IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received September 13, 2019, accepted October 3, 2019, date of publication October 9, 2019, date of current version October 23, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2946185

Privacy Protection and Data Security in Cloud Computing: A Survey, Challenges, and Solutions

PAN JUN SUN
School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai 200240, China
e-mail: sunpanjun2008@163.com

This work was supported by the National Development and Reform Commission, Information Security Special Project, Development and Reform Office, No. [2012] 1424.

ABSTRACT Privacy and security are the most important issues to the popularity of cloud computing service. In recent years, there are many research schemes of cloud computing privacy protection based on access control, attribute-based encryption (ABE), trust and reputation, but they are scattered and lack unified logic. In this paper, we systematically review and analyze relevant research achievements. First, we discuss the architecture, concepts and several shortcomings of cloud computing, and propose a framework of privacy protection; second, we discuss and analyze basic ABE, KP-ABE (key policy attribute-based encryption), CP-ABE (ciphertext policy attribute-based encryption), access structure, revocation mechanism, multi-authority, fine-grained, trace mechanism, proxy re-encryption(PRE), hierarchical encryption, searchable encryption(SE), trust, reputation, extension of tradition access control and hierarchical key; third, we propose the research challenge and future direction of the privacy protection in the cloud computing; finally, we point out corresponding privacy protection laws to make up for the technical deficiencies.

INDEX TERMS Cloud computing, privacy, access control, attribute-based encryption, trust.

I. INTRODUCTION

Cloud computing combines the concept of grid computing, distribution and utility computing, and so on, which links a large amount of computing resources, storage resources and software resources together, and form a huge pool of shared virtual resource [1]–[6].

In the cloud, the owners are not able to control the data that can be executed on the platform. For example, the owner does not know whether the data is protected or not and the task is executed or not. In order to allow enterprises and organizations to apply cloud computing technology and deliver their own data to CSP (cloud service provider), it is necessary to analyze and solve privacy and security, encryption, access control and trust problems in the cloud computing [4].

There are many research schemes of privacy protection based on access control, encryption and trust, but they are scattered and mostly not systematic [7]–[10]. Therefore, it is necessary to conclude the recent research results of several technologies to facilitate privacy protection in cloud computing [14].

The associate editor coordinating the review of this manuscript and approving it for publication was Sedat Akleylek.

Most of the existing privacy protection schemes do not have dynamic protection function, and their scalability is not strong. Overall, the current research and progress on cloud computing privacy protection is still in infant stage, and a complete research system has not yet been formed [5]. Therefore, how to achieve fine-grained security and privacy protection in the process of dynamic data updating will be a major challenge [11]–[13].

A. RELATED WORKS

This sub-section focuses on discussing privacy and security in the cloud computing, and moderately involves in related areas, such as edge computing, fog computing, IoT and blockchain. These survey articles are compared with our paper in the Table 1.

Cloud computing privacy and security issues have always been a hot topic in academic discussion. Reference [4] identified five most representative security and privacy attributes (confidentiality, integrity, availability, accountability and privacy) and demonstrated their relationships, but lacked a specific performance comparison description. Reference [5] investigated various methods of secret communication, such as secret channel, side channel attack and fuzzy technology,

TABLE 1. Comparison of several survey papers.

Survey work	Year	Covered technology/ application	Current research works	Category
This work	2019	Cloud computing	Trust, encryption, access control	Hybrid
[4]	2013	Cloud computing	Policy and encryption	Single
[5]	2017	Cloud computing	Side channel	Single
[7]	2015	Cloud computing	Encryption	Single
[86]	2019	Cloud medical	Encryption	Single
[131]	2019	IoT	Trust, reputation	Single
[189]	2019	Blockchain	Access control, authentication	Single
[190]	2018	Fog computing, IoT	Encryption	Hybrid
[194]	2018	Healthcare cloud	Searchable encryption	Single
[195]	2019	Ehealth cloud	Encryption	Single

discussed the secret communication technology related to application scenarios, and showed their advantages and limitations. Similarly, [7] summarized the key security and privacy challenges in cloud computing, classified existing solutions, compared their advantages and limitations, but lack of comparison with other review articles.

Cloud computing is a new computing model in the medical field. Reference [86] focused on the research challenges of electronic health reword (EHR) in terms of the following tasks: 1) EHR security and privacy; 2) security and privacy requirements of electronic health data in cloud environment; 3) EHR cloud architecture; 4) different EHR encryption and non-encryption program. Reference [194] summarized four SE technologies: searchable symmetric encryption (SSE), public key encryption with keyword search (PEK), attribute-based encryption with keyword search (ABK) and proxy re-encryption (PRES), but only give a technical overview. Reference [195] summarized different attribute-based cooperative electronic health encryption schemes, compared and analyzed the security, revocation ability and efficiency. However, the privacy protection technology mentioned in this paper is relatively single.

Reference [85] introduced the concept and characteristics of edge computing, and proposed some requirements for edge computing security data analysis by analyzing the potential security threats of edge computing, and give a comprehensive review of the advantages and disadvantages of existing edge computing data analysis work. Reference [131] provided a subject classification of trust in the Internet of Things, and considered the role of trust entities, trust attributes, trust applications, trust management, trust measurement, trust computing schemes.

Reference [189] studied several security methods based on block chain, which included authentication, confidentiality, privacy and access control lists, data and resource sources, and integrity assurance. But they lacked other aspects of privacy technology, such as trust and reputation and access control. Reference [190] mainly focused on the construction and future development of the Internet of Things system. In this article, the security protection of privacy is only a small aspect, which lacks systematic discussion.

B. CONTRIBUTIONS

Based on the basic concepts, privacy and security issues of cloud computing, this paper focuses on the key technologies, such as access control, encryption, trust and reputation, and carries out the latest research results of cloud computing. The main contributions of the paper are summarized as follows:

- We discuss these shortcomings of cloud computing privacy security risk, and propose a framework of privacy protection.
- We summarize several important modes of ABEs, such as CP-ABE, KP-ABE, revocation mechanism, multi-authority, fine grained, trace mechanism, proxy re-encryption and hierarchical encryption.
- We analyze several searchable encryption schemes of cloud outsource service, such as searchable asymmetric encryption (SAE) and searchable symmetric encryption (SSE).
- We discuss and compare cloud computing privacy and security issues based on trust and reputation.
- We analyze that the combination and extension of trust, reputation, access control, multi-tenant and hierarchical key.
- We analyzed the challenges and issues in the cloud privacy, and pointed out the future direction of development.

The rest of this paper is organized as follows. In section II, we discuss the problems of privacy protection in cloud computing, and propose an overall framework. In section III, we discuss related research of ABE, such as access structure, revocation mechanism, multi-authority, fine grained, trace mechanism, proxy re-encryption and hierarchical encryption. In section IV, we discuss several searchable encryption

schemes of cloud computing. In section V, we mainly discuss privacy protection of cloud services based on trust and reputation. In section VI, we analyze the extension work of MAC, UCON, RBAC, ABAC, trust and hierarchical key in privacy protection. In section VII, we discuss challenges, issues and future directions of cloud computing. In section VIII, we propose corresponding privacy laws to make up for the technical deficiencies. In order to clearly illustrate the overall structure, this paper presents an organizational framework in Fig.1.

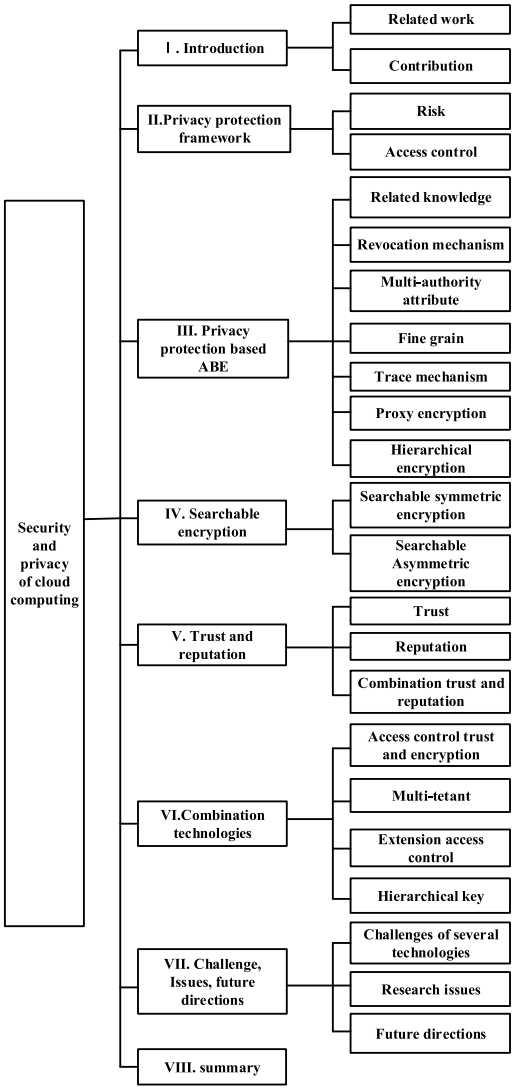


FIGURE 1. The organization and classification research.

II. PRIVACY PROTECTION FRAMEWORK OF CLOUD COMPUTING

In cloud computing, the user's privacy data is confidential. Data outsourcing storage, virtualization and multi-tenant, big data and other technologies make people concern the risk of privacy disclosure, details are shown in Fig. 2.

A. RISKS OF CLOUD COMPUTING

Privacy protection is taken to prevent the exposure of personal information and sensitive information stored in the cloud, the sharing of data, computing, integrity verification, delete and other operations, as well as the entire life [1]. In order to protect the user's information and personal privacy, several solution methods usually are taken, such as access control, encryption, trust technology or a variety of combination of the above methods [2], [4]–[6]. Dynamic computing and storage services of cloud computing promote significant changes in information technology field [12], [14], at the same time, which also has brought tremendous impact to security and privacy, as follows:

(1) Virtualization technology and the relevant multi-tenant model can cause data loss in the same physical device.

(2) There is lack of trust between the user and the cloud platform, so users do not believe that the data is used in the cloud platform.

(3) The information is highly centralized, and security method must meet the requirements of processing in the cloud.

B. TRADITION ACCESS CONTROL

Privacy and security are the core of cloud, how to achieve secure and efficient access control of data resources has become a key issue in cloud computing [4]. After identifying the legitimate identity of the user, the access control system restricts the ability and scope of the requester to access the data, which is usually used to protect key information resources and prevent the intrusion of illegal operation of legitimate users [8], [9], [11], [12].

There are many important access control technologies [8]–[10], such as DAC (discretionary access control), MAC (mandatory access control), RBAC (role based access control), TBAC (task based access control), UCON (usage control), ABAC (attribute based access control), the performance comparisons are shown in Table 2, both '$\surd$' and '$\times$' denote 'yes' and 'no', respectively. Based on the content evolution of policies, multiple access control models have inherent relationship logic as shown in Fig. 3. A group of rules and procedures can enable legitimate users' authority to various data access in the access control, which is a key technology to guarantee the information confidentiality, integrity and data privacy in the network security [1], [6], [16]. Compared the traditional network environment, the access control technology is more important in cloud environment [5], [8]. When using the services of storage and computing of cloud, the users must pass authentication of the CSP and take the appropriate policies to access data and services. In order to ensure the cloud computing security, mutual authentication and access control between service providers are needed, and cloud customers not only need to prevent side channel attack, but also need relevant mechanisms to ensure data security [14], [15].

At the present market, CSP make use of different access control mechanisms in the cloud platform to provide security protection, and the academic circles study security and

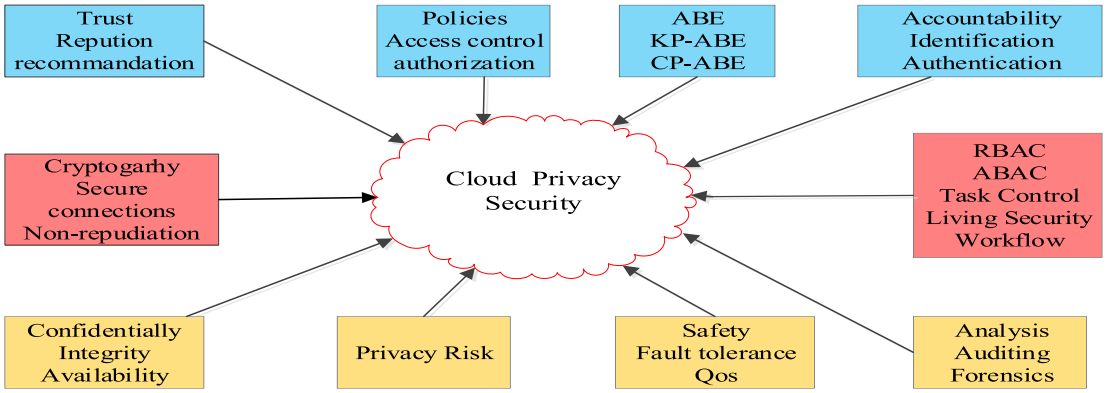


FIGURE 2. Cloud computing risks and related technologies.

TABLE 2. Comparison of general access control models.

	RBAC	TBAC	ABAC	UCON	MAC	DAC
Safety	×	×	×	√	√	×
Confidentiality	×	×	×	×	√	√
Authority flexibility	√	√	√	√	×	√
Minimum privilege	√	√	√	√	√	×
Separation of duty	√	√	√	×	√	×
Descriptive ability	√	√	√	×	√	√
Fine-grain	×	√	√	√	√	√
Constraint description	√	×	√	√	√	×
Dynamic	×	√	√	√	×	√
Compatibility	√	×	√	√	×	√
Expansibility	×	√	√	√	×	√
Management ease	√	×	×	×	√	×
Modeling ease	√	×	√	×	√	√

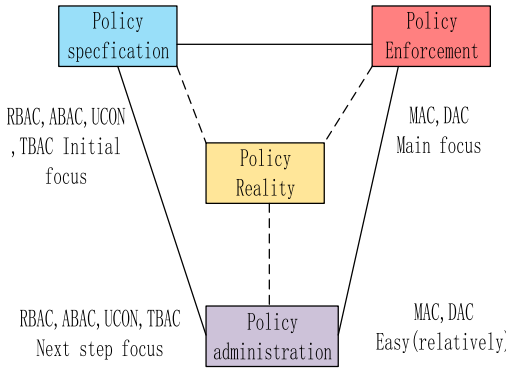


FIGURE 3. Relationship of multiple access control models.

privacy from the view of system and structure technology [9], but there are still many problems:

- Cloud security architecture: Both subjects and objects have not been clearly distinguished from the past time, and the corresponding access control technologies have expanded from the user's authority in a secure way, access virtual resources and storage data in the cloud environment [2]. In addition, there are contradictions between traditional distributed access control and centralized resource management in the cloud computing, and open policies have formed a severe test for cloud security management [3], [4].
- Cloud security mechanisms: because lots of the applications belong to different security management domains in the cloud, when users need to cross domains access resources, the certification services need to be set up in the domain boundaries to formulate public policies [2], [6]. When multiple tenants have caused side channel attack, this can easily lead to privacy leakage [12].
- Cloud access control security model: the concept and connotation of subjects and objects in the cloud has changed greatly, so the traditional access control model has been unable to meet the requirements of the cloud computing [9]–[12]. In the cloud environment, the relationships of the roles are complex, the scale of users changes frequently, the number of the administrator is numerous, the level is complex, and the assignment of authority is different from the traditional model.

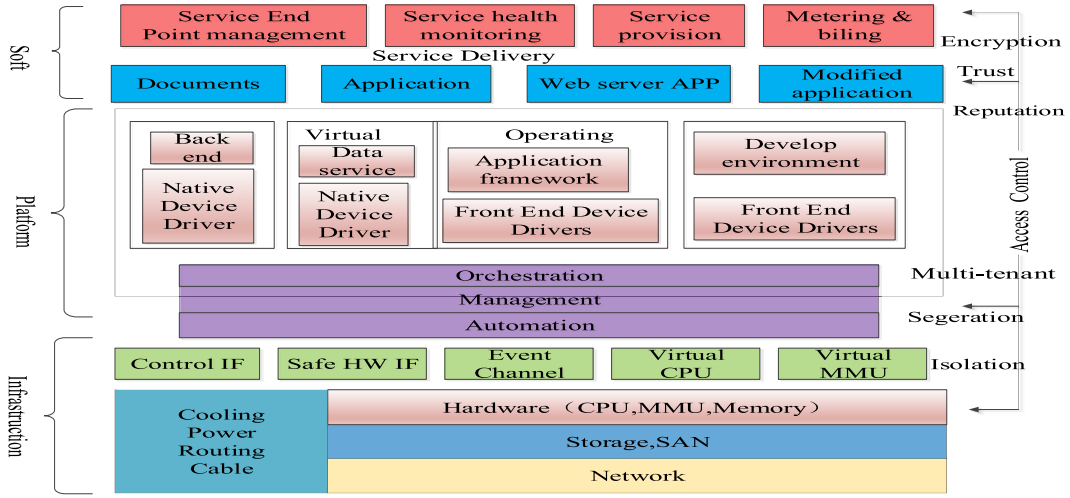


FIGURE 4. Privacy protection framework of cloud computing system.

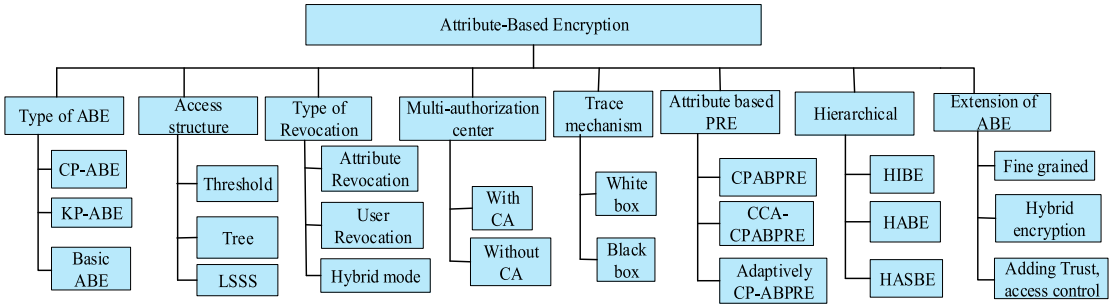


FIGURE 5. The main research content of ABE.

In the traditional mode, the user can handle data in a reliable and trust environment, but it is completely different in the cloud environment [4]. Because both user and the server are not completely credible, users must ensure data security, prevent CSP malicious disclosure or analysis of mining user privacy data. In a word, it is necessary to combine a variety of technologies to build a comprehensive privacy protection framework of cloud computing (Fig. 4), we will introduce attribute-based encryption, access control, search encryption, trust and reputation technology and so on.

III. PRIVACY PROTECTION BASED ABE

User and CSP do not trust each other in the public cloud environment, so the user uploads the ciphertext to the cloud platform [4]. In order to ensure the data security and protect the user's privacy, it requires that the encryption key is generated and managed by the data owner [8]. At present, many schemes of privacy protection based on access control have been proposed in the industry domain. An important problem is how to selectively share documents based on fine grained attribute access control policies in public cloud [6], [11].

An approach is that the encrypt documents satisfy different policies with different keys in the different cryptosystems, such as symmetric encryption, attribute-based encryption, proxy re-encryption [12], [13], [16]. However, such an approach has some weaknesses, which cannot efficiently handle adding/revoking users or identity attributes, and require to keep multiple encrypted copies of the same documents, further incur high computational costs [15]. Without utilizing public key cryptography and allowing users to dynamically derive the symmetric keys at the time of decryption, one can address the above weaknesses [9], [14].

A. RELATED KNOWLEDGE

ABE belongs to public key encryption mechanism. Its object of decryption is a group, not a single user [16]. The key feature is the introduction of attribute concept. Group refers to users with certain combination of attribute values [17]. For example, undergraduate students in computer colleges refer to a group of undergraduates whose attributes are computer colleges.

1) DEVELOPMENT OF ABE

Since 2005, ABE has made significant progress in KP-ABE, CP-ABE, revocation mechanism, access structure, multi-authority, hierarchical architecture, trace mechanism, proxy-encryption, and other extension of ABE [15], [18], details are shown in the Fig. 5.

ABE uses the combination of attributes as the public key of the group, and all users send data to the group by using

the phase public key [18]. In the example above, {computer, college, undergraduate} is the public key to send cryptography to undergraduates of computer college. The private key is calculated and distributed to individuals by the attribute authority [17].

