electronics

MDPI

Review

Attribute-Based Searchable Encryption: A Survey

Li Yan [1], Gaozhou Wang [1], Tian Yin [2,*], Peishun Liu [2,*], Hongxin Feng [2], Wenbin Zhang [1], Hailin Hu [1] and Fading Pan [1]

[1] Information and Telecommunication Company, State Grid Shandong Electric Power Company, Jinan 250013, China
[2] College of Information Science and Engineering, Ocean University of China, Qingdao 266400, China
* Correspondence: yintian@stu.ouc.edu.cn (T.Y.); liups@ouc.edu.cn (P.L.)

Abstract: With the advent of the big data era, the size and complexity of data continue to increase, which makes the requirement for data privacy and security increasingly urgent. However, traditional encryption methods cannot meet the demand for efficient searching in large-scale datasets. To solve this problem and enable users to search within encryped data and without decrypting the entire dataset, trapdoor functions and other cryptograhic techniques are introduced in searchable encryption. However, searchable encryption still cannot meet the needs in the real world. Therefore, researchers have introduced the concept of attribute-based encryption into searchable encryption, resulting in attribute-based searchable encryption (ABSE). This approach aims to achieve efficient search by attributes in encrypted datasets. ABSE has a wide range of applications in the fields of privacy protection, data sharing, and cloud computing. In this paper, we describe the trends in development, focusing on enhancing security, improving computational efficiency, and increasing flexibility. We also present the related schemes. In addition, several common application areas are introduced and the relevant schemes proposed by researchers are summarized. Moreover, the challenges and future directions of ABSE are discussed in this paper.

Keywords: attribute-based encryption; searchable encryption; attribute-based searchable encryption; privacy preservation; data sharing; cloud computing

Citation: Yan, L.; Wang, G.; Yin, T.; Liu, P.; Feng, H.; Zhang, W.; Hu, H.; Pan, F. Attribute-Based Searchable Encryption: A Survey. *Electronics* **2024**, *13*, 1621. https://doi.org/10.3390/electronics13091621

Academic Editor: Paris Kitsos

Received: 20 March 2024
Revised: 18 April 2024
Accepted: 22 April 2024
Published: 24 April 2024

1. Introduction

The smart grid represents an advanced evolution of the traditional electrical grid, incorporating advanced communication, control, and information technologies. These advancements enable real-time monitoring, precise control, and efficient optimization of power distribution. Integrating numerous sensors, communication devices, and intelligent control equipment, the smart grid monitors and manages various aspects of the power system.

In cloud computing and big data environments, outsourcing smart grid system data to cloud servers is cost-effective. While the power grid system stores a large amount of sensitive information, to prevent external attacks and protect user privacy, the current effective approach is to encrypt the data for data owners before uploading it to the server and to download and decrypt it for data users when needed.

After data are encrypted, they lose plaintext characteristics, making it difficult for users to efficiently search. Therefore, it is crucial to devise methods for searching encrypted data stored in the cloud. Searchable encryption (SE) methods offer effective solutions to encrypted data searches. In 2000, Song et al. [1] proposed a Searchable Symmetric Encryption (SSE) scheme based on symmetric encryption, which enables keyword search capabilities on encrypted data while only returning results matching the search criteria. In 2004, Boneh et al. [2] introduced a scheme called public-key encryption with keyword search (PEKS), employing public key cryptographic techniques. Subsequently, numerous searchable encryption techniques emerged, enhancing the security and efficiency of algorithms [3].

These searchable encryption methods cannot achieve fine-grained access control for multiple users. Attribute-based encryption (ABE) addresses this issue by providing fine-grained access control policies. ABE originates from identity-based encryption (IBE) schemes, with its predecessor being the fuzzy identity binary encryption (FIBE) scheme proposed by Sahai et al. [4] in 2005. In 2006, Goyal et al. [5] introduced the key-policy attribute-based encryption (KP-ABE) scheme based on FIBE, while Bethencourt et al. [6] implemented the ciphertext-policy attribute-based encryption (CP-ABE) scheme. These two schemes are widely recognized as the two fundamental mechanisms of ABE. ABE offers flexible and fine-grained access control mechanisms, allowing data sharing while maintaining data security. Moreover, users can decrypt data using attributes without disclosing their identity, effectively protecting user privacy.

In order to achieve efficient searching and access control mechanisms while ensuring data security and privacy, some researchers have proposed Attribute-Based Searchable Encryption (ABSE) schemes by integrating the concept of ABE. Therefore, the current searchable encryption techniques are commonly classified into symmetric searchable encryption, asymmetric searchable encryption, and ABSE.

In 2013, Wang et al. [7] proposed an Attribute-Based Public Key Searchable Encryption scheme based on CP-ABE, which combines ABE and PEKS to realize ciphertext retrieval with access control policies. They also presented a construction scheme based on bilinear pairings and demonstrated that the scheme can resist both internal and external attacks. In 2014, Zheng et al. [8] proposed a verifiable attribute-based keyword search (VABKS) scheme. In this scheme, the attribute encryption mechanism ensures that data owners can specify access control policies, providing decryption and searching permissions to data users who satisfy the attribute requirements. While searchable encryption technology achieves retrieval of ciphertext data and it is applicable to scenarios with high requirements for data security in power grid or medical systems.

1.1. Related Work

With the widespread application of outsourced cloud services, the demand for secure and efficient searching over encrypted data has been increasing. As a result, many optimized SE schemes have emerged. Some researchers have summarized and discussed these schemes, resulting in a number of review articles. In 2018, Varri et al. [3] classified SE schemes into symmetric, public-key, and attribute-based searchable encryption schemes. As shown in Figure 1, we conducted a detailed analysis based on index functionality and search capability. In 2022, Andola et al. [9] analyzed the current SE schemes in terms of their technical aspects and key performance indicators and conducted a comprehensive study on the robustness against attacks.

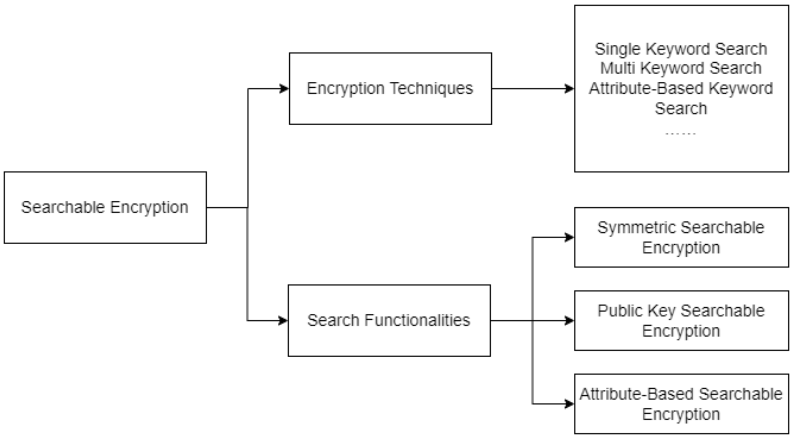

Figure 1. Taxonomy of searchable encryption.

1.2. Main Contributions

There are also many review articles on ABE. In 2016, Sookhak et al. [10] classified ABE into three categories based on its architecture, centralized, decentralized, and hierarchical, and pointed out their advantages and disadvantages. In 2018, Kumar et al. [11] conducted an in-depth exploration of CP-ABE, focusing on aspects such as hidden policies, proxy re-encryption, revocation mechanisms, and layered attribute encryption. Recently, there have been some reviews and schemes [12,13] related to ABE technology.

Although after 2014, a substantial amount of research on ABSE emerged, there is no comprehensive study that systematically reviews and summarizes ABSE.

This paper aims to explore the current state of ABSE in terms of security, efficiency, and expressiveness, focusing particularly on its applications in the IoT, such as smart grids, and in healthcare. We also aim to identify potential research directions in this field. The paper provides an overview of the recent development of ABSE, highlighting the following main contributions:

1. Detailed discussion on the current status and trends of ABE research from the aspects of enhancing security, improving computational efficiency, and enhancing flexibility.
2. Summarization of the common application domains of ABSE, such as smart grids, healthcare, and the Internet of Things (IoT), along with relevant schemes.
3. Discussion on the challenges and future directions of ABSE development.

1.3. Research Methodology

To delve into the recent advancements of ABSE in the fields of IoT and healthcare applications, we employed a systematic approach. Initially, we conducted searches in academic databases such as IEEE Xplore, Scopus, and Web of Science. The search query consisted of keywords including "Attribute-Based Searchable Encryption" or those simultaneously containing "Attribute-Based Encryption" and "Searchable Encryption", ensuring their presence in the title, abstract, or keywords of the literature. This methodology ensured the retrieval of research closely related to ABSE. As such, the main research query used was:

(*Attribute-Based Searchable Encryption*) *OR* (*Attribute-Based Encryption AND Searchable Encryption*)

The search was conducted in April 2024, and Table 1 presents the number of research publications obtained in each searched database. A total of 923 results were returned.

Table 1. Number of search results obtained in each academic database.

Database	N of Results
IEEE Xplore	245
Web of Science	383
Elsevier ScienceDirect	295
Total	923

It can be observed that ABSE is a popular research topic, necessitating the need for some restrictions to retrieve the required articles. It is necessary to undergo another screening process to establish a set of inclusion and exclusion criteria, as shown in the Table 2.

After applying the inclusion and exclusion criteria, 46 papers were found to meet the requirements. Therefore, we selected these 46 papers as the subject of our analysis.

1.4. Organization

The paper introduces ABSE in Section 2, elaborates on its development progress in security, computational efficiency, and flexibility in Sections 3–5, outlines common application domains and related implementation schemes in Section 6, briefly discusses future challenges and development directions in Section 7, and concludes the paper in Section 8.

Table 2. Inclusion and exclusion criteria.

Type of Criterion	Criterion ID	Description
Inclusion	IC1	Focuses on researching ABSE schemes and belongs to the computer science or cryptography field.
	IC2	Written in English.
	IC3	Published after 2018.
	IC4	Has an impact factor of 5.0 or above.
Exclusion	EC1	Not relevant to the research content of this paper.
	EC2	Written in languages other than English.
	EC3	Has a low impact factor.
	EC4	Published before 2018.

2. Attribute-Based Searchable Encryption

2.1. Introduction to Attribute-Based Searchable Encryption

ABSE is a searchable encryption scheme that allows data encryption based on data attributes. It primarily addresses the balance between data privacy protection and data search functionality, enabling efficient searching and access control mechanisms while ensuring data security and privacy.

