# A Comprehensive Survey of Attribute-Based Encryption Techniques in Cloud Computing

[1]Dr. Ruksar Fatima, Professor, Khaja Bandanawaz University, India.
[2]Mr. Mohammed Naveeduddin, Khaja Bandanawaz University, India.

Corresponding Author: Dr. Ruksar Fatima, Professor, Khaja Bandanawaz University, India.

**ABSTRACT**
Cloud computing has become a dominant paradigm for data storage and service delivery, allowing users to outsource sensitive information to remote servers while accessing resources on demand. However, outsourcing data across different trust domains raises significant challenges in ensuring security, privacy, and fine-grained access control. Traditional encryption mechanisms fall short in providing scalable and flexible access management for dynamic cloud environments. Attribute-Based Encryption (ABE), a public key cryptographic approach, addresses these concerns by binding ciphertext access to user attributes and defined policies. Recent advancements such as Ciphertext-Policy ABE (CP-ABE), Key-Policy ABE (KP-ABE), Hierarchical ABE (HABE), and Multi-Authority ABE (MA-ABE) have introduced stronger security guarantees, decentralized control, and improved scalability. Moreover, emerging trends in lightweight ABE for IoT-cloud integration, blockchain-assisted ABE for decentralized trust, and post-quantum ABE for resistance against quantum attacks are shaping the future of secure cloud services. This survey critically analyzes existing ABE schemes, highlights their limitations, and discusses potential solutions and enhancements for achieving robust, efficient, and privacy-preserving data sharing in cloud computing.

**KEYWORDS:** Attribute-Based Encryption, Ciphertext-Policy, Key-Policy, Fine-Grained Access Control, Multi-Authority, Post-Quantum Security, Blockchain-Assisted ABE

## 1. INTRODUCTION

Cloud computing has emerged as a transformative paradigm in modern computing, enabling ubiquitous, on-demand access to shared resources such as storage, applications, and computational power [20]. By outsourcing data and services to third-party providers, individuals and organizations can reduce infrastructure costs and improve scalability. However, this shift from local storage to cloud-based systems introduces critical security and privacy challenges. Since cloud environments often span multiple trust domains, data confidentiality, integrity, and fine-grained access control become primary concerns [19], [21].

Traditional cryptographic methods, while effective for securing data at rest or in transit, are not sufficient to handle dynamic and complex access requirements in cloud environments. Users demand mechanisms that not only ensure data confidentiality but also provide flexible and scalable access policies, allowing data owners to define who can access specific resources under varying conditions [17], [18].

Attribute-Based Encryption (ABE) has emerged as a promising solution to address these challenges. ABE is a form of public-key cryptography where access control is enforced through attributes associated with users and defined policies embedded in the ciphertext [20]. This fine-grained access control model ensures that only users with matching attributes can decrypt and access the data. Two main variants of ABE dominate research: Key-Policy ABE (KP-ABE), where access policies are embedded in private keys, and Ciphertext-Policy ABE (CP-ABE), where policies are attached to the ciphertext [19], [21]. Over time, advanced extensions such as Hierarchical ABE (HABE) and Multi-Authority ABE (MA-ABE) have been proposed to improve scalability, decentralization, and resistance against single points of failure [2], [3], [5].

Recent research has further explored lightweight ABE schemes for resource-constrained devices [6], [11], integration with the Internet of Things (IoT) [12], and blockchain-assisted ABE to provide decentralized trust management [15]. Additionally, with the anticipated rise of quantum computing, post-quantum ABE schemes are gaining attention to ensure long-term data security in the cloud [9], [16].

This survey provides a comprehensive review of ABE techniques in cloud computing, analyzing their design principles, advantages, and limitations. It also highlights emerging trends and future research directions to achieve efficient, scalable, and privacy-preserving data sharing in cloud-based environments [13], [14].

## 2. METHODS

This survey adopts a structured review methodology to examine the evolution, strengths, and limitations of Attribute-Based Encryption (ABE) techniques in cloud computing. The primary goal is to analyze existing schemes and highlight emerging advancements that address the challenges of data security, privacy, and fine-grained access control [19], [20], [21].

### 2.1. Literature Selection

Relevant research papers, conference proceedings, and survey articles were collected from reputed digital libraries including IEEE Xplore, ACM Digital Library, SpringerLink, Elsevier ScienceDirect, and Google Scholar. Publications from 2010 to 2025 were considered to capture both foundational contributions and the most recent developments, including lightweight [6], [11], decentralized [2], [5], and post-quantum ABE schemes [9], [16].