2) RELATED DEFINITION

ABE mechanism uses access structure representation policy, takes bilinear pairing as the technical basis, and constructs security based on various mathematical problems and assumptions [17]. The following are the formal definitions of the basic concepts.

Definition 1 (Access Structure A *[17]):* Assuming that $\{P_1, P_2, \cdots, P_n\}$ is a collection of participants, $P = 2^{\{P_1, P_2, \cdots, P_n\}}$. Access structure A is a non-empty subset of $\{P_1, P_2, \cdots, P_n\}$, and A $\subseteq$ $P\backslash\{\emptyset\}$. if A is monotonous, $\forall B, C$, if $B \in$ A and $B \subseteq C$, then $C \in$ A.

The expressive ability of access structure is an important factor that restricts the development of ABE technology, and it is related to the efficiency of the whole access control system and the definition of protection granularity. Current types of access structure can be divided into three categories: threshold, access control tree and secret sharing mechanism. [18] proposed threshold content as an access control structure for the first time. The threshold structure (k, n) divides the secret information s into n parts by Lagrange interpolation theorem, the secret s can be reconstructed only when no less than k information cooperates.

As shown in Fig. 6, k_x represents the threshold requirement to recover secret information, when $k_x = 1$, threshold denotes (''OR''); when $k_x = n$, threshold denotes (''AND'').

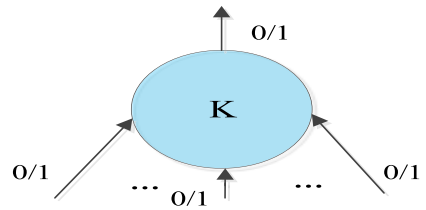


FIGURE 6. Threshold access structure.

Threshold scheme has the advantages of simple implementation and low system complexity. The development of ABE started from the threshold structure. Many studies are based on the threshold structure. However, due to the single operation of the threshold structure, only a single ''AND'' or ''OR'' operation can be performed. This method can simply reflect the relationship between attributes.

The introduction of tree structure effectively improves the expressive ability of access structure [18]. As shown in Fig. 7, tree structure combines multiple ''AND'', ''OR'' and ''threshold'' operations to enable access structure to reflect more complex logical relationships among attributes. T is a tree access structure in which non-leaf nodes represent a threshold structure described by their children and corresponding thresholds. Leaf nodes represent a corresponding attribute, and $k_x = 1$, when x is a leaf node, the corresponding attribute is denoted as $attr(x)$. Let num_x denotes the number of sub nodes of node x, the sub nodes of each parent node are numbered sequentially from 1 to num_x. The following methods are used to determine whether the set of attributes satisfy the access control policy described by the access control tree. Let T represents an access structure tree. T_x denotes a subtree that is considered x root in T, when the root node is r, then T can be expressed as T_r. If attribute set ω conforms to the access control policy of T_x, then $T_x(\omega) = 1$. $T_x(\omega)$ can be calculated recursively as follows.

(1) If x is a leaf node, and $attr(x) \in \omega$, then $T_x(\omega) = 1$.

(2) If x is not a leaf node, x' is the subnote of x, and computing $T_{x'}(\omega)$, if k_x number of subnodes x' satisfy with $T_{x'}(\omega) = 1$, then $T_x(\omega) = 1$.

(3) Although the tree scheme has made some improvements on the basis of the threshold scheme to enhance the expressive ability of the access structure, it needs to specify the size of the attribute and user space in the initial stage of the system, which can't meet the dynamic growth of the number of users and attributes in the new computing environment.

In order to improve the security of the system, researchers proposed an access structure based on LSSS (Linear Secret-Sharing Schemes [20]). LSSS can effectively prevent key loss and malicious user attacks, and reduce the risk among secret sharing users.

Assuming that (M, ρ) represents access structure A. M is a $l \times K$ matrix, ρ is a function of mapping row element $\{1, 2, \cdots, l\}$ in a matrix to secret sharing participant P. The specific linear secret sharing method includes the following steps:

(1) Secret sharing algorithms. Let us random choose $k-1$ number of $v_1, v_2, \cdots, v_{k-1}$ from Z_p, combine secret s_{to} form a k dimensional vector $v = (s, v_1, v_2, \cdots, v_{k-1})$; if A_i is the i line element in the matrix, then the secret shared component of secret participant $\rho(i)$ is defined as $\sigma_i = A_i \bullet v$.

(2) Secret recovery algorithms. If a set of attributes of a secret participant is $\omega \in A$, let $L = \{i|\rho(i) \in \omega\}$, then a set of recovery coefficients $\{\mu_i\}_{i \in L}$ can be calculated according to A, and $\sum_{i \in L} \mu_i \bullet \sigma_i = s$.

(3) Although the transition of access structure from threshold structure and tree structure to more complex LSSS can solve the requirement of attribute space and user space in the initial stage of the system, it also increases the complexity of public key design and the computational cost of the system.

Definition 2 (Bilinear Pairings [21]): Map: $e : G_1 \times G_1 \rightarrow G_2$. It satisfy these characteristics:(1) Bilinearity : $\forall a, b \in Z_q, \forall f, h \in G_1$, we have $e(f^a, h^b) = e(f, h)^{ab}$, then $e : G_1 \times G_1 \rightarrow G_2$ is bilinearity; (2) Non-degeneracy: $\exists f \in G_1$, then $e(f, f) \neq 1$; (3) Computation: $\forall f, h \in G_1$, there is an efficient algorithm for computing $e(f, h)$. Noting: $e(f^a, h^b) = e(f, h)^{ab} = e(f^b, h^a)$, and $e(*, *)$ is symmetric operation.

Definition 3 (Computation Diffie-Hellman Assumption [22]): Let us random choose $a, b \in Z_q^*$, compute g^{ab} based on a predefined triple couple (g, g^a, g^b).

Definition 4 (Decision Bilinear Diffie-Hellman (DBDH) [22]): Let us random choose $a, b, c \in Z_q^*$, $R \in G_2$, and judge whether equation $e(g, g)^{abc} = R$ is valid or not based on a preset triple couple (g, g^a, g^b, g^c, R).

Definition 5 (Decisional Linear(D-Linear) [23]): Let us random choose generator g, f, v of group G with order q, random select exponent $a, b \in Z_q$, $R \in G$, determine whether equation $v^{a+b} = R$ is validate or not based on the preset element (g, f, v, g^a, g^b, R).

Definition 6 (Indistinguishability Under Chosen Ciphertext Attack (IND-CCA) [24]): The interaction between the adversary and the challenger is as follows:

(1) The challenger establishes the encryption scheme systematically, outputs the public-private key pair and gives the public key to the adversary.

(2) The adversary can make some decryption inquiries to the challenger who decrypts the ciphertext and returns the result to the adversary.

(3)The adversary chooses plaintext M_0 and M_1, and sends them to the challenger who tosses a fair coin $b\{0, 1\}$, encrypts plaintext M_b, and gets ciphertext C^* and sends it to the adversary.

(4) The adversary can continue to ask the challenger for decryption except ciphertext C^*.

(5) Finally, the challenger must answer 0 or 1 (denoted as $b^{'}$) as a guess of ciphertext. If $b^{'} = b$, the adversary wins the game. The advantage of the adversary in the game is defined as $\Pr[b' = b] - 1/2$. For an encryption scheme, if the adversary of probability polynomial time has negligible advantages in the above-mentioned games, the encryption scheme is called IND-CCA security [24]. In order to understand of this article, several relevant notations and meanings are given in Table 3.

3) SEVERAL MECHANISMS OF ABE

The participating entities of ABE system include authority agencies and users. Authority agencies supervise attributes and issue attribute keys to users [18], [25]. Users are divided into message senders and receivers, [18] proposed basic ABE (fuzzy identity-based encryption). Each attribute in the system is mapped to Z_q^* by hash function, and both ciphertext and user key are related to attributes. This mechanism supports attribute-based threshold policy, for example, if the attribute set of a paper in the library is {computer, security, English, doctor} and the number of attribute encryption threshold parameter is 2, then the attribute set of user is {computer, English, doctor} can access the paper, else can't access the paper while the attribute set is {English, doctor}.

The basic ABE mechanism includes four algorithms: Setup, Extract, Encrypt and Decrypt. During initialization, the system runs according to the security parameters and generates two groups G_1, G_2 with prime value q and bilinear pairs $e : G_1 \times G_1 \rightarrow G_2$, d is threshold parameter.

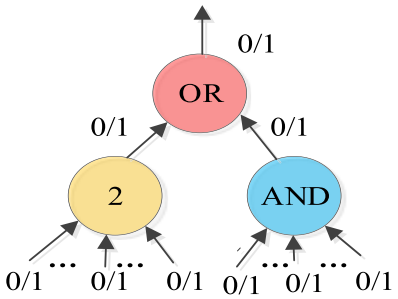


FIGURE 7. Tree access structure.

(1)Setup: Authorize agency randomly selects $y, t_1, t_2, \cdots, t_n \in Z_q$, system public key PK is $(T_1 = g^{t_1}, \cdots, T_n = g^{t_n}, Y = e(g, g)^y)$, $(y, t_1, \cdots, t_n)$ is master key MK.

(2) KeyGen: Authorize agency generates private key of user u, randomly selects a polynomial p of $(d - 1)$ degree, let $p(0) = y$, private key of user SK is $\{D_i = g^{p(i)/t_i}\}_{\forall i \in A_C}$.

(3) Encrypt: Sender encrypts messages with attribute A_C, random selects $s \in Z_q$, ciphertext is $(A_C, E = Y^s M = e(g, g)^{ys} M, \{E_i = g^{t_i s}\}_{\forall i \in A_C}) M \in G_2$.

(4) Decrypt: If $|A_u \cap A_C| > d$, receiver can choose d attribute, if $i \in A_u \cap A_C$, and compute $e(E_i, D_i) = e(g, g)p(i)s$, get $M = E/Y^s$ when finding $Y^s = e(g, g)^{p(0)s} = e(g, g)^{ys}$ with Lagrange interpolation method.

In the above mechanism, KeyGen algorithm uses Shamir threshold secret sharing mechanism [26], which embed secret y into each component D_i of SK to implement threshold policy. SK is related to random polynomial p, which makes it impossible for different users to carry out collusion attacks with their private keys. Encrypt algorithm uses bilinear pairing to encrypt messages, and the ciphertext components E_i are related to attributes, thus specify the necessary attributes for decryption. Random numbers s can prevent users from decrypting subsequent ciphertext successfully. In the above basic ABE mechanisms, PK is linearly related to the number of system attributes, and the number of power operations and bilinear logarithms is more [26]. The specific process is described in the following Table 4.

The basic ABE can only represent the "threshold" operation of attributes, and the threshold parameter is set by the authority center [18]. Many practical applications need to support 'AND', 'OR', 'threshold' and non-operation of attributes in accordance with flexible access control strategies, so that the sender can specify access control strategies. ABE is a type of public-key encryption in which the secret key of a user and the ciphertext are dependent upon attributes. In such a system, the decryption of ciphertext is possible only if the set of key attributes of user matches the attributes of the ciphertext. There are two types of attribute-based encryption schemes: key-policy attribute-based encryption (KP-ABE, Fig. 8) [19] and ciphertext-policy attribute-based encryption (CP-ABE, Fig. 9) [27].

KP-ABE: As shown in Fig. 8, user's keys adopt tree structure to describe access policy A_{u-KP}, the set of leaf nodes of

TABLE 3. Related notations and meanings.

Notation	Meanings	Notation	Meanings
G_i	Operation in group(exponentiation, multiplication,($i=1,2$), g is a random generator of G_1	$\|V\|$	Number of classes in the access graph G ;
C_e	e operation, e denotes bilinear pairing	n	Number of attributes in system
N'	$N'=\sum_{i=1}^{n} n_i$ is the total number of possible value of attributes, where attribute i has n_i possible values	ρ	Size of ciphertext in a symmetric key encryption scheme;
AA_k	The kth authority, $k \in \{1,2, \ ,N\}$, N denotes the number of authorities	$C_{ECC-DES}$	Decryption time of an elliptic curve based public key encryption scheme
s	Least interior nodes satisfying an access structure	A_u	Attributes of user u
$L*$	Bit-length of element in $*$	$\|*\|$	Number of elements in $*$
Z_q	Group $\{0, \ , q-1\}$ under multiplication modulo q . q is a prime number	C_{PRF}	Time of calculating the PRF (prediction random function)
$n_{c,aid}$	The total number of attributes belongs to the authorized institutions AA_{aid} in the ciphertexts	$n_{c,x}$	The number of ciphertexts which contain the revoked attribute x
$n_{non,x}$	The number of non-revoked users who hold the revoked attribute x	C_F	Time of calculating the value of polynomial;
$\|E\|$	The number of edges in the access graph G	C_H	Time of calculating the hash function;
$\|Z_p\|$	The size of an element in Z_p	$\|G\|$	The size of an element G
h	Path length between class V_i and V_j when class V_i wants to derive the encryption key of class V_j	C_{SE-DES}	Decryption time of a symmetric key encryption scheme
$\|G_T\|$	The size of an element G_T	$\|A\|$	The size of an access structure A
n	The number of cloud servers	A_k	Attributes managed by AA_k
l	Rows of the matrix M for LSSS	j	The number of attributes
y	The number of leaf nodes	A_C	Attributes with ciphertext C

TABLE 4. Steps of ABE algorithm.

Setup	Authority center generates master key MK and system public key PK
Encrypt	$CT = Encrypt(PK, M, T)$ sender encrypts attribute set T and message M , generates ciphertext CT
KeyGen	$SK = KeyGen(MK, A)$, authority center generates user's private key SK
Decrypt	$M = Decrypt(CT.SK)$ receiver gets M by private key

a tree is A_u. Ciphertext is related to attribute set A_C, when A_C satisfies A_{u-KP}, users can decrypt ciphertext.

The difference between KP-ABE and basic ABE mechanism are KeyGen and Decrypt algorithm. KeyGen algorithm can use secret sharing mechanism and adopt top-down method to define a random polynomial p_x whose number of times is less than the threshold value of nodes for each node x in the tree.

If $px(0) = p_{parent(x)}(index(x))$, and $parent(x)$ represents parent node of x, $index(x)$ represents the number index of x, when r is root note, then $p_r(0) = y$, and the master key y is dispersed into the private key component D_i corresponding to the leaf node.

Decryption algorithm decrypts each node by recursive process from bottom to top, and obtains the secret value needed to recover plaintext. In Fig. 8, A_C satisfies policy A_{u1-KP}, node set S in decryption tree is $\{AND\}$, the ciphertext adopts tree structure to describe the access policy A_{C-CP} and achieves the access control policy decided by the sender.

In CP-ABE, the user's key is related to attribute set A_u, when A_u, satisfies A_{C-CP}, the user can decrypt the ciphertext. Unlike the basic ABE algorithm, the length of PK and MK is independent of the number of system attributes in the CP-ABE. Both KeyGen and CP-ABE use two-stage random mask to prevent collusion among users. The user's private key is related to the second-stage random number.

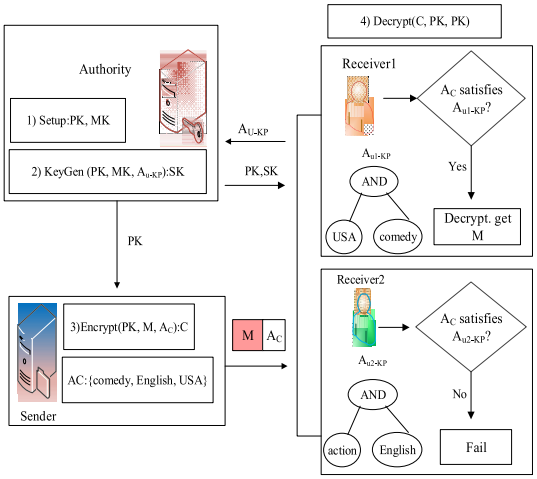


FIGURE 8. KP-ABE mechanism.

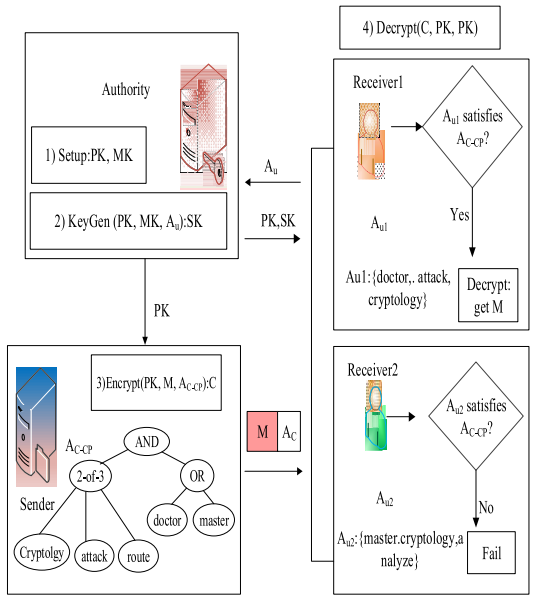


FIGURE 9. CP-ABE mechanism.

In encrypt algorithm, the implementation of access tree is similar to KeyGen algorithm of KP-ABE, the difference is $p_r(0) = s$, and the leaf node corresponds to the ciphertext component E_i. Decrypt algorithm is same as KP-ABE, but the number of bilinear pairing is two times. In Fig. 9, A_{u1} satisfies A_{C-CP}, and the set of internal nodes s in the tree is decrypted {or, 2-of-3, AND}.

Because the encryption rules are contained in the encryption algorithm, the cost has been greatly reduced in network bandwidth and node processing overhead. In KP-ABE, users' secret keys are generated based on an access tree that defines the permission scope of relevant users, and data are encrypted over a set of attributes.

However, CP-ABE uses access tree to encrypt data, and users' secret keys are generated over a set of attributes. The access control policy is associated with the ciphertree, the decryption key is bound by a set of attributes that can be described, and the decryption key can be obtained when the decryption party own the attributes matched polices.

CP-ABE algorithm is quite popular in the cloud environment [28]. In short, three ABE schemes are quite different, specific details are shown in Tables 5 and 6, basic ABE can only use threshold police, the scope of application is relatively limited; both KP-ABE and CP-ABE have much wider applications, but the burden of encryption, decryption and communication is very heavy.

The encryption party has no need to know who decrypt the encryption information, when the decryption party can meet the appropriate policy, which can decrypt the ciphertext. ABE algorithm is based on Bilinear pairing theory of elliptic curve, which is impossible to be deciphered [29]. ABE is attached to an access structure in the security simulation, which is difficult to be embedded into an ordinary hard assumption because of the complexity of the access structure, so it is very safe in theory and practice [30].

B. REVOCATION MECHANISM

When the user's attribute changes, the system cannot be accessed the data in the ABE system. How to efficiently revoke or change the user's attribute in the ABE mechanism is a very important problem [31].

Several revocation mechanisms are shown in Table 7, "/" denotes that a specific performance is not discussed. AA (attribute authority) expresses authority, if the user is offline, he can get updated information; else if the user is online, he can get the information from the online party. Reference [29] proposed a revocation mechanism; each attribute contains an active period. If an attribute of the system is removed, then the latest attribute will be stopped, when all users' keys are updated, the relevant attributes are not released. However, the encryption party needs to negotiate with the agency in the key update phase, users interacts with the agency online, the attribute cannot be revoked before the expiration time [32].

Reference [30] proposed a new update method of CP-ABE. In this scheme, authority department granted termination date for each user's attribute, the start time was attached to the plain text, and the end date is attached to the ciphertext. Reference [33] proposed a scheme based on CP-ABE mechanism, which used proxy encryption technology to support the revocation of KP-ABE, and the relevant member of the master key was updated with the revocation attribute, then it generated a new proxy key to comply the attribute of the instant revocation.

References [30], [36] presented an encryption method of identity attributes, improved the efficiency of the key update, and reduced the number of keys to the logarithmic order, but the scope of application is small and the conditions are harsh. References [33]–[35] proposed a new revocation mechanism that had no need to update the user key, but there is still a problem of heavy computing burden on the client side. Reference [37] proposed a new CP-ABE algorithm to achieve

TABLE 5. Comparison of KP-ABE and CP-ABE.