ABSE is mainly divided into two categories: key-policy ABSE (KP-ABSE) and ciphertext-policy ABSE (CP-ABSE). These two strategies differ in key generation and encryption processes, providing different levels of flexibility and control methods to meet the requirements of various security aspects and access control. In CP-ABSE, keys are associated with a set of attributes, and documents and indexes are encrypted based on access policies. In KP-ABSE, keys are associated with access policies, and documents and indexes are encrypted using a set of attributes.

2.2. Syntax of Attribute-Based Searchable Encryption

ABSE typically involves four types of entities: the data owner (DO), data user (DU), cloud server (CS), and trusted application (TA). The TA initializes the system and generates public keys or key pairs for the DO and DU. The DO encrypts files, establishes secure indexes, and uploads ciphertexts to the CS. The DU can search encrypted files and access encrypted files when authorized. The CS provides various services, including data storage, computation, and retrieval. The DU encrypts keywords into search traps and uploads them to the CS for matching, and then the CS returns the corresponding query results, as illustrated in Figure 2.

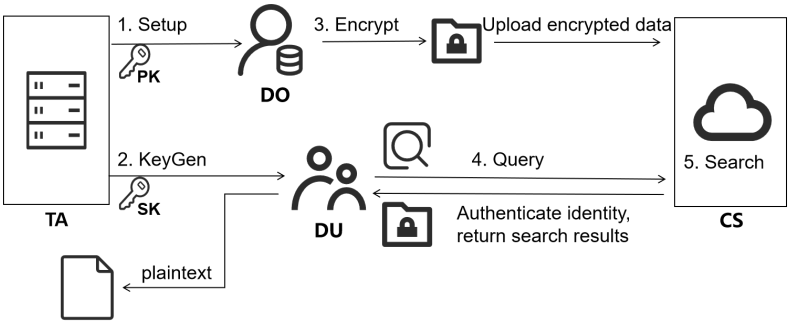

Figure 2. ABSE process.

An ABSE scheme typically consists of five algorithms, all of which are polynomial-time algorithms over the keyword set W:

$Setup(\lambda, U) \rightarrow (PK, MK)$: The TA executes this algorithm. Given the security parameters λ and the set of attributes U as input, it outputs the public parameters PK and the master secret key MK.

$KeyGen(PK, MK, S) \rightarrow sk$: The TA executes this algorithm. Given PK,MK, and the user's attributes set S as input, and it outputs the user's secret key sk.

$Enc(W, P) \rightarrow C_W$: The DO executes this algorithm. Given the set of keywords W and the access policy P as input, it encrypts the set of keywords W using the access policy P to obtain ciphertext C_W.

$Trapdoor(sk, \omega) \rightarrow T_\omega$: The DU executes this algorithm. This algorithm generates a trapdoor T_ω based on the user's identity sk and keywords ω.

$Query(C_W, T_\omega) \rightarrow b$: CS executes this algorithm. If the keywords in the index C_ω match the keywords in the trapdoor T_ω, the algorithm returns $b = 1$; otherwise, it returns $b = 0$.

Next, we will introduce the development progress of ABSE in terms of security, computational efficiency, and flexibility.

3. Enhanced Security

As a crucial privacy protection technology, ABSE continues to attract attention from researchers. This section mainly introduces the progress of ABSE schemes in enhancing privacy protection and optimizing access control techniques. Additionally, common security models are discussed, and recent ABSE schemes are summarized.

3.1. Enhanced Privacy Protection

The ABSE scheme aims to protect users' privacy and ensure that searching encrypted data does not leak sensitive information. In recent years, researchers have proposed more secure ABSE schemes, and the following techniques are commonly used to enhance privacy protection:

3.1.1. Policy Hiding

In the CP-ABE scheme [6] proposed, the access policies, in plaintext form, are embedded into the data ciphertext. Anyone who obtains the data ciphertext, regardless of whether they have decryption permissions, can access the contents of the access policies. Attackers may exploit access policies to gather relevant information, potentially leading to privacy breaches and identity theft. Therefore, policy hiding techniques are one of the important means of privacy protection.

Policy hiding is mainly divided into two categories: partial policy hiding and full policy hiding. Partial policy hiding includes schemes such as wildcard substitution and attribute name-value separation, while complete policy hiding primarily employs the inner product encryption (IPE) mechanism.

In 2008, Nishide et al. [14] proposed the concept of partial policy hiding and provided a scheme implementation using wildcard substitution. However, it only supports the "AND" gate structure and can only be proved secure in the random oracle model. In 2011, Lai et al. [15] made improvements based on Nishide et al. [14] using the IPE mechanism to implement a full policy-hiding CP-ABE scheme. However, this scheme still only supports the "AND" gate access control structure, and the length of the ciphertext linearly increases with the number of attributes in the access control policy. In 2010, Balu et al. [16] proposed a full policy-hiding ABE scheme based on access control trees, but it is prone to problems such as excessive iteration levels when the access control policy is complex. In 2012, Lai et al. [17] achieved partial policy hiding of access policies by separating each attribute into attribute names and values, introducing an adaptive secure partial policy hiding scheme based on a linear secret sharing scheme (LSSS) access structure for the first time. In 2018, Zhang et al. [18] reduced some redundant operations based on Lai's work [17], improving the efficiency of encryption and decryption. However, since this scheme still uses the composite-order bilinear group, the overall efficiency remains relatively low.

In ABSE systems, policy hiding is also crucial for enhancing security. In 2013, Koo et al. [19] proposed an ABSE scheme that implements access policy hiding, supporting fast ciphertext search and rich access policy expressions. However, later research [20] proved its insecurity.

In 2014, Shi et al. [21] used an LSSS structure to hide access policies, which is a low-cost method for protecting access policies. However, it requires a large number of bilinear pair calculations when generating search tokens. In 2020, Wang et al. [22] proposed a scheme with hidden access policies and optimized search performance. This scheme is multi-value independent, with unchanged storage overhead, but its search capability is limited, only supporting single-keyword search. In the same year, Chaudhari et al. proposed KeySea [23], which hides access policies and optimizes search time. Regardless of the number of attributes in the access policy, the number of pairing operations is minimized and constant. The time complexity for searching documents with a single index is constant, and for searching documents with multiple indexes, it is linear. In 2021, Miao et al. [24] proposed the ABKS-SM system, which can protect privacy by hiding access policies in shared multi-owner settings and tracking malicious DUs. However, a study [25] indicated that the ABKS-SM scheme cannot resist the claimed offline keyword guessing attack.

3.1.2. Keyword Privacy Protection

When the access policy of a system is not robust enough and the entropy of keywords is relatively low, the ABSE system faces severe keyword guessing attacks (KGAs). In such attacks, attackers, upon obtaining the trapdoor, can detect the keywords used to generate it by guessing or exhaustively trying possible keywords. KGAs can be categorized into offline KGAs and online KGAs. Offline KGAs, proposed by Byun et al. [26], involve attackers pre-intercepting trapdoors and guessing the keywords contained in the trapdoor offline. The online KGA mainly refers to external attackers intercepting publicly transmitted keyword trapdoors. They use the server as an oracle to generate ciphertexts for guessed keywords and online monitoring of the server's return results to obtain the actual keywords contained in the keyword trapdoor.

In traditional PEKS schemes, a secure channel is required to transmit keyword trapdoors between the server and the recipient to prevent offline KGA by external attackers. However, building a secure channel incurs significant costs. To address this, Baek et al. [27] proposed the concept of public-key encryption with keyword search without a secure channel, primarily using the idea of signcryption to ensure indistinguishability and non-malleability. However, it was later proven to be unable to resist online KGAs and offline KGAs by internal attackers [28]. Jeong et al. [29] pointed out that the security vulnerability of PEKS is due to its consistency requirements. Rhee et al. [30] proposed the concept of trapdoor indistinguishability and constructed a trapdoor-secure dPEKS scheme. Although it is also unable to resist inside KGAs, it was the first to propose a secure dPEKS scheme against KGAs and formally prove the security of ciphertexts and trapdoor queries. In 2014, Wang et al. [31] proposed a system that utilizes two servers which cannot conspire with each other to resist inside KGAs. In 2017, Huang et al. [32] introduced the concept of public-key authenticated encryption with keyword search (PAEKS), where the data sender encrypts and authenticates keywords, and the server does not need to handle plaintext keywords, thus preventing internal KGAs.

In ABSE schemes, online attacks require direct interaction with the system and are easier to detect, current ABSE schemes mainly focus on resisting offline KGAs. Yu et al. [33] proposed a method to resist KGAs launched by outside adversaries utilizing the server's private key during trapdoor generation. However, this approach does not prevent KGAs from insiders. In 2016, Qiu et al. [34] proposed a secure CP-ABKS scheme that supports keyword search, hides access structure, and is resistant to KGAs. In 2021, Miao et al. [24] improved it and provided traceability. However, Sun et al. [25] pointed out that such models cannot resist four types of inside offline KGAs. In 2023, Luo et al. [35] proposed a new concept of attribute-based keyword search (ABAEKS) authenticated encryption and presented an effective ABAEKS scheme. By authenticating keywords, it can resist internal KGAs, and based on the learning with errors (LWE) assumption, it is widely regarded as resistant to quantum attacks.

3.2. Optimization of Access Control Techniques

Traceability and revocability are two crucial capabilities in access control techniques, often combined with the ABSE scheme to enhance its security and flexibility.

3.2.1. Traceability

Traceability refers to the ability of a system to trace the usage and access records of encrypted data, which can address data sharing issues. It is mainly divided into white-box traceability and black-box traceability. White-box traceability involves tracing malicious users based on known leaked keys, while black-box traceability is a stronger tracing concept that requires tracing decryption devices [36].

Traceability is a technique in ABE systems. In 2008, Hinek et al. [37] first proposed a system with traceability. In this system, the decryptor needs to interact with a trusted third-party agency during decryption, reducing the scalability and increasing computational overhead of the system. In 2009, Yu et al. [38] proposed achieving traceability in KP-ABE systems by embedding identity information in access policies. In 2011, Katz et al. [39] introduced the concept of traceability in predicate encryption. The following year, Liu et al. [40,41] proposed both white-box and black-box traceability methods and implemented selective tracing. However, the computational overhead of the traceable systems proposed by Katz and Liu based on predicate encryption increases linearly with the number of users, making the systems only suitable for environments with fewer users. In 2016, Lui et al. [42] proposed a black-box traceability scheme supporting large universe, but with high tracing costs and without forward security. In 2021, Ziegler et al. [43] proposed white-box decentralized traceability, while Luo et al. [44] proposed black-box traceability based on lattice cryptography, which has resistance against quantum attacks but with high computational overhead.

