Journal Pre-proof

Security and privacy protection in cloud computing: Discussions and challenges

Pan Jun Sun

PII: S1084-8045(20)30116-8

DOI: https://doi.org/10.1016/j.jnca.2020.102642

Reference: YJNCA 102642

To appear in: *Journal of Network and Computer Applications*

Received Date: 1 August 2019

Revised Date: 11 March 2020

Accepted Date: 20 March 2020

Please cite this article as: Sun, P.J., Security and privacy protection in cloud computing: Discussions and challenges, *Journal of Network and Computer Applications* (2020), doi: https://doi.org/10.1016/j.jnca.2020.102642.

Graphic abstract

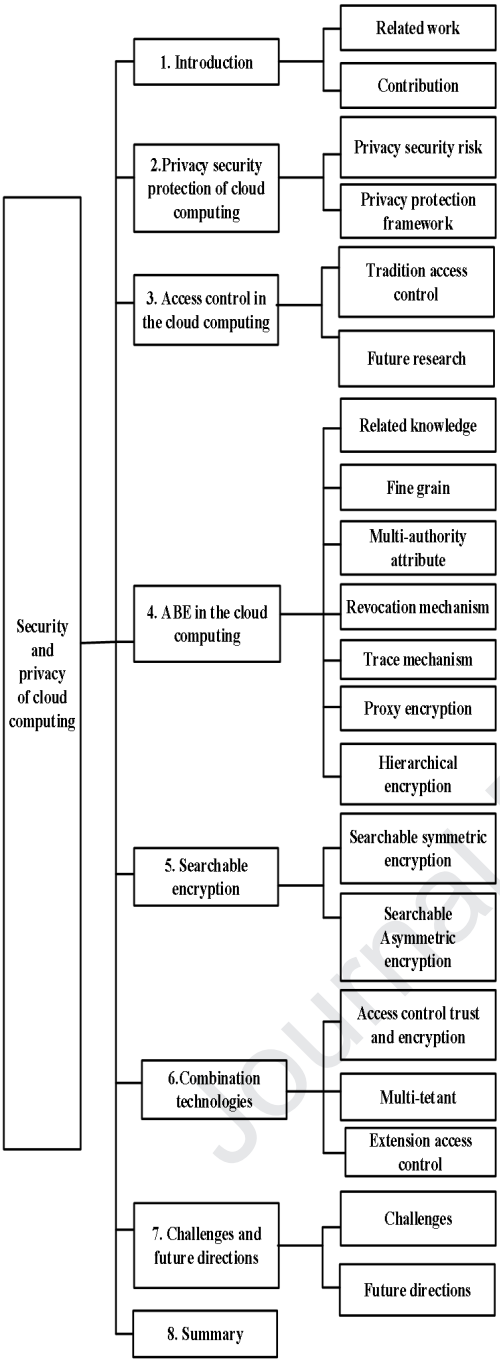


Fig.1. The organization framework of this paper

With the development of cloud computing, the privacy security issues become more and more prominent, which have been widely concerned by the industry and academia. We review the research progress from the perspective of privacy security protection technology in the cloud computing. Firstly, we introduce some privacy security risks of cloud computing, propose a comprehensive privacy security protection framework; secondly, we describe the research progress of several technologies, for example, access control, ciphertext policy attribute-based encryption (CP-ABE), key policy attribute-based encryption (KP-ABE), fine-grain, multi-authority, revocation mechanism, trace mechanism, proxy re-encryption(PRE), hierarchical encryption, searchable encryption (SE), multi-tenant, trust, and combination of multiple technologies and so on, then compare and analyze the

characteristics and application scope of typical schemes; finally, we discuss the current challenges, and point out possible research directions in the future.

Security and Privacy Protection in Cloud Computing: Discussions and Challenges

Pan Jun Sun

School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, 800 Dongchuan RD, Minhang, Shanghai, China

ABSTRACT: With the development of cloud computing, privacy security issues have become increasingly prominent, which is of concern to industry and academia. We review the research progress on privacy security issues from the perspective of several privacy security protection technologies in cloud computing. First, we introduce some privacy security risks of cloud computing and propose a comprehensive privacy security protection framework. Second, we show and discuss the research progress of several technologies, such as access control; ciphertext policy attribute-based encryption (CP-ABE); key policy attribute-based encryption (KP-ABE); the fine-grain, multi-authority, revocation mechanism; the trace mechanism; proxy re-encryption (PRE); hierarchical encryption; searchable encryption (SE); and multi-tenant, trust, and a combination of multiple technologies, and then compare and analyze the characteristics and application scope of typical schemes. Last, we discuss current challenges and highlight possible future research directions.

Keywords: cloud computing, privacy security, access control, attribute-based encryption, trust.

1. Introduction

Cloud computing connects many computing resources, storage resources, and software resources to form a vast shared virtual resource pool, from which users can purchase corresponding services, such as hydropower. With the rapid popularization of cloud computing applications, cloud computing has penetrated various fields, such as scientific research, production, education, consumption, entertainment, etc. (http://www.cloudsecurityalliance.org/).

1.1. Basic concepts of cloud computing

The technology of cloud computing virtualization provides efficient resources for end users. The characteristics of cloud computing include manageability, scalability and availability. In addition, cloud computing has the advantages of economy, on-demand service, convenience, universality, multi tenancy, flexibility and stability. Cloud computing mainly provides three service delivery models and four development patterns (http://www.cloudsecurityalliance.org/): infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS), public cloud, private cloud, hybrid cloud, community cloud and virtual private cloud (Fig 1.).

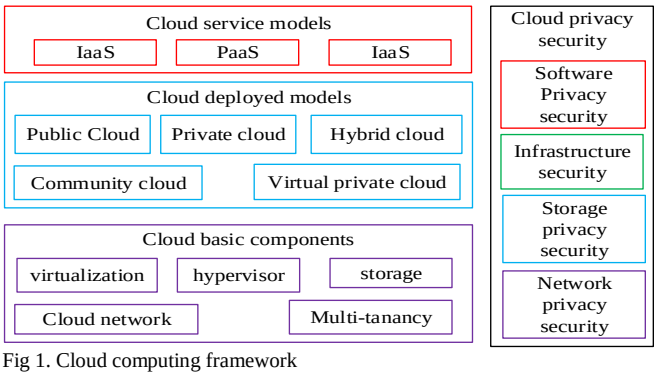


Fig 1. Cloud computing framework

IaaS treats computer hardware (network storage, virtual server/computer, data center, processor and memory) as a service and provides infrastructure scalability and provisioning issues without requiring significant capital and time. IaaS also focuses on firewall, intrusion detection, virtual machine monitoring and other security areas.

PaaS locates in the middleware of the service model and provides services in the form of development tools, frameworks, architectures, programs and integrated development environments. PaaS faces many challenges, such as third-party relationships, lifecycle development, and underlying infrastructure security.

SaaS is a collection of remote computing services that enables third-party vendors to remotely deploy applications. A customer can use the Internet for applications of cloud service providers on the cloud infrastructure.

Private Cloud: cloud computing is runs and managed within the data center of an organization, which is referred to as a private cloud. In a private cloud, customer and supplier relationships are easier to identify because the infrastructure is owned and operated by the same organization.

Public cloud: enterprises, academia or government organizations have a public cloud environment, which can cause many problems because users do not know the locations or owners of resources, which increases the difficulty of protecting resources from attacks.

Community cloud: an organization's cloud infrastructure has common concerns with consumers (tasks, security needs, policies and compliance considerations). This cloud is driven by one or more organizations that own and manage community organizations or third parties.

Hybrid cloud: it is a combination of two or more clouds (public, private, community). A hybrid cloud provides the advantages of different cloud deployment models. However, when accessing entities via the Internet, a hybrid cloud is

better organized and more secure than a public cloud.

Virtual private cloud: it is a semi private cloud with less resources that is composed of a virtual private network (VPN). This cloud is the shared resource pool allocated in the cloud environment.

Virtualization: it has an important role in deploying a cloud. Virtualization creates virtual instances of resources or devices, such as operating systems, servers, network resources, and storage devices, where the framework leverages resources in multiple execution environments.

Multi-tenant: a multi-tenant environment can have multiple customers or users who cannot see or share each other's data but can share resources or applications even if they may not belong to the same organization.

Cloud storage: it is a component that can be maintained, managed and backed up via the network.

Hypervisor: It enables multiple virtual machines (VMS) to run on a single hardware host. A hypervisor manages and monitors the various operating systems in a shared system.

Cloud network: it can operate multiple traditional data centers; a data center can contain many servers. A cloud network needs an Internet connection and a virtual private network to ensure that users can safely access webs, documents, etc.

In cloud computing, a vast amount of data needs to be uploaded to a cloud computing center. Because of the loss of full control of resources, users are more concerned about privacy security (Shareeful and Moussa, 2018). Due to the complexity and real-time nature of the cloud computing service model, multi-source heterogeneity and perception of data, as well as the limited resources of terminals, the traditional data security and privacy protection mechanism is not suitable for the protection of massive data generated by cloud computing (Muhammad et al, 2017).

Therefore, various security problems must be comprehensively analyzed and solved by cloud computing.

1) New requirements for lightweight data encryption and fine-grained data sharing based on multi-authorized parties in cloud computing. Because cloud computing integrates multi-trust domains with authorized entities, the traditional data encryption and sharing policy is not applicable. Therefore, the design of a new encryption method for multiple authorization centers.

2) Multi-source data transmission and service management in cloud computing. Due to the outsourcing characteristics of data, both ownership and control are separated, so an effective security scheme is necessary to ensure integrity.

3) Security privacy challenges between large scale internet services and resource-constrained terminals in cloud computing. Due to the multi-source data fusion characteristics, the superposition of mobile and Internet networks, and the resource limitations of terminal storage, both traditional encryption algorithms and access control and privacy protection methods cannot be applied in cloud computing.