		KP-ABE	CP-ABE
$Setup(\lambda, U)$	Input	Safe parameters	Safe parameters
		Attribute Space Size	Attribute Space Size
		User Space Size	User Space Size
	Output	Public key PK	Public key PK
$Encrypt(PK, M, A)$	Input	Master key MK	Master key MK
		Public key PK	Public key PK
		Information M	Information M
		Attribute Set γ	Access structure A
	Output	Encrypt Data CT	Encrypt Data CT
$KeyGen(MK, S)$	Input	Master key PK	Master key PK
		Access structure A	Attribute Set γ
		Public key PK	NA
	Output	Encrypt key CT	User Private Key SK
$Decrypt(PK, CT, SK)$	Input	Public key PK	public key PK
		Encrypted Data CT	Encrypted Data CT
		Decrypt Key D	User Private Key SK
	Output	Raw data M	Raw data M

TABLE 6. Comparison cost of basic ABE, KP-ABE and CP-ABE.

System	Ciphertext	User's secret key	Encrypt	Decrypt	Policy
Basic ABE	$\lvert A_C \rvert L_{G_1} + L_{G_2}$	$\lvert A_C \rvert L_{G_1}$	$\lvert A_C \rvert G_1 + 2G_2$	$dC_e + 2dG_2$	Threshold
KP-ABE	$\lvert A_C \rvert L_{G_1} + L_{G_2}$	$\lvert A_u \rvert L_{G_1}$	$\lvert A_C \rvert G_1 + 2G_2$	$\lvert \mathrm{A_C} \rvert \mathrm{C_e} + 2 \lvert S \rvert G_2$	AND, OR, threshold
CP-ABE	$(2 \lvert A_C \rvert + 1)L_{G_1} + L_{G_2}$	$(2 \lvert A_u \rvert + 1)L_{G_1}$	$\lvert A_C \rvert G_1 + 2G_2$	$2 \lvert \mathrm{A_u} \rvert \mathrm{C_e} + (2 \lvert S \rvert + 2)G_2$	AND, OR, threshold

TABLE 7. Comparison of revocation schemes.

System	Executor	Online party	Support schemes		Speed	Revocation		
			KP-ABE	CP-ABE	Slow	User	User attribute	System attribute
[29]	AA	AA	Yes	Yes	Slow	Yes	Yes	Yes
[30]	AA	AA	/	Yes	Slow	Yes	Yes	Yes
[31]	AA	/	Yes	/	Fast	Yes	/	Yes
[32]	Third party	Third party	/	Yes	Fast	Yes	Yes	Yes
[33]	Third party	Third party	Yes	Yes	Fast	Yes	Yes	Yes
[34]	Sender	/	/	Yes	Fast	Yes	/	Yes
[35]	Sender	/	Yes	Yes	Fast	Yes	/	Yes
[36]	Hybrid	/	Yes	/	Medium	Yes	/	Yes

the access control of the encrypted text, but the encryption was in the client, so customers had to bear huge heavy encryption costs. Reference [38] proposed a secure and efficient data sharing framework with obligation capabilities in hybrid cloud. The scheme achieved the purpose of revocation, but the program's revocation unit was lack of fine grained access control.

Reference [39] proposed to add a time limit to the user's attributes, each attribute authority can dynamically delete any user from its domain, and those who are revoked cannot

TABLE 8. Comparison of three kinds of ciphertext access control.

Scheme	Procession				Encrypt	proxy Re encryption	Lazy encryption
	Initialization	Encryption	Generate user private key	Decryption			
[39]	Generate MK and PK	CT=encrypt （PK, M, T）	SK=KeyGen （MK, A）	M=Decrypt (CT, SK)	Client	Nonsupport	Nonsupport
[40]	Generate MK and PK	CT=encrypt （PK, M, A）	SK=KeyGen （MK, T）	M=Decrypt (CT, SK)	Client	Nonsupport	Nonsupport
[41]	Generate MK and PK	CT=encrypt （PK, M, A）	SK=KeyGen （MK, T）; Send the PK to cloud	M=Decrypt (CT, SK)	Cloud	Support	Support

access subsequent outsourced data, the specific mechanism is shown in the Fig. 10. Reference [40] proposed an attribute revocation scheme based on CP-ABE, CSP has a certain trust degree, the data owner would deliver the CSP implementation, but the access program structure tree only supported the ''AND'', therefore, it cannot provide a fine grained and flexible access control policy, these details are shown in Table 8. Reference [41] described the KP-ABE mechanism, and complied the fine grained access control policy simultaneously, greatly reduced the computational burden of the client.

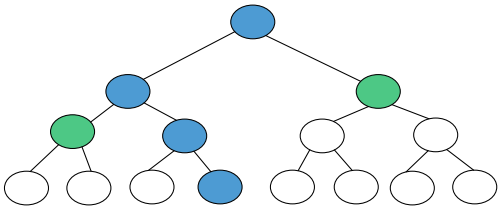


FIGURE 10. Revocation binary tree corresponding to time. Users are assigned to the leaf nodes. Blue nodes represent the revoked path of user. Green nodes are the minimum nodes that cover the reserve users [39].

C. MULTI-AUTHORITY ATTRIBUTE BASED ENCRYPTION (MA-ABE)

Every attribute of the user needs to obtain a private key with a trust authority in the ABE mechanism, which requires many authority centers, and can lead to increase the work load of the single authority and reduce the efficiency, so the emergence of the multi-authority centers is logical (Fig. 11). Multi-attributes are regulated by different authority, each attribute generates an encrypted private key to prevent the authority center to steal the private key [43], [46].

Each policy authority has a master key, in order to ensure the correct decryption operation, the total keys of the attribute authority are equal to the master key for the system [42]. Different collusion users can recover the master key, thus threat the system security, so the contradiction between the correctness and the security of the system is a difficult problem in the research of ABE. Because the central authority (CA) guarantees the operation of decryption, the research of

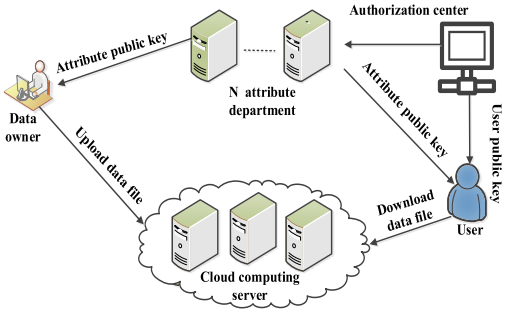


FIGURE 11. Multi-authority encryption.

multi-authority is divided into two categories: ABE with CA and ABE without CA.

Reference [43] constructed a new multi-privilege ciphertext strategy ABE scheme for cloud storage data access control system, which was proved to be self-adaptive and secure in the standard model, and supported monotonous access strategy. Reference [44] proposed an efficient and secure multi-privilege access control scheme for cloud storage, which did not need global permissions and can support any LSSS access mode, and proved security in random oracle model. Reference [45] designed an efficient and revocable data access control scheme for multi-privilege cloud storage system, then simulation results showed that the access control scheme is secure and more efficient in the random oracle model. Reference [46] proposed a hierarchical attribute set access control scheme, that added attribute set signature based on the CP-ABE, multi-authority was performed by hierarchical procession, each layer of authority was responsible for different algorithms. However, the revocation granularity is insufficient, so the scheme is difficult to play an advantage in the cloud computing. These comparison results of several articles are shown in the Table 9.

D. FINE GRAIN

These above encryption models are based on user's identity or attribute, there are a lot of risks in the multi-tenant cloud

TABLE 9. Comparison of multi-authority schemes.

Scheme	Central Authority	Revocation Message	Backward Security	Forward Security	Revocation Enforcer	Ciphertext Updater
[43]	Yes	$O(n_{c,x} \bullet n_{non,x})$	Yes	Yes	Owner	Owner
[44]	No	$O(n_{c,aid} + n_{non,x})$	Yes	Yes	Authority	Server
[45]	No	$O(n_{non,x})$	Yes	Yes	Authority	Server

TABLE 10. Comparison of several fine-grained access control scheme.

Schemes	KeyGen	Encryption	Decryption	Type
[56]	$(2+2j)\|G\|+2j\|Z_p\|$	$(1+3l)\|G\|+2l\|Z_p\|$	$\|A\|+\|G_T\|$	Offline
[57]	$2y\|G\|$	$(1+3l)\|G\|+2l\|Z_p\|$	$\|A\|+\|G_T\|$	online
[58]	$2y\|G\|$	$n(\|A\|+2y\|G\|)$	$\|A\|+\|G_T\|$	online

environment. Therefore, it is necessary to build a flexible, efficient and fine-grained ABE to protect the privacy and integrity of the user data in the dynamic cloud environment [51].

Reference [47] proposed a fine-grained data access control scheme to support cloud-based expressive access policy with fully hidden attributes in the internet of things. Specifically, because of random characterizes, attribute information is completely hidden in access policy, and a fuzzy attribute mechanism based on Bloom filter is developed to decrypt ciphertext successfully. Reference [48] proposed a hybrid access control scheme, which divided user's domain into private and public party. The private party is used for CP-ABE, while the public party is used for the hierarchic access control in order to compensate for fine-grained access. However, encryption had been achieved on client party, which did not make full use of cloud computing capabilities and increased the burden on customers. Reference [49] proposed an effective compatible encryption system that held the feature of RBAC and ABE, users accessed the cloud data when ABE encryption is adopted. Reference [50] proposed a license scheme based on trust and reputation mechanism. In the scheme, an ABE mechanism is proposed to enable data owners and authentication centers to identify cloud data by peer-to-peer encryption and token strategy. Especially, in a less trust cloud environment, data owners can still control their data. Based on CP-ABE mechanism, [51] proposed a secure access control scheme for cloud storage, which formalized 'read' and 'write' operation through public and private keys, and accessed data through passwords. The scheme was more transparent to users, and the key generation was almost independent of users.

In the [52], a kind of access control framework based on the ABE was proposed to realize the privacy protection and permission authentication in the cloud. In this framework, cloud platform can carry out an authentication before the data was uploaded by the data owner. Reference [53] proposed a scheme to ensure both efficiency and security by combining symmetric encryption with asymmetric encryption. Both CP-ABE and XACML were combined through the public attribute set; symmetric cryptography was used to achieve the confidentiality of massive data in the cloud storage. During the transmission of medical data, it is easy to lead to the leakage of patient's privacy information, so [54] provided a robust and lightweight heartbeat protocol to deal with the key revocation problem. Based on the constant-size ciphertext policy comparative attribute-based encryption, [55] proposed a new effective framework which supported negative attributes, embedded relevant attributes into the user's key, and merged these attributes constraint into a ciphertext in the encryption process, and implemented flexible access control strategies with different range relationships.

Reference [56] developed a new technology for ABE, which divided the computation of these algorithms into two stages: the preparatory stage completed the work policy of encrypting messages or creating keys before knowing the message or attribute list/access control policy; the action stage assembled ABE ciphertext or key. Although existing outsourcing ABE solutions can offload some intensive computing tasks to third parties, the verifiability of results from third party has not yet been resolved, so [57] proposed a general and efficient solution, which introduced security outsourcing technology into ABE. Further, [58] proposed a new ABE system, which supported the issuance of security outsourcing keys and decryption, and performed a fixed number of simple operations locally for the attribute issuer. These corresponding comparison results are shown in Table 10, in terms of the burden of decryption, these four articles [16], [56]–[58] are the same, and [58] performs better in terms of key generation and encryption than other three schemes.

TABLE 11. Comparison of trace schemes.

Traceability	Literature	Mechanism	Safety	Collusion	Expression	System space
White Box	[59]	CP-ABE	Selection	No	Monotone	Limited
	[60]	CP-ABE	Complete	Yes	Any Monotone	Infinite
Black Box	[61]	CP-ABE	Selection	Yes	Monotone	Limited
	[62]	KP-ABE	Complete	No	Monotone	Limited
	[63]	CP-ABE	Complete	No	Any Monotone	Limited
	[64]	CP-ABE	Complete	No	Any Monotone	Limited

E. TRACE MECHANISM

In ABE mechanism, users can acquire new attributes set by collusion, and obtain the corresponding permissions. In order to solve these problems, it is necessary to enhance the security of access control system [16]. According to the different requirement by the algorithm, the research of traceability can be divided into white-box and black-box mechanism [59]. White-box uses the key as the input content of the trace algorithm to track the key of the user. According to the decryption device, black-box does not know the decryption algorithm and the information of the decryption key [60]. Black-box mechanism provides the device with ciphertext and gets the deciphered plaintext from the device, so that it can be traced to at least one user [61].

Based on the DBDH, [59] proposed a white-box scheme, which adds unique identity attributes to each ABE user. When generating user's private key, besides the attributes of access control policy, the user submits the corresponding body. The scheme solved the problem of malicious key distribution and collusion attack; however, it only supported selective security. In order to improve the security of white-box mechanism and the expressive ability of access control system, [60] proposed an efficient and expressive traceable ABE mechanism based on signature mechanism, which can support arbitrary monotonous access structure. Then, [61] proposed a collusion-proof black-box KP-ABE mechanism, which supported arbitrary monotonous access structure under the standard model, and had more efficient efficiency.

Based on the DBDH and D-Linear, [62] proposed a traceable CP-ABE scheme. Two different encryption algorithms are designed in this scheme. When using ordinary encryption algorithm, the encryption of information does not contain personal identification information, and all users satisfy the access control policy that can decrypt ciphertext. Because users can't distinguish between encryption and ordinary encryption algorithm, the strategy hiding is realized. However, the trace mechanism may significantly increase the length of decryption key and ciphertext while protecting the privacy of users. Reference [63] proposed a black-box scheme, which has the following advantages: (1) it supported the traceability of completely anti-collusion black-box; (2) the traceability of the new system did not require secret input. Reference [64] proposed a specific scheme to support black-box mechanism, which can identify a user's key from multiple users. The relevant comparison results of trace schemes are shown in Table 11.

F. PROXY RE-ENCRYPTION (PRE)

The attribute-based proxy re-encryption (ABPRE) scheme combines the traditional proxy re-encryption with ABE, and the user can decrypt the re-encrypted ciphertext with the associated attributes (Fig. 12). However, many ABPRE schemes required a lot of pairing operations, which meant huge computing overhead [65].

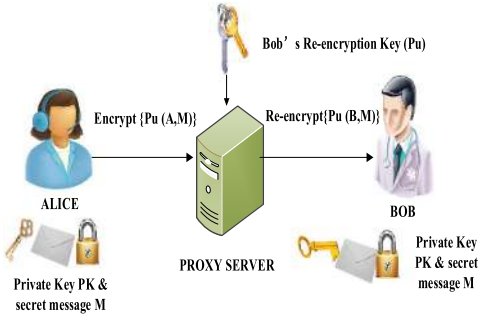


FIGURE 12. Proxy re-encryption.

In order to reduce the number of pairing based on exponential operations, a new ABPRE scheme can reduce the burden of operation delay by constant pairing [66]. In order to support multiple attributes, [67] proposed a new access strategy based on LSSS matrix structure. The scheme allowed the encryption program to decide whether the ciphertext can be re-encrypted and the proxy to be added access policies. Reference [68] proposed a new CCA-CP-ABPRE to solve the selected password text attack, which supported attribute-based re-encryption of any monotonous access structure. Reference [69] proposed a new CP-ABPRE which combined dual-system encryption technology with selective authentication technology to support monotonous access structure. Reference [70] proposed a new proxy re-encryption scheme, which can provide a fine-grained access control in cloud storage systems. This scheme required linear number of exponential and constant number of pairing calculations for encryption and decryption, which greatly reduced the

TABLE 12. Performance comparison of PRE (1).

Sys	Encryption	Decryption	Reencryption	Redecryption
[66]	$(n+2)G+2G_T$	$2P+(3n+2)G+2G_T$	$2P+3nG+G_T$	$3P+3nG+4G_T$
[67]	$(4\mid A_C\mid+2)G+2G_T$	$(2\mid A_u\mid+1)P+3G_T$	$(2\mid A_C\mid+1)P+4\mid A_C\mid G+3\mid A_C\mid G_T$	$(2\mid A_u\mid+1)P+(3\mid A_u\mid+2)G_T$
[68]	$(4\mid A_C\mid+2)G+G_T$	$(2\mid A_u\mid+1)P+3\mid A_u\mid G_T$	$(2\mid A_u\mid+2)P+(3\mid A_u\mid+1)G_T$	$(2\mid A_u\mid+2)P+3\mid A_u\mid G_T$
[69]	$(4\mid A_C\mid+4)G+2G_T$	$(2\mid A_u\mid+1)P+(2\mid A_u\mid+1)G_T$	$(2\mid A_u\mid+2)P+(2\mid A_u\mid+2)G_T$	$(2\mid A_u\mid+3)P+(2\mid A_u\mid+4)G_T$
[70]	$(n+3)G+2G_T$	$nG+2P$	$nP+(n-1)G$	$nP+2G+G_T$
[71]	$(4\mid A_C\mid+2)G+2G_T$	$2P+(4\mid A_u\mid-1)G+2G_T$	$2P+(4\mid A_u\mid-1)G+2G_T$	$3P+(4\mid A_u\mid-1)G+4G_T$

TABLE 13. Performance comparison of PRE (2).

Sys	PK	MK	SK	CP
[66]	$(3n+2)L_G+L_{G_T}+3nL_{Z_q}$	$(3n+3)L_{Z_q}$	$(n+1)L_G+L_{Z_q}$	$(3n+2)L_G+L_{G_T}+3nL_{Z_q}$
[67]	$(n+2)L_G+L_{G_T}$	L_G	$(\mid A_u\mid+2)L_G$	$(2\mid A_C\mid+2)L_G+L_{G_T}$
[68]	$3L_G+L_{G_T}+6Hash$	L_G	$(\mid A_u\mid+2)L_G$	$(2\mid A_C\mid+3)L_G+L_{\{0,1\}^{2k}}$
[69]	$(n+6)L_G+L_{G_T}$	$2L_G$	$(\mid A_u\mid+3)L_G$	$(2\mid A_C\mid+5)L_G+L_{G_T}$
[70]	$(n+2)L_G+L_{G_T}$	$L_G+(n+1)L_{Z_q}$	$(n+1)L_G$	$3L_G+L_{GT}+nL_{Z_q}$
[71]	$(n+2)L_G+L_{G_T}$	$L_G+L_{Z_q}$	$(\mid A_u\mid+2)L_G$	$(2\mid A_C\mid+2)L_G+L_{G_T}$

computational burden. Reference [71] proposed a secure CP-ABPRE scheme based on Waters' dual system encryption technology, which was constructed in composite order bilinear groups and proven secure under the complexity assumptions of the subgroup decision problem. The comparisons of trace schemes are shown in Tables 12 and 13, [70] needed a constant number of paring operations in reencryption and decryption when compared with [66]–[69] and [71], computation burden is much lower.

G. HIERARCHICAL ENCRYPTION

In practical applications of cloud computing service, hierarchical management mode is usually used for such applications, such as hierarchical identity-based encryption (HIBE), hierarchical attribute-based encryption (HABE, Fig. 13) and hierarchical attribute-set-based encryption (HASBE) and so on [72].

1) HIERARCHICAL IDENTITY-BASED ENCRYPTION (HIBE)

Identity-based encryption (IBE) system is a simple, certificate-free public key infrastructure (PKI) model. HIBE improves the scalability of IBE by sharing the workload of root private key generator (PKG) among several lower-level pkg, thus facilitating the private key delegation. Because of its structure, HIBE can be deployed in cloud computing, pervasive computing systems, wireless sensor networks to provide access control [72]. At present, almost all existing HIBE schemes have a disadvantage that ciphertext size or private key size must depend on the hierarchical depth of

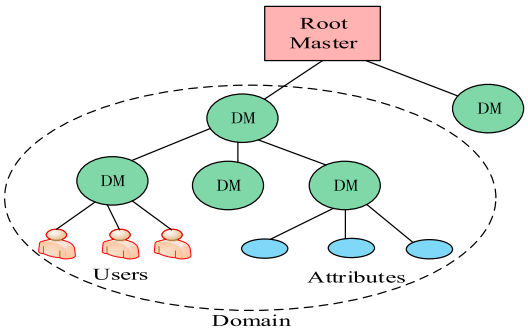


FIGURE 13. Hierarchical attribute based encryption scheme.

identity. To solve this problem, [73] proposed a new efficient HIBE scheme which had a constant size of ciphertext and private key, the size of ciphertext and private key was independent of the hierarchical level. In the standard model, many structures of HIBE must be fixed to the maximum depth. Reference [74] proposed a new anonymous HIBE scheme, which did not impose additional restrictions on system functions in public parameters. Because of static assumption, a nested two-system encryption parameter was adopted to prove complete security. Reference [75] proposed a hierarchical identity-based encryption (HIBE) scheme which was represented by scheme H1 and H2. In terms of provable security attributes, the direct construction of ciphertext of HIBE has one or more shortcomings, such as the security of selective identity attacks. Both H1 and H2 avoided these shortcomings

TABLE 14. Performance comparison of several HIBE schemes.