In recent years, the technologies combined with ABSE mainly focused on white-box traceability. In 2020, Yang et al. [45] proposed LiST, a lightweight mobile health system with shareable and traceable security. However, it requires well-formatted keys during decryption. In 2021, Miao et al. [24] proposed the ABKS-SM scheme in a shared multi-owner setting, achieving white-box traceability in the improved system but later found it unable to meet its claimed security. In the same year, Sun et al. [25] proposed an ABSE scheme in multi-authority settings capable of tracing malicious attribute management organizations. In 2022, Varri et al. [46] proposed the FELT-ABKS system, which supports traceability and transfers most computations to fog nodes to minimize computational overhead on the user side but still requires well-formatted keys.

3.2.2. Revocability

Revocability refers to the capability to revoke granted access permissions or sharing privileges for encrypted data, often combined with traceability. Revocability includes user-level revocation and attribute-level revocation, which can be achieved through direct revocation, indirect revocation, or hybrid revocation. In direct revocation, the DO executes revocation, while in indirect revocation, authorities or third parties perform the revocation. Hybrid revocation involves a combination of indirect and direct revocation methods.

In 2006, Pirretti et al. [47] first proposed an attribute revocation encryption algorithm using timestamps to set expiration periods, but this method requires interaction with an authority center, increasing the system's communication overhead. In 2007, Ostrovsky et al. [48] introduced a CP-ABE scheme with direct revocation, where the user's identity ID information serves as an attribute, and revoking a user involves adding the user's ID as a negative attribute to the access structure, thereby denying access to encrypted data. However, this scheme incurs significant overhead. In 2009, to address computational overhead issues, Attrapadung et al. [49] proposed a broadcast ABE system that maintains a user list to provide hybrid revocability, but it only supports user revocation, not attribute revocation. In 2018, Wang et al. [50] utilized attribute group keys to achieve direct attribute revocation, but it incurred high computational overhead and had security issues. To address

the limitations of the aforementioned schemes, Tu et al. [51] implemented a secure attribute revocation scheme in 2021, but the key updates also incurred high computational overhead. In 2020, Dong et al. [52] proposed a lattice-based revocation scheme with resistance to quantum attacks. In 2021, Wei et al. [53] introduced an ABE scheme supporting dynamic user revocation with low overhead and high security, but user revocation cannot be executed immediately. In 2022, Zhang et al. [54] provided a key escrow-free CP-ABE scheme with the user revocation. In 2023, Chen et al. [55] provided an efficient and revocable ABE scheme with data integrity, while they did not implement more fine-grained revocation.

In ABSE, revocability enables DO or authorities to revoke access permissions, restricting further data access. This flexibility enhances data access management, control, and security and improves overall privacy protection. In the past five years, several papers have implemented revocability in ABSE, often outsourcing some operations to CS to improve system efficiency.

In 2022, Bao et al. [56] achieved indirect revocation by constructing a binary tree to restrict revoked users' access permissions, but the computation is complex. In the same year, Varri et al. [46] proposed FELT-ABKS, supporting white-box traceability and attribute revocation at fog nodes, significantly improving system speed, but it cannot be used for user revocation. Schemes [45,57] implemented user-level revocation using user revocation lists maintained on the CS. Schemes [58,59] implemented user-level revocation based on blockchain technology. However, none of them support attribute revocation. In 2023, Yu et al. [60] proposed decentralized user revocation and attribute updates (revocation).

3.3. Security Models

With the continuous advancement and development of computing capabilities, encryption schemes need to have sufficient security to withstand increasingly powerful computational resources. Security models serve as a framework or specification used in the fields of cryptography and information security to describe and evaluate the security attributes and performance of a secure system or algorithm. Security models define the capabilities of attackers, attack strategies, and system objectives to facilitate security analysis and the design of systems.

In this section, we mainly focus on the different attacks that may exist in SE schemes and the solutions proposed by different authors to avoid the following attacks. In recent years, common security models in the ABSE framework include KGAs, chosen keywords attack (CKA), chosen plaintext attack (CPA), chosen ciphertext attack (CCA), and so on. Table 3 provides an introduction.

Indistinguishability security (IND) is a common security objective, referring to the inability of attackers to infer any information about the plaintext from the ciphertext. Considering the attack goals and capabilities, different combinations yield different security definitions. For example, Chaudhari et al. [23] proposed an ABSE scheme with indistinguishability against ciphertext policy and chosen keyword attacks. Wang et al. [61] presented a scheme with IND-CK-CCA security, Yang et al. [62] introduced a randomized CCA scheme with indistinguishability. Liu et al. [63] proposed a scheme achieving indistinguishability against chosen keyword attacks, and Niu's [64] scheme satisfies indistinguishability security under chosen plaintext and CCAs. Table 3 illustrates a comparison of security properties for some recent ABSE schemes.

Table 3. Comparison of common security models.

Security Models	Description	Schemes
Chosen Plaintext Attack (CPA)	Attackers may choose random plaintexts that are encrypted to obtain the corresponding ciphertexts.	[46,58,64–66]
Chosen Ciphertext Attack (CCA)	Attackers can not only obtain ciphertext corresponding to plaintext but can also obtain plaintext corresponding to a limited number of ciphertexts.	[61,64]
Chosen Keywords Attack (CKA)	Attackers selectively target keywords to obtain the decryption of the chosen keywords.	[23,46,57,58,61,63–65,67,68]
Keyword Guessing Attack (KGA)	Attackers attempt to guess potential keywords and generate ciphertexts for testing.	[24,33,69,70]
Indistinguishability under CKA (IND-CKA)	In the CKA model, it is examined whether encryption algorithms can achieve indistinguishability of ciphertexts.	[23,61,63]
Indistinguishability under CPA (IND-CPA)	In the CPA model, it is examined whether encryption algorithms can achieve indistinguishability of ciphertexts.	[64]
Indistinguishability under CCA (IND-CCA)	In the CCA model, it is examined whether encryption algorithms can achieve indistinguishability of ciphertexts.	[61,62,64]

3.4. Discussion

ABSE leads in privacy protection technologies, with security research focusing on policy hiding, resistance against keyword guessing attacks, and access control optimization. Table 4 provides a comparison of the security of recent ABSE systems. Currently, most schemes are built on the bilinear pairing assumption, which may be vulnerable to quantum computing attacks, considering ABSE systems resilient to quantum attacks will be one of the important directions for improving security.

Table 4. Comparison of search security.

System	Publication Time	Policy Hiding	Traceability	Revocability	Security Model
[71]	2020	×	×	✓	CKA/CPA
[58]	2020	×	✓	✓	CPA/CKA
[22]	2020	✓	×	×	IND-CPA/CKA
[33]	2020	×	×	×	KGA/CKA
[24]	2021	×	✓	×	KGA
[51]	2021	×	×	✓	FS/BS [2]
[46]	2022	×	✓	✓	CKA/CPA
[23]	2022	✓	×	×	IND-CKA
[72]	2022	×	×	×	IND-CKA
[63]	2023	✓	×	×	IND-CKA
[57]	2023	×	×	✓	CKA
[64]	2023	×	×	✓	IND-CKA/CCA
[73]	2023	×	×	✓	CKA
[60]	2023	×	×	✓	RCCA [1]/CKA
[74]	2024	✓	×	×	IND-CPA/CKA
[57]	2024	×	×	✓	CKA

[1] RCCA means replayable chosen-ciphertext attack [75]. [2] FS means forward secrecy, BS means backward security.

4. Efficiency Improvement

To ensure security, ABSE technology often incurs significant computational overhead. Researchers have proposed various efficient computational ABSE schemes, including intro-

ducing outsourcing computation, online/offline encryption mechanisms, and optimizing index structures. These techniques can reduce search time and computational overhead, making ABSE more practical for real-world applications.

4.1. Outsourcing Computation

With the increasing popularity of cloud computing, cloud users can outsource data to the CS for storage and computation. This enables cloud users to leverage the advantages provided by cloud computing, reducing computational overhead on the user or terminal side and alleviating local computing burdens. In 2014, Zheng et al. [8] proposed ABKS and combined it with outsourcing computation to enhance search efficiency. Currently, outsourcing computation is widely used to improve the computational efficiency of ABSE.

When dealing with large and complex data computations, researchers need to consider algorithm simplification and other efficiency enhancement schemes. Simply outsourcing expensive operations like decryption to CS without considering system scalability and performance improvements may not achieve the expected results.

For example, Miao et al. [76] proposed precomputing intermediate ciphertexts in 2021 and combined them with outsourcing computation to the CS to achieve lightweight systems. Zhang et al. [77] proposed using tree structures to optimize queries in 2023. However, outsourcing computation involves handing sensitive data over to the CS for processing. Due to the honest-but-curious nature of the CS, while using outsourcing computation to improve efficiency, it is necessary to ensure the security of sensitive information, such as access policies. Recent proposals [45,60,64,65,78,79] have demonstrated their security while outsourcing expensive computations to the cloud.

For some application scenarios with high real-time requirements, low latency, and large bandwidth demands, relying solely on cloud computing may also fail to meet the requirements. For example, Varri et al. [46] proposed transferring the maximum computation load to fog nodes in 2022 to achieve minimal computing overhead at the user end. Solutions [68,80] transfer computing tasks to edge servers, leveraging edge resource advantages to improve computational efficiency and reduce latency.

4.2. Online/Offline Encryption Mechanism

The concept of the online/offline mechanism was first proposed by Even et al. [81] in 1990. In 2014, Hohenberger et al. [82] first combined the online/offline mechanism with ABE schemes in their OOABE scheme. In the offline phase, intermediate ciphertexts are pregenerated, allowing most computations to be performed offline. The online phase requires only a small amount of computation to generate the final ciphertext. However, it lacks high security. In 2015, Datta et al. [83] proposed the first fully secure online/offline predicate encryption. In 2018, Liu et al. [84] proposed an ABE scheme using an online/offline mechanism for sharing medical data. However, both schemes involve a large number of pairing and exponentiation operations at the decryption.

The online/offline mechanism is also used in ABSE systems to alleviate the computational burden on the encryption side. Recent schemes have considered the computational overhead at the decryption end. For example, the OO-KP-ABKS scheme proposed by Cui et al. [85] in 2019 and the ERPF-DS-KS scheme proposed by Bao et al. [79] in 2022 belong to the KP-ABSE schemes, while the MABKS scheme proposed by Miao et al. [76] in 2021 and the EMK-ABSE scheme proposed by Liu et al. [72] in 2022 belong to the CP-ABSE schemes. They all adopt online/offline mechanisms and outsourcing computation, reducing the computational resource pressure on the encryption side and the computational overhead on the decryption side. However, the online/offline encryption mechanism merely "transfers" some operations of ciphertext component generation to idle time, without actually reducing the consumption of computational resources and energy. Researchers still need to explore solutions to alleviate computational pressure in ABSE systems.

