ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 12, Issue 12, December 2025

A Comprehensive Review on Attribute-Based Encryption Techniques for Securing Healthcare Data in Cloud Environments

[1] P. Karthik, [2] Dr. D. Latha

[1] Research Scholar, Department of Computer Science and Engineering, Adikavi Nannaya University, Rajamahendravaram, Andhra Pradesh, India

[2] Associate Professor, Department of Computer Science and Engineering, Adikavi Nannaya University, Rajamahendravaram, Andhra Pradesh, India

Corresponding Author Email: [1] karthikp2518@gmail.com, [2] latha.cse@aknu.edu.in

Abstract*— With the rapid growth of cloud-based healthcare systems, ensuring data confidentiality, access control, and patient privacy has become a major research priority. Attribute-Based Encryption (ABE) has emerged as a flexible and fine-grained cryptographic solution that enables secure data sharing based on user attributes. This paper reviews seven recent research contributions focusing on various ABE schemes—including Ciphertext-Policy (CP-ABE), Key-Policy (KP-ABE), and traceable or verifiable extensions—applied to secure Electronic Health Records (EHR) and medical data in cloud settings. The reviewed studies highlight improvements in policy expression, revocation, outsourced decryption, and computational efficiency. The paper concludes that modern ABE variants offer a promising trade-off between strong security and practical performance, making them suitable for next-generation healthcare data protection. This paper is an extended continuation of our previous review work published in 2023, focusing on recent developments in Attribute-Based Encryption (ABE) techniques (2023–2025) for securing healthcare data in cloud environments.[1]

Keywords: Cloud Security, Attribute-Based Encryption, Electronic Health Records, Access Control, Healthcare Data Privacy.

I. BACKGROUND

Cloud computing has transformed healthcare data management by providing scalable and cost-effective storage for Electronic Health Records (EHRs). However, outsourcing sensitive patient data to third-party clouds raises critical security challenges related to unauthorized access and privacy breaches. Traditional models like Role-Based Access Control (RBAC) or Identity-Based Encryption (IBE) fail to provide the required flexibility for dynamic healthcare environments.

Attribute-Based Encryption (ABE), first proposed by Sahai and Waters, offers fine-grained access control where data owners define policies based on user attributes (e.g., role, department, clearance level). Recent research has adapted ABE for healthcare applications to ensure confidentiality, efficiency, and interoperability in distributed cloud environments.

This study extends our earlier review paper titled “A Review on Cloud Security Issues and Usage of ABE Mechanism to Safeguard Healthcare Data in the Cloud” (P.Karthik, Dr.D.Latha. et al., 2023).[1] The previous paper [1] provided a foundational overview of cloud security challenges and ABE’s role in healthcare data protection. In continuation, the present work focuses on recent advancements (2023–2025) in ABE frameworks, including performance optimizations, revocation mechanisms, and hybrid approaches integrating blockchain and IoT for enhanced healthcare data security.

II. LITERATURE REVIEW

Recent studies have explored various enhancements to Attribute-Based Encryption (ABE) for securing healthcare data. Redwan Walid et al. (2024) focused on improving healthcare data confidentiality by implementing CP-ABE for cloud-based Electronic Health Record (EHR) sharing, enabling fine-grained access control. Ximing Li et al. (2024) advanced this idea by integrating CP-ABE with blockchain to provide traceability, which enhances transparency and minimizes key misuse. Gurupriya et al. (2024) contributed a lightweight ABE scheme optimized for Internet of Medical Things (IoMT) environments, achieving faster computation and efficient decryption on resource-limited devices. Addressing dynamic user environments, Dr. R. Kaviarasan et al. (2024) introduced a revocable ABE mechanism that supports user revocation and key updates, offering protection against unauthorized access. To reduce user-side computational burden, Zhongxiang He et al. (2023) proposed an outsourced decryption ABE model where cloud servers assist with decryption while maintaining data security. Further strengthening trust in cloud operations, Malte Kerl et al. (2025) developed verifiable ABE, allowing users to confirm the correctness of outsourced decryption and ensuring accountability. Finally, Senthilkumar Kalarani et al. (2025) addressed scalability and trust issues through a multi-authority ABE framework for EHRs, distributing key

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 12, Issue 12, December 2025

generation across multiple authorities to eliminate single-point-of-trust vulnerabilities. Together, these works demonstrate significant progress in enhancing security, efficiency, transparency, and scalability of ABE-based healthcare data protection.