### 2.2. Inclusion and Exclusion Criteria

- *Inclusion:* Studies focusing on ABE models (KP-ABE, CP-ABE, HABE, MA-ABE) [19], [20], [2], [3], [21], their applications in cloud storage [6], [11], IoT-cloud integration [12], blockchain-based ABE [15], and post-quantum approaches [9].
- *Exclusion:* Works that address only general cloud cryptography without specific reference to ABE or those lacking a comparative evaluation.

### 2.3. Classification Framework

To provide a comprehensive analysis, the reviewed schemes were categorized based on:

- **Core model:** KP-ABE, CP-ABE, HABE, MA-ABE [19], [20], [2], [3]
- **Optimization strategies:** lightweight design [6], [11], revocation mechanisms [17], [18], re-encryption [8], scalability improvements [1], [16]
- **Application domains:** secure cloud storage [6], [13], IoT-cloud [12], healthcare data [13], e-government [10], and blockchain-assisted systems [15]
- **Security considerations:** resistance to collusion attacks [5], [18], forward/backward secrecy [19], [20], post-quantum resilience [9], [16]

### 2.4. Comparative Analysis

The selected schemes were systematically compared in terms of computational efficiency [1], [16], storage overhead [6], scalability [2], [17], and level of access control granularity [19], [20]. Strengths and limitations of each approach were summarized to identify research gaps and future directions [14].

Through this methodology, the survey ensures a balanced evaluation of both classical and state-of-the-art ABE techniques, offering insights into their practical applicability in modern cloud environments [13].

## 3. RESULTS AND DISCUSSION

This section presents the findings of the survey by analyzing existing Attribute-Based Encryption (ABE) schemes and discussing their applicability in cloud computing environments. The results highlight how ABE provides fine-grained access control, the trade-offs between different models, and the emerging directions in research [14].

### 3.1. Key-Policy ABE (KP-ABE)

KP-ABE schemes embed access policies into user keys, allowing data owners to assign attributes to ciphertext [19]. These schemes provide flexibility in delegating access but are limited when data owners need direct control over access policies [3]. While KP-ABE is efficient for hierarchical access, it suffers from scalability issues when managing large user groups [2], [17].

### 3.2. Ciphertext-Policy ABE (CP-ABE)

In CP-ABE, access policies are embedded within the ciphertext, giving data owners explicit control over who can access their data [20], [21]. This makes CP-ABE particularly suitable for secure data sharing in cloud environments. However, traditional CP-ABE incurs significant computational overhead in encryption and decryption operations, making it unsuitable for resource-constrained environments without optimization [18].

### 3.3. Hierarchical ABE (HABE)

HABE extends ABE by introducing multiple levels of authorities, which reduces the burden on a single key issuer and enhances scalability [3], [17]. It is particularly effective for enterprise-level applications where hierarchical structures (e.g., departments, organizations) define access. Nonetheless, HABE remains vulnerable to key management complexity and potential trust issues between authorities [2].

### 3.4. Multi-Authority ABE (MA-ABE)

A-ABE addresses the single point of failure by distributing key generation across multiple authorities [21], [5]. This decentralization strengthens trust and prevents collusion but requires efficient coordination among authorities. Recent blockchain-assisted MA-ABE approaches provide tamper-proof logging and decentralized trust management, improving reliability [15].

### 3.5. Lightweight ABE for IoT-Cloud Integration

With the rapid growth of IoT devices connected to cloud platforms, lightweight ABE schemes have been developed to reduce computational and storage costs [6]. These approaches use techniques such as outsourcing decryption [8], hybrid encryption [11], and attribute compression. While they improve performance, they sometimes compromise on flexibility and require additional trust in semi-trusted third parties [12].

### 3.6. Post-Quantum ABE

Quantum computing poses a significant threat to classical cryptographic primitives. Recent research has introduced lattice-based and code-based ABE schemes resistant to quantum attacks [9]. Although still in early stages, these schemes demonstrate the potential to future-proof cloud security but often suffer from large ciphertext sizes and computational overhead [1], [7], [16].

### 3.7. Comparative Insights

The comparative analysis reveals that:

