

A Seminar on

SECURE HEALTH: DYNAMIC INTEGRITY- ASSURED SHARED EHR DATABASE WITH PRIVACY-PRESERVING FUNCTIONAL COMMITMENT

Team Details

Team No-17

1. A.Nagaraju (21EG505803)
2. G.Ramya (21EG505823)
3. M.Keerthana (21EG505847)

Project Supervisor

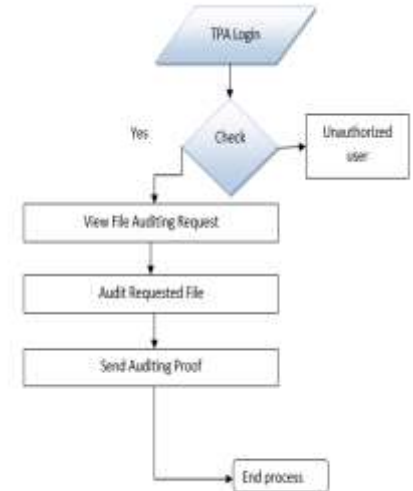
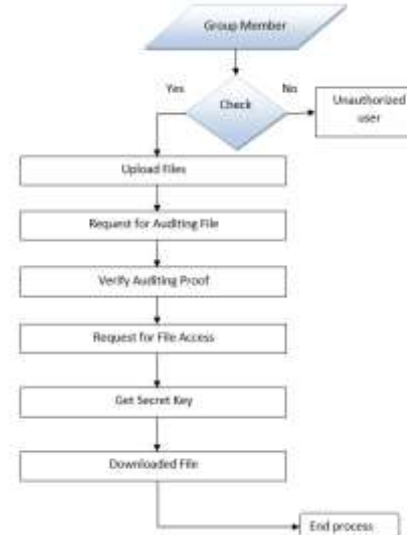
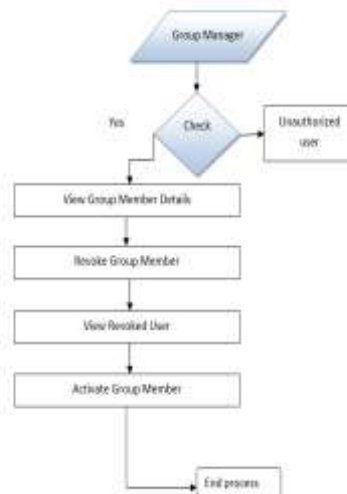
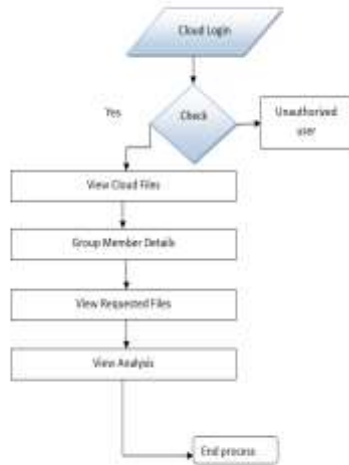
Mrs.A.Durga Bhavani

Assistant Professor

Introduction

The increasing reliance on Electronic Health Record (EHR) systems, coupled with the rise of resource-constrained IoT devices, demands robust solutions. In response, we propose a Publicly Verifiable Shared Updatable EHR Database Scheme. Unlike existing Verifiable Database (VDB) models, our approach prioritizes real-time proof generation, minimizing user overhead for storage integrity checks. By modifying the Functional Commitment (FC) scheme and incorporating a verifier-local revocation group signature, our scheme ensures privacy preservation, batch integrity checking, and dynamic group member operations. This innovative solution addresses the dual challenges of security and efficiency in EHR systems, contributing to the seamless and secure exchange of sensitive patient information in the digital healthcare landscape.

Concept Tree



Literature

Author(s)	Method	Advantages	Disadvantages
Wei L, Wu C, Zhou S. (2022)	Functional Commitment, Privacy-Preserving Integrity Auditing Dynamic Group Operations, Sparse Vector for Sampling Auditing.	<ol style="list-style-type: none"> 1.Efficiency Improvement 2.Privacy Preservation 3.Dynamic Group Management 4.Minimum User Communication Cost 	<ol style="list-style-type: none"> 1.Complexity 2.Security Assumptions 3.Auditor Involvement 4.Scalability
Dan B, Shacham H. (2022)	Verifier-Local Revocation: The group signature scheme likely employs a strategy where a verifier can locally revoke a member's signature. This allows for efficient management of user access rights and enhances the scheme's flexibility.	<ol style="list-style-type: none"> 1.Granular Revocation: Verifier-local revocation allows for targeted revocation of specific users without affecting the entire group, providing a granular and efficient approach to access control. 2.Enhanced Flexibility 	<ol style="list-style-type: none"> 1.Complexity: Implementing verifier-local revocation may introduce additional complexity to the system, potentially making it more challenging to design, implement, and maintain.

