ISSN: 2454-9940

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

E-Mail :
editor.ijasem@gmail.com
editor@ijasem.org

www.ijasem.org

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN2454-9940

www.ijasem.org

Vol 18, Issue.2 April 2024

Secure Health: Dynamic Integrity-Assured Shared EHR Databases with Privacy-Preserving Functional Commitment

Mrs. A.Durga Bhavani	Avula Nagaraju	Ganapuram Ramya	Mande Keerthana
Assistant Professor, CSE	21eg505803	21eg505823	21eg505847
Anurag group of institutions	Anurag group of Institutions	Anurag group of Institutions	Anurag group of Institutions
durgabhavanicse@anurag.edu.in	21eg505803@anurag.edu.in	21eg505823@anurag.edu.in	21eg505847@anurag.edu.in

ABSTRACT: Electronic health record (EHR) is a system that collects patients' digital health information and shares it with other healthcare providers in the cloud. Since EHR contains a large amount of significant and sensitive information about patients, it is required that the system ensures response correctness and storage integrity. Meanwhile, with the rise of IoT, more low-performance terminals are deployed for receiving and uploading patient data to the server, which increases the computational and communication burden of the EHR systems. The verifiable database (VDB), where a user outsources his large database to a cloud server and makes queries once he needs certain data, is proposed as an efficient updatable cloud storage model for resource-constrained users. To improve efficiency, most existing VDB schemes utilize proof reuse and proof updating technique to prove correctness of the query results. However, it ignores the "real-time" of proof generation, which results in an overhead that the user has to perform extra process (e.g. auditing schemes) to check storage integrity. In this paper, we propose a publicly verifiable shared updatable EHR database scheme that supports privacy-preserving and batch integrity checking with minimum user communication cost. We modify the existing functional commitment (FC) scheme for the VDB design and construct a concrete FC under the computational l -BDHE assumption. In addition, the use of an efficient verifier-local revocation group signature scheme makes our scheme support dynamic group member operations, and gives nice features, such as traceability and non-frameability.

KEYWORDS: Verifiable database, cloud storage, functional commitment, privacy-preserving auditing, user revocation

I. Introduction

In today's rapidly evolving digital landscape, the proliferation of global information has ignited an unprecedented surge in the cloud service industry. Leading the charge are tech giants like Amazon, Google, Alibaba, Microsoft, and Huawei, each vying to establish dominance by offering cutting-edge cloud platforms and products. This meteoric rise in cloud adoption has ushered in a new era of data management, enabling users to offload the burden of large-scale data storage and processing onto Cloud Service Providers (CSPs). No longer bound by the limitations of local infrastructure, individuals and organizations alike are embracing the scalability, flexibility, and accessibility offered by cloud-based solutions. Among the myriad applications of cloud storage, one of the most notable is the emergence of Electronic Health Record (EHR) systems. These systems, championed by esteemed organizations such as the Office of the National Coordinator for Health Information Technology (ONC) in the United States and Canada Health Infoway, represent a paradigm shift in healthcare data management. By digitizing and centralizing patients' medical records, EHR systems facilitate seamless data sharing across healthcare providers, enhancing collaboration, improving patient care, and driving advancements in medical research and public health initiatives. However, with the convenience and efficiency afforded by cloud-

