Computer Systems
Science and Engineering

Tech Science Press

Doi:10.32604/csse.2025.072267

ARTICLE

Attribute-Based Encryption for Secure Access Control in Personal Health Records

Dakshnamoorthy Manivannan*

Department of Computer Science, University of Kentucky, Lexington, KY 40506, USA

*Corresponding Author: Dakshnamoorthy Manivannan. Email: manivann@cs.uky.edu

Received: 23 August 2025; Accepted: 29 October 2025; Published: 08 December 2025

ABSTRACT: Attribute-based Encryption (ABE) enhances the confidentiality of Electronic Health Records (EHR) (also known as Personal Health Records (PHR)) by binding access rights not to individual identities, but to user attribute sets such as roles, specialties, or certifications. This data-centric cryptographic paradigm enables highly fine-grained, policy-driven access control, minimizing the need for identity management and supporting scalable multi-user scenarios. This paper presents a comprehensive and critical survey of ABE schemes developed specifically for EHR/PHR systems over the past decade. It explores the evolution of these schemes, analyzing their design principles, strengths, limitations, and the level of granularity they offer in access control. The review also evaluates the security guarantees, efficiency, and practical applicability of these schemes in real-world healthcare environments. Furthermore, the paper outlines the current state of ABE as a mechanism for safeguarding EHR data and managing user access, while also identifying the key challenges that remain. Open issues such as scalability, revocation mechanisms, policy updates, and interoperability are discussed in detail, providing valuable insights for researchers and practitioners aiming to advance the secure management of health information systems.

KEYWORDS: Attribute-based encryption; attribute-based access control; data security; cloud security; privacy-preserving healthcare; IoMT security; blockchain-based access control

1 Introduction

As more sensitive data is shared and stored on third-party platforms, strong encryption is increasingly essential. Traditional encryption offers limited, coarse-grained access control–sharing data often means giving others full access via your private key. This lack of flexibility makes it hard to share specific information securely. Therefore, there's a growing need for advanced encryption methods that enable fine-grained access control, allowing users to share only selected data without compromising everything.

ABE [1,2] extends identity-based encryption [3,4], by using attributes, rather than identities, to control access to encrypted data. In ABE, users can decrypt data only if their attributes (e.g., role, department, clearance level) meet the conditions defined by the data owner. This enables flexible, fine-grained access control, making ABE ideal for cloud computing, Internet of Things (IoT), and distributed systems where access must be dynamic and role-based. ABE is especially effective for securely sharing data with many users while maintaining precise access control. There are two main types of ABE schemes, discussed below:

1.1 Ciphertext-Policy Attribute-Based Encryption (CP-ABE)

CP-ABE, introduced by Bethencourt et al. [1], enables fine-grained access control over encrypted data, even when storage servers are untrusted. CP-ABE resists collusion attacks, ensuring that users cannot collude to decrypt data unless their combined attributes meet the specified access policy. Unlike earlier ABE schemes, which embedded access policies in users' keys, CP-ABE assigns attributes to users and lets the data owner define the access policy during encryption. This design aligns more closely with traditional access control models like Role-Based Access Control (RBAC). Bethencourt et al. [1] also provided a working implementation and evaluated its performance, demonstrating CP-ABE's practicality for real-world, secure data sharing scenarios.

1.2 Key-Policy Attribute-Based Encryption (KP-ABE)

KP-ABE, introduced by Goyal et al. [2], enables fine-grained access control by encrypting data with a set of attributes and issuing users private keys tied to access structures. Unlike CP-ABE, where policies are embedded in ciphertexts, KP-ABE defines policies in the decryption keys. A key feature of KP-ABE is its support for hierarchical delegation of decryption rights. Inspired by Hierarchical Identity-Based Encryption (HIBE) [5,6], KP-ABE allows users to delegate subsets of their access privileges without contacting a central authority. This makes it ideal for scalable, layered access control systems that reflect real-world hierarchies, such as organizational roles or clearance levels. Only users whose access structures match the ciphertext's attributes can decrypt the data, ensuring secure and flexible policy enforcement.

1.3 Attribute-Based Signature (ABS) Scheme

Attribute-Based Signature (ABS) [7,8] schemes allow users to sign messages based on predicates over their attributes, issued by a trusted authority. Rather than verifying a signer's identity, ABS verifies that the signer possesses attributes satisfying the predicate. ABS ensures unforgeability—even colluding users cannot produce valid signatures for attributes they don't hold. At the same time, it preserves anonymity: valid signatures reveal nothing about the signer beyond the satisfied predicate. This makes ABS especially useful for privacy-preserving applications like anonymous credentials and fine-grained access control systems.

Goal of This Paper

EHRs are dynamic, interoperable, and structured digital systems that go well beyond traditional medical charts. They are integral to modern healthcare delivery—enabling real-time access, secure data sharing, improved quality of care, and operational efficiency. Their successful use hinges on functionality, usability, data standards adherence, and maintaining trust through robust privacy and security protections.

Over the past decade, a rich ecosystem of ABE variants has emerged for healthcare: CP-ABE, KP-ABE, and Multi-Authority ABE (MA-ABE), along with attribute-based signcryption (ABSC) and signature/multi-signature integration, aiming to deliver confidentiality, authenticity, and auditability simultaneously [9].

This paper presents a comprehensive and critical survey of ABE schemes developed specifically for EHR systems over the past decade. It explores the evolution of these schemes, analyzing their design principles, strengths, limitations, and the level of granularity they offer in access control. The review also evaluates the security guarantees, efficiency, and practical applicability of these schemes in real-world healthcare environments.

Furthermore, the paper outlines the current state of ABE as a mechanism for safeguarding EHR data and managing user access, while also identifying the key challenges that remain. Open issues such as scalability, revocation mechanisms, policy updates, and interoperability are discussed in detail, providing

valuable insights for researchers and practitioners aiming to advance the secure management of health information systems.

Justification for Our Survey

In this section, we review recent survey papers on ABE published over the past five years.

Rasori et al. [10] examine ABE schemes for IoT applications, focusing on three performance indicators: CPU efficiency, bandwidth efficiency for data producers, and bandwidth efficiency for key authorities. They evaluate representative schemes through simulations, concluding that while no scheme excels in all metrics, some perform well in two metrics simultaneously. Zhang et al. [11] provide a comprehensive taxonomy of ABE, classifying schemes into KP-ABE, CP-ABE, anti-quantum ABE, and generic constructions. CP-ABE is further divided into nine categories based on functionality, revocation, accountability, policy management, multi-authority settings, and computation models. Their survey systematically compares schemes by security and performance, offering a broader and more holistic assessment than prior works, and highlighting open research challenges.

Penuelas-Angulo et al. [12] focus on revocation in ABE schemes for fog-enabled IoT. They present a taxonomy of revocation methods, compare qualitative and quantitative costs, and discuss the unique challenges posed by fog environments compared to cloud-based IoT. Perazzo et al. [13] evaluate the performance of three representative ABE schemes on resource-constrained IoT devices (ESP32 and RE-Mote). Their results show that ABE can be practical under hardware acceleration with up to 10 attributes, and they propose a new benchmarking method demonstrating that worst-case assumptions in prior work overestimate energy and time costs.

Table 1 presents a comparison of the related surveys presented in the literature over the past five years on attributed-based encryption. As highlighted in Table 1, none of the above surveys address ABE and access control for managing EHRs. Our survey aims to fill this gap.

Table 1: Comparison of the survey papers on attribute-based encryption and access control

Authors (year)	Focus	Methodology	Key findings	Limitations
Rasori et al. [10] (2022)	ABE for IoT	Performance indicators (CPU, bandwidth); simulations	Some schemes perform well w.r.t two metrics but none excel in all	Limited to IoT
Zhang et al. [11]	Comprehensive taxonomy of ABE	Classification (KP-ABE, CP-ABE, anti-quantum, generic); 9 CP-ABE subcategories	Systematic comparison; holistic view; open challenges	Very broad, less focus on application-specific domains
Penuelas- Angulo et al. [12]	Revocation in ABE for fog-enabled IoT	Taxonomy of revocation; qualitative and quantitative comparison	Revocation methods evaluated; fog-specific issues discussed	Focused on fog-IoT
Perazzo et al. [13] (2020)	ABE performance on IoT devices	Experiments on ESP32 and RE-Mote; benchmarking	ABE feasible with hardware acceleration and ≤10 attributes	Only considers IoT
Our Survey (2025)	ABE for EHR management Literature review	First dedicated survey on ABE for EHRs; addresses access control challenges	Previous surveys overlooked healthcare-specific ABE	Healthcare/ EHRs

We conducted an extensive search for survey papers focused on ABE and access control mechanisms for managing EHRs. However, we did not find any comprehensive surveys published in reputable journals or conference proceedings from leading publishers such as IEEE, ACM, Elsevier, or Springer. This indicates

a significant gap in the existing literature, despite the increasing relevance of secure and privacy-preserving data sharing in modern healthcare systems.

