International Journal of
AI ELECTRICAL CIVIL AND MECHANICAL ENGINEERING
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0434 www.zesterapublications.com Original Research Paper

UNIFIED FINE-GRAINED ACCESS CONTROL FOR PERSONAL HEALTH RECORDS IN CLOUD COMPUTING

[1] THALLAPALLI ROHITH VARMA, [2] Mrs. G. PRIYANKA
[1] M. Tech Student, [2] Assistant Professor
Department Of Computer Science and Engineering
KLR College Of Engineering and Technology, B.C.M Road, Paloncha, Bhadradri Kothagudem Dist.,Telangana,507115

ABSTRACT

Attribute-based encryption has been a promising encryption technology to secure personal health records (PHRs) sharing in cloud computing. PHRs consist of the patient data often collected from various sources including hospitals and general practice centres. Different patients' access policies have a common access sub-policy. In this paper, we propose a novel attribute-based encryption scheme for fine-grained and flexible access control to PHRs data in cloud computing. The scheme generates shared information by the common access sub-policy, which is based on different patients' access policies. Then, the scheme combines the encryption of PHRs from different patients. Therefore, both time consumption of encryption and decryption can be reduced. Medical staff require varying levels of access to PHRs. The proposed scheme can also support multi-privilege access control so that medical staff can access the required level of information while maximizing patient privacy. Through implementation and simulation, we demonstrate that the proposed scheme is efficient in terms of time. Moreover, we prove the security of the proposed scheme based on security of the ciphertext-policy attribute-based encryption scheme.

Keywords: Attribute-Based Encryption (ABE), Ciphertext-Policy Attribute-Based Encryption (CP-ABE), Personal Health Records (PHRs), Cloud Computing, Fine-Grained Access Control, Multi-Privilege Access Control, Healthcare Data Security, Privacy Preservation

I. INTRODUCTION

The rapid advancement of cloud computing has transformed the healthcare industry by enabling secure storage, efficient management, and convenient sharing of medical information. Personal Health Records (PHRs) are digital repositories that contain an individual's complete medical history, including diagnoses, prescriptions, laboratory reports, medical imaging, allergies, immunization records, and treatment details. Unlike Electronic Health Records (EHRs), which are primarily managed by healthcare institutions, PHRs are controlled by patients, allowing them to decide who can access their sensitive medical information.

Cloud computing provides an ideal platform for storing PHRs because it offers scalability, cost-effectiveness, remote accessibility, and high availability. Patients, doctors, hospitals, insurance providers, laboratories, and researchers can access health records from anywhere at any time, improving healthcare quality and enabling better collaboration among healthcare providers. However, outsourcing sensitive medical data to cloud servers introduces significant privacy and security concerns. Since cloud servers are often managed by third-party service providers, there is always a risk of unauthorized access, data leakage, identity theft, and misuse of confidential patient information.

Traditional access control mechanisms, such as Role-Based Access Control (RBAC), are inadequate for modern cloud-based healthcare systems because they cannot efficiently handle dynamic users and complex access requirements. For example, a cardiologist may require access to heart-related reports, while a

Received: 22-05-2026 | Accepted: 30-06-2026 | Published: 06-07-2026

International Journal of
AI ELECTRICAL CIVIL AND MECHANICAL ENGINEERING
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0434 www.zesterapublications.com Original Research Paper

laboratory technician may only need permission to upload diagnostic results. Patients may also wish to grant temporary access to family members or emergency medical personnel. These requirements demand a more flexible and fine-grained access control mechanism.

Attribute-Based Encryption (ABE) has emerged as a promising cryptographic technique for secure data sharing in cloud environments. In ABE, access permissions are determined based on user attributes such as profession, department, organization, specialization, or designation rather than individual identities. Only users whose attributes satisfy the predefined access policy can decrypt the encrypted data. This approach provides fine-grained, scalable, and patient-centric access control while maintaining data confidentiality.

Despite the advantages of ABE, conventional schemes often suffer from computational overhead, complex key management, and redundant encryption operations when multiple patients define similar access policies. Many healthcare organizations share common access requirements, such as allowing licensed doctors, emergency physicians, or authorized laboratory staff to access particular categories of medical records. Repeatedly generating separate encryption policies for these common requirements increases storage costs and encryption time.

The **Unified Fine-Grained Access Control for Personal Health Records in Cloud Computing** addresses these challenges by introducing a unified access control framework that efficiently manages common access policies while preserving patient-specific privacy requirements. The proposed system identifies shared access sub-policies among multiple users and generates common encrypted components that can be reused across different PHRs. This significantly reduces encryption complexity, minimizes storage overhead, and improves the efficiency of secure data sharing in cloud environments.

The proposed framework integrates cloud computing with advanced cryptographic techniques to provide confidentiality, authentication, authorization, integrity, and secure key management. Patients retain complete ownership and control over their health records while healthcare professionals receive access only to the information necessary for their responsibilities. Emergency access mechanisms can also be incorporated to provide authorized medical personnel with temporary access during critical situations without compromising overall system security.

Furthermore, the unified fine-grained access control model supports dynamic user management by allowing efficient addition, removal, and updating of user attributes without requiring complete re-encryption of stored data. This feature makes the system highly scalable for large healthcare organizations where users frequently join or leave the network.

The proposed system enhances privacy protection while ensuring compliance with healthcare security standards and regulations. It provides a practical solution for secure cloud-based healthcare services by balancing strong security, efficient access control, reduced computational costs, and improved usability. The framework contributes to building a trustworthy healthcare ecosystem where patients can confidently store and share their medical records while maintaining complete control over their sensitive information.

