Journal of
Cyber Security

Tech Science Press

Doi:10.32604/jcs.2025.072810

REVIEW

Attribute-Based Encryption Methods That Support Searchable Encryption

Daskshnamoorthy Manivannan*

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

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

Received: 04 September 2025; Accepted: 30 October 2025; Published: 28 November 2025

ABSTRACT: Attribute-Based Encryption (ABE) secures data by linking decryption rights to user attributes rather than user identities, enabling fine-grained access control. While ABE is effective for enforcing access policies, integrating it with Searchable Encryption (SE)—which allows searching encrypted data without decryption—remains a complex challenge. This paper presents a comprehensive survey of ABE schemes that support SE proposed over the past decade. It critically analyzes their strengths, limitations, and access control capabilities. The survey offers insights into the security, efficiency, and practical applicability of these schemes, outlines the current landscape of ABE-integrated SE, and identifies key challenges and open research problems that need to be addressed for broader adoption in real-world systems.

KEYWORDS: Attribute-based encryption; attribute-based access control; searchable encryption; data security; cloud security

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.

Attribute-Based Encryption (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, 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.

Pairing-based cryptography (PBC) is a branch of modern cryptography that constructs cryptographic schemes using bilinear pairings (also called bilinear maps). The book by Boneh and Shoup [9], which is available online, provides an excellent introduction to PBC. In addition, the seminal papers by Boneh and Franklin [4] and by Boneh et al. [10] are highly recommended for understanding its foundational concepts. PBC has been widely applied in the development of identity-based encryption schemes, attribute-based encryption, short signatures, and other cryptographic primitives. Lattice-based cryptography (LBC) is a branch of public-key cryptography that relies on the computational hardness of mathematical problems defined on lattices. Peikert [11] provides a comprehensive survey of LBC, while the seminal work by Ajtai [12] is essential for understanding the origins of lattice-based cryptography. LBC is believed to be resistant to attacks by quantum computers, making it a promising candidate for post-quantum cryptography.

1.4 Motivation for This Survey

In recent years, particularly over the last five years, there has been a notable surge in research centered on attribute-based searchable encryption (ABSE). This growing body of work underscores the increasing significance of ABSE as a security primitive in modern and evolving data protection frameworks, especially in cloud computing, big data systems, and privacy-preserving information retrieval. The ability of ABSE to support fine-grained, attribute-driven access control while enabling efficient search functionality makes it highly relevant for emerging applications.

Despite this progress, to the best of our knowledge, there is no dedicated and systematic survey published by leading venues such as IEEE, ACM, Elsevier, or Springer that thoroughly examines ABSE schemes. Existing reviews on related cryptographic techniques either overlook ABSE entirely or address it only in passing, leaving researchers without a consolidated reference point.

This gap serves as the primary motivation for our work. We aim to provide a comprehensive, structured, and up-to-date survey of ABSE research. Our study not only synthesizes and organizes the literature but also highlights recurring design patterns, emerging trends, unresolved challenges, and open research directions. In doing so, this survey seeks to serve as a valuable resource for both researchers and practitioners, offering clarity on the current state of ABSE and guiding future innovation in this domain.

Organization of the Paper

The rest of the paper is organized as follows. In Section 2, we present a critical overview of research works on attribute-based encryption and access control mechanisms that support searchable encryption, presented in the literature primarily over the last ten years. In Section 3, we discuss the open issues. Section 4 discusses the related surveys and also presents justification for this survey. Section 5 concludes the paper.

Criteria Used for Selecting Papers

To ensure a comprehensive and high-quality literature review, we selected research papers from leading peer-reviewed journals and top international conferences published by reputable sources such as IEEE, ACM, Elsevier, and Springer. These venues are known for their rigorous standards and significant contributions to computer science and information security. The curated literature serves as a valuable resource for researchers and practitioners working on ABE schemes in IoT environments.

2 Research Works That Support Searching Data Encrypted Using ABE

Searchable Encryption (SE) is a critical cryptographic technology that enables users to perform search operations over encrypted data without decrypting it. This capability is particularly important in cloud computing environments, where data confidentiality must be preserved even when leveraging third-party storage providers. SE allows cloud service providers to retrieve specific encrypted files on behalf of users based on search queries, all while maintaining the privacy and integrity of the underlying data.

Despite its benefits, Searchable Encryption faces several significant challenges. These include ensuring fine-grained data ownership and access control, enabling secure and privacy-preserving data deduplication, and preventing unauthorized access during the search and retrieval process. Addressing these challenges is essential for the practical and secure deployment of SE in real-world applications. ABE is a promising approach for enhancing SE by enabling flexible, policy-based access control and supporting complex query functionalities over encrypted data.

In this section, we review recent research and developments in attribute-based searchable encryption (ABSE), categorizing them according to their applicability in general cloud environments, healthcare systems, Fog/Edge-Computing Environments, and Internet of Things. A dedicated subsection is allocated to research contributions that integrate blockchain technology. Within the literature, varying terminologies are employed: some studies adopt the term Searchable ABE, while others utilize Attribute-Based Searchable Encryption (ABSE). Although the majority of these schemes provide support exclusively for keyword search, certain works explicitly emphasize this restriction by employing the term Attribute-Based Keyword Search (ABKS). In order to preserve the integrity of the original contributions, we adhere to the terminologies used by the respective authors when discussing their approaches.

2.1 Research Works That Support Attribute-Based Searchable Encryption for Cloud Environments

Li et al. [13] introduce KSF-OABE, an extension of the outsourced attribute-based encryption (OABE) framework, introduced earlier, that incorporates keyword search functionality to it. The scheme is proven to be secure under chosen-plaintext attacks. In this model, the cloud servers are responsible for performing partial decryption on behalf of the data user, yet gains no knowledge of the underlying plaintext. Additionally, the Cloud Service Provider (CSP) is capable of executing search operations over encrypted data without learning the keywords contained in the search trapdoor. The scheme proposed by Zheng et al. [14] was one of the first searchable encryption schemes based on CP-ABE for cloud environments.

Symmetric Searchable Encryption (SSE) is a specialized form of searchable encryption that leverages symmetric key cryptography to enable efficient and privacy-preserving searches over encrypted data. In SSE schemes, the same secret key is used both to encrypt the data and to generate secure search tokens, allowing users to retrieve relevant encrypted records without revealing the content of either the data or the search queries. The hybrid protocol proposed by Michalas et al. [15] combines the strengths of both Symmetric Searchable Encryption (SSE) and CP-ABE. This approach is designed to harness the performance and efficiency of SSE for search operations, while integrating the fine-grained access control capabilities of CP-ABE for secure key distribution and policy enforcement. By combining these two cryptographic primitives, the protocol provides a robust solution that supports efficient search functionality alongside scalable and secure access management.

The Verifiable Multi-Keyword Searchable Attribute-Based Encryption (VMKS-ABE) scheme for cloud storage presented by Wang et al. [16], mitigates the inherent limitation of many SABE schemes that only support single-keyword search. Their approach enables users to search using multiple keywords while maintaining search privacy—the cloud server can execute the search using a trapdoor but gains no knowledge of the actual keywords. To improve efficiency, the scheme offloads intensive computations to a cloud proxy server, significantly reducing the resource load on user devices. Additionally, it includes a mechanism to verify the correctness of outsourced private keys, ensuring integrity in key management. Security analysis proves that the scheme offers indistinguishability of keyword indexes under adaptive keyword attacks in the general group model and selective security of ciphertexts under plaintext attacks in the random oracle model. Experimental evaluations confirm that the scheme is both secure and practically efficient for real-world deployment.

The attribute-based online/offline searchable encryption scheme presented by Eltayieb et al. [17] makes the following key contributions. First, the encryption and trapdoor generation processes are divided into online and offline phases. Second, both message encryption and attribute policy enforcement are handled during the offline phase, reducing real-time computation. Third, the scheme is proven secure against both chosen-plaintext and chosen-keyword attacks. Finally, the authors demonstrate its applicability to cloud-based smart grids, emphasizing the need for adaptive encryption schemes to address challenges inherent in cloud computing.

For strengthening the search and fine-grained access control capabilities, Bakas et al. [18] present a hybrid encryption framework that integrates Symmetric Searchable Encryption (SSE) with Attribute-Based Encryption (ABE)—SSE for efficient search capabilities and ABE for fine-grained access control. Unlike many existing approaches, their design introduces a revocation mechanism that operates independently of the ABE system. This revocation process is implemented entirely using the secure execution environment provided by Intel® Software Guard Extensions (SGX). By isolating the revocation logic within SGX enclaves, the scheme enhances security and modularity, allowing for dynamic user revocation without compromising the core encryption infrastructure.

