**🔐 Abstract**

Cloud infrastructure reduces computing costs but poses challenges in searching and sharing encrypted data. To address this, we propose **CPAB-KSDS** (Ciphertext-Policy Attribute-Based Keyword Search and Data Sharing), a secure scheme that:

* Supports **both attribute-based keyword search and data sharing**, unlike prior solutions that support only one.
* Enables **keyword updates during sharing** without needing PKG interaction.
* Ensures **data confidentiality** while allowing efficient search.
* Is proven secure against **chosen ciphertext and keyword attacks**.
* Demonstrates **practical performance** through evaluation.

**🔐 Introduction**

* Cloud computing offers scalability but raises serious data privacy and security concerns.
* Existing systems lack secure keyword search and controlled data sharing.
* This project proposes a Java-based encryption framework enabling searchable, shareable encrypted data.
* Focuses on data confidentiality, fine-grained access control, and resilience to key exposure.
* Enhances trust and compliance in cloud environments.

**📌 Existing System**

* Uses **attribute-based encryption (ABE)**, which is inflexible for dynamic search and sharing.
* Requires **data owner to stay online** for decryption—inefficient with large datasets.
* Some systems **delegate tasks to third parties**, risking exposure of private keys.
* Often stores data in **plain text** or with **weak encryption** methods.
* Lacks robust mechanisms for **secure keyword search and sharing**.

**⚠️ Disadvantages**

* **Data privacy** is poorly protected—vulnerable to unauthorized access during search/sharing.
* Weak **integrity checks** fail to prevent tampering or unauthorized modifications.
* **Scalability** issues arise with high data volume or user load.
* High **system complexity** increases risk of misconfiguration and exploitation.
* Ineffective **key management** (distribution, rotation, revocation) weakens security.

**🚀 Proposed System**

* Introduces **CPAB-KSDS**: Ciphertext-Policy Attribute-Based Encryption with Keyword Search and Data Sharing.
* Enables **secure search and sharing** without decryption or reliance on a **Private Key Generator (PKG)**.
* Supports **keyword updates** during the data sharing phase.
* Allows data owners to **fully control access** to encrypted data.
* Designed to be **CCA-secure** and resistant to **collusion attacks**.
* Ensures security even if encryption key is exposed—**plaintext is unrecoverable unless all ciphertext blocks are accessed**.

**✅ Advantages**

* **Strong security**: CCA & CKA secure.
* **Efficient** and matches top systems.
* **Multiple keys** enhance decryption protection.
* **No trusted third party** required.
* Secures **data at rest and in transit**.

**⚙️ System Requirements**

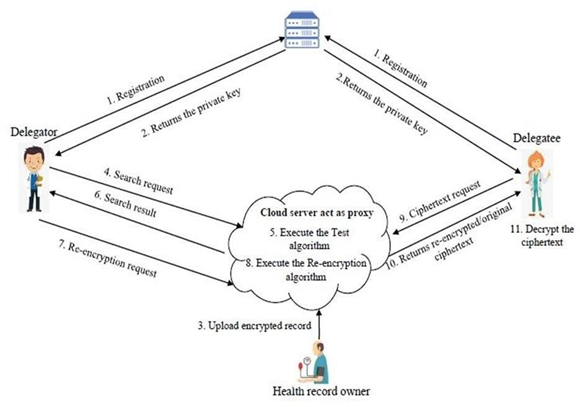
**Functional Requirements:**

* **Health Record Owner**: Controls access to personal data.
* **Delegator**: Grants permissions to delegatees.
* **Delegatee**: Accesses shared health records securely.
* **PKG**: Manages cryptographic keys (if included).
* **Cloud Server**: Stores and encrypts data using AES & RSA.