4.3. Index Structure Optimization

In ABSE, computational overhead mainly focuses on encryption/decryption algorithms and search algorithms. Optimizing index construction is crucial for improving search efficiency. Currently, inverted index and tree-based index construction are popular techniques for building efficient indexes.

In 2015, Wang et al. [86] introduced a tree-based index structure in searchable encryption to improve search efficiency, which has been commonly used in ABSE schemes. In 2016, Xia et al. [87] proposed a searchable encryption scheme based on tree-based index structure, supporting range searches and achieving sublinear search complexity. However, as the search data volume increases, the depth of the tree structure increases, leading to a decrease in search speed. To address this drawback of tree structure, Zhang et al. [77] proposed aggregating similar entities and designing index tree structure, updating dynamic index vectors only when the state changes, thereby achieving efficient search and index updates. Although tree structures can achieve sublinear search complexity and support range searches, they have a large space overhead and cannot support high-dimensional data.

The inverted index can compensate for this deficiency by constructing a set of pointers to documents for keywords, allowing for quick retrieval of documents based on user provided keywords, thereby reducing time costs and memory storage. In 2011, Curtmola et al. [88] first introduced the inverted index structure in searchable encryption, implementing an SSE scheme with sublinear complexity but with lower security. In 2013, Cash et al. [89] implemented an SSE scheme with inverted index structure but only considered a symmetric scenario, limiting its scalability in multi-user sharing scenarios. In 2021, Zhang et al. [90] introduced a new attribute-based authorization paradigm for inverted index scheme, achieving sublinear search complexity while addressing sharing issues among multiple users. In 2020, Yin et al. [91] applied inverted index in real-world data in an ABSE scheme, achieving sublinear search complexity. Although it did achieve the expected results, it incurred significant computational overhead in authorization and search processes. To address this issue, Yin et al. [92] recently proposed using XOR-linked inverted index and introduced a dynamic data update mechanism.

4.4. Discussion

To enhance the practical feasibility of ABSE, researchers have focused on addressing computational overhead issues, leading to the emergence of several efficiency-improving techniques. Currently, mainstream approaches include outsourcing computation, online/offline encryption, and index structure optimization. Table 5 provides a brief overview of the advantages and disadvantages of these three methods for improving computational efficiency, along with relevant ABSE schemes. With the rise of the IoT, there is an urgent need to achieve secure and efficient search on resource-constrained IoT devices. Researchers must continue to explore solutions that strike a balance between security and efficiency.

Table 5. Methods of efficiency enhancement.

Methods	Advantages	Disadvantages	Related ABSE Schemes
Outsourcing Computation	Leveraging the advantages of cloud computing to alleviate local computational burden	May result in partial decryption results without guaranteed correctness	[45,46,60,65,68,78–80]
Online/Offline Encryption	Reducing the computational burden on the encryption side	Does not necessarily reduce the total computational workload of encryption algorithms	[60,72,76,85,93]
Index Structure Optimization	Enhancing search efficiency through optimizing index structures	May incur significant space overhead	[88,90,92]

5. Enhanced Flexibility

In the ABSE system, flexibility is primarily manifested in its ability to support more elaborate access policy expressions and more complex search conditions. ABSE allows users to specify access policies and search conditions according to their own requirements.

5.1. Enhanced Search Capability

Search capability mainly includes single-keyword queries and multi-keyword queries. A single-keyword query refers to a query operation that uses a single keyword for searching. However, single-keyword queries are often insufficient to meet the increasingly complex user requirements. Multi-keyword queries are suitable for more complex and precise search demands. Researchers have further extended functionalities such as range queries and subset queries based on this.

Since 2000, Song et al. [1] introduced the concept of SSE, researchers have been extending it for single-keyword queries. It was not until 2004 when Golle et al. [94] first proposed the concept of conjunctive keyword search (CKS), which involves searching encrypted data containing several keywords in a single query. In the same year, Park et al. [95] defined a PEKS security model using conjunctive keyword search. Subsequently, a series of multi-keyword solutions emerged, including conjunctive queries, Boolean queries, range queries, and subset queries.

In the ABSE framework, authorized users can search encrypted data items that meet specific conditions by retrieving keywords. In 2014, Shi et al. [21] proposed an authorized keyword search scheme that supports arbitrary Boolean formula searches. It utilized a variant of a dual-policy ABE scheme with partially hidden access structures. However, this scheme is based on compound order bilinear groups, resulting in a large amount of computational overhead, and only supports single-user queries. In 2014, Zheng et al. [8] proposed an attribute-based verifiable keyword search scheme for encrypted data, which was carried out in a multi-user environment but only supported single-keyword search. Then, Zhang et al. [96] proposed support for Boolean queries in a multi-user setting. Cui et al. [85] and Miao et al. [67] respectively proposed ABSE schemes supporting conjunctive queries, but these two schemes are selectively secure rather than fully secure. In 2023, Huang et al. [97] implemented multi-keyword queries supporting AND, OR, NOT, and threshold value expressions, with sorting of results. Also in the same year, Miao et al. [57] proposed an electronic health system that can match users with specified intervals, but it does not support hidden access policies. Liu et al. [59] further proposed subset multi-keyword queries implemented on blockchain but also did not consider hidden access policies. Liu et al. [63] proposed subset multi-keyword retrieval, returning all files containing the searched multiple keywords, and implemented policy hiding.

5.2. Expressiveness Diversity

In ABSE, expressiveness typically refers to the diversity and complexity of query types and operations supported by the system. In this context, it specifically refers to the complexity of attributes and policies that the system can handle. In ABE systems, the expressiveness and flexibility of access policies are important metrics for evaluating systems. The access structure is the logical structure of access control policies. The earliest access structure, based on Shamir's (t, n) threshold structure [98], divides secret information into n secret shares, and a user must obtain at least t secret shares to reconstruct the shared secret information. However, its expressive power is too simplistic to express complex access policies. Subsequently, Goyal et al. [5] and Bethencourt et al. [6] constructed an access tree structure, treating "AND" operations as (n, n) thresholds and "OR" operations as $(1, n)$ thresholds, enabling access policies to support AND, OR, and threshold operations. However, their security proofs are based on generic group models. In 2007, Cheung et al. [99] achieved CP-ABE provable in the standard model, using AND gates on positive and negative attributes to construct a scheme that satisfies Boolean access policies. However, its expressiveness is not flexible enough. In 2011, Waters et al. [100] proposed an

LSSS matrix, also based on the idea of linear secret sharing schemes, mapping the access tree to an LSSS matrix, which can achieve AND, OR, and threshold expressions and is provably secure in the standard model.

Current ABSE schemes generally adopt the four aforementioned monotonic access structures [101] to achieve fine-grained access control and extend their applications based on these structures. For instance, Zhang et al. [96] implemented an access control policy scheme supporting AND conjunction based on a threshold structure. Inspired by programs [82,102], they implemented an authorized switch module that can update access policies non-interactively. However, its expressiveness is relatively limited. In 2022, Bao et al. [79] proposed a policy based on the LSSS structure supporting AND, OR, and threshold expressions and provided a rigorous proof. In 2023, Zhang et al. [66] proposed the ABCKS system, which was designed based on an access tree structure to support both AND and OR access policies.

Most comparisons between access policies and attributes are based on equality relationships and are rarely related to inequality relationships. Of course, a simple approach is to use equality relationships to express inequality relationships, but this would lead to a significant amount of additional computation and storage overhead. In 2018, Miao et al. [67] based on Xue's work [103] and used 0-encoding and 1-encoding to convert comparable attributes into strings, enabling the matching of attribute inequality relationships.

5.3. Support for Large Universe

ABE algorithms can be classified into two categories based on the size of the attribute domain: small universe and large universe. Traditional ABE algorithms require input of a certain attribute set, with the size and types of attributes established at system setup. If new attributes emerge after system initialization, they cannot be included in subsequent encryption and decryption algorithms, severely affecting the flexibility and scalability of the system.

In 2011, Bishop et al. [104] constructed a KP-ABE scheme that supports large universe and proved the scheme's selective security in the standard model. This scheme is the first true ABE scheme to support large universe characteristics. The distinguishing feature of supporting a wide range of patterns is that there is no need to pre-determine the set of properties during system setup. Attributes can be any string and can be added as needed during the operation of the scheme. In 2012, Bishop et al. [105] constructed another KP-ABE scheme which supports large universe and proved the scheme's adaptive security in the standard model. However, its access control policy expressiveness is limited, and it incurs significant computational overhead. In 2013, Rouselakis et al. [106] first constructed a CP-ABE scheme which supports large universe based on prime-order bilinear mappings and proved its plaintext-selective security.

In recent years, lots of new ABSE schemes support large universe, making the schemes more flexible. For example, schemes [23,62,72], among others, support large attribute domains.

5.4. Discussion

In summary, the flexibility of the ABSE framework lies primarily in its search capabilities, expressiveness, and support for large universe, which are closely related to the access structures of the schemes. The flexibility of different schemes in recent years is compared in Table 6. However, current research mainly focuses on equality searches, leaving inequality search problems unresolved. When facing more diverse and personalized search needs, researchers need to delve deeper into exploring new solutions to enhance the adaptability and flexibility of the ABSE framework in different scenarios.

Table 6. Comparison of flexibility.

Method	Year	Large Universe	Access Structure	Expression	Search Capabilities
[71]	2020	✓	Access tree	OR | AND | threshold	Multi-Keyword Search
[58]	2020	✓	LSSS	OR | AND | threshold	Single-Keyword Search
[33]	2020	✓	Access tree	OR | AND | threshold	Single-Keyword Search
[24]	2021	×	AND gate on multi-valued attributes	AND	Single-Keyword Search
[65]	2021	✓	AND gate on multi-valued attributes	AND	Multi-Keyword Search
[90]	2021	×	LSSS	OR | AND | threshold	Multi-Keyword Search
[46]	2022	×	LSSS	OR | AND | threshold	Multi-Keyword Search
[23]	2022	✓	AND gate on multi-valued attributes	AND	Single-Keyword Search
[61]	2022	✓	AND gate on multi-valued attributes	AND	Multi-Keyword Search
[72]	2022	✓	LSSS	OR | AND | threshold	Multi-Keyword Search
[63]	2023	×	IPE	AND	Multi-Keyword Search
[62]	2023	✓	LSSS	OR | AND | threshold	Single-Keyword Search
[63]	2023	✓	IPE	AND	Multi-Keyword Search
[68]	2023	✓	LSSS	OR | AND | threshold	Single-Keyword Search
[74]	2024	✓	AND gate on multi-valued attributes	AND	Single-Keyword Search
[57]	2024	✓	Access tree	OR | AND | threshold	Single-Keyword Search

6. Application Areas

With the rapid development of cloud computing technology, an increasing number of organizations are choosing to store user data in the cloud. These data often include personal information, such as healthcare records, sports data, behavioral information, and medical prescriptions. This poses security risks of data leakage and misuse. ABSE schemes are particularly suitable for data sharing scenarios such as the IoT and healthcare, providing data availability while also protecting the privacy of user data.