Many existing SE schemes are inadequate when it comes to managing hierarchical shared records effectively. In response to this inadequacy, Miao et al. [19] introduce an innovative approach known as Attribute-Based Keyword Search over Hierarchical Data (ABKS-HD), which employs CP-ABE. Despite its advancements, ABKS-HD has some limitations. Firstly, single keyword searches tend to return a high volume of irrelevant results, undermining the effectiveness of the search process. Secondly, there is a security concern wherein revoked users may still gain access to unauthorized data through old or outdated secret keys. Miao et al. [19] address the above two drawbacks and propose two enhanced schemes: ABKS-HD-I and ABKS-HD-II. These schemes not only facilitate multi-keyword searches but also incorporate user revocation capabilities. A notable distinction of their approach is that it scales with user attributes rather than total system attributes. Comprehensive security analyses confirm that the proposed schemes exhibit resilience against both chosen-plaintext and chosen-keyword attacks, thereby enhancing their robustness. Furthermore, real-world testing validates the practicality and efficiency of these enhancements, indicating a significant advancement in the capabilities of searchable encryption for hierarchical records.

The novel searchable encryption scheme proposed by Yu et al. [20] supports fine-grained access control through the implementation of KP-ABE. This approach facilitates the generation of trapdoors capable of supporting AND, OR, and threshold gate operations. The core concept involves the data owner encrypting the index keywords according to a specified access policy. A data user can then generate a trapdoor to search the data only if their attributes comply with the access policy. The scheme is accompanied by formal security proofs that demonstrate the indistinguishability of ciphertexts and trapdoors, which are critical in defending against chosen keyword and keyword guessing attacks launched by external adversaries. A comprehensive security analysis is conducted alongside implementation results, confirming that the proposed scheme is both provably secure and practical for real-world applications.

The comprehensive security approach, presented by Morales-Sandoval et al. [21], is suitable for cloud-based storage, sharing, and retrieval of encrypted data; they employ ABE to enforce access control over both the data and search operations. Their method optimizes encryption across three levels: bulk encryption for outsourced data, key management through ABE digital envelopes, and a novel framework known as attribute-based searchable encryption (ABSE). Utilizing Type-III pairings for 128-bit security, the approach is validated against benchmark datasets, demonstrating practical implementations utilizing Barreto-Naehrig curves.

He et al. [22] introduce a searchable encryption primitive that incorporates attribute-based access control to support hybrid Boolean keyword searches over encrypted data stored in the cloud. The proposed scheme offers several key features: (1) Data owners can define access control policies to specify who can search the encrypted data; (2) Any user whose attributes meet the access policy is permitted to perform search operations; and (3) Authorized users can execute more expressive queries, including complex Boolean keyword expressions. The scheme is formally proven secure under a defined security model, and a prototype implementation demonstrates its practicality and effectiveness in real-world scenarios.

The novel ABE scheme, called Sub-String Searchable ABE (SSS-ABE), proposed by Sun et al. [23], supports both secure data sharing and flexible querying over encrypted content. In this scheme, data is encrypted using an access policy, ensuring that only users whose attributes meet the policy can perform queries and decryption. Unlike traditional searchable encryption methods, SSS-ABE allows users to perform substring searches directly on the ciphertext without needing to predefine specific keywords. To accommodate resource-constrained environments such as IoT, the authors also incorporate an outsourced decryption mechanism, significantly reducing the computational burden on end-user devices.

The Multi-authority ciphertext-policy Attribute-Based Keyword Search (MABKS) scheme, presented by Miao et al. [24], overcomes the limitations of single-authority schemes and reduce the computational and storage overhead on resource-constrained devices in cloud environments. The system is further enhanced to support malicious attribute authority tracing and dynamic attribute updates, ensuring greater accountability and adaptability. Through rigorous security analysis, the MABKS system is shown to be selectively secure under both the selective-matrix and selective-attribute models. Experimental results using real-world datasets confirm its efficiency, scalability, and practicality for real-world deployment.

The single-keyword searchable encryption scheme, developed by Chaudhari et al. [25], is suitable for scenarios involving multiple data owners and multiple data users. The scheme employs ABE to enable users to access specific subsets of encrypted data stored in the cloud, without disclosing their access privileges to the cloud server. Security analysis demonstrates that the scheme is adaptively secure against chosen-keyword attacks under the random oracle model. The implementation on a Google Cloud instance confirms that the scheme is efficient and practical for real-world applications.

To enhance security of data outsourced to CSPs, Liu et al. [26] propose an Efficient Multikeyword Attribute-based Searchable Encryption (EMK-ABSE) scheme. In this scheme, encrypted data is stored in the cloud, while encrypted indexes are uploaded to nearby edge nodes, facilitating multikeyword searches and assisted decryption. A hybrid online/offline encryption mechanism serves to reduce the computational load on clients. Security analyses verify that EMK-ABSE is resistant to chosen keyword attacks, with performance evaluations indicating that it provides efficient, fine-grained access control with reduced computational complexity compared to similar schemes.

Zhao et al. [27] propose an attribute-based collaborative searchable encryption scheme for multi-user environments (ABCSE-MU). Using an access tree policy and introducing translation nodes, the scheme enables secure collaborative search while maintaining flexible access control. It addresses the issue of users with limited search rights by allowing cooperation at specific nodes without compromising data security. Random blinding protects secret key confidentiality, and the scheme is proven secure under the Decisional Bilinear Diffie-Hellman (DBDH) assumption. Security analysis confirms resistance to chosen-keyword and collusion attacks.

Many existing Ciphertext-Policy Attribute-Based Keyword Search (CP-ABKS) systems limit users to single-keyword searches, resulting in inaccurate outcomes and wasted resources. Additionally, untrusted servers may yield incomplete search results to conserve bandwidth, and most CP-ABKS implementations only facilitate unshared multi-owner setups, leading to increased computational and storage demands. Zhang et al. [28] propose a multi-keyword search scheme that incorporates verifiable results, melding CP-ABE with a shared multi-owner mechanism. Their scheme is designed to resist offline keyword guessing attacks, uphold signature unforgeability, and demonstrate enhanced efficiency and functionality through comparative experimental analysis.

The ABSE scheme proposed by Khan et al. [29] addresses several performance bottlenecks commonly found in traditional approaches. Specifically, their scheme avoids the computationally expensive bilinear pairing operations during the search phase and eliminates the need for Lagrange interpolation in secret reconstruction, thereby significantly improving efficiency. In addition, the proposed scheme allows for dynamic updates to access control policies without requiring full re-encryption of the existing ciphertext, which enhances its practicality in real-world scenarios where access requirements may change over time. The security of the scheme is proven in the selective-set model under the DBDH assumption. Furthermore, the scheme is designed to be collision-free, ensuring robustness against cryptographic collisions. Experimental results and detailed performance evaluations confirm that the proposed scheme achieves improved communication efficiency and overall performance compared to existing solutions.

The searchable Attribute-Based Signcryption (sABSC) scheme, presented by Rao et al. [30], offers multiple advanced features: (1) support for Boolean formula-based searches over signcrypted data, (2) protection of keyword privacy, (3) verifiable outsourced unsigncryption, and (4) self-verifiable search results. The proposed scheme enables data users to independently verify the accuracy of the search results returned by the cloud, without needing assistance from any trusted authority. The authors also extend existing security models by formulating more comprehensive definitions for the sABSC setting and conducting a formal security analysis. Performance evaluations demonstrate that the scheme is both efficient and suitable for real-world deployment.

2.2 Research Works That Support Blockchain-Based Searchable Encryption Schemes Suitable for General/Medical/IoT Data Sharing

The blockchain-based searchable encryption scheme using Ethereum, developed by Su et al. [31], employs two smart contracts: (i) a Search Smart Contract (SSC) for trapdoor-index matching and (ii) a Verify Smart Contract (VSC) for result verification. To enhance search precision, they implement a ranked multi-keyword search that returns the top-k most relevant documents. The scheme also integrates a new ABE mechanism that preserves data confidentiality and enforces access control, while supporting policy hiding to protect user privacy during data sharing. To ease the computational load on users, a cloud-assisted decryption system is introduced. Security analysis and performance evaluation confirm the scheme's efficiency and robustness.

Many existing ABSE schemes expose access policies in plaintext, risking user privacy, and rely on cloud servers for search operations, which can lead to tampering. To address these issues Zhang et al. [32] prosed a Blockchain-based Anonymous ABSE scheme for secure Data Sharing (BADS). BADS conceals access policy attributes, ensuring attribute confidentiality. By integrating ABSE with blockchain, the scheme benefits from tamper resistance, integrity verification, and non-repudiation. Secure indexes are stored on the blockchain, while encrypted data is kept on InterPlanetary File System (IPFS), a distributed storage system, to avoid single points of failure. The scheme includes a matching algorithm that performs a fixed number of pairing operations before initiating the search. Security analysis and performance evaluation confirm BADS's efficiency and practicality.

The medical data sharing scheme, presented by Niu et al. [33], is built on permissioned blockchain technology; it incorporates ciphertext-policy attribute-based encryption to safeguard data confidentiality and enforce access control. To protect patient's privacy, the scheme uses a polynomial equation method that allows flexible keyword associations, which are then integrated with the blockchain. Furthermore, the scheme achieves keyword indistinguishability under adaptive chosen-keyword attacks within the random oracle model. Performance analysis demonstrates that the scheme offers efficient and secure data retrieval.