4) New requirements of cloud computing privacy protection. How to combine traditional privacy schemes in cloud computing and how to realize user privacy protection in a diversified service environment are urgent problems.

1.2. Related works

This section focuses on the privacy and security issues of cloud computing and the corresponding technical solutions. To show the characteristics of this article, we compared it with some articles in Table 1.

Table 1. Contrast of several survey papers

Article	Year	Application	Technology	Compare complexity	Review
Ours	2019	Cloud computing	Access control, encryption, trust	Yes	Yes
(Xiao and Xiao et al, 2013)	2013	Cloud computing	Trust, encryption	No	No
(Johanna and Tanja, 2017)	2017	Cloud computing	Secret communication	No	Yes
(SHEKHA et al, 2019)	2015	Cloud medical	Encryption, EHR, non-encryption	No	Yes
(Zhang and Xue, 2018)	2019	Healthcare cloud	Searchable encryption	Yes	Yes
(Liu and Yan, 2019)	2019	Edge computing	Encryption	Yes	Yes
(Tara and Maede,2019)	2019	Blockchain	Access control, PKI	No	Yes
(Ni and Zhang, 2018)	2019	IOT, fog computing	Access control, authentication	No	Yes

The privacy security of cloud computing has always been a hot topic in academic circles. Xiao and Xiao et al. (2013) discussed five security and privacy attributes (confidentiality, privacy protection, integrity, availability and accountability) and showed security vulnerabilities, threat models and defense strategies but lacked specific performance contrast description. Johanna and Tanja (2017) investigated various methods of secret communication, such as secret channel, bypass and fuzzy technology. However, these methods comprise a kind of non-mainstream technology and application, and the application scope is very narrow. Medical records in cloud computing are likely to be leaked. SHEKHA and KHANDAKAR et al.(2019) discussed and investigated the following aspects: 1) Electronic Health Record (EHR) security and privacy; and 2) security and privacy requirements of health data in a cloud environment; 3) EHR cloud architecture; and 4) different EHR encryption and non-encryption schemes.

Zhang and Xue (2018) summarized several SE technologies: searchable symmetric encryption (SSE), public key encryption keyword search (PEKS), attribute-based encryption keyword search (ABKS) and proxy re-encryption keyword search (PRES). However, they only gave a technical overview of the searchable encryption model, which lacked relevant algorithms and performance contrast analysis.

Liu and Yan et al. (2019) introduced the concept and characteristics of edge computing and proposed some

requirements by analyzing the potential security threats of edge computing based on encryption. Tara and Maede (2019) investigated several security service methods based on blockchain, such as authentication, confidentiality, access control list, resource sources and integrity assurance, and discussed the challenges of security services.

Ni and Zhang (2018) showed the potential challenges of fog protection and summarized the latest solutions to security and privacy problems. However, the paper mainly explored the development of the Internet of Things, rarely discussed the research progression of privacy security protection, and lacked systematic discussion.

1.3. Contributions

In cloud computing, researchers have made numerous privacy protection achievements, such as access control, encryption and trust, but they are dispersive and lack overall logic (RajaniKanth and Lakshm 2015, SUN et al.2019)

Therefore, systematically summarizing, analyzing and discussing relevant research progress is necessary to understand cloud computing privacy protection from a more comprehensive perspective.

This paper focuses on several important technologies, such as access control, attribute-based encryption, trust, and search encryption, and highlights the future development direction. The main innovations are presented as follows:

- We discuss the privacy security risks of cloud computing and propose a comprehensive privacy protection framework.
- We analyze the characteristics of several access control models and highlight their advantages and disadvantages based on various factors.
- We summarize the algorithm flow and development of ABE, and discuss several important achievements in cloud privacy protection, such as fine-grained, revocation mechanism, multi-authority, trace mechanism, proxy re-encryption and hierarchical encryption.
- We discuss and compare two searchable encryption schemes, such as searchable asymmetric encryption (SAE) and searchable symmetric encryption (SSE).
- We discuss and analyze the integration technology scheme of access control, trust and encryption and discuss the challenges and future research directions.

The organization of this article is arranged as follows: In section 2, we describe the risk of privacy security in cloud computing and propose a comprehensive framework. In section 3, we discuss the characteristics and future direction of access control. In section 4, we discuss several ABEs, such as the fine-grain, multi-authority, revocation mechanism; trace mechanism; proxy re-encryption and hierarchical encryption. In section 5, we analyze two searchable encryption schemes of cloud computing for several conditions. In section 6, we analyze the integration of access control, trust and encryption to implement privacy protection. In section 7, we discuss privacy security issues and future directions of cloud computing. In section 8, we consider that privacy protection needs not only technology but also corresponding laws. To understand this paper, a structural framework is given in Fig. 2.

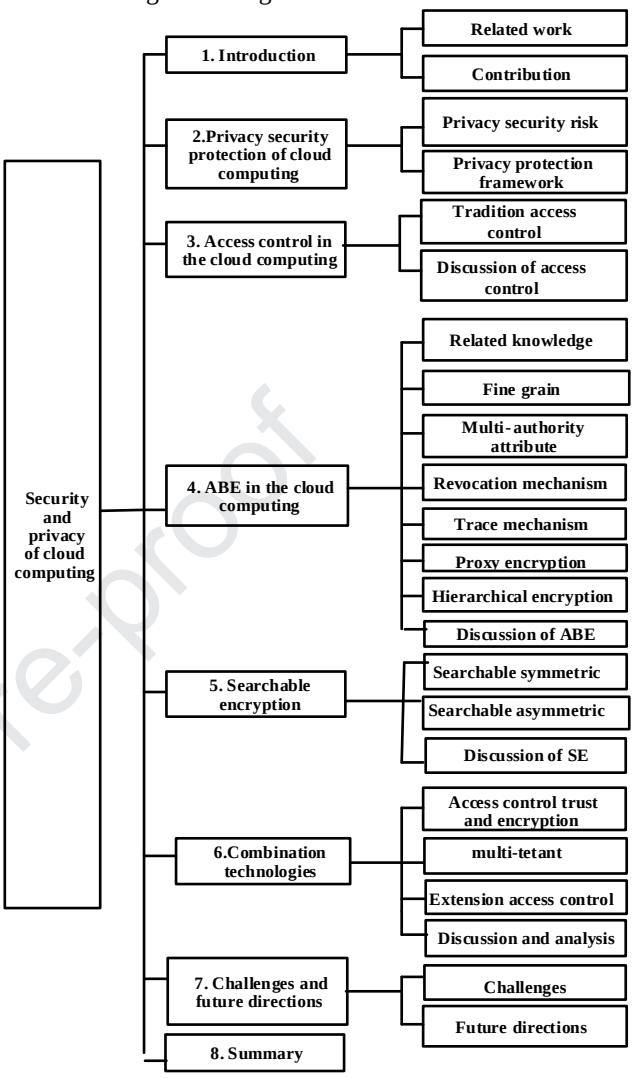


Fig. 2. Organization framework of this paper

2. Privacy security of cloud computing

The structural characteristics of the cloud computing environment are the main causes of security problems. First, the nodes involved in computing are diverse, sparsely distributed and often unable to be effectively controlled. Second, the cloud service provider (CSP) has the risk of disclosing privacy in the process of transmission, processing and storage. Because cloud computing is based on technology, the security vulnerabilities of existing technologies will be directly transferred to a cloud computing platform and have even greater security threats.

2.1. Privacy security risk

From information security, network security to cloud computing security, the constant requirement of security is the confidentiality and privacy protection of information. According to the annual report of the Cloud Security Alliance

(CSA) and the research results of relevant scholars in literature, we can conclude several threats to privacy security risk (Fig. 3) (Reza and Satyajayant 2018).

(1) Privacy data security: Due to the service outsourcing mode, the security risk of cloud privacy, such as data disclosure, privacy disclosure, access rights management, and data destruction difficulties, is particularly prominent.

(2) Access control and identity authentication: Cloud computing involves massive resources; the management complexity of access control and identity authentication expands dramatically.

(3) Virtualization security: Although service providers have designed and implemented isolation strategies for virtual machines, the attacks among virtual machines cannot be completely avoided; virtual machine migration will also produce changes in the security domain.

(4) Multi-tenant and cross-domain sharing: Multi-tenant isolation and multi-user security need to be guaranteed. A cross-domain makes service authorization and access control more complex, and trust transfer between two cloud computing entities needs to be reexamined.

(5) Advanced Persistent Threat (APT): APT is a planned intrusion and attack on a cloud computing system that has formed some underground interest chains.

(6) System security vulnerability: Due to the complexity of a cloud computing system, many service providers have different management and service levels; so security vulnerabilities will increase the danger in the cloud.

(7) Insider threat: The unintentional or intentional information leakage of the service provider's insiders often makes the security policy invalid, which has become an important issue of cloud computing security.

(8) Wrong application of cloud service: The misuse of cloud computing will cause troubles for users, service providers or third parties, and the illegal use of cloud service will cause serious consequences.

(9) Service availability: Many security events are manifested as the unavailability of cloud computing services, and the denial of service attacks has become an important security target for cloud service providers.