**Non-Functional Requirements:**

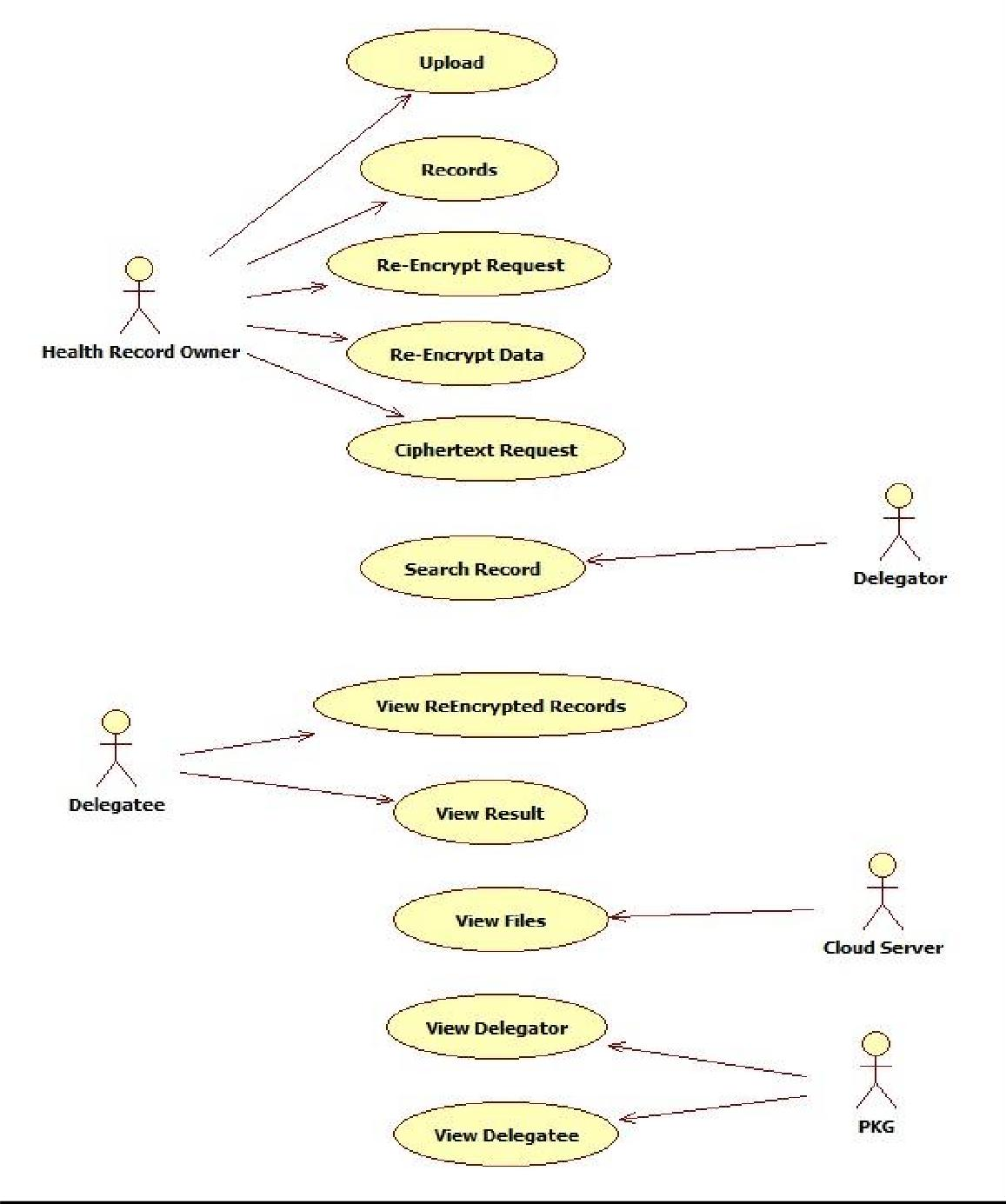
* **OS**: Windows 7+
* **Tech**: Java 7 / J2EE, HTML, CSS, JS
* **IDE**: Eclipse
* **Server**: Apache Tomcat
* **DB**: MySQL
* **Java SDK**: JDK 1.5+
* **Hardware**: Dual Core, 1 GB RAM, 20 GB Disk