Liu et al. [34] present a Blockchain-based Medical Data Sharing Scheme (BMDS) that incorporates attribute-based searchable encryption. In this framework, encrypted Electronic Medical Records (EMRs) are stored in the InterPlanetary File System (IPFS), while related indexes and metadata are maintained on a medical consortium blockchain. BMDS offers several key features, including tamper resistance, privacy protection, result verifiability, and secure key management, all while avoiding a single point of failure. Security analysis and performance evaluation demonstrate that BMDS provides robust protection, low computational overhead, and practical deployment potential in real-world medical environments.

Xiang et al. [35] introduce a blockchain-assisted searchable attribute-based encryption (SABE) scheme tailored for e-health systems, where secure and privacy-preserving access to sensitive medical records is of paramount importance. The proposed framework integrates the fine-grained access control capabilities of attribute-based encryption with the decentralized and tamper-resistant features of blockchain technology. A notable contribution of the scheme is its support for hidden access policies, which ensures that sensitive attributes associated with access structures remain concealed, thereby offering stronger privacy guarantees. From a security perspective, the scheme is formally proven to resist chosen keyword attacks, a critical requirement for safeguarding searchable encryption systems. Furthermore, extensive experimental evaluation demonstrates not only the feasibility of the design but also its efficiency and practicality in real-world e-health scenarios, highlighting its potential for deployment in secure healthcare data-sharing environments.

The attribute-based multi-keyword searchable encryption scheme for IoT, presented by Yan et al. [36], is capable of hiding access policies using blockchain. By integrating an attribute Bloom filter, the scheme filters out unauthorized queries early, reducing bilinear pairing overhead and improving search efficiency. Valid requests are processed by the cloud for access verification and keyword search. Encrypted data is stored using InterPlanetary File System (IPFS) for scalable and efficient storage, while blockchain ensures secure, tamper-proof, and traceable search records. Security and performance evaluations confirm the scheme's practicality for IoT applications.

Table 1 provides a thematic analysis of the blockchain-based searchable encryption schemes discussed above. The rows in the table let you compare how each paper tackles blockchain-ABSE integration. The columns show recurring themes (Role of blockchain, privacy and policy hiding, domain adaptation, efficiency, hybrid storage, and security guarantees).

Table 1: A comparative thematic analysis of the blockchain-based searchable encryption schemes discussed above

Author/Year	Blockchain role	Privacy and policy hiding	Application domain	Search enhancements	Storage and computation	Security guarantees
Su et al. [31]/2022	Ethereum smart contracts (SSC for search, VSC for verification)	Policy hiding via new ABE mechanism	General data sharing	Ranked multi-keyword search, Top-k results	Cloud-assisted decryption to reduce user overhead	Efficiency and robustness validated via analysis
Zhang et al. [32]/2024	Blockchain for tamper resistance, integrity verification, non-repudiation	Conceals access policy attributes	General data sharing	Matching algorithm with fixed pairing operations before search	Indexes on blockchain; encrypted data stored on IPFS	Security and performance confirm practicality
Niu et al. [33]/2020	Permissioned blockchain integrated with CP-ABE	Polynomial method for flexible keyword associations	Medical data sharing	Keyword indistinguishability, adaptive chosen-keyword attack resistance	Blockchain for metadata, ciphertext-policy ABE for access	Formal proof of indistinguishability and efficiency
Liu et al. [34]/2021	Consortium blockchain for metadata and indexes	Privacy protection mechanisms	Medical data sharing (EMRs)	Emphasis on verifiability and secure key management	Encrypted EMRs on IPFS; avoids single point of failure	Robust protection, low overhead, real-world feasibility
Xiang et al. [35]/2022	Blockchain-assisted SABE framework	Hidden access policies for privacy	E-health systems	Standard ABSE search and chosen keyword security	Blockchain for integrity, ABE for confidentiality	Secure against chosen keyword attacks
Yan et al. [36]/2025	Blockchain for tamper-proof and traceable search records	Hidden access policies	IoT data sharing	Attribute Bloom filter reduces pairing overhead; efficient multi-keyword search	Encrypted data on IPFS; cloud processes valid requests	Security and performance confirm practicality for IoT

2.3 Research Works That Support Attribute-Based Searchable Encryption Suitable for Healthcare Environments

Many existing ABKS schemes typically support only keyword encryption, necessitating separate encryption for messages. Furthermore, these schemes often lack robust defenses against offline keyword guessing attacks by semi-honest insiders, such as servers. To address these challenges, Guo et al. [37] propose a secure-channel-free, Ciphertext-Policy Decryptable ABKS (CP-DABKS) scheme. This innovative approach enables authorized users to decrypt ciphertext without relying on a secure channel, while also effectively resisting insider keyword guessing attacks. The researchers rigorously verify the security of their scheme and illustrate its application within an eHealth cloud platform, demonstrating its practical utility in secure data management.

Walid et al. [38] propose an innovative framework designed to enable efficient searchable encryption for large-scale Electronic Health Records (EHR) systems. Their approach integrates ABE with multi-keyword search capabilities to provide both fine-grained access control and flexible search functionality over encrypted medical data. A key aspect of their solution is the outsourcing of computationally intensive search operations to the cloud, which offloads the burden from resource-constrained clients. By doing so, the system significantly reduces both network bandwidth consumption and client-side computational overhead, making it highly suitable for scalable and practical deployment in cloud-based healthcare environments.

The integration of IoT and cloud technology in healthcare offers real-time health monitoring, enabling prompt responses from healthcare providers during emergencies. However, to protect patient privacy, cloud-stored health data must be encrypted, which complicates data retrieval and places strain on resource-limited devices on both the patient and provider sides. Bao et al. [39] tackle this challenge with a Lightweight Attribute-Based Searchable Encryption (LABSE) scheme that provides fine-grained access control, keyword search capabilities, and maintains low computational overhead for resource-constrained devices. Their rigorous proofs of semantic security complement experimental comparisons, showcasing LABSE's advantages over existing methods.

Chaudhari et al. [40] proposed a scheme enabling keyword-based search over attribute-based (KeySea) encrypted data while preserving receiver anonymity. This feature is particularly valuable in privacy-sensitive domains such as healthcare, where both data confidentiality and user anonymity are critical. KeySea leverages hidden access policies within the attribute-based searchable encryption framework to protect access rules from exposure. The scheme offers a secure and practical solution for privacy-preserving search over encrypted data stored in the public cloud. Security analysis and experimental results confirm both the robustness and efficiency of the proposed approach.

Zhang et al. [41] 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 personal health records (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.

Chen et al. [42] introduce a Hidden Policy ABSE (HP-ABSE) scheme to address the privacy concerns arising from the use of explicit attribute values in access policies. They note, however, that many existing HP-ABSE models remain vulnerable to attribute guessing attacks, where an adversary attempts to infer attribute values used in the access structure. To mitigate this, the authors propose a new scheme called Partially Hidden Policy Attribute-Based Multi-Keyword Searchable Encryption with Verification and Revocation (PHP-ABMKSE-VR). This enhanced scheme supports multi-keyword search, user revocation, and result verification, while partially hiding access policies to strengthen privacy. Security analysis and experimental results demonstrate that PHP-ABMKSE-VR is secure, efficient, and suitable for practical applications, particularly in domains like smart healthcare.

Chen et al. [43] introduce a novel encryption framework called Fair-and-Exculpable Attribute-Based Searchable Encryption with Revocation and Verifiable Outsourced Decryption (FE-ABSE-RV), which leverages smart contracts to enforce fair and secure data access in cloud environments. The proposed scheme addresses critical challenges such as user revocation, verifiable outsourced decryption, and accountability in ABSE systems. The "fairness" aspect ensures that honest users can perform searches and decrypt data without being denied access, while "exculpability" guarantees that no one–including the cloud server–can falsely implicate an honest user for malicious behavior. By integrating smart contracts, the system automates policy enforcement and auditability, reducing reliance on trusted third parties. Security analysis confirms that FE-ABSE-RV is resilient against both chosen-plaintext attacks (CPA) and chosen-keyword attacks (CKA), ensuring strong data confidentiality and search privacy. Furthermore, both theoretical evaluation and simulation experiments demonstrate that the scheme achieves a high level of expressiveness (in terms of flexible access control), computational efficiency, and practicality, making it well-suited for real-world applications such as secure data sharing in decentralized healthcare or financial systems.

In real-world scenarios, Multi-Authority Ciphertext-Policy Attribute-Based Searchable Encryption (MA-CP-ABSE) is well-suited for securing electronic medical records (EMRs) due to its fine-grained access control, efficient key management, and encrypted data search capabilities. However, most existing MA-CP-ABSE schemes rely heavily on a central authority, especially for key generation. To overcome this limitation, Ghopur et al. [44] proposed a Decentralized MA-CP-ABSE (DMA-CP-ABSE) scheme, where each attribute authority can independently issue secret keys without central control. To address the issue of irrelevant results from single-keyword searches, they enhance this scheme by adding a multi-keyword search feature for more accurate retrieval. They also introduce an attribute revocation mechanism to support dynamic access control. Security analysis confirms resistance to chosen-keyword attacks (CKA), and experimental results demonstrate the scheme's practicality and efficiency.