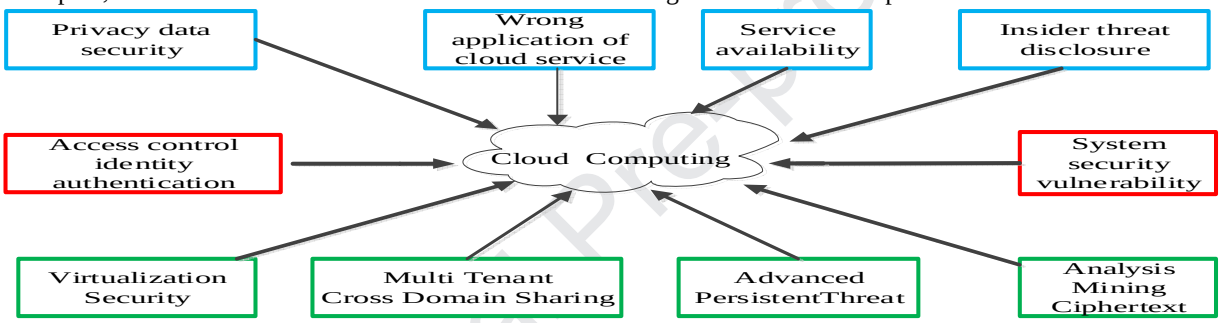


Fig .3. Privacy security risk in cloud computing

2.2. Privacy protection framework

Due to the higher resource concentration and architecture complexity of a cloud computing system, these security issues pose a greater threat to the cloud computing system (SUN et al.2019, RajaniKanth and Lakshm 2015). In a complex situation, this paper proposes a comprehensive cloud computing privacy protection security system based on a variety of technologies, such as access control, trust, attribute-based encryption, search encryption and other technologies, as shown in Fig. 4.

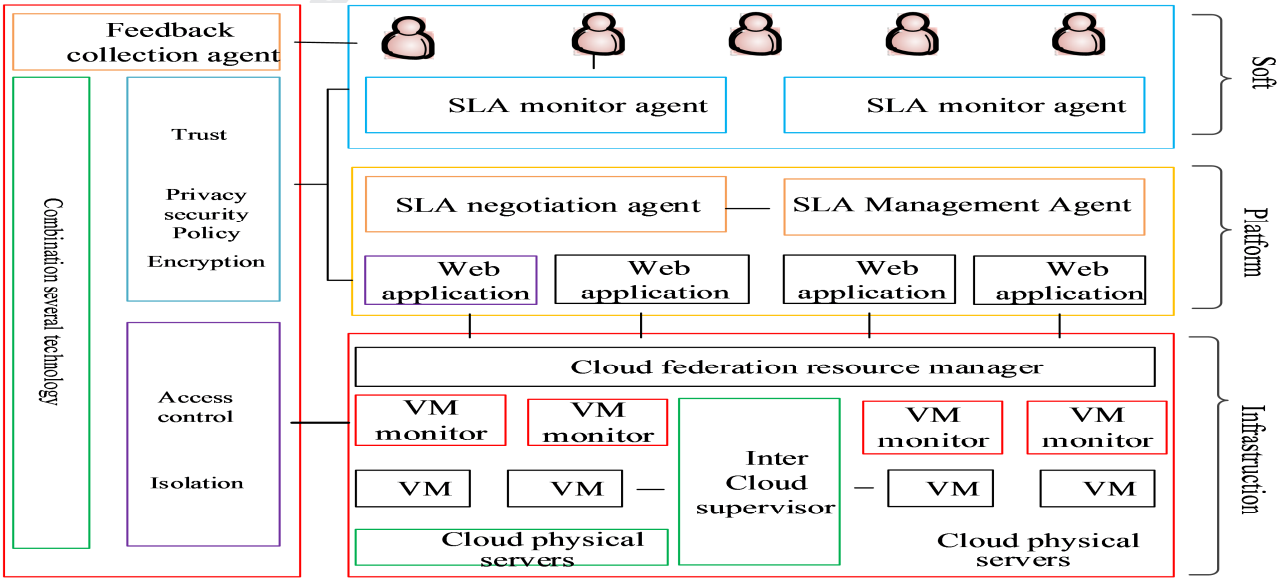


Fig. 4. Privacy protection framework of cloud computing system

In the infrastructure layer, physical isolation and corresponding policy management rules are generally employed. In the platform layer and software application layer, encryption, trust and privacy policies are mostly applied. Of course, these technologies do not have strict application restrictions but need specific analysis

.3. Access control in cloud computing

In the era of cloud computing, both the computing and storage mode have changed substantially, which creates new challenges to access control research: how to develop traditional access control technology to solve new cloud computing security problems (Reza and Satyajayant, 2018).

3.1. Tradition access control

Access control has an important role in: (1) preventing illegal users from accessing information resources; (2) allowing legal users to access information resources; and (3) preventing legal users from accessing information resources (RajaniKanth and Lakshm 2015). In cloud computing, according to the different functions of the access control model, the research content and methods are also different (SUN et al. 2019). With the continuous development of network technology, researchers have proposed many extended models, such as discretionary access control (DAC), mandatory access control (MAC), role based access control (RBAC, Fig. 5) (Ferraiolo and Sandhu, 2001), attribute based access control (ABAC, Fig. 6), reference monitoring access control (RMAC), task based access control (TBAC), and usage control (UCON, Fig. 7). These models can solve the problem of access control in a system from different levels and ensure the legitimacy, security and controllability of information access (Fig. 8).

	MAC	DAC	RBAC	TBAC	ABAC	RMAC	UCON
Security	√	-	-	-	-	√	√
Confidentiality	√	√	-	-	-	√	-
Flexibility	-	√	√	√	√	√	√
Minimum privilege	√	-	√	√	√	-	√
Duty separation	√	-	√	√	√	-	-
Description	√	√	√	√	√	-	-
Granularity	√	√	-	√	√	√	√
Constraint	√	-	√	-	√	√	√
Dynamic	-	√	-	√	√	√	√
Compatibility	-	√	√	-	√	-	√
Expansibility	-	√	-	√	√	-	√
Management	√	-	√	-	-	-	-
Modeling	√	√	√	-	√	-	-

Table 2. Contrast results of common access control models

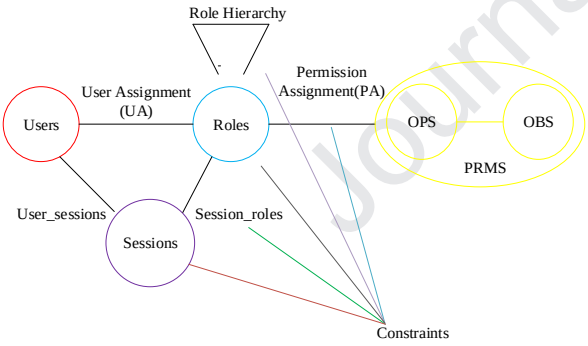
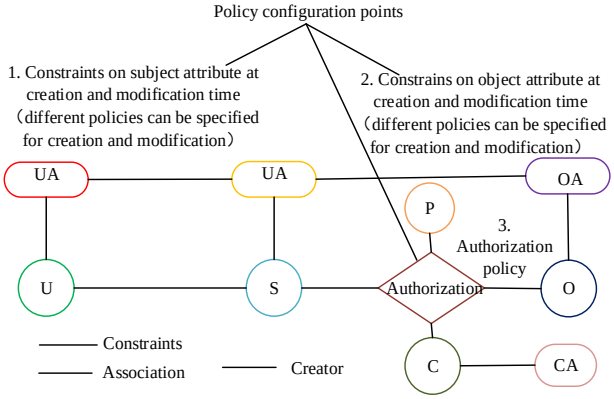


Fig. 5. Basic RBAC model



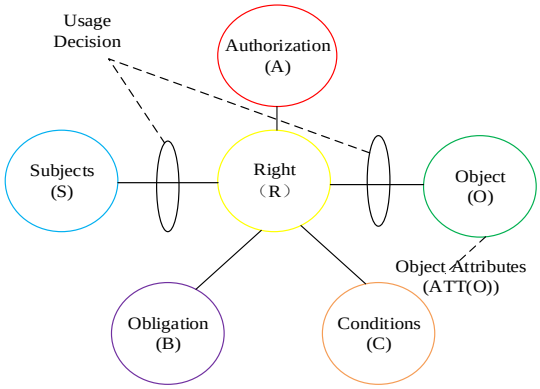


Fig. 6. Basic ABAC model

Fig. 7. Basic UCON model

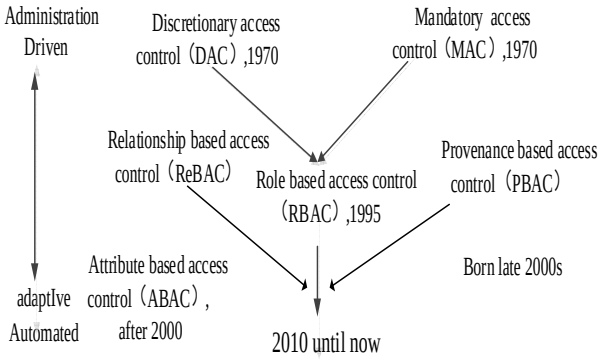


Fig. 8. Relationship of multiple access control models

To analyze and compare the capability, performance and security of each access control model more intuitively and concisely, we give 13 factors: security, confidentiality, flexibility, minimum privilege, duty separation, description ability, granularity control, constraint description, dynamics, compatibility, expansibility, management difficulty and modeling difficulty. In Table 2, the symbol "√" indicates that the factor has suitable performance, and the symbol "-" indicates that the factor is poor or does not have index characteristics.

3.2 Discussion of access control

According to the characteristics and specific needs of cloud computing, an excellent access control mechanism must be flexible, scalable and network independent (Ning and Elisa, 2013). We suggest that the future access control technology in cloud computing should focus on the following aspects:

(1) Research on access control based on virtualization technology. Because virtual machines of different organizations or departments often run on the same physical host, although virtual technology has excellent isolation, communication among virtual machines in many applications is necessary, and the frequent interaction among virtual machines introduces new security challenges.

(2) Research on the impact of virtual machine dynamic migration on access control. With the migration of a virtual machine, the policy cannot be changed; if it is virtual machine storage, the data are likely to be migrated to other networks, and the access rights may also change. Therefore, how to ensure the impact of a network and permission changes on data access control is very important.

(3) Research on access control based on information resource attributes. The traditional access control model can be better combined with cloud computing, which greatly reduces problems that may occur in the access control process of various resources, and conforms to the real model of cloud computing.