Moreover, we observed that substantial research interest in applying ABE and advanced access control techniques to EHR systems has emerged only within the past five years. This growing attention reflects the rapid integration of technologies such as cloud computing, Internet of Medical Things (IoMT), and blockchain into healthcare, all of which necessitate robust access control solutions.

Given this context, our survey aims to fill this critical gap by providing a timely and comprehensive review of recent advancements in ABE-based access control for EHRs. We believe it will serve as a valuable resource for researchers, practitioners, and system designers working in the areas of health informatics, cybersecurity, and privacy-preserving data sharing.

Organization of the Paper

The rest of the paper is organized as follows. Section 2 classifies and presents a critical review of the ABE-based encryption and access-control mechanisms for EHRs, presented in the literature over the past ten years. Section 3 highlights open challenges and unresolved research gaps. Section 4 concludes the paper.

2 Research Works on Attribute-Based Encryption and Access Control for EHRs/PHRs/IoMT Criteria Used for Selecting Papers

We selected high-quality papers published in leading peer-reviewed journals and top-tier conferences, primarily from reputable publishers such as IEEE, ACM, Elsevier, Springer, Tech Science Press, and other outlets recognized for their rigorous editorial and review standards. The inclusion criteria emphasized originality, technical depth, and relevance to Attribute-Based Encryption (ABE) in the context of secure storage and access of Electronic Health Records (EHRs). Particular attention was given to papers that introduced novel ABE schemes, enhanced existing frameworks, or addressed practical challenges such as efficiency, scalability, revocation, interoperability, and privacy preservation. Both theoretical contributions and experimental evaluations were considered, ensuring a balanced representation of foundational research and applied work. By curating this body of literature, we provide a reliable and comprehensive reference point for researchers, practitioners, and policymakers seeking to understand current advances and open challenges in applying ABE to healthcare data management. We used the keywords attribute-based encryption, medical records, IoMT, EHR, PHR to find published in the last years. We found that there has been increased interest in this area during the last five years.

Under ABE, data is encrypted under a policy (e.g., Role=Cardiologist $\wedge$ Hospital=A $\wedge$ Consent=TRUE) and only holders of keys bearing the required attributes can decrypt. Enhancements—such as policy hiding, proxy re-encryption for revocation/updates, and outsourced decryption at fog/edge nodes—improve privacy and performance. On the other hand blockchain provides a tamper-evident log for auditing, consent management, and access governance. Smart contracts codify consent rules, log access attempts, and orchestrate key/attribute updates. Together, blockchain and ABE form a strong foundation for access control over EHR/PHR data. In the following subsection, we survey research that combines blockchain with ABE-based access control for EHRs/PHRs.

2.1 Research Works Using Blockchain and Attribute-Based Encryption and Access Control for EHRs/PHRs

Jiang et al. [14] propose CEC-ABE, an attribute-based encryption scheme for protecting EHRs in edge-cloud environments by integrating blockchain with ABE. In this framework, the patient-hospital agreement is established before the ABE process, and treatment details (e.g., time, physician, and additional notes) are securely transmitted using encryption. Encrypted EHRs are stored on the blockchain as transaction records,

ensuring integrity and traceability. Access control is enforced through outsourced ciphertext-policy ABE, with fine-grained attribute revocation for enhanced security. Experimental evaluations comparing CEC-ABE with CP-ABE and other algorithms show that CEC-ABE achieves notable improvements in key generation, outsourced decryption, and overall efficiency, reducing computational overhead by 1.73% and 5.2% compared with the next-best scheme. Overall, CEC-ABE demonstrates superior comprehensive performance.

PHRs offer patients a platform for storing and sharing critical medical information. However, they are accompanied by notable security risks, including data leakage, unauthorized access, and potential tampering. Traditional solutions, such as ABE and blockchain technologies, address these issues only partially, leaving unresolved challenges like single points of failure and ensuring fair keyword searches. To tackle these challenges, Zhang et al. [15] propose a distributed PHR-sharing scheme that combines blockchain technology with CP-ABE for secure and efficient encryption. The blockchain component ensures data integrity and traceability by recording all operations as transactions, while the nodes play the role of attribute authorities within the CP-ABE framework. Malicious nodes can be traced using cryptographic algorithms, and fair ciphertext retrieval is facilitated through smart contracts. Additionally, the scheme employs both on-chain and off-chain storage to mitigate the storage limitations inherent to blockchain technology. Security analyses demonstrate resilience against indistinguishable chosen plain-text (IND-CPA) and keyword attacks (IND-CKA), highlighting the feasibility and efficiency of the proposed scheme.

Liu et al. [16] propose a blockchain-based framework for PHR sharing that enables reliable search and traceability. A hybrid scheme, BC-SPSC (Blockchain-backed Searchable Proxy Signcryption), is introduced, using identity-based proxy signatures (IBPS) to authorize doctors on behalf of patients, ensuring authentic patient-centric control and traceable data linkage. BC-SPSC supports two search modes: (1) attribute-based encryption with keyword-based search (SABE), allowing all authorized users to search, but only those meeting access policies to decrypt; and (2) attribute-based searchable encryption (ABSE), enabling fine-grained control over who can search and access data. Simulations show BC-SPSC offers strong performance with reduced storage and computation overhead.

He et al. [17] introduce a fine-grained access control scheme tailored for identity resolution and Prognostics and Health Management (PHM) systems. Their approach combines a unique identifier encoding technique with attribute-based encryption, allowing for dynamic data categorization and permission control suited to industrial environments. To address threats such as unauthorized access and identity misuse, they incorporate blockchain technology to trace malicious activity while maintaining user privacy. The scheme's security is formally verified under the decisional bilinear Diffie-Hellman (DBDH) assumption. Experimental comparisons show that their solution outperforms existing methods in terms of computation time and storage efficiency.

Fugkeaw et al. [18] proposed a blockchain-based access control scheme for outsourced IoT-enabled EHRs in a fog-assisted cloud environment. It ensures secure, fine-grained access control and efficient, scalable user revocation using pseudo-random encryption, symmetric encryption, CP-ABE, and graph-based modeling. Fog computing offloads heavy CP-ABE operations, while an adaptive load sharing algorithm optimizes task distribution across fog nodes. Blockchain is used for user authentication and EHR integrity verification. Security and performance evaluations show that encryption/decryption costs are comparable to existing methods, and the proposed ciphertext retrieval mechanism improves re-encryption efficiency after user revocation.

Wu et al. [19] note that existing searchable encryption schemes for EHRs lack fine-grained access control with wildcards, do not hide access policies, and may yield incomplete search results due to untrusted cloud servers. To address this, they propose a blockchain-aided attribute-based searchable scheme using inner

product predicates. This approach enables wildcard-based fine-grained access, fully hidden policies to preserve privacy, and blockchain-backed integrity verification for complete and reliable multi-keyword searches. Security proofs and performance evaluations confirm the scheme's effectiveness and privacy guarantees.

Qiao et al. [20] propose LCBS, a lightweight CP-ABE scheme for cloud-based EHR systems that integrates blockchain and secure multi-party computation. The scheme introduces a multi-authority model and uses secure multi-party computation for decentralized system initialization without disrupting other operations. A tailored blockchain records user key information, enabling key verification across multiple stages and preventing unauthorized EHR access. The scheme also supports efficient attribute updates with minimal computation. Formal security analysis and simulations demonstrate strong data security and improved performance.

Thushara et al. [21] propose a blockchain-based framework integrating Ciphertext-Policy Attribute-Based Signcryption (CP-ABSC) for secure fog-enabled IoMT data sharing. The fog layer is split into two: the child layer handles secure, unforgeable data sharing via signcryption, while the parent layer manages load balancing and uses Erasure Encoding Techniques (EET) to enhance latency and storage efficiency. Blockchain ensures data integrity and authenticity. The system defends against attacks targeting data confidentiality and unforgeability, relying on Elliptic Curve Computational Diffie-Hellman (ECCDH) and Elliptic Curve Decisional Diffie-Hellman (ECDDH) hard problems. Experimental results show strong security and efficiency for resource-constrained IoMT applications.

A thematic comparison of the research works using Blockchain-ABE Schemes, discussed in this subsection, is presented in Table 2. This table captures the comparative strengths and weaknesses of the various works discussed in this subsection:

Revocation is explicitly supported in Jiang et al. [14], Fugkeaw et al. [18], and Qiao et al. [20]. Others either rely on indirect mechanisms (e.g., node tracing in Zhang et al. [15], authorization via proxy signcryption in Liu et al. [16]) or leave revocation unaddressed. Revocation remains a challenge, with only a few works offering strong solutions.