6.1. Smart Grid

In recent years, security and privacy issues in smart grids have received widespread research and attention. In 2010, Zhang et al. [107] proposed a security framework for smart grids, guiding the implementation of information security protection in various business systems of smart grids. There are some classic security solutions that address the security challenges in smart grids. For example, Rogers et al. [108] proposed an identity authentication and integrity protocol using timestamps and digital signatures.

Smart grids contain a large amount of power data, which may contain sensitive information on one hand, and involve multiple parties such as power supply companies, users, and energy management companies on the other hand. In the process of data sharing and authorization, it is also necessary to prevent privacy information leakage. This has led to increasing applications of ABE in smart grids. For example, Su et al. [109] proposed using ABE to ensure the privacy of electricity trading users in a distributed environment. Ge et al. [110] improved ABE control schemes and applied them to collaborative data control in smart grids based on the characteristics of grid transmission capabilities and collaborative access data. However, encrypted data are challenging. Most advanced searchable algorithms are designed for general text and cannot be applied to smart grids. To achieve search functionality based on data encryption, Li et al. [111] proposed a searchable encryption system based on symmetric encryption for protecting privacy data generated in smart grids.

To simultaneously achieve both searchability and access control capability, using ABSE is an optimal choice. Consider a smart grid scenario as illustrated below (shown as Figure 3), consisting of millions of smart meters connected to the grid. These smart

meters may contain user's electricity usage patterns, enterprises' electricity information, and information on the city's public facility electricity distribution, among other data. To protect privacy data and achieve fine-grained data sharing, ABSE can be used for encryption. For instance, in analyzing the electricity usage patterns of a specific area, a search token is uploaded to the smart grid cloud servers for matching. Only users whose attributes match the specified access policy can decrypt the data. Eltayieb et al. [112] proposed an attribute-based online/offline searchable encryption scheme, ABOOSE, which is deployed on smart grid servers to authorize users to search for electricity usage data. Thus, users can prevent issues such as manipulating electricity usage by checking their own electricity meter readings.

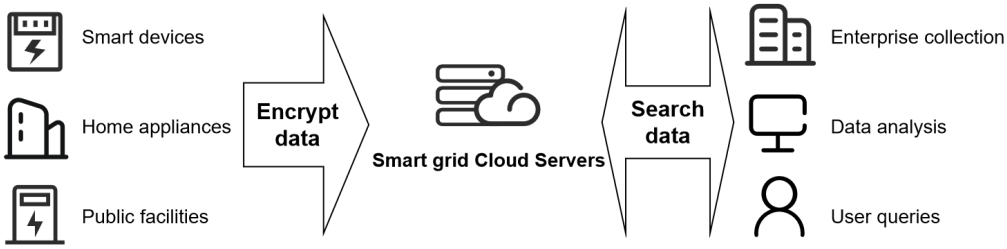

Figure 3. Smart grid application scenarios.

6.2. Healthcare

With the widespread application of technologies such as cloud computing and the IoT, electronic medical records (EMRs) and personal health records (PHRs) have been utilized more extensively. However, ensuring secure sharing of these records has become a major concern. ABSE is one solution. By using ABSE, sensitive data can be encrypted, and attribute-based search can be implemented. This allows doctors and researchers to search for medical records based on specific attributes while protecting patient privacy.

Schemes [45,57,113,114] are cloud-assisted ABSE systems for sharing medical data, utilizing the storage and computing capabilities of the CS to reduce local storage burden and facilitate data sharing among medical researchers. Schemes [59,68] are blockchain-assisted ABSE schemes for EMR and PHR sharing, ensuring data integrity and providing traceability through the adoption of blockchain and smart contracts. Schemes [78,79,79] are designed for ABSE-based medical IoT (mIoT) data sharing, enabling more effective monitoring of patients' physiological conditions by collecting large amounts of real-time data.

6.3. Internet of Things

The IoT is becoming increasingly popular, gathering vast amounts of real-time data through sensors and embedded devices. This necessitates strong privacy protection and data processing capabilities for the IoT. By integrating ABSE, the IoT can ensure the security of data stored on it while providing searchability. The IoT is often combined with other scenarios, such as the mIoT and Industrial IoT (IIoT) mentioned earlier. Schemes [65,115–118] are all ABSE schemes applied in the Industrial IoT to achieve data security and searchability.

6.4. Discussion

ABSE is primarily used in systems where data sensitivity is critical. For example, in smart grid applications, data play a crucial role in ensuring grid security and protecting the privacy of individuals and businesses regarding their electricity usage patterns. Similarly, in healthcare systems, which manage highly sensitive personal health information, safeguarding patient privacy and securing medical data are essential. Additionally, IoT devices often collect data containing privacy information about users or businesses. Table 7 summarizes the differences in the three application scenarios mentioned above.

Table 7. The differences among the three application areas.

Domain	Application Area	Data Sources	Data Sensitivity	Data Scale	Latency Requirements	Systems
Smart Grid	Power Management	Power Sensors, Smart Meters, Monitoring Systems	Critical	Large Scale	High	[112]
Healthcare	Medical Information	Electronic Health Records, Medical Devices, Sensors	Critical	Large Scale	High	[45,57,59,68,78,79,113,114]
IoT	Device Management	Sensors, Device Monitoring Systems	Elevated	Large Scale	High	[65,93,115–118]

7. Future Directions

7.1. Enhanced Security

ABSE needs to ensure the security and privacy protection of search operations. Future research will focus on further enhancing the security of ABSE schemes, including countering different types of attacks such as keyword guessing attacks and side-channel attacks. Additionally, more robust and provably secure ABSE schemes need to be designed to provide higher security assurance. Furthermore, there have been significant breakthroughs in quantum computing construction in recent years, indicating the arrival of the quantum era. This emphasizes the importance and urgency of constructing quantum-safe ABSE schemes. However, current ABSE implementations mostly rely on traditional hardness assumptions, such as scheme [33], which is based on bilinear maps and does not possess resistance to quantum attacks. Therefore, constructing new ABSE schemes considering quantum attacks will be a new direction. For example, lattice-based encryption schemes, rooted in lattice theory from discrete mathematics, are known for their resistance to quantum attacks. This makes them potential candidates for addressing quantum computing threats. Scheme [35], a lattice-based ABSE system, can resist quantum attacks, but it requires a large amount of computational resources.

7.2. Improved Efficiency

The search operations of ABSE typically require significant computational and storage resources. Given the current societal context of data explosion, ABSE will increasingly be applied in big data scenarios. In the current era of data explosion, the application of ABSE in big data scenarios is poised for significant growth. Future research should focus on enhancing security and efficiency by improving search algorithms and leveraging technologies such as parallel computing and hardware acceleration. This is to adapt to resource-constrained devices, large-scale datasets, and real-time search scenarios.

7.3. Integration into Multiple Application Areas

ABSE can be applied not only in traditional data privacy protection but also in combination with other application areas. Currently, common application areas include smart grids, healthcare, the IoT, and big data analytics. In the future, ABSE will explore application solutions in various fields to meet various practical requirements.

7.4. Integration with Advanced Technologies

ABSE can be combined with other advanced technologies to enhance its functionality and performance. Currently, integrating blockchain technology with ABSE provides decentralized attribute management and auditing mechanisms to improve data privacy, which has become a common practice. For example, Zhang et al. [66] proposed an ABCKS scheme with verifiability and fairness, using blockchain and smart contract technology to verify search results and ensure fair payment in untrusted scenarios. Gao et al. [68] proposed a blockchain-based knowledge storage and sharing architecture for secure knowledge management in the smart IoT, achieving confidentiality and security of data storage and transmission on the chain through on-chain encryption. Future research will continue to explore the integration of ABSE with other technologies such as differential privacy and secure hardware modules to provide more robust and comprehensive solutions.

8. Conclusions

This paper provides an overview of research on ABSE in recent years, focusing on enhancing security, improving computational efficiency, and increasing flexibility. It discusses the achievements of ABSE in enhancing security in terms of privacy protection enhancement and permission management technologies. It also lists common security models and summarizes the security of ABSE systems in recent years. After analysis, most systems support using outsourced computation to improve efficiency. Additionally, some schemes use online/offline encryption and adjust the index structure to improve search efficiency. The enhancement of access policy expression capabilities and search capabilities in the ABSE system are discussed in this paper. Attribute matching is mainly achieved through the use of different access structures to achieve different matching capabilities. As an important feature of ABSE, search capability is continuously explored with more complex functions in addition to traditional single-keyword search and multi-keyword search, such as ranking keyword search. Based on the review, we have identified the challenges. For example, combining blockchain technology and secure hardware can enhance security and improve efficiency.

Author Contributions: Formal analysis, T.Y.; Investigation, L.Y. and G.W.; Resources, H.F.; Data curation, L.Y. and H.H.; Writing—review and editing, H.F. and P.L.; Supervision, P.L., F.P. and W.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Key Research and Development Program of China, grant number 2022YFB3305300, and supported by the State Grid Shandong Electric Power Company Technology Project (No. 520627230004).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Acknowledgments: We are grateful to the anonymous reviewers for their comments on this manuscript.