based EHR systems comes a host of security challenges. Entrusting sensitive medical data to external CSPs raises valid concerns regarding data privacy, integrity, and confidentiality. Users relinquish direct control over their EHRs to third-party entities, introducing inherent risks such as unauthorized access, data breaches, and potential regulatory non-compliance. Moreover, the reliance on CSPs for data storage and processing exposes EHR systems to external threats, including malicious attacks, hardware failures, and service disruptions, which could compromise the integrity and availability of critical healthcare information. To mitigate these risks and ensure the reliability of cloud-based EHR systems, innovative approaches to data verification and integrity assurance are paramount. One such approach, proposed by Benabbas et al., is the concept of Verifiable Databases (VDBs). By allowing clients to verify the correctness of server responses when accessing stored data, VDBs offer a mechanism for enhancing data integrity and trust in cloud-based environments. However, while VDBs address the issue of server response correctness, they fall short in providing comprehensive data integrity assurance, particularly for frequently accessed data and in resource-constrained settings. In parallel, various audit schemes have been developed to verify the integrity of data stored in the cloud. These schemes aim to detect and prevent unauthorized modifications to data, thereby safeguarding its accuracy and reliability. However, the implementation of audit schemes alongside VDBs poses logistical challenges, including increased computational overhead, storage requirements, and communication overhead, especially for devices with limited resources such as wearable health monitors and IoT devices. Against this backdrop, it becomes evident that a holistic approach to security and efficiency is essential for ensuring the integrity and reliability of cloud-based EHR systems. Such an approach must not only address the challenges posed by data verification and integrity assurance but also cater to the unique requirements of EHR systems, including privacy preservation, scalability, and interoperability across diverse stakeholders in the healthcare ecosystem. In light of these considerations, this paper proposes novel methodologies to address the security and efficiency concerns inherent in large-scale database storage, with a specific focus on cloud-based EHR systems. Leveraging the principles of Functional Commitment (FC) and group signatures, our approach aims to enhance data integrity, privacy preservation, and scalability while minimizing computational overhead and communication costs. By offering a comprehensive framework for secure and efficient EHR storage, our methodology seeks to advance the state-of-the-art in cloud-based healthcare data management and pave the way for transformative innovations in the field of digital health.

II. Related Work

The transition from paper-based to electronic health records (EHR) has revolutionized medical data management, offering benefits such as reduced medical errors, cost savings, and enhanced data sharing capabilities. However, ensuring the security of EHR systems remains a critical concern, prompting research efforts in areas such as searchable encryption, privacy preservation, access control, and data storage integrity. Numerous studies have addressed these challenges, including those focusing on the security of large database storage, such as EHRs. [1].

Benabbas et al. introduced the concept of Verifiable Databases (VDBs) as a secure and efficient dynamic cloud storage model for resource-limited users. Their scheme allows users to verify the correctness of server responses when accessing the database, independent of its size. However, existing VDB schemes typically only support private verifiability, limiting verification to the database owner. Sun et al. addressed this limitation by proposing a confidentiality-preserving publicly verifiable computation scheme, ensuring public verification while keeping the final result confidential.[2]

Vector Commitment (VC) schemes, proposed by Catalano and Fiore, offer an approach to construct VDBs. However, vulnerabilities were identified by Chen et al., who presented attacks on VC protocols and proposed a new VDB framework to mitigate these threats. Additionally, the

concept of Verifiable Databases with Incremental Updates (Inc-VDB) was formalized, and hierarchical commitment was introduced to enhance VDB schemes by Miao et al. [3].

To ensure the integrity of cloud storage data, various auditing schemes have been developed. Public integrity auditing schemes enable efficient data auditing by third-party auditors (TPAs), but may expose user data during the auditing process. To address privacy concerns, Li et al. proposed a certificateless public auditing scheme with integrated privacy protection for Wireless Body Sensor Networks. Dynamic auditing schemes, such as Divide and Conquer Table proposed by Sookhak et al., support frequent database updates. [4].

To reduce the computational burden on clients, lightweight cloud storage auditing schemes leveraging Third-Party Mediums (TPMs) have been introduced. Group-oriented auditing schemes, enabling cloud data sharing among group members in an anonymous manner, have also been proposed. Commitment schemes, such as Vector Commitment and Functional Commitment, play a fundamental role in many cryptographic protocols. Functional Commitment schemes, inspired by Vector Commitment and Polynomial Commitment, offer a flexible approach to commit to and open commitments, satisfying properties such as perfectly hiding and computational binding. [5].

Group signature schemes allow verification of signatures without revealing the signer's identity, offering anonymity while maintaining traceability through a trusted group manager. Verifier-Local Revocation (VLR) group signature schemes address member revocation but lack backward unlinkability. Achieving non-frameability in group signatures ensures that no entity, including the group manager, can sign on behalf of other members. Efficient verifier-local signature schemes with these properties have been developed to address practical challenges in group signature schemes.[6].

III. Existing Method

Benabbas et al. proposed 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 fre-quently 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.