Scheme	Public parameters	MK	Private Key	CP
[73]	$(2Ln+3)G1, Z_p$	Z_p	$3G_1, Z_p$	$2G_1, 2G_T$
[74]	$8G_1$	$5G_1$	$(7+4j)G_1$	$(1+3j)G_1, G_T$
[75] (H1)	$(L+4)G_1$	$2G_2, (2L+5)Z_p$	$2(2(L-j)+5)G_2$	$3G_1, G_T, Z_p$
[75] (H2)	$(L+4)G_1, (2L+5)G_2$	$2Z_p$	$2(2(L-j)+5)G_2$	$3G_1, G_T, Z_p$
[76]	$(3L+6)G_1, 3G_2$	$(L+3)G_2$	$(6(L-j)+12)G_2$	$6G_1, G_T$

which can also be avoided by specifically HIBE schemes for internal product encryption. The anonymous HIBE scheme is suitable for anonymous communication system and public key encryption system with keyword search function. However, previous HIBE schemes have some drawbacks, such as weak security, short ciphertext size, and the construction of bilinear groups based on compound order, so [76] proposed an efficient anonymous HIBE scheme for short ciphertext based on prime order bilinear groups. Table 14 shows the comparison result of several schemes [73]–[76], such as public parameters, keys and ciphertext.

2) HIERARCHICAL ATTRIBUTE-BASED ENCRYPTION (HABE)

The HABE scheme offers fine-grained access control, scalability, and full delegation by combining the features of HIBE and ABE. HABE works in a disjunctive clause fashion and assumes that all attributes in one conjunctive clause are administered by the same domain master [77].

Cloud storage greatly facilitates the sharing of data between individuals and organizations on the Internet. Reference [77] proposed an attribute-based first-order bilinear group encryption scheme based on forward secure ciphertext strategy, which is the core construction of attribute-based data sharing scheme. The security of the scheme is proved in the standard model. Reference [78] proposed an attribute-based hierarchical encryption scheme, which combined the hierarchical identity-based encryption (HIBE) system with the ciphertext attribute-based encryption system. Reference [79] proposed a new ciphertext policy hierarchical ABE (CP-HABE). In this scheme, attributes are organized in a matrix, and users can delegate their access rights to lower-level users. These features enable the CP-HABE system to carry many users from different organizations through keys and achieve efficient data sharing.

3) HIERARCHICAL ATTRIBUTE-SET-BASED ENCRYPTION (HASBE)

HASBE combines the characteristics of attribute set based on encryption (ASBE) and HIBE, each user or data owner is managed by a domain authority [80]. There are five kinds of participants that can participate in the system: data owner, user, domain authority, parent/trusted authority and cloud service provider. The scheme uses the delegation algorithm to establish the hierarchy of system users. Reference [81] proposed a hierarchical encryption based on attribute set, which extended the user hierarchy to ASBE. This scheme not only had scalability of hierarchical structure, but also inherited flexibility and fine-grained access control in supporting composite attributes. Reference [82] proposed a HASBE scheme, which extended attribute set encryption based on ciphertext strategy of user hierarchical structure, and inherited the fine-grained access control of ASBE. In cloud computing, data owners and service providers are usually not in the same trusted domain. Further, [83] proposed a secure and efficient cloud computing data collaboration scheme based on hierarchical attribute encryption. When users decrypted ciphertext, this scheme provided partial decryption structure and constructed partial signatures by outsourcing signature computation. Reference [84] proposed a hierarchical attribute-set-based encryption. This scheme not only had the scalability of hierarchical structure, but also inherited the flexibility and fine-grained access control that supports ASBE composite attributes.

H. DISCUSS AND ANALYSIS OF ABE

Based on the above research, the advantages and disadvantages of various models are summarized in the following Table 15.

In short, ABE can well demonstrate advantages in cloud computing. On the one hand, ABE is suitable for cloud computing architecture, on the other hand, ABE can fully implement data access control in cloud platform [77]. The previous sections discuss the research process of ABE which has made considerable achievements, such as policy flexibility, attribute revocation, multi-authority center, proxy re-encryption and hierarchical encryption so on. But there are still many problems worthy of further study. According to the recent requirements and the drawbacks of existing algorithms, future work can be studied the following aspects:

- Optimizing the construction of CP-ABE scheme: many existing construction methods add additional restrictions or redundancy, researcher can try to design a new access structure, which can be represented by a monotone Boolean formula and implemented by a LSSS matrix as small as possible [74].
- Improving the efficiency of ABE schemes: most of existing ABE schemes use bilinear pairing as a convenient construction way. However, bilinear pairing has high

TABLE 15. Performance evaluation and comparison of several ABE mechanisms.

Algorithm	Fine-grained	Computation overhead	Revocation efficiency	Efficiency	Collision resistance	Association attributes	Access policy
ABE	Low	Average	Average	Average	Average	With cipher	With key
KP-ABE	Low	High	Low	Average	Average	With cipher	With key
CP-ABE	Average	Average	Low	Average	Good	With key	With cipher
CCP-CABE	Low	Low	Good	High	Good	With key	With cipher
MA-ABE	Average	High	Average	High	Average	Key or cipher	Key or cipher
PRE	Low	Low	Average	High	Average	Key or cipher	Key or cipher
HIBE	Low	High	Good	High	Good	With key	With cipher
HABE	High	Average	Average	High	Good	With key	With cipher
HASBE	High	Average	Average	High	Good	With key	With cipher

computational complexity, which makes the algorithm inefficiently, so researcher can construct ciphertext by mathematical method and decrypt ciphertext by constant pair or another method [77].

- Constructing new ABE schemes: identity-based encryption scheme can be constructed by bilinear pairing, quadratic residue, lattice theory. ABE is widely regarded as the generalization and extension of IBE, but it only consists bilinear pairs which have limitations in efficiency [75].
- Accountable ABE: accountability is a good method to prevent key abuse. For further research, it is necessary to design an efficient ABE scheme under these assumptions of the subgroup decision making problem with three primes [78], [79].
- Focusing on the applicability and practicability of ABE: a preliminary proposal of ABE can be put forward to achieve data confidentiality and fine-gained access control.

ABE has made considerable achievements in theory; however, it has not been widely used in applications because of huge computation burden and lack of trust among proxy nodes. Future research can pay more attention to the combination of ABE and other technologies in cloud computing environment, such as the combination of ABE and access control model, trust technology and so on.

IV. SEARCHABLE ENCRYPTION OF CLOUD COMPUTING

Due to the large growth of information technology, there is a large-scale data outsourcing to cloud servers, various attacks will destroy the confidentiality of cloud data. In order to prevent information leakage and protect data security, user' data often is encrypted to upload the cloud [85]. Because ciphertext is stored in the third-party servers, normal search schemes cannot be applied. It requires relevant searchable encryption method to find the target data [86].

To solve these problems, searchable encryption (SE) technology can guarantee the privacy and availability of data, and support the query and retrieval of ciphertext data. A searchable encryption scheme usually contains these algorithms: encryption, token, search and decryption, as shown in Fig. 14.

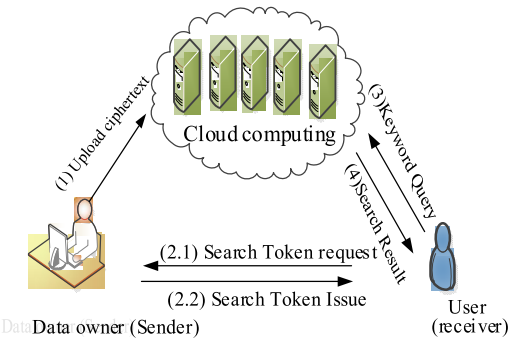


FIGURE 14. Architecture of searchable encryption.

1) Encryption: The user encrypts the data and generates the index structure, then uploads the index and ciphertext to the server.

2) Token: Users use a key to generate a trapdoor for keywords, which requires token not to reveal any information about keywords.

3) Keyword search: The server implements the search algorithm with the keyword, and returns the ciphertext containing the corresponding keywords. The server is required to obtain no more information except the keyword information in the ciphertext.

4)Decryption: Users use the key to decrypt the encrypted files feedback by the server and get the search results.

Searchable encryption schemes can be divided into two main types (Fig. 15):

1) Searchable symmetric encryption (SSE): SSE is an efficient ciphertext retrieval scheme based on symmetric encryption. Data owners and users share the same key information.

2) Searchable asymmetric encryption (SAE): SAE is suitable for one-to-many data sharing scenarios based on public key encryption systems. Its security is based on different

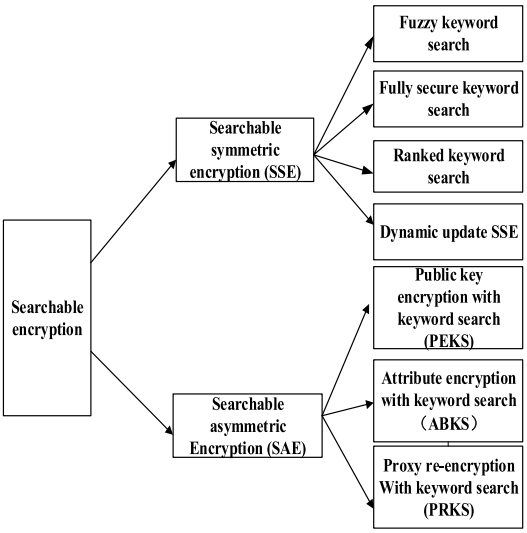


FIGURE 15. Classification of searchable encryption.

assumptions, such as, Decision Bilinear Diffie-Hellman (DBDH) [22]. Because SAE scheme is usually inefficient based on bilinear pairings, which leads to high complexity of the algorithm, because of the separation of public key and private key, it still very suitable for multi-user data sharing system.

A. SEARCHABLE SYMMETRIC ENCRYPTION (SSE)

SSE is a symmetric key encryption technology by selective search function. Some projects support more expressive keyword search, such as fuzzy keyword search [87]–[89], search based on fully secure keywords [90]–[92], multi-keyword ranked search [94], [95], dynamic update SSE [98]–[100].

1) FUZZY KEYWORD SEARCH

Fuzzy keyword search makes system utilities by providing possible matching files for user based on similarity semantics keyword. In this solution, the edit distance is used to evaluate the similarity of keywords.

Reference [87] provided a search scheme, which use locality-sensitive hashing (LSH) to ensure similar biometric readings from the same person. For the input with a smaller hamming distance, the LSH's output has the same hash value. Reference [88] proposed a general similarity search structure to measure the similarity distance by JacCard distance. This protocol is also interactive, which requires two rounds of communication to retrieve documents. Reference [89] proposed a fuzzy keyword search scheme based on similar semantics of editing distance. The idea is to estimate the fuzzy keyword set by editing distance of each keyword.

2) FULLY SECURE KEYWORD SEARCH

Reference [90] proposed a symmetric encryption scheme based on inner product. This scheme provided searchable indexes and tags as vectors and compute their inner product during the search phase. Further, they give a completely secure definition, that is the scheme implements predicate privacy (search tokens do not leak information about encoding query predicates) and plaintext privacy. Reference [91] also proposed a scheme based on inner product, which combined index generation technology with some homomorphic encryption, separated the query phase from file retrieval by introducing communication. So, this scheme had more flexibility and allowed users to retrieve documents selectively and efficiently.

Reference [92] proposed a keyword search scheme to support dynamic encrypted data based on reverse index. This scheme not only supported binary search (the time complexity is reduced from $O(n^2)$ to $O(\log n)$, n is the number of keywords), but also provided stronger security concepts: statistical plain text privacy and statistical predicate privacy. Reference [93] proposed a three-group symmetric key predicate encryption scheme. This scheme satisfied the selective security model under the non-interactive assumption, which used three hidden groups instead of four hidden groups.

3) RANKED KEYWORD SEARCH

Ranked keyword search refers to the system feedback results by the relevant criteria, such as keyword frequency which enhances the applicability of the system and meets the actual requirement of privacy protection in cloud computing.

Reference [94] proposed a multi-keyword search scheme based on similarity ranking to protect privacy. This scheme built search index based on word frequency, and vector space model can get higher search result precision based on cosine similarity. Reference [95] proposed a ciphertext keyword ranking search algorithm. According to secure inner product computation, they choose ''coordinate matching'' and ''inner product similarity'' to quantitatively measure the similarity. Reference [96] proposed a ranked search symmetric encryption (RSSE) scheme with small leakage of relevance score information. In order to search the encrypted file set, this scheme also designed a new encryption primitive, which used one-to-many mappings to protect privacy and verify the search results.

By constructing coordinate matching mechanism, a multi-keyword ranked search scheme was proposed to capture the correlation between data documents and search queries [97]. In addition, the scheme also quantitatively evaluated the related similarity measure by using the inner product similarity.

4) DYNAMIC UPDATE

SSE scheme can support to add or delete new files from the encrypted document set. After the client generates ciphertext, once new records are created, data must be updated in time. Reference [98] proposed a dynamic SSE (DSSE) scheme, but it leaked the hash of the unique keyword contained in the update document. Reference [99] deployed a dynamic symmetric searchable encryption scheme in databases. Although it shows progressive better performance than previous work, it also leaks more information. Reference [100] proposed an

TABLE 16. Comparison of SSE schemes.

scheme	security	Leakage function	Index size	Search time	Query type	Dynamics	Verifiability
[90]	FS	AP	$O(n^2)$	$O(n^2)$	Inner product	No	No
[92]	FS	AP	$O(n^2)$	$O(n \log n)$	Inner product	Yes	No
[93]	FS	AP	$O(n^2)$	$O(n^2)$	Inner product	No	No
[98]	IND-CKA2	SP, AP	$O(\Sigma_{i=1}^{n} \mid D_i \mid + n)$	$O(\mid D_i \mid)$	Single equality test	Yes	No
[99]	IND-CKA2	SP, AP	$O(\Sigma_{i=1}^{n} \mid D_i \mid + n)$	$O(\mid D_i \mid)$	Conjunctive Boolean	Yes	No
[100]	UC-CKA2	AP	$O(\Sigma_{i=1}^{n} \mid D_i \mid + n)$	$O(n)$	Conjunctive	Yes	Public/private

^{n} is the number of keywords in files. D is the ensemble of files. $\mid D_i \mid$ is the number of files in the keyword. FS, SP and AP stand for full security, search pattern and access pattern, respectively.

SSE scheme which allowed users to conduct secure joint keyword search, update outsourced file collection, and effectively verify the authenticity of search results. The verification mechanism of the scheme can be entrusted to a public trust agency.

5) COMPARISON OF SSE

Table 16 shows the comparison results of several SSE schemes from six important indicators: security, storage space complexity, search time complexity, query type, dynamics and verifiability. Reference [99] is more practical, because it has the characteristics of high efficiency, keyword search and dynamic update. Reference [100] is more suitable for public clouds, because it considers the reliability and privacy of stored files. Reference [92] provided a higher security of keyword privacy, it can be applied to cloud computing.

We discuss the investigation of searchable encryption techniques, further classify and compare different SE schemes according to safety, efficiency and function. However, many SSE schemes are impractical in terms of the performance and key management issues, they are not the preferred method of querying cloud service searches.

B. SEARCHABLE ASYMMETRIC ENCRYPTION (SAE)

In this section, we will analyze public key encryption with keyword search (PEKS), attribute-based encryption with keyword search (ABKS), and proxy re-encryption with keyword search (PRKS). Although these three solutions have relatively high computational complexity, both PEKS, ABKS and PRKS have shown better performance in terms of security and privacy with the revolutionary progress of hardware.

1) PUBLIC KEY ENCRYPTION WITH KEYWORD SEARCH (PEKS)

PEKS is an encryption method that uses public key system to search among ciphertexts. Because of good confidentiality performance, it has a wide range of applications.

Reference [101] proposed a novel PEKS to support privacy protection based on randomization without interaction between potential senders and receivers. Reference [102] proposed the concept of token privacy within the framework of PEKS. When two tokens are given, it is difficult to guess whether they correspond to the same keyword, so the security is guaranteed.

Reference [103] proposed the security concept of non-linkable IBE key, which guaranteed the privacy of search token in PEKS. However, this scheme is constructed on complex order groups. Compared with prime order elliptic curves, it need larger parameters and longer time to complete matching. Reference [104] proposed a keyword search scheme. It not only effectively supports binary search, but also significantly reduces the search complexity from $O(n)$ to $O(\log n)$, n is the number of keywords, which has strong security concepts, namely statistical IND-PEKS-CKA security and statistical search mode privacy.

Reference [105] proposed a new fuzzy keyword search scheme. In this scheme, the untrusted server can obtain the fuzzy search trap gate, but can't exact trap gate, and defines semantic security under chosen keyword attack (SS-CKA). Reference [106] proposed a new public verifiable search asymmetric encryption framework. It provided strong support for outsourcing encrypted data based on IND-PEKS-CKA security.

Table 17 show the several PEKS schemes according to the six important indicators: security, storage space complexity, search time complexity, query type, dynamics and verifiability; both [101], [102] and [103] have higher query efficiency, both [104] and [106] provide better security protection. Reference [104] has higher search efficiency, and [106] provides more flexible and secure verification.

2) ATTRIBUTE-BASED ENCRYPTION WITH KEYWORD SEARCH (ABKS)

ABKS is an important encryption search method that uses attribute-based encryption mechanism to encrypt data. This search technology allows users to search keywords for encoding cloud data when the attributes of users satisfy the access policy.

Reference [107] proposed an attribute based encryption with keyword search scheme of feedback results. However, the validation of correctness of keywords is very expensive. Reference [108] proposed a new primitive ciphertext-policy attribute-based encryption with keyword search. If the attribute credentials of user cannot satisfy the access control policy of data owner, the user cannot search the ciphertext.

Reference [109] proposed an efficient keyword search scheme based on key policy attributes, which greatly reduced the complexity of computation. However, the scheme was

TABLE 17. Comparison of several PEKS schemes.

Scheme	Security	Leakage function	Index size	Search time	Query type	Dynamics	Verifiability
[101]	Predicate privacy	Sp,Ap	$O(n)$	$O(n)$	Single equality test	No	No
[102]	IND-PEKS, PKP	Sp,Ap	$O(n)$	$O(n)$	Single equality test	No	No
[103]	Key unlinkabilty	Sp,Ap	$O(n)$	$O(n)$	Single equality test	No	No
[104]	IND-PEKS-CKA	Sp,Ap	$O(n)$	$O(\log n)$	Inner product	No	No
[105]	SS-CKA	Ap	$O(2n)$	$O(2n)$	Fuzzy	No	No
[106]	IND-PEKS, SPP	Sp,Ap	$O(n)$	$O(n)$	Inner product	No	Public/private

^{n} is the total number of keywords in files; both PKP, SPP stand for perfect keyword privacy, search pattern privacy, respectively.

TABLE 18. Comparison of ABKS schemes.

Scheme	Security	Query type	Verifiability	User revocation
[107]	CKA, keyword, secrecy	Single	No	No
[108]	KGA	Single	No	No
[109]	CKA, Key secrecy	Single	No	No
[110]	CKA, trapdoor unlinkability	Conjunctive	No	Yes
[111]	N/A	No	Public/private	No
[112]	CPA	No	No	No

not dynamic enough to adapt to the multi-attribute situation. Reference [110] presented a keyword search scheme, which can effectively remove users in the cloud system. This scheme allowed owner to independently encrypt data and outsource cloud servers. Reference [111] studied application scenarios of multi-sender and multi-user, and proposed a flexible synonym keyword search scheme. Further, [112] proposed a new ABE scheme, which achieved keyword search through key publishing, CSP can execute partial decryption without knowing the plaintext to reduce the computational burden.

Table 18 shows the comparison results of several ABKS schemes in terms of security, query type, verifiability and user revocation, [110] can provide keyword search, verifiability and user revocation, so it has strong security. Although [108] considers both keyword privacy and access strategy, it does not support joint keyword search, verifiability and user revocation. Therefore, [110] is more suitable for cloud services than other existing ABKS schemes.