Conflicts of Interest: Author Li Yan, Gaozhou Wang, Wenbin Zhang, Hailin Hu and Fading Pan were employed by the company State Grid Shandong Electric Power Company. The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

ABE	Attribute-Based Encryption
ABSE	Attribute-Based Searchable Encryption
CCA	Chosen Ciphertext Attack
CKA	Chosen Keyword Attack
CPA	Chosen Plaintext Attack
CP-ABE	Ciphertext-Policy Attribute-Based Encryption
CS	Cloud Server
DO	Data Owner
DU	Data User
EMR	Electronic Medical Record
FIBE	Fuzzy Identity Binary Encryption
IBE	Identity-Based Encryption
IoT	Internet of Things
IIoT	Industrial Internet of Things

IND	Indistinguishability Security
KGA	Keyword Guessing Attack
KP-ABE	Key-Policy Attribute-Based Encryption
LSSS	Linear Secret Sharing Scheme
mIoT	Medical Internet of Things
PEKS	Public-Key Encryption with Keyword Search
PHR	Personal Health Records
SE	Searchable Encryption
SSE	Searchable Symmetric Encryption
TA	Trusted Application

References

1. Song, D.X.; Wagner, D.; Perrig, A. Practical techniques for searches on encrypted data. In Proceedings of the 2000 IEEE Symposium on Security and Privacy. S&P 2000, Berkeley, CA, USA, 14–17 May 2000; pp. 44–55. [CrossRef]
2. Boneh, D.; Di Crescenzo, G.; Ostrovsky, R.; Persiano, G. Public Key Encryption with Keyword Search. In Proceedings of the Advances in Cryptology-EUROCRYPT 2004: International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, 2–6 May 2004; Cachin, C., Camenisch, J.L., Eds.; Springer: Berlin/Heidelberg, Germany, 2004; pp. 506–522.
3. Varri, U.; Varri, U.; Pasupuleti, S.K.; Kadambari, K.V. A scoping review of searchable encryption schemes in cloud computing: taxonomy, methods, and recent developments. *J. Supercomput.* **2019**, *76*, 3013–3042. [CrossRef]
4. Sahai, A.; Waters, B. Fuzzy Identity-Based Encryption. In Proceedings of the Advances in Cryptology—EUROCRYPT 2005: 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, 22–26 May 2005; Cramer, R., Ed.; Springer: Berlin/Heidelberg, Germany, 2005; pp. 457–473.
5. Goyal, V.; Pandey, O.; Sahai, A.; Waters, B. Attribute-based encryption for fine-grained access control of encrypted data. *IACR Cryptol. ePrint Arch.* **2006**, *2006*, 309.
6. Bethencourt, J.; Sahai, A.; Waters, B. Ciphertext-Policy Attribute-Based Encryption. In Proceedings of the 2007 IEEE Symposium on Security and Privacy (SP '07), Berkeley, CA, USA, 20–23 May 2007; pp. 321–334.
7. Wang, C.; Li, W.; Li, Y.; Xu, X. A Ciphertext-Policy Attribute-Based Encryption Scheme Supporting Keyword Search Function. In Proceedings of the Cyberspace Safety and Security: 5th International Symposium, CSS 2013, Zhangjiajie, China, 13–15 November 2013; Wang, G., Ray, I., Feng, D., Rajarajan, M., Eds.; Springer: Cham, Switzerland, 2013; pp. 377–386.
8. Zheng, Q.; Xu, S.; Ateniese, G. VABKS: Verifiable attribute-based keyword search over outsourced encrypted data. In Proceedings of the IEEE INFOCOM 2014—IEEE Conference on Computer Communications, Toronto, ON, Canada, 27 April–2 May 2014; pp. 522–530. [CrossRef]
9. Andola, N.; Gahlot, R.; Yadav, V.K.; Venkatesan, S.; Verma, S. Searchable encryption on the cloud: A survey. *J. Supercomput.* **2022**, *78*, 9952–9984. [CrossRef]
10. Sookhak, M.; Yu, F.R.; Khan, M.K.; Xiang, Y.; Buyya, R. Attribute-based data access control in mobile cloud computing: Taxonomy and open issues. *Future Gener. Comput. Syst.* **2017**, *72*, 273–287. [CrossRef]
11. Kumar, P.; Alphonse, P.J. Attribute based encryption in cloud computing: A survey, gap analysis, and future directions. *J. Netw. Comput. Appl.* **2018**, *108*, 37–52. [CrossRef]
12. Porwal, S.; Mittal, S. A Review of Key Delegation Schemes in Ciphertext Policy-Attribute Based Encryption. In Proceedings of the 2023 International Conference on Computational Intelligence, Communication Technology and Networking (CICTN), Ghaziabad, India, 20–21 April 2023; pp. 309–314.
13. Bhajantri, L.B.; Mujawar, T.N. A Comprehensive Review of Access Control Mechanism Based on Attribute Based Encryption Scheme for Cloud Computing. *Res. Anthol. Artif. Intell. Appl. Secur.* **2021**, *11*, 33–52.
14. Nishide, T.; Yoneyama, K.; Ohta, K. Attribute-Based Encryption with Partially Hidden Encryptor-Specified Access Structures. In Proceedings of the Applied Cryptography and Network Security: 6th International Conference, ACNS 2008, New York, NY, USA, 3–6 June 2008; Bellovin, S.M., Gennaro, R., Keromytis, A., Yung, M., Eds.; Springer: Berlin/Heidelberg, Germany, 2008; pp. 111–129.
15. Lai, J.; Deng, R.H.; Li, Y. Fully Secure Cipertext-Policy Hiding CP-ABE. In Proceedings of the Information Security Practice and Experience: 7th International Conference, ISPEC 2011, Guangzhou, China, 30 May–1 June 2011; Bao, F., Weng, J., Eds.; Springer: Berlin/Heidelberg, Germany, 2011; pp. 24–39.
16. Balu, A.; Kuppusamy, K. Privacy Preserving Ciphertext Policy Attribute Based Encryption. In Proceedings of the Applied Cryptography and Network Security: 6th International Conference, ACNS 2008, New York, NY, USA, 3–6 June 2008; Meghanathan, N., Boumerdassi, S., Chaki, N., Nagamalai, D., Eds.; Springer: Berlin/Heidelberg, Germany, 2010; pp. 402–409.
17. Lai, J.; Deng, R.H.; Li, Y. Expressive CP-ABE with partially hidden access structures. In Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security, ASIACCS '12, Seoul, Republic of Korea, 2–4 May 2012; pp. 18–19.
18. Zhang, Y.; Deng, R.H.; Han, G.; Zheng, D. Secure smart health with privacy-aware aggregate authentication and access control in Internet of Things. *J. Netw. Comput. Appl.* **2018**, *123*, 89–100. [CrossRef]

19. Koo, D.; Hur, J.; Yoon, H. Secure and efficient data retrieval over encrypted data using attribute-based encryption in cloud storage. *Comput. Electr. Eng.* **2013**, *39*, 34–46. [CrossRef]
20. Chaudhari, P.; Das, M.L. On the Security of a Searchable Anonymous Attribute Based Encryption. In Proceedings of the Mathematics and Computing: Third International Conference, ICMC 2017, Haldia, India, 17–21 January 2017; Giri, D., Mohapatra, R.N., Begehr, H., Obaidat, M.S., Eds.; Springer: Singapore, 2017; pp. 16–25.
21. Shi, J.; Lai, J.; Li, Y.; Deng, R.H.; Weng, J. Authorized Keyword Search on Encrypted Data. In Proceedings of the Computer Security-ESORICS 2014: 19th European Symposium on Research in Computer Security, Wroclaw, Poland, 7–11 September 2014; Kutyłowski, M., Vaidya, J., Eds.; Springer: Cham, Switzerland, 2014; pp. 419–435.
22. Wang, H.; Dong, X.; Cao, Z. Multi-Value-Independent Ciphertext-Policy Attribute Based Encryption with Fast Keyword Search. *IEEE Trans. Serv. Comput.* **2020**, *13*, 1142–1151. [CrossRef]
23. Chaudhari, P.; Das, M.L. KeySea: Keyword-Based Search with Receiver Anonymity in Attribute-Based Searchable Encryption. *IEEE Trans. Serv. Comput.* **2022**, *15*, 1036–1044. [CrossRef]
24. Miao, Y.; Liu, X.; Choo, K.K.R.; Deng, R.H.; Li, J.; Li, H.; Ma, J. Privacy-Preserving Attribute-Based Keyword Search in Shared Multi-owner Setting. *IEEE Trans. Dependable Secur. Comput.* **2021**, *18*, 1080–1094. [CrossRef]
25. Sun, J.; Xiong, H.; Nie, X.; Zhang, Y.; Wu, P. On the Security of Privacy-Preserving Attribute-Based Keyword Search in Shared Multi-Owner Setting. *IEEE Trans. Dependable Secur. Comput.* **2021**, *18*, 2518–2519. [CrossRef]
26. Byun, J.W.; Rhee, H.S.; Park, H.A.; Lee, D.H. Off-Line Keyword Guessing Attacks on Recent Keyword Search Schemes over Encrypted Data. In Proceedings of the Secure Data Management, Seoul, Republic of Korea, 10–11 September 2006; Jonker, W., Petković, M., Eds.; Springer: Berlin/Heidelberg, Germany, 2006; pp. 75–83.
27. Baek, J.; Safavi-Naini, R.; Susilo, W. Public Key Encryption with Keyword Search Revisited. In Proceedings of the Computational Science and Its Applications–ICCSA 2008: International Conference, Perugia, Italy, 30 June–3 July 2008; Gervasi, O., Murgante, B., Laganà, A., Taniar, D., Mun, Y., Gavrilova, M.L., Eds.; Springer: Berlin/Heidelberg, Germany, 2008; pp. 1249–1259.
28. Yau, W.C.; Phan, R.C.W.; Heng, S.H.; Goi, B.M. Keyword guessing attacks on secure searchable public key encryption schemes with a designated tester. *Int. J. Comput. Math.* **2013**, *90*, 2581–2587. [CrossRef]
29. Jeong, I.R.; Kwon, J.O.; Hong, D.; Lee, D.H. Constructing PEKS schemes secure against keyword guessing attacks is possible? *Comput. Commun.* **2009**, *32*, 394–396. [CrossRef]
30. Rhee, H.S.; Park, J.H.; Susilo, W.; Lee, D.H. Trapdoor security in a searchable public-key encryption scheme with a designated tester. *J. Syst. Softw.* **2010**, *83*, 763–771. [CrossRef]
31. Wang, C.H.; Tu, T.Y. Keyword search encryption scheme resistant against keyword-guessing attack by the untrusted server. *J. Shanghai Jiaotong Univ.* **2014**, *19*, 440–442. [CrossRef]
32. Huang, Q.; Li, H. An efficient public-key searchable encryption scheme secure against inside keyword guessing attacks. *Inf. Sci.* **2017**, *403*, 1–14. [CrossRef]
33. 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*, 1242–1251. [CrossRef]
34. Qiu, S.; Liu, J.; Shi, Y.; Zhang, R. Hidden policy ciphertext-policy attribute-based encryption with keyword search against keyword guessing attack. *Sci. China Inf. Sci.* **2017**, *60*, 052105:1–052105:12. [CrossRef]
35. Luo, F.; Wang, H.; Lin, C.; Yan, X. ABAEKS: Attribute-Based Authenticated Encryption with Keyword Search Over Outsourced Encrypted Data. *IEEE Trans. Inf. Forensics Secur.* **2023**, *18*, 4970–4983. [CrossRef]
36. Liu, Z.; Cao, Z.; Wong, D.S. Traceable CP-ABE: How to Trace Decryption Devices Found in the Wild. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 55–68.
37. Hinek, M.J.; Jiang, S.; Safavi-Naini, R.; Shahandashti, S.F. Attribute-Based Encryption with Key Cloning Protection. *IACR Cryptol. ePrint Arch.* **2008**, *2008*, 478.
38. Yu, S.; Ren, K.; Lou, W.; Li, J. Defending against Key Abuse Attacks in KP-ABE Enabled Broadcast Systems. In Proceedings of the Security and Privacy in Communication Networks: 5th International ICST Conference, SecureComm 2009, Athens, Greece, 14–18 September 2009; Chen, Y., Dimitriou, T.D., Zhou, J., Eds.; Springer: Berlin/Heidelberg, Germany, 2009; pp. 311–329.
39. Katz, J.; Schröder, D. Tracing Insider Attacks in the Context of Predicate Encryption Schemes. Available online: http://www.cs.umd.edu/~jkatz/papers/ACITA11.pdf (accessed on 21 April 2024).
40. Liu, Z.; Cao, Z.; Wong, D.S. White-Box Traceable Ciphertext-Policy Attribute-Based Encryption Supporting Any Monotone Access Structures. *IEEE Trans. Inf. Forensics Secur.* **2013**, *8*, 76–88.
41. Liu, Z.; Cao, Z.; Wong, D.S. Blackbox traceable CP-ABE: How to catch people leaking their keys by selling decryption devices on ebay. In Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security, Berlin, Germany, 4–8 November 2013.
42. Liu, Z.; Wong, D.S. Traceable CP-ABE on Prime Order Groups: Fully Secure and Fully Collusion-Resistant Blackbox Traceable. In Proceedings of the Information and Communications Security, Beijing, China, 9–11 December 2015; Qing, S., Okamoto, E., Kim, K., Liu, D., Eds.; Springer: Cham, Switzerland, 2016; pp. 109–124.
43. Ziegler, D.; Marsalek, A.; Palfinger, G. White-Box Traceable Attribute-Based Encryption with Hidden Policies and Outsourced Decryption. In Proceedings of the 2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Shenyang, China, 20–22 October 2021; pp. 331–338.