Table 2: Thematic comparison of the research works based on blockchain and attribute-based encryption

Work	Efficiency	Scalability	Revocation support	Privacy-preservation	Distinctive features
Jiang et al. [14] (2022)	Improves key generation and uses outsourced decryption	Edge–cloud integration enhances performance	Fine-grained attribute revocation supported	Blockchain ensures integrity and traceability; encrypted treatment info	Patient-hospital agreement before ABE; blockchain for traceable EHRs
Zhang et al. [15] (2022)	On-/off-chain storage balances efficiency & storage costs	Distributed architecture avoids single points of failure	Malicious node tracing, but no fine-grained revocation	Fair search & integrity via blockchain and smart contracts	Blockchain nodes act as attribute authorities; fair ciphertext retrieval
Liu et al. [16] (2023)	Reduced storage & computation; two search modes (SABE, ABSE)	Hybrid model supports reliable, large-scale PHR sharing	Proxy signcryption offers authorization, but no explicit revocation	Strong privacy with patient-centric control & traceability	Identity-based proxy signcryption (IBPS); dual search modes
He et al. [17] (2024)	Outperforms others in computation & storage efficiency	Blockchain integration allows traceability across industrial systems	No explicit revocation, focused on identity misuse detection	Privacy preserved via identifier encoding & hidden policies	Identifier encoding for dynamic access; tailored to PHM systems

(Continued)

Table 2 (continued)

Work	Efficiency	Scalability	Revocation support	Privacy-preservation	Distinctive features
Fugkeaw et al. [18] (2024)	Comparable encryption/ decryption costs; efficient ciphertext retrieval	Fog nodes and adaptive load sharing improve scalability	Efficient, scalable revocation using graph based modeling	Blockchain ensures authentication & integrity verification	Fog-assisted CP-ABE; adaptive load sharing; graph-based revocation
Wu et al. [19] (2024)	Efficient multi-keyword search with wildcards	Blockchain backed search ensure completeness	No explicit revocation	Wildcard-based fine-grained access; hidden policies	Inner product predicates; wildcard-based access control
Qiao et al. [20] (2025)	Lightweight; efficient attribute updates; strong performance	Multi-authority model enhances scalability	Efficient attribute update & key verification across blockchain	Privacy ensured via secure multi-party computation	Multi-authority with secure MPC; blockchain for key verification
Thushara et al. [21]	Strong efficiency with CP-ABSC; fog-layer load balancing improves latency	Dual fog-layer design with erasure encoding improves scalability	No explicit revocation focus	Strong confidentiality & authenticity; resistant to unforgeability attacks	Fog-layer split (child: signcryption, parent: load balancing and EET)

Scalability is achieved primarily through distributed or layered architectures and mitigate single points of failure. Examples include multi-authority frameworks (Qiao et al. [20]), fog-enabled designs (Fugkeaw et al. [18], Thushara et al. [21]), and blockchain decentralization (Zhang et al. [15] and He et al. [17]).

Privacy-preservation is consistently prioritized, often reinforced with advanced features like hidden policies, wildcard searches, and multi-party computation, but Wu et al. [19] stand out for wildcards and hidden policies, while Liu et al. [16] emphasize patient-centric traceability. Blockchain-based traceability with confidentiality is supported in (Jiang et al. [14], Zhang et al. [15] and He et al. [17]).

Efficiency improvements are claimed in all, but with different emphases (fog computing, outsourced decryption, lightweight designs, or load balancing). Common techniques used include outsourced decryption (Jiang et al. [14]), lightweight designs (Qiao et al. [20]), and load balancing/fog offloading (Fugkeaw et al. [18], Thushara et al. [21]). Efficiency is usually measured via simulations comparing against CP-ABE baselines.

Heatmap of Thematic Support in Blockchain-ABE Schemes discussed in this subsection is shown in Fig. 1.

2.2 Research Works on Attribute-Based Encryption and Access Control for EHRs/PHRs with Fog/IoMT Integration

Modern medical systems increasingly rely on IoMT devices, enhancing remote healthcare and contributing significantly to PHRs, which now include data from both IoT devices and medical professionals. Secure and private sharing of PHRs can improve diagnostic accuracy, but IoMT systems must balance strong security (e.g., secure access, anomaly detection, and network segmentation) with clinical usability. ABE plays a key role by enabling fine-grained access control and ensuring data confidentiality in IoMT environments.

EHRs, meanwhile, are comprehensive digital records containing a patient's complete medical history, shared securely across healthcare settings. EHRs integrate diverse data sources and use standards like HL7 and FHIR to ensure interoperability across systems. Since IoMT devices contribute to maintaining and

enriching EHRs, ABE-based access control in IoMT is critical. This subsection reviews recent ABE-based approaches in the IoMT context.

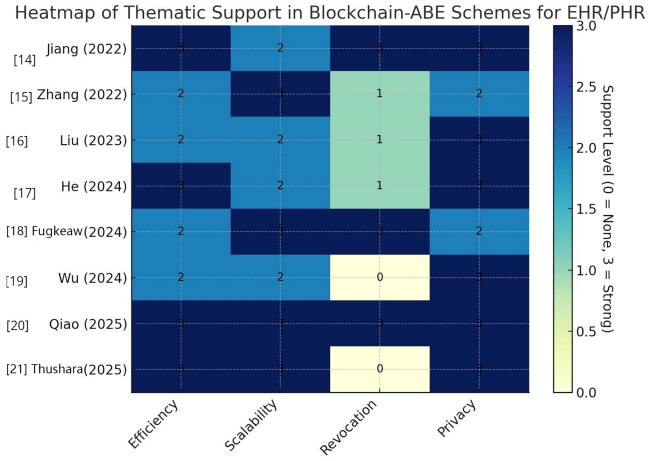

Figure 1: Heatmap of thematic support in Blockchain-ABE schemes [14–21]

Fog computing's ability to reduce data transfer requirements and latency is increasingly favored for applications demanding secure, fine-grained access control. CP-ABE is well-suited for fog-enabled applications; however, conventional CP-ABE faces challenges regarding effective access revocation. Zhao et al. [22] address this with an efficient CP-ABE scheme called AC-FEH, designed specifically for fog-based E-health systems. This scheme delegates encryption and decryption tasks to fog nodes, significantly alleviating computational burdens on users. Proven selectively secure based on the q-parallel Bilinear Diffie-Hellman Exponent (BDHE) problem, AC-FEH achieves lower computational costs than competing CP-ABE-based access control systems.

Zeng et al. [23] have introduced an efficient ABE scheme known as PTIoMT, which incorporates partially hidden access policies. This innovative approach only displays non-sensitive attribute labels, thereby enhancing privacy. Additionally, PTIoMT is scalable, accommodating an unlimited number of attributes without compromising system performance. It also includes public traceability features to detect key misuse, making it a more secure option for managing sensitive medical data. Notably, the scheme reduces the number of bilinear pairing operations required in the decryption process, contributing to enhanced efficiency. Comprehensive security and performance analyses substantiate PTIoMT's effectiveness for practical applications within the IoMT landscape, marking a significant step forward in the integration of advanced security measures in modern healthcare systems.

Cloud-assisted IoMT represents an emerging paradigm in the healthcare sector, involving the collection, storage, and utilization of medical data. Given the need for confidentiality and accessibility in outsourced data, secure and fine-grained data sharing is critical in ensuring patient protection. Although ABE offers a promising solution to this problem, the challenge of flexibly and efficiently updating access privileges for specific users without impacting others remains significant. Hao et al. [24] propose a secure and fine-grained data-sharing scheme with flexible user privilege updates designed for cloud-assisted IoMT environments. By building upon ABE, they incorporate proxy re-encryption and key blinding techniques to enable cloud servers to efficiently re-encrypt ciphertexts impacted by revocation while also updating keys for authorized users. Additionally, user attributes can be added, extending access rights without the need for reissuing keys. This design empowers patients to efficiently manage data sharing and access privileges. Both formal proofs and performance evaluations substantiate the security and efficacy of this approach.

Bao et al. [25] propose a lightweight attribute-based searchable encryption (LABSE) scheme for Cloud-assisted IoMT that provides fine-grained access control and keyword search capabilities on encrypted data; it also maintains low computational overhead for resource-constrained devices. Their rigorous proofs of semantic security complement experimental comparisons, showcasing LABSE's advantages over existing methods.

Wang et al. [26] propose an Efficient and Auditable Privacy-preserving Data Sharing (EAPDS) scheme tailored for the IoMT, leveraging a MA-ABE model. EAPDS introduces an auditable anonymous authentication mechanism that ensures strong identity privacy protection, preventing unauthorized tracking or profiling of users. At the same time, it incorporates an optimized MA-ABE approach to enable secure, scalable, and efficient data sharing among multiple entities in the healthcare ecosystem. The scheme is rigorously evaluated through formal security analysis, which confirms its resistance to replayable chosen-ciphertext attacks—an important consideration for safeguarding sensitive medical data. Extensive experimental results and functional evaluations further highlight EAPDS's superior performance compared to existing medical data-sharing methods, particularly in terms of efficiency, privacy preservation, and real-world applicability. Given these strengths, EAPDS presents a highly promising solution for secure and practical data sharing in IoMT environments. Thushara et al. [21] discussed in the previous subsection, also proposed blockchain-based framework integrating CP-ABSC for secure fog-enabled IoMT data sharing.

Table 3 presents a thematic comparison of the research works based on attribute-based Encryption and access control for EHRs/PHRs with fog/IoMT integration, discussed in this subsection.