3) PROXY RE-ENCRYPTION WITH KEYWORD SEARCH (PRKS)

PRKS is a basic encryption technology that uses proxy re-encryption system to search encrypted data. It allows authenticated data users to grant search functions to other users by re-encrypting out-of-source data.

Reference [113] proposed two security concepts of PRES: message privacy and keyword privacy. For message privacy, adversary can obtain plaintext of almost all ciphertexts. For keyword privacy, adversary can obtain plain text of any ciphertext, as well as almost all tokens, but it cannot determine which keyword corresponds to a given ciphertext. Reference [114] proposed a new searchable proxy reencryption scheme, which extended the original definition of PRKS for encrypting key generation and keyword ciphertext. This approach separated the encryption of messages from the encryption of keywords, so that it has the flexibility to choose the PRKS schemes to meet practical requirements.

References [115] and [116] presented proxy keyword search encryption scheme, respectively. Both schemes achieve the security of ciphertext, keyword anonymity, unidirectionality, non-interaction and collusion resistance. Reference [117] further introduced a new primitive: constrained one-hop proxy re-encrypted to support connection keyword search. However, PRKS can only consider coarse-grained enforcement, which delegates search functions to a specific authorized user. Based on the combination of attribute-based encryption and proxy re-encryption, [118] proposed a new method, which allows data owners to delegate keyword search functions to users who conform to specific access control strategies.

Table 19 shows the comparison results of several PRKS schemes in terms of security, query types and multiple users. [118] can delegate keyword search functions to multiple users who conform to specific access control strategies. Other PRKS schemes cannot re-authorize search privileges for multiple users in one operation. Therefore, [118] is more suitable than other PRKS schemes.

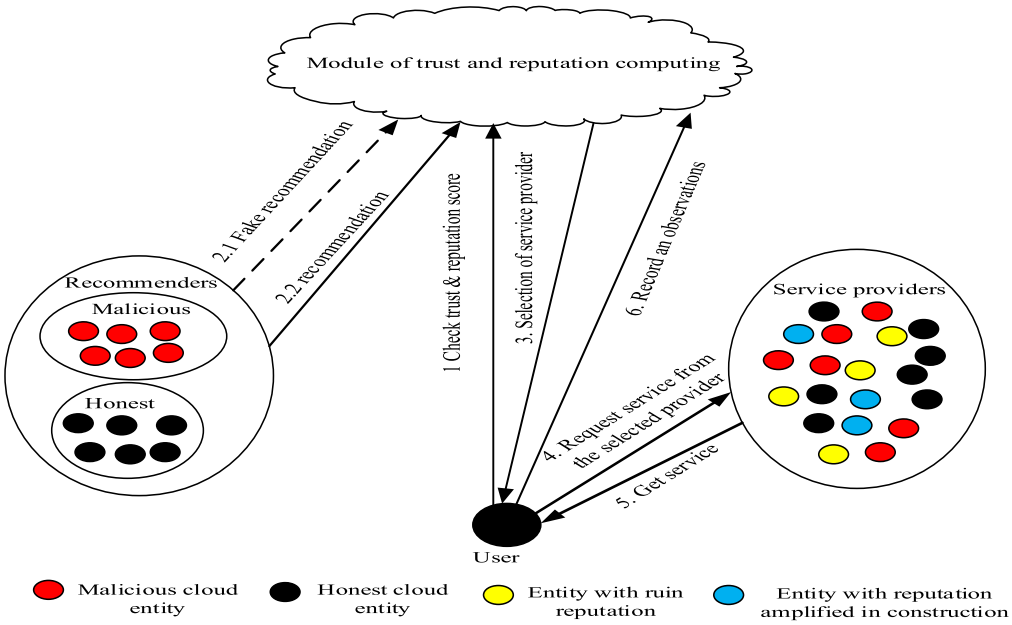


FIGURE 16. Trust and reputation in the cloud computing.

TABLE 19. Comparison of several PRKS schemes.

Scheme	Security	Query	Mul-user
[113]	Keyword privacy	Single	No
[114]	Message privacy	Single	No
[115]	C-PRKS-IND-ANON-CCA	Single	No
[116]	C-PRKS-IND-ANON-CCA	Single	No
[117]	Keyword/ciphertext security	Joint	No
[118]	Selective CKA	Single	Yes

C. DISCUSS AND ANALYSIS OF SEARCH ENCRYPTION

Many scholars of network security have studied the security of searchable encryption, the search expressive ability and the search efficiency, further produced a series of important research results [85]. However, there are still some problems that need further study.

1) Study the expressive ability of ciphertext search statements. Flexible ciphertext search statements can't only enable users to locate accurately the encrypted data, but also enable users to express search requirements flexibly.

2) Study the security of searchable encryption schemes. Based on different security levels, seek simple and efficient assumptions to prove the security of searchable encryption schemes.

3) Study the attribute-based encryption scheme with abundant expressive ability. The abundant expressive ability is the most important feature of attribute-based encryption, which directly reflects the searchable ability.

4) Study efficient decryption algorithm and ciphertext outsourcing computing schemes. Pairing computation will consume a lot of time, and reducing the number of pairings will improve the efficiency of encryption and decryption.

5) Study simple hypothesis. Under the same level of security, the simpler hypothesis will greatly promote the application of attribute-based encryption.

6) Study lightweight searchable encryption. On the premise of the expressive ability and the security searchable encryption, the lightweight method can reduce the burden of encryption.

V. TRUST AND REPUTATION OF CLOUD COMPUTING

Trust and reputation (TR) are important considerations for cloud service adoption and are closely related to privacy protection [119]. Cloud computing system requires users' trust and reputation-related information to be fully disclosed, which will bring hidden risk to users' privacy (Fig. 16). Recently, the combination of various methods provides an almost optimal solution for TR management in privacy protection of cloud computing services [120].

A. PRIVACY BASED ON TRUST

Trust and privacy are closely related in the cloud environment. It's a popular technology for privacy protection research. Recently, there have been many achievements of trust-based privacy protection in academia [119], [120].

Reference [121] designed a two-layered certification scheme based on the private non-profit organization cloud association. This showed how the organization can motivate suppliers to provide high data security and provide privacy protection for users. Reference [122] proposed a privacy-based cross-cloud trust evaluation protocol. First, feedback is protected by homomorphic encryption and

TABLE 20. Comparison of several trust schemes.

Literature	Scheme	Technical approach	Application
[122]	A privacy-based cross-cloud distributed trust evaluation protocol	Homomorphic encryption, trust assessment	Privacy protection
[123]	A privacy-preserving mobile application recommendation system	Security protocol, homophobic encryption	Choose candidate
[124]	A privacy-preserving online medical service recommendation	Reputation score, calculate similarity	Medical privacy
[125]	Strong privacy preservation and accurate task allocation	Proxy re-encryption, signature technology	Task allocation
[129]	A privacy-preserving trust model for block chain	Certificate revocation, reputation evaluation algorithm	Privacy protection
[130]	Cloud security method based on trust spanning tree protocol	Trust spanning tree, specification state model	Validity trust

verifiable secret sharing. Secondly, trust assessment can be done in a distributed way, even when some parties are offline. Thirdly, in order to facilitate customized trust assessment, innovative mechanisms are adopted to store feedback, which can be handled flexibly while protecting feedback privacy. There are many candidates in the cloud service, so how to let users select suitable objects is an important issue. Reference [123] proposed two privacy schemes for mobile applications based on the trust behavior of users. User's private data can be saved by applying this security protocol and homophobic encryption. In order to ensure the accuracy of recommendation, [124] take the similarity between doctor reputation score and user's requirement and doctor's information as the basis of medical service recommendation, and proposed two specific algorithms to calculate similarity and reputation score. Finally, security analysis illustrated the superiority of this scheme. Mobile cloud involves a large number of task allocations in the scheduling process. How to solve the contradiction between cloud user privacy and task allocation is a challenge for mobile cloud. Reference [125] proposed a privacy-preserving awareness scheme which supported accurate task allocation based on geographic information and mobile user credit points. Sensing tasks were protected by proxy re-encryption and signature technology, and anonymity is reported to prevent privacy leakage. Reference [126] proposed a cloud service evaluation method to calculate trust values based on compliance and reputation. Reputation is calculated based on collective feedback from user. Feedback ratings are the views of each user about the service being invoked. This method can greatly improve the service selection process in cloud applications, but the calculation process is more complex and the burden of client is very huge.

Reference [127] proposed two new methods to identify false feedback. Feedback evaluation component was used to check the received feedback and identify its possible false identity, Bayesian game model was used to correct its wrong behavior. The results show that the feedback evaluation component can correctly identify and correct false feedback. Malicious dissemination of patient's medical records will bring various risks to patient's privacy. Reference [128] proposed a system MedShare which solved the problem of sharing medical data in a distrustful environment. Medshare monitored entities that access data from data storage systems for malicious use. By implementing MedShare, CSP and other data protection personnel will be able to achieve data sources and protect data privacy.

Reference [129] proposed an anonymous reputation system based on block chain, and established a trust model for privacy protection of van truck based on block chain. The transparency of certificate and revocation is effectively realized through the proof of existence and non-existence. However, the scheme is complex, which is not conducive to the mastery and use of medical personnel. In order to verify the validity of the trust protocol, [130] proposed a new trust evaluation method of STP (Spanning Tree Protocol) based on the specification state model. Experiments showed that the trust protocol can achieve security objectives, and has low computational overhead and good convergence performance. The comparison results are shown in Table 20.

B. PRIVACY BASED ON REPUTATION

Reputation is also an important consideration when adopting cloud services. The development trend of reputation management is demand-driven. Recently, different reputation management methods in cloud services have been proposed [131].

Reference [132] proposed a privacy-preserving reputation system to support anonymous ratings. In this system, the user can approve the corresponding comments, and the user who received the predefined quantity of content was considered experienced and gets the "senior member" level. With the emergence of Vehicle Edge Computing (VEC),

TABLE 21. Comparison of several reputation schemes.

Literature	Scheme	Technical approach	Application
[132]	A privacy-preserving reputation system	Reputation and reward	Privacy protection
[133]	Secure and efficient distributed reputation management	Multi-weight subjective logic	Security protection
[134]	Privacy-preserving decentralized reputation systems	Trust privacy protocol	Privacy protection
[136]	Reputation and attribute based dynamic access control framework	Reputation and access control	Detect behavior
[137]	Privacy-friendly weighted reputation aggregation protocols	Homomorphic encryption, knowledge proof	Privacy protection

service providers can directly host services in the vicinity of mobile vehicles. Reference [133] focused on reputation management, in the implementation of VEC process, to ensure security protection and improve network efficiency. The system has significant functions to improve the overall performance: 1) distributed reputation maintenance; 2) credible reputation performance; 3) accurate reputation update; 4) availability of reputation.

In order to realize the protection of dynamic and private decentralized reputation, [134] proposed a dynamic privacy protection reputation system, which supported many functions, provided the protocols to realize these functions, and described the construction process of the protocols. Reference [135] proposed a privacy-preserving reputation management system, which allowed the secure transfer of reputation. The prototype implementation of the reputation transfer protocol and the experimental deployment of the reputation management solution in the e-learning forum are all conceptual validation.

Reference [136] proposed a reputation and attributes dynamic access control framework (RADAC) for privacy protection in the cloud computing environment. First, RADAC is used to encourage honest users to take good action in the cloud environment. Secondly, RADAC is used to restrict malicious users 'destructive behaviors in the cloud environment. Finally, RADAC is developed to detect malicious behavior of dishonest users and automatically prevent their further behavior from threatening the security of cloud computing. Reference [137] proposed two weighted reputation aggregation privacy protocols: one is a semi-honest model, the other is a malicious model by using homomorphic encryption primitives, verifiable encryption and knowledge proof of discrete logarithms, and result showed that they are practical and superior than previous works.

Users are reluctant to submit negative feedback because they are afraid of receiving retaliation from users. Reference [138] proposed a privacy-preserving reputation protocol, which did not require centralized entities, trusted third parties or specialized platforms, such as anonymous networks and trusted hardware. Furthermore, this protocol required the exchange of messages which are the number of users in the protocol. Reference [139] proposed a reputation mechanism to encourage CPS to differentiate between honest and malicious users and to allocate resources in a non-shared way. Further, the effectiveness of the reputation management system is verified by experiment. The comparison results are shown in Table 21

C. COMBINE TRUST AND REPUTATION

With the requirement for privacy, trust and reputation gradually converge and become the key factors in cloud service applications. TR has recently received a lot of attention and obtained a lot of research results [140].

Trust involves many factors, [141] proposed a new multi-dimension trust and reputation computing model for cloud computing, which integrated many trust factors and improved the novelty of the model. In addition, this paper used weighted moving average and ordered weighted average (WMA-OWA) combination algorithm to dynamically assign a weight to both trust and reputation coefficient. Reference [142] proposed a decentralized privacy protection reputation system based on block chain, proved correctness and security, eliminated the requirement for users to trust any third party or even other users, described the reputation system in e-commerce applications.

Reference [143] proposed a reputation trust and privacy protection scheme for mobile cloud computing (MCC). In the first stage, they used reputation-aware to select and utilize cloud services. In the second stage, they proposed an anonymous secure shell ciphertext strategy based on attribute encryption to manage privacy protection. In addition, this scheme proposed an outsourced service mechanism for mobile devices that further utilize encryption and decryption service providers for complex operations. Reference [144] discussed the impact of malicious servers on different trust and reputation models in wireless sensor networks. First, five trust and reputation models, BTRM-WSN, Eigen trust, peer trust, power trust and linguistic vague trust are analyzed.

TABLE 22. Comparison of several schemes' combination trust and reputation.

Literature	Scheme	Technical approach	Application
[141]	A multi-dimensional trust and reputation calculation model	Ordered weighted average combination algorithm	Trust, reputation evaluation
[143]	Reputation-aware trust and privacy-preservation scheme	Reputation-aware, attribute encryption	Privacy protection
[145]	Reputation and trust in privacy-preserving mobile sensing	Trust assessment, reputation management protocols	Identity trust
[147]	Reputation based trust model for service providers	Customer feedback, server rejection rate and server workload	Service reputation
[148]	Reputation-based trust management framework	Trust feedback, trust counter	Protect consumer 's privacy

Second, they compared the overall framework of the above trust and reputation models. Finally, they deployed a trust model to the overall evaluation of WSN, however, the computational complexity is relatively high.

Anonymity and trust are two conflicting goals in mobile networks. Reference [145] proposed a framework to solve the problem of ''no identity trust'' in mobile networks, which included three parts: privacy-preserving source models, data trust assessment schemes, and anonymous reputation management protocols. Compared with other recent solutions, this solution did not require a trusted third party and can enforce positive and negative reputation updates. Reference [146] proposed an approach for managers of trust and reputation. Firstly, the user accessed the resource block through the scheduling manager, and the structure was sent to the user after accessing the resource block. Secondly, after calculating the safety factor and reputation value, it is allocated to the fuzzy logic system, and the security score of the resource center is obtained.

Reference [147] proposed a reputation-based trust model, which evaluated the reputation of service providers by considering customer feedback, server rejection rate and server workload trust evaluation algorithms. There are many factors involved in the trust evaluation, but the weight formula of each trust attribute is not given, so the accuracy of trust is low. Reference [148] designed a reputation-based trust management framework (Cloud Armor) which provided several trust functionalists as a service, including 1) a new protocol to prove the credibility of trust feedback and retain the user's public relations; 2) a measure of counter-trust; and 3) trust service of availability model used to manage decentralized implementations. The comparison results of several article are shown in Table 22.

D. DISCUSS AND ANALYZE OF TRUST

In the above sections, many trust and reputation methods have been introduced, such as, weight, Bayesian inference, and fuzzy logic. Reputation is the extension of trust, so we discuss and analyze the future of trust research, which include trust composition, propagation, update and formation and so on [148].

Trust composition: Most trust measures involve social indicators, because friendship deserves attention in recommendation because of social similarity and interest.

Trust propagation: The major challenge of cloud central trust communication is the design of infrastructure, which can disseminate trust information in cloud computing.

Trust update: Time is sensitive to trust-updates, the time differences between executing instances of a transaction will affect trust scores.

Trust formation: Multi-trust formation method needs to consider multiple trust measures or proprieties. Therefore, in the process of trust computing, besides several common attributes, more measures and attributes must be considered.

VI. COMBINITION TECHNOLOGIES IN PRIVACY PROTECTION

With the further development of research, both ABE, trust and access control technologies are combined to achieve a dynamic operation authority [122].

A. ACCESS CONTROL, TRUST AND ENCRYPTION

Trust alone is not enough to solve privacy and security problems in cloud computing. It is necessary to integrate multiple technologies to achieve better privacy protection security performance from multiple perspectives. User can rely on a trusted cloud to carry out encryption and decryption of complex key management, which not only can ensure the security of cloud data, but also fully utilize the computing power of the cloud platform to reduce the cost of client (Fig. 17).

Reference [149] proposed a trust access control model which added trust and environmental conditions to realize the integration of the trust and authority, achieved the effective implementation in the new network service entity, and can

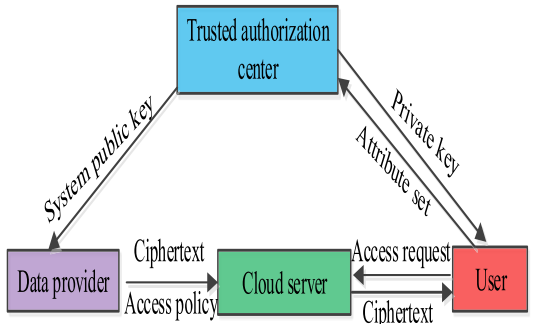


FIGURE 17. Trust authority based on ABE.

protect the personal privacy and service providers in Ad Hoc Networks. Reference [150] analyzed the challenges of multiple access control models in the cloud, and used the graph theory technology to analyze the interaction between service provider and data owner.

Reference [151] proposed a model of access control HDFS (Hadoop distributed file system) based on user trust value. It combined the third-party authentication system Kerberos, realized the authentication of users, and sated up a trust value for each user. Further, in order to improve verification efficiency, [153] designed a trust cloud computing platform to perform remote user authentication information by enclosing the ''virtual machine'' and trust coordinator. Reference [152] proposed an encrypted RBAC trust model to explain and improve the security of data in cloud storage system. This trust model considered role inheritance and hierarchical structure to evaluate role credibility. Combining with practical application scenarios, it explained how to use trust evaluation to reduce risk and improve decision quality of cloud storage services. But the structure is too complex to cope with the complex and changeable cloud environment.

B. MULTI-TENANT

Virtualization technology is the foundation of cloud computing, which directly led to the birth of multi-tenant of cloud computing [156]. Multi-tenant often runs on the same physical host, which is likely to affect other users, such as channel attack. The virtual machine can be dynamically migrated according to the performance and requirements, the access permission is changed, so how to guarantee privacy protection is very important.

Reference [154] absorbed the concept of isolation and used the virtual machine monitor to provide a private space for the virtual machine of the specified program, only decryption and plaintext can run. Memory is not accessible by the operating system or other programs; isolation guarantees a high degree of data privacy in a virtualized environment. Based on the trust concept, [155] developed the trust authentication system model, which can be flexible to assign the virtual environment to the corresponding tenants, and analyze the form of trust in multi-tenant, which can effectively separate applications and data. Reference [156] proposed a multi-tenant and flexible access control policy which guaranteed the strong isolation of data of enterprises in cloud store. It can make an enterprise unauthorized user that have no access to others, and ensure the appropriate isolation of cloud data.

Reference [157] proposed a new multi-tenant access control model that was based on the principle of safety obligation separation. In this model, CSP can operate the security issues of the tenants in the cloud such as addition, deletion, and management. Reference [158] proposed a service-oriented multi-tenant access control model that can meet the requirements of the users and automatic generate related roles in the cloud environment.

Reference [159] proposed semantic access control model, which carried out privacy protection, prevention of unauthorized attacks by digital signature usage, revocation list for credential to prevent the usage of expired credentials. Reference [160] further proposed an efficient access control model-based attribute role, and provided the ability to issue certificate authority in the cloud computing. Reference [161] proposed a fine-grained access control model in cloud health systems. Permissions are activated or deactivated based on the current task, which are indirectly related to users and are allocated according to actual needs. These relevant comparison results of several articles are shown in Table 23.

