IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Inference Attack-Resistant E-Healthcare System with Fine-Grained Access Control

V. Venkata Sai Teja[1], R. Naga Sowmya Priya[1], R. Yagnika[1], SK. Laahira [1] , Mr. CH. Ambedkar[2]

Student[1], Department of computer science and engineering, SRK Institute of Technology, NTR, Andhra Pradesh, India

Associate Professor[2], Department of computer science and engineering, SRK Institute of Technology, NTR, Andhra Pradesh, India

ABSTRACT

The e-healthcare cloud system has shown its potential to improve the quality of healthcare and individuals' quality of life. Unfortunately, security and privacy impede its widespread deployment and application. There are several research works focusing on preserving the privacy of the electronic healthcare record (EHR) data. 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 We proposed User revocation is commonly supported in such schemes, as users may be subject to group membership changes for various reasons. Previously, the computational overhead for Auto user revocation. We include binary key generation for file storage. File encryption we proposed time enable proposed re encryption.

Key Words: Electronic healthcare record (EHR) , Inference Attack-Resistant, Fine Grained Access Control, Three layered encryption.

INTRODUCTION

The Electronic healthcare, providing timely, accurate, and low-cost healthcare services, has shown its potential to improve the quality of healthcare and individuals. 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. 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. the first-layer encryption, the data owner conceals this is access policy, and conducts the second-layer encryption. After that, the data owner outsources the encrypted EHR data, the encrypted first-layer access policy, and the second-layer access policy to the cloud. Finally, the data user conducts the first-layer decryption and obtains the authorized data attributes in the EHR.

PROBLEM STATEMENT

In modern e-healthcare systems, electronic health records (EHRs) are widely used to store and manage sensitive patient data. While access control mechanisms are implemented to prevent unauthorized access, traditional models often fail to prevent **inference attacks**, where attackers can derive sensitive information by analyzing access patterns or correlating authorized data. Furthermore, existing systems frequently lack **fine-grained access control**, leading to over-privileged access and increased risk of privacy breaches.

There is a critical need for a secure e-healthcare framework that not only enforces fine-grained, role- and context-aware access control but also effectively resists inference attacks. The challenge lies in balancing **data utility**, **user accessibility**, and **patient privacy**, while maintaining **system scalability** and **performance efficiency**.

This research aims to design and develop an inference attack-resistant e-healthcare system that ensures only the minimum necessary information is disclosed, based on the user's role, intent, and context, without compromising the integrity and confidentiality of patient data.

MOTIVATION

The rapid digitization of the healthcare sector has revolutionized the management and accessibility of patient data. Electronic Health Records (EHRs) allow healthcare providers to deliver faster and more efficient services. However, this digital transformation also introduces significant **privacy and security challenges**.

Key Features:

- **Fine-Grained Access Control**
  Access based on user role, purpose, and data sensitivity.
- **Inference Attack Resistance**
  Prevents indirect data leaks through smart access monitoring.
- **Role & Purpose-Based Access**
  Ensures users only access data they truly need.
- **Audit & Logging**
  Tracks all access for transparency and security.
- **Dynamic Policy Updates**
  Adapts access rules in real time (e.g., emergencies, consent changes).

LITERATURE REVIEW

1.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.

Zhu et al. (2013) proposed **dynamic audit services** for outsourced cloud storage, ensuring data integrity and secure access in untrusted environments. Their work laid a foundation for access control frameworks in e-healthcare cloud systems, where both **security** and **auditability** are critical.

2. Shaobo Zhang et al. – "A Fine-Grained Access Control Scheme for Electronic Health Records Based on Roles and Attributes" (2022):[2]

This study proposes a hybrid access control model combining Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) to enhance security in EHR systems. The model aims to mitigate inference attacks by ensuring that access decisions consider both user roles and specific attributes, thereby providing a more granular level of access control..

3.Qin Liu et al. – "Fine-Grained Access Control with User Revocation in Cloud-Based Personal Health Record System" (2017): [3]

This paper presents a scheme that integrates Broadcast Ciphertext-Policy Attribute-Based Encryption (BCP-ABE) with an attribute hierarchy to achieve fine-grained access control and real-time user revocation in cloud-based Personal Health Record (PHR) systems. The approach aims to balance security requirements with system performance.