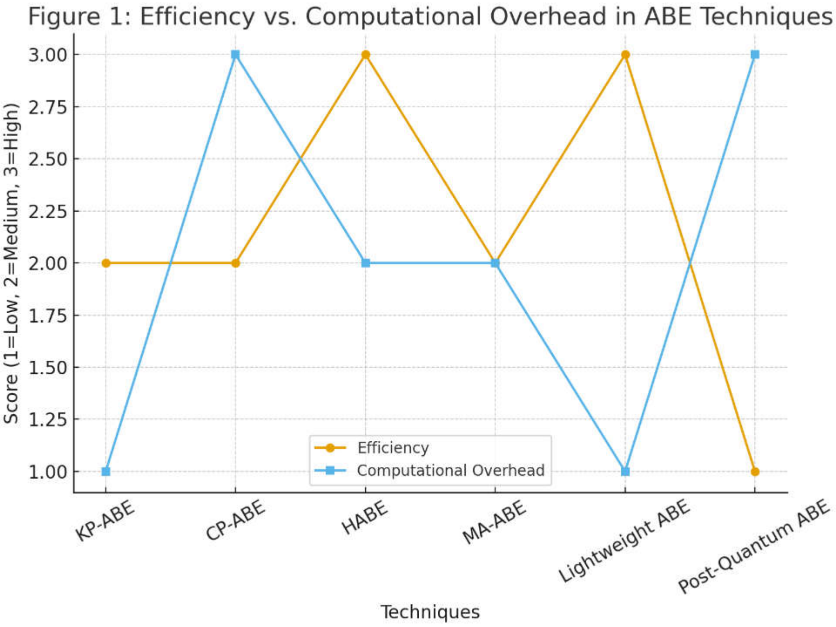
- CP-ABE remains dominant for fine-grained cloud data sharing but requires efficiency improvements [20], [18].
- KP-ABE is suited for hierarchical access structures but lacks owner-controlled policies [19], [3].
- HABE and MA-ABE address scalability and decentralization but introduce complexity in coordination [2], [5], [17].
- Lightweight and outsourced ABE are promising for IoT-cloud but depend on third-party trust models [6], [8], [11], [12].
- Post-quantum ABE is critical for long-term security but is currently less practical for deployment [9], [16].

Overall, no single scheme offers a complete solution. A hybrid approach—combining lightweight design [6], decentralized trust [5], efficient revocation [17], [18], and quantum resilience [9], [16]—appears to be the most promising future direction [13].

**Table 1: Comparative Analysis of Efficiency and Computational Overhead in ABE Techniques**

| Technique | Efficiency | Computational Overhead |
|---|---|---|
| KP-ABE | Medium | Low |
| CP-ABE | Medium | High |
| HABE | High | Medium |
| MA-ABE | Medium | Medium |
| Lightweight ABE | High | Low |

| Technique | Efficiency | Computational Overhead |
|---|---|---|
| Post-Quantum ABE | Low | High |



**graph (Figure 1)** showing their efficiency versus computational overhead.

## 4. CONCLUSION

Cloud computing continues to revolutionize data storage and service delivery but raises persistent concerns regarding security, privacy, and fine-grained access control. Attribute-Based Encryption (ABE) has emerged as a powerful cryptographic approach to address these issues by allowing data access to be governed by attributes and access policies.

From this survey, it is evident that different ABE variants offer unique strengths and limitations. **KP-ABE** provides flexibility for hierarchical structures but limits data owners' control. **CP-ABE** enables fine-grained access management but suffers from high computational overhead. **HABE** improves scalability by supporting hierarchical trust models, while **MA-ABE** eliminates single points of failure through decentralized authority. Emerging **lightweight ABE schemes** enhance efficiency for IoT-cloud integration, and **post-quantum ABE** offers future-proof resilience against quantum attacks, though practical deployment remains challenging.

The comparative analysis indicates that no single scheme fully addresses the diverse requirements of cloud environments. A promising direction lies in **hybrid approaches** that integrate efficiency, decentralized trust, scalability, revocation mechanisms, and quantum resistance. Additionally, blockchain-assisted ABE, outsourcing-based optimizations, and lattice-based cryptography are shaping the next generation of secure and privacy-preserving cloud systems.

In conclusion, ABE remains central to building trust in cloud computing. Continuous research toward lightweight, decentralized, and quantum-resistant models will be vital to ensure robust data security, user privacy, and scalable access control in future cloud ecosystems.

**Acknowledgments**

The authors are very grateful to their family and friends who were very supportive throughout the process.

**Conflict of Interest**

The authors declare no conflict of interest. None of the authors are affiliated with or have financial involvement in any organization or entity with direct financial involvement in the subject matter or materials of the research discussed in this manuscript.

**Ethical Approval**
Not Applicable

**Consent to Participate**
Not Applicable

**Consent to Publish**
Yes

**Data Availability Statement**
Not Applicable

**Authors Contributions:**
The authors reviewed and approved the final manuscript and share responsibility for its integrity and scholarly quality.