C. EXTENSION ACCESS CONTROL OF PRIVACY PROTECTION

Traditional access control model can't meet the requirement of privacy protection in the new network environment, however, due to the security and privacy policy of access control for the same resources set, there is conflict with each other, it can need new access control to facilitate privacy protection of cloud.

Reference [162] introduced a comprehensive privacy-aware access control framework. The key component of the framework is a family P-RBAC that extended the RBAC in order to provide full support for expressing highly complex privacy related policies, such as purposes and obligations. References [163], [164] proposed several features of the obligation: 1) association with action request, 2) temporal constraints and 3) conditional attribute. Reference [165] has developed a framework for expressing and enforcing policies by giving a formal definition of purpose, proposed a modal expression logic language for purpose constraints. However, it lacked corresponding verification examples and comparative analysis results. Reference [166] proposed a multi-purpose access control model, which was based on subject attributes, context attributes and authority policies; access purposes were verified through a dynamic behavior, intended purposes were dynamically associated with the requested data object during the decision. From the perspective of policy application, [167] extended architecture of XACML, realized privacy protection based on effective credentials and management, demonstrated efforts.

Reference [168] proposed a mandatory content access control (MCAC), enabled content provider (CP) to control

TABLE 23. Comparison of several trust encryption multi- tenant access control scheme.

Literature	Classification	Scheme	Technical Approach	Application	Scalability
[149]	Trust and Access Control	A Trust Centrality Degree-Based Access Control	Trust Degree and Access Authority	Personal Privacy and Providers	Average
[150]		Trust-Based Access Control for Secure Cloud Computing	Multiple Access Control, Graph Theory	Cloud Auditing and Applications	Average
[151]	Trust and Encryption	Access Control Model Research for HDFS	Trust, Third-Party Authentication	HDFS	Average
[152]		Trust Enhanced Cryptographic Role-Based Access Control	Encryption, Inheritance Trust, Role Structure	Cloud Data Storage	Low
[153]		Public Auditing for Secure Cloud Storage	Remote User Authentication	Secure Cloud Storage	Average
[154]	Multi-Tenant	Dependability for Disaster Tolerant Cloud Systems	Virtual Machine Isolation	Cloud Disaster Tolerant	Low
[155]		Multidimensional Trust-Aware Access Control	Assign the Virtual Machine to The Tenant	Internet of Things	High
[156]		Policy-Driven Data Management Middleware for Multi-Cloud Storage	A Multi-Tenant and Flexible Access Control Policy	SaaS	Average
[157]		Multi-Tenant Attribute-Based Access Control	Safety Obligation Separation	Cloud Infrastructure	Average

network nodes which can cache their content. In MCAC, CP defined different security labels for different content. Content router checked these labels to determine whether content objects should be cached. Many digital rights management (DRM) schemes use attribute-based encryption, but it is difficult to support dynamic updates of usage rights stored in the cloud. Reference [169] proposed a new DRM scheme based on secure key management and dynamic use control. When attributes satisfy the access policy of encrypted content, users can decrypt content and allow content providers to selectively provide fine-grained access control for content in a group of users.

RBAC is a general mechanism to describe the principle of access control, [170] proposed a data center access control solution, which has abundant role-based expressive capabilities. This solution utilized the logical formalism provided to implement advanced rule management, such as semantic conflict detection. According to combination RBAC with ciphertext policy attributes, [171] proposed a RBAC-CP-ABE scheme of data protection mechanism. Security analysis showed that this scheme maintained the security and efficiency characteristics of the CP-ABE scheme, but greatly improved the access control capability. Reference [172] proposed a model to generate executable access control tests using predicate/transformation networks, which transformed the implementation into executable code by mapping relationship, and evaluated the effectiveness of rules of RBAC.

Reference [173] developed a new access control protocol to provide privacy for honest users and prevent network owners and users from assuming responsibility for misconduct without the participation of any trusted third party. Reference [174] proposed a role-based access control using smart contract (RBAC-SC), which used intelligent contract and block chain technology to express the trust relationship, and implemented a challenge-response protocol to verify user's role ownership. Reference [175] proposed a set of protocols to solve sensitive location information problem. Specifically, users provided role and location tokens to service providers. Service providers negotiated role and location permissions to validate tokens and evaluate policies. Reference [176] proposed a role-based encryption (RBE) scheme, which allowed the implementation of RBAC policy for data stored in public clouds, and maintained sensitive information related to organizational structure in private clouds.

Reference [177] proposed a hierarchical virtual role assignment scheme based on negotiation, which can't only manage a resource server or agent, but also negotiate and support through multiple collaborative resource servers or agents. Reference [178] proposed a distributed role-based multi-tenant access control architecture, both access

specification and description are provided to meet the requirements of cloud users. Fog computing is an example of extending cloud computing, Reference [179] proposed an access control (CP-ABE) scheme for attribute updating and outsourcing capabilities, burden of encryption and decryption were transferred to fog nodes, so the computation of data owner and user is independent of the access structure. Reference [180] proposed a secure fine-grained data access control scheme based on ciphertext updating and computing outsourcing for fog computing. Based on attribute-based signature technology, the attributes of users can satisfy the update strategy. In the ABAC, users with high-level attribute values get low privileges. Reference [181] used bilinear method to construct a practical ABE group based on forward and backward functions, which can significantly reduce private keys and ciphertexts and provide flexible strategies for data services.

Flexible access control become the most urgent needs of data center, [182] proposed a more effective access control scheme with audit mechanism, introduced central organization to generate keys for validating users. Reference [183] designed a secure and lightweight data access control scheme based on CP-ABE, which can protect the confidentiality of outsourced data for mobile cloud computing. These comparisons of several articles are shown in Table 24.

D. HIERARCHICAL KEY

Hierarchical key is an important method of privacy protection. Reference [184] designed a reliable hierarchical key distribution scheme that supported dynamic key distribution without redistribution of private information. Based on pseudo-random function, [185] implemented the worst and average bit operands of key derivation, and its exponential level was better than the depth of balance hierarchy. Reference [186] proposed a new security key management scheme to provide better security requirements. The scheme has the following characteristics: (1) It is simple to perform key generation and key derivation stages. (2) It can resist some potential attacks. Reference [187] proposed a new security model that provided a simple, effective and secure structure for key distribution at any level using pseudo-random function and forward-secure pseudo-random generator. Reference [188] proposed a hierarchical key distribution scheme based on linear geometry. In this scheme, the keys of hierarchical structure are associated with a private vector, both the inner product of the private sector and the common vector can be used to obtain the subclass encryption key. Table 25 shows the comparison results; private information is metric by class in access graph $G = (V, E)$, and public parameters are measured for the whole system.

E. DISCUSS AND ANALYZE

In the above sections, we can know that the combination of trust, encryption, hierarchical key and access control can prevent the privacy disclosure in the cloud [149]. So, we believe that the following aspects should be further studied:

1) Both trust and access control can be combination. Before a user gains a role, the trust value can determine whether the user can gain the corresponding privileges to ensure the security of the host and the server [150], [151], [186].

2) Both trust, hierarchical key and ABE can be combination. When access control model carries out ABE mechanism, system can determine the trust relationship among providers, cloud platforms and users through the trust value [152], [153].

VII. CHALLENGES, ISSUES AND FUTURE DIRECTIONS

The above sections have discussed and analyzed various technologies, such as access control, ABE, search encryption, trust, reputation and so on. It is necessary to synthesize this article and make a general summary of the current challenges, issues and future directions.

A. CHALLENGES OF SEVERAL TECHNOLOGIES

In this sub-section, we analyze related challenges of several technologies in the cloud computing.

1) CHALLENGES OF TRUST

Although trust has made a lot of progress, there are some following challenges of trust-based schemes.

- Trust evaluation criteria are inconsistent in the different study. Due to the lack of standardized evaluation criteria, it is very difficult to compare different trust evaluation results.
- The trust of entities is mainly evaluated qualitatively. In order to accurately evaluate and compare the reliability of entities, quantitative trust computing algorithm is needed.
- A unified framework needs to be designed to integrate the comprehensive trust assessment of different entities involved in the cloud environment.

2) CHALLENGES OF ACCESS CONTROL

Currently, there are some challenges of access control in the cloud computing.

Fine-grained

- access control schemes can bring high complexity, which limits their scalability and flexibility. How to achieve the goal of fine granularity and elasticity of access control in cloud computing at the same time is still a huge challenge.
- Access control policy is formulated by the data owner. There is still a great risk that cloud servers can access data arbitrarily or not strictly control third-party access by the policy.
- There are many problems to be solved urgently in the process of cross-domain access control, such as attribute management, key management, policy management, access conflict, unauthorized access and so on.

3) CHALLENGES OF ENCRYPTION

Although ABE is the most efficient among encryption schemes, it still faces the following challenges.

TABLE 24. Comparison of several access control model-based encryption.

Literature	Classification	Scheme	Technical approach	Application	Scalability
[168]	MAC	Mandatory content access control	Security label	Privacy security	Average
[169]	UCON	Attribute based DRM scheme with dynamic usage control	Secure key management and usage control	Cloud service privacy	Middle
[170]	RBAC	SecRBAC: secure data in the clouds	Novel identity-based and proxy re-encryption	Cloud service privacy	Middle
[171]		Flexible and self-contained data protection	ABE with ciphertext policy attributes	Cloud service privacy	Middle
[172]		Automated model-based testing of RBAC	Access control rules with functional test models	Network service privacy	Middle
[173]		Accountable privacy scheme	Trust and access control	Wireless networks	Middle
[174]		RBAC-SC: role-based access control	Intelligent contract and block chain technology	Block chain privacy	Middle
[175]		Privacy of spatially aware	RBAC and tokens	Mobile network	Middle
[176]		Cloud storage architecture based on role encryption	Role-based encryption scheme	Cloud service privacy	Middle
[177]		Hierarchical role assignment for negotiation-based RBAC scheme	Hierarchical encryption and role hierarchy	Large information service privacy	High
[178]		Distributed access control architecture for cloud computing	Role-based distributed encryption scheme	Cloud service privacy	High
[179]	ABAC	An efficient access control scheme	Attribute encryption based on ciphertext	Mobile cloud privacy	High
[180]		Secure data access control with ciphertext update and computation outsourcing	Combination attributes with signature satisfy the update policy	Fog computing privacy	Middle
[181]		Constructing flexible data access control for storage	Hierarchic attribute encryption	Cloud service privacy	Middle
[182]		Multi-attribute authorized access control framework	Attribute encryption and proxy re-encryption	Cloud service privacy	Middle
[183]		Lightweight attribute access control scheme	Attribute encryption based on ciphertext	Cloud service privacy	High

- The construction of revocable, traceable, expressible and efficient attribute encryption scheme based on elliptic curve is a very important challenge.
- Because pairing-based attribute-based encryption schemes are more troublesome for cloud computing, it is important to construct efficient ABE schemes with side channel flexibility based on prime-order bilinear groups.
- Designing a lightweight encryption scheme based on multi-authorization attributes to resist privacy leaks is also a huge challenge.
- How to search ciphertext efficiently and quantitatively control privacy leaks is also a huge challenge.

B. RESEARCH ISSUES

In order to prevent illegal access to cloud systems, provide secure, reliable and trust services, we believe that the following key issues will continue to be addressed:

1. How to efficiently store and compute privacy-preserving cloud data?

2. Which access control mechanisms are more effective for secure cloud transmission?

3. Which encryption scheme can be used to protect data security and privacy?

4. How to share data with multiple cloud service providers efficiently and safely?

TABLE 25. Comparison with several hierarchical key schemes.

Scheme	Private content	Public content	Key derivation	Dynamic	Security assumption
[184]	L	$L\mid E\mid+\rho\mid V\mid$	$(C_{SE-DEC}+C_{PRF})h$	Yes	CPABE-Secure-PRF
[185]	L	$(3\mid V\mid+\Sigma_{i=2}^{\mid V\mid}k_i+4)L$	$2_{CH}+C_F+C_{ECC-DEC}$	Yes	CPABE-Secure
[186]	L	$(\mid E\mid+2\mid V\mid)\rho$	$(h+2)C_{SE-DEC}$	Yes	CPABE-Secure
[187]	L	$2L$	$(h+1)C_{PRF}$	No	PRF(prediction random function)
[188]	$4L$	$(\mid V\mid^2+1)L$	$4M+2A$	Yes	PRF(prediction random function)

5. Who can provide data with CSP in critical emergencies?

6. What kind of rights can administrators provide to resist internal attacks?

7. How to deal with user revocation when authorized users leave the system?

8. How to deal with the relational complexity of cloud service providers?

9. How to provide the location and identity privacy for cloud computing?

10. How to deal with the security and privacy issues when a node leaves or joins the cloud?

11. After the cloud service provider detects the user's wrong behavior, how to keep the user's anonymity and track the user with its real identity?

12. How to build a secure keyword search scheme in distributed storage service model and extend it to the intelligent cloud environment?

13. How to effectively construct a secure index suitable for cloud computing and design a distributed searchable encryption algorithm is an urgent issue?

14. How to efficiently integrate encryption schemes with parallel distributed architecture, resource billing and dynamic requirements in cloud computing is an urgent issue?

C. FUTURE DIRECTIONS

The research and progress of cloud computing privacy and security in industry and academia is still in initial stage, future research work can focus on the following several aspects.

- Lightweight method for big data processing: In order to protect the security and privacy of large amounts of data, an efficient and lightweight encryption algorithm can greatly reduce the computing cost of resource-constrained devices [190].
- Encryption-based access and privacy control: In order to ensure the security and privacy required by cloud regulations, it is an effective solution to protect privacy by combining encryption, authentication, access control, key management and other means.
- Finer-grained access and privacy control: The different sensitivity of different cloud domains is very important for privacy control. A feasible method is to divide a record into several parts according to its sensitivity and encrypt each part with different keys.
- Security risk management and mitigation: It is very important to design a secure migration method for intelligent clouds. In many applications, it is necessary to migrate applications from information to virtual servers, regardless of the security level of data.
- Adoption with privacy laws: Clouds need to collect information and transmit it to local or remote data centers for batch or online data analysis. However, in the process of data collection, the important privacy information is faced with privacy protection and management as well as legal issues. Therefore, the corresponding law also need to be upgraded [187].
- Heterogeneous network architecture for cloud privacy: It is an important direction in the future to design a reasonable topology so that all heterogeneous network elements can coordinate communication and maximize the efficiency of each participant [190].
- Compatibility of cloud computing mechanisms: Many well-known companies have released their own cloud computing products. Compatibility with related cloud computing products is a major direction in the future, from improving computing efficiency, reducing waste and saving energy.
- Integration of cloud computing and new concepts: New concepts of Internet emerge endlessly. In order to maintain vitality and competitiveness, it is necessary to integrate cloud computing, Internet of Things, fog computing, edge computing, block chain and other concepts. Developing safer, intelligent, fast, efficient and personalized Internet products are the future research trend [194], [195].

SUMMARY

How to protect the security and privacy is a big problem in the cloud computing [189]. We have summarized a variety of solutions in cloud computing privacy protection in this paper. We mainly discuss the research results of various ABE models, summarize their advantages and disadvantages, and analyze the integration trend of access control, encryption, trust and other technologies to achieve better privacy protection, finally, give the general summary of the current challenges, issues and future directions.

In addition to the above several technology aspects, we need to take more comprehensive consideration to form a complete security protection system, such as standardization, legal regulations and so on. At present, there are relevant legal professions in foreign countries, such as the HIPAA [192] (Health Insurance Portability and Accountability Act) and FAPA [193] (Financial Agency Privacy Act), which required relevant units to protect the privacy of clients. Existing enterprise had to take the manner to protect customer privacy and convey their privacy policies, such as P3P privacy statement [196] or privacy seal programs [197], in order to effectively ensure the long-term evolution of data security and privacy protection in cloud computing, and achieve the healthy and orderly development of cloud computing services [198].

REFERENCES

[1] Cloud Security Alliance. (2017). *Security Guidance for Critical Areas of Focus in Cloud Computing V4.0*. [Online]. Available: http://www.cloudsecurityalliance.org/

[2] Y. Zhang, "Research on the security mechanism of cloud computing service model," *Autom. Control Comput. Sci.*, vol. 50, no. 2, pp. 98–106, Mar. 2016.

[3] L. S. Nishad, J. Paliwal, R. Pandey, S. Beniwal, and S. Kumar, "Security, privacy issues and challenges in cloud computing: A survey," in *Proc. 2nd Int. Conf. Inf. Commun. Technol. Competitive Strategies*, 2016, p. 47.

[4] R. K. Kalluri and C. V. G. Rao, "Addressing the security, privacy and trust challenges of cloud computing," *Int. J. Comput. Sci. Inf. Technol.*, vol. 5, no. 5, pp. 6094–6097, 2014.

[5] P. G. Shynu and K. J. Singh, "A comprehensive survey and analysis on access control schemes in cloud environment," *Inf. Technol.*, vol. 16, no. 1, pp. 19–38, 2016.

[6] M. S. Inamdar and A. Tekeoglu, "Security analysis of open source network access control in virtual networks," in *Proc. 32nd Int. Conf. Adv. Inf. Netw. Appl. Workshops*, May 2018, pp. 475–480.

[7] D. Stevenson and J. Pasek, "Privacy concern, trust, and desire for content personalization," in *Proc. Res. Conf. Commun., Inf. Internet Policy*, 2015, pp. 1–30.

[8] R. K. Aluvalu and L. Muddana, "A survey on access control models in cloud computing," in *Proc. 49th Annu. Conv. Comput. Soc. India (CSI)*, vol. 1, 2015, pp. 653–664.

[9] F. Cai, N. Zhu, J. He, P. Mu, W. Li, and Y. Yu, "Survey of access control models and technologies for cloud computing," *Cluster Comput.*, to be published.

[10] D. F. Ferraiolo, R. Sandhu, S. Gavrila, D. R. Kuhn, and R. Chandramouli, "Proposed NIST standard for role-based access control," *ACM Trans. Inf. Syst. Secur.*, vol. 4, pp. 224–274, Aug. 2001.

[11] M. Nabeel, N. Shang, and E. Bertino, "Privacy preserving policy-based content sharing in public clouds," *IEEE Trans. Knowl. Data Eng.*, vol. 25, no. 11, pp. 2602–2614, Nov. 2013.

[12] W. Jiang and Z. Wang, "Towards efficient update of access control policy for cryptographic cloud storage," in *Proc. Int. Conf. Secur. Privacy Commun. Netw.*, in Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 153, 2015, pp. 341–356.

[13] J. Li, Y. Zhang, X. Chen, and Y. Xiang, "Secure attribute-based data sharing for resource-limited users in cloud computing," *Comput. Secur.*, vol. 72, pp. 1–2, Jan. 2018.

[14] H. Takabi, "Privacy aware access control for data sharing in cloud computing environments," in *Proc. 2nd Int. Workshop Secur. Cloud Comput.*, 2014, pp. 27–34.

[15] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in *Proc. Int. Workshop Public Key Cryptogr.*, in Lecture Notes in Computer Science, vol. 6571, 2011, pp. 53–70.

[16] R. Zhang, H. Ma, and Y. Lu, "Fine-grained access control system based on fully outsourced attribute-based encryption," *J. Syst. Softw.*, vol. 125, pp. 344–353, Mar. 2017.

[17] A. Beimel, "Secure schemes for secret sharing and key distribution," Ph.D. dissertation, Technion-Israel Inst. Technol., Haifa, Israel, 1996.

[18] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.*, in Lecture Notes in Computer Science, vol. 3494, 2005, pp. 457–473.

[19] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proc. 13th ACM Conf. Comput. Commun. Secur.*, 2006, pp. 89–98.

[20] A. Beimel and A. Ben-Efraim, "Multi-linear secret-sharing schemes," in *Proc. Theory Cryptogr. Conf.*, in Lecture Notes in Computer Science, vol. 8349, 2014, pp. 394–418.

[21] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in *Advances in Cryptology* (Lecture Notes in Computer Science), vol. 2139, J. Kilian, ed. Berlin, Germany: Springer-Verlag, 2001, pp. 213–229.

[22] T. Iwasaki, N. Yanai, M. Inamura, and K. Iwamura, "Tightly-secure identity-based structured aggregate signature scheme under the computational diffie-hellman assumption," in *Proc. IEEE 30th Int. Conf. Adv. Inf. Netw. Appl.*, Mar. 2016, pp. 669–676.