2.4 Research Works That Support Attribute-Based Searchable Encryption Suitable for Clouds That Support Fog/Edge-Computing Environment

Varri et al. [45] propose a Fog-Enabled Lightweight Traceable Attribute-Based Keyword Search (FELT-ABKS) scheme aimed at achieving secure, efficient, and privacy-preserving search over encrypted data in distributed environments. The scheme builds upon ciphertext-policy ABKS to provide fine-grained access control and keyword-based retrieval, thereby facilitating flexible and controlled data sharing. A key innovation of FELT-ABKS lies in its use of fog computing infrastructure to offload most of the computational overhead from end users, significantly improving efficiency and scalability for resource-constrained devices, such as those commonly found in IoT settings. In addition to efficient search and access control, the scheme integrates mechanisms for user revocation and attribute revocation, ensuring adaptability in dynamic environments where user privileges and attribute values may change over time. Importantly, FELT-ABKS incorporates traceability features, enabling the identification of malicious users who misuse or leak their secret keys–an essential property for accountability in practical systems. Through rigorous security analysis, the authors demonstrate that FELT-ABKS provides robustness against chosen-keyword attacks, chosen-plaintext attacks, and secret key modification attacks. Complementing the theoretical guarantees, experimental evaluations confirm that FELT-ABKS maintains lightweight performance characteristics while offering practical deployability in real-world applications. These results underscore the scheme's potential for secure data management in fog-assisted and IoT-enabled environments.

Niu et al. [46] propose an attribute-based encryption scheme for edge computing environments that supports keyword search without revealing private information to the cloud during the search phase. The scheme is designed with computational efficiency in mind, especially for lightweight users, and allows for partial decryption outsourcing, enhancing flexibility and practicality. It also supports efficient attribute revocation and ciphertext updates. The scheme is proven to be Indistinguishability under Selective Ciphertext Policy Chosen Plaintext Attack (IND-sCP-CPA) and Indistinguishability under Chosen Keyword Attack (IND-CKA) secure. Performance analysis shows that it achieves low storage and computation overhead compared to existing methods, making it well-suited for edge computing scenarios.

2.5 Research Works That Support Attribute-Based Searchable Encryption Suitable for IoT Environments

Wang et al. [47] propose a keyword-searchable attribute-based encryption scheme with equality test (KS-ABESwET) for IoT environments. By integrating ABSE with an equality test mechanism and inverted index-based keyword search, the scheme allows the cloud server to return only matching ciphertexts. An authorized server then performs equality tests to determine whether ciphertexts, encrypted under different policies, contain the same plaintext–without decryption. This reduces the need for extensive decryption by IoT devices, minimizing storage use and computational complexity. Leveraging outsourcing, most computations are handled by the server, significantly lowering the resource burden on IoT devices. Security is proven under the decisional q-1 and DDH assumptions, ensuring chosen-plaintext and chosen-keyword security. Experimental results and analysis confirm the scheme's efficiency and suitability for IoT scenarios.

Yin et al. [48] present an Attribute-Based Searchable Encryption scheme tailored for cloud-assisted Industrial Internet of Things (IIoT) applications. Their construction introduces a novel access policy-based structured secure index along with an attribute-based search token mechanism. This design enables fine-grained control over keyword search privileges on encrypted IIoT data. To the best of the authors' knowledge, this work represents the first ABSE construction specifically designed for the IIoT context. The authors provide formal correctness proofs and security analyses to validate the soundness of their approach. Additionally, experimental evaluations conducted on a real-world dataset demonstrate both the correctness and practical search efficiency of the proposed approach.

Zhang et al. [49] introduce an attribute-based keyword searchable encryption scheme designed to protect power grid data. The scheme enables secure retrieval of encrypted data while enforcing fine-grained access control–only users whose attributes meet the specified access policies are allowed to search and decrypt the data. To meet the demands of power grid systems, the scheme supports a large attribute universe and conceals access policies to protect user privacy. These hidden policies ensure that sensitive user information is not exposed. Security and performance evaluations show that the scheme is both efficient and suitable for real-world deployment. In addition, comparative analysis with existing approaches highlights the superior features and effectiveness of the proposed method.

Tables 2–5 present a concise summary of the research works reviewed in this paper, categorizing them based on the type of attribute-based encryption (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 properties.

Table 2: Classification of the papers discussed based on the encryption techniques used and their application area

ABE technique used	Paper and year	Application area/Properties
Searchable CP-ABE	Michalas et al. [15], 2019	Cloud/Integrates SSE and CP-ABE for implementing efficient search functionality along with scalable and secure access management
Searchable CP-ABE	Niu et al. [33], 2020	Cloud-EHR/Uses permissioned blockchain and CP-ABE to safeguard data confidentiality and enforce access control and the scheme achieves keyword indistinguishability under adaptive chosen-keyword attacks
Searchable CP-ABE	Varri et al. [45], 2022	Fog-enabled Cloud/A lightweight traceable attribute-based keyword search scheme with support for fine-grained access control, user and attribute revocation, and tracing malicious users
Searchable Multi-authority ABE	Ghopur et al. [44], 2025	Cloud-EHR/A decentralized multi-authority searchable KP-ABE without centralized control for secret key distribution, and supports secure multi-keyword search for more accurate retrieval
Searchable Multi-authority ABE	Miao et al. [24], 2021	Cloud/A multi-authority searchable CP-ABE which supports keyword search, and supports malicious attribute authority tracing and dynamic attribute updates
Searchable ABE	Bakas et al. [18], 2019	Cloud/SSE and ABE are combined to make SE efficient, and it supports efficient revocation implemented using SGX
Searchable ABE	Eltayieb et al. [17], 2019	Cloud-based-Smart-Grid/Suitable for Cloud-based Smart-Grid environments, bot message encryption and attribute policy enforcement are handled offline, reducing real-time computation
Searchable ABE	Wang et al. [16], 2019	Cloud/Supports privacy-preserving multi-keyword search and offloads computation to cloud for improving performance
Searchable ABE	Wang et al. [47], 2019	Cloud-IoT/Suitable for resource-poor IoT nodes, because decryption and search operations are outsourced to cloud
Searchable ABE	Liu et al. [50], 2020	Cloud/Verifiable keyword search, supports data deduplication, ensures data integrity and has less computational overhead
Searchable ABE	Morales-Sandoval et al. [21], 2020	Cloud/Access control on both data and search operations
Searchable ABE	Guo et al. [37], 2020	Cloud-IoT/Keyword search support, low overhead

Table 3: 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
Searchable ABE	Yu et al. [20], 2020	Cloud-Ehealth/Does not require a secure channel to decrypt and resists keyword guessing attack
Searchable ABE	Miao et al. [19], 2020	Cloud/Fine-grained access control and support for keyword search
Searchable ABE	Walid et al. [38], 2020	Cloud-EHR/Supports efficient searching for large scale EHR systems as well as multi-keyword search capabilities to provide both fine-grained access control and flexible search functionality over encrypted medical data
Searchable ABE	He et al. [22], 2020	Cloud/Supports hybrid Boolean keyword searches over encrypted data; it has several other features such as data owners can define access control policies to specify who can access data, and also allows authorized users to execute more expressive queries

(Continued)

Table 3 (continued)

ABE technique used	Paper and year	Application area/Properties
Searchable ABE	Liu et al. [34], 2021	EHR/Uses tamper resistant IPFS to store records, supports privacy protection, result verifiability, and secure key management, and is not susceptible to single point of failure
Searchable ABE	Sun et al. [23], 2021	Cloud-IoT/Supports searching for substrings (not just keywords) on encrypted data, outsourced decryption is used to support resource-constrained IoT devices
Searchable ABE	Chaudhari et al. [25], 2021	Cloud/A single-keyword searchable encryption scheme that enable users to access specific subsets of encrypted data
Searchable ABE	Bao et al. [39], 2022	Cloud-IoT/A lightweight ABSE scheme that provides fine-grained access control, keyword search capabilities, and maintains low computational overhead for resource-constrained device
Searchable ABE	Liu et al. [26], 2022	Cloud-edge/Supports multi-keyword search and encrypted indexes are stored in Edge nodes for improved performance
Searchable ABE	Su et al. [31], 2022	Cloud/A blockchain-based searchable encryption scheme using Ethereum that supports secure search and result verification, ranked multi-keyword search
Searchable ABE	Xiang et al. [35]	Cloud-Ehealth/A blockchain-assisted searchable ABE which combines the strengths of ABE with blockchain technology, enabling support for hidden access policies to enhance privacy
Searchable ABE	Chaudhari et al. [25], 2021	Cloud/A single-keyword searchable encryption scheme that enable users to access specific subsets of encrypted data