Unified Fine-Grained Access Control for Personal Health Records in Cloud Computing is targeting to configure an effective and versatile access regulation model for the protection of sensitive health data in cloud computing and its applications. By means of context-aware fine-grained permissions, the control framework confirms that only properly cleared individuals can use the designated set of PHRs at any given time. The control framework combines state-of-the-art encryption

Received: 22-05-2026 | Accepted: 30-06-2026 | Published: 06-07-2026

International Journal of
AI ELECTRICAL CIVIL AND MECHANICAL ENGINEERING
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0434 www.zesterapublications.com Original Research Paper

technologies to safeguard data while in motion and while in storage as well as user authentication mechanisms such as multi-factor authentication (MFA) to give a more controlled and real-time identity verification. The system was developed in a way to be capable of interoperability with the current Healthcare Information Systems, Electronic Health Records and Cloud based health-care application without much hassle and integration issues using designed protocols and APIs.

EXISTING SYSTEM

The existing cloud-based Personal Health Record (PHR) systems primarily rely on conventional access control mechanisms to protect sensitive medical data. These systems allow patients to store their health records on cloud servers and share them with healthcare professionals such as doctors, nurses, hospitals, laboratories, and insurance providers. Although cloud computing offers scalability and easy accessibility, the existing systems face several security, privacy, and access control challenges.

Traditional access control models such as **Role-Based Access Control (RBAC)** and **Identity-Based Access Control (IBAC)** are commonly used in healthcare applications. In RBAC, users are granted permissions based on predefined roles such as doctor, nurse, or administrator. Similarly, IBAC grants access based on the identity of individual users. While these methods are suitable for small and static organizations, they become inefficient in large-scale cloud environments where users frequently change roles and access requirements.

To overcome these limitations, several research works introduced **Attribute-Based Encryption (ABE)** for secure PHR sharing. ABE enables fine-grained access control by allowing data owners to define access policies based on user attributes such as profession, department, specialization, or organization. Only users whose attributes satisfy the access policy can decrypt the encrypted health records. Although ABE significantly improves security and flexibility compared to traditional methods, existing ABE-based systems still suffer from several practical limitations.One major drawback is the **high computational overhead** during encryption and decryption. Each patient's health record is encrypted independently with a separate access policy, even when multiple patients share similar access requirements. This results in repeated encryption operations, increased processing time, and higher computational costs.Another limitation is **complex key management**. Existing systems require generating, distributing, updating, and revoking cryptographic keys for a large number of users. As the number of patients and healthcare providers increases, managing these keys becomes difficult and inefficient, affecting system scalability.

Most existing systems also fail to efficiently manage **common access policies** shared among multiple users. For example, several patients may wish to grant access to licensed doctors, emergency physicians, or laboratory technicians using identical access conditions. Current systems repeatedly generate separate encryption components for these common policies, leading to redundant storage, unnecessary computation, and inefficient resource utilization.

Additionally, many traditional PHR systems provide **limited support for dynamic user management**. Whenever a user's attributes change or access rights are updated, the data often needs to be re-encrypted or access policies must be recreated. This increases maintenance costs and causes delays in granting or revoking permissions.

Privacy is another significant concern in existing cloud-based PHR systems. Since health records are stored on third-party cloud servers, there is a risk of unauthorized access, insider attacks, data leakage, and misuse of confidential patient information. Many systems

Received: 22-05-2026 | Accepted: 30-06-2026 | Published: 06-07-2026

International Journal of
AI ELECTRICAL CIVIL AND MECHANICAL ENGINEERING
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0434 www.zesterapublications.com Original Research Paper

rely heavily on the trustworthiness of cloud service providers, which may expose sensitive medical data if adequate cryptographic protection is not implemented.

Furthermore, emergency access scenarios are not efficiently handled in many existing solutions. During medical emergencies, authorized healthcare professionals require immediate access to patient records. However, traditional access control mechanisms may either deny timely access or compromise security by granting excessive permissions.

Overall, the existing systems provide basic security and controlled access to cloud-based Personal Health Records but suffer from computational inefficiency, redundant encryption, complex key management, limited scalability, and inadequate support for dynamic access control. These limitations highlight the need for a more efficient and unified fine-grained access control framework that can securely manage PHR sharing while reducing encryption overhead and improving overall system performance.

Limitations of the Existing System

- Relies on traditional RBAC or identity-based access control, which lacks flexibility.
- High computational cost during encryption and decryption.
- Repeated encryption for identical access policies causes redundancy.
- Complex cryptographic key generation, distribution, and revocation.
- Increased storage overhead due to duplicate encrypted policy components.
- Limited scalability for large healthcare organizations.
- Inefficient handling of dynamic user addition, removal, and attribute updates.
- Higher communication and maintenance overhead.
- Risk of unauthorized access and data leakage in cloud environments.
- Poor support for emergency access and real-time healthcare data sharing.
- Reduced efficiency when managing large numbers of patients and healthcare providers.
- Increased processing time, affecting the overall performance of the cloud-based PHR system

PROPOSED SYSTEM :

The proposed system introduces a **Unified Fine-Grained Access Control Framework** for secure sharing of **Personal Health Records (PHRs)** in cloud computing. The framework is designed to provide strong data confidentiality, flexible access control, reduced computational overhead, and efficient management of encryption policies. It combines **Attribute-Based Encryption (ABE)** with a unified access policy mechanism to enable secure and scalable data sharing among patients, healthcare providers, hospitals, laboratories, insurance companies, and other authorized users.