Literature

Author(s)	Method	Advantages	Disadvantages
Chaum, David, and T. P. Pedersen. (2021)	Wallet Databases: The paper likely introduces the concept of wallet databases, indicating a focus on secure and privacy-preserving storage solutions for digital wallets.	<p>1.Security Enhancement: Wallet databases could enhance the security of digital wallets by introducing cryptographic techniques to protect sensitive financial information.</p> <p>2.Privacy Considerations: The use of observers in wallet databases suggests a privacy-centric approach, allowing controlled access to wallet information.</p>	<p>1.Implementation Challenges: Depending on the proposed mechanisms, implementing secure wallet databases may pose challenges, particularly in integrating with existing financial systems and user interfaces.</p>

Literature

Author(s)	Method	Advantages	Disadvantages
B. Dan, X. Boyen, E. J. Goh(2023)	Hierarchical Identity-Based Encryption (HIBE): The paper likely presents an encryption scheme that supports a hierarchical identity structure, enabling efficient key management.	1.Scalability 2.Constant Size Ciphertext: The achievement of constant-size ciphertext is advantageous for efficient data transmission and storage.	1.Key Management Complexity: Implementing HIBE schemes may introduce complexities in key management, particularly in maintaining the hierarchical structure securely.
A. Kate, G. M. Zaverucha, I. Goldberg(2022)	Constant-Size Commitments: The paper likely introduces techniques for achieving constant-size commitments to polynomials, a useful concept in cryptographic protocols	1.Efficient Cryptographic Protocols: Constant-size commitments can enhance the efficiency of cryptographic protocols, particularly in scenarios where data size is a critical factor. 2.Application Flexibility	1.Applicability Constraints: Depending on the specific use cases, achieving constant-size commitments may have constraints or limitations in certain cryptographic scenarios.

Problem Statement

- In the context of Electronic Health Records (EHR) storage, existing verifiable database (VDB) approaches face challenges in proof reuse and server-driven updates, hindering effective data integrity checks. We propose an innovative updatable VDB scheme based on functional commitment, addressing privacy-preserving integrity auditing and group member operations. Our scheme prioritizes server response correctness and data storage integrity, aiming for security without excessive computational overhead. We design an updatable functional commitment scheme and present a practical VDB scheme under computational assumptions. Batch auditing enhances efficiency in multi-cloud, multi-user scenarios. Theoretical proofs affirm desired security properties, with our scheme outperforming alternative algorithms
- **Existing Method Disadvantages:**
 1. The primary challenge in EHR systems lies in ensuring real-time verification of server responses.
 2. The existing VLR group signature scheme does not have backward unlinkability (BU), which means that even if a member is revoked at a certain time, the signature before that time remains anonymous. It poses a threat to user identity privacy.


Problem Illustration

The verifiable database (VDB) as a secure and efficient updatable cloud storage model for resource-limited users. In a VDB scheme, a client can outsource the storage of a collection of data items to an untrusted server. Later, the client can query the server for an item (a message) at position i , the server returns the stored message at this position along with a proof that it is the correct answer. However, the security of only verifying the server response correctness is far from enough for the EHR system, and it is not clear whether data that is not frequently accessed is still stored correctly. If these data are destroyed and not discovered in time, it can cause huge losses in the event of an emergency.

Proposed Method

Focusing on secure and efficient storage, emphasizing server response correctness and data storage integrity for Electronic Health Records (EHR). Utilizes functional commitment (FC) to design a publicly verifiable updatable database scheme, addressing privacy-preserving integrity auditing and dynamic group operations. Enhances an existing FC scheme for an auditable Verifiable Database (VDB) scheme, proposing an efficient, publicly verifiable updatable VDB with minimal computational overhead and storage costs. Applicable for large-scale data storage, ensuring minimum user communication cost. Preserves original VDB scheme properties while achieving efficient privacy features and auditability.

Proposed Method Illustration



Select File :

(You file selected)

Select Access/Members :

- ☐ Clinic
- ☐ HealthCare
- ☐ Hospital
- ☐ Medicine Center
- ☐ Insurance

Preview File :



File ID	File Name	Member Name	Role	Uploaded Time
1	check.txt	Abdul	[Clinic, HealthCare, Hospital]	2021/04/05 15:46:07
2	laptop.txt	Abdul	[Clinic, MedicineCenter, Insurance]	2021/04/05 15:50:38
3	mobile.txt	Iadhi	[Clinic, HealthCare, Hospital]	2021/04/05 16:16:55
4	check.txt	Abdul	[Clinic]	2021/04/07 11:29:35
5	keypolicy flow.txt	santosh	[MedicineCenter]	2021/04/07 11:32:08

Parameters Considering :

- ❖ The scheme preserves data privacy from the auditor by using a random masking technique and the sparse vector is used for sampling auditing.
- ❖ Our scheme supports dynamic group member operations which include join and revocation. In addition, our VDB supports batch auditing and it supports multi-cloud server, multiuser and multi-storage vector scenarios.
- ❖ Security analysis and experimental comparison with existing schemes are provided and it shows that our VDB is secure and efficient.
- ❖ Our VDB scheme can securely and efficiently query and update database stored in the cloud and publicly audit data storage integrity

Experiment Environment

Tools:

- NETBEANS
- MY SQL

Language:

- JAVA

Frontend:

- HTML
- CSS
- JAVASCRIPT

Project Status

S.No	Functionality	Status (Completed /in-progress/Not started)
01	Research Paper Collection	Completed
02	Collection of Information	Completed
03	Code Implementation	In-Progress
04	Documentation	Not Started

References

1. Wei L, Wu C, Zhou S. efficient verifier-local revocation group signature schemes with backward unlinkability. Chinese Journal of Electronics, 2022, e90-a(2):379-384.
2. Dan B, Shacham H. Group signatures with verifier-local revocation. Acm Conference on Computer & Communications Security. 2022.
3. Chaum, David, and T. P. Pedersen. Wallet Databases with Observers. International Cryptology Conference on Advances in Cryptology 2021.
4. B. Dan, X. Boyen, E. J. Goh, “Hierarchical identity based encryption with constant size ciphertext”, International Conference on Theory and Applications of Cryptographic Techniques. Springer-Verlag, pp. 440- 456, 2023.
5. A. Kate, G. M. Zaverucha, I. Goldberg, “Constant-Size Commitments to Polynomials and Their Applications”, Advances in Cryptology - ASIACRYPT 2010 -, International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 5-9, 2022. Proceedings. DBLP, pp. 177-194, 2022.

Thank You