[23] A. Lewko, A. Sahai, and B. Waters, "Revocation systems with very small private keys," in *Proc. IEEE Symp. Secur. Privacy*, May 2010, pp. 273–285.

[24] M. Bellare, D. Hofheinz, and E. Kiltz, "Subtleties in the definition of IND-CCA: When and how should challenge decryption be disallowed?" *J. Cryptol.*, vol. 28, no. 1, pp. 29–48, 2015.

[25] X. Li, B. Yang, and M. Zhang, "New construction of fuzzy identity-based encryption," in *Proc. WASE Int. Conf. Inf. Eng.*, 2009, pp. 647–651.

[26] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[27] S. D. C. di Vimercati, S. Foresti, R. Moretti, S. Paraboschi, G. Pelosi, and P. Samarati, "A dynamic tree-based data structure for access privacy in the cloud," in *Proc. IEEE 8th Int. Conf. Cloud Comput. Technol. Sci.*, Dec. 2016, pp. 391–398.

[28] S. Hohenberger and B. Waters, "Attribute-based encryption with fast decryption," in *Proc. Int. Workshop Public Key Cryptogr.*, in Lecture Notes in Computer Science, vol. 7778, 2013, pp. 162–179.

[29] C. Chen and J. Chen, "Fully secure attribute-based systems with short ciphertexts/signatures and threshold access structures," in *Proc. Cryptographers' Track RSA Conf.*, in Lecture Notes in Computer Science, vol. 7779, 2013, pp. 50–67.

[30] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proc. IEEE Symp. Secur. Privacy*, Washington, DC, USA, May 2007, pp. 321–334.

[31] C. Wang, J. Fang, and Y. Li, "An improved cloud-based revocable identity-based proxy re-encryption scheme," in *Applications and Techniques in Information Security*. 2015, pp. 14–26.

[32] Y. Chen and Z. L. Jiang, "Fully secure ciphertext policy attribute based encryption with security mediator," in *Proc. Int. Conf. Inf. Commun. Secur.*, in Lecture Notes in Computer Science, vol. 8958, 2015, pp. 274–289.

[33] L. Xue, Y. Yu, Y. Li, M. H. Au, X. Du, and B. Yang, "Efficient attribute-based encryption with attribute revocation for assured data deletion," *Inf. Sci.*, vol. 479, pp. 640–650, Apr. 2019.

[34] S. Yamada, N. Attrapadung, G. Hanaoka, and N. Kunihiro, "A framework and compact constructions for non-monotonic attribute-based encryption," in *Proc. Int. Workshop Public Key Cryptogr.*, 2014, pp. 275–292.

[35] M. Raseena1 and G. R. Harikrishnan, "Secure sharing of personal health records in cloud computing using attribute-based broadcast encryption," *Int. J. Eng. Trends Appl.*, vol. 1, no. 2, pp. 1–7, Sep./Oct. 2014.

[36] A. Balu and K. Kuppusamy, "Ciphertext-policy attribute-based encryption with user revocation support," in *Proc. Int. Conf. Heterogeneous Netw. Qual., Rel., Secur. Robustness*, 2013, pp. 696–705.

[37] Y. R. Chen, C. K. Chu, W. G. Tzeng, and J. Zhou, "CloudHKA: A cryptographic approach for hierarchical access control in cloud computing," in *Proc. Int. Conf. Appl. Cryptogr. Netw. Secur.*, 2013, pp. 37–52.

[38] X. Liu, Y. Xia, Y. Xiang, M. M. Hassan, and A. Alelaiwi, "A secure and efficient data sharing framework with delegated capabilities in hybrid cloud," in *Proc. Int. Symp. Secur. Privacy Social Netw. Big Data*, Nov. 2015, pp. 7–14.

[39] J. Wei, W. Liu, and X. Hu, "Secure and efficient attribute-based access control for multiauthority cloud storage," *IEEE Syst. J.*, vol. 12, no. 2, pp. 1731–1742, Jun. 2018.

[40] D. Vaduganathan, "Secure data sharing using attribute based encryption with revocation in cloud computing," *South Asian J. Eng. Technol.*, vol. 2, no. 15, pp. 145–150, 2016.

[41] U. K. Jyothi, N. Reddy, and B. R. Prasad, "Review of 'achieving secure, scalable, and fine-grained data access control in cloud computing,'" *Int. J. Eng. Comput. Sci.*, vol. 2, no. 8, pp. 2440–2447, Aug. 2013.

[42] Y. Rouselakis and B. Waters, "Efficient statically-secure large-universe multi-authority attribute-based encryption," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.*, 2015, pp. 315–332.

[43] Q. Li, J. Ma, R. Li, X. Liu, J. Xiong, and D. Chen, "Secure, efficient and revocable multi-authority access control system in cloud storage," *Comput. Secur.*, vol. 59, pp. 45–59, Jun. 2016.

[44] K. Yang and X. Jia, "Attributed-based access control for multi-authority systems in cloud storage," in *Proc. 32th IEEE Int. Conf. Distrib. Comput. Syst.*, Jun. 2012, pp. 1–10.

[45] K. Yang and X. Jia, "Expressive, efficient, and revocable data access control for multi-authority cloud storage," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 7, pp. 1735–1744, Jul. 2014.

[46] X. Liu, Y. Xia, S. Jiang, F. Xia, and Y. Wang, "Hierarchical attribute-based access control with authentication for outsourced data in cloud computing," in *Proc. 12th IEEE Int. Conf. Trust Secur. Privacy Comput. Commun.*, Jul. 2013, pp. 477–484.

[47] J. Hao, C. Huang, J. Ni, H. Rong, M. Xian, and X. S. Shen, "Fine-grained data access control with attribute-hiding policy for cloud-based IoT," *Comput. Netw.*, vol. 153, pp. 1–10, Apr. 2019.

[48] D. Chen, J. Shao, and X. Fan, "MAH-ABE based privacy access control in cloud computing," *Acta Electron. Sinica*, vol. 42, no. 4, pp. 821–827, 2014.

[49] Y. Zhu, D. Ma, C.-J. Hu, and D. Huang, "How to use attribute-based encryption to implement role-based access control in the cloud," in *Proc. Cloud Comput.*, May 2013, pp. 33–40.

[50] W. Ahmad and S. Wang, "Reputation-aware trust and privacy-preservation for mobile cloud computing," *IEEE Access*, vol. 6, 2018.

[51] J. Li, W. Yao, Y. Zhang, H. Qian, and J. Han, "Flexible and fine-grained attribute-based data storage in cloud computing," *IEEE Trans. Services Comput.*, vol. 10, no. 5, pp. 785–796, Sep./Oct. 2017.

[52] M. Xiao, M. Wang, X. Liu, and J. Sun, "Efficient distributed access control for big data in clouds," in *Proc. 3rd Int. Workshop Secur. Privacy Big Data*, Apr. 2015, pp. 202–207.

[53] N. D. Hua and M. J. Feng, "Enhanced cloud storage access control scheme based on attribute," *J. Commun.*, vol. 34, no. Z1, Aug. 2013.

[54] Y. Chen, W. Sun, N. Zhang, Q. Zheng, W. Lou, and Y. T. Hou, "Towards efficient fine-grained access control and trustworthy data processing for remote monitoring services in IoT," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 7, pp. 1830–1842, Jul. 2019.

[55] Z. Wang, D. Huang, Y. Zhu, B. Li, and C.-J. Chung, "Efficient attribute-based comparable data access control," *IEEE Trans. Comput.*, vol. 64, no. 12, pp. 3430–3443, Dec. 2015.

[56] S. Hohenberger and B. Waters, "Online/offline attribute-based encryption," in *Proc. Int. Workshop Public Key Cryptogr. (PKC)*, 2014, pp. 293–310.

[57] J. Li, X. Chen, J. Li, C. Jia, and J. Ma, "Fine-grained access control system based on outsourced attribute-based encryption," in *Proc. Eur. Symp. Res. Comput. Secur.*, in Lecture Notes in Computer Science, vol. 8134, 2013, pp. 592–609.

[58] J. Li, X. Huang, J. Li, X. Chen, and Y. Xiang, "Securely outsourcing attribute-based encryption with checkability," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 8, pp. 2201–2210, Oct. 2014.

[59] J. Li, K. Ren, and K. Kim, "A2BE: Accountable attribute-based encryption for abuse free access control," IACR Cryptol. ePrint Arch. [Online]. Available: http://eprint.iacr.org/2009/118.pdf

[60] Z. Liu, Z. Cao, and D. S. Wong, "White-box traceable ciphertext-policy attribute-based encryption supporting any monotone access structures," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 1, pp. 76–88, Jan. 2013.

[61] J. Li, K. Ren, B. Zhu, and Z. Wan, "Privacy-aware attribute-based encryption with user accountability," in *Proc. Int. Conf. Inf. Secur. (ISC)*, 2009, pp. 347–362.

[62] Z. Liu, Z. Cao, and D. S. Wong, "Fully collusion-resistant traceable key-policy attribute-based encryption with sub-linear size ciphertexts," in *Proc. Inf. Secur. Cryptol.*, 2014, pp. 403–423.

[63] Z. Liu and Z. Cao, "Expressive black-box traceable ciphertext-policy attribute-based encryption," IACR Cryptol. ePrint Arch., Tech. Rep. 2012/669, 2012. [Online]. Available: http://eprint.iacr.org/

[64] Z. Liu, Z. Cao, and D. S. Wong, "Blackbox traceable CP-ABE: How to catch people leaking their keys by selling decryption devices on eBay," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2013, pp. 475–486.

[65] Z. Qin, H. Xiong, S. Wu, and J. Batamuliza, "A survey of proxy re-encryption for secure data sharing in cloud computing," *IEEE Trans. Services Comput.*, to be published.

[66] H.-J. Seo and H.-W. Kim, "Attribute-based proxy re-encryption with a constant number of pairing operations," *Int. J. Inf. Commun. Eng.*, vol. 10, no. 1, pp. 53–60, 2012.

[67] K. Li, "Matrix access structure policy used in attribute-based proxy re-encryption," 2012, *arXiv:1302.6428*. [Online]. Available: https://arxiv.org/abs/1302.6428

[68] K. Liang, L. Fang, W. Susilo, and D. S. Wong, "A ciphertext-policy attribute-based proxy re-encryption with chosen-ciphertext security," IACR Cryptol. ePrint Arch., Lyon, France, Tech. Rep. 2013/236, 2013.

[69] K. Liang, M. H. Au, W. Susilo, D. S. Wong, G. Yang, and Y. Yu, "An adaptively CCA-secure ciphertext-policy attribute-based proxy re-encryption for cloud data sharing," in *Information Security Practice and Experience* (Lecture Notes in Computer Science). Berlin, Germany: Springer, 2014, pp. 448–461.

[70] M. Backes, M. Gagné, and S. A. K. Thyagarajan, "Fully secure inner-product proxy re-encryption with constant size ciphertext," in *Proc. 3rd Int. Workshop Secur. Cloud Comput.*, Singapore, Apr. 2015, pp. 31–40.

[71] H. Li and L. Pang, "Efficient and adaptively secure attribute-based proxy reencryption scheme," *Int. J. Distrib. Sensor Netw.*, vol. 12, no. 5, 2016, Art. no. 5235714.

[72] R. M. Daniel and E. B. Rajsingh, "Analysis of hierarchical identity based encryption schemes and its applicability to computing environments," *J. Inf. Secur. Appl.*, vol. 36, pp. 20–31, Oct. 2017.

[73] X. Hu, J. Wang, H. Xu, and Y. Yang, "Constant size ciphertext and private key HIBE without random oracles," *J. Inf. Sci. Eng.*, vol. 30, no. 2, pp. 333–345, 2014.

[74] H. Wang and L. Wu, "Unbounded anonymous hierarchical identity-based encryption in the standard model," *J. Netw.*, vol. 9, no. 7, pp. 1846–1853, 2014.

[75] S. C. Ramanna and P. Sarkar, "Efficient (anonymous) compact HIBE from standard assumptions," in *Proc. Int. Conf. Provable Secur.*, in Lecture Notes in Computer Science, vol. 8782, 2014, pp. 243–258.

[76] K. Lee, J. H. Park, and D. H. Lee, "Anonymous HIBE with short ciphertexts: Full security in prime order groups," *Des., Codes, Cryptogr.*, vol. 74, no. 2, pp. 395–425, 2015.

[77] J. Wei, X. Huang, W. Liu, and X. Hu, "Cost-effective and scalable data sharing in cloud storage using hierarchical attribute-based encryption with forward security," *Int. J. Found. Comput. Sci.*, vol. 28, no. 7, pp. 843–868, 2017.

[78] G. Wang, Q. Liu, J. Wu, and M. Guo, "Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers," *Comput. Secur.*, vol. 30, no. 5, pp. 320–331, 2011.

[79] H. Deng, Q. Wu, B. Qin, J. Domingo-Ferrer, L. Zhang, J. Liu, and W. Shi, "Ciphertext-policy hierarchical attribute-based encryption with short ciphertexts," *Inf. Sci.*, vol. 275, pp. 370–384, Aug. 2014.

[80] N. Krishna and L. Bhavani, "Hasbe: A hierarchical attribute set based encryption for flexible, scalable and fine grained access control in cloud computing," *Int. J. Comput. Org. Trends*, vol. 3, no. 9, pp. 294–301, 2013.

[81] D. H. Rachel and S. Prathiba, "An enhanced Hasbe for cloud computing environment," *Int. J. Comput. Sci. Mobile Comput.*, vol. 2, no. 4, pp. 396–401, 2013.

[82] Z. Wan, J. Liu, and R. H. Deng, "HASBE: A hierarchical attribute-based solution for flexible and scalable access control in cloud computing," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 743–754, Apr. 2012.

[83] Q. Huang, Y. Yang, and M. Shen, "Secure and efficient data collaboration with hierarchical attribute-based encryption in cloud computing," *Future Gener. Comput. Syst.*, vol. 72, pp. 239–249, Jul. 2017.

[84] S. Gokuldev and S. Leelavathi, "HASBE: A hierarchical attribute-based solution for flexible and scalable access control by separate encryption/decryption in cloud computing," *Int. J. Eng. Sci. Innov. Technol.*, vol. 2, no. 3, pp. 1–7, 2013.

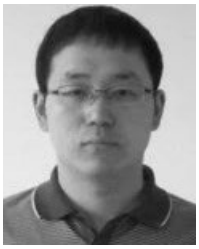
[85] J. Zhang, B. Chen, Y. Zhao, X. Cheng, and F. Hu, "Data security and privacy-preserving in edge computing paradigm: Survey and open issues," *IEEE Access*, vol. 6, pp. 18209–18237, 2018.

[86] S. Chenthara, K. Ahmed, H. Wang, and F. Whittaker, "Security and privacy-preserving challenges of e-Health solutions in cloud computing," *IEEE Access*, vol. 7, pp. 74361–74382, 2019.

[87] M. Adjedj, J. Bringer, H. Chabanne, and B. Kindarji, "Biometric identification over encrypted data made feasible," in *Proc. 5th Int. Conf. Inf. Syst. Secur.*, 2009, pp. 86–100.
[88] M. Kuzu, M. S. Islam, and M. Kantarcioglu, "Efficient similarity search over encrypted data," in *Proc. IEEE 28th Int. Conf. Data Eng.*, Apr. 2012, pp. 1156–1167.
[89] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy keyword search over encrypted data in cloud computing," in *Proc. IEEE INFOCOM*, Mar. 2010, pp. 441–445.
[90] E. Shen, E. Shi, and B. Waters, "Predicate privacy in encryption systems," in *Proc. 6th Theory Cryptogr. Conf. Theory Cryptogr.*, 2009, pp. 457–473.
[91] C. Bosch, Q. Tang, P. Hartel, and W. Jonker, "Selective document retrieval from encrypted database," in *Proc. Conf. Inf. Secur.*, 2012, pp. 224–241.
[92] R. Zhang, R. Xue, T. Yu, and L. Liu, "Dynamic and efficient private keyword search over inverted index–based encrypted data," *ACM Trans. Internet Technol.*, vol. 16, no. 3, pp. 21:1-21:20, Aug. 2016.
[93] M. Yoshino, N. Kunihiro, K. Naganuma, and H. Sato, "Symmetric inner-product predicate encryption based on three groups," in *Proc. 6th Int. Conf. Provable Secur.*, vol. 7496, 2012, pp. 215–234.
[94] W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y. T. Hou, and H. Li, "Privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking," in *Proc. 8th ACM SIGSAC Symp. Inf. Comput. Commun. Secur.*, 2013, pp. 71–82.
[95] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," in *Proc. IEEE INFOCOM*, Apr. 2011, pp. 829–837.
[96] C. Wang, N. Cao, K. Ren, and W. Lou, "Enabling secure and efficient ranked keyword search over outsourced cloud data," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 8, pp. 1467–1479, Aug. 2012.
[97] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 1, pp. 222–233, Nov. 2013.
[98] S. Kamara, C. Papamanthou, and T. Roeder, "Dynamic searchable symmetric encryption," in *Proc. ACM Conf. Comput. Commun. Secur.*, 2012, pp. 965–976.
[99] D. Cash, J. Jaeger, S. Jarecki, C. S. Jutla, H. Krawczyk, M.-C. Rosu, and M. Steiner, "Dynamic searchable encryption in very-large databases: Data structures and implementation," in *Proc. NDSS Symp.*, 2014, pp. 23–26.
[100] W. Sun, X. Liu, W. Lou, Y. T. Hou, and H. Li, "Catch you if you lie to me: Efficient verifiable conjunctive keyword search over large dynamic encrypted cloud data," in *Proc. IEEE INFOCOM*, Apr. 2015, pp. 2110–2118.
[101] B. Zhu, B. Zhu, and K. Ren, "PEKsrand: Providing predicate privacy in public-key encryption with keyword search," in *Proc. IEEE Int. Conf. Commun.*, Jun. 2011, pp. 1–6.
[102] M. Nishioka, "Perfect keyword privacy in PEKS systems," in *Proc. Int. Conf. Provable Secur.*, vol. 7496, 2012, pp. 175–192.
[103] A. Arriaga, Q. Tang, and P. Ryan, "Trapdoor privacy in asymmetric searchable encryption schemes," in *Proc. Cryptol. Conf. Africa-(AFRICACRYPT)*, vol. 8469, 2014, pp. 31–50.
[104] R. Zhang and R. Xue, "Efficient keyword search for public-key setting," in *Proc. IEEE Mil. Commun. Conf.*, Oct. 2015, pp. 1236–1241.
[105] P. Xu, H. Jin, Q. Wu, and W. Wang, "Public-key encryption with fuzzy keyword search: A provably secure scheme under keyword guessing attack," *IEEE Trans. Comput.*, vol. 62, no. 11, pp. 2266–2277, Nov. 2013.
[106] R. Zhang, R. Xue, T. Yu, and L. Liu, "PVSAE: A public verifiable searchable encryption service framework for outsourced encrypted data," in *Proc. IEEE Int. Conf. Web Services*, Jun. 2016, pp. 428–435.
[107] Q. Zheng, S. Xu, and G. Ateniese, "VABKS: Verifiable attribute-based keyword search over outsourced encrypted data," in *Proc. IEEE INFOCOM*, Apr. 2014, pp. 522–530.
[108] Q. Shuo, L. Jiqiang, and S. Yanfeng, "Hidden policy ciphertext-policy attribute-based encryption with keyword search against keyword guessing attack," *Sci. China Inf. Sci.*, vol. 60, no. 5, 2017, Art. no.052105.
[109] P. Liu, J. Wang, H. Ma, and H. Nie, "Efficient verifiable public key encryption with keyword search based on KP-ABE," in *Proc. 9th Int. Conf. Broadband Wireless Comput. Commun. Appl.*, Nov. 2014, pp. 584–589.
[110] W. Sun, S. Yu, W. Lou, Y. T. Hou, and H. Li, "Protecting your right: Verifiable attribute-based keyword search with fine-grained owner-enforced search authorization in the cloud," *IEEE Trans. Parallel Distrib. Syst.*, vol. 27, no. 4, pp. 1187–1198, Apr. 2016.
[111] Y. Yang, "Attribute-based data retrieval with semantic keyword search for e-health cloud," *J. Cloud Comput.*, vol. 4, no. 1, pp. 1–10, 2015.
[112] J. Li, X. Lin, Y. Zhang, and J. Han, "KSF-OABE: Outsourced attribute-based encryption with keyword search function for cloud storage," *IEEE Trans. Services Comput.*, vol. 10, no. 5, pp. 715–725, Sep./Oct. 2017.
[113] J. Shao, Z. Cao, X. Liang, and H. Lin, "Proxy re-encryption with keyword search," *Inf. Sci.*, vol. 180, no. 13, pp. 2576–2587, 2010.
[114] W.-C. Yau, R. C.-W. Phan, S.-H. Heng, and B.-M. Goi, "Proxy reencryption with keyword search: New definitions and algorithms," in *Proc. Secur. Technol. Disaster Recovery Bus. Continuity*, 2010, pp. 149–160.
[115] W. Zhong, X. A. Wang, Z. Wang, and Y. Ding, "Proxy re-encryption with keyword search from anonymous conditional proxy re-encryption," in *Proc. 7th Int. Conf. Comput. Intell. Secur.*, Dec. 2011, pp. 969–973.
[116] L. Fang, W. Susilo, C. Ge, and J. Wang, "Chosen-ciphertext secure anonymous conditional proxy re-encryption with key word search," *Theor. Comput. Sci.*, vol. 462, pp. 39–58, Nov. 2012.
[117] X. A. Wang, X. Huang, X. Yang, L. Liu, and L. Liu, "Further observation on proxy re-encryption with keyword search," *J. Syst. Softw.*, vol. 85, no. 3, pp. 643–654, 2012.
[118] Y. Shi, J. Liu, Z. Han, Q. Zheng, R. Zhang, and S. Qiu, "Attribute-based proxy re-encryption with keyword search," *PLoS ONE*, vol. 9, no. 12, 2014, Art. no. e116325.
[119] J. Granatyr, N. Osman, J. Dias, M. A. S. N. Nunes, J. Masthoff, F. Enembreck, O. R. Lessing, C. Sierra, A. M. Paiva, and E. E. Scalabrin, "The need for affective trust applied to trust and reputation models," *ACM Comput. Surv.*, vol. 50, no. 4, p. 48, Aug. 2017.
[120] F. A. M. Ibrahim and E. E. Hemayed, "Trusted cloud computing architectures for infrastructure as a service: Survey and systematic literature review," *Comput. Secur.*, vol. 8, no. 2, pp. 196–226, 2019.
[121] J. Prüfer, "Trusting privacy in the cloud," *Inf. Econ. Policy*, vol. 45, pp. 52–67, Dec. 2018.
[122] Y. Dou, H. C. B. Chan, and M. H. Au, "A distributed trust evaluation protocol with privacy protection for intercloud," *IEEE Trans. Parallel Distrib. Syst.*, vol. 30, no. 6, pp. 1208–1221, Nov. 2019.
[123] K. Xu, W. Zhang, and Z. Yan, "A privacy-preserving mobile application recommender system based on trust evaluation," *J. Comput. Sci.*, vol. 26, pp. 87–107, May 2018.
[124] C. Xu, J. Wang, L. Zhu, C. Zhang, and K. Sharif, "PPMR: A Privacy-preserving online Medical service Recommendation scheme in eHealth-care system," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 5665–5673, Jun. 2019.
[125] J. Ni, K. Zhang, Q. Xia, X. Lin, and X. S. Shen, "Enabling strong privacy preservation and accurate task allocation for mobile crowdsensing," *IEEE Trans. Mobile Comput.*, to be published.
[126] V. V. Rajendran and S. Swamynathan, "Hybrid model for dynamic evaluation of trust in cloud services," *Wireless Netw.*, vol. 22, no. 6, pp. 1807–1818, 2016.
[127] S. Siadat and A. M. Rahmani, "Identifying fake feedback in cloud trust management systems using feedback evaluation component and Bayesian game model," *J. Supercomput.*, vol. 73, pp. 2682–2704, 2017.
[128] Q. I. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "MeDShare: Trust-less medical data sharing among cloud service providers via blockchain," *IEEE Access*, vol. 5, pp. 14757–14767, 2017.
[129] Z. Lu, W. Liu, Q. Wang, G. Qu, and Z. Liu, "A privacy-preserving trust model based on blockchain for VANETs," *IEEE Access*, vol. 6, pp. 45655–45664, 2018.
[130] Y. Lai, Z. Liu, Q. Pan, and J. Liu, "Study on cloud security based on trust spanning tree protocol," *Int. J. Theor. Phys.*, vol. 54, pp. 3311–3330, Sep. 2015.
[131] A. I. A. Ahmed, S. H. A. Hamid, A. Gani, and M. K. Khan, "Trust and reputation for Internet of Things: Fundamentals, taxonomy, and open research challenges," *J. Netw. Comput. Appl.*, vol. 145, Jul. 2019, Art. no. 102409.
[132] N. Busoma, R. Petrlic, F. Sebé, C. Sorge, and M. Valls, "A privacy-preserving reputation system with user rewards," *J. Netw. Comput. Appl.*, vol. 80, pp. 58–66, Feb. 2017.
[133] X. Huang, R. Yu, J. Kang, and Y. Zhang, "Distributed reputation management for secure and efficient vehicular edge computing and networks," *IEEE Access*, vol. 5, pp. 25408–25420, 2017.
[134] M. R. Clark, K. Stewart, and K. Stewart, "Dynamic, privacy-preserving decentralized reputation systems," *IEEE Trans. Mobile Comput.*, vol. 16, no. 9, pp. 2506–2517, Sep. 2017.

