Publicly Verifiable Shared Dynamic Electronic

Health Record Databases with Functional

Commitment Supporting Privacy-Preserving

Integrity Auditing

**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

**Existing System:**

We modify the existing functional commitment scheme in order to use the function binding of functional commitment to design an auditable VDB scheme. Two algorithms for updating are added based on the original scheme in . And a modified concrete FC with updates under the computational assumption is constructed. Our construction has fewer parameters and is more efficient than the original scheme in . We point out security problems with 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.

**Disadvantages**

1. 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.

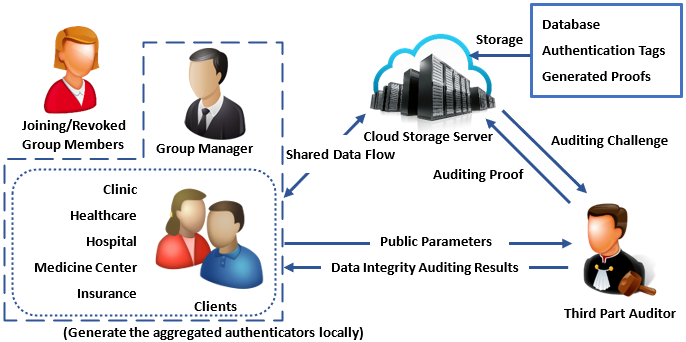
**Proposed System:**

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 un-trusted 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.

**Advantages**

1. Improving the efficiency.
2. Proof reuse and proof updating technique to prove correctness of the query results.

**System Architecture:**



IMPLEMENTAION

**MODULES**

1. Client
2. TPA
3. Manager
4. Cloud

**MODULE DESCRIPTION**

**Client**

In this module client(clinic, health care, hospital, medicine center, insurance ) should register with our Application after their successful register they must joined by the manage.

If they joined by the manager into the application he can perform some operations such as upload patient data and view patient data and also can search for other patient data, view patient data and share to other group member.

**TPA**

here TPA should login with the application after successful login he can perform some operations such as view patients records and audit records if any records has already modified by any user or not and also send the audit request to cloud

**Manage**

Here manager can login with the application after successful login he can perform some operations such as view client and join client or revoke clients

**Cloud**

Here cloud can login with the application after successful login he can perform some operations such as view clients details and patient details and check audit proof

USE CASE DIAGRAM:  
A use case diagram within the Unified Modeling Language (UML) could be a kind of behavioural diagram outlined by and created from a Use-case analysis. Its purpose is to gift a graphical summary of the practicality provided by a system in terms of actors, their goals (represented as use cases), and any dependencies between those use cases. the most purpose of a use case diagram is to indicate what system functions area unit performed that actor. Roles of the actors within the system is pictured.









CLASS DIAGRAM:   
  
In programming building, a category chart within the Unified Modeling Language (UML) could be a kind ofstatic structure define that portrays the structure of a framework by demonstrating the framework's categories, their properties, activities (or strategies), and therefore the connections among the categories. It clarifies that category contains knowledge.

  
SUCCESSION DIAGRAM:   
  
A succession graph in Unified Modeling Language (UML) could be a kind of collaboration chart that shows however forms work with one another and in what prepare. it's a develop of a Message Sequence Chart. Grouping graphs area unit once in a very whereas referred to as occasion outlines, occasion things, and temporal arrangement charts.

  
  
ACTION DIAGRAM:   
  
Action charts area unit graphical portrayals of labor processes of stepwise exercises and activities with facilitate for call, cycle and timing. within the Unified Modeling Language, movement graphs is utilised to depict the business and operational well ordered work processes of components in a very framework. associate action define demonstrates the overall stream of management.

Activity

start

Login

login

Client

TPA

cloud

Loginagain

Login again login again no

login

No no

yes yes yes

auditFiles

Search

sendAuditProof

ViewPatientDetesils

ViewData

UploadEHR

viewPatients

viewClients

auditProof

sharedData

end

Collaboration

****

**SYSTEM REQUIREMENTS:**

**HARDWARE REQUIREMENTS:**

* PROCESSOR : I3.
* Hard Disk : 40 GB.
* Ram : 2 GB.

**SOFTWARE REQUIREMENTS:**

* Operating system : Windows.
* Coding Language : JAVA/J2EE
* Data Base : MYSQL
* IDE :Netbeans8.1