iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** V **Month of publication:** May 2023

DOI: https://doi.org/10.22214/ijraset.2023.52030

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: 7.538
Volume 11 Issue V May 2023- Available at www.ijraset.com

Surmising Assault Resistant E-Healthcare Cloud Framework with Fine-Grained Access Control

Mr. D.Shanmugavel[1], M.Sushanth Varma[2], G.Harish[3]
[1, 2, 3]*Department Of Computer science and engineering, Sri Muthu Kumaran Institute of Technology, Chennai*

Abstract: ***The e-medicinal services cloud framework has demonstrated its capability to enhance the nature of social insurance and people's personal satisfaction. Shockingly, security and protection obstruct its broad arrangement and application. There are a few research works concentrating on saving the security of the electronic human services record (EHR) information. In any case, these works have two principle restrictions. In the first place, they just help the 'dark or white' access control strategy. Second, they experience the ill effects of the deduction assault. In this paper, out of the blue, we outline a deduction assault safe e-human services cloud framework with fine-grained get to control. We initially propose a two-layer encryption plot. To guarantee a productive and fine-grained get to authority over the EHR information, we outline the primary layer encryption, where we devise a particular access strategy for every datum trait in the EHR, and encode them independently with high proficiency. To save the security of job traits and access strategies utilized in the principal layer encryption, we deliberately develop the second-layer encryption. To take full favorable position of the cloud server, we propose to give the cloud a chance to execute computationally concentrated chips away at benefit of the information client without knowing any delicate data. To save the entrance example of information properties in the EHR, we additionally build a visually impaired information recovering convention. At last, we lead broad security investigations and execution assessments, which affirm the viability and effectiveness of our plans .***

I. SMART INTRO ABOUT PROJECT

Cloud based health system's main focus is the patient's data collection, storage, acces ,analysis, and presentation etc. The current patient data collection techniques are time consuming, inefficient, laborious for the staffs . It is also obvious that currents technique is violating the real time data access for monitoring the patients .

II. SCOPE

To achieve the fine-grained access control, we need to define a specialized access policy for each data attribute in the EHR. Since different data attributes in the EHR usually share many role attributes in their access policies, for security concerns, we need to conceal the frequency of role attributes occurring in the EHR. Therefore, how to ensure an efficient and correct encryption on the data attributes while preserving the statistical data of the role attributes is a challenging problem.

III. OBJECTIVE

To improve the efficiency of the whole system, the cloud is expected to execute computationally intensive works on behalf of the data users. Thus, how to prevent the cloud from deducing sensitive data, while achieving the above functionality is very important. Since the cloud possesses all the EHR data and is responsible for returning accessed data, how to ensure the cloud correctly and efficiently returns the data attributes without knowing which data attributes are actually returned is also a challenging problem.

IV. EXISTING SYSTEM

Security and privacy will impede the widespread deployment and application of the e-healthcare cloud system. The fundamental reason is that, once the sensitive EHR data are outsourced to the cloud, data owners would lose their control. Although the cloud service providers promise they will preserve these data by installing anti-virus software's, firewalls, and intrusion detection and prevention systems, they cannot stop their employees from accessing these data. For example, an employee in the department of veteran's affairs once takes away million sensitive data without authorization, which includes the social security numbers and sensitive health data. When these sensitive data are abused, more serious problems will occur. For example, insurance companies would refuse to provide insurance to those who have serious health problems. Therefore, it is vital to preserve the security and privacy of EHR data stored in the e-healthcare cloud system.

V. LITERATURE SURVEY

TITLE: Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption.
AUTHOR: M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou.
SURVEY :
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 file attributes, 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.

VI. PROPOSED SYSTEM

We design an patient attack-resistant e-healthcare cloud system with fine-grained access control. We first propose a two-layer encryption scheme. To ensure an efficient and fine-grained access control over the EHR data, we design the first-layer encryption, where we devise a specialized access policy for each data attribute in the EHR, and encrypt them individually with high efficiency. To preserve the privacy of role attributes and access policies used in the first-layer encryption, we systematically construct the second-layer encryption. To take full advantage of the cloud server, we propose to let the cloud execute computationally intensive works on behalf of the data user without knowing any sensitive information. To preserve the access pattern of data attributes in the EHR, we further construct a blind data retrieving protocol. We also demonstrate that our scheme can be easily extended to support search functionality. Finally, we conduct extensive security analyses and performance evaluations, which confirm the efficacy and efficiency of our schemes.