(4) Research on access control model of space-time awareness. When the cloud computing environment is expanded to a certain scale, the user's location is very important, which can determine what kind of resources the user can obtain, and the user can be judged by location information.

(5) Research on access control technology based on trust relationship. With the development of research on the trust model, the trust relationship among the data provider, cloud platform and user in a cloud computing system is different.

(6) Research and implement a cross-domain, cross group, hierarchical dynamic fine-grained access control system. Many problems in the cross-domain access control, such as unauthorized access, access conflict, key management, policy management, and attribute management.

Many cloud access control schemes have different descriptions of rules, which cannot satisfy the application requirements due to many shortcomings. Therefore, the development of a unified, easy-to-use, clear and efficient access control rule description method is necessary. Attribute-based encryption is an attractive research topic because it provides a fine-grained, non-interactive access control mechanism for encrypted data and has great application potential in many fields (Ning and Elisa, 2013).

4. ABE in cloud computing

ABE is an encryption mechanism that is suitable for cloud computing (Xu and Yang, 2018) and can also realize privacy protection during data sharing (He and Li, 2014). To protect users' privacy sensitive data, researchers have proposed many ABEs for different participating entities in a cloud computing system (Fig. 9).

ABE can realize not only the encryption of cloud storage data (Wang and Liang, 2016) but also the fine-grained access control of data. Attribute encryption has the following four advantages:

1 The data owner needs to encrypt according to the attributes and does not need to pay attention to the number and identities of users;

2 Users can decrypt ciphertext when they satisfy the attribute requirements;

3 The key of ABE is related to a random number, which can prevent the collusion attack of users;

4 Support flexible fine-grained access control.

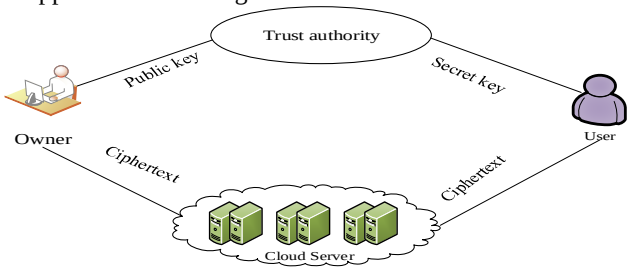


Fig. 9. Architecture of attribute-based encryption

4.1. Related knowledge

When encrypting information, the encryptor does not need to know who decrypts ciphertext, and the decryptor party only needs to satisfy the corresponding attribute conditions to decrypt it (Brent et al, 2011). Moreover, ABE contains the related rules in the encryption algorithm (Huang and Yang, 2017), which can avoid the frequent key distribution cost in the access control of ciphertext (Beime et al, 1996).

4.1.1. Category of ABE

Currently, ABE is mainly investigated from the following aspects in the cloud computing environment: fine-grained, multi-authority, revocation mechanism, hierarchical architecture, trace mechanism, and proxy-encryption (Amit and Brent, 2005), as shown in Fig. 10.

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 (Goyal and Pandey, 2006). In the following example, {computer, college, undergraduate} is the public key to send cryptography to undergraduates of a computer college (Mihir and Dennis, 2015). The private key is calculated and distributed to individuals by the attribute authority (Joon and Willy, 2007).

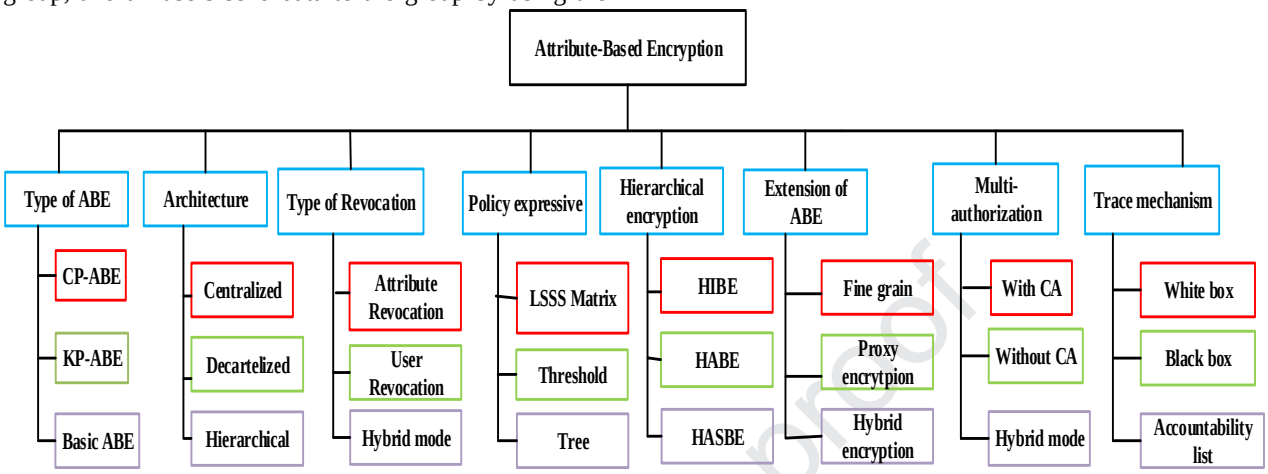


Fig. 10. Main content of ABE in this paper

4.1.2. Several definitions

The ABE mechanism employs an access structure representation policy, considers bilinear pairing as the technical basis, and constructs security based on various mathematical problems and assumptions. In (Beime et al, 1996), several basic concepts exist.

Lagrange interpolation polynomial: For a set of $k+1$ given data points, $(x_0, y_0), \cdots, (x_j, y_j), \cdots, (x_k, y_k)$. x_j has different values, and the function $f(x)$ can satisfy all $k+1$ data points on the curve of $F(x)$, which can be generated by the Lagrange polynomial formula:

$$F(x) = y_0 f_0(x) + y_1 f_1(x) + \cdots + y_j f_j(x) + \cdots + y_k f_k(x)$$

$F(x)$ is a combination of the basis polynomial $f(x)$, and $f_j(x)$ is expressed as follows:

$$f_j(x) = \frac{(x - x_0)}{(x_j - x_0)} \cdots \frac{(x - x_{j-1})}{(x_j - x_{j-1})} \frac{(x - x_{j+1})}{(x_j - x_{j+1})} \cdots \frac{(x - x_k)}{(x_j - x_k)}$$

When $x = x_j$, the value of $f_j(x)$ is 1; otherwise, $x \neq x_i (i \neq j)$, and the value of $f_j(x)$ is 0.

Definition 1. (Access structure: A) (Beime et al, 1996). Assuming that $\{P_1, P_2, \cdots, P_n\}$ is a collection of participants, $P = 2^{\{P_1, P_2, \cdots, P_n\}}$. A is a non-empty subset of $\{P_1, P_2, \cdots, P_n\}$, and $\mathrm{A} \subseteq P \setminus \{\varnothing\}$. If A is monotonous, $\forall B, C$; if $B \in \mathrm{A}$ and $B \subseteq C$, then $C \in \mathrm{A}$.

An access tree is an expression of access structure, which supports not only supports the access policy of threshold mode but also logical operations such as "and"\"or". In Amit and Brent (2005), node x in the access tree is defined as follows:

$Parent(x)$: The parent node of node x is valid for all nodes except the $root$.

$Children(x)$: The set of children of node x.

$Num(x)$: The number of children of node x.

$index(x)$: The sequence number of node x on the same node level.

$attr(x)$: The attribute of node x.

Each node in the access tree represents a threshold, and the value of n_x satisfies $1 \le n_x \le Num(x)$. The value of "or" is $n_x = 1$, and the value of "and" is $n_x = Num(x)$.

Amit and Brent (2005) proposed the threshold (k, n) that divides the secret information s into n sections by the Lagrange interpolation theorem. In Fig. 11, k_x denotes the threshold requirement for recovering secret information.; When $k_x = 1$, the threshold policy is ("OR"); when $k_x = n$, the threshold policy is ("AND").

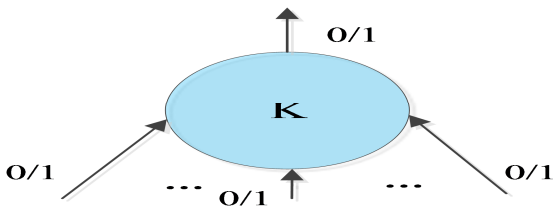


Fig. 11. Threshold access structure

The basic ABE has only a "threshold" operation; so the flexibility is severely limited. However, many applications need to support a flexible access control policy to realize the encryption target of the sender. As shown in Fig. 12, the tree structure contains "and", "or" and "threshold" operations to represent more complex logical relationships.

Linear Secret-Sharing Schemes (LSSS), Amos and Aner 2014) can protect the key, resist malicious attacks, and reduce the risk of secret disclosure.

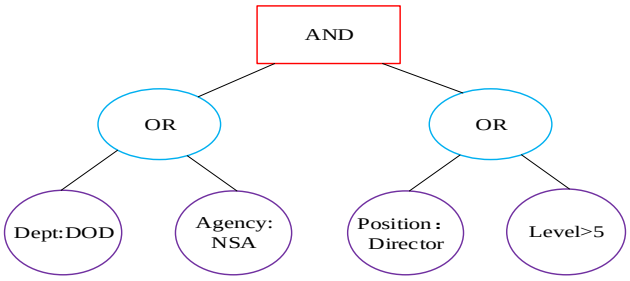


Fig. 12. Tree access structure

Assume that (M,ρ) expresses the access structure A, M is a $l\times K$ matrix, and function ρ maps $\{1,2,\cdots,l\}$ of matrix M to the secret sharing participant P. The process of LSSS includes the following steps:

(1) Secret sharing algorithms. Randomly choose $v_1,v_2,\cdots,v_{k-1}$ from Z_p, and merge the secret s to constitute the vector $v=(s,v_1,v_2,\cdots,v_{k-1})$. If A_i is the ith line element of M, the secret shared element of participant $\rho(i)$ can be expressed as $\sigma_i=A_i\bullet v$.