Table 4: 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
Searchable ABE	Bao et al. [39], 2022	Cloud-IoT/A lightweight ABSE scheme that provides fine-grained access control, keyword search capabilities, and maintains low computational overhead for resource-constrained device
Searchable ABE	Liu et al. [26], 2022	Cloud-edge/Supports multi-keyword search and encrypted indexes are stored in Edge nodes for improved performance
Searchable ABE	Su et al. [31], 2022	Cloud/A blockchain-based searchable encryption scheme using Ethereum that supports secure search and result verification, ranked multi-keyword search
Searchable ABE	Xiang et al. [35]	Cloud-Ehealth/A blockchain-assisted searchable ABE which combines the strengths of ABE with blockchain technology, enabling support for hidden access policies to enhance privacy
Searchable ABE	Chaudhari et al. [40], 2022	Cloud-EHR/Supports keyword-based while preserving receiver anonymity leveraging on hidden access policies within the ABE framework
Searchable ABE	Zhao et al. [27], 2023	Cloud/Supports secure collaborative search without compromising data security while maintaining flexible access control
Searchable ABE	Yin et al. [48], 2023	Cloud-IIoT/First Searchable ABE scheme proposed for IIoT, and supports fine-grained control over keyword search privileges
Searchable ABE	Zhang et al. [28], 2023	Cloud/Combines CP-ABE with a shared multi-owner mechanism to support multi-keyword search with verifiable results, and it can resist offline keyword guessing attacks, uphold signature unforgeability
Searchable ABE	Niu et al. [46], 2023	Cloud-EHR/CP-ABE is combined with permissioned blockchain technology to enforce access control and to protect privacy a polynomial equation method is used

(Continued)

Table 4 (continued)

ABE technique used	Paper and year	Application area/Properties
Searchable ABE	Zhang et al. [49], 2023	Cloud-power-grid/Designed to protect power grid data, supports a large attribute universe and hence is scalable and conceals access policies to protect user privacy
Searchable ABE	Zhang et al. [41], 2024	Cloud-PHR/Conceals access policies to enhance privacy, supports fine-grained access control, and is efficient with respect to storage and computation overhead

Table 5: 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
Searchable ABE	Khan et al. [29], 2024	Cloud/Makes searching efficient by not using bilinear pairing operations, eliminates Lagrange interpolation in secret reconstruction and allows for dynamic updates to access control policies without requiring full re-encryption
Searchable ABE	Zhang et al. [32], 2024	Cloud/Blockchain-based scheme that conceals access policy attributes, ensuring attribute confidentiality
Searchable ABE	Rao et al. [30], 2024	Cloud/A secure Searchable AB signcryption scheme that supports boolean formula-based searches over signcrypted data, protection of keyword privacy, verifiable outsourced unsigncryption, and self-verifiable search results
Searchable ABE	Yan et al. [36], 2025	Cloud-IoT/Supports multi-keyword searchable encryption scheme that hides access policies using blockchain. The scheme filters out unauthorized queries early, and valid requests are processed by the cloud for access verification and keyword search
Searchable ABE	Chen et al. [42], 2025	Cloud/Supports multi-keyword search, user revocation, and result verification, while partially hiding access policies to strengthen privacy
Searchable ABE	Chen et al. [43], 2025	Cloud/Supports user revocation, verifiable outsourced decryption, accountability and supports high level of expressiveness and computational efficiency

Tables 6–12 provide a comparative thematic analysis of the searchable encryption schemes, discussed in this paper, that do not use Blockchain. Here is the short legend of the codes used in this table which would help reading the contents of the table.

Table 6: A comparative thematic analysis of the searchable encryption schemes that do not use blockchain

Author/ Year	Core idea	Search type (support)	Outsourcing/ Offloading	Policy privacy	Multi-authority/ Multi-owner	Verification/ Auditing	Target Env./ Use-case	Security model/ Assumptions	Exp. Eval/ Efficiency notes	Special techniques/ Remark
Michalas et al. [15]/ 2019	Hybrid SSE and CP-ABE protocol	SSE searches and ABE access control	SSE handles search; ABE for key distribution	Depends on ABE part (explicit)	Can support multi-owner via ABE	–	Scalable searchable systems	Security: combined primitives (analyses provided)	Focus on practical performance (SSE benefits)	Hybrid design to leverage SSE efficiency and ABE expressiveness
Wang et al. [16]/ 2019	VMKS-ABE with verifiability	Multi-keyword searchable	Offloads computation to cloud proxy	Explicit	Single authority and proxy	Verifies correctness of outsourced private keys and results	Cloud storage	Indistinguishability of indexes; ciphertext security in ROM	Experiments show practical efficiency	Proxy-assisted computation; verifiable outsourced key correctness
Eltayieb et al. [17]/ 2019	Online/ offline ABSE	Keyword search; online/offline operations	Offline phase handles heavy work	Explicit	Single authority	–	Smart-grid cloud apps	Proven secure against CPA and CKA	Emphasizes reduced online computation	Online/ offline split to reduce real-time cost
Bakas et al. [18]/ 2019	Hybrid SSE and ABE; SGX for revocation	Multi-keyword SSE with ABE access control	SSE searches outsourced; SGX enclave for revocation	Depends on ABE part	Can support multi-owner	–	EHR/Large systems	Security relies on ABE and SGX protection	Practical focus; leverages SGX to handle revocation securely	Uses Intel SGX enclaves to isolate revocation logic

Table 7: A comparative thematic analysis of the searchable encryption schemes that do not use blockchain contd...

Author/ Year	Core idea	Search type (support)	Outsourcing/ Offloading	Policy privacy	Multi-authority/ Multi-owner	Verification/ Auditing	Target Env./ Use-case	Security model/ Assumptions	Exp. Eval/ Efficiency notes	Special techniques/ Remark
Miao et al. [19]/ 2020	ABKS-HD (hierarchical data)–BKS-HD-I/II	Multi-keyword search	–	Explicit	Single-owner but scales with user attributes	–	Hierarchical shared records	Proofs based on CPA/CKA	Experiments show practical efficiency	Designed to scale with attributes
Yu et al. [20]/ 2020	KP-AB index encryption supporting AND/OR/ threshold	Multi-keyword; boolean and threshold gates	–	Explicit	KP-ABE style key-policy	–	General cloud use	Indistinguishability proofs based on chosen keyword attacks	Implementation and performance analysis	Trapdoors that support logical gates (AND/OR/ threshold)
Morales-Sandoval et al. [21]/ 2020	ABSE framework and ABE digital envelopes	Multi-keyword search and layered encryption	Bulk encryption outsourcing; key management via ABE envelopes	Explicit	Framework supports many deployments	–	Cloud storage/practical deployments	Uses Type-III pairings; 128-bit BN curves	Benchmarked on datasets (practical validation)	Focus on practical, layered approach; pairing-based
He et al. [22]/ 2020	AB primitive for hybrid Boolean keyword search	Boolean keyword expressions	–	Explicit	Single authority	–	Cloud storage	Formal security model and proof	Prototype demonstrates practicality	Expressive Boolean queries for authorized users

Table 8: A comparative thematic analysis of the searchable encryption schemes that do not use blockchain contd...

Author/ Year	Core idea	Search type (support)	Outsourcing/ Offloading	Policy privacy	Multi-authority/ Multi-owner	Verification/ Auditing	Target Env./ Use-case	Security model/ Assumptions	Exp. Eval/ Efficiency notes	Special techniques/ Remark
Sun et al. [23]/ 2021	Substring searchable ABE	Substring search	Outsourced decryption for IoT	Explicit	Single authority	–	IoT/resource-constrained devices	Security proofs provided	Designed for resource constrained devices; outsourced decryption	Supports substring search without predefining keywords
Miao et al. [24]/ 2021	Multi-authority CP ABKS	Multi-keyword search	Reduced overhead; offloading considered	Explicit	Multi-authority	Tracing of malicious AA	Cloud/ resource constrained devices	Selective security (selective-matrixe and selective-attribute)	Experiments on real datasets confirm efficiency	Adds malicious AA tracing and dynamic updates
Chaudhari et al. [25]/ 2021	Single-keyword SE for multiple owners/users	Single-keyword searchable	Implementation on Google Cloud	Explicit (does not leak privilege)	Multi-owner	–	Cloud (multi-owner scenarios)	Adaptive security under CKA in ROM	Implemented on Google Cloud	Focus on multi-owner practicality
Liu et al. [26]/ 2022	Edge assistance	Multikeyword search	Encrypted indexes placed on edge nodes; edge assisted decryption	Explicit	Hybrid cloud and edge	–	Edge computing and cloud	Resistant to CKA; security analyses given	Online/offline hybrid reduces client load; experiments show efficiency	Uses edge nodes to host encrypted indexes and aid searches

Table 9: A comparative thematic analysis of the searchable encryption schemes that do not use blockchain contd...