Table 3: Thematic comparison of the research works based on attribute-based encryption and access control for EHRs/PHRs with fog/IoMT integration

Work	Efficiency	Scalability	Revocation support	Privacy preservation	Distinctive features
Zhao et al. [22] (2021)	Delegates heavy encryption/ decryption tasks to fog nodes	Effective in fog-enabled E-health but not explicitly designed for unbounded attributes	Supports efficient revocation through fog delegation mechanisms	Basic privacy protection via secure CP-ABE model	Fog-assisted CP-ABE tailored for E-health; significantly lowers latency and computation at user side
Zeng et al. [23] (2021)	Uses fewer bilinear pairings in decryption which means high efficiency	Supports unlimited attributes without loss of performance	Public traceability enables detection of misuse rather than direct revocation	Partially hidden policies conceal sensitive attribute labels	Partially hidden access policies & public traceability for IoMT security
Hao et al. [24] (2022)	Cloud-assisted IoMT, Proxy re-encryption and key blinding reduce overhead for updates	Supports adding attributes and extending rights flexibly in cloud	Flexible privilege updates: ciphertext re-encryption and key updates without reissuing all keys	Maintains confidentiality with fine-grained access control in cloud IoMT	Dynamic privilege management: efficient user addition/removal with patient-controlled sharing

(Continued)

Table 3 (continued)

Work	Efficiency	Scalability	Revocation support	Privacy preservation	Distinctive features
Bao et al. [25] (2022)	Lightweight; minimal computational overhead; efficient searchable encryption	Designed for cloud-assisted IoMT, adaptable to constrained devices	No explicit revocation mechanism highlighted	Ensures data confidentiality with secure keyword search	Combines ABE with searchable encryption; fine-grained access control
Wang et al. [26] (2025)	Optimized MA-ABE ensures efficiency; experimentally validated superior to existing schemes	Multi-authority structure supports scalability across large healthcare ecosystems	Implicit revocation handling via MA-ABE; not primary focus	Strong privacy with anonymous authentication and resistance to profiling and replayable CCA	Supports auditable anonymous authentication and multi-authority ABE for secure IoMT data sharing

Key observations and trends based on these works are:

Efficiency: All schemes aim to reduce computational costs, with Zhao et al. [22] offloading to fog nodes, Zeng et al. [23] using fewer bilinear pairings, Hao et al. [24] using proxy re-encryption, and Bao et al. [25] offering lightweight searchable encryption. Wang et al. [26] extend efficiency through optimized MA-ABE and experimental validation.

Scalability: PTIoMT, by Zeng et al. [23], stands out with unlimited attribute support. Wang et al. [26] MA-ABE also scales well in multi-entity IoMT ecosystems.

Revocation Support: Hao et al. [24] provide the most flexible and fine-grained revocation mechanism. Zhao et al. [22] address revocation efficiency via fog delegation. Zeng et al. [23] focus on traceability instead of direct revocation.

Privacy-Preservation: Wang et al. [26] achieve the strongest privacy guarantees with anonymous authentication. Zeng et al. [23] enhance privacy by hiding sensitive attributes. Others preserve confidentiality mainly through ABE mechanisms.

Distinctive Features: Zhao et al. [22] use Fog-assisted ABE for latency-sensitive E-health. Zeng et al. [23] support partial policy hiding and misuse traceability. Hao et al. [24] support dynamic privilege updates and patient empowerment. Bao et al. [25] support lightweight searchable encryption for IoMT. Wang et al. [26] support auditable, anonymous, multi-authority model with strong attack resistance.

Heatmap of Thematic Support in Fog/IoMT Integrated Schemes, discussed in this subsection, is shown in Fig. 2.

Clinical roles and relationships change constantly—clinicians rotate departments, residents graduate, vendors off-board—so previously issued keys must be invalidated immediately. Lost devices, phishing, or insider misuse likewise demand rapid termination of decryption capability. Patients may withdraw consent, and Health Insurance Portability and Accountability Act (HIPAA) and General Data Protection Regulation (GDPR) require timely restriction with auditable control. Because encrypted records are replicated across cloud and edge caches, revocation is the only way to prevent future decryptions of those copies. Robust revocation must ensure forward security (revoked users cannot decrypt new ciphertexts) and, where required, backward security (they also cannot decrypt prior ciphertexts, typically via key or ciphertext updates). Therefore, revocation is fundamental to ABE-based access control. In the next subsection, we survey schemes that focus on revocation.

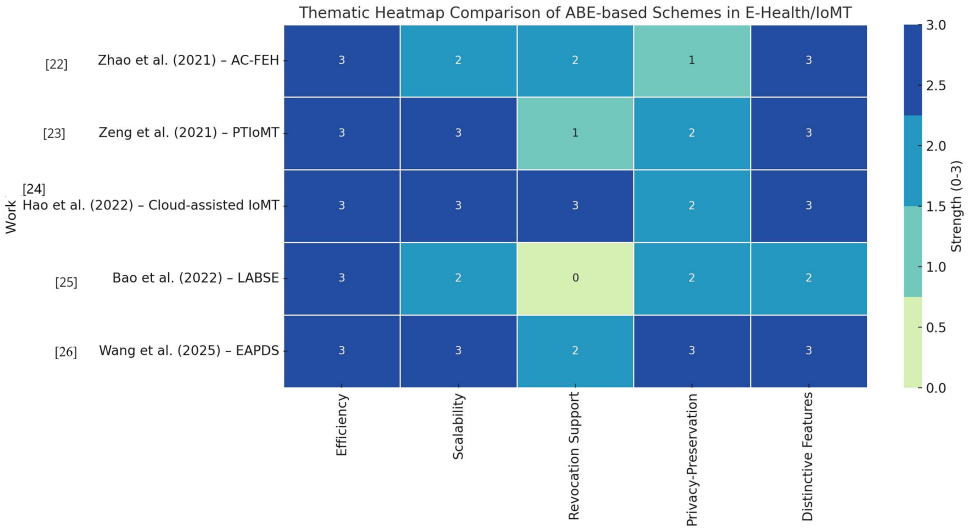

Figure 2: Heatmap of thematic support in Fog/IoMT integrated schemes [22–26]

2.3 Research Works on Attribute-Based Encryption and Access Control for EHRs/PHRs That Focus on Revocation Schemes

Wei et al. [27] introduce a revocable-storage hierarchical ABE (RS-HABE) scheme for storing PHRs in the cloud that enhances security through features like user revocation, secret key delegation, and ciphertext updates. The RS-HABE scheme ensures both forward and backward security, demonstrating selective security under bilinear group assumptions while achieving superior functionality and computational efficiency. Experimental results validate its practicality for real-world applications.

Zhang et al. [28] present an efficient attribute-based data sharing scheme for IoMT that supports policy hiding and dynamic policy updating. A key feature of the proposed scheme is its support for user revocation, effectively mitigating the risk of collusion between revoked users, non-revoked users, or the cloud service provider. In their design, attributes are separated into attribute names and attribute values, with only the sensitive attribute values being concealed within the access policies to enhance user privacy. This granularity enables more flexible and secure access control without compromising system usability. To reduce the computational burden on users—particularly those with resource-constrained IoMT devices—the scheme incorporates outsourcing techniques for encryption and decryption, as well as efficient policy update mechanisms. Importantly, the authors formally prove that their scheme achieves full security, which provides stronger guarantees than most existing solutions in this domain. Comprehensive comparisons and simulation results demonstrate that the proposed approach outperforms existing schemes in terms of efficiency, scalability, and privacy preservation, making it especially well-suited for secure and practical data sharing in IoMT environments.

Table 4 presents a thematic comparison of research works discussed in this subsection whose main focus is revocation. Key observations and trends based on these works are:

Table 4: Thematic comparison of the research works whose main focus is revocatio

Work	Efficiency	Scalability	Revocation support	Privacy preservation	Distinctive features
Wei et al. [27] (2021)	Achieves computational efficiency via hierarchical structure; validated experimentally for practical use	Hierarchical design supports large-scale cloud-based EHR storage	Supports strong revocation with ciphertext updates; ensures both forward & backward security	Provides confidentiality under bilinear group assumptions; privacy not the primary emphasis	Revocable-Storage Hierarchical ABE with secret key delegation and support for forward/backward security for EHRs
Zhang et al. [28] (2024)	Outsourced encryption/ decryption reduces device burden; simulation results confirm superior efficiency	Scales well for IoMT through dynamic policy updates and outsourcing	Strong revocation mechanism mitigating collusion risks involving revoked users and non-revoked users/ cloud	Policy hiding: conceals sensitive attribute values while keeping attribute names visible	Supports policy hiding and dynamic policy updates; full security proof; highly suitable for resource-constrained IoMT

Efficiency: Wei et al. [27] focus on computational efficiency for cloud-based hierarchical EHR storage whereas Zhang et al. [28] improve efficiency for IoMT devices through outsourcing encryption/decryption tasks.

Scalability: Wei et al. [27] hierarchical structure scales well in cloud storage settings. Zhang et al. [28] ensure scalability in IoMT by allowing dynamic policy updating and lightweight operations.