In the proposed system, patients maintain complete ownership and control over their health records. Before uploading medical data to the cloud, the records are encrypted using Attribute-Based Encryption. Instead of assigning permissions to individual users, access rights are defined through a set of attributes such as **Doctor**, **Cardiologist**, **Hospital Staff**, **Laboratory Technician**, **Insurance Officer**, or **Emergency Physician**. Only users whose attributes satisfy the specified access policy can decrypt and access the encrypted records.

A key innovation of the proposed system is the **unified access policy management**. Many patients often define similar access requirements for healthcare professionals. Instead of repeatedly encrypting identical policy components for every patient, the system identifies common access sub-policies and generates shared encryption components. These reusable encrypted components

Received: 22-05-2026 | Accepted: 30-06-2026 | Published: 06-07-2026

International Journal of
AI ELECTRICAL CIVIL AND MECHANICAL ENGINEERING
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0434 www.zesterapublications.com Original Research Paper

significantly reduce encryption time, computational complexity, storage overhead, and communication costs while maintaining the security of patient data.

The framework employs multiple trusted authorities to manage user attributes and cryptographic keys securely. Authorized users receive secret keys corresponding to their verified attributes. When a user requests access to a patient's health record, the system verifies whether the user's attributes satisfy the encrypted access policy. If the policy conditions are fulfilled, the record is decrypted successfully; otherwise, access is denied.

To support real-world healthcare environments, the proposed system also provides **dynamic user management**. Healthcare professionals can be added, removed, or updated without requiring complete re-encryption of all stored records. Efficient key update and revocation mechanisms ensure that revoked users cannot access future records while minimizing system overhead.

The proposed framework also strengthens privacy protection by ensuring that the cloud server stores only encrypted data and never gains access to plaintext medical information. Even if the cloud server is compromised, attackers cannot decrypt patient records without possessing the required attribute-based secret keys.

Additionally, the system supports secure emergency access by allowing authorized emergency personnel to obtain temporary access to critical medical information under predefined emergency policies. This ensures timely treatment while preserving patient privacy and preventing unauthorized disclosure.

Overall, the proposed system offers a secure, scalable, and efficient solution for cloud-based healthcare data sharing. By integrating unified policy generation with fine-grained attribute-based encryption, the framework minimizes redundancy, improves system performance, and provides flexible patient-centric access control suitable for modern healthcare applications.

WORKING OF THE PROPOSED SYSTEM

The proposed system operates through the following steps:

1. **Patient Registration:** Patients register with the healthcare system and securely upload their Personal Health Records.
2. **Attribute Assignment:** Trusted authorities verify users and assign cryptographic keys based on their attributes.
3. **Policy Definition:** Patients define fine-grained access policies specifying which attributes are required to access their records.
4. **Data Encryption:** Health records are encrypted using Attribute-Based Encryption before being uploaded to the cloud.
5. **Unified Policy Generation:** Common access sub-policies are identified and shared encryption components are generated to reduce redundancy.
6. **Cloud Storage:** Only encrypted PHRs are stored on the cloud server.
7. **Access Request:** Authorized healthcare users request access to encrypted medical records.
8. **Attribute Verification:** The system checks whether the user's attributes satisfy the defined access policy.
9. **Data Decryption:** If authorized, the user decrypts and accesses the required medical information.
10. **Dynamic Updates:** User attributes, permissions, and cryptographic keys can be updated efficiently without complete re-encryption.

Advantages of the Proposed System

- Provides **fine-grained access control** based on user attributes.
- Ensures **complete privacy and confidentiality** of Personal Health Records.

Received: 22-05-2026 | Accepted: 30-06-2026 | Published: 06-07-2026

International Journal of
AI ELECTRICAL CIVIL AND MECHANICAL ENGINEERING
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0434 www.zesterapublications.com Original Research Paper

- Reduces **encryption and decryption overhead** through unified access policy management.
- Eliminates redundant encryption of common access policies.
- Supports **efficient key generation, distribution, and revocation**.
- Allows **patients to maintain full ownership and control** over their health records.
- Provides **secure cloud storage** by storing only encrypted medical data.
- Improves **system scalability** for large healthcare organizations.
- Supports **dynamic user addition, removal, and attribute updates**.
- Minimizes storage and communication overhead.
- Enables **secure emergency access** through predefined emergency policies.
- Protects against unauthorized access, insider attacks, and cloud security threats.
- Enhances overall system performance and resource utilization.
- Provides a **patient-centric, flexible, and secure** healthcare data-sharing environment.
- Suitable for modern cloud-based healthcare systems requiring high security and efficient access management

II. LITERATURE SURVEY

1. Title: ***"Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data"***

Authors: Vipul Goyal, Omkant Pandey, Amit Sahai, Brent Waters

Description:

This paper introduced the concept of Key-Policy Attribute-Based Encryption (KP-ABE), which enables fine-grained access control over encrypted data. Instead of assigning permissions directly to users, decryption rights are determined by a user's attributes. The work laid the foundation for secure cloud data sharing and significantly influenced the development of privacy-preserving healthcare systems. However, the scheme has limitations in handling dynamic access policies and large-scale cloud environments efficiently.