4. Yuemin Zhang, et al. "A Fine-Grained Access Control Scheme for Electronic Health Records Based on Trust and Role" (2019): [4]

This paper combines **Role-Based Access Control (RBAC)** with a **trust management** approach to implement **fine-grained access control** in **electronic health records (EHR)**. It assigns **trust levels** to users based on their past interactions with the system, allowing dynamic access control based on **trustworthiness** in addition to user roles.

5. Shuangfei Wu, et al. "Privacy-Preserving Fine-Grained Access Control for Electronic Health Records in Cloud Computing" (2020): [5]

This study presents a **privacy-preserving fine-grained access control mechanism** for **cloud-based EHR systems**. The system leverages **Cryptographic Techniques** such as **Attribute-Based Encryption (ABE)** and **Access Control Lists (ACLs)** to ensure that health data is shared securely. This method also guarantees the privacy of medical records while allowing **flexible and granular access** to data.

6. S. S. Dinesh, A. S. Rajasekaran, and K. Duraiswamy, "A Secure and Efficient Fine-Grained Access Control Scheme for Electronic Health Records in Cloud Computing" (2018):[6]

This paper presents a **fine-grained access control scheme** for **cloud-based Electronic Health Records (EHRs)** using a combination of **Attribute-Based Encryption (ABE)** and **Role-Based Access Control (RBAC)**. It aims to ensure **secure sharing** of health data while allowing healthcare providers to access specific records based on user roles and attributes like medical conditions.

7. A. Subashini, A. S. Sadiq, and P. A. Venkatesh, "Privacy-Preserving and Fine-Grained Access Control for E-Health Records in Cloud Computing" (2020):[7]

This research focuses on a **privacy-preserving fine-grained access control mechanism** for **E-health records** in the cloud. It uses a combination of **attribute-based encryption** and a hybrid approach to implement **dynamic access controls** that can adapt to the roles and attributes of users while maintaining patient privacy.

8. R. Srinivasan, M. S. Ravi, and K. R. Ramakrishnan, "Fine-Grained Access Control for Electronic Health Records Using Role-Based Access Control and Attribute-Based Encryption" (2017): [8]

This paper introduces a hybrid model that combines **Role-Based Access Control (RBAC)** with **Attribute-Based Encryption (ABE)** for **fine-grained access control** of **electronic health records**. The model ensures that sensitive health data is accessible only by authorized users based on their roles and specific attributes, such as medical history or specialization.

9.K. N. Radhakrishnan, A. C. Sreeja, and R. Vishal, "Secure Data Sharing and Fine-Grained Access Control for Health Information Systems" (2019): [9]

This paper proposes a **fine-grained access control** mechanism based on **cloud-based health information systems**. The system uses a hybrid approach, integrating **RBAC** with **Attribute-Based Access Control (ABAC)** to ensure that health information can be shared securely among healthcare professionals.

10. V. S. Venkatesh, P. S. Manogaran, and K. S. Srinivas, "Privacy-Preserving Fine-Grained Access Control for E-Health Records in Cloud Systems" (2021): [10]

This paper presents a **privacy-preserving approach** to **fine-grained access control** for **E-health records** in cloud environments. The method combines **policy-based access control** and **encryption techniques** to secure sensitive health data. The system ensures that users access only the necessary information, without exposing unrelated sensitive data.

EXISTING SYSTEM:

First Specifically, once a data user is authorized, he can access all the data attributes in the EHR. For example, if a dentist is authorized to access a patient‘s EHR, then he can even access the patient‘s social status Second, they suffer from the inference attack. The inference attack includes the frequency analysis attack, sorting attack, and cumulative attack. Among them, the most well-known attack is the frequency analysis attack, which breaks the classical encryption algorithms. Existing schemes adopt the conventional ciphertext policy attribute-based encryption to encrypt the EHR, which inevitably exposes the access policy to the cloud. Third, they have to spend a large amount of time on secret generation for the repeated items. Each data attribute has its own role attributes. As we can see, there are a lot of repeated role attributes in the EHR. In conventional schemes, instead of generating ciphertext. The efficiency can be improved by nearly three times in this example. Since the data attributes in the EHR often have a lot of repeated role attributes, we need to propose schemes to save the computation cost spent on the repeated role attributes.