**Funding**
This Research was not funded in any manner either internally or externally by any agency.

**Competing Interests**
Nil

**References**

[1] S. Agrawal and M. Chase, "FAME: Fast Attribute-based Message Encryption," in *Proc. ACM SIGSAC Conf. Computer and Communications Security (CCS)*, 2017. Scholar GPSMicrosoft

[2] M. Ali, S. M. S. Hashemi, M. R. Aref, and M. Ahmadian, "Fully Distributed Hierarchical Attribute-Based Encryption with Constant-Size Ciphertexts," *IEEE Access*, vol. 8, pp. 206 540–206 560, 2020. ScienceDirect

[3] M. Asim, T. Ignatenko, M. Petković, D. Trivellato, and N. Zannone, "Enforcing Access Control in Virtual Organizations Using Hierarchical Attribute-Based Encryption," *arXiv:1205.5757*, 2012. arXiv

[4] M. Chegenizadeh, M. Ali, J. Mohajeri, and M. R. Aref, "HUAP: Practical Attribute-based Access Control Supporting Hidden Updatable Access Policies for Resource-Constrained Devices," *arXiv:2107.10133*, 2021. arXiv

[5] P. Datta, D. E. Kim, S. Han, J. Katz, and D. J. Wu, "Decentralized Multi-Authority Attribute-Based Inner-Product Functional Encryption," *Cryptology ePrint Archive: 2023/1113*, 2023. NTT Research, Inc.

[6] Z. Feng, L. Shuai, D. Su, S. Yang, and M. Li, "A Lightweight Ciphertext-Policy Attribute-Based Encryption Scheme for Cloud Storage," *arXiv:2307.00806*, 2023. arXiv

[7] V. Gorbunov, V. Vaikuntanathan, and H. Wee, "Attribute-Based Encryption for Circuits," in *Proc. ACM Symp. Theory of Computing (STOC)*, 2013. ResearchGate

[8] M. Green, S. Hohenberger, and B. Waters, "Outsourcing the Decryption of ABE Ciphertexts," in *Proc. USENIX Security Symp.*, 2011. USENIX

[9] C.-Y. Hsieh, B. Waters, and D. Wichs, "Attribute-Based Encryption from Lattices: From Theory to Practice," in *Proc. IEEE FOCS*, 2023. ACM Digital Library

[10] T. Jung, X.-Y. Li, Z. Wan, and M. Wan, "Control Cloud Data Access Privilege and Anonymity with Fully Anonymous Attribute-Based Encryption," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 1, pp. 190–204, 2015. staff.ustc.edu.cnAstrophysics Data System

[11] J. Li, Z. Guan, X. Du, Z. Zhang, and J. Wu, "An Efficient Encryption Scheme with Verifiable Outsourced Decryption in Mobile Cloud Computing," *arXiv:1810.10750*, 2018. arXiv

[12] R. Nakanishi, Y. Zhang, M. Sasabe, and S. Kasahara, "Combining IOTA and Attribute-Based Encryption for Access Control in the Internet of Things," *arXiv:2103.04016*, 2021. arXiv

[13] S. Panwar, N. Agarwal, A. Gupta, G. Guo, and H. Mahmood, "A Strong Privacy-Preserving Ciphertext-Policy Attribute-Based Encryption Scheme for Cloud-Based Electronic Health Record Systems," *Computer Standards & Interfaces*, vol. 96, 103789, 2024.

[14] S. Rani, G. Sainarayanan, S. A. Edalatpanah, and B. K. Paul, "Attribute-Based Encryption Schemes for Next Generation Wireless Networks: A Survey," *Sensors*, vol. 23, no. 11, 2023. PMC

[15] Z. Ren, R. Susilo, Y. Wang, J. Zhou, M. H. Au, and X. Dong, "A Secure and Efficient Blockchain-based CP-ABE Scheme for Data Sharing," *Journal of King Saud University – Computer and Information Sciences*, 2024 (early access). ScienceDirect

[16] D. Riepel and H. Wee, "FABEO: Fast Attribute-Based Encryption with Optimal Security," in *Proc. IEEE EuroS&P Workshops*, 2022; extended technical report, 2022. casa.rub.deSciSpace

[17] C. Wang, Z. Liu, Q. Xia, and B. Li, "Hierarchical Attribute-Based Encryption with Scalable Revocation," *Computers & Security*, vol. 30, no. 5, pp. 320–329, 2011. ACM Digital Library

[18] S. Xu, J. Yuan, G. Xu, Y. Li, X. Liu, Y. Zhang, and Z. Yang, "Efficient Ciphertext-Policy Attribute-Based Encryption with Black-Box Traceability," *Information Sciences*, vol. 538, pp. 19–38, 2020, doi:10.1016/j.ins.2020.05.115. InKScienceDirect

[19] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute-Based Data Sharing with Attribute Revocation," in *Proc. ACM ASIACCS*, pp. 261–270, 2010. DBLP

[20] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing," in *Proc. IEEE INFOCOM*, 2010. SCIRP

[21] A. B. Lewko and B. Waters, "Decentralizing Attribute-Based Encryption," in *Proc. EUROCRYPT*, pp. 568–588, 2011. IACR