44. Luo, F.; Al-Kuwari, S.M. Generic Construction of Black-Box Traceable Attribute-Based Encryption. *IEEE Trans. Cloud Comput.* **2023**, *11*, 942–955. [CrossRef]
45. Yang, Y.; Liu, X.; Deng, R.H.; Li, Y. Lightweight Sharable and Traceable Secure Mobile Health System. *IEEE Trans. Dependable Secur. Comput.* **2020**, *17*, 78–91. [CrossRef]
46. Varri, U.; Kasani, S.; Pasupuleti, S.K.; Kv, K. FELT-ABKS: Fog-Enabled Lightweight Traceable Attribute-Based Keyword Search Over Encrypted Data. *IEEE Internet Things J.* **2022**, *9*, 7559–7571. [CrossRef]
47. Pirretti, M.; Traynor, P.; Mcdaniel, P.; Waters, B. Secure attribute-based systems. *J. Comput. Secur.* **2006**, *18*, 799–837. [CrossRef]
48. Ostrovsky, R.M.; Sahai, A.; Waters, B. Attribute-based encryption with non-monotonic access structures. *IACR Cryptol. ePrint Arch.* **2007**, *2007*, 323.
49. Attrapadung, N.; Imai, H. Conjunctive Broadcast and Attribute-Based Encryption. In Proceedings of the Pairing-Based Cryptography–Pairing 2009: Third International Conference, Palo Alto, CA, USA, 12–14 August 2009; Shacham, H., Waters, B., Eds.; Springer: Berlin/Heidelberg, Germany, 2009; pp. 248–265.
50. Wang, S.; Zhang, X.; Zhang, Y. Efficient revocable and grantable attribute-based encryption from lattices with fine-grained access control. *IET Inf. Secur.* **2017**, *12*, 141–149. [CrossRef]
51. Tu, S.; Waqas, M.M.; Huang, F.C.; Abbas, G.; Abbas, Z.H. A revocable and outsourced multi-authority attribute-based encryption scheme in fog computing. *Comput. Netw.* **2021**, *195*, 108196. [CrossRef]
52. Dong, X.; Zhang, Y.; Wang, B.; Chen, J. Server-Aided Revocable Attribute-Based Encryption from Lattices. *Secur. Commun. Netw.* **2020**, *2020*, 1460531. [CrossRef]
53. 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 Secur. Comput.* **2019**, *18*, 2301–2315. [CrossRef]
54. Zhang, R.; Li, J.; Lu, Y.; Han, J.; Zhang, Y. Key escrow-free attribute based encryption with user revocation. *Inf. Sci.* **2022**, *600*, 59–72. [CrossRef]
55. Chen, S.; Li, J.; Zhang, Y.; Han, J. Efficient Revocable Attribute-Based Encryption with Verifiable Data Integrity. *IEEE Internet Things J.* **2024**, *11*, 10441–10451. [CrossRef]
56. Bao, Y.; Qiu, W.; Tang, P.; Cheng, X. Efficient, Revocable, and Privacy-Preserving Fine-Grained Data Sharing with Keyword Search for the Cloud-Assisted Medical IoT System. *IEEE J. Biomed. Health Inform.* **2022**, *26*, 2041–2051. [CrossRef] [PubMed]
57. Miao, Y.; Li, F.; Li, X.; Liu, Z.; Ning, J.; Li, H.; Choo, K.K.; Deng, R. Time-Controllable Keyword Search Scheme with Efficient Revocation in Mobile E-health Cloud. *IEEE Trans. Mob. Comput.* **2023**, *23*, 3650–3665. [CrossRef]
58. Liu, S.; Yu, J.; Xiao, Y.; Wan, Z.; Wang, S.; Yan, B. BC-SABE: Blockchain-Aided Searchable Attribute-Based Encryption for Cloud-IoT. *IEEE Internet Things J.* **2020**, *7*, 7851–7867. [CrossRef]
59. 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*, 3210–3223. [CrossRef]
60. Yu, J.; Liu, S.; Xu, M.; Guo, H.; Zhong, F.; Cheng, W. An Efficient Revocable and Searchable MA-ABE Scheme with Blockchain Assistance for C-IoT. *IEEE Internet Things J.* **2023**, *10*, 2754–2766. [CrossRef]
61. Wang, H.Y.; Fan, K.; Zhang, K.; Wang, Z.; Li, H.; Yang, Y. Secure and Efficient Data-Privacy-Preserving Scheme for Mobile Cyber–Physical Systems. *IEEE Internet Things J.* **2022**, *9*, 22375–22388. [CrossRef]
62. Yang, K.; Shu, J.; Xie, R. Efficient and Provably Secure Data Selective Sharing and Acquisition in Cloud-Based Systems. *IEEE Trans. Inf. Forensics Secur.* **2023**, *18*, 71–84. [CrossRef]
63. Liu, J.; Fan, Y.; Sun, R.; Liu, L.; Wu, C.; Mumtaz, S. Blockchain-Aided Privacy-Preserving Medical Data Sharing Scheme for E-Healthcare System. *IEEE Internet Things J.* **2023**, *10*, 21377–21388. [CrossRef]
64. 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*, 3503–3514. [CrossRef]
65. Zhang, K.; Long, J.; Wang, X.; Dai, H.; Liang, K.; Imran, M. Lightweight Searchable Encryption Protocol for Industrial Internet of Things. *IEEE Trans. Ind. Inform.* **2021**, *17*, 4248–4259. [CrossRef]
66. Zhang, D.; Wang, S.; Zhang, Q.; Zhang, Y. Attribute Based Conjunctive Keywords Search with Verifiability and Fair Payment Using Blockchain. *IEEE Trans. Serv. Comput.* **2023**, *16*, 4168–4182. [CrossRef]
67. Miao, Y.; Ma, J.; Liu, X.; Li, X.; Liu, Z.; Li, H. Practical Attribute-Based Multi-Keyword Search Scheme in Mobile Crowdsourcing. *IEEE Internet Things J.* **2018**, *5*, 3008–3018. [CrossRef]
68. Gao, H.; Huang, H.; Xue, L.; Xiao, F.; Li, Q. Blockchain-Enabled Fine-Grained Searchable Encryption with Cloud–Edge Computing for Electronic Health Records Sharing. *IEEE Internet Things J.* **2023**, *10*, 18414–18425. [CrossRef]
69. Cui, H.; Wan, Z.; Deng, R.H.; Wang, G.; Li, Y. Efficient and Expressive Keyword Search Over Encrypted Data in Cloud. *IEEE Trans. Dependable Secur. Comput.* **2016**, *15*, 409–422. [CrossRef]
70. Shi, J.; Yu, Y.; Yu, Q.; Li, H.; Wang, L. Toward Data Security in 6G Networks: A Public-Key Searchable Encryption Approach. *IEEE Netw.* **2022**, *36*, 166–173. [CrossRef]
71. 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*, 985–998. [CrossRef]
72. Liu, J.; Li, Y.; Sun, R.; Pei, Q.; Zhang, N.; Dong, M.; Leung, V.C.M. EMK-ABSE: Efficient Multikeyword Attribute-Based Searchable Encryption Scheme Through Cloud-Edge Coordination. *IEEE Internet Things J.* **2022**, *9*, 18650–18662. [CrossRef]