PROPOSED SYSTEM:

To ensure an efficient and fine-grained access control over the EHR data. e 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 provide rigorous security analyses and conduct extensive experiments to confirm the efficacy and efficiency of our proposed schemes. : Our proposed scheme should control the privacy protection to a specific level. We measure the privacy disclosure of our scheme by the attacker‘s confidence in the success of an attack. our proposed scheme, and show that the security and privacy goals have been achieved. We first prove the two-layer encryption scheme. User revocation is commonly supported in such schemes, as users may be subject to group membership. We include binary key generation for file storage. file encryption we proposed time enable proposed re encryption.

METHODOLOGY: Alumni Management System has 7 modules:

1. Identification of Data Sensitivity and Access Requirements

Data Classification:

- Identify and classify different types of healthcare data, such as **patient personal information**, **medical records**, **test results**, and **treatment histories**.
- Label data based on **sensitivity**, such as highly sensitive data (e.g., mental health records, HIV status) and less sensitive data (e.g., general consultation notes).

Access Levels:

- Define **access levels** for different roles (e.g., doctors, nurses, administrative staff, and patients).
- **Specify which roles can access specific data types based on the level of sensitivity.**

2. Fine-Grained Access Control Mechanism Design

- **Role-Based Access Control (RBAC)**: Roles are defined based on job functions within the healthcare system. Each role is assigned specific permissions to access the required data. For example, a **doctor** might have access to a patient's medical history, while a **nurse** may only access basic treatment data.
- **Attribute-Based Access Control (ABAC)**: In addition to roles, the system uses attributes like a patient's **medical condition**, **department**, **time of access**, and **location** to make dynamic access control decisions. This allows the system to grant access only when certain conditions (attributes) are met.
- **Policy Enforcement**: Policies for access control are enforced based on roles, user attributes, and

environmental conditions (e.g., device type, access time).

3. Preventing Inference Attacks

Data Minimization:

- Only provide the **necessary data** to users based on their access rights. This ensures that users cannot infer sensitive information by piecing together multiple non-sensitive records.
- For example, when a nurse accesses a patient's medication record, the system should ensure that **diagnostic details** that could be used to infer sensitive medical conditions (e.g., HIV status) are **excluded**.

Access Pattern Obfuscation:

- Use **query obfuscation** techniques to hide access patterns from attackers. For example, if an unauthorized user tries to infer information by examining access logs, the system can obfuscate or randomize access timestamps and patterns.
- **Fake records** or **dummy data** could be inserted into access logs, making it difficult for attackers to infer sensitive information based on access history.

4. Attribute-Based Encryption (ABE)

- **Key Generation**: Each user is assigned a set of **attributes** that define the level of access they have to encrypted data.
- **Data Encryption**: The healthcare data is encrypted using an encryption algorithm that links the data to certain **attributes**. Only users who meet the required attributes (e.g., role, department, medical condition) can decrypt the data.
- **Fine-Grained Decryption**: When a user attempts to access a record, the system checks if the user's attributes match the encrypted data's required attributes, and only then will the data be decrypted.

5. Ongoing Monitoring and Maintenance

- **Continuous Monitoring**:
  After deployment, continuously monitor access patterns and audit logs for suspicious activities that could suggest inference attempts.
- **System Updates**:
  Regularly update encryption algorithms, access control policies, and user authentication methods to keep up with evolving threats and technological advancements.

6. Data Auditing and Monitoring

- **Audit Logs**:
  Maintain detailed **audit logs** for every access attempt to healthcare data, including successful and failed access attempts, queries, and modifications.
  The system should log **who** accessed **what** data and **when**, to allow administrators to detect unusual or unauthorized access patterns.

- **Access Pattern Analysis**: Access pattern analysis is a **critical vulnerability vector** in e-healthcare systems. Even if data is encrypted and access is controlled, patterns in data access can **leak private information**. Combining fine-grained access control with techniques like **ORAM, PIR, and noise injection** is essential to build a system that is **resistant to inference attacks**.