(2) Secret recovery algorithms. If the set of attributes is $\omega\in A$, $L=\{i\,|\,\rho(i)\in\omega\}$ and the set of recovery coefficients $\{\mu_i\}_{i\in L}$ can be computed by A, $\sum_{i\in L}\mu_i\bullet\sigma_i=s$.

(3) Although LSSS can alleviate the initial needs of the system for attribute and user space, the complex access structure increases the difficulty of public key design and the calculation cost of the system (Shamir et al, 1979).

Definition 2. (Bilinear pairings, Boneh and Franklin 2001). Map: $e:G_1\times G_1\to G_2$. This definition has three features: (1) Bilinear: $\forall a,b\in Z_q,\forall f,h\in G_1$, if $e(f^a,h^b)=e(f,h)^{ab}$, then $e:G_1\times G_1\to G_2$ is bilinear; (2) Non-degenerate: if $\exists f\in G_1$, then $e(f,f)\neq 1$; and (3) Computable: if $\forall f,h\in G_1$, we have an efficient computing algorithm of $e(f,h)$, $e(f^a,h^b)=e(f,h)^{ab}=e(f^b,h^a)$, and $e(*,*)$ is a symmetric operation.

Definition 3. (Computation Diffie-Hellman Assumption, Shao et al, 2009). Randomly choose $a,b\in Z_q^*$, compute g^{ab} by a triple couple (g,g^a,g^b).

Definition 4. (Decision Bilinear Diffie-Hellman (DBDH), Shao et al, 2009). Randomly choose $a,b,c\in Z_q^*,R\in G_2$, and determine whether equation $e(g,g)^{abc}=R$ is effective by the triple couple (g,g^a,g^b,g^c,R).

Definition 5. (Decisional Linear (D-Linear), Lewko and Sahai, 2010). Randomly choose generator g,f,v of group G with q order and random select element $a,b\in Z_q,R\in G$, and assess whether $v^{a+b}=R$ is effective by (g,f,v,g^a,g^b,R).

Definition 6. (Indistinguishability under Chosen Ciphertext Attack (IND-CCA), Mihir and Dennis, 2015). The process among challenger and opponent is expressed as five steps:

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

(2) The opponent can decrypt part of the ciphertext and return the result to the challenger for some decryption queries.

(3) The opponent chooses plaintext M_0 and M_1 and transmits them to the challenger. Based on the fair coin $b\{0,1\}$, the challenger chooses to encrypt M_b, obtains ciphertext C^* and transmits it to the opponent.

(4) In addition to ciphertext C^*, the opponent can continue to ask the challenger for decryption operation.

(5) The challenger must reply 1 or 0 (expressed as b') as a ciphertext guess. If $b'=b$, the opponent gains the game. The advantage of the opponent in the game can be expressed as $\Pr[b'=b]-1/2$. If the opponent has the advantage of probability polynomial time, which cannot be disregarded in this game, the encryption scheme has IND-CCA security (Mihir and Dennis, 2015). For the convenience of reading this article, we give some important symbols in Table 3.

Table 3. Related symbols and meanings

Symbol	Meanings	Symbol	Meanings
G_i	Operation in set, g is a generator of G_1, $i=1,2$	Pub	Public parameter
C_e	e denotes bilinear pairing	n	Number of attributes in system
$\Gamma_{\omega*}$	Access policy	R	Attribute revocation information
Γ	Attribute set	T	Accountability list
MK	Master key	A_u	Attributes of user u
λ	Security parameter	SK	Private key
ω	Keyword	q	Prime number
I	Index	id	User's identity
$D(\omega)$	File identifier	$\|G\|$	Element size of G
K	Key	A	Access structure
PK	Public key	$\|A\|$	Access structure size of A
CT	Ciphertext	l	Size of keyword set
T_ω	Trapdoor	D	Plaintext information

4.1.3. Several types of ABE

Presently, three types of ABES exist: basic ABE (Amit and Brent, 2005), key-policy attribute-based encryption (KP-ABE, Fig. 12) (Goyal and Pandey, 2006) and ciphertext-policy attribute-based encryption (CP-ABE, Fig. 13) (Chen and Hui, 2014).

The basic ABE mechanism has four algorithms (Susan and Brent, 2013): Setup, Extract, Encrypt and Decrypt. During

initialization, the system runs according to the public parameters and generates two groups G_1, G_2 by prime number q and bilinear pairs $e: G_1 \times G_1 \to G_2$, and d is the threshold parameter.

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

(2) KeyGen: The authorize institute generates the private key SK of user u and selects polynomial p with degree $(d-1)$. If $p(0) = y$, the private key SK is $\{D_i = g^{p(i)/t_i}\}_{\forall i \in A_C}$.

(3) Encrypt: The sender executes encryption with A_C and randomly selects $s \in Z_q$, and the 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 $|A_u \cap A_C| > d$, the receiver chooses d number of attributes. If $i \in A_u \cap A_C$ and calculates $e(E_i, D_i) = e(g,g) p(i) s$, $M = E / Y^s$ when $Y^s = e(g,g)^{p(0)s} = e(g,g)^{ys}$ with the Lagrange interpolation polynomial.

In an ABE system, decryption is possible only if the set of key attributes of a user matches the attributes of the ciphertext. KP-ABE: As shown in Fig. 13, a user's keys adopt a tree structure to describe the access policy A_{u-KP}, and the set of leaf nodes of a tree is A_u. Ciphertext is related to the attribute set A_C. When A_C satisfies A_{u-KP}, users can decrypt ciphertext.

The differences between KP-ABE and the basic ABE mechanism are the KeyGen and Decrypt algorithms. The KeyGen algorithm employs a secret sharing mechanism and adopts a top-down method to define the polynomial p_x, whose number of times is less than the threshold value of the node x.

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

The decryption algorithm decrypts each node by a recursive process from bottom to top and obtains the secret value that is needed to recover plaintext. In Fig. 13, A_C satisfies the policy A_{u-KP}, S is $\{AND\}$ in the decryption tree, and the ciphertext adopts a tree structure to describe the access policy A_{u-KP} and achieve relevant policies by the sender.

In CP-ABE, the user's key is related to the attribute set A_C. When A_u satisfies A_{u-CP}, the user can decrypt the ciphertext, and the lengths of PK and MK are independent of the number of system attributes. In the encryption algorithm, the implementation of an access tree is similar to the KeyGen algorithm of KP-ABE, and the leaf node corresponds to the ciphertext component E_i. In Fig. 14, A_u satisfies A_{u-CP}, and the set of internal nodes s in the tree is decrypted $\{\text{or}, 2\text{-of-}3, \text{AND}\}$.

In ABE, the access policy is associated with the password tree, and the decryption key is bound by a set of describable attributes (Susan and Brent, 2013). When the decryption party has a matching policy, the decryption key can be obtained. The specific contents and details of the three ABE schemes are quite different (Qin and Wu 2012, Bethencourt and Saha 2007). Please refer to Tables 4 and 5 for the similarities, differences and processes.

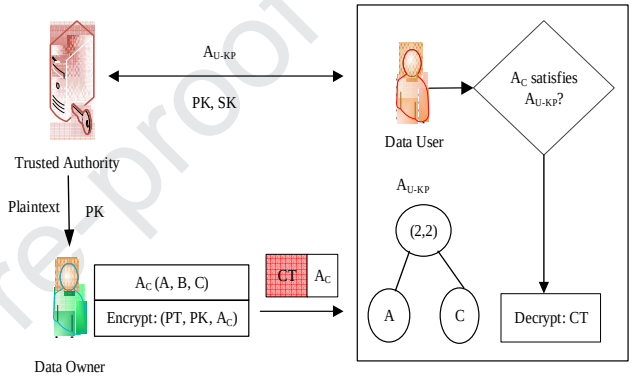


Fig. 13. KP-ABE mechanism

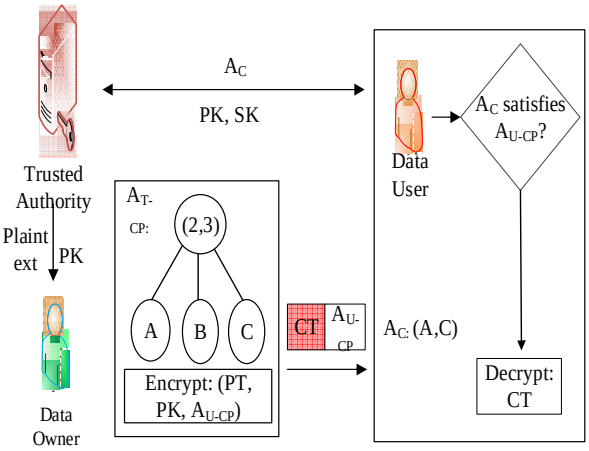


Fig. 14. CP-ABE mechanism

Table 4. Process step of KP-ABE and CP-ABE

		KP-ABE	CP-ABE
$Setup(\lambda, U)$	Input	Safe parameters	Safe parameters
		Attribute Space	Attribute Space
		User Space	User Space
	Output	Public key PK	Public key PK
$Encrypt(PK, M, A)$	Input	Master key MK	Master key MK
		Public key PK	Public key PK
		Plaintext M	Plaintext M
		Attribute Set γ	Access structure A

	Output	Ciphertext CT	Ciphertext CT
$KeyGen(MK,S)$	Input	Master key PK	Master key PK
		Access structure A	Attribute Set γ
		Public key PK	NA
	Output	Decrypt Key K	Private Key SK
$Decrypt(PK,CT,SK)$	Input	Public key PK	Public key PK
		Ciphertext CT	Ciphertext CT
		Decrypt Key K	Private Key SK
	Output	Plaintext M	Plaintext M

Table 5. Contrast cost of basic ABE, KP-ABE and CP-ABE

System	Ciphertext	Private key	Encrypt	Decrypt	Policy
Basic ABE	$\|A_C\|L_{G_1}+L_{G_2}$	$\|A_C\|L_{G_1}$	$\|A_C\|G_1+2G_2$	dC_e+2dG_2	Threshold
KP-ABE	$\|A_C\|L_{G_1}+L_{G_2}$	$\|A_u\|L_{G_1}$	$\|A_C\|G_1+2G_2$	$\|A_C\|C_e+2\|S\|G_2$	Threshold, AND, OR
CP-ABE	$(2\|A_C\|+1)L_{G_1}+L_{G_2}$	$(2\|A_u\|+1)L_{G_1}$	$\|A_C\|G_1+2G_2$	$2\|A_u\|C_e+(2\|S\|+2)G_2$	Threshold, AND, OR

4.2 Fine grain

ABE integrates flexible access control with encryption functionality; every file can be encrypted with a flexible access policy. Fig. 15 presents the basic process of ABE.