73. Wang, M.; Miao, Y.; Guo, Y.; Huang, H.; Wang, C.; Jia, X. AESM2 Attribute-Based Encrypted Search for Multi-Owner and Multi-User Distributed Systems. *IEEE Trans. Parallel Distrib. Syst.* **2023**, *34*, 92–107. [CrossRef]
74. 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*, 1685–1697. [CrossRef]
75. Green, M.; Hohenberger, S.; Waters, B. Outsourcing the decryption of ABE ciphertexts. In Proceedings of the 20th USENIX Conference on Security, SEC'11, Sanfrancisco, CA, USA, 8–12 August 2011; p. 34.
76. Miao, Y.; Deng, R.H.; Liu, X.; Choo, K.R.; Wu, H.; Li, H. Multi-Authority Attribute-Based Keyword Search over Encrypted Cloud Data. *IEEE Trans. Dependable Secur. Comput.* **2021**, *18*, 1667–1680. [CrossRef]
77. Zhang, P.; Chui, Y.; Liu, H.; Yang, Z.; Wu, D.O.; Wang, R. Efficient and Privacy-Preserving Search Over Edge–Cloud Collaborative Entity in IoT. *IEEE Internet Things J.* **2023**, *10*, 3192–3205. [CrossRef]
78. Liu, X.; Yang, X.; Luo, Y.; Zhang, Q. Verifiable Multikeyword Search Encryption Scheme with Anonymous Key Generation for Medical Internet of Things. *IEEE Internet Things J.* **2022**, *9*, 22315–22326. [CrossRef]
79. 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*, 2513–2526. [CrossRef]
80. Wang, J.; Lin, X.; Wu, Y.; Wu, J. Blockchain-Enabled Lightweight Fine-Grained Searchable Knowledge Sharing for Intelligent IoT. *IEEE Internet Things J.* **2023**, *10*, 21566–21579. [CrossRef]
81. Even, S.; Goldreich, O.; Micali, S. On-line/off-line digital signatures. *J. Cryptol.* **1996**, *9*, 35–67. [CrossRef]
82. Hohenberger, S.; Waters, B. Online/Offline Attribute-Based Encryption. In Proceedings of the Public-Key Cryptography–PKC 2014: 17th International Conference on Practice and Theory in Public-Key Cryptography, Buenos Aires, Argentina, 26–28 March 2014; Krawczyk, H., Ed.; Springer: Berlin/Heidelberg, Germany, 2014; pp. 293–310.
83. Datta, P.; Dutta, R.; Mukhopadhyay, S. Fully Secure Online/Offline Predicate and Attribute-Based Encryption. In Proceedings of the Information Security Practice and Experience, Beijing, China, 5–8 May 2015; Lopez, J., Wu, Y., Eds.; Springer: Cham, Switzerland, 2015; pp. 331–345.
84. Liu, Y.; Zhang, Y.; Ling, J.; Liu, Z. Secure and fine-grained access control on e-healthcare records in mobile cloud computing. *Future Gener. Comput. Syst.* **2018**, *78*, 1020–1026. [CrossRef]
85. Cui, J.; Zhou, H.; Xu, Y.; Zhong, H. OOABKS: Online/offline attribute-based encryption for keyword search in mobile cloud. *Inf. Sci.* **2019**, *489*, 63–77. [CrossRef]
86. Wang, B.; Li, M.; Wang, H. Geometric Range Search on Encrypted Spatial Data. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 704–719. [CrossRef]
87. Xia, Z.; Wang, X.; Sun, X.; Wang, Q. A Secure and Dynamic Multi-Keyword Ranked Search Scheme over Encrypted Cloud Data. *IEEE Trans. Parallel Distrib. Syst.* **2016**, *27*, 340–352. [CrossRef]
88. Curtmola, R.; Garay, J.A.; Kamara, S.; Ostrovsky, R.M. Searchable symmetric encryption: Improved definitions and efficient constructions. *IACR Cryptol. ePrint Arch.* **2006**, *2006*, 210.
89. Cash, D.; Jarecki, S.; Jutla, C.; Krawczyk, H.; Roşu, M.C.; Steiner, M. Highly-Scalable Searchable Symmetric Encryption with Support for Boolean Queries. In Proceedings of the Advances in Cryptology–CRYPTO 2013: 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, 18–22 August 2013; Canetti, R., Garay, J.A., Eds.; Springer: Berlin/Heidelberg, Germany, 2013; pp. 353–373.
90. Zhang, K.; Wen, M.; Lu, R.; Chen, K. Multi-Client Sub-Linear Boolean Keyword Searching for Encrypted Cloud Storage with Owner-Enforced Authorization. *IEEE Trans. Dependable Secur. Comput.* **2021**, *18*, 2875–2887. [CrossRef]
91. Yin, H.; Qin, Z.; Zhang, J.; Deng, H.; Li, F.; Li, K. A fine-grained authorized keyword secure search scheme with efficient search permission update in cloud computing. *J. Parallel Distrib. Comput.* **2020**, *135*, 56–69. [CrossRef]
92. Yin, H.; Li, Y.; Deng, H.; Zhang, W.; Qin, Z.; Li, K. Practical and Dynamic Attribute-Based Keyword Search Supporting Numeric Comparisons Over Encrypted Cloud Data. *IEEE Trans. Serv. Comput.* **2023**, *16*, 2855–2867. [CrossRef]
93. Niu, S.; Hu, Y.; Su, Y.; Yan, S.; Zhou, S. Attribute-based searchable encrypted scheme with edge computing for Industrial Internet of Things. *J. Syst. Archit.* **2023**, *139*, 102889. [CrossRef]
94. Golle, P.; Staddon, J.; Waters, B. Secure Conjunctive Keyword Search over Encrypted Data. In Proceedings of the Applied Cryptography and Network Security: Second International Conference, ACNS 2004, Yellow Mountain, China, 8–11 June 2004; Jakobsson, M., Yung, M., Zhou, J., Eds.; Springer: Berlin/Heidelberg, Germany, 2004; pp. 31–45.
95. Park, D.J.; Kim, K.; Lee, P.J. Public Key Encryption with Conjunctive Field Keyword Search. In Proceedings of the Information Security Applications, Jeju Island, Republic of Korea, 23–25 August 2004; Lim, C.H., Yung, M., Eds.; Springer: Berlin/Heidelberg, Germany, 2005; pp. 73–86.
96. Zhang, K.; Wang, X.; Ning, J.; Wen, M.; Lu, R. Multi-Client Boolean File Retrieval with Adaptable Authorization Switching for Secure Cloud Search Services. *IEEE Trans. Dependable Secur. Comput.* **2023**, *20*, 4621–4636. [CrossRef]
97. Huang, Q.; Yan, G.; Wei, Q. Attribute-Based Expressive and Ranked Keyword Search Over Encrypted Documents in Cloud Computing. *IEEE Trans. Serv. Comput.* **2023**, *16*, 957–968. [CrossRef]
98. Shamir, A. How to share a secret. *Commun. ACM* **1979**, *22*, 612–613. [CrossRef]
99. Cheung, L.; Newport, C. Provably secure ciphertext policy ABE. In Proceedings of the 14th ACM Conference on Computer and Communications Security, CCS '07, Alexandria, VA, USA, 31 October–2 November 2007; pp. 456–465.

100. Waters, B. Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization. *IACR Cryptol. ePrint Arch.* **2011**, *2008*, 290.
101. Chen, Y. Research on Attribute-Based Encryption Scheme and Its Applications. Ph.D. Thesis, Nanjing University of Posts and Telecommunications, Nanjing, China, 2014.
102. Lai, J.; Deng, R.H.; Yang, Y.; Weng, J. Adaptable Ciphertext-Policy Attribute-Based Encryption. In Proceedings of the Pairing-Based Cryptography–Pairing 2013: 6th International Conference, Beijing, China, 22–24 November 2013; Cao, Z., Zhang, F., Eds.; Springer: Cham, Switzerland, 2014; pp. 199–214.
103. Xue, K.; Hong, J.; Xue, Y.; Wei, D.S.L.; Yu, N.; Hong, P. CABE: A New Comparable Attribute-Based Encryption Construction with 0-Encoding and 1-Encoding. *IEEE Trans. Comput.* **2017**, *66*, 1491–1503. [CrossRef]
104. Bishop, A.; Waters, B. Unbounded HIBE and Attribute-Based Encryption. *IACR Cryptol. ePrint Arch.* **2011**, *2011*, 49.
105. Lewko, A.; Waters, B. New Proof Methods for Attribute-Based Encryption: Achieving Full Security through Selective Techniques. In Proceedings of the Advances in Cryptology–CRYPTO 2012, Santa Barbara, CA, USA, 19–23 August 2012; Safavi-Naini, R., Canetti, R., Eds.; Springer: Berlin/Heidelberg, Germany, 2012; pp. 180–198.
106. Rouselakis, Y.; Waters, B. Practical constructions and new proof methods for large universe attribute-based encryption. In Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security, CCS '13, Berlin, Germany, 4–8 November 2013; pp. 463–474. [CrossRef]
107. Tao, Z.; Lin, W.; Wang, Y.; Deng, S.; Shi, C.; Chen, L. The design of information security protection framework to support Smart Grid. In Proceedings of the 2010 International Conference on Power System Technology, Hangzhou, China, 24–28 October 2010; pp. 1–5.
108. Rogers, K.M.; Klump, R.P.; Khurana, H.; Aquino-Lugo, A.A.; Overbye, T.J. An Authenticated Control Framework for Distributed Voltage Support on the Smart Grid. *IEEE Trans. Smart Grid* **2010**, *1*, 40–47. [CrossRef]
109. Su, Q.; Zhang, R.; Xue, R.; Sun, Y.; Gao, S. Distributed Attribute-Based Signature with Attribute Dynamic Update for Smart Grid. *IEEE Trans. Ind. Inform.* **2023**, *19*, 9424–9435. [CrossRef]
110. Ge, J.; Wen, M.; Wang, L.; Xie, R. Attribute-Based Collaborative Access Control Scheme with Constant Ciphertext Length for Smart Grid. In Proceedings of the ICC 2022–IEEE International Conference on Communications, Seoul, Republic of Korea, 16–20 May 2022; pp. 540–546.
111. Li, J.; Sun, J. A Practical Searchable Symmetric Encryption Scheme for Smart Grid Data. In Proceedings of the ICC 2019–2019 IEEE International Conference on Communications (ICC), Shanghai, China, 20–24 May 2019; pp. 1–6.
112. 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*, 165–172. [CrossRef]
113. Ge, X.; Yu, J.; Hao, R.; Lv, H. Verifiable Keyword Search Supporting Sensitive Information Hiding for the Cloud-Based Healthcare Sharing System. *IEEE Trans. Ind. Inform.* **2022**, *18*, 5573–5583. [CrossRef]
114. Mamta; Gupta, B.B.; Li, K.C.; Leung, V.C.M.; Psannis, K.E.; Yamaguchi, S. Blockchain-Assisted Secure Fine-Grained Searchable Encryption for a Cloud-Based Healthcare Cyber-Physical System. *IEEE/CAA J. Autom. Sin.* **2021**, *8*, 1877–1890. [CrossRef]
115. Wang, W.; Xu, P.; Liu, D.; Yang, L.T.; Yan, Z. Lightweighted Secure Searching Over Public-Key Ciphertexts for Edge-Cloud-Assisted Industrial IoT Devices. *IEEE Trans. Ind. Inform.* **2020**, *16*, 4221–4230. [CrossRef]
116. Ali, M.G.; Sadeghi, M.R.; Liu, X.; Miao, Y.; Vasilakos, A.V. Verifiable online/offline multi-keyword search for cloud-assisted Industrial Internet of Things. *J. Inf. Secur. Appl.* **2022**, *65*, 103101. [CrossRef]
117. Zhou, R.; Zhang, X.; Wang, X.; Yang, G.; Dai, H.; Liu, M. Device-Oriented Keyword-Searchable Encryption Scheme for Cloud-Assisted Industrial IoT. *IEEE Internet Things J.* **2022**, *9*, 17098–17109. [CrossRef]
118. 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*, 11014–11023. [CrossRef]