseases but often struggle to identify subtypes of diseases caused by the occurrence of another disease. They also fail to predict all possible conditions a patient might experience. Existing systems primarily handle structured data, making their predictions broad and ambiguous. In recent times, numerous disease prediction models have been developed and are in use. These systems typically combine machine learning algorithms that are relatively accurate in predicting diseases. However, they have notable limitations. First, these systems are expensive and often affordable only to wealthy individuals, with costs increasing significantly when applied to larger populations. Second, the prediction systems are nonspecific and vague, meaning that while a machine can predict a primary disease, it cannot accurately foresee subtypes or secondary conditions arising from it. For instance, if a group is predicted to have diabetes, some individuals may also be at high risk for heart diseases due to diabetes, but current systems fail to predict such complex scenarios. Thus, existing models do not account for all potential conditions of a patient.

Proposed System:

We propose a proxy-invisible condition-hiding proxy re-encryption scheme with keyword search to address the issues of inefficiency and condition privacy in the e-healthcare system. Encrypting is considered to be a simple and efficient solution to guarantee data confidentiality, but it also makes search over encrypted data extremely difficult. Searchable encryption technology realizes the search operation of encrypted data without decryption, and solves the problem that users cannot control remotely because of data encryption. Hence, searchable is necessary in the e-healthcare system. In this proposed system, we aim to design an efficient, searchable and privacy-preserving e-healthcare system.



International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)



www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|



Fig 1: Usecase Diagram.

- Data Collection Module
- Preparing the data Module
- Training a model
- Disease prediction Module

IV. IMPLEMENTATION

1. Data Collection and Preprocessing:

The first step in the implementation of the disease prediction system involves collecting relevant health datasets. These datasets typically include information such as patient age, gender, symptoms, medical history, vital signs, and in some cases, sensor-based data like heart rate or oxygen saturation. Once the raw data is collected, it undergoes a thorough preprocessing phase where missing values are handled, categorical variables are encoded, and noise is removed. Normalization or standardization is also applied to ensure all features are on a similar scale, which helps improve the performance of machine learning models.

2. Feature Selection and Engineering:

Once the data is cleaned, the next step is to identify which features are most important for predicting diseases. This process is called feature selection. Techniques like correlation matrix analysis, chi-square tests, and recursive feature elimination are employed to select the most relevant features. Additionally, feature engineering is performed to derive new attributes from existing data. For instance, combining 'age' and 'smoking status' could give a risk factor variable, which might enhance prediction accuracy

3. Model Selection and Training:

After identifying the appropriate features, various machine learning algorithms are considered for training. In our system, we focus on both traditional and advanced models such as Logistic Regression, Decision Trees, Random Forest, Support Vector Machine (SVM), and XGBoost. These models are trained on the preprocessed and labeled dataset using supervised learning techniques.



International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)



www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|



Fig 2: Data flow diagram

V. RESULTS AND CONCLUSION

The implementation of the BIO-HASH Secured Hardware e-Health Record System was aimed at creating a secure, accessible, and privacy-preserving solution for storing and sharing personal health records (PHRs). After successful development and deployment, the system was evaluated under various scenarios to test its efficiency, reliability, and robustness. The results proved the system's capability in securely encrypting PHRs and allowing authorized parties to access them without compromising the data integrity or confidentiality. The encryption mechanism using secure bio-hashing combined with cryptographic algorithms such as AES and RSA provided a strong defense against unauthorized access. The biometric input ensured that only the legitimate user could decrypt or share the health data, which significantly reduced the possibility of identity theft or data misuse. Additionally, the dual authentication model offered an extra layer of security, especially when delegating access to secondary healthcare professionals.



Fig 3: Usecase Diagram



International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)



www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404351| VI. LIMITATIONS AND FUTURE WORK

- The Future scope of this project offers a wide range of promising direction for research, development, and practical deployment in the healthcare domain.
- One of the most significant improvements could be the integration of advanced Artificial Intelligence(AI) and Machine Learning(ML) algorithms with the encrypted searchable re-encryption system.
- These technologies can enable smart search suggestions, predictive analysis, even early diagnosis recommendations, all while maintaining the privacy and confidentiality of patient data.
- Another important enhancement would be the seamless Integration of real-time health monitoring devices such as smartwatches, fitness trackers, and medical-grade wearables

REFERENCES

[1] A. Singh et al., "Heart Disease Prediction Using Machine Learning Algorithms", 2020 International Conference on Electrical and Electronics Engineering (ICE3), pp. 452-457, February 2020.

[2] A Narin, C Kaya and Z. Pamuk, "Automatic detection of coronavirus disease (COVID-19) using x-ray images and deep convolutional neural networks", Mar 2020.

[3] Rajesh. Ranjan, "Predictions for COVID-19 outbreak in India using Epidemiological models", 2020.

[4] Mohan Senthilkumar, Chandrasegar Thirumalai and Gautam Srivastava, "Effective heart disease prediction using hybrid machine learning techniques", IEEE Access, vol. 7, pp. 81542- 81554, 2019.

[5] Mohan Senthilkumar, Chandrasegar Thirumalai and Gautam Srivastava, "Effective heart disease prediction using hybrid machine learning techniques", IEEE Access, vol. 7, pp. 81542- 81554, 2019.

[6] M. Bayati, S. Bhaskar and A. Montanari, "Statistical analysis of a low cost method for multiple disease prediction", Statistical Methods Med. Res., vol. 27, no. 8, pp. 2312-2328, 2018.

[7] A. K. Shrivas and S. Kumar Sahu, "Classification of Chronic Kidney Disease using Feature Selection Techniques", IJCSE, vol. 6, no. 5, pp. 649-653, 2018.

[8] N Chaithra and B Madhu, "Classification Models on Cardiovascular Disease Prediction using Data Mining Techniques", Journal of Cardiovascular Diseases & Diagnosis, vol. 6, pp. 1-4, 2018.

[9] P. K. Mehta, S. Gaignard, A. Schwartz, and J. E. Manson, "Traditional and emerging sex- specific risk factors for cardiovascular disease in women," Rev. Cardiovascular Med., vol. 23, no. 8, p. 288, 2022.

[10] J. M. Alves-silva, M. Zuzarte, and H. Gir, "The role of essential oils and their main compounds in the management of cardiovascular disease risk factors," Molecules, vol. 26, no. 3506, pp. 1–26, 2021.









INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY





www.ijirset.com