2. Title: ***"Ciphertext-Policy Attribute-Based Encryption"***

Authors: John Bethencourt, Amit Sahai, Brent Waters

Description:

This paper proposed Ciphertext-Policy Attribute-Based Encryption (CP-ABE), allowing data owners to define access policies directly within encrypted data. Users can decrypt information only if their attributes satisfy the embedded access policy. CP-ABE became one of the most widely adopted cryptographic techniques for secure cloud storage and healthcare applications. Although it provides strong security and flexible access control, it introduces considerable computational overhead during encryption and key management.

3. Title: ***"Patient Self-Controllable and Multi-Level Privacy-Preserving Cooperative Authentication in Cloud-Based Healthcare Systems"***

Authors: Ximeng Liu, Robert H. Deng, Kim-Kwang Raymond Choo

Description:

This research presents a privacy-preserving authentication framework for cloud healthcare environments. The proposed system enables patients to control access to their medical information while supporting secure authentication among healthcare providers. The framework enhances confidentiality, identity protection, and access control. However, the system primarily focuses on authentication and does not completely address redundant encryption or unified policy management.

4. Title: ***"Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption"***

Received: 22-05-2026 | Accepted: 30-06-2026 | Published: 06-07-2026

International Journal of
AI ELECTRICAL CIVIL AND MECHANICAL ENGINEERING
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0434 www.zesterapublications.com Original Research Paper

Authors: Ming Li, Shucheng Yu, Yao Zheng, Kui Ren, Wenjing Lou

Description:

This paper proposed a scalable framework for secure Personal Health Record (PHR) sharing using Attribute-Based Encryption. The framework divides users into multiple security domains and provides patient-centric access control. It improves privacy and scalability while supporting secure data sharing among healthcare organizations. However, repeated encryption of common access policies increases computational cost and storage overhead in large-scale deployments.

5. Title: *"Efficient and Secure Fine-Grained Access Control for Cloud-Assisted Personal Health Record Systems"*

Authors: Jian Shen, Jin Li, Xiaofeng Chen

Description:

This paper introduces an efficient fine-grained access control mechanism for cloud-assisted PHR systems. It combines Attribute-Based Encryption with optimized key management techniques to improve system efficiency while preserving patient privacy. The proposed method reduces computational complexity compared to earlier approaches but still requires improvements in handling shared access policies and reducing redundant encryption operations.

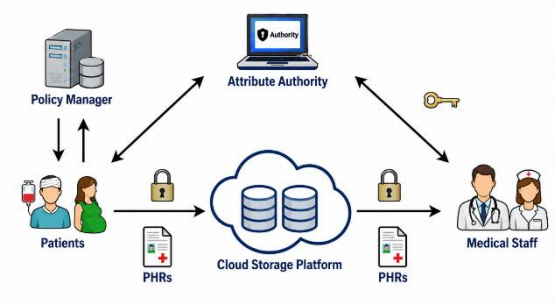
6. Title: *"Unified Fine-Grained Access Control for Personal Health Records in Cloud Computing"*

Authors: *Research Authors (Original Proposed Framework)*

Description:

This work proposes a unified fine-grained access control framework for secure Personal Health Record sharing in cloud computing. The system identifies common access sub-policies among multiple patients and generates shared encrypted components to reduce redundant encryption. By integrating Attribute-Based Encryption with unified policy management, the framework minimizes computational overhead, improves storage efficiency, supports dynamic user management, and enhances patient privacy. The proposed approach provides a scalable and secure solution for modern cloud-based healthcare systems while maintaining fine-grained access control and strong data confidentiality.

SYSTEM ARCHITECTURE



EXPLANATION OF THE SYSTEM ARCHITECTURE

Unified Fine-Grained Access Control for Personal Health Records in Cloud Computing

The proposed **Unified Fine-Grained Access Control for Personal Health Records (PHRs) in Cloud Computing** architecture provides a secure, scalable, and patient-centric framework for storing, sharing, and accessing electronic health records in a cloud environment. The architecture integrates **Attribute-Based Encryption (ABE)** with **Unified Access Policy Management** to ensure that only authorized healthcare professionals can access sensitive medical information while preserving patient privacy.

The system consists of **six major modules**, each responsible for a specific functionality in secure PHR management.

1. DATA OWNERS (PATIENTS)

This module represents the **patients**, who are the owners of their Personal Health Records (PHRs). Patients have complete control over who can access their medical records.

Components

a) Patient / Record Owner

The patient is responsible for creating, updating, and sharing medical records.

Examples of stored information include:

Received: 22-05-2026 | Accepted: 30-06-2026 | Published: 06-07-2026

International Journal of
AI ELECTRICAL CIVIL AND MECHANICAL ENGINEERING
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0434 www.zesterapublications.com Original Research Paper

- Personal Information
- Medical History
- Laboratory Reports
- Prescriptions
- Medical Imaging
- Allergies
- Vaccination Records
- Diagnosis Reports
- Treatment History

The patient decides which healthcare providers are allowed to access specific parts of the medical record.

b) PHR Data

The PHR database contains:

- Demographic Details
- Medical History
- Lab Test Results
- Prescriptions
- X-ray / MRI / CT Images
- Allergy Information
- Clinical Notes

Before uploading, all medical records remain under the patient's control.

c) Pre-processing and Encryption

Before uploading records to the cloud, the patient performs the following operations:

- Defines the access policy
- Specifies user attributes (Doctor, Nurse, Lab Technician, etc.)
- Encrypts the PHR using **Attribute-Based Encryption (ABE)**
- Generates encrypted ciphertext

Only encrypted records are uploaded to the cloud.

d) Upload Encrypted PHR

After encryption:

- Plain medical data never leaves the patient's device.
- Only encrypted PHR files are transmitted.
- Secure communication protects data during upload.

This ensures confidentiality even if the cloud server is compromised.

2. TRUSTED AUTHORITIES

The Trusted Authority is responsible for user authentication, attribute verification, and secure key management.

The architecture divides this module into three authorities.

a) Attribute Authority

Responsibilities include:

- Managing user attributes
- Verifying user identity
- Assigning healthcare roles
- Issuing attribute certificates

Example attributes:

- Doctor
- Cardiologist
- Nurse
- Laboratory Technician
- Insurance Officer
- Emergency Physician

b) Key Generation Authority

This authority generates cryptographic keys.

Responsibilities:

- System Initialization
- Master Key Generation
- User Secret Key Generation
- Secure Key Distribution

Each authorized user receives secret keys corresponding to their verified attributes.

c) Policy Authority

Responsible for access policy management.

Functions include:

- Creating standard access policies
- Managing policy templates
- Updating access rules
- Reviewing authorization policies

Example policy:

(Doctor AND Cardiology Department)
OR
(Emergency Physician)

Only users satisfying this policy can decrypt the record.

3. CLOUD SERVER

The Cloud Server provides secure storage and cloud services without accessing plaintext patient information.

a) Encrypted PHR Repository

Received: 22-05-2026 | Accepted: 30-06-2026 | Published: 06-07-2026

International Journal of
AI ELECTRICAL CIVIL AND MECHANICAL ENGINEERING
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0434 www.zesterapublications.com Original Research Paper

The repository stores:

- Encrypted Medical Records
- Encrypted Images
- Encrypted Laboratory Reports
- Encrypted Prescriptions

The cloud server cannot decrypt any stored information.

b) Unified Ciphertext Storage

This is the main innovation of the proposed architecture.

Traditional systems encrypt identical policies repeatedly.

The proposed system:

- Identifies common access sub-policies
- Creates shared encrypted components
- Eliminates redundant encryption
- Reduces storage requirements
- Improves encryption efficiency

For example,

Instead of encrypting

Doctor

Hospital

Cardiology

thousands of times,

the system creates one common encrypted component that multiple patients can reuse.

This significantly reduces computational cost.

c) Other Cloud Services

The cloud also provides:

- Secure Storage
- Backup Services
- High Availability
- Cloud Computation

These services improve reliability while keeping all records encrypted.

4. AUTHORIZED USERS (HEALTHCARE PROVIDERS)

Authorized users access patient records according to their assigned attributes.

Examples include:

- Doctors
- Nurses
- Laboratory Technicians
- Insurance Agents
- Emergency Physicians
- Medical Researchers

User Attributes

Every healthcare provider possesses verified attributes.

Examples include:

- Role
- Specialization
- Department
- Organization
- License Number
- Security Clearance
- Location

These attributes determine access permissions.

Access Process

Whenever a healthcare provider requests a medical record, the following process occurs:

Step 1

User Login

↓

Step 2

Authentication

↓

Step 3

Attribute Verification

↓

Step 4

Policy Matching

↓

Step 5

Ciphertext Decryption (If Authorized)

↓

Step 6

View Patient Health Record

If the user's attributes do not satisfy the policy, access is denied.

5. UNIFIED ACCESS CONTROL MANAGER

This module is the heart of the proposed architecture.

It manages access policies efficiently while minimizing encryption redundancy.

a) Policy Analysis and Optimization

This module performs:

- Identifying common access sub-policies
- Extracting shared attributes

Received: 22-05-2026 | Accepted: 30-06-2026 | Published: 06-07-2026

International Journal of
AI ELECTRICAL CIVIL AND MECHANICAL ENGINEERING
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0434 www.zesterapublications.com Original Research Paper

- Creating unified encrypted components
- Reducing duplicate encryption
- Improving storage efficiency
- Reducing computational overhead

This is the major improvement over conventional ABE systems.

b) Unified Policy Management

Responsibilities include:

- Creating unified access structures
- Maintaining policy indexes
- Updating access policies
- Adding new users
- Revoking users
- Dynamic permission updates
- Efficient key revocation

The system supports dynamic healthcare environments.

c) Access Decision Engine

Whenever an access request is received, the engine:

- Evaluates access requests
- Matches user attributes with policy
- Generates access tokens
- Grants or denies permissions

Only authorized users receive decryption capability.

6. AUDIT AND MONITORING MODULE

This module continuously monitors system security.

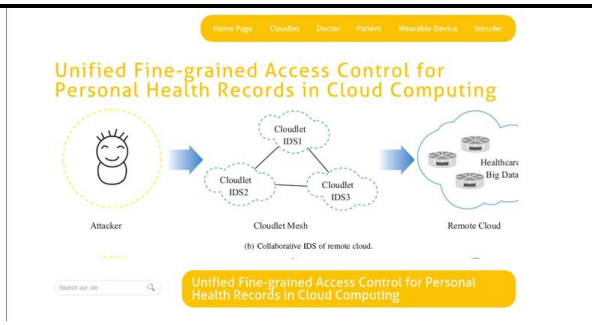
It records every activity performed in the cloud.

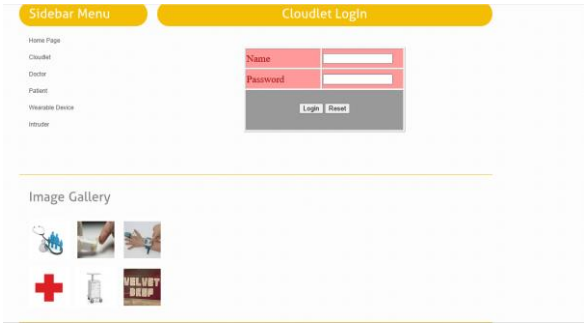
Functions

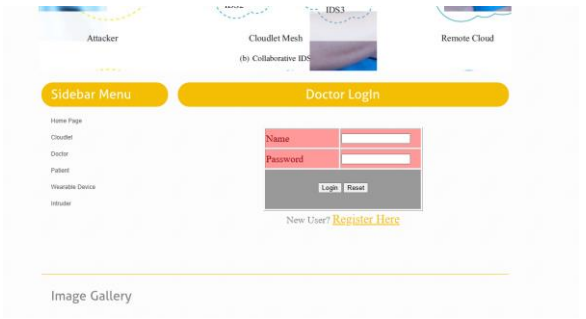
The module stores:

- User Login Records
- Access Logs
- User Activities
- Policy Changes
- Security Alerts
- Unauthorized Access Attempts
- Anomaly Detection Reports
- Dashboard Statistics

III. SCREEN SHOTS

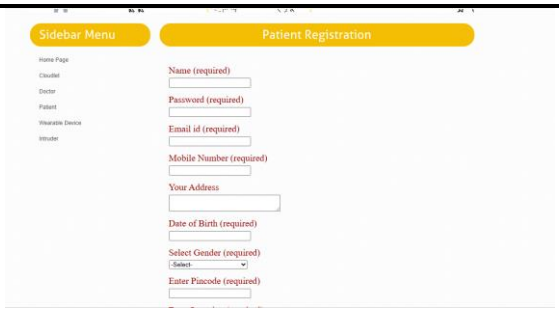


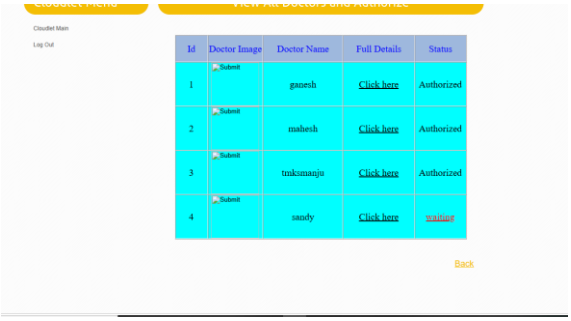


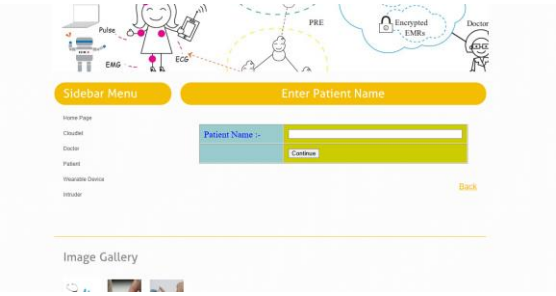


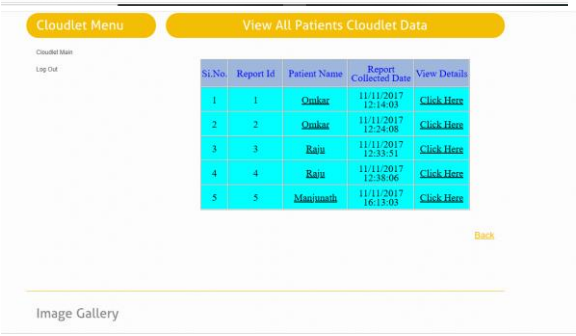
Received: 22-05-2026 | Accepted: 30-06-2026 | Published: 06-07-2026

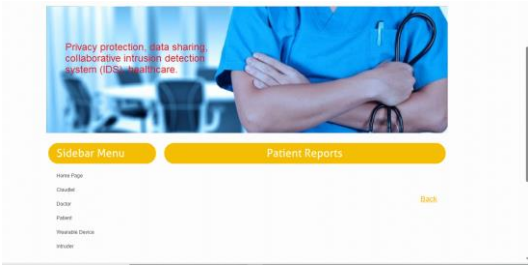
International Journal of
AI ELECTRICAL CIVIL AND MECHANICAL ENGINEERING
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0434 www.zesterapublications.com Original Research Paper





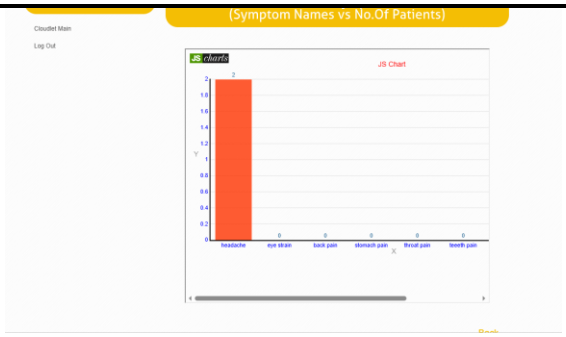


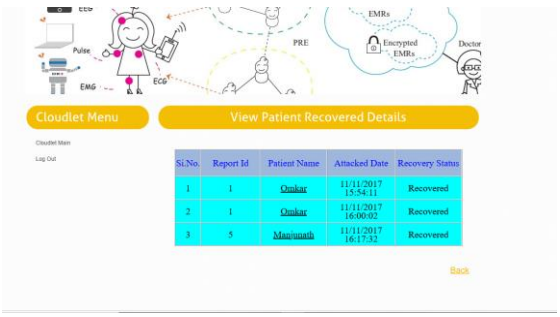


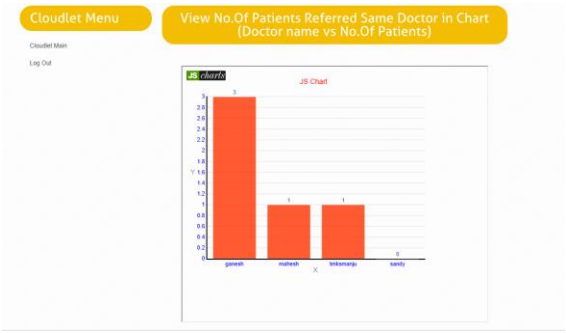


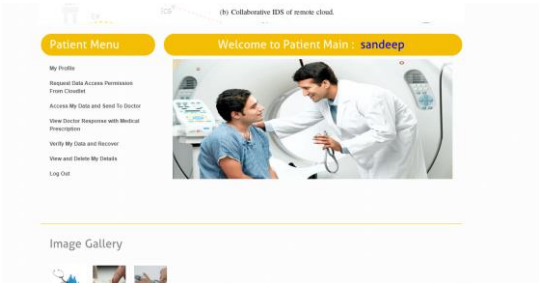
Received: 22-05-2026 | Accepted: 30-06-2026 | Published: 06-07-2026

International Journal of
AI ELECTRICAL CIVIL AND MECHANICAL ENGINEERING
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0434 www.zesterapublications.com Original Research Paper









IV. CONCLUSION

The **Unified Fine-Grained Access Control for Personal Health Records in Cloud Computing** project presents a secure, scalable, and patient-centric solution for protecting sensitive healthcare information stored in cloud environments. The proposed framework integrates **Attribute-Based Encryption (ABE)** with **unified access policy management** to provide fine-grained access control, ensuring that only authorized users whose attributes satisfy predefined access policies can access encrypted Personal Health Records (PHRs).

Unlike traditional cloud-based healthcare systems that rely on role-based or identity-based access control, the proposed system eliminates redundant encryption by identifying common access sub-policies and generating shared encrypted components. This significantly reduces computational overhead, storage requirements, and encryption time while improving the overall efficiency of secure data sharing.

The architecture enables patients to retain complete ownership and control over their medical records, allowing them to define customized access policies for doctors, nurses, laboratory technicians, insurance providers, and emergency physicians. The use of trusted authorities for attribute verification and secure key generation further enhances the confidentiality, integrity, and authenticity of the healthcare data.

Additionally, the proposed framework supports dynamic user management, efficient key revocation, secure cloud storage, and comprehensive audit logging, making it suitable for large-scale healthcare environments. Even if the cloud server is compromised, patient data remains protected because only encrypted records are stored, and decryption is possible only for authorized users possessing valid attribute-based secret keys.

Overall, the proposed system successfully addresses the limitations of existing cloud-based PHR systems by providing **strong**

Received: 22-05-2026 | Accepted: 30-06-2026 | Published: 06-07-2026

International Journal of
AI ELECTRICAL CIVIL AND MECHANICAL ENGINEERING
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0434 www.zesterapublications.com Original Research Paper

privacy protection, flexible access control, reduced computational complexity, improved storage efficiency, and secure healthcare data sharing. It offers a reliable and practical solution for modern cloud computing environments where protecting patient privacy while enabling efficient medical collaboration is of paramount importance. The framework has the potential to improve the security, trustworthiness, and interoperability of digital healthcare systems and serves as a strong foundation for future advancements in secure cloud-based health information management.

FUTURE SCOPE OF THE PROJECT

The **Unified Fine-Grained Access Control for Personal Health Records (PHRs) in Cloud Computing** project provides a secure and efficient framework for protecting sensitive healthcare data. Although the proposed system successfully addresses privacy, security, and access control challenges, several enhancements can further improve its functionality, scalability, and applicability in future healthcare environments.

One significant future enhancement is the integration of **Blockchain technology** to provide decentralized and tamper-proof storage of access logs and policy updates. Blockchain can ensure transparency, traceability, and immutability of healthcare transactions while eliminating dependence on a single trusted authority.

The system can also be extended by incorporating **Artificial Intelligence (AI)** and **Machine Learning (ML)** techniques to detect suspicious access patterns, identify insider threats, and predict potential cyberattacks. Intelligent security monitoring can automatically recognize abnormal user behavior and generate real-time alerts to prevent unauthorized access.

Another promising direction is the implementation of **Multi-Authority Attribute-Based Encryption (MA-ABE)**. Instead of relying on a single authority for issuing attribute keys, multiple independent authorities can manage different sets of attributes, improving security, scalability, and trust in large healthcare ecosystems.

Future versions of the system can support **Internet of Medical Things (IoMT)** devices, enabling wearable health sensors, smart medical equipment, and remote monitoring devices to securely upload real-time patient data to the cloud. This will facilitate continuous health monitoring and improve telemedicine services.

The framework can also be enhanced by integrating with **Electronic Health Record (EHR)** systems and national healthcare databases using interoperability standards such as **HL7** and **FHIR**. This will enable seamless exchange of patient information among hospitals, laboratories, clinics, and healthcare organizations while maintaining strong privacy protection.

To improve accessibility, dedicated **mobile applications** for Android and iOS platforms can be developed. These applications would allow patients and healthcare providers to securely access health records, manage permissions, receive notifications, and monitor health information from anywhere.

Another important enhancement is the implementation of **emergency access management** using intelligent break-glass mechanisms. During critical medical situations, authorized emergency physicians could receive temporary access to essential patient records under strictly monitored conditions without compromising long-term privacy.

Future research may also focus on improving the efficiency of cryptographic operations by developing **lightweight Attribute-Based Encryption algorithms** that reduce encryption, decryption, and key management overhead, making the system suitable for resource-constrained devices and large-scale cloud deployments.

The proposed framework can further incorporate **privacy-preserving data**

Received: 22-05-2026 | Accepted: 30-06-2026 | Published: 06-07-2026

International Journal of
AI ELECTRICAL CIVIL AND MECHANICAL ENGINEERING
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0434 www.zesterapublications.com Original Research Paper

analytics using technologies such as Secure Multi-Party Computation (SMPC), Homomorphic Encryption, or Federated Learning. These techniques would enable medical researchers to analyze healthcare data without exposing sensitive patient information. Finally, deploying the system on commercial cloud platforms such as **Amazon Web Services (AWS)**, **Microsoft Azure**, or **Google Cloud Platform (GCP)** would improve scalability, availability, disaster recovery, and real-time healthcare service delivery.

Future Enhancements

- Integrate **Blockchain** for decentralized and tamper-proof access control.
- Implement **Multi-Authority Attribute-Based Encryption (MA-ABE)** for enhanced security.
- Apply **Artificial Intelligence and Machine Learning** for intelligent threat detection and anomaly analysis.
- Support **Internet of Medical Things (IoMT)** devices for real-time patient monitoring.
- Integrate with **Electronic Health Records (EHRs)** using **HL7** and **FHIR** interoperability standards.
- Develop **Android and iOS mobile applications** for secure remote access.
- Implement secure **emergency (break-glass) access** mechanisms for critical healthcare situations.
- Optimize encryption algorithms to reduce computational and storage overhead.
- Enable **privacy-preserving healthcare analytics** using Homomorphic Encryption, Secure Multi-Party Computation, or Federated Learning.
- Deploy the solution on public cloud platforms such as **AWS**, **Microsoft Azure**, or **Google Cloud Platform**.
- Introduce **biometric and multi-factor authentication** to strengthen user authentication.
- Support multilingual interfaces and cross-hospital interoperability for broader adoption.

These enhancements will further strengthen the security, efficiency, scalability, and interoperability of cloud-based Personal Health Record systems, making the framework more suitable for next-generation digital healthcare infrastructures.

REFERENCES

- **Bethencourt, J., Sahai, A., & Waters, B. (2007).** Ciphertext-Policy Attribute-Based Encryption. *Proceedings of the IEEE Symposium on Security and Privacy (SP'07),* 321–334.
  Foundational paper introducing Ciphertext-Policy Attribute-Based Encryption (CP-ABE) for fine-grained access control in encrypted cloud data.
- **Goyal, V., Pandey, O., Sahai, A., & Waters, B. (2006).** Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data. *Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS),* 89–98.
  Introduces Key-Policy Attribute-Based Encryption (KP-ABE), providing the foundation for attribute-based access control mechanisms.
- **Li, M., Yu, S., Zheng, Y., Ren, K., & Lou, W. (2013).** Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption. *IEEE Transactions on Parallel and Distributed Systems, 24(1),* 131–143.
  Presents a patient-centric PHR sharing framework using Attribute-Based Encryption with scalable access control.
- **Waters, B. (2011).** Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably

Received: 22-05-2026 | Accepted: 30-06-2026 | Published: 06-07-2026

International Journal of
AI ELECTRICAL CIVIL AND MECHANICAL ENGINEERING
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0434 www.zesterapublications.com Original Research Paper

Secure Realization. *Proceedings of the International Workshop on Public Key Cryptography (PKC),* 53–70. Proposes an efficient CP-ABE scheme with expressive access structures suitable for secure cloud applications.

- **Chase, M. (2007).** Multi-Authority Attribute-Based Encryption. *Proceedings of the Theory of Cryptography Conference (TCC),* 515–534. Introduces Multi-Authority ABE, enabling multiple trusted authorities to manage user attributes securely.
- **Sahai, A., & Waters, B. (2005).** Fuzzy Identity-Based Encryption. *Advances in Cryptology – EUROCRYPT 2005,* 457–473. Introduces the concept that later evolved into Attribute-Based Encryption for flexible access control.
- **Liu, X., Deng, R. H., Choo, K. K. R., & Yang, Y. (2018).** Privacy-Preserving Healthcare Data Sharing in Cloud Computing: A Survey. *IEEE Access, 6,* 51933–51952. Reviews privacy-preserving techniques and secure healthcare data-sharing models in cloud environments.
- **Shen, J., Li, J., Chen, X., & Huang, X. (2017).** Secure and Efficient Fine-Grained Access Control for Cloud-Assisted Personal Health Record Systems. *Future Generation Computer Systems, 78,* 719–731. Presents an efficient fine-grained access control framework for secure PHR management in cloud computing.
- **Mell, P., & Grance, T. (2011).** The NIST Definition of Cloud Computing. *National Institute of Standards and Technology (NIST) Special Publication 800-145.* Defines the essential characteristics, service models, and deployment models of cloud computing.
- Xhafa, F., Barolli, L., & Takizawa, M. (2019). **Cloud Computing Security: Foundations and Challenges.** ***Academic Press.*** **Provides comprehensive coverage of cloud security mechanisms, privacy preservation, and secure data management techniques applicable to healthcare systems.**