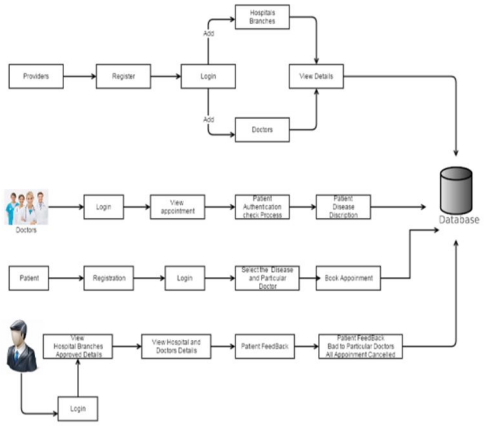
VII. ADVANTAGES

Our scheme not only ensures novel functionalities, but also achieves higher efficiency on encryption, decryption, and role attribute revocation. We design a blind data retrieving protocol, which preserves the access pattern of data attributes in the EHR, and achieves high efficiency. We provide rigorous security analyses and conduct extensive experiments to confirm the efficacy and efficiency of our proposed schemes.

VIII. DISADVANTAGES

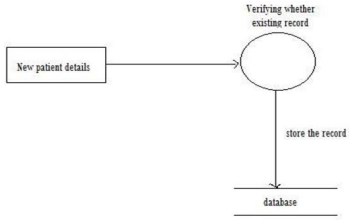
They suffer from the patient attack. The patient attack includes the frequency analysis attack, sorting attack, and cumulative attack.
They have to spend a large amount of time on secret generation for the repeated items.
Cannot assume that the trusted authority and data owners are trusted.

IX. ARCHITECTURE DIAGRAM

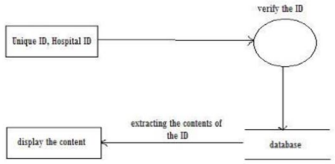


DF(DATA FLOW) DIAGRAM :

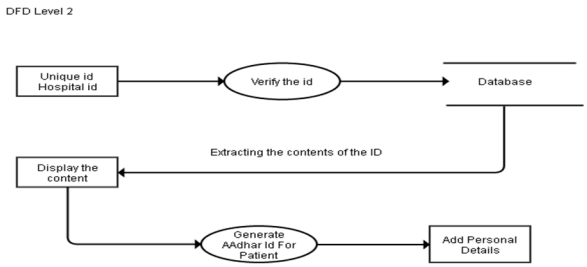
DFD LEVEL 0 :



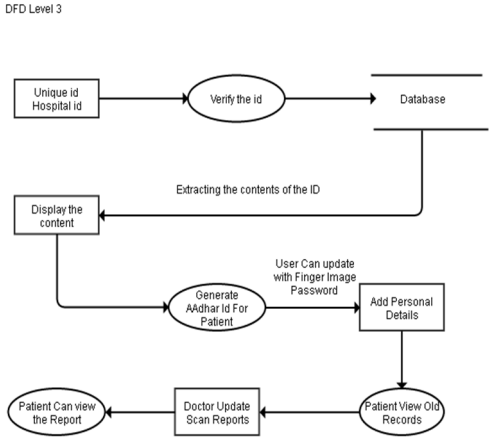
DFD LEVEL 1:



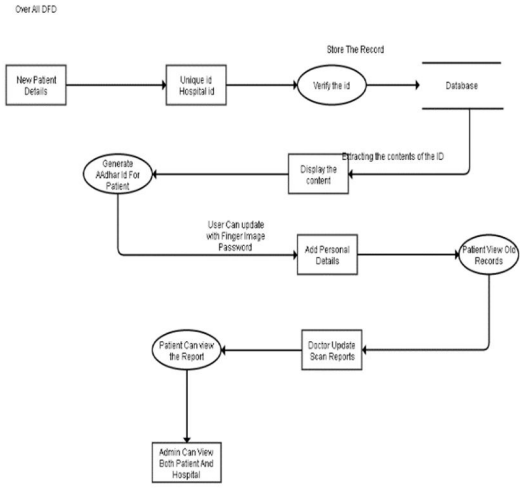
DFD LEVEL 2:



DFD LEVEL 3:



OVER ALL DFD:



X. IMPLEMENTATION PROCEDURE

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective. The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

Each program is tested individually at the time of development using the data and has verified that this program linked together in the way specified in the programs specification, the computer system and its environment is tested to the satisfaction of the user. The system that has been developed is accepted and proved to be satisfactory for the user and so the system is going to be implemented very soon. A simple operating procedure is included so that the user can understand the different functions clearly and quickly.