Author/ Year	Core idea	Search type (support)	Outsourcing/ Offloading	Policy privacy	Multi-authority/ Multi-owner	Verification/ Auditing	Target Env./ Use-case	Security model/ Assumptions	Exp. eval/ Efficiency notes	Special techniques/ Remark
Guo et al. [37]/ 2020	Secure-channel-free CP-ABKS	Keyword search and message included	Supports secure-channel-free decryption	Explicit	Single authority	–	eHealth cloud platform	Security proofs; resistant to insider guessing	Practical demonstration in eHealth use case	Defends against insider/offline keyword guessing
Walid et al. [38]/ 2020	ABE	Multi-keyword search support for large EHRs	Outsources search to cloud for efficiency	Explicit	Likely multi-owner support	–	Large-scale EHR systems	Security analysis and scalability focus	Focus on reducing client load and bandwidth	Designed for large EHR systems; scalability emphasis
Bao et al. [39]/ 2022	Light-weight ABSE	Keyword search	Low computation overhead for devices	Explicit	Single authority	–	IoT/ health-care	Semantic security proofs	Experiments compare favorably with prior schemes	Designed for IoT/healthcare envs. with strict resource limits
Chaudhari et al. [40]/ 2022	Keyword search with receiver anonymity	Keyword search; preserves receiver anonymity	–	Hidden access policies used	Single authority	–	Healthcare/ privacy-sensitive domains	Security analysis and experimental evaluation	Efficient and practical per authors	Hidden access policies; receiver anonymity emphasis

Table 10: A comparative thematic analysis of the searchable encryption schemes that do not use blockchain contd...

Author/ Year	Core idea	Search type (support)	Outsourcing/ Offloading	Policy privacy	Multi-authority/ Multi-owner	Verification/ Auditing	Target Env./ Use-case	Security model/ Assumptions	Exp. Eval/ Efficiency notes	Special techniques/ Remark
Zhang et al. [28]/ 2023	Verifiable search results; shared multi-owner	Multi-keyword searchable with verifiability	–	Explicit (but multi-owner shared)	Shared multi-owner	Verifiable results	Cloud multi-owner setups	Resists offline guessing; supports unforgeability	Comparative experiments show improved efficiency	Focus on verifiability and shared multi-owner support
Khan et al. [29]/ 2024	Efficient ABSE avoiding pairings in search	Multi-keyword/ searchable; dynamic policy updates	–	Explicit	Single authority	–	General cloud use	Security in selective-set model under DBDH	Experimental evaluations show improved performance	Avoids pairing operations and Lagrange interpolation during search
Rao et al. [30]/ 2024	Secure Attribute-Based Signcryption	Boolean searches over signcrypted data; verifiable outputs	Verifiable outsourced unsigncryption	Explicit	Single authority	Self-verifiable search results	Cloud (general real-world deployment)	Formal security models extended; proofs	Performance evaluations show efficiency	Emphasis on verifiability and signcryption
Varri et al. [45]	Fog-enabled light-weight traceable ABKS	Keyword search	Computation offload to fog nodes	Explicit	Single authority	Traceability of malicious users	Fog/edge environments	Security based on chosen-keyword/plaintext/ secret key modification	Experiments show lightweight and deployable	Fog node offloading; traceability and revocation

Table 11: A comparative thematic analysis of the searchable encryption schemes that do not use blockchain contd...

Author/ Year	Core idea	Search type (support)	Outsourcing/ Offloading	Policy privacy	Multi-authority/ Multi-owner	Verificaion/ Auditing	Target Env./ Use-case	Security model/ Assumptions	Exp. Eval/ Efficiency notes	Special techniques/ Remark
Niu et al. [46]	ABE for edge computing	Keyword search	Partial decryption outsourcing to edge nodes	Explicit	Single authority	–	Edge computing/lightweight devices	IND-sCP-CPA and IND-CKA security	Low storage and computation overhead	Tailored for edge computing scenarios
Wang et al. [47]/ 2019	Equality test and ABSE for IoT	Inverted index keyword search and equality test	Outsourcing to server; authorized server does equality test	Explicit	Single authority	–	IoT environments	Security under decisional q-1 and DDH; CPA/CKA proven	Experiments show low overhead for IoT	Equality test enables cross-policy matching without decrypting
Yin et al. [48]/ 2023	ABSE for IIoT with structured secure index	Keyword search using structured index and token	Cloud-assisted IIoT; index structuring	Explicit	Single authority	–	IIoT	Formal correctness and security analyses	Real-world dataset experiments validate efficiency	First ABSE designed for IIoT, per authors
Zhang et al. [49]/ 2023	ABKS for power grid	Keyword search; hides access policies	–	Hidden policies	Single authority	–	Power grid data protection	Security and performance evaluations	Comparative analysis shows suitability	Targets large attribute universe and policy hiding
Zhao et al. [27]/ 2023	Collaborative searchable encryption	Collaborative search; uses translation nodes	–	Explicit	Multi-user collaborative model	–	Multi-user collaborative environments	Security under DBDH; resists collusion	–	Uses translation nodes for cooperative search rights

Table 12: A comparative thematic analysis of the searchable encryption schemes that do not use blockchain contd...

Author/ Year	**Core idea**	**Search type (support)**	**Outsourcing/ Offloading**	**Policy privacy**	**Multi-authority/ Multi-owner**	**Verification/ Auditing**	**Target Env./ Use-case**	**Security model/ Assumptions**	**Exp. eval/ Efficiency notes**	**Special techniques/ Remark**
Zhang et al. [32]/ 2024	Hidden-policy ABKS for PHRs	Keyword search; hidden access policies	Scalable performance optimizations	Policy privacy (hidden)	Single authority	–	Personal Health Records (PHRs)	Security under q-DBDHE and DDH	Simulations show strong performance and scalability	Hides access structures; improves scalability
Chen et al. [42]/ 2025	Partially hidden policy	Multi-keyword search, verification of results and revocation	Outsourced decryption and verification	Partially hidden policies	Multi-authority/ multi-owner? (multi-keyword and multi-user focus)	Result verification	Smart healthcare use case	Security analysis and experiments show efficiency	Aims to prevent attribute guessing and supports partial hiding of policies	
Chen et al. [43]/ 2025-2	Fair and exculpable ABSE with smart contracts	Multi-keyword search; revocation; verifiable outsourced decryption	Outsourced decryption; smart contract enforcement	Explicit (aims for fairness and accountability)	Supports accountability; may be multi-owner	Verifiable outsourced decryption; fairness via smart contracts	Decentralized health-care/financial systems	CPA and CKA security proofs	Simulations and theoretical evaluation	Integrates smart contracts for policy enforcement and auditability
Ghopur et al. [44]/ 2025	Decentralized MA-CP-ABSE	Multi-keyword search	Decentralized multi-AA issues keys (no central TA)	Explicit	Decentralized multi-authority	–	Electronic medical records	Security based on CKA; experimental validation	Experiments demonstrate efficiency and practicality	Removes central authority; multi-AA key issuance

Core idea—main cryptographic building block (CP/KP/Hybrid/SSE/ABE and feature) used.

Search type—whether it supports single, multi-keyword, substring, Boolean, equality, threshold/gate support.

Outsourcing/Offload—whether heavy computation work is offloaded to cloud/edge/fog/proxy/SGX enclave/smart contract.

Policy privacy—Explicit = access structures visible; Hidden/Partially hidden = policies concealed to various degrees.

Multi-authority/multi-owner—supports distributed attribute authorities (AAs) or shared multi-owner setups.

Verification/Auditing—integrated verification of search results, key correctness, auditors, or smart-contract enforcement.

Security model/assumptions—short tag of the main cryptographic assumption or model used (e.g., ROM = random oracle model; LWE, DBDH, q-DBDHE, DBDHE, IND-CPA, etc.).

Exp. eval/Efficiency notes—denotes whether the paper includes implementation/experiments and notable efficiency claims.

Special techniques/Remark—any special techniques used/general comments.

3 Discussion of Open Issues

Supporting searchable encryption over files encrypted with ABE presents a number of open challenges. These stem from the complexity of combining fine-grained access control (supported by ABE) with the ability to efficiently and securely search encrypted data. Some of the key open issues are:

- **Efficient Search with Fine-Grained Access Control:** Attribute-Based Encryption (ABE) enforces encryption and access control based on user attributes, offering fine-grained access control for data protection. In contrast, Searchable Encryption (SE) schemes—such as Public Key Encryption with Keyword Search (PEKS) and Searchable Symmetric Encryption (SSE)—are typically built for simpler public-key or symmetric-key settings. Integrating ABE with SE introduces significant computational and communication overhead, especially during search and decryption operations. While several approaches have explored this integration, not all of them are efficient for practical use. Further research is needed to develop SE methods that combine the expressive access control capability of ABE with the low overhead that is required for real-world applications.
- **Policy Hiding with Searchability:** ABE schemes that hide access policies aim to protect user privacy by concealing the attributes or conditions required to decrypt the data. This is particularly important in sensitive domains like healthcare, where revealing access policies could unintentionally disclose private information about users or the data itself. However, this approach conflicts with the typical design of SE schemes, which often rely on exposing access policies or metadata to enable efficient keyword search. In many SE schemes, the system needs to know which users meet the access criteria in order to correctly match search queries with encrypted documents. When the access policy is hidden, it becomes significantly more difficult for the server to determine which ciphertexts a given search token should apply to—without violating privacy or leaking sensitive information. As a result, designing SE schemes that both preserve access policy privacy and support accurate, efficient search remains an open challenge. It requires careful cryptographic construction to balance search correctness, efficiency, and privacy. Addressing this challenge is essential for building privacy-preserving, searchable ABE systems suitable for real-world applications like cloud storage, healthcare, and Internet of Medical Things (IoMT).