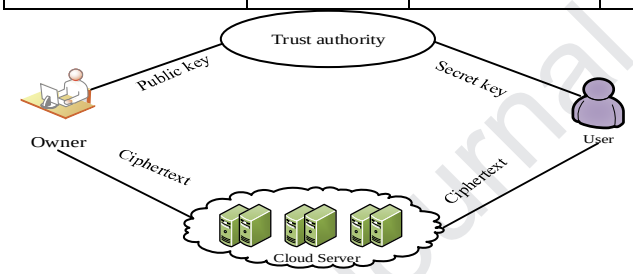


Fig. 15. The framework of attribute-based encryption

Li and Huang (2014) proposed a new security outsourcing ABE system, which can delegate many operations to a third party and substantially reduce the burden. Zhang and Ma (2017) proposed an ABE scheme for completely outsourcing ciphertext policy, which realized the generation, encryption and decryption of an outsourcing key and optimized the communication cost.

Scheme	KeyGen	Enc.user	KeyGen.user	Dec.user for CT	Dec.user for RCT
(Li and Huang, 2014)	$3Exp$	$(3+l)Exp+1P$	-	$1Exp$	-
(Zhang and Ma,2017)	0	$1Exp$	-	$1Exp$	-
(Shao and Lu, 2015)	$(3+4y)Exp$	$0Exp$	$0Exp$	$(2\|I\|+1)Exp+(2+3\|I\|)P$	$(2\|I\|+1)Exp+(3+3\|I\|)P$
(Ma and Zhang,2018)	0	0	0	$1Exp$	$2Exp+1P$

Table 6. Contrast of several fine-grained access control scheme

Shao and Lu (2015) proposed a new cloud computing data sharing protocol, which employed a new encryption primitive online /offline attribute agent re-encryption and key conversion technology. Ma and Zhang (2018) proposed a novel fine-grained access control model and data sharing mechanism, in which both the sender and the receiver did not have complex computing, and optimized the communication cost. The contrasts of these contents are shown in Table 6.

4.3. Multi-authority attribute based encryption

In the ABE mechanism, many attributes exist in the encryption process, and each attribute of a user needs to obtain a private key (Han and Mu, 2015), which requires multiple permission centers (Fig. 16). Each attribute generates an encrypted private key to prevent the authority center from stealing the private key, which effectively ensures data privacy security.

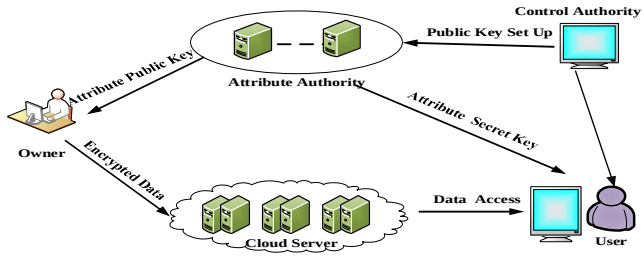


Fig. 16 Multi-authority attribute encryption (MA-ABE)

Table 7. Storage contrast of several multi-authority schemes

Scheme	Decryption	Ciphertext	Sign encryption	Decryption (user side)
(Han and Mu, 2015)	$(6N+U^d_{\max})\|G\|$	$(3N+2Nl_{e,\max})\|G\|+\|G_T\|$	$NT^e_{G_T}+(3N+3Nle,\max)T^e_G$	$(4N+2Nle,\max)T^p+Nle,\max T^e_{G_T}$
(Jiang and Wu, 2016)	$(2+6N+U^d_{\max})\|G\|+N\|G_T\|$	$(2+3Nl_{e,\max})\|G\|+\|G_T\|$	$2NT^e_{G_T}+(3+N+4Nle,\max)T^e_G$	$T^e_{G_T}$
(Lewko et al, 2011)	$U^d_{\max}\|G\|$	$(1+Nl_{e,\max})\|G_T\|+2Nl_{e,\max}\|G\|$	$3Nle,\max T^e_G+(1+2Nle,\max)T^e_{GT}$	$2Nle,\max T^p+Nle,\max T^e_{G_T}$

(Ruj et al, 2014)	$U^d_{\max}\|G\|$	$(1+Nl_{e,\max})\|G_T\|+(2+2Nl_{e,\max}+2Nl_{s,\max})\|G\|$	$3Nle,\max T^e_G+(1+2Nle,\max)T^e_{G_T}$	$2Nle,\max T^p$
(Sourya and. Ruj, 2017)	$(1+U^d_{\max}\|G\|)\|G\|$	$(3Nl_{e,\max}+1)\|G_T\|+4Nl_{e,\max}\|G\|$	$5Nle,\max T^e_G+(1+2Nle,\max)T^e_{G_T}$	$2T^e_{G_T}$
(Yang and Jia, 2013)	$(2N+U^d_{\max}\|G\|)\|G\|$	$(2+3Nl_{e,\max})\|G\|+\|G_T\|$	$NT^e_{G_T}+(1+5Nle,\max)T^e_G$	$T^e_{G_T}$
(XU and TAN, 2018)	$(9N+U^d_{\max})\|G\|$	$\|G_T\|+(4N+3Nl_{e,\max}+Nl_{s,\max})\|G\|$	$NT^e_{G_T}+(4N+5Nle,\max)T^e_G$	$T^p++T^e_{G_T}+(3N+3Nle,\max)T^e_G$

(Han and Mu 2015, Jiang and Wu 2016) proposed a decentralized CP-ABE to protect the privacy of users, in which each permission can work independently without any collaboration to initialize the system and deliver the key to users. Jiang and Wu (2016) constructed a secure data sharing scheme, which realized fine-grained access control and efficient decryption, and supported immediate revocation of user attributes (XU and TAN, 2018). Lewko and Waters (2011) proposed an encryption system that is based on multi-authority, in which any party can be an authority and no global coordination is needed except for creating a set of initial public reference parameters. Ruj and Stojmenovic (2014) proposed a distributed access control scheme in the cloud storage, which prevented replay attacks and supported creation and modification of cloud data (Sourya and. Ruj, 2017). The contrasting results of several articles are shown in Table 7.

4.4. Revocation mechanism

Because each attribute in ABE can be shared by multiple users, the revocation of any attribute may affect other users with the same attribute in the system. Therefore, how to effectively revoke attributes is an important and challenging problem in an ABE scheme (Boldyreva and Goyal, 2008).

In ABE, the ciphertext is associated with an assertion $(\Gamma, term)$, where Γ represents the attribute set, and Φ represents the non-empty subset of the Γ satisfying $term$. Assume that ω is the attribute set of the decryptor who can successfully decrypt the ciphertext, only if $\omega' \in \Phi$ exists to ensure that $\omega' \subseteq \omega$.

The CP-ABE scheme involves three entities—system center, attribute authority and user—which consist of the following six algorithms (Qin and Zhao, 2017).

(1) $Setup(1^\lambda) \to (PK, MK)$: The probabilistic random algorithm is run by the system center, which inputs the security parameter 1^λ, output public key PK and the master key MK;

(2) $KeyGen(ID, \omega, MK) \to SK_{ID,\omega}$: The probabilistic random algorithm is run by the attribute authority, which inputs MK, user's identity ID and attribute set ω and outputs the private key $SK_{ID,\omega}$;

(3) $Encrypt(\Gamma_{\omega^*}, D, R, PK) \to CT$: The probabilistic random algorithm is run by the data owner, which inputs the public key PK, plaintext message D, access policy Γ_{ω^*} and attribute revocation information R and outputs the ciphertext CT.

(4) $\mathrm{Re}\,Encrypt(\Gamma_{\omega^*}, D, R, PK) \to CT$: The probabilistic random algorithm is run by the system center, which inputs the public key PK, ciphertext CT, access policy Γ_{ω^*} and attribute revocation information R and outputs the new ciphertext CT.

(5) $Decrypt(\Gamma_{\omega^*}, SK_{ID,\omega}, CT, R) \to D$: The deterministic algorithm is run by the decryptor, which inputs the private key $SK_{ID,\omega}$, ciphertext CT of the policy Γ_{ω^*}, and the attribute revocation information R. If $\Gamma_{\omega^*}(\omega) = 1$, and $SK_{ID,\omega}$ does not involve the revocation event in R, then output the plaintext message D; otherwise, output the error symbol $\perp$.

(6) $\mathrm{Re}\,vocation(MK, ID_k, \lambda_k, attri(j)) \to R$: The deterministic algorithm is run by the attribute authority, which inputs the attribute $attr(j)$ and user ID_k and outputs the revocation information R.