Table 1. Summary of literature review

Author	Focus	Approach and Techniques	Key Findings
RedwanWalid et al. (2024) [2]	ABE-based healthcare data security	Implemented CP-ABE for EHR sharing in cloud	Ensures fine-grained access and confidentiality
Ximing Li et al. (2024) [3]	Hybrid ABE and Blockchain	Combines CP-ABE with blockchain for traceability	Improved transparency and reduced key abuse
Gurupriya et al. (2024) [4]	Lightweight ABE for IoMT	Optimized ABE for real-time healthcare IoT	Lower computation time and efficient decryption
Dr. R.Kaviarasan et al. (2024) [5]	Revocable ABE	Introduced user revocation and key update mechanism	Effective against user revocation threats
Zhongxiang He et al. (2023) [6]	Outsourced Decryption ABE	Enables cloud-assisted decryption	Reduces client computation cost while preserving security
Malte Kerl et al. (2025) [7]	Verifiable ABE	Allows verification of outsourced decryption	Adds accountability to cloud storage operations
Senthilkumar Kalarani et al. (2025) [8]	Multi-authority ABE for EHRs	Distributed key generation via multiple authorities	Enhances scalability and avoids single-point trust issues

III. COMPARATIVE ANALYSIS

The reviewed works collectively address major security and efficiency concerns in healthcare data encryption.

- **Security:** All models ensure data confidentiality and resistance to unauthorized access.
- **Performance:** Outsourced and lightweight ABE models reduce encryption/decryption times, improving usability in real-time systems.
- **Revocation & Verification:** Recent models integrate traceability and revocation to enhance reliability.
- **Scalability:** Multi-authority ABE improves distributed healthcare network support.

IV. DISCUSSION

While ABE-based systems have demonstrated significant potential, implementation in real-world healthcare systems still faces challenges:

- Managing **large attribute sets** increases policy complexity and encryption overhead.
- Ensuring **key management efficiency** remains critical for large user groups.
- **Policy updates and revocations** need more automation for dynamic hospital environments.

Emerging trends include integration of ABE with blockchain, artificial intelligence (for adaptive policy generation), and homomorphic encryption (for privacy-preserving computation).

V. CONCLUSION

This review concludes that Attribute-Based Encryption is an effective cryptographic technique for protecting sensitive healthcare data in the cloud. The analyzed papers demonstrate how ABE models continue to evolve with stronger security, reduced computation costs, and better scalability. Future research should focus on hybrid ABE-blockchain systems, lightweight designs for IoT healthcare, and interoperability frameworks to meet compliance standards like HIPAA.

REFERENCES

[1] A Review on Cloud Security issues and usage of ABE mechanism to safeguard Health care data in the cloud. P.Karthik, Dr.D.Latha, 2023

[2] Comparison of attribute-based encryption schemes in securing healthcare systems, RedwanWalid1*, Karuna Pande Joshi1 & SeungGeol Choi2, 2024

[3] Revocable and verifiable weighted attribute-based encryption with collaborative access for electronic health record in cloud, Ximing Li1, Hao Wang1, Sha Ma1*, Meiyan Xiao1 and Qiong Huang1, 2024

[4] A Survey on ciphertext policy Attribute-Based Encryption encryption scheme based cloud E-health care secure frame work, Gurupriya KG, Dr. AS Annesh Kumar, 2024

[5] Enhancing Data Security in cloud using CP-ABE, Dr. R.Kaviarasan, GM Gayathri, K.Dinesh Kumar, P.Surya Pratap, S.Ashok Kumar, 2024

[6] Revocable and Traceable Undeniable Attribute-Based Encryption in Cloud-Enabled E-Health Systems Zhongxiang

He 1, Yuling Chen 1,*, Yun Luo 1, Lingyun Zhang 2 and Yingying Tang 2, 2023

[7] Privacy-preserving attribute-based access control using homomorphic encryption, Malte Kerl1*, Ulf Bodin1 and Olov Schelén1, 2025

[8] A secure and cloud-based patient management system using attribute-based encryption algorithm,Senthilkumar Kalarani1, Mahalingam Shobana2, Edamakanti Uma Shankari3, Bolly Joshi Praveena4, Subramaniam Shanthi5, Rathinasabapathy Ramadevi6, Rajendar Sandiri7, 2025