- **Support for Complex Queries:** Most existing ABE schemes that support SE are limited to simple keyword searches. However, real-world applications—especially in healthcare and IoMT—often require more advanced search capabilities, such as Boolean queries, range searches, fuzzy matching, and multi-keyword ranking. Supporting these complex queries over ABE-encrypted data remains a largely unresolved challenge. Efficiently enabling such functionality while maintaining strong security, privacy, and fine-grained access control is essential for making ABE-SE schemes truly practical and scalable in sensitive, data-intensive environments.
- **Revocation Handling:** While user and attribute revocation has been partially addressed in ABE schemes, it becomes significantly more complex when searchable functionality is incorporated. Revoking users or attributes typically involves re-encrypting data or rebuilding search indexes, both of which are resource-intensive and hinder scalability. These operations are especially problematic in environments with large datasets or frequent access changes. Therefore, designing efficient and scalable revocation mechanisms that support both SE and data deduplication remains a major challenge. Achieving this balance is critical for real-world deployment in dynamic systems like cloud-based healthcare or IoMT networks.
- **Search Result Privacy:** Search queries and results in searchable encryption systems can inadvertently leak sensitive information, such as keywords, access patterns, or even user identities. Ensuring query privacy, access pattern hiding, and result unlinkability—all while maintaining practical performance—remains an open research challenge. Developing solutions that protect against such leakage without introducing significant computational or communication overhead is critical for building secure and privacy-preserving systems.
- **Dynamic Updates:** Designing ABE schemes integrated with SE that support dynamic data operations—such as adding or removing files, and adding/updating attributes of users—in a secure and efficient manner remains a significant challenge. Most existing ABE-SE solutions assume static datasets, making them unsuitable for real-world applications where data is constantly evolving. In dynamic environments like cloud storage, healthcare, or IoMT systems, users frequently update data, change access policies, or modify search criteria. Achieving efficient, scalable, and privacy-preserving dynamic updates in ABE-SE systems is therefore an ongoing research priority.
- **Lightweight Design for IoT/IoMT:** IoT and IoMT devices typically operate with limited computational power, memory, and energy resources, which poses a significant challenge for deploying cryptographic schemes like ABE combined with SE. These schemes are often computationally intensive, especially during encryption, search token generation, and policy evaluation. As a result, executing ABE-SE operations directly on resource-constrained devices can lead to unacceptable delays, battery drain, or even system failure. To address this, further research is needed in the following directions: (i) Lightweight cryptographic constructions tailored for constrained devices; (ii) Outsourcing techniques that offload heavy computation to fog or cloud nodes while preserving data confidentiality; (iii) Optimized key management and search mechanisms that reduce overhead.

  Developing such lightweight and efficient ABE-SE frameworks is essential for enabling secure, real-time data sharing and search in IoT and IoMT ecosystems.
- **Multi-Authority Environments:** Multi-Authority ABE (MA-ABE) enhances system flexibility, scalability, and decentralization by allowing multiple independent authorities to issue and manage user attributes. This is especially valuable in large-scale, distributed environments such as healthcare, smart cities, or federated IoT networks, where no single authority governs all users or data sources.

  However, integrating SE into MA-ABE frameworks introduces new challenges. Coordinating secure and efficient keyword search across multiple attribute authorities without revealing sensitive data or access structures is inherently complex. Additionally, MA-ABE already requires mechanisms for inter-authority trust, attribute validation, and key management, and layering SE on top of this increases the risk of High computational and communication overhead, Coordination complexity among authorities, and Potential privacy leaks during search operations.

Despite its potential, this integration remains underexplored. Research is still needed to design lightweight, privacy-preserving, and scalable SE mechanisms that can function effectively within multi-authority ABE settings—without sacrificing usability, performance, or security.

- **Forward and Backward Privacy:** Preventing information leakage from both past and future queries and data updates is a critical concern. Ensuring forward/backward privacy is still inadequately addressed in ABE schemes that support SE. Developing robust solutions that provide these privacy guarantees remains an open and important area of research.
- **Formal Security Models:** To our knowledge, there are no standardized frameworks or models for jointly evaluating the security of ABE schemes that support SE. Existing proposals often lack rigorous, composable security definitions and formal proofs that comprehensively cover both access control and search functionality. Establishing unified, robust security models is essential for advancing the practical deployment of ABE-SE systems.

4 Related Works and Justification for Our Work

This section presents a review of recent surveys relevant to our area of investigation and establishes the motivation for conducting the present study.

Rasori et al. [51] survey ABE schemes designed for IoT applications. Penuelas-Angulo et al. [52] focus on the revocation mechanisms in ABE schemes within the context of fog-enabled IoT environments. Sravya et al. [53] provide a comprehensive analysis of lattice-based ciphertext-policy ABE (LCP-ABE) schemes, with an emphasis on post-quantum security.

Although these surveys make significant contributions within their respective sub-domains of ABE, none address the integration of ABE with searchable encryption—a feature of growing importance in applications requiring fine-grained access control over encrypted data, along with efficient keyword search capabilities. Over the past five years, there has been a marked increase in research activity focused on attribute-based searchable encryption (ABSE), reflecting its relevance in emerging data security paradigms.

To the best of our knowledge, no existing survey (published by IEEE, ACM, Elsevier or Springer) offers a dedicated and systematic overview of ABSE schemes. This motivates our work, which aims to fill this critical gap by providing a comprehensive and up-to-date survey of recent advancements in ABSE. Our survey consolidates the literature, identifies key trends and design challenges, and serves as a reference point for future research in this area.

5 Conclusion

Attribute-Based Encryption (ABE) offers a powerful framework for fine-grained, attribute-based access control. However, its practical deployment in real-world systems faces significant challenges across multiple dimensions, including efficiency, security, scalability, usability, and integration with existing infrastructures. Designing efficient ABE schemes that also support Searchable Encryption is particularly complex.

In this paper, we present a comprehensive and critical survey of recent research developments in ABE schemes that support Searchable Encryption, as documented in the literature. We evaluate the strengths and limitations of various approaches, emphasizing their practical applicability while highlighting unresolved challenges that continue to drive future research in this area.

In the past five years, research on ABSE has grown significantly, highlighting its importance in modern data security. Yet, to our knowledge, no survey from major publishers (IEEE, ACM, Elsevier, Springer) has provided a focused and systematic review of ABSE. This work addresses that gap by presenting a comprehensive, up-to-date survey that summarizes existing literature, highlights key trends and challenges, and offers a reference for future studies.

Acknowledgement: No support was received from any source.

Funding Statement: No external funding were received for this.

Availability of Data and Materials: No data was used for this paper.

Ethics Approval: No human or animal subjects were used.

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); 2007 May 20–23; Berkeley, CA, USA: IEEE. 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; 2006 Oct 30–Nov 3; Alexandria, VA, USA: ACM. 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. Berlin/Heidelberg, Germany: 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); 2010 Apr 10–13; Beijing, China: ACM. p. 60–9.
9. Boneh D, Shoup V. A Graduate course in applied cryptography; 2020 [Online]. [cited 2025 Oct 29]. Available from: https://crypto.stanford.edu/$\sim$dabo/cryptobook/BonehShoup$\delimiter"0383383$_0$\delimiter"0383383$_5.pdf.
10. Boneh D, Lynn B, Shacham H. Short signatures from the weil pairing. J Cryptol. 2004 Jul;17(4):297–319. doi:10.1007/s00145-004-0314-9.
11. Peikert C. A decade of lattice cryptography. Found Trends Theor Comput Sci. 2016;10(4):283–424. doi:10.1561/0400000074.
12. Ajtai M. Generating hard instances of lattice problems (extended abstract). In: Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing, STOC '96; 1996 May 22–24; Philadelphia, PA, USA. New York, NY, USA: Association for Computing Machinery. p. 99–108. doi:10.1145/237814.237838.
13. Li J, Lin X, Zhang Y, Han J. KSF-OABE: outsourced attribute-based encryption with keyword search function for cloud storage. IEEE Trans Serv Comput. 2017;10(5):715–25. doi:10.1109/tsc.2016.2542813.
14. Zheng Q, Xu S, Ateniese G. VABKS: verifiable attribute-based keyword search over outsourced encrypted data. In: Proceedings of IEEE INFOCOM 2014-IEEE Conference on Computer Communications; 2014 Apr 27–May 2; Toronto, ON, Canada. p. 522–30.