Based on the idea of the fuzzy IBE primitive and binary tree data structure, Boldyreva and Goyal (2008) proposed an IBE scheme, which can significantly improve the key update efficiency of the trusted party. Qin and Zhao (2017) established a server assisted revocable ABE and maintained the features of attribute revocation, short ciphertext and fast decryption. Cui and Deng (2016) proposed a revocable ABE concept, in which the workload of user revocation can be delegated to a server, and each data user only needed to store a fixed size key, which greatly reduced the operating burden of the client. Based on the direct and indirect revocation methods, Attrapadung and Imai (2009) proposed a mixed and revocable ABE scheme, which enabled the sender to dynamically choose whether to use a direct revocation or indirect revocation mode.

Sahai and Seyalioglu (2012) proposed a new method to revoke the stored data, which enables the storage server to update the stored ciphertext to disqualify the revoked user from accessing the encrypted data. Yang and Liu (2015) proposed an extended proxy assisted method, which bound the private key to the data decryption operation and effectively prevented collusion. Ma and Zhang (2015) proposed a practical revocable access control mechanism, which not only realized efficient fine-grained access control but also provided fast and robust user revocation. Several revocation mechanisms are presented in Table 8.

Table 8. Contrast results of several revocation schemes

4.5. Trace mechanism

In the ABE mechanism, improving the security of attribute management and tracing the direction of each attribute is necessary. According to different requirements of the algorithm, traceability research can be divided into a white box and a black box (Liu and Cao 2013). The white box uses a key to track the user's attribute. The black box mechanism provides ciphertext for the device and obtains the decrypted plaintext to ensure that at least one user can be traced.

An online/offline traceable mechanism includes six algorithms (Liu and Cao 2013): Setup, KeyGen, offline encryption and online encryption, decryption and trace.

1) $Setup(\lambda,U)$. The algorithm inputs the security parameter λ and attribute set U and outputs the public key PK and the master key MK. The algorithm initializes the accountability list $T=\varnothing$.

2) $KeyGen(MK,PK,id,S)$. The algorithm inputs the master key MK, public key PK, user's identity id and attribute set $S\subseteq U$, outputs the user's private key SK_{id} of (id,S), and adds id to the list T.

3) $Offline-Encrypt(PK)$. The algorithm inputs the public key PK and outputs the indirect ciphertext IT.

4) $Onine-Encrypt(PK,IT,(M,\rho))$. The algorithm inputs the public key PK, indirect ciphertext IT and an access policy (M,ρ) and outputs the session key key and ciphertext CT.

5) $Decrypt(SK_{id,s},PK,CT)$. The algorithm inputs the public key PK, private key $SK_{id,S}$ of the attribute set S, and ciphertext CT of the access policy (M,ρ). If the attribute set S does not satisfy the access policy (M,ρ), and the output $\perp$ indicates that the decryption fails; otherwise, the output is the session key key.

6) $Trace(PK,T,SK)$. The algorithm inputs the public key PK, accountability list T and private key SK. First, the algorithm checks whether SK is a reasonable private key to determine whether accountability should be pursued. If SK is a reasonable private key, the corresponding identity id of SK is output; otherwise, the symbol $\wedge$ indicates that SK is not a reasonable private key.

Liu and Cao (2013) proposed a new CP-ABE to support the representation policy in any monotonic access structure, which improved the traceability and expression without compromising security or performance. Liu and Wong (2013) can identify the users whose keys have been used to establish the decryption device from multiple keys and the superset attribute but must be utilized to build the underlying decryption device. Ning and Cao (2014) presented a practical CP-ABE system that supports white box tracking, which is suitable for commercial applications. The scheme included three advantages: (1) the number of attributes is not polynomial bounded; (2) it can track malicious users who leak the decryption key; and (3) the storage cost of the trace mechanism is constant (Ning and Dong, 2015). Ning and Cao (2018) proposed two non-interactive traitor tracing commitments and constructed a fully secure and traceable cloud storage service CP-ABE system, which can effectively capture users with compromised access credentials. The relevant results of the trace schemes are shown in Table 9.

Scheme	Public key	Private key	Ciphertext size	Pairing	Storage cost
(Liu and Cao, 2013)	$\|u\|+4$	$\|s\|+4$	$2l+3$	$2\|I\|+1$	N
(Liu and Wong, 2013)	$\|u\|+3+4\sqrt{N}$	$\|s\|+4$	$2l+17\sqrt{N}$	$2\|I\|+10$	$\sqrt{N}$
Ning and Cao (2014)	7	$2\|s\|+4$	$3l+3$	$3\|I\|+1$	$INS(t,n)$
(Ning and Dong, 2015)	7	$2\|s\|+4$	$3l+3$	$3\|I\|+1$	$INS(t,n)$
(Ning and Cao, 2018)	$\|u\|+5$	$\|s\|+7$	$2l+4$	$2\|I\|+2$	0

Table 9. Contrast of several trace schemes

$|u|$ is the size of the attribute universe, $|s|$ is the size of the attribute set of a private key, l is the size of an access policy, and $|I|$ is the number of attributes.

	(Boldyreva and Goyal, 2008)	(Qin and Zhao, 2017)	(Cui and Deng, 2016)	(Attrapadung and Imai, 2009)	(Sahai and Seyalioglu, 2012)	(Yang and Liu, 2015)	(Ma and Zhang, 2015)
Rev	Indirect	Indirect/Direct	Indirect	Indirect	Indirect	Direct	Direct
ABE	KP	KP	KP	CP	CP	CP	CP
Key size	$O(R\log(\frac{N}{R}))$	$O(R\log(\frac{N}{R}))$	$O(R\log(\frac{N}{R}))$	$O(R\log(\frac{N}{R}))$	$O(R\log(\frac{N}{R}))$	–	$O(1)$
Key	$O(l\log N)$	$O(l\log N)$	$O(l\log N)$	$O(1)$	$O(1)$	$O(1)$	$O(1)$
Communication	$\|G_T\|+(2k+1)\|G\|$	$\|G_T\|+(k+1)\|G\|$	$\|G_T\|+(k+1)\\|G\|$	$2\|G_T\|$	$\|G_T\|+2\|G\|$	$2\|G_T\|$	$2\|G_T\|$
Computation	$2\|I\|E+4\|I\|P$	$3\|I\|E+4\|I\|P$	$2\|I\|E+2\|I\|P$	$1E$	$2P$	$1E$	$1E$

4.6. Proxy Re-encryption (PRE)

The calculation of encryption and decryption needs numerous hardware facilities, which will cause a great burden to personal computing. Therefore, users usually choose a third

proxy party to execute encryption and decryption. With the premise of ensuring security and safety, the attribute-based proxy re-encryption (ABPRE) scheme combines proxy re-encryption with ABE, and users can decrypt the re-encrypted ciphertext using relevant attributes (Fig. 17).

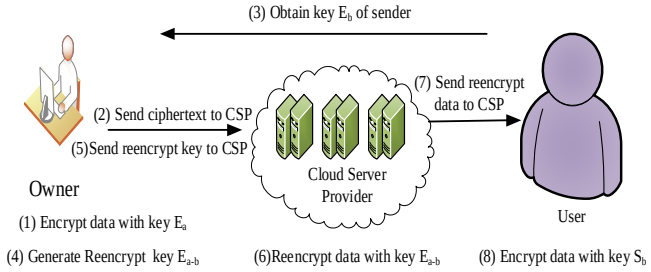


Fig. 17. Proxy re-encryption

Based on the Diffie Hellman (DDH) hypothesis, Shao and Cao (2009) proposed a non-pairing proxy re-encryption scheme, which was secure against the chosen ciphertext attack and collusion attack in the random oracle model. Lin and Lu (2016) investigated the verifiability of the re-encryption process, formalized the proxy encryption security model, proposed an authentication scheme, and gave the security proof.

Guo and Zhang (2014) defined the concept of the unforgeability of a re-encryption key to capture the previously described attacks and proposed a non-interactive security scheme, which can resist a collusion attack when forging a re-encryption key. Zhan and Wang (2019) proposed a more secure re-encryption scheme to prevent attackers from forging effective ciphertext and signatures and resist a selective ciphertext attack. The contrasts of PRE are shown in Table 10. Shao and Cao (2009) needed a constant number of pairing operations in re-encryption and decryption compared with Lin and Lu (2016), Guo and Zhang (2014) and Zhan and Wang (2019); the computation burden is substantially lower.

Table 10. Contrast of several PRE schemes

Paper	Computation cost					
	keygen	Enc1	Enc1	Re-enc	Dec1	Dec1
(Shao and Cao,2009)	$m+2e$	$2m+3e$	$2m+3e$	$e+p$	$7m+9e$	$4m+p+5e$
(Lin and Lu, 2016)	$3e$	$3m+6e+b$	$2m+8e$	$3m+5e+10b$	$3m+3b+4e$	$2m+9b+4e$
(Guo and Zhang, 2014)	$e+2p$	$3m+7e+2p$	$2m+4e+p$	$2b+4e+p$	$2m+3e+2p+4b$	$m+3b+4e+p$
(Zhan and Wang, 2019)	$3e+p$	$3m+9e+p+b$	$2m+8e$	$3m+5e+p+10b$	$4m+4e+p+5b$	$2m+9b+4e$

4.7. Hierarchical encryption

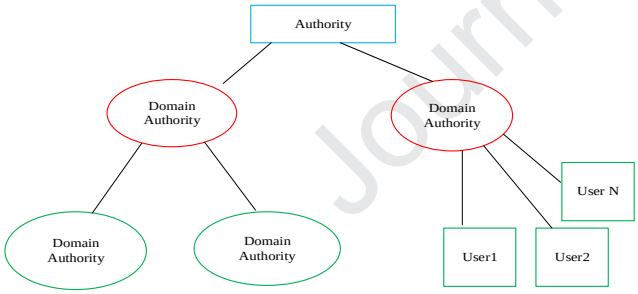


Fig. 18. Hierarchical attribute-based encryption scheme

In practical applications of a cloud computing service, such as hierarchical identity-based encryption (HIBE), hierarchical attribute-based encryption (HABE, Fig. 18) and hierarchical attribute-set-based encryption (HASBE), a hierarchical management mode is usually employed.