**SYSTEM ARCHITECTURE**

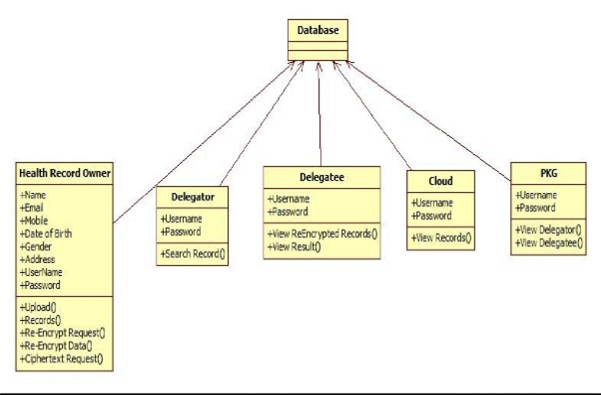


**UML DIAGRAMS**

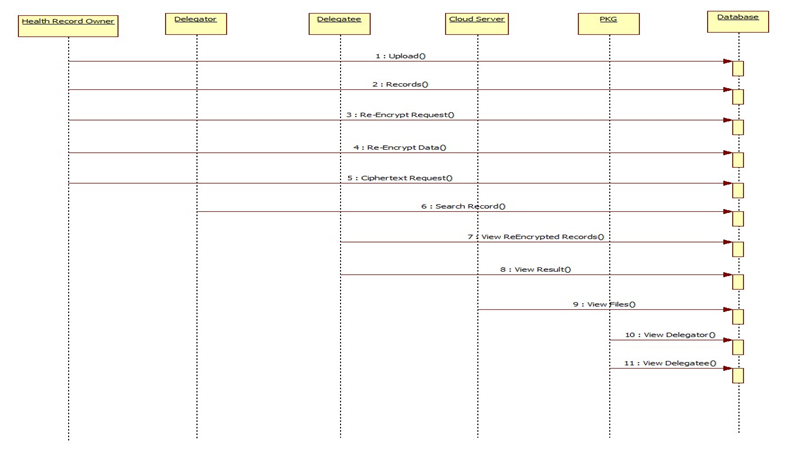
**USE CASE DIAGRAM**



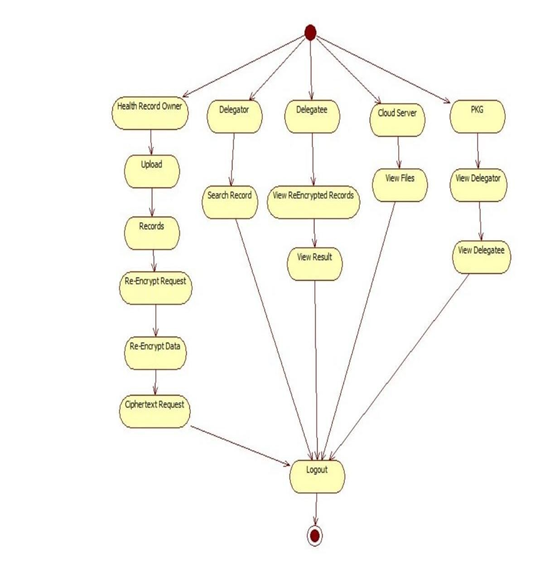
**CLASS DIAGRAM**



**SEQUENCE DIAGRAM**



**ACTIVITY DIAGRAM**

**Implementation – Modules Overview**

**1. Health Record Owner**  
Subject of the health record; retains ownership and control over personal health data.

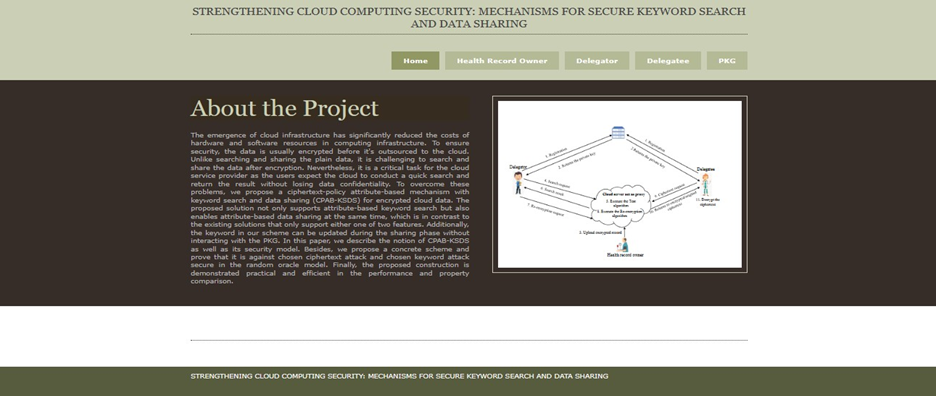