Revocation Support: Wei et al. [27] provide forward and backward security with ciphertext updates, a strong form of revocation while Zhang et al. [28] emphasize revocation with anti-collusion properties, preventing revoked users from exploiting cooperation with others.

Privacy-Preservation: Wei et al. [27] primarily emphasize access security, with privacy as a secondary effect. Zhang et al. [28] explicitly integrate policy hiding, keeping sensitive values private while allowing flexible enforcement.

Distinctive Features: Wei et al. [27] design revocable-storage hierarchical ABE with secret key delegation and dual-direction security. Zhang et al. [28] support policy hiding and dynamic updating with full security proofs and outsourcing support for IoMT.

2.4 Research Works on Attribute-Based Encryption and Access Control for EHRs/PHRs That Focus on Fine-Grained Access Policies and Privacy-Aware Access Policies/Control

Fine-grained access policies enable: (i) Least privilege: only what's needed (e.g., labs—not psychotherapy notes). (ii) Context awareness: encode role, purpose, time window, location (e.g., "treating cardiologist, current admission, last 32 h"). (iii) Lifecycle agility: smoother onboarding/offboarding and targeted revocation. (iv) Compliance and audit: clean mapping to HIPAA/GDPR with transparent trails. (v) Privacy-aware control and consent: enforce patient preferences; support granular withdrawal that actually blocks decryption.

Bottom line: Fine-grained, privacy-aware controls deliver only the necessary information to the right party at the right time—improving safety, usability, and compliance. ABE without policy/attribute privacy can still leak metadata; privacy-aware designs close this gap for real EHR/PHR sharing across cloud/edge, multi-institution, and audited settings. In this subsection, we review papers focused on fine-grained access policies and privacy-aware access policies/controls.

Seol et al. [29] introduced a cloud-based EHR model that utilizes ABAC to significantly enhance security and privacy in the management of patient records. Their approach employs the Extensible Access Control

Markup Language (XACML) to establish and enforce fine-grained access policies tailored to the attributes of the requester. This ensures that only authorized individuals can access sensitive medical information, thereby strengthening the confidentiality of patient data.

A pivotal aspect of this model is its emphasis on security during the transmission of patient data. When a patient's document is dispatched to a requester, the system employs partial encryption, ensuring that only the relevant sections of the record are accessible, rather than the entire document. This method of selective encryption effectively minimizes the exposure of unnecessary information while safeguarding the privacy of patients.

In addition to encryption, the model incorporates electronic signatures to authenticate both the sender and the document, thereby providing assurance that the data has not been altered during transmission. To implement these robust security measures, the authors utilize XML encryption and XML digital signature technology, which are recognized standards for securing data in web services. These technologies facilitate the secure transmission and authentication of medical records across cloud platforms, thereby bolstering the overall integrity and confidentiality of electronic health records. Through this innovative framework, Seol et al. [29] address critical challenges in health information security, illustrating the potential of cloud-based solutions in protecting patient privacy.

Despite its ability to provide fine-grained access control, traditional CP-ABE is unsuitable for smart-health (s-health) environments for the following reasons: (i) access policies are exposed in clear text, which may compromise sensitive health information, and (ii) CP-ABE typically accommodates a limited attribute universe, making it impractical due to the increased size of public parameters.

To tackle the above challenges, Zhang et al. [30] introduce the privacy-aware s-health (PASH) access control system. PASH incorporates a large-universe CP-ABE framework with partially concealed access policies, which obscures sensitive attribute values in encrypted smart health records (SHRs) while only revealing attribute names. Since attribute values are typically more critical than names, this design significantly enhances privacy. Additionally, PASH features an efficient decryption test that requires few bilinear pairings, supports a broad attribute universe, and maintains constant public parameter sizes. Security analyses indicate PASH's robustness, and performance evaluations demonstrate it to be more efficient and versatile than prior models. Zhang et al. [31] also developed a CP-ABE scheme with efficient decryption tailored for protecting healthcare records, ensuring constant public parameter size and low decryption costs. This scheme achieves full security based on standard model assumptions while utilizing dual system encryption.

Large-scale EHRs are frequently outsourced to Cloud Service Providers (CSPs), which raises significant privacy concerns due to the risk of unauthorized access. To address these issues, Liu et al. [32] propose an anonymous EHR sharing scheme that employs decentralized hierarchical ABE to enhance privacy and facilitate secure sharing. Their methodology incorporates multiple attribute authorities to enable fine-grained and scalable access control, alongside the use of hierarchical access trees to optimize encryption processes. The implementation of a global identifier (GID) effectively mitigates the risk of user collusion, while an anonymous key mechanism ensures that attribute authorities cannot profile users. Furthermore, a double verification process is employed to maintain EHR integrity. Efficiency analyses validate the scheme's security and practicality, demonstrating its reliability under the decisional DBDH assumption.

Existing ABE schemes for multi-user collaboration overlook user weight differences, leading to redundant attributes and reduced efficiency. To address this, Li et al. [33] introduce RVWABE-CA—a revocable, verifiable, and weighted ABE scheme with collaborative access–for secure and efficient sharing of EHRs in public cloud environments. It features a weighted access tree to eliminate redundant attributes, and uses encryption versioning for user revocation. It uses a Merkle Hash Tree for data integrity verification. The

scheme is proven secure against chosen plain-text attacks and achieves higher computational efficiency than related approaches without added storage or communication overhead.

Zhang et al. [34] identify a significant limitation in most existing Attribute-Based Encryption with Keyword Search (ABKS) schemes: they typically expose access policies, which can inadvertently leak sensitive information. To address this vulnerability, the authors propose a novel and efficient ABKS scheme that conceals access policies while preserving system functionality. Their approach offers several key advantages:

Fine-grained access control: Data owners can precisely specify access permissions, enabling only authorized users to retrieve and search encrypted PHRs.

Policy privacy: The access structures embedded in the encryption process remain hidden, thereby protecting the underlying sensitive criteria used for access control.

Scalable performance: The proposed scheme is designed to be efficient, with both storage overhead and computational complexity not increasing linearly with the number of attributes, making it suitable for large-scale applications.

The security of their scheme is rigorously analyzed under standard cryptographic assumptions, specifically relying on the truncated q-Decisional Bilinear Diffie-Hellman Exponent (q-DBDHE) and Decisional Diffie-Hellman (DDH) hardness assumptions. To demonstrate practical viability, the authors conduct extensive simulations, showing that their method achieves strong performance and security guarantees in realistic settings.

Lu et al. [35] propose zk-AHSNARK, an efficient zero-knowledge proof protocol by combining linear secret sharing scheme (LSSS) and zero-knowledge succinct non-interactive argument of knowledge (zkSNARK) to verify user attributes while preserving their privacy. Building on this, they introduce a PHR sharing scheme that protects attribute information, secures data using interplanetary file system (IPFS), and enables fast keyword-based search through a smart contract. These contracts also ensure trustworthy execution. Simulations confirm the scheme's security and practical viability.

Kapil et al. [36] present an encryption framework designed to protect large-scale healthcare data stored in the cloud. They implement a ciphertext-policy attribute-based honey encryption (CP-ABHE) algorithm to ensure fine-grained access control and robust security for sensitive medical records. Initially, password protection strengthens system security, followed by the generation of honey-words—decoy passwords—to defend against unauthorized access attempts.

Attribute-based proxy re-encryption (ABPRE) enables dynamic, fine-grained access control for encrypted EHRs, but many existing schemes face key limitations: fixed attribute universes, privacy leaks in verification, and access policies that expose sensitive patient information. To address these issues, Zhao et al. [37] propose a large-universe, verifiable, and privacy-preserving ABPRE scheme for e-health clouds. Their approach supports an unbounded attribute universe (no need to predefine attributes), uses non-interactive zero-knowledge proofs for public verification without leaking EHR data, and employs partially hidden policies–revealing attribute names while hiding their values–to protect patient privacy. Experiments show the scheme offers enhanced functionality with minimal computational overhead.