Jiang et al.'s scheme proposed to use vector commitment scheme to construct the audit scheme. Although the reduction of tags has been achieved, their scheme fails to achieve the expected security due to the neglect of the real-time performance of proof generation. There is still no good way to minimize the communication for low performance users.

Disadvantages:

The primary problem faced by the EHR system is on how to verify that the server responses correctly each time.

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.

In the existing system, due to the fact that their model did not consider a notion of "real-time" proof, the use of these techniques makes their audit scheme and other VDB schemes incapable of checking storage integrity. In this case, only the queried data is involved in the verification process. This leads to verification only on the data being queried, while storage integrity of other cloud data is not checked. If the cloud data which is not queried is damaged, it will not be detected in time. When the damaged data is needed, there will be varying degrees of loss.

IV. Proposed Method

Our research focuses on the security and efficiency of large database storage, such as EHR. According to the characteristics of EHR system, two aspects of security deserve our attention, namely, the server response correctness and the data storage integrity. In order to deal with above problems, we use a new tool called functional commitment (FC) and design a publicly verifiable updatable database scheme based on functional commitment supporting privacy-preserving integrity auditing and dynamic group operation.

We modify the existing functional commitment scheme in order to use the function binding of functional commitment to design an auditable VDB scheme. We point out security problems with existing scheme and propose a publicly verifiable updatable VDB scheme based on the functional commitment and group signature without incurring too much computational overhead and storage cost. Moreover, our scheme is applicable for large-scale data storage with minimum user communication cost.

Our proposed scheme not only preserves all the properties of the original VDB scheme, but also implements efficient privacy-preserving integrity auditing, non-frameability and traceability.

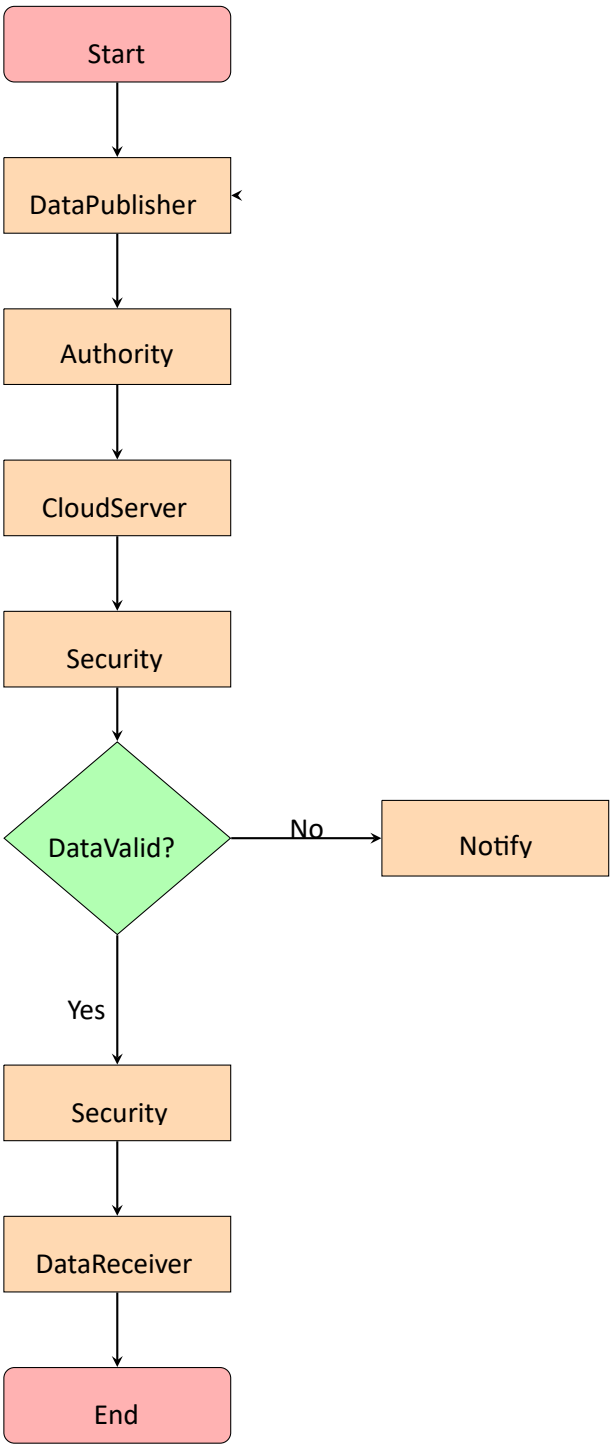
Adavantages:

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



Secure Health: Dynamic Integrity-Assured Shared EHR Databases with Privacy-Preserving Functional Commitment.