**2. Delegatee**  
Authorized person/entity assigned tasks (e.g., data access or management); must maintain confidentiality and follow legal/ethical standards.

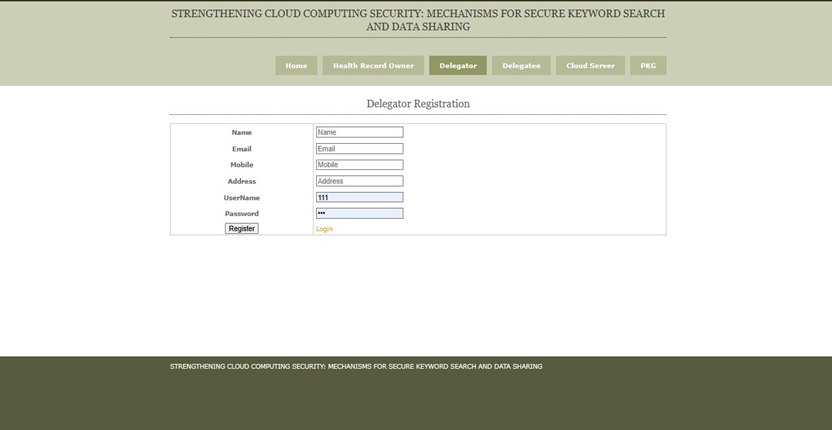
**3. Delegator**  
Healthcare provider who assigns responsibilities to delegatees; remains accountable for actions and patient data integrity.

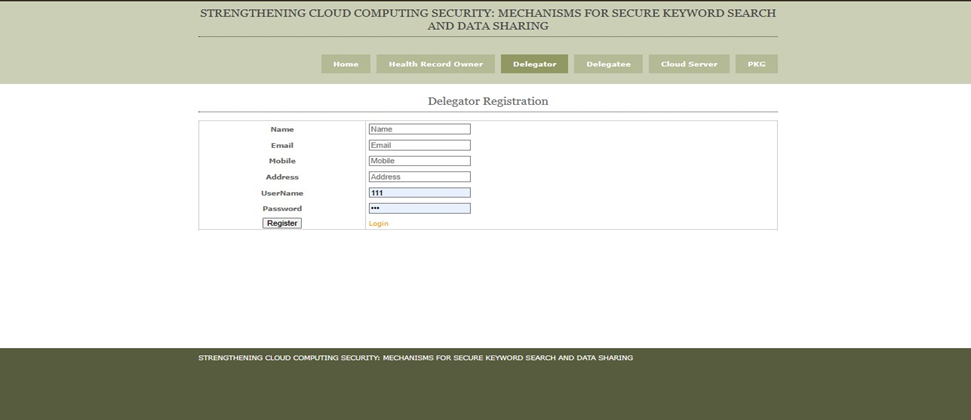
**4. PKG (Private Key Generator)**  
Generates and manages cryptographic keys and attributes required for secure encryption, decryption, and access control.