Tables 5 and 6 present a thematic comparison of the research works on attribute-based encryption and access control for EHRs/PHRs that focus on fine-grained access policies and privacy-aware access policies/control, discussed in this subsection. Key observations and trends based on these works are:

Table 5: Thematic comparison of the research works on attribute-based encryption and access control for EHRs/PHRs that focus on fine-grained access policies and privacy-aware access policies/control

Work	Efficiency	Scalability	Revocation Support	Privacy preservation	Distinctive features
Seol et al. [29] (2018)	Selective encryption reduces unnecessary computation; XML encryption & signatures improve security	Suitable for cloud-based EHR but not focused on large-scale system	No explicit revocation mechanism	Selective encryption and digital signatures protect confidentiality & integrity	ABAC with XACML enforcement; XML-based encryption & signature for secure transmission
Zhang et al. [30] (2018)	Efficient decryption test with few pairings; constant-size public parameters	Large-universe CP-ABE supports wide attribute sets	Limited revocation (not primary focus)	Partially hidden policies (hide values, reveal names)	Privacy-aware s-health access control with strong efficiency & flexibility
Zhang et al. [31] (2019)	Constant-size public parameters, low decryption costs via dual system encryption	Supports broad attribute universe	Not revocation-oriented	Full security proofs to show confidentiality	CP-ABE scheme optimized for healthcare with efficient decryption
Liu et al. [32] (2020)	Hierarchical ABE reduces computation; double verification ensures integrity	Decentralized and multiple authorities enhance scalability	Collusion resistance via GID; revocation not primary but partially handled	Anonymous keys prevent profiling; privacy protection through decentralization	Decentralized hierarchical ABE with multi-authority control & global identifiers
Li et al. [33] (2024)	Weighted access tree eliminates redundancy; higher computational efficiency	Cloud-suitable with collaborative access	Version- based revocation via encryption updates	Integrity verified through Merkle Hash Tree	Revocable, verifiable, weighted ABE with collaborative sharing

Table 6: Thematic comparison of the research works on attribute-based encryption and access control for EHRs/PHRs that focus on fine-grained access policies and privacy-aware access policies/control continued

Work	Efficiency	Scalability	Revocation support	Privacy preservation	Distinctive features
Zhang et al. [34] (2024)	Efficient keyword search with ABE; storage & computation overhead does not grow linearly	Designed for large-scale health data search	Revocation not focus; supports fine-grained control	Hidden policies prevent leakage of access criteria	Attribute-based keyword search with concealed policies under q-DBDHE & DDH
Lu et al. [35] (2024)	Provide fast attribute verification; IPFS + contracts ensure efficiency	Scalable via blockchain & IPFS storage	Revocation not central but contract-based rules can adapt	Strong privacy: ZK proofs hide attributes, IPFS prevents data leaks	Combines with LSSS for attribute verification; IPFS storage and smart contracts with keyword search

(Continued)

Table 6 (continued)

Work	Efficiency	Scalability	Revocation support	Privacy preservation	Distinctive features
Kapil et al. [36] (2025)	Honey encryption adds negligible overhead to CP-ABE	Supports cloud-scale EHRs	Revocation not addressed	Honeywords & decoy passwords provide privacy/security	Ciphertext-policy honey encryption with password-hardening with honeywords defense
Zhao et al. [37]	Large-universe design avoids redefinition overhead; lightweight zero-knowledge verification	Unlimited attribute scalability	Flexible revocation via proxy re-encryption	Partially hidden policies and NIZK proofs protect sensitive values	Large-universe verifiable ABPRE with policy hiding and public verifiability

Efficiency: Some schemes focus on reducing decryption costs (Zhang et al. [30], Zhang et al. [31]), or introducing lightweight verification (Zhao et al. [37]). Others add selective encryption (Seol et al. [29]) or honey encryption (Kapil et al. [36]) for stronger but still efficient protection.

Scalability: Liu et al. [32] and Zhao et al. [37] stand out with decentralized/large-universe approaches. Zhang et al. [30], Zhang et al. [31] and Li et al. [33] ensure broader attribute support without efficiency loss.

Revocation Support: Li et al. [33] provide explicit version-based revocation. Liu et al. [32] use GIDs for collusion-resistance. Zhao et al. [37] enable dynamic revocation through proxy re-encryption. Others have limited or no revocation mechanisms.

Privacy-Preservation: Zhang et al. [30] and Zhang et al. [31] support strong privacy with policy hiding, Liu et al. [32], Lu et al. [35] and Zhao et al. [37] also provide support for strong privacy preservation. Seol et al. [29] ensure privacy via selective encryption and signatures.

Distinctive Features: Seol et al. [29] use XML-based ABAC for secure transmission. Zhang et al. [30] and Zhang et al. [31] support efficient decryption and policy hiding. Liu et al. [32] use a decentralized, multi-authority model with anonymity. Li et al. [33] use Weighted access tree and supports verifiability of results. Zhang et al. [34] support keyword search on ABE with hidden policies. Lu et al. [35] support zkSNARK-based verification and uses IPFS and contracts. Kapil et al. [36] use honey encryption with honeywords. Zhao et al. [37] support large-universe attributes and public verifiability. Heatmap visualization of the comparative table for the nine works discussed in this section is shown in Heatmap visualization of the thematic comparison of papers discussed in this subsection is shown in Fig. 3.

Tables 7 and 8 present a concise summary of the research works reviewed in this paper, categorizing them based on the type of ABE employed and the architectural approach adopted–centralized or distributed. For each reviewed scheme, we specify the application domain it is best suited for and outline its main characteristics.

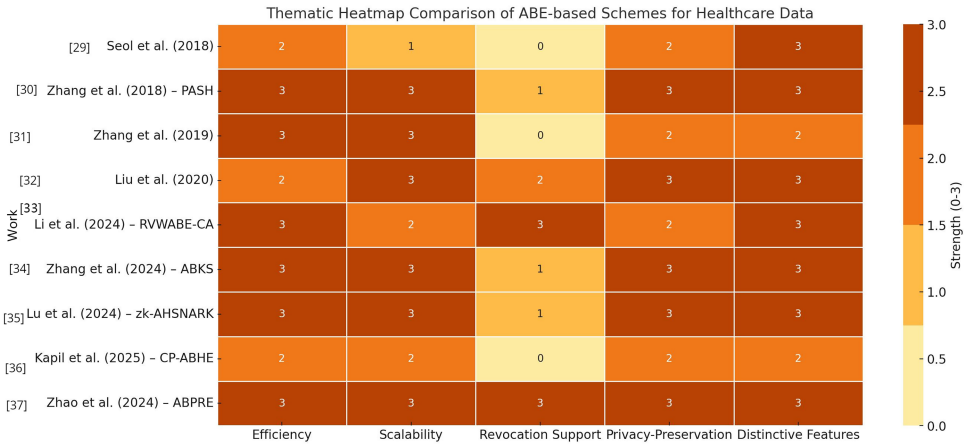

Figure 3: Heatmap of thematic support for fine-grained access control and privacy [29–37]

Table 7: Classification of the papers discussed based on the encryption techniques used and their application area

ABE technique used	Paper and year	Application area/properties
CP-ABE	Zhang et al. [30], 2018	Cloud-Smart-health/Supports partially concealed access policies to enhance privacy and uses fewer bilinear pairings for decryption test, and supports a broad attribute universe
CP-ABE	Jiang et al. [14], 2022	Edge-EHR/A secure EHR sharing scheme based on blockchain and CP-ABE, ensuring integrity and traceability
CP-ABE	Zhang et al. [15], 2022	Cloud-PHR/A distributed PHR-sharing scheme based on blockchain and CP-ABE that supports malicious node tracking, data integrity
CP-ABE	Fugkeaw et al. [18], 2024	IoT-Enabled-EHR-Fog-Cloud/Supports fine-grained access control and efficient, scalable user revocation using pseudo-random encryption, symmetric encryption, CP-ABE, and graph-based modeling
CP-ABE	Kapil et al. [36], 2025	Cloud-PHR/Supports fine-grained access control, and uses decoy passwords to defend against unauthorized access attempts
CP-ABE	Qiao et al. [20], 2025	Cloud-EHR/Supports efficient attribute updates with little overhead, blockchain used for key verification across multiple stages to prevent unauthorized EHR access
CP-ABE	Thushara et al. [21], 2025	Cloud-IoMT/Supports fog-enabled IoMT data sharing, fog layer is used for secure data sharing and load balancing, blockchain is used to ensure data integrity and authenticity
Hierarchical/ multi-party ABE	Liu et al. [32], 2020	Cloud-EHR/Supports fine-grained and scalable privacy-preserving access control, prevents collusion, double verification used to ensure integrity of data

(Continued)

Table 7 (continued)

ABE technique used	Paper and year	Application area/properties
Hierarchical/ multi-party ABE	XLi et al. [33], 2024	Cloud-EHR/Present a revocable, verifiable, and weighted ABE scheme with collaborative access, and uses weighted access tree and Merkle hash tree in their design
Centralized ABE	Seol et al. [29], 2018	Cloud-EHR/Enhanced security and privacy, uses XACML to establish and enforce fine-grained access policies, and uses electronic signatures to authenticate both the sender and the document
Centralized ABE	Hao et al. [24], 2022	Cloud-IoMT/A fine-grained data-sharing scheme that supports flexible user privilege updates, incorporates proxy re-encryption and key blinding techniques to efficiently re-encrypt ciphertexts impacted by revocation

Table 8: Classification of the papers discussed based on the encryption techniques used and their application area continued