Fig 1: Flow Chart

V. Simulation Results

In this system, various stakeholders, including patients, clinics, hospitals, medicine centers, and insurance entities, can upload large databases to the cloud server. Unlike typical auditing methods, clients generate authentication tags locally and send them to the cloud for data integrity verification. A dynamic group membership model allows users to share databases, with a group manager overseeing membership.

The Group Manager functions as the system administrator, managing member details and revoking or activating users as needed. A Third Party Auditor (TPA) checks the integrity of cloud-stored data on behalf of users, using public key methods for efficient auditing. The cloud server provides storage and computing resources for users, facilitating seamless data sharing..

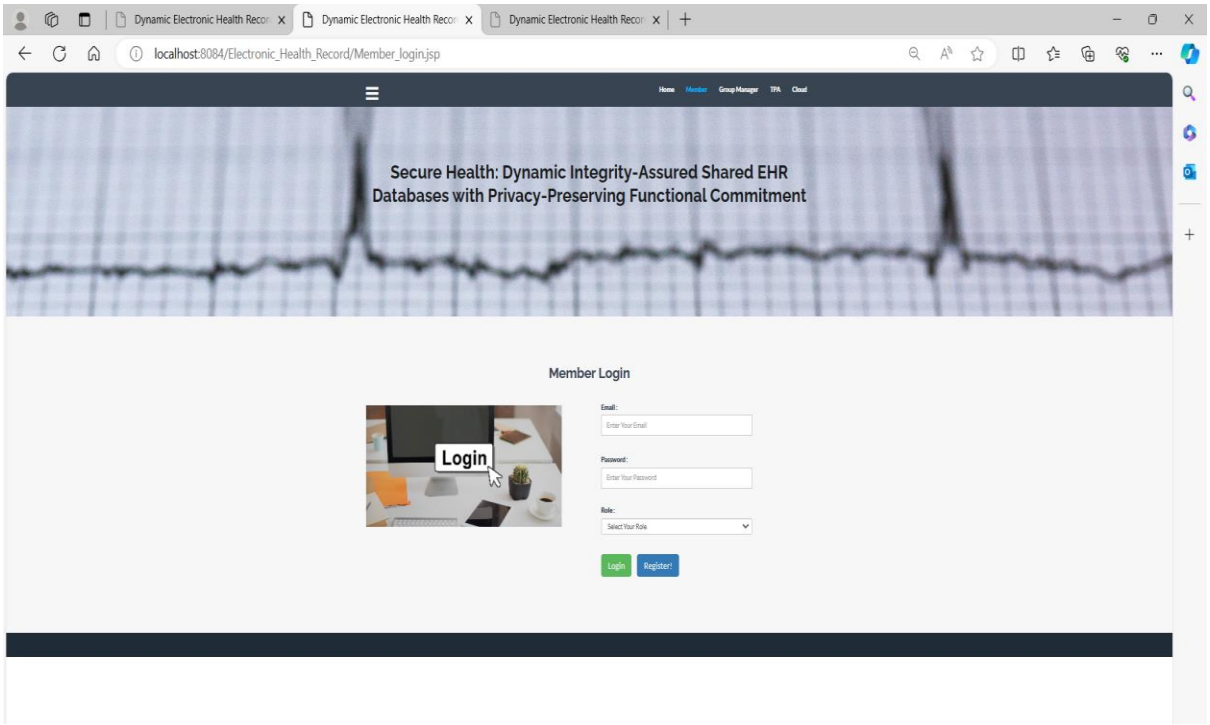


Fig 2.1: Member Login

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN2454-9940

www.ijasem.org

Vol 18, Issue.2 April 2024

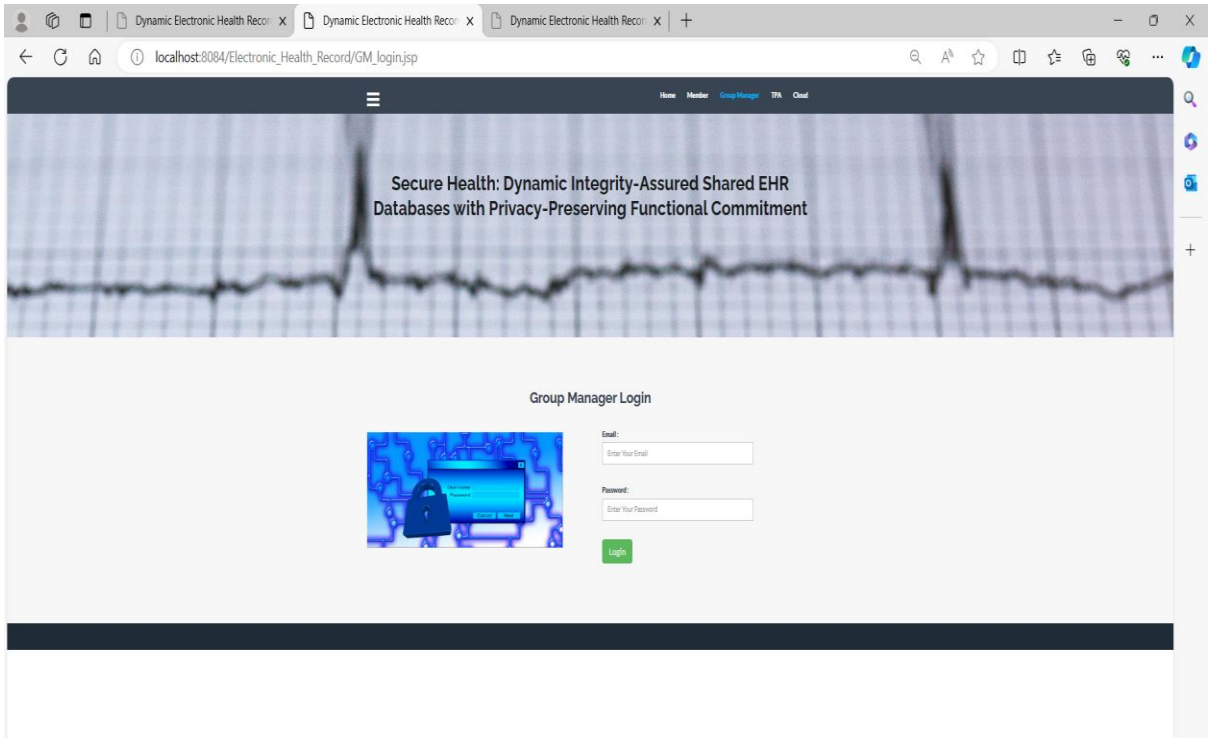


Fig :2.2 :Group Manager login

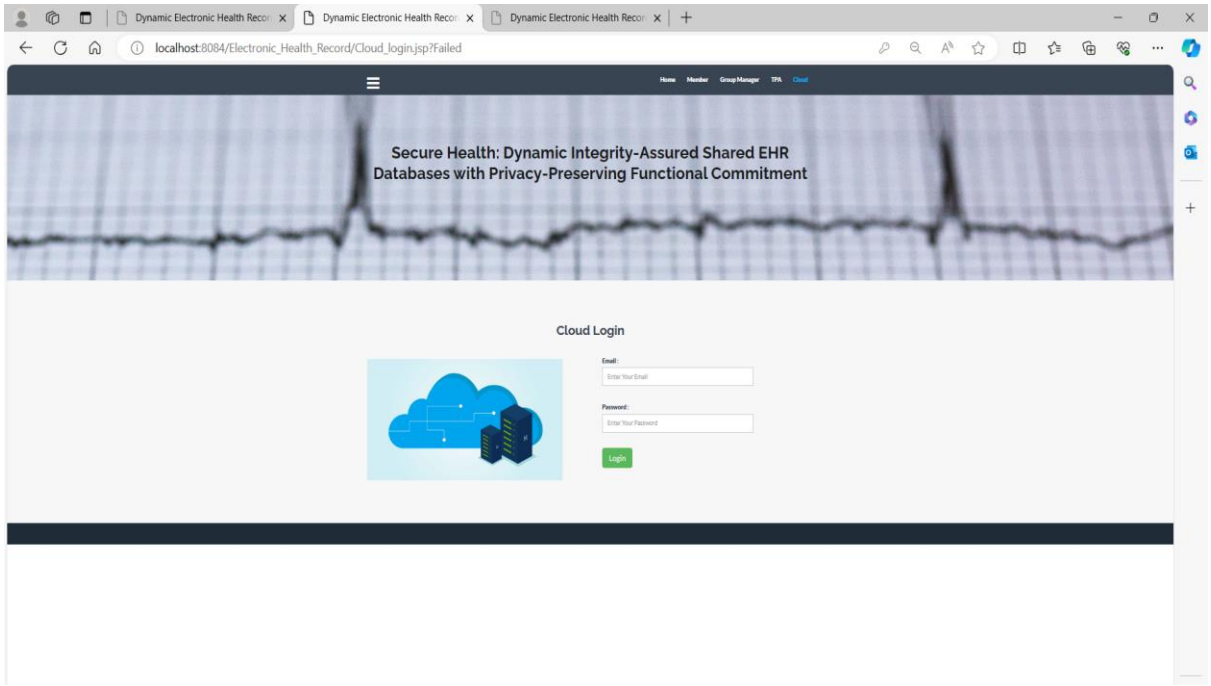


Fig:2.3:cloud login

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN2454-9940

www.ijasem.org

Vol 18, Issue.2 April 2024

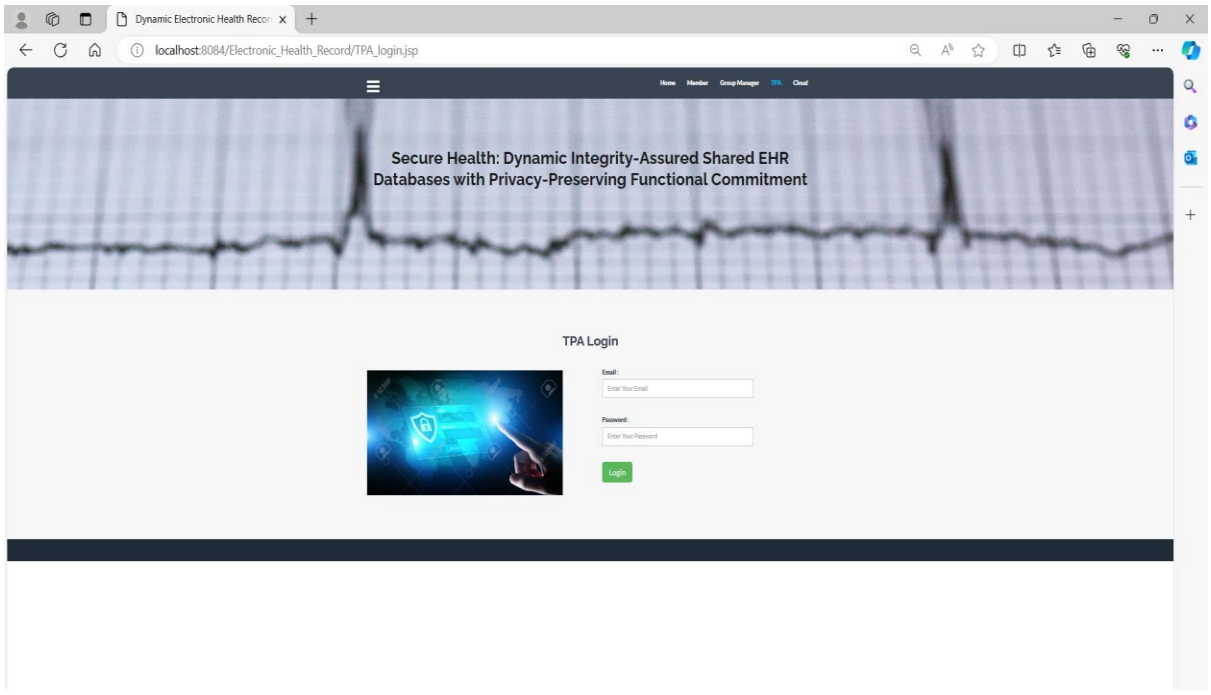


Fig:2.4: TPA login

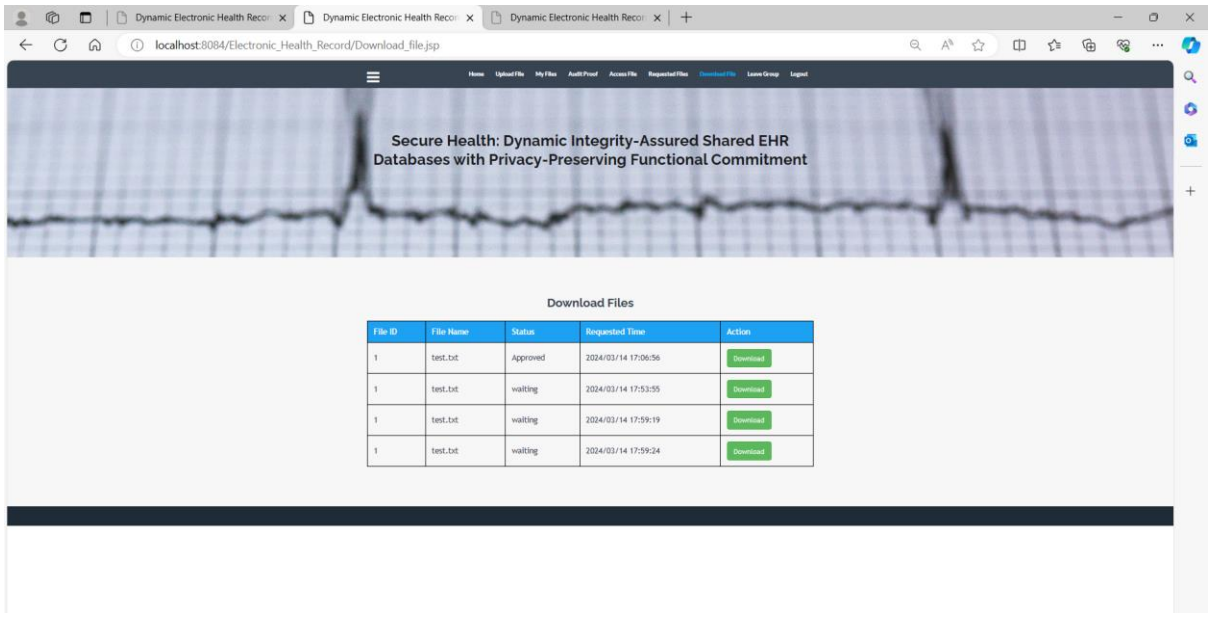


Fig :2.6 : download files

VI. Conclusion and Future Work

The concept of verifiable database is a great tool for verifiable EHR storage. However, proof reuse and the technique of proof updating by the server to improve system efficiency fails to achieve data integrity checking. In this work, we propose a novel updatable VDB scheme based on the functional commitment that supports privacy-preserving integrity auditing and group member operations, including join and revocation. Two security requirements of HER are implemented: the server response correctness and the data storage integrity. Our VDB scheme achieves the desired security goals without incurring too much computational increase. And our VDB scheme provides the minimum communication cost for the terminal with limited performance. To design a functional commitment scheme that applies to our program, two algorithms are added to make the FC scheme updatable. A practical improved concrete VDB scheme under computational l −BDHE assumption is presented. In addition, batch auditing for our VDB scheme supports multi-cloud server, multi-user and multi-storage vector scenarios. It makes the auditing process more efficient. Furthermore, we prove that our functional commitment scheme with updates and our VDB scheme can achieve the desired security properties. The performance of our scheme is more efficient compared with other different algorithms.

VII. 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