The HIBE is comprised of five algorithms (Okamoto and Takashima, 2012): root set-up, key extraction, delegation, encryption and decryption.

Root setup (λ): During the setup phase, the PKG takes the security parameter λ and computes the system public parameters Pub and generates the master key MK.

Key extraction (I, Pub, MK): The key extraction algorithm uses the master key MK and public parameters PP to compute the private key for identity vector I at depth j; $j \le L$; L is the maximum hierarchy depth; and the private key for I is denoted as SK_I.

Delegation (I, Pub, I', SK_I): Identity I at depth j generates the private key for identity I' at depth $j+1$ using the public parameters Pub and private key SK_I, and $j+1 \le L$. L is the maximum depth of the hierarchy; the public key for I' is denoted as $I:I'$, and the private key is $SK_{I:I'}$.

Encryption (D, Pub, I): To encrypt a message for a recipient with the identity vector I, the sender uses the public parameters Pub and public key PK to generate the ciphertext CT.

Decryption (CT, Pub, SK_I): The intended recipient with the identity vector I decrypted the ciphertext CT to obtain the message D by using the public parameters Pub and private key SK_I.

4.7.1. HIBE

The identity-based encryption (IBE) system is a simple, certificate-free public key infrastructure model. HIBE improves the scalability of IBE by sharing the workload of PKG, which can be deployed in cloud computing, pervasive computing systems, and wireless sensor networks to provide access right.

Okamoto and Takashima (2011) proposed two schemes of zero inner product encryption: the first schemeone is a full-attribute hidden scheme with a constant size key, and the

second scheme is a layered scheme with a constant size ciphertext. Ducas et al (2010) discussed how to use asymmetric pairs to transform a large class of IBE and HIBE structures into anonymous IBE and HIBE systems. Okamoto and Takashima (2012) proposed a hierarchical inner product encryption scheme, which can realize a shorter public key and add a new form of ciphertext and key. Lee and Park (2015) proposed an efficient anonymous HIBE scheme with short ciphertext in prime order bilinear groups and gave an effective reduction. The contrasts of the HIBE schemes are shown in Table 11.

Table 11. Contrast of several HIBE schemes

	(Wang and Zhou, 2016)	(Li and Chen, 2019)
Encryption time	$(k+2\mid A_{le}\mid)E_{G_0}+(2j\mid A_{nt}\mid+k)E_{G_T}+\mid A_{le}\mid\Delta_{H_1}$ $+\ j\mid A_{nt}\mid\Delta_{H_2}+(k+j\mid A_{nt}\mid)M_{G_T}$	$(k+2\mid A_{le}\mid)E_{G_0}+(2j\mid A_{nt}\mid+k)E_{G_T}+\mid A_{le}\mid\Delta_{H_1}$ $+\ j\mid A_{nt}\mid\Delta_{H_2}+(k+j\mid A_{nt}\mid)M_{G_T}$
Decryption time	$(k+2\mid A_{le}\mid)e+\mid A_{le}\mid E_{G_T}+\mid A_{le}\mid\Delta_{H_1}$ $+\ j\mid A_{nt}\mid\Delta_{H_2}+(\mid A_{le}\mid+2k+j\mid A_{nt}\mid)M_{G_T}$	$(k+2\mid A_{le}\mid)e+(k+\mid A_{le}\mid)E_{G_T}+k\Delta_{H_1}+\mid A_{le}\mid\Delta_{H_2}$ $+\ j\mid A_{nt}\mid\Delta_{H_3}+(\mid A_{le}\mid+k+j\mid A_{nt}\mid)M_{G_T}$
Size of PK	$3L_{G_0}+L_{G_T}$	$3L_{G_0}+L_{G_T}$
Size of MSK	$L_{G_0}+L_{Z_P}$	$L_{G_0}+L_{Z_P}$
Size of SK	$L_{G_0}(2\mid S\mid+1)$	$L_{G_0}(2\mid S\mid+1)$
Size of CT	$(k+2\mid A_{le}\mid)L_{G_0}+(k+j\mid A_{nt}\mid)L_{G_T}$	$(k+2\mid A_{le}\mid+j\mid A_{nt}\mid)L_{G_0}+j\mid A_{nt}\mid)L_{G_T}+kl$

4.7.2. HABE

The Hierarchical attribute-based encryption (HABE) offers fine-grained access control, scalability, and full delegation by combining HIBE and ABE. HABE works in a disjunctive clause manner and assumes that all attributes are administered by the same domain master.

Li and Yu (2019) gave the formal definition and security model of hierarchical attribute encryption (HABE) with continuous recovery capability, and proposed a scheme with continuous leak elasticity. Deng and Wu (2014) proposed a formal definition and security model of hierarchical attribute encryption (HABE) with continuous leak recovery capability. The security of the scheme is proved with the assumption of a compound order bilinear group. The contrasts of several HABE schemes are in presented in Table 12.

Table 12. Contrast of several HABE schemes

Schemes	Size of MK	Size of SK	Leakage of MK	Leakage of SK
(Li and Yu, 2019)	$3(\mid U\mid+2)\lambda$	$3(\mid S\mid+l+2)\lambda$	No	No
(Deng and Hu, 2014)	$3(\mid U\mid+2+n)\lambda$	$3\lambda(\mid S\mid+l+2+n)$	$(n-2\Lambda-1)\lambda$	$(n-2\Lambda-1)\lambda$

4.7.3. HASBE

Hierarchical attribute set based encryption (HASBE) combines an attribute set based on encryption and HIBE. HASBE has better privacy performance, flexibility and application range but the operation is more complex.

Wang and Zhou (2016) proposed an encryption scheme that is based on file hierarchy, integrated the hierarchical access structure into a single access structure, and then utilized the integrated access structure to encrypt the hierarchical files. Li and Chen (2019) proposed the efficient hierarchy CP-ABE, which can encrypt multiple files at the same access level, especially for large organizations. The contrast results of these several HASBE schemes are shown in Table 13.

Table 13. Contrast of several HASBE schemes

4.8. Discussion and analysis of ABE

Attribute encryption algorithm is particularly suitable for the distributed architecture of cloud computing, which can reduce the cost of network communication and facilitate the combination with other security technologies. We summarize the characteristics of several ABE models in Table 14.

Scheme	Reduction loss	Public prime	Secret key	Ciphertext
(Okamoto and Takashima,2011)	$\Omega(q)$	$O(l^4\lambda)$	$O(l^4\lambda)$	$133k+k_T$
(Ducas et al,2010)	$\Omega(2^{\lambda l})$	$O(l^4\lambda)$	$O(l^4\lambda)$	$3k+k_T$
(Okamoto and Takashima, 2012)	$\Omega(lq)$	$O(l^2\lambda)$	$O(l^2\lambda)$	$O(l\lambda)$
(Lee and Park, 2015)	$\Omega(q)$	$O(l\lambda)$	$O(l\lambda)$	$6k+k_T$

Table 14. Contrast of several ABE schemes

The ABE mechanism employs an access structure to express the access policy, and the flexibility of the policy will increase the complexity of access structure. Large-scale distributed applications need an ABE mechanism to support a multi-authorization center to satisfy the needs of scalability and fault tolerance. These factors introduce challenges to ABE research, including the following aspects:

1 Designing the access structure of the CP-ABE mechanism is difficult. The public key of the CP-ABE system is generated by the authority; the access structure is designed by the encryptor and the decryption is controlled by the authority. Therefore, in CP-ABE, the complexity of the access structure increases the complexity of the public key and limits the design of the access structure.

2 Attribute key revocation is a heavy burden. In ABE, the user key is related to the attribute, and the dynamic change of the system often causes attribute invalidation. Therefore, the revocation of ABE becomes the research focus.

3 Key abuse of ABE. When a pirated key exists, determining whether users or authorized institutions have disclosed the private keys is difficult. Preventing and defining the responsibility of the private key is difficult, which causes a key abuse problem in ABE.

4 Trust of authorized institutions. In an ABE system, an authorized organization may cause security risks to the system. Once the authorized organization is destroyed, the attacker can obtain the key of any user and decrypt all ciphertext.

5. Searchable encryption

Data in a cloud service often exists in the form of ciphertext. How to ensure the privacy security of a cloud service without reducing the efficiency of a cloud service is an important issue. Because searchable encryption (SE) technology can provide keyword-based retrieval of ciphertext, it is very suitable for the protection of cloud privacy data (Kamara and Papamanthou, 2012). As an important network security method, both symmetric and asymmetric searchable encryption can be combined with other technologies to solve various forms of keyword retrieval problems in various scenarios (Fig. 19). Currently, many research results have been achieved.

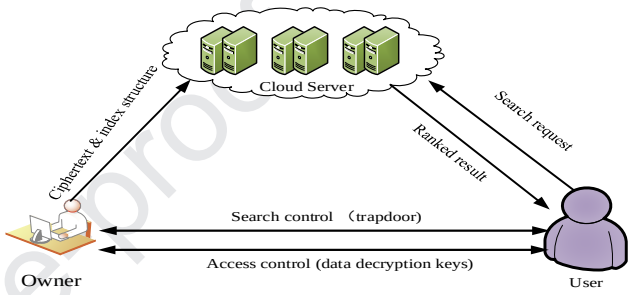


Fig. 19. Process of searchable encryption

Algorithm	Fine-grained	Computation overhead	Revocation efficiency	Efficiency	Collision resistance	Association attributes	Access policy
ABE	Poor	Common	Common	Common	Common	Cipher	Key
KP-ABE	Poor	Good	Poor	Common	Common	Cipher	Key
CP-ABE	Common	Common	Poor	Common	Good	Key	