ABE technique used	Paper and year	Application area/properties
Centralized ABE	Liu et al. [16], 2023	Cloud-EHR/Enables reliable keyword search and traceability, it allows all authorized users to search, but allows only those meeting access policies to decrypt and enables fine-grained control over who can search and access data
Centralized ABE	He et al. [17], 2024	Cloud-PHR/Uses identifier encoding and ABE for permission control and blockchain technology for tracing malicious activity
Centralized ABE	Zhang et al. [28], 2024	Cloud-IoMT/Supports policy hiding and dynamic policy updating, efficient user revocation and prevents collusion attack of revoked users
Centralized ABE	Lu et al. [35], 2024	IPFS-PHR/Using IPFS for storing data, zkSNARK is used to verify user attributes while preserving their privacy, enables fast keyword-based search through smart contracts.
Centralized ABE	Zhao et al. [37], 2024	Cloud-EHR/Supports a large attribute universe and hence is scalable, verifiable, uses privacy-preserving AB proxy re-encryption scheme and uses partially hidden policies to preserve privacy
Multi-authority ABE	Wang et al. [26], 2025	Cloud-IoMT/Supports auditable authentication, prevents unauthorized tracking and supports scalable, efficient data sharing among multiple entities in the healthcare domain
Searchable ABE	Bao et al. [25], 2022	Cloud-IoMT/Supports fine-grained and privacy-preserving access control and keyword search, and is scalable

(Continued)

Table 8 (continued)

ABE technique used	Paper and year	Application area/properties
Searchable ABE	Zhang et al. [34], 2024	Cloud-PHR/Conceals access policies, supports fine-grained access control and is efficient, with respect to both storage overhead and computational complexity
Searchable ABE	Wu et al. [19], 2024	Cloud-EHR/Uses blockchain-aided AB searchable scheme using inner product predicates, supports fine-grained access control and ensures privacy of users using fully hidden policies, and supports reliable multi-keyword searches

3 Open Issues

In this section, we summarize some of the open issues related to designing ABE-Based Access Control methods for storing and accessing Personal Health Records.

- **Fine-Grained Access Control:** Designing access policies that are both expressive and efficient for various healthcare roles and scenarios remains a significant challenge. Advanced policies often demand the creation, management, and processing of increasingly large ciphertexts and keys in ABE systems. This results in greater overhead for encryption, decryption, and key management. Such growing complexity can severely affect the system's efficiency and scalability, especially in resource-constrained environments with limited processing power, memory, or bandwidth. While some progress has been made in addressing these issues [14,17,24,28,29,32,34,36], further research is essential to develop scalable, fine-grained access control mechanisms with minimal overhead.
- **Efficient User and Attribute Revocation:** Efficiently supporting user and attribute revocation in EHR systems-without requiring re-encryption of existing data or extensive key redistribution-presents a significant challenge. In dynamic healthcare environments, where users' roles and access privileges frequently change due to personnel shifts or policy updates, traditional ABE schemes often incur substantial computational and communication overhead during revocation. Re-encrypting large volumes of historical medical data or frequently updating and redistributing keys can severely impact system performance, usability, and scalability. Several approaches have been proposed to address these issues [14,18,22,27,28], including proxy re-encryption, key encapsulation mechanisms, and time-based attributes. However, these solutions still face limitations in terms of efficiency, scalability, and real-time applicability in large-scale EHR systems. Therefore, further research is necessary to design revocation mechanisms that are both secure and lightweight, enabling fine-grained access control without the need to re-encrypt existing data.
- **User-Friendly Policy Management:** Simplifying the creation and management of access policies for non-expert users—such as patients and healthcare providers—remains a significant challenge. Designing ABE schemes for EHR systems requires balancing the expressiveness and dynamism of access policies with the demands for efficiency, scalability, and usability. However, many ABE schemes that use plain-text policy representations risk leaking sensitive information about users' roles or attributes, thus compromising privacy. Several studies [17,23,26,28–30,32,34] have addressed this concern by designing mechanisms that prevent users from inferring private information about others based on their attributes.

These approaches offer varying levels of privacy protection, but challenges remain in achieving strong, formal guarantees of attribute confidentiality.

- **Interoperability with Healthcare Standards:** The integration of ABE with healthcare data standards such as Health Level Seven (HL7)—a set of international protocols for exchanging electronic health information—and Fast Healthcare Interoperability Resources (FHIR)—a modern standard designed to enable interoperability across heterogeneous EHR systems—remains an open and largely under-explored research area. Effective incorporation of ABE into these widely adopted standards is essential for ensuring secure and fine-grained access control in practical healthcare environments, yet current efforts have not sufficiently addressed this challenge.

Following are some insights into addressing compliance with regulations and clinical workflow integration

Fine-grained attribute control on FHIR resources: ABE can enforce attribute-based policies (e.g., Cardiologist ∧ Hospital ∧ A Patient Consent=TRUE) over encrypted FHIR resources, letting patients or hospitals define decryption rights without exposing policies. FHIR metadata (roles, consent, encounter type, location) maps naturally to attributes—for instance, a lab report (observation) encrypted with Role=Oncologist, Institution=Hospital B, Consent=Yes. Since FHIR is Application Programming Interface (API)-driven, ciphertexts remain portable across EHR systems, with enforcement handled cryptographically. Blockchain integration can add immutable access logs, aligning with FHIR's AuditEvent.

Compliance with with HIPAA (US), GDPR (EU) regulations: HIPAA requires confidentiality, integrity, and availability of Protected Health Information (PHI). ABE enforces minimum necessary access (e.g., only a treating physician can decrypt) and supports patient-driven control, aligning with HIPAA's consent and disclosure requirements. GDPR emphasizes data minimization and purpose limitation; ABE with policy hiding prevents leaking sensitive details. While revocation is challenging, proxy re-encryption and versioning (Hao et al. [24] and Li et al. [33]) enable dynamic updates.

Interoperability with compliance frameworks: FHIR Consent resources can directly generate ABE policies—for example, revoking consent can trigger policy re-encryption and exclude revoked attributes.

Clinical Workflow Integration: ABE must balance security with usability. Clinician roles from EHR logins can be mapped to attribute keys via Identity and access management (IAM) systems. Emergency access can be enabled through time-limited delegated keys with audit trails. Performance demands outsourced/fog-assisted decryption so clinicians get near-instant record access. Cross-institutional care is supported as ABE enforces policies cryptographically across FHIR APIs without requiring central trust.

- **Auditing and Accountability:** Enabling secure, tamper-proof logging of data access events—without compromising user privacy—is a critical yet challenging requirement in healthcare systems. Without the support of sophisticated, and often computationally expensive, traitor tracing mechanisms, it becomes difficult to accurately identify the source of a data breach or unauthorized access. In the absence of effective tracking and auditing systems, detecting and mitigating key misuse or leakage may be delayed or unreliable, thereby weakening the security guarantees of the encryption scheme and complicating incident response and accountability.
- **Decentralized Key Management:** Eliminating reliance on a single trusted authority; supporting multi-authority or blockchain-based trust models. Some research has explored the use of multi-authority ABE systems [26,32,38] to manage user attributes more securely and distribute trust. However, further investigation is needed to develop efficient, privacy-preserving auditing and accountability mechanisms that can operate in large-scale, dynamic healthcare environments.

Standardization Efforts for Internet Engineering Task Force (IETF), International Standards Organizations (ISO) and Others: Following are some standardization efforts for ABE-based EHR systems that are still nascent and fragmented, since most ABE work remains at the research or prototype stage. However, there are several directions where standardization (or steps toward it) is happening. There have been discussions in IETF research groups (e.g., Crypto Forum Research Group (CFRG)) about post-quantum and advanced cryptographic primitives. ABE is not yet standardized but proposals exist to define interoperable ciphertext and key formats for CP-ABE an KP-ABE. HL7 and FHIR are Widely used for EHR interoperability. Researchers are working on integrating ABE with FHIR APIs for fine-grained attribute-based access policies. While not an official standard, ABE is proposed as a privacy-preserving mechanism to complement existing FHIR security modules. Some proposals are trying to combine cryptographic enforcement (ABE) with policy standards (HL7 ABAC models) for healthcare.

Attribute-Based Encryption offers a powerful foundation for fine-grained access control in EHR systems, but its practical deployment faces several critical challenges. These include performance overhead, security under complex threat models, scalability to large user bases, limited usability for non-experts, and integration difficulties with existing infrastructure. ABE schemes often suffer from computational inefficiencies, and adapting them to real-world healthcare environments requires not only cryptographic innovation but also advancements in systems design and user-friendly implementation.

4 Conclusion

In this paper, we presented a comprehensive survey of recent research in the field of attribute-based encryption and access control for managing Electronic Health Records. Our review systematically covers the key advancements, design approaches, cryptographic techniques, and practical implementations proposed to ensure secure, fine-grained, and privacy-preserving access to EHRs in cloud and IoMT-based healthcare environments.

By examining the strengths, limitations, and emerging trends in the existing literature, we aim to provide researchers with a clear understanding of the current state of the art, identify open challenges, and highlight promising directions for future work. Given the increasing adoption of digital healthcare systems and the growing need for robust data protection, we believe this survey will serve as a timely and valuable reference for academics, developers, and security professionals working in the intersecting domains of health informatics, cryptography, and access control.

Acknowledgement: Not applicable.

Funding Statement: The author received no specific funding for this study.

Availability of Data and Materials: This article does not involve data availability, and this section is not applicable.

Ethics Approval: Not applicable.

Conflicts of Interest: The author declares no conflicts of interest to report regarding the present study.