**5. Cloud Server**  
Securely stores encrypted health data; enables data sharing and attribute-based keyword search using AES and RSA encryption.

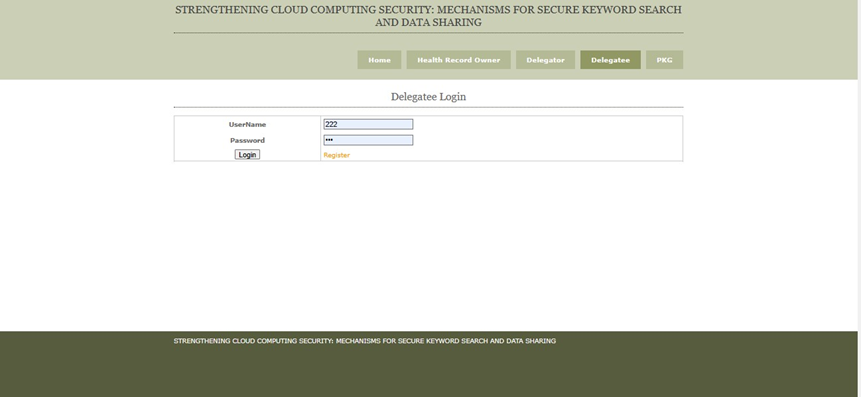
**SCREENSHOTS OF EXECUTION**

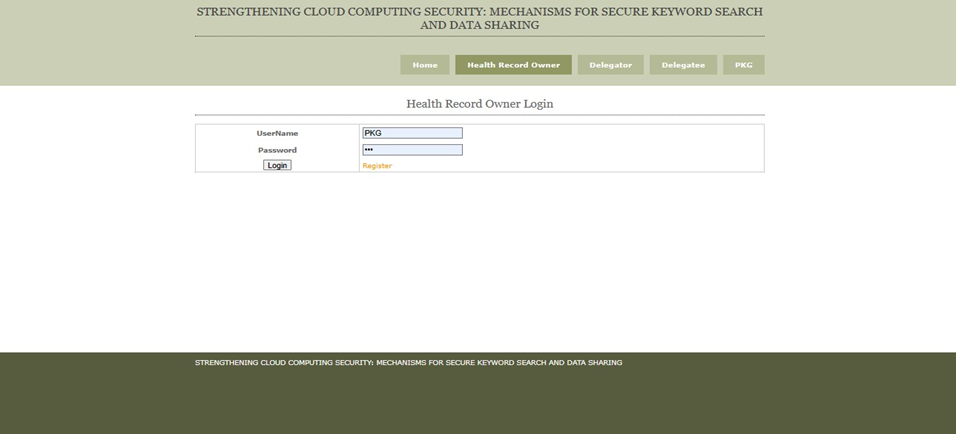












**Conclusion**

* **Proposed CPAB-KSDS, a new scheme for encrypted cloud data.**
* **Supports both attribute-based keyword search and data sharing.**
* **Eliminates the need for PKG during the sharing phase.**
* **Proved CCA-security in the random oracle model.**
* **Demonstrated to be efficient and practical in performance.**
* **Addresses an open challenge from prior work.**
* **Opens new directions for:**
  + **Designing schemes without random oracles.**
  + **Supporting more expressive keyword searches.**

**Future Scope**

* **Java remains relevant for cloud, microservices, and IoT due to its portability, security, and scalability.**
* **Ongoing updates (e.g., Java modularization) enhance modern development.**
* **Strong presence in enterprise systems and backend solutions.**
* **Research opportunities in:**
  + **Secure keyword search without random oracles**
  + **Advanced data sharing in encrypted cloud environments**