XI. TESTING

A. Testing Objectives

The main objective of testing is to uncover a host of errors, systematically and with minimum effort and time.

The tests are inadequate to detect possibly present errors

The software more or less confirms to the quality and reliable standards

B. Testing Levels

System testing is stage of implementation which is aimed at ensuring that the system works accurately and efficient before live operation commences. Testing is vital the success of the system. System testing makes a logical assumption that if all the parts of the system are correct, the goal will be successfully achieved.

XII. PROJECT DESCRIPTION

A. Problem Definition

This leads to overhead to the public who wishes to change their doctor of hospital for which the person need to go through all the medical inspections again.

B. Overview

Whenever they go for a treatment, their medical data will be stored into the database using their identification number. 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.

C. Input Design

The input of a system can be defined as the information that is provided to the system. This is used for future processing by the system to obtain meaningful information, which helps in decision-making. Input design is the process of converting user-oriented inputs to a computer-based format.

Input is a part of overall system design, which requires special attention. Inaccurate input data are the most common cause of errors in error processing. Input design can control errors entered by users. Appropriate error message have to be displayed. When an invalid data is entered, the user should not be allowed to type that data.

XIII. CONCLUSION

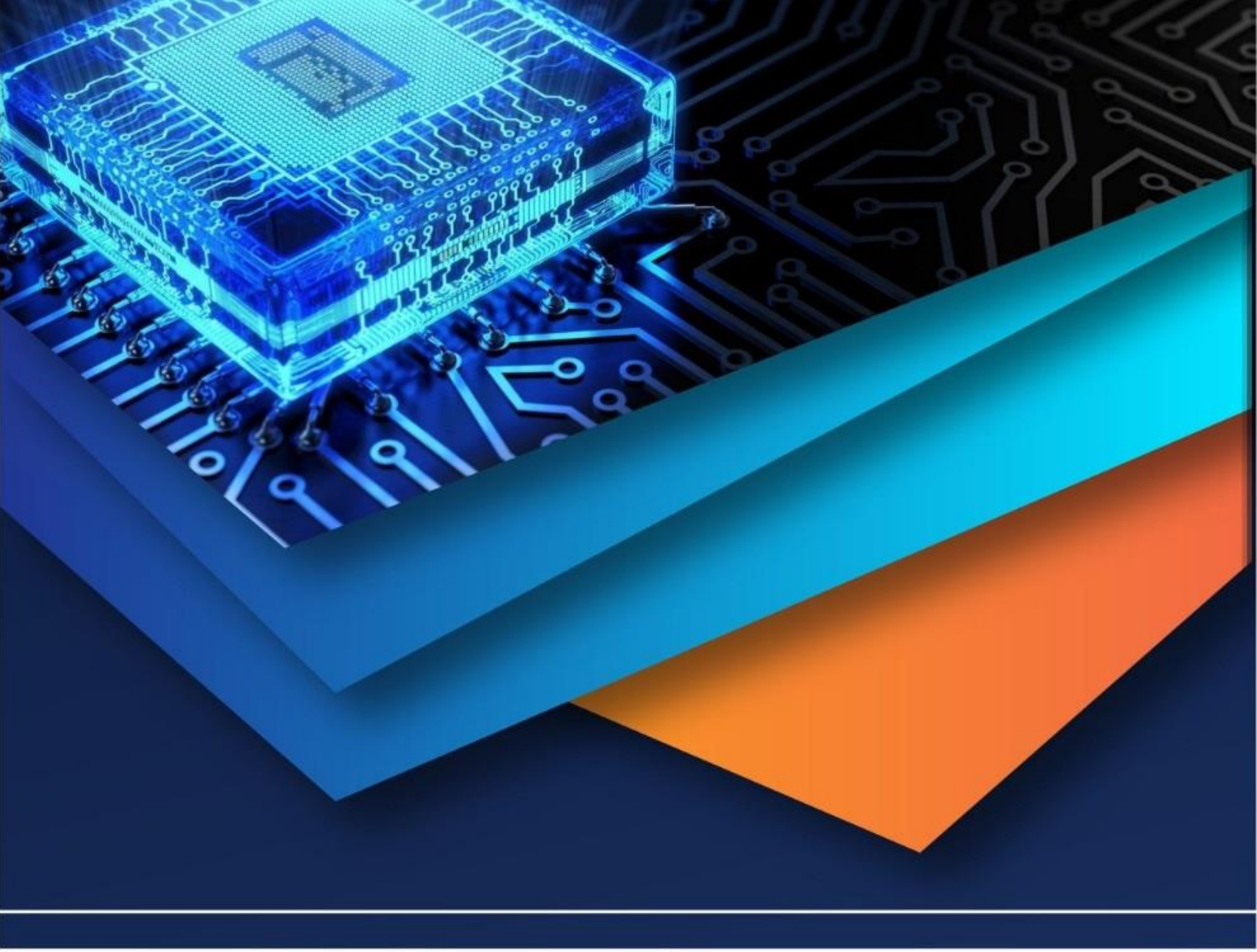
We first propose a two-layer encryption scheme. In the first-layer encryption, we propose to define a specialized access policy for each data attribute in the EHR, generate a secret share for every distinct role attribute, and reconstruct the secret to encrypt each data attribute, which ensures a fine grained access control, saves much encryption time, and conceals the frequency of role attributes occurring in the EHR. In the second-layer encryption, we propose to preserve the privacy of role attributes and access policies used in the first-layer encryption. Additionally, to take full advantage of the cloud server, we propose to let the cloud execute computationally intensive works on behalf of the data user without knowing any sensitive information. To preserve the access pattern of the data attributes in the EHR, we construct a blind data retrieving protocol based on the Paillier encryption.