References

1. Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption. In: Proceedings of 2007 IEEE Symposium on Security and Privacy (SP '07). Berkeley, CA, USA; 2007 May 20–23. p. 321–34.
2. Goyal V, Pandey O, Sahai A, Waters B. Attribute-based encryption for fine-grained access control of encrypted data. In: Proceedings of 13th Computer and Communications Security Conference. New York, NY, USA: ACM; 2006. p. 89–98.

3. Shamir A. Identity-based cryptosystems and signature schemes. Adv Cryptol. 1985;196:47–53. doi:10.1007/3-540-39568-7_5.
4. Boneh D, Franklin M. Identity-based encryption from the weil pairing. SIAM J Comput. 2003;32(3):586–615. doi:10.1137/s0097539701398521.
5. Gentry C, Silverberg A. Hierarchical ID-based cryptography. In: Zheng Y, editor. Advances in Cryptology—ASIACRYPT 2002. Berlin/Heidelberg, Germany: Springer; 2002. p. 548–66.
6. Horwitz J, Lynn B. Toward hierarchical identity-based encryption. In: International Conference on the Theory and Applications of Cryptographic Techniques. Cham, Switzerland: Springer; 2002. p. 466–81.
7. Maji HK, Prabhakaran M, Rosulek M. Attribute-based signatures. In: Kiayias A, editor. Topics in Cryptology–CT-RSA 2011. Berlin/Heidelberg, Germany: Springer; 2011. p. 376–92.
8. Li J, Au MH, Susilo W, Xie D, Ren K. Attribute-based signature and its applications. In: Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security (ASIACCS '10). New York, NY, USA: ACM; 2010. p. 60–9.
9. Ming Y, Zhang T. Efficient privacy-preserving access control scheme in electronic health records system. Sensors. 2018;18(10):3520. doi:10.3390/s18103520.
10. Rasori M, Manna MLa, Perazzo P, Dini G. A survey on attribute-based encryption schemes suitable for the internet of things. IEEE Internet Things J. 2022;9(11):8269–90. doi:10.1109/jiot.2022.3154039.
11. Zhang Y, Deng RH, Xu S, Sun J, Li Q, Zheng D. Attribute-based encryption for cloud computing access control: a survey. ACM Comput Surv. 2020;53(4):83. doi:10.1145/3398036.
12. Peñuelas-Angulo A, Feregrino-Uribe C, Morales-Sandoval M. Revocation in attribute-based encryption for fog-enabled internet of things: a systematic survey. Internet Things. 2023;23(4):100827. doi:10.1016/j.iot.2023.100827.
13. Perazzo P, Righetti F, Manna MLa, Vallati C. Performance evaluation of attribute-based encryption on constrained IoT devices. Comput Commun. 2021;170:151–63. doi:10.1016/j.comcom.2021.02.012.
14. Jiang Y, Xu X, Xiao F. Attribute-based encryption with blockchain protection scheme for electronic health records. IEEE Trans Netw Serv Manag. 2022;19(4):3884–95. doi:10.1109/tnsm.2022.3193707.
15. Zhang L, Zhang T, Wu Q, Mu Y, Rezaeibagha F. Secure decentralized attribute-based sharing of personal health records with blockchain. IEEE Internet Things J. 2022;9(14):12482–96. doi:10.1109/jiot.2021.3137240.
16. Liu S, Chen L, Wu G, Wang H, Yu H. Blockchain-backed searchable proxy signcryption for cloud personal health records. IEEE Trans Serv Comput. 2023;16(5):3210–23. doi:10.1109/tsc.2023.3272770.
17. He Y, Yan Z, Yuan T. Attribute-based access control scheme for secure identity resolution in prognostics and health management. IEEE Internet Things J. 2024;11(13):23140–55. doi:10.1109/jiot.2024.3387079.
18. Fugkeaw S, Prasad Gupta R, Worapaluk K. Secure and fine-grained access control with optimized revocation for outsourced IoT EHRs with adaptive load-sharing in fog-assisted cloud environment. IEEE Access. 2024;12:82753–68. doi:10.1109/access.2024.3412754.
19. Wu Z, Wang H, Wan J, Zhang L, Huang J. An inner product predicate-based medical data-sharing and privacy protection system. IEEE Access. 2024;12(2):68680–96. doi:10.1109/access.2024.3400611.
20. Qiao J, Wang N, Fu J, Deng L, Wang J, Liu J. A lightweight CP-ABE scheme for EHR over cloud based on blockchain and secure multi-party computation. Trans Emerg Telecomm Technol. 2025;36(2):e70053. doi:10.1002/ett.70053.
21. Thushara GA, Bhanu SMS. A blockchain-assisted attribute-based signcryption for secure sharing of medical IoT data in fog environment. Secur Priv. 2025;8(3):e70034. doi:10.1002/spy2.70034.
22. Zhao J, Zeng P, Choo K-KR. An efficient access control scheme with outsourcing and attribute revocation for fog-enabled e-health. IEEE Access. 2021;9:13789–99. doi:10.1109/access.2020.3025140.
23. Zeng P, Zhang Z, Lu R, Choo K-KR. Efficient policy-hiding and large universe attribute-based encryption with public traceability for internet of medical things. IEEE Internet Things J. 2021;8(13):10963–72. doi:10.1109/jiot.2021.3051362.
24. Hao J, Tang W, Huang C, Liu J, Wang H, Xian M. Secure data sharing with flexible user access privilege update in cloud-assisted IoMT. IEEE Trans Emerg Top Comput. 2022;10(2):933–47. doi:10.1109/tetc.2021.3052377.
25. Bao Y, Qiu W, Cheng X. Secure and lightweight fine-grained searchable data sharing for IoT-oriented and cloud-assisted smart healthcare system. IEEE Internet Things J. 2022;9(4):2513–26. doi:10.1109/jiot.2021.3063846.

26. Wang H, Xie Y, Luo M, Liu Y, Shirazi SH. EAPDS: efficient auditable and privacy-preservation data sharing scheme based on attribute-based encryption for IoMT. IEEE Internet Things J. 2025;12(14):26844–54. doi:10.1109/jiot.2025.3562541.
27. Wei J, Chen X, Huang X, Hu X, Susilo W. RS-HABE: revocable-storage and hierarchical attribute-based access scheme for secure sharing of e-Health records in public cloud. IEEE Trans Dependable Secure Comput. 2021;18(5):2301–15. doi:10.1109/tdsc.2019.2947920.
28. Zhang L, Xie S, Wu Q, Rezaeibagha F. Enhanced secure attribute-based dynamic data sharing scheme with efficient access policy hiding and policy updating for IoMT. IEEE Internet Things J. 2024;11(16):27435–47. doi:10.1109/jiot.2024.3399734.
29. Seol K, Kim Y-G, Lee E, Seo Y-D, Baik D-K. Privacy-preserving attribute-based access control model for XML-based electronic health record system. IEEE Access. 2018;6:9114–28. doi:10.1109/access.2018.2800288.
30. Zhang Y, Zheng D, Deng RH. Security and privacy in smart health: efficient policy-hiding attribute-based access control. IEEE Internet Things J. 2018;5(3):2130–45. doi:10.1109/jiot.2018.2825289.
31. Zhang L, Hu G, Mu Y, Rezaeibagha F. Hidden ciphertext policy attribute-based encryption with fast decryption for personal health record system. IEEE Access. 2019;7:33202–13. doi:10.1109/access.2019.2902040.
32. Liu X, Yang X, Luo Y, Wang L, Zhang Q. Anonymous electronic health record sharing scheme based on decentralized hierarchical attribute-based encryption in cloud environment. IEEE Access. 2020;8:200180–93. doi:10.1109/access.2020.3035468.
33. Li X, Wang H, Ma S. Revocable and verifiable weighted attribute-based encryption with collaborative access for electronic health record in cloud. Cybersecurity. 2024;7(1):18. doi:10.1186/s42400-024-00211-1.
34. Zhang B, Yang W, Zhang F, Ning J. Efficient attribute-based searchable encryption with policy hiding over personal health records. IEEE Trans Dependable Secure Comput. 2025;22(2):1299–312. doi:10.1109/tdsc.2024.3432769.
35. Lu C, Yu Z, Wang G, Dong A, Tian X. A blockchain-based PHR sharing scheme with attribute privacy protection. In: Proceedings of 2024 IEEE 23rd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom); 2024 Dec 17–21; Sanya, China. p. 2068–77.
36. Kapil G, Kumar N, Mourya AK, Kumar V. Securing big healthcare data using attribute and honey-based encryption in cloud environment. Supercomputing. 2025;81(1):181. doi:10.1007/s11227-024-06535-6.
37. Zhao J, Zhang K, Gong J, Qian H. Lavida: large-universe, verifiable, and dynamic fine-grained access control for E-health cloud. IEEE Trans Inf Forensics Secur. 2024;19:2732–45. doi:10.1109/tifs.2024.3350925.
38. Li M, Yu S, Zheng Y, Ren K, Lou W. Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. IEEE Trans Parallel Distrib Syst. 2013;24(1):131–43. doi:10.1109/tpds.2012.97.