15. Michalas A. The lord of the shares: combining attribute-based encryption and searchable encryption for flexible data sharing. In: Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing, SAC '19; 2019 Apr 8–12; New York, NY, USA: Association for Computing Machinery. p. 146–55. doi:10.1145/3297280.3297297.
16. Wang S, Jia S, Zhang Y. Verifiable and multi-keyword searchable attribute-based encryption scheme for cloud storage. IEEE Access. 2019;7:50136–47. doi:10.1109/access.2019.2910828.
17. Eltayieb N, Elhabob R, Hassan A, Li F. An efficient attribute-based online/offline searchable encryption and its application in cloud-based reliable smart grid. J Syst Archit. 2019;98:165–72. doi:10.1016/j.sysarc.2019.07.005.
18. Bakas A, Michalas A. Modern Family: a revocable hybrid encryption scheme based on attribute-based encryption, symmetric searchable encryption and sgx. In: Chen S, Choo K-KR, Fu X, Lou W, Mohaisen A, editors. Proceedings of Security and Privacy in Communication Networks. Cham, Switzerland: Springer International Publishing; 2019. p. 472–86. doi:10.1007/978-3-030-37231-6_28.
19. Miao Y, Ma J, Liu X, Li X, Jiang Q, Zhang J. Attribute-based keyword search over hierarchical data in cloud computing. IEEE Trans Serv Comput. 2020;13:985–98. doi:10.1109/tsc.2017.2757467.
20. Yu Y, Shi J, Li H, Li Y, Du X, Guizani M. Key-policy attribute-based encryption with keyword search in virtualized environments. IEEE J Sel Areas Commun. 2020;38(6):1242–51. doi:10.1109/jsac.2020.2986620.
21. Morales-Sandoval M, Cabello MH, Marin-Castro HM, Compean JLG. Attribute-based encryption approach for storage, sharing and retrieval of encrypted data in the cloud. IEEE Access. 2020;8:170101–16. doi:10.1109/access.2020.3023893.
22. He K, Guo J, Weng J, Weng J, Liu JK, Yi X. Attribute-based hybrid boolean keyword search over outsourced encrypted data. IEEE Trans Dependable Secure Comput. 2020;17(6):1207–17. doi:10.1109/tdsc.2018.2864186.
23. Sun X, Wang H, Fu X, Qin H, Jiang M, Xue L, et al. Substring-searchable attribute-based encryption and its application for IoT devices. Digit Commun Netw. 2021;7(2):277–83. doi:10.1016/j.dcan.2020.07.008.
24. Miao Y, Deng RH, Liu X, Choo K-KR, Wu H, Li H. Multi-authority attribute-based keyword search over encrypted cloud data. IEEE Trans Dependable Secure Comput. 2021;18(4):1667–80. doi:10.1109/tdsc.2019.2935044.
25. Chaudhari P, Das ML. Privacy preserving searchable encryption with fine-grained access control. IEEE Trans Cloud Comput. 2021;9(2):753–62. doi:10.1109/tcc.2019.2892116.
26. Liu J, Li Y, Sun R, Pei Q, Zhang N, Dong M, et al. EMK-ABSE: efficient multikeyword attribute-based searchable encryption scheme through cloud-edge coordination. IEEE Internet Things J. 2022;9(19):18650–62. doi:10.1109/jiot.2022.3163340.
27. Zhao F, Peng C, Xu D, Liu Y, Niu K, Tang H. Attribute-based multi-user collaborative searchable encryption in COVID-19. Comput Commun. 2023;205:118–26. doi:10.1016/j.comcom.2023.04.003.
28. Zhang Y, Zhu T, Guo R, Xu S, Cui H, Cao J. Multi-keyword searchable and verifiable attribute-based encryption over cloud data. IEEE Trans Cloud Comput. 2023;11(1):971–83. doi:10.1109/tcc.2023.3312918.
29. Khan S, Khan S, Waheed A, Mehmood G, Zareei M, Alanazi F. An optimized dynamic attribute-based searchable encryption scheme. PLoS One. 2024;19(10):e0268803. doi:10.1371/journal.pone.0268803.
30. Rao YS, Prasad S, Bera S, Das AK, Susilo W. Boolean searchable attribute-based signcryption with search results self-verifiability mechanism for data storage and retrieval in clouds. IEEE Trans Serv Comput. 2024;17(4):1382–99. doi:10.1109/tsc.2023.3327816.
31. Su J, Zhang L, Mu Y. BA-RMKABSE: blockchain-aided ranked multi-keyword attribute-based searchable encryption with hiding policy for smart health system. Future Gener Comput Syst. 2022;132:299–309. doi:10.1016/j.future.2022.01.021.
32. Zhang K, Zhang Y, Li Y, Liu X, Lu L. A blockchain-based anonymous attribute-based searchable encryption scheme for data sharing. IEEE Internet Things J. 2024;11(1):1685–97. doi:10.1109/jiot.2023.3290975.
33. Niu S, Chen L, Wang J, Yu F. Electronic health record sharing scheme with searchable attribute-based encryption on blockchain. IEEE Access. 2020;8:7195–204. doi:10.1109/access.2019.2959044.
34. Liu J, Wu M, Sun R, Du X, Guizani M. BMDS: a blockchain-based medical data sharing scheme with attribute-based searchable encryption. In: Proceedings of ICC 2021—IEEE International Conference on Communications; 2021 Jun 14–23; Montreal, QC, Canada. p. 1–6.

35. Xiang X, Zhao X. Blockchain-assisted searchable attribute-based encryption for e-health systems. J Syst Archit. 2022;124(6):102417. doi:10.1016/j.sysarc.2022.102417.
36. Yan Z, Zhang B. An efficient attribute-based multi-keyword searchable encryption with access policy hiding in iot using blockchain. IEEE Internet Things J. 2025;12(5):32148–60. doi:10.1109/jiot.2025.3575802.
37. Guo L, Li Z, Yau W-C, Tan S-Y. A decryptable attribute-based keyword search scheme on ehealth cloud in internet of things platforms. IEEE Access. 2020;8:26 107–18. doi:10.1109/access.2020.2971088.
38. Walid R, Joshi KP, Geol Choi, S, Kim D-Y. Cloud-based encrypted EHR system with semantically rich access control and searchable encryption. In: Proceedings of 2020 IEEE International Conference on Big Data (Big Data); 2020 Dec 10–13; Atlanta, GA, USA. p. 4075–82.
39. 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.
40. Chaudhari P, Das ML. KeySea: keyword-based search with receiver anonymity in attribute-based searchable encryption. IEEE Trans Serv Comput. 2022;15(2):1036–44. doi:10.1109/tsc.2020.2973570.
41. 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.
42. Chen L, Xu S, Jin C, Zhang H, Weng J. Partially hidden policy attribute-based multi-keyword searchable encryption with verification and revocation. IEEE Trans Mob Comput. 2025;24(9):9020–35. doi:10.1109/tmc.2025.3558955.
43. Chen L, Xu S, Zhang H, Weng J. Fair-and-exculpable-attribute-based searchable encryption with revocation and verifiable outsourced decryption using smart contract. IEEE Internet Things J. 2025;12(4):4302–17. doi:10.1109/jiot.2024.3484227.
44. Ghopur D, Ma J, Ma X, He F, Liu K, Jiang T, et al. Decentralized multiauthority attribute-based searchable encryption for e-health cloud. IEEE Internet Things J. 2025;12(11):15 723–35. doi:10.1109/jiot.2025.3529480.
45. Varri US, Kasani S, Pasupuleti SK, Kadambari KV. FELT-ABKS: fog-enabled lightweight traceable attribute-based keyword search over encrypted data. IEEE Internet Things J. 2022;9(10):7559–71. doi:10.1109/jiot.2021.3139148.
46. Niu S, Hu Y, Zhou S, Shao H, Wang C. Attribute-based searchable encryption in edge computing for lightweight devices. IEEE Syst J. 2023;17(3):3503–14. doi:10.1109/jsyst.2023.3283389.
47. Wang S, Yao L, Chen J, Zhang Y. KS-ABESwET: a keyword searchable attribute-based encryption scheme with equality test in the internet of things. IEEE Access. 2019;7:80675–96. doi:10.1109/access.2019.2922646.
48. Yin H, Zhang W, Deng H, Qin Z, Li K. An attribute-based searchable encryption scheme for cloud-assisted IIoT. IEEE Internet Things J. 2023;10(12):11014–23. doi:10.1109/jiot.2023.3242964.
49. Zhang X, Mu D, Zhao J. Attribute-based keyword search encryption for power data protection. High-Confid Comput. 2023;3(2):100115. doi:10.1016/j.hcc.2023.100115.
50. Liu X, Lu T, He X, Yang X, Niu S. Verifiable attribute-based keyword search over encrypted cloud data supporting data deduplication. IEEE Access. 2020;8:52062–74. doi:10.1109/access.2020.2980627.
51. Rasori M, Manna ML, 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.
52. 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.
53. Sravya G, Kumar PS, Padmavathy R. Survey of post-quantum lattice-based ciphertext-policy attribute-based encryption schemes for cloud storage: taxonomy, open issues, and future directions. IEEE Trans Serv Comput. 2024;17(6):4540–57. doi:10.1109/tsc.2024.3479930.