RESULTS & ANALYSIS

Figure1: Admin Panel

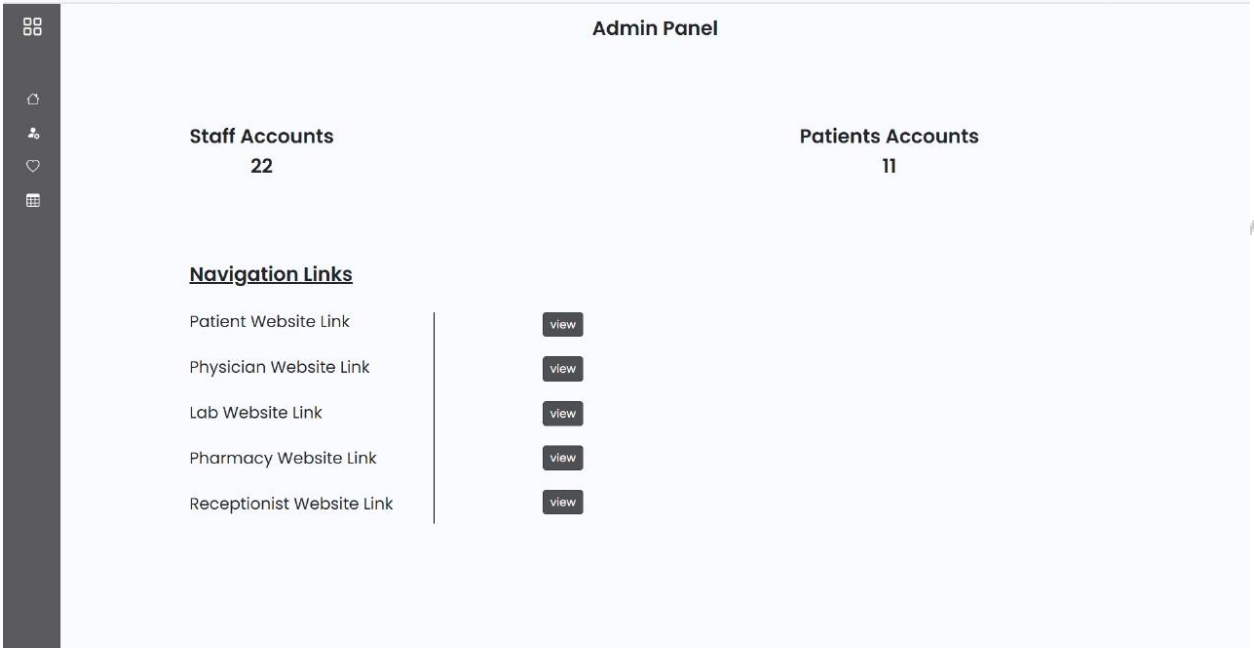

Figure2: Admin panel after login

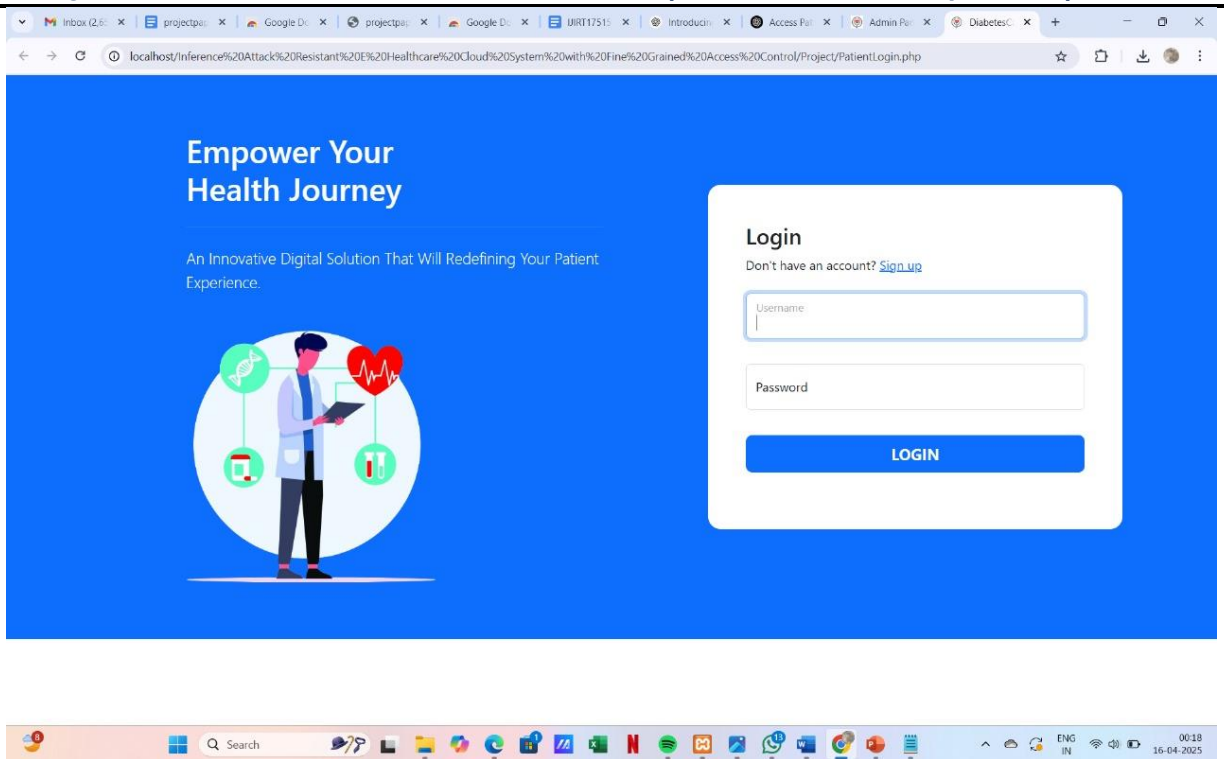

Figure 3: Patient Login

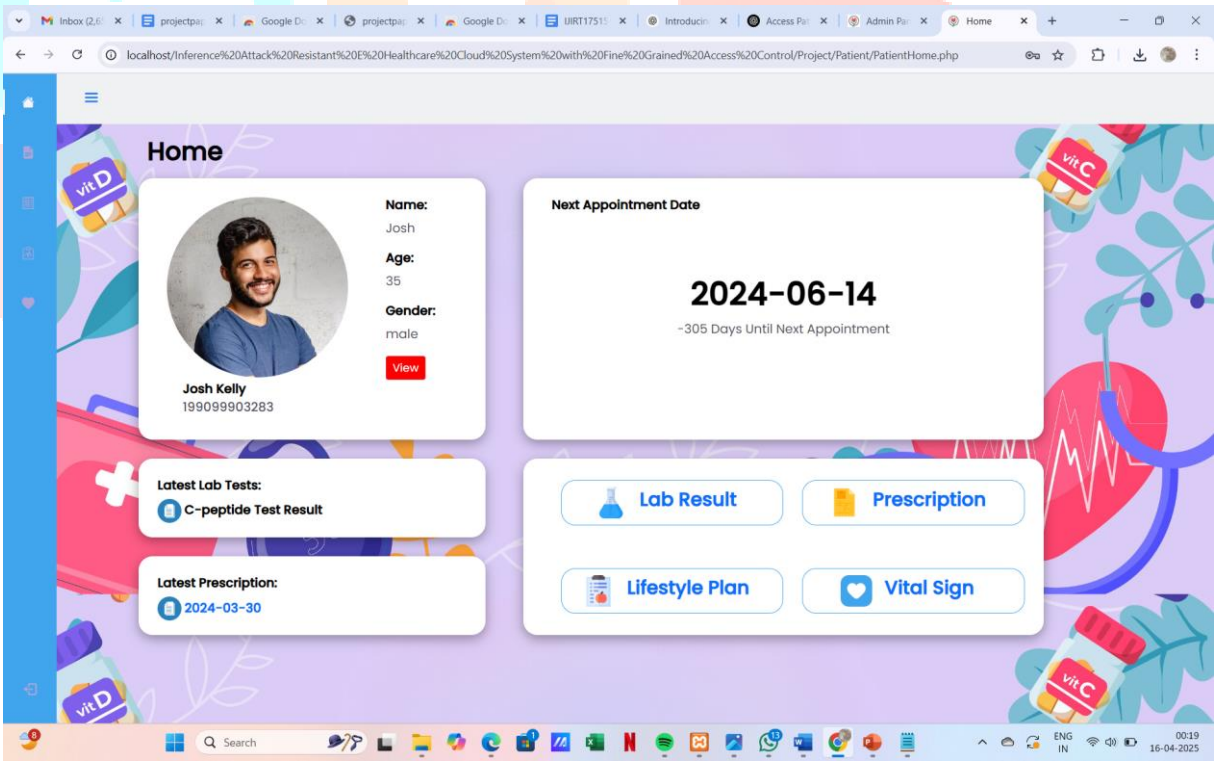

Figure 4: Patient Details

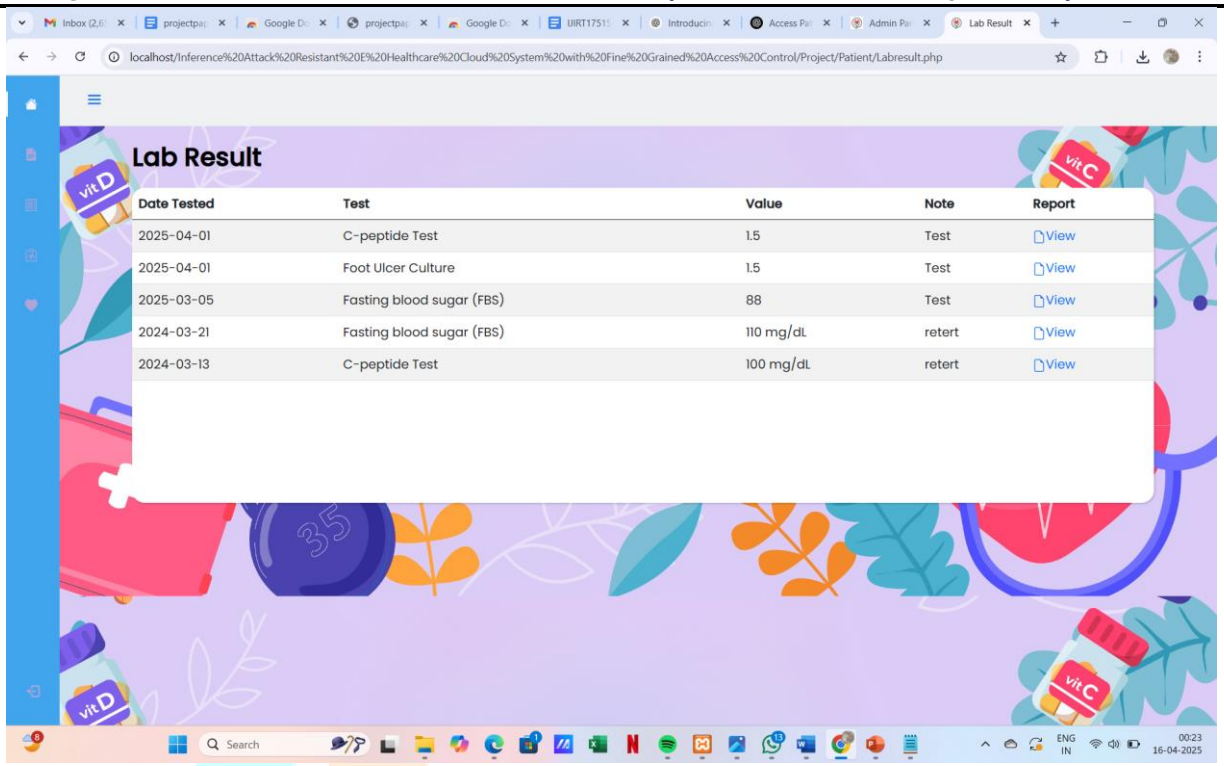

Figure5: Patient Lab Reports

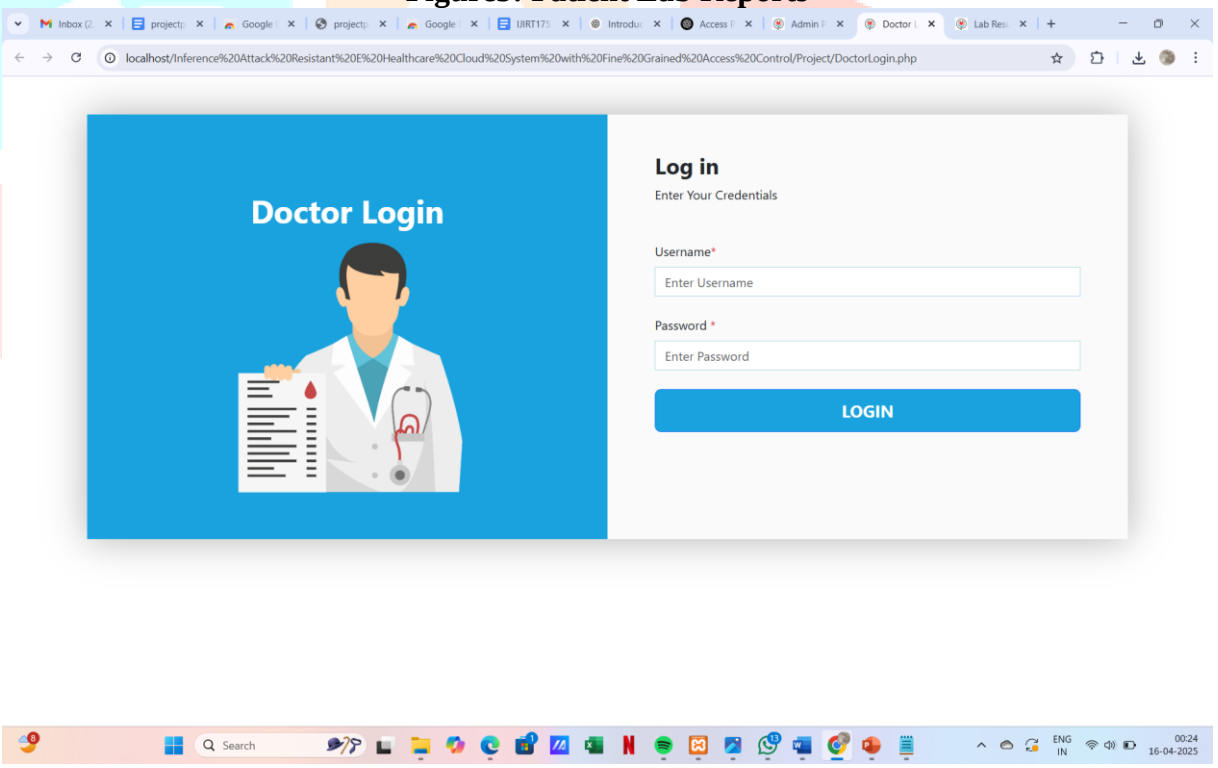

Figure8: Doctor Login

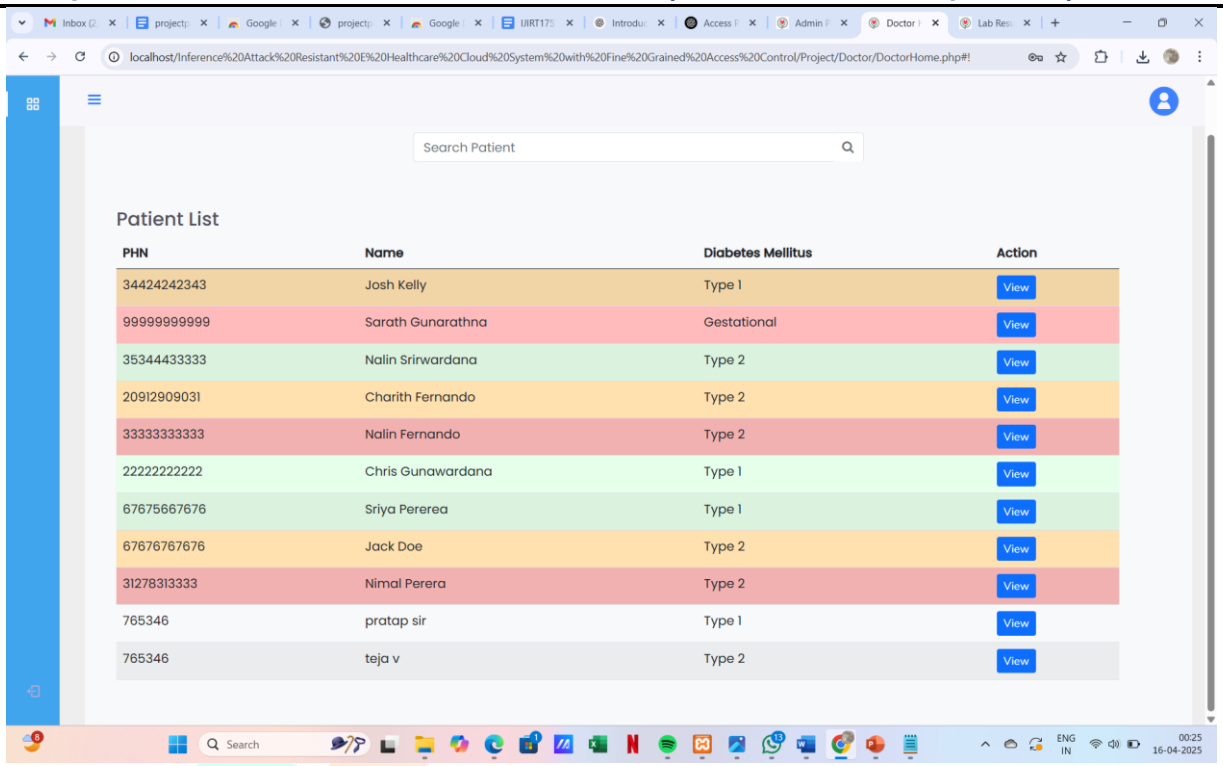

Figure 9: Doctor's Patients list.

CONCLUSION:

We design an inference attack resistant e healthcare cloud system with fine grained access control. We first propose a Time proxy re encryption scheme. 