XIV. FUTURE WORK

The need of an online certificate authority (CA) and one unique key encryption for each symmetric key k for data encryption at the portal of authorized physicians made the overhead of the construction grow linearly with size of the group. Furthermore, the anonymity level depends on the size of the anonymity set making the anonymous authentication impractical in specific surroundings where the patients are sparsely distributed .

REFERENCES

[1] Google fit. [Online]. Available: https://developers.google.com/fit
[2] Healthkit. [Online]. Available: https://developer.apple.com/healthkit
[3] Ibm Watson health cloud. [Online]. Available: http://www.ibm.com/smarterplanet/us/en/ibmwatson/health
[4] Y. Zhu, G.-J. Ahn, H. Hu, S. S. Yau, H. G. An, and C.-J. Hu, "Dynamic audit services for outsourced storages in clouds," IEEE Transactions on Services Computing, vol. 6, no. 2, pp. 227– 238, 2013.
[5] H. Tian, Y. Chen, C.-C. Chang, H. Jiang, Y. Huang, Y. Chen, and J. Liu, "Dynamic-hash-table based public auditing for secure cloud storage," IEEE Transactions on Services Computing, pp. 1–10, 2015.
[6] W. Zhang, Y. Lin, S. Xiao, Q. Liu, and T. Zhou, "Secure distributed keyword search in multiple clouds," in Proc. IEEE/ACM IWQOS'14. Hongkong: IEEE/ACM, May 2014, pp. 370–379.
[7] W. Zhang, S. Xiao, Y. Lin, T. Zhou, and S. Zhou, "Secure ranked multi-keyword search for multiple data owners in cloud computing," in Proc. 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN2014). Atlanta, USA: IEEE, jun 2014, pp. 276–286.
[8] D. Nascimento and M. Correia, "Shuttle: Intrusion recovery for paas," in Proc. IEEE Distributed Computing Systems (ICDCS'15), Ohio, USA, Jun. 2015, pp. 10–20.
[9] At risk of exposure -in the push for electronic medical records, concern is growing about how well privacy can be safeguarded. [Online]. Available: http://articles.latimes.com/2006/jun/26/health/heprivacy26



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY