GLOBUS PUBLICATION

**Globus** An International Journal of Medical Science, Engineering and Technology
A Refereed Research Journal
Vol 13 / No 2 / Jul-Dec 2024 ISSN: 2319-8958

# SECURE CLOUD SHARING OF MEDICAL RECORDS USING ATTRIBUTE-BASED ENCRYPTION (ABE) WITH DATA OWNER-DEFINED ACCESS CONTROL

*Anoop Srivastava
**Shakeeb Khan

**Paper Received**: 26.11.2024 / **Paper Accepted**: 18.12.2024 / **Paper Published**: 20.12.2024
**Corresponding Author:** Anoop Srivastava; doi: 10.46360/globus.met.320242009

## Abstract

With the growing adoption of cloud-based healthcare systems, ensuring the security and privacy of medical records is a critical challenge. Traditional encryption methods often lack the flexibility required for fine-grained access control, making it difficult for data owners to define and enforce customized access policies. Attribute-Based Encryption (ABE) offers a robust solution by enabling data encryption based on predefined attributes, ensuring that only authorized users can access sensitive medical information. This study explores the implementation of ABE for secure cloud sharing of medical records, allowing data owners to define and enforce access control policies dynamically. It analyzes the effectiveness of Key-Policy ABE (KP-ABE) and Ciphertext-Policy ABE (CP-ABE) in managing hierarchical access structures while ensuring confidentiality, integrity, and scalability. Additionally, it discusses challenges such as computational overhead, key management complexities, and revocation mechanisms, proposing optimized solutions for real-world healthcare applications. By integrating ABE with blockchain and decentralized identity management, the study highlights potential advancements in securing electronic health records (EHRs) against unauthorized access and cyber threats.

**Keywords:** Cloud Security, Attribute-Based Encryption (ABE), Medical Data Privacy, Secure Cloud Sharing, Data Owner-Defined Access Control, Electronic Health Records (EHRs), Ciphertext-Policy ABE (CP-ABE), Key-Policy ABE (KP-ABE), Access Control Mechanisms, Blockchain in Healthcare.

## Introduction

The adoption of cloud computing in healthcare has revolutionized medical data storage, accessibility, and sharing. Cloud-based Electronic Health Records (EHRs) enable seamless collaboration among healthcare providers, improve patient care, and enhance operational efficiency. However, ensuring the security and privacy of medical records remains a major challenge, as cloud environments are vulnerable to unauthorized access, data breaches, and cyber threats. Conventional encryption techniques provide security but often lack the flexibility required for fine-grained access control, making it difficult for data owners to regulate who can access specific medical information.

To address these security concerns, Attribute-Based Encryption (ABE) has emerged as a promising cryptographic solution for secure cloud sharing of medical records. ABE allows data owners to define and enforce access control policies dynamically based on user attributes rather than static encryption keys. Unlike traditional encryption methods, ABE enables role-based and condition-based data access, ensuring that only authorized users—such as doctors, specialists, and insurance providers—can decrypt and access medical records while maintaining patient privacy.

There are two primary forms of ABE:

1. **Key-Policy ABE (KP-ABE):** The access structure is embedded in the user's private key, and data is encrypted based on attributes.
2. **Ciphertext-Policy ABE (CP-ABE):** The access policy is embedded in the ciphertext, and users possess attribute-based private keys to decrypt the data.

This study explores how ABE enhances secure cloud sharing of medical records while giving data owners the ability to define customized access control policies. It also examines challenges such as computational complexity, key management, user revocation, and scalability in real-world healthcare applications.

*Research Scholar, Maharaja Agrasen Himalayan Garhwal University, Shiv Nagar, Pokhra, India.
**Supervisor, Maharaja Agrasen Himalayan Garhwal University, Shiv Nagar, Pokhra, India.

Furthermore, the integration of ABE with emerging technologies like blockchain and decentralized identity management is discussed as a means to further enhance data security, auditability, and access control. By implementing ABE-based secure medical data sharing, healthcare organizations can improve data confidentiality, integrity, and compliance with regulations such as HIPAA and GDPR, ensuring that cloud-stored medical records remain protected against unauthorized access and cyber threats.

## Review of Literature

Sekhar (2023) explores the transformative impact of Artificial Intelligence (AI) in cloud computing environments, highlighting its potential to revolutionize data processing, analysis, and storage. As AI-driven cloud solutions gain widespread adoption, they offer unparalleled efficiency and scalability, enabling businesses and institutions to leverage vast amounts of data for decision-making, automation, and innovation. However, this integration also presents complex security and privacy challenges, requiring advanced protective measures to mitigate the risks posed by evolving cyber threats. This scholarly article delves into the critical need for strengthening security in cloud-based AI systems, proposing innovative AI-driven security mechanisms that enhance data encryption, anomaly detection, and intrusion prevention. Through an in-depth examination of existing vulnerabilities within cloud-based AI infrastructures, the study identifies key security gaps and evaluates how AI can be leveraged to fortify cloud environments against sophisticated cyberattacks. The research focuses on the development and implementation of advanced AI algorithms that enable real-time threat detection, automated response mechanisms, and predictive analytics to counter emerging cybersecurity risks.

A significant aspect of this study is its emphasis on privacy-preserving AI techniques, ensuring that data processing, machine learning, and AI-driven analytics do not compromise sensitive personal information. The research explores methods such as homomorphic encryption, federated learning, and differential privacy, which allow AI models to be trained on decentralized datasets without exposing raw user data. These privacy-enhancing techniques play a crucial role in maintaining compliance with global data protection regulations, such as GDPR and HIPAA, while fostering user trust in AI-powered cloud applications.

By integrating these AI-driven security advancements, the study advocates for a comprehensive and resilient security framework capable of defending against present and future cyber threats. This framework ensures that cloud-based AI ecosystems remain secure, efficient, and ethically responsible, fostering confidence in AI's ability to drive digital transformation without jeopardizing user privacy. Through its comprehensive analysis and proposed methodologies, this research significantly contributes to the ongoing discourse on AI security and privacy, offering valuable insights for the development of trustworthy and robust AI applications within cloud computing.

Mary (2023) examines the impact of electronic health records (EHRs) and digital medical systems on modern healthcare, emphasizing their role in enhancing patient care, information management, and clinical efficiency. While these technological advancements have significantly improved the accessibility and organization of medical data, they have also heightened concerns about the privacy and security of sensitive patient information. Given the increasing reliance on digital healthcare solutions, it is essential to equip future healthcare professionals-particularly medical and dental students-with the necessary knowledge and competencies to safeguard patient data against potential breaches and unauthorized access.

This study seeks to assess the awareness, understanding, and attitudes of medical and dental students regarding privacy and security issues related to patient health information. A cross-sectional study was conducted among a representative sample of students from diverse academic institutions. Participants were evaluated through a structured questionnaire, which measured their knowledge, perceptions, and practices related to patient data privacy and security. The study utilized descriptive statistical analysis to interpret the findings, while also examining associations between demographic factors and levels of awareness.

The results highlight a significant disparity in knowledge among students. While 71.7% (n=232) of participants preferred electronic patient records (EHRs) due to their ease of accessibility, and 61.4% (n=198) strongly valued privacy, many lacked a comprehensive understanding of key security measures, encryption protocols, access controls, and legal frameworks governing patient data protection. Students exhibited varying degrees of familiarity with data security mechanisms, including two-factor authentication, audit trails, and national and international privacy regulations such as HIPAA and GDPR. These findings underscore the urgent need for enhanced education and training programs in medical and dental curricula, with a stronger focus on data security, cybersecurity best practices, and ethical responsibilities related to patient information. As future healthcare practitioners,

medical and dental students must develop practical competencies in data protection to foster a more secure and privacy-conscious healthcare environment. By integrating specialized training modules on healthcare cybersecurity, secure digital communication, and legal compliance, educational institutions can better prepare students to handle the evolving challenges of digital healthcare, ultimately ensuring the integrity and confidentiality of patient data in clinical practice.

## Analysis

Cloud-based healthcare systems have significantly improved medical data accessibility and efficiency, but they also pose serious security and privacy risks. Unauthorized access, cyber threats, and lack of fine-grained access control mechanisms make traditional encryption methods insufficient for protecting Electronic Health Records (EHRs). Attribute-Based Encryption (ABE) presents a robust solution by enabling data owners to define access policies based on user attributes, ensuring a balance between data security, privacy, and accessibility. This section analyzes how ABE enhances cloud security for medical records, examines its advantages and challenges, and explores potential improvements through advanced cryptographic techniques.

### Enhancing Security and Access Control with ABE

Traditional encryption models, such as symmetric and asymmetric encryption, restrict data access to predefined users with static keys. However, in cloud-based healthcare, where multiple entities (doctors, specialists, researchers, insurance providers) require different levels of access, a more dynamic and flexible encryption mechanism is needed. ABE enables:

- **Fine-Grained Access Control**: Unlike role-based access control (RBAC), ABE allows data owners to define specific attribute-based policies. For example, a patient's medical record can be accessible to a cardiologist and primary care physician but remain encrypted for general practitioners.
- **Data Confidentiality and Integrity**: Only users who satisfy the attribute-based conditions can decrypt and access the data, ensuring secure cloud storage.
- **Minimized Risk of Unauthorized Access**: Even if cloud servers are compromised, ABE ensures that only authorized users with valid attributes can decrypt the data.

**Table 1: Comparison of Key-Policy ABE (KP-ABE) and Ciphertext-Policy ABE (CP-ABE)**

| Feature | Key-Policy ABE (KP-ABE) | Ciphertext-Policy ABE (CP-ABE) |
|---|---|---|
| Access Policy Defined In | Private Key | Ciphertext |
| Flexibility | Limited, as users' keys are predefined | High, allows dynamic access control |
| Best Used For | Fixed role-based access | Dynamic policy enforcement |
| Example Usage | A hospital pre-defines access for doctors and staff | A patient encrypts medical records with rules (e.g., "Doctor AND Specialist") |

CP-ABE is generally more suitable for cloud-based medical data sharing, as it allows patients or data owners to define dynamic access policies without requiring key modifications for every new user.

### Challenges and Limitations of ABE for Cloud-Based Healthcare Systems

**a. Computational Complexity and Performance Overhead**

- ABE requires complex encryption and decryption operations, making it computationally expensive, especially for large-scale cloud applications.
- Encrypting and decrypting medical records with numerous attributes increases processing time and impacts real-time data access.
- Solutions:
    - **Outsourced Decryption**: Delegating part of the decryption process to cloud servers while ensuring that they cannot access plaintext data.
    - **Lightweight ABE Schemes**: Optimizing algorithms to reduce computational costs, such as Efficient CP-ABE models with fewer cryptographic operations.

**b. Key Management and User Revocation Issues**

- **Key distribution and revocation** remain challenging in ABE-based systems, particularly in healthcare environments

where staff and patient access frequently change.

- Revoking a user's access requires re-encrypting data or redistributing new keys, increasing administrative burden.
- Solutions:
  - **Revocable ABE (R-ABE)**: Enhancing traditional ABE by allowing dynamic revocation without requiring complete re-encryption.
  - **Blockchain-Based Key Management**: Using decentralized identity verification through blockchain to improve revocation efficiency and access tracking.

**c. Scalability and Storage Overhead**

- Storing attribute-based policies and managing multiple access requests can lead to increased storage consumption and processing delays.
- Larger datasets (e.g., high-resolution medical images, genomic data) require efficient encryption without excessive storage expansion.
- Solutions:
  - **Hierarchical ABE (HABE)**: Organizing attributes into hierarchical structures to improve efficiency.
  - **Cloud-Assisted Computation**: Leveraging cloud processing to offload encryption tasks while maintaining zero-trust security principles.

### Integration of ABE with Emerging Technologies

**a. Blockchain for Secure and Transparent Medical Record Sharing**

- Blockchain technology ensures tamper-proof logging of access requests, improving transparency in data sharing and compliance (e.g., HIPAA, GDPR).
- Smart contracts can enforce attribute-based access control, ensuring that only valid users retrieve encrypted medical records.
- Example: A decentralized blockchain-enabled EHR system where ABE-encrypted patient data is shared with verified medical professionals based on blockchain-authenticated identities.

**b. AI-Driven Attribute Management**

- AI-based systems can dynamically adjust access policies based on patient preferences, emergency scenarios, and real-time conditions.
- Example: In an emergency, an AI-driven ABE system temporarily grants access to specific doctors while maintaining logs for future audits.

**c. Federated Learning for Secure Medical Data Sharing**

- Instead of sharing raw medical data, federated learning allows hospitals to collaborate on AI training models using encrypted patient data.
- ABE ensures that only authorized parties can participate in federated training without exposing sensitive health records.

### Case Study: Secure Cloud Sharing of Medical Records Using ABE Scenario: A Cloud-Based EHR System with Attribute-Based Access Control

A hospital network adopts CP-ABE to securely share patient records among doctors, specialists, and researchers while protecting patient privacy.

**Implementation Steps:**

1. **Encryption & Access Control Definition**:
   - Patients encrypt medical records using CP-ABE with attributes such as "Doctor AND Cardiologist" or "Insurance Provider AND Approved by Patient".
2. **Attribute-Based Key Generation**:
   - The hospital generates decryption keys based on user roles and permissions.
3. **Secure Cloud Storage & Retrieval**:
   - Encrypted records are stored on AWS, Google Cloud, or Azure, ensuring zero-trust security.
4. **Revocation and Monitoring**:
   - The hospital updates access policies dynamically to revoke access from retired doctors or unauthorized users.

**Outcome & Benefits:**

- **Enhanced Privacy & Security**: Only authorized users with matching attributes can decrypt medical records.
- **Fine-Grained Access Control**: Patients retain control over who can access their health data.
- **Scalability**: Cloud-based encryption allows seamless access across multiple healthcare institutions.
- **Regulatory Compliance**: Meets HIPAA, GDPR, and HITECH Act data security standards.

Attribute-Based Encryption (ABE) offers a powerful solution for securing cloud-based medical records while allowing data owners to define dynamic access policies. CP-ABE is the preferred approach for fine-grained, user-defined access control in healthcare environments, ensuring confidentiality, integrity, and accessibility. Despite its benefits, computational overhead, key management challenges, and scalability issues must be addressed for ABE to be fully practical in real-world cloud applications. Integrating blockchain, AI-driven access control, and federated learning can further enhance security, transparency, and efficiency in medical data sharing. By adopting ABE-based secure cloud sharing, healthcare providers can ensure privacy-preserving, flexible, and efficient access control for medical records, ultimately improving patient data security and regulatory compliance.

## Conclusion

The increasing adoption of cloud-based healthcare systems necessitates robust security mechanisms to protect Electronic Health Records (EHRs) while ensuring controlled access to authorized users. Attribute-Based Encryption (ABE) provides a flexible and fine-grained access control model, allowing data owners to define dynamic access policies based on user attributes rather than static encryption keys. By implementing Ciphertext-Policy ABE (CP-ABE), healthcare providers can enhance privacy, confidentiality, and security while ensuring seamless data sharing among medical professionals, researchers, and insurers.

The analysis highlights key advantages of ABE, including improved data security, fine-grained access control, and resistance to unauthorized access. However, challenges such as high computational overhead, key management complexity, and scalability concerns must be addressed to ensure its efficient deployment in large-scale healthcare environments. Solutions like Revocable ABE (R-ABE), blockchain-based access control, AI-driven attribute management, and federated learning offer promising advancements in enhancing security, efficiency, and regulatory compliance. Integrating ABE with cloud storage, AI automation, and decentralized identity management can significantly improve the trustworthiness and transparency of medical record sharing while complying with HIPAA, GDPR, and other healthcare regulations. Moving forward, further research and optimization in lightweight encryption models and hybrid security frameworks will be essential in making ABE-based cloud security more scalable and efficient for global healthcare applications. By adopting ABE-driven security solutions, healthcare institutions can achieve a balance between accessibility, security, and privacy, ultimately strengthening patient data protection and fostering a secure digital healthcare ecosystem.

## Conflict of Interest

The authors declare that there are no significant competing financial, professional, or personal interests that might have influenced the performance or presentation of the work described in this manuscript.

## References


1. Emmanni, Phani Sekhar (2023). Security and Privacy Enhancements in Cloud-Based AI Systems. 49-54. 10.5281/zenodo.11078428.
2. Mary, Vinita, Ramakrishnan, Kesavan, Susil, Allwyn & Rahuman, Aysha (2023). Cognizance About Privacy and Security of Patients Health Information Among Medical and Dental Students.
3. Yi, Haibo (2023). Improving cloud storage and privacy security for digital twin based medical records. Journal of Cloud Computing, 12. 10.1186/s13677-023-00523-6.
4. Bohomia, V.I., & Kochegarov, V.S. (2023). Cybersecurity in cloud services using cryptographic methods. Water Transport, 1(37), 239-246. doi: 10.33298/2226-8553.2023.1.37.27.
5. Nafiiev, A., & Lande, D. (2023). Malware detection model based on machine learning. Bulletin of Cherkasy State Technological University, 3, 40-50. doi: 10.24025/2306-4412.3.2023.286374.
6. G., Dhanalakshmi, Victo, G & George, G. Victo (2023). Secure and Privacy-Preserving Storage of E-Healthcare Data in the Cloud: Advanced Data Integrity Measures and Privacy Assurance. International Journal of Engineering Trends and Technology, 71, 238-253. 10.14445/22315381/IJETT-V71I10P222.
7. Patel, R.K., Gidwani, P., & Patel, N.R. (2023). Privacy preservation and cloud computing. In D. Lakshmi & A.K. Tyagi (Eds.), Privacy preservation and secured data storage in cloud computing (pp. 88-107). Hershey: IGI Global. doi: 10.4018/979-8-3693-0593-5.ch004.
8. S, Gayathri & S, Gowri (2023). Securing medical image privacy in cloud using deep learning network. Journal of Cloud Computing, 12. 10.1186/s13677-023-00422-w.
9. Geetha Rani, E., & Chetana, D.T. (2023). A survey of recent cloud computing data security and privacy disputes and defending strategies. In J.C. Bansal, H. Sharma & A. Chakravorty (Eds.), Congress on smart computing technologies. CSCT 2022. Smart innovation, systems and technologies (Vol. 351; pp. 407-418). Singapore: Springer. doi: 10.1007/978-981-99-2468-4_31.

10. Abdulsalam, Y., & Hedabou, M. (2022). Security and privacy in cloud computing: Technical review. Future Internet, 14(1), article number 11. doi: 10.3390/fi14010011.
11. Mazur, V. (2023). Security assessment of using cloud technologies and development of methods for protection against cyber-attacks on cloud services. (Bachelor thesis, Ternopil Ivan Puluj National Technical University, Ternopil, Ukraine).
12. Aljwari, F.K. (2023). Privacy and security in cloud-based computing: Challenges and solutions. In X. Wang (Ed.), Research and applications towards mathematics and computer science (Vol. 2; pp. 1-15). Kolkata: B.P. International. doi: 10.9734/bpi/ratmcs/v2/19324D
13. Reema, S. (2023). Cloud computing as a solution for security and privacy concerns. International Journal for Research in Applied Science and Engineering Technology, 11(3), 183-187. doi: 10.22214/ijraset.2023.49375.
14. Javaid, Mohd, Haleem, Abid, Singh, Ravi, Rab, Shanay & Suman, Rajiv & Haleem Khan, Ibrahim (2022). Evolutionary Trends in Progressive Cloud Computing based Healthcare: Ideas, Enablers, and Barriers. International Journal of Cognitive Computing in Engineering, 3. 10.1016/j.ijcce.2022.06.001.
15. Sultanova, L., & Prokofieva, M. (2022). Digital security in higher education. Adult Education: Theory, Experience, Prospects, 21(1), 106-117. doi: 10.35387/od.1(21).2022.106-117.
16. Mittal, Shikha, Bansal, Ankit, Deepali, Gupta, Juneja, Sapna, Elarabawy, Mahmoud, Sharma, Ashish & Bitsue, Zelalem (2022). Using Identity-Based Cryptography as a Foundation for an Effective and Secure Cloud Model for E-Health. Computational Intelligence and Neuroscience, 7016554. 10.1155/2022/7016554.