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. To preserve the access pattern of the data attributes in the EHR, we construct a blind data retrieving protocol based on the Paillier encryption. provides the encryption module for the re-encryption and also time privileges for accessing particular files. This will enable each user's access right to be effective in a predetermined period of time, and enable the CSP to re-encrypt cipher texts automatically, based on its own time. In order to deal with user revocation, Time based PRE was implemented to provide access. since we embed randomness there. Additionally, the inference attack described in our paper is launched by observing the role attributes, access policy, and access pattern(access frequency). With our constructions, we can prevent the attackers from achieving the inference attacks. We aim to systematically construct a secure and privacy preserving e-health cloud system, so that it is immune to the inference attack and runs efficiently.

REFERENCES

[1] Y. Zhu, G.-J. Ahn, H. Hu, S. S. au, 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.

[2] Shaobo Zhang et al. – "A Fine-Grained Access Control Scheme for Electronic Health Records Based on Roles and Attributes" (2022).

[3] Qin Liu et al. – "Fine-Grained Access Control with User Revocation in Cloud-Based Personal Health Record System" (2017).

[4] Yuemin Zhang, et al. "A Fine-Grained Access Control Scheme for Electronic Health Records Based on Trust and Role" (2019).

[5] Shuangfei Wu, et al. "Privacy-Preserving Fine-Grained Access Control for Electronic Health Records in Cloud Computing" (2020)

[6] S. S. Dinesh, A. S. Rajasekaran, and K. Duraiswamy, "A Secure and Efficient Fine-Grained Access Control Scheme for Electronic Health Records in Cloud Computing" (2018)

[7] A. Subashini, A. S. Sadiq, and P. A. Venkatesh, "Privacy-Preserving and Fine-Grained Access Control for

E-Health Records in Cloud Computing" (2020).

[8] R. Srinivasan, M. S. Ravi, and K. R. Ramakrishnan, "Fine-Grained Access Control for Electronic Health Records Using Role-Based Access Control and Attribute-Based Encryption" (2017)

[9] K. N. Radhakrishnan, A. C. Sreeja, and R. Vishal, "Secure Data Sharing and Fine-Grained Access Control for Health Information Systems" (2019)

[10]V. S. Venkatesh, P. S. Manogaran, and K. S. Srinivas, "Privacy-Preserving Fine-Grained Access Control for E-Health Records in Cloud Systems" (2021)