[135] M. Anwar and J. Greer, "Facilitating trust in privacy-preserving e-learning environments," *IEEE Trans. Learn. Technol.*, vol. 5, no. 1, pp. 62–73, May 2011.
[136] S. Donghong, L. Wu, R. Ping, and L. Ke, "Reputation and attribute based dynamic access control framework in cloud computing environment for privacy protection," in *Proc. 12th Int. Conf. Natural Comput., Fuzzy Syst. Knowl. Discovery (ICNC-FSKD)*, Aug. 2016, pp. 1239–1245.
[137] M. Zhang, Y. Xia, O. Yuan, and K. Morozov, "Privacy-friendly weighted-reputation aggregation protocols against malicious adversaries in cloud services," *Int. J. Commun. Syst.*, vol. 29, no. 12, pp. 1863–1872, 2016.
[138] O. Hasan, L. Brunie, E. Bertino, and N. Shang, "A decentralized privacy preserving reputation protocol for the malicious adversarial model," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 6, pp. 949–962, Jun. 2013.
[139] S. Thakur and J. G. Breslin, "A robust reputation management mechanism in federated cloud," *IEEE Trans. Cloud Comput.*, to be published.
[140] I. N. Oteyo and D. P. Mirembe, "Scaling trust and reputation management in cloud services," *Int. J. Appl. Sci. Technol.*, vol. 6, no. 3, pp. 1–8, Sep. 2016.
[141] A. Singh and K. Chatterjee, "A multi-dimensional trust and reputation calculation model for cloud computing environments," in *Proc. ISEA Asia Secur. Privacy (ISEASP)*, Jan./Feb. 2017, pp. 1–8.
[142] A. Schaub, R. Bazin, O. Hasan, and L. Brunie, "A trustless privacy-preserving reputation system," in *Proc. Int. Fed. Inf. Process.*, 2016, pp. 398–411.
[143] W. Ahmad, S. Wang, A. Ullah, and Z. Mahmood, "Reputation-aware trust and privacy-preservation for mobile cloud computing," *IEEE Access*, vol. 6, pp. 46363–46381, 2018.
[144] V. K. Verma, S. Singh, and N. P. Pathak, "Impact of malicious servers over trust and reputation models in wireless sensor networks," *Int. J. Electron.*, vol. 103, no. 3, pp. 530–540, 2016.
[145] X. O. Wang, W. Cheng, P. Mohapatra, and T. Abdelzaher, "Enabling reputation and trust in privacy-preserving mobile sensing," *IEEE Trans. Mobile Comput.*, vol. 13, no. 12, pp. 2777–2790, Dec. 2014.
[146] K. Chandran, V. Shanmugasudaram, and K. Subramani, "Designing a fuzzy-logic based trust and reputation model for secure resource allocation in cloud computing," *Int. Arab J. Inf. Technol.*, vol. 13, no. 1, pp. 30–37, 2015.
[147] P. S. Challagidad, V. S. Reshmi, and M. N. Birje, "Reputation based trust model in cloud computing," *Internet Things Cloud Comput.*, vol. 5, nos. 1–5, pp. 5–12, 2017.
[148] T. H. Noor, Q. Z. Sheng, L. Yao, S. Dustdar, and A. H. H. Ngu, "CloudArmor: Supporting reputation-based trust management for cloud services," *IEEE Trans. Parallel Distrib. Syst.*, vol. 27, no. 2, pp. 367–380, Feb. 2015.
[149] J. Duan, D. Gao, C. H. Foh, and H. Zhang, "TC-BAC: A trust and centrality degree based access control model in wireless sensor networks," *Ad Hoc Netw.*, vol. 11, no. 8, pp. 2675–2692, 2013.
[150] I. Ray and I. Ray, "Trust-based access control for secure cloud computing," in *High Performance Cloud Auditing and Applications*. Aug. 2013, pp. 189–213.
[151] W. Shi, G. Jiang, X. Qin, and S. Wang, "Access control model research for HDFS based on user trust value," *J. Frontiers Comput. Sci. Technol.*, vol. 10, no. 1, pp. 25–35, 2016.
[152] L. Zhou, V. Varadharajan, and M. Hitchens, "Trust enhanced cryptographic role-based access control for secure cloud data storage," in *Proc. Int. Conf. Secur. Cryptogr. (SECRYPT)*, Jul. 2015, pp. 1–5.
[153] M. N. Kulkarni, B. A. Tidke, and R. Arya, "An improved privacy-preserving public auditing for secure cloud storage," in *Proc. 5th Int. Conf. Soft Comput. Problem Solving, Adv. Intell. Syst.*, 2016, pp. 853–866.
[154] B. Silva, P. Maciel, E. Tavares, and A. Zimmermann, "Dependability models for designing disaster tolerant cloud computing systems," in *Proc. IEEE/IFIP Int. Conf. Dependable Syst. Netw. (DSN)*, Jun. 2013, pp. 1–6.
[155] J. B. Bernabe, J. L. H. Ramos, and A. F. S. Gomez, "TACIoT: Multidimensional trust-aware access control system for the Internet of Things," *Soft Comput.*, vol. 20, no. 5, pp. 1763–1779, May 2016.
[156] A. Rafique, D. V. Landuyt, B. Lagaisse, and W. Joosen, "Policy-driven data management middleware for multi-cloud storage in multi-tenant SaaS," in *Proc. IEEE Int. Symp. Big Data Comput. (BDC)*, Dec. 2015, pp. 78–84.
[157] C. Ngo, Y. Demchenko, and C. de Laat, "Multi-tenant attribute-based access control for cloud infrastructure services," *J. Inf. Secur. Appl.*, vol. 27, pp. 65–84, Apr. 2016.
[158] D. Gonzales, J. M. Kaplan, E. Saltzman, Z. Winkelman, and D. Woods, "Cloud-trust—A security assessment model for infrastructure as a service (IaaS) clouds," *IEEE Trans. Cloud Comput.*, vol. 5, no. 3, pp. 523–536, Jul./Sep. 2017.
[159] M. Sicuranza and M. Ciampi, "A semantic access control for easy management of the privacy for EHR systems," in *Proc. 9th Int. Conf. P2P, Parallel, Grid, Cloud Internet Comput.*, Nov. 2014, pp. 400–405.
[160] A. Abo-Alian, N. L. Nagwa, and M. T. Tolba, "Hierarchical attribute-role based access control for cloud computing," in *Proc. 1st Int. Conf. Adv. Intell. Syst. Inform.*, 2015, pp. 381–389.
[161] P. H. Thike and N. Nyein, "Ensuring fine-grained authorized access control for healthcare applications on cloud provisioned platform," in *Proc. Int. Conf. Future Comput. Technol.*, 2015, pp. 184–190.
[162] D.-F. Yan and Y. Tian, "Privacy policy composition of privacy-aware RBAC model for composite WEB services," in *Proc. IEEE IC-BNMT*, Nov. 2013, pp. 312–316.
[163] S. Veloudis and N. Nissanke, "A novel permission hierarchy for RBAC for dealing with SoD in MAC models," *Comput. J.*, vol. 59, no. 4, pp. 462–492, 2016.
[164] L. Gomez and S. Trabelsi, "Obligation based access control," in *Proc. OTM Workshops*, in Lecture Notes in Computer Science, vol. 8842, 2014, pp. 108–116.
[165] M. Jafari and R. S. Naini, "A framework for expressing and enforcing purpose-based privacy policies," *ACM Trans. Inf. Syst. Secur.*, vol. 17, no. 1, pp. 1–3, Aug. 2014.
[166] R. Elgendy, A. Morad, H. G. Elmongui, A. Khalafallah, and M. S. Abougabal, "Role-task conditional-purpose policy model for privacy preserving data publishing," *Alexandria Eng. J.*, vol. 56, pp. 459–468, Dec. 2017.
[167] Z. Sainan and H. Yu, "Research and application of XACML-based fine-grained security policy for distributed system," in *Proc. Int. Conf. Mechatronic Sci., Electr. Eng. Comput.*, Dec. 2013, pp. 1848–1851.
[168] Q. Li, R. Sandhu, X. Zhang, and M. Xu, "Mandatory content access control for privacy protection in information centric networks," *IEEE Trans. Dependable Secure Comput.*, vol. 14, no. 5, pp. 494–506, Sep./Oct. 2017.
[169] H. Qinlong, Z. Ma, Y. Yang, X. Niu, and J. Fu, "Attribute based DRM scheme with dynamic usage control in cloud computing," *China Commun.*, vol. 11, no. 4, pp. 50–63, Apr. 2014.
[170] J. M. M. Pérez, G. M. Pérez, and A. F. S. Gómez. "SecRBAC: Secure data in the clouds," *IEEE Trans. Services Comput.*, vol. 10, no. 5, pp. 726–740, Sep./Oct. 2017.
[171] B. Lang, J. Wang, and Y. Liu, "Achieving flexible and self-contained data protection in cloud computing," *IEEE Access*, vol. 5, pp. 1510–1523, 2017.
[172] D. Xu, M. Kent, L. Thomas, T. Mouelhi, and Y. Le Traon, "Automated model-based testing of role-based access control using predicate/transition nets," *IEEE Trans. Comput.*, vol. 64, no. 9, pp. 2490–2505, Sep. 2015.
[173] D. He, S. Chan, and M. Guizani, "Accountable and privacy-enhanced access control in wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 1, pp. 389–398, Jan. 2015.
[174] J. P. Cruz, Y. Kaji, and N. Yanai, "RBAC-SC: Role-based access control using smart contract," *IEEE Access*, vol. 6, pp. 12240–12251, 2018.
[175] M. S. Kirkpatrick, G. Ghinita, and E. Bertino, "Privacy-preserving enforcement of spatially aware RBAC," *IEEE Trans. Dependable Secure Comput.*, vol. 9, no. 5, pp. 627–640, Oct. 2012.
[176] L. Zhou, V. Varadharajan, and M. Hitchens, "Achieving secure role-based access control on encrypted data in cloud storage," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 12, pp. 1947–1960, Oct. 2013.
[177] H. C. Chen, "A hierarchical virtual role assignment for negotiation-based RBAC scheme," in *Proc. 10th Int. Conf. Broadband Wireless Comput., Commun. Appl.*, Nov. 2015, pp. 538–543.
[178] A. Almutairi, M. Sarfraz, S. Basalamah, W. Aref, and A. Ghafoor, "A distributed access control architecture for cloud computing," *IEEE Softw.*, vol. 29, no. 2, pp. 36–44, Mar./Apr. 2012.
[179] P. Zhang, Z. H. Chen, and J. K. Liu, "An efficient access control scheme with outsourcing capability and attribute update for fog computing," *Future Gener. Comput. Syst.*, vol. 78, pp. 753–762, Jan. 2018.
[180] Q. Huang, Y. Yang, and L. Wang, "Secure data access control with ciphertext update and computation Outsourcing in fog computing for Internet of Things," *IEEE Access*, vol. 5, pp. 12941–12950, 2017.
[181] Y. Zhu, D. Huang, C.-J. Hu, and X. Wang, "From RBAC to ABAC: Constructing flexible data access control for cloud storage services," *IEEE Trans. Serv. Comput.*, vol. 8, no. 4, pp. 601–616, Jul./Aug. 2015.
[182] K. Xue, Y. Xue, J. Hong, W. Li, H. Yue, D. S. L. Wei, and P. Hong, "RAAC: Robust and auditable access control with multiple attribute authorities for public cloud storage," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 4, pp. 953–967, Apr. 2017.

[183] Y. Jin, C. Tian, H. He, and F. Wang, "A secure and lightweight data Access control scheme for mobile cloud computing," in *Proc. 5th Int. Conf. Big Data Cloud Comput.*, vol. 15, Aug. 2015, pp. 172–179.
[184] A. D. Santis, A. L. Ferrara, and B. Masucci, "Efficient provably-secure hierarchical key assignment schemes," *Theor. Comput.*, vol. 412, no. 41, pp. 5684–5699, 2011.
[185] M. J. Atallah, M. Blanton, N. Fazio, and K. B. Frikken, "Dynamic and efficient key management for Access hierarchies," *ACM Trans. Inf. Syst. Secur.*, vol. 12, no. 3, p. 18, 2009.
[186] Y.-L. Lin and C.-L. Hsu, "Secure key management scheme for dynamic hierarchical access control based on ECC," *J. Syst. Softw.*, vol. 84, no. 4, pp. 679–685, 2011.
[187] E. S. V. Freire, K. G. Paterson, and B. Poettering, "Simple, efficient and strongly KI-secure hierarchical key assignment schemes," in *Proc. Cryptograph. Track RSA Conf.*, 2013, pp. 101–114.
[188] S. Tang, X. Li, X. Huang, Y. Xiang, and L. Xu, "Achieving simple, secure and efficient hierarchical Access control in cloud computing," *IEEE Trans. Comput.*, vol. 65, no. 7, pp. 2325–2331 Jul. 2016.
[189] T. Salman and M. Zolanvari, "Security services using blockchains: A state of the art survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 858–880, 1st Quart., 2019.
[190] J. Ni and K. Zhang, "Securing fog computing for Internet of Things applications: Challenges and solutions," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 1, pp. 601–628, 1st Quart., 2018.
[191] J. Zhou, Z. Cao, X. Dong, and A. V. Vasilakos, "Security and privacy for cloud-based IoT: Challenges, countermeasures, and future directions," *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 26–33, Jan. 2017.
[192] M. Trevors and R. A. Vrtis. A mapping of the health insurance portability and accountability act (HIPAA) security rule to the cyber resilience review (CRR). Carnegie Mellon University. [Online]. Available: https://resources.sei.cmu.edu/asset_files/TechnicalNote/2018_004_001_516844.pdf
[193] K. Colorafi and B. Bailey, "It's time for innovation in the health insurance portability and accountability act (HIPAA)," *JMIR Med. Inform.*, vol. 4, no. 4, p. e34, 2016.
[194] R. Zhang, R. Xue, and L. Liu, "Searchable encryption for healthcare clouds: A survey," *IEEE Trans. Service Comput.*, vol. 11, no. 6, pp. 978–996, Nov./Dec. 2018.
[195] K. Edemacu, H. K. Park, B. Jang, and J. W. Kim, "Privacy provision in collaborative Ehealth with attribute-based encryption: Survey, challenges and future directions," *IEEE Access*, vol. 7, pp. 89614–89636, 2019.
[196] J. Iyilade and J. Vassileva, "P2U: A privacy policy specification language for secondary data sharing and usage," in *Proc. IEEE Secur. Privacy Workshops*, May 2014, pp. 18–22.
[197] A. Ghorbel, M. Ghorbel, and M. Jmaiel, "Privacy in cloud computing environments: A survey and research challenges," *J. Supercomput.*, vol. 73, no. 6, pp. 2763–2800, Jun. 2017.
[198] S. Kokolakis, "Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon," *Comput. Secur.*, vol. 64, pp. 122–134, Jan. 2017.



PAN JUN SUN received the M.S. degree in control theory and application from the Taiyuan University of Science and Technology, in 2010. He is currently pursuing the Ph.D. degree in information and communion system from Shanghai Jiao Tong University. His research interests include cloud computing, privacy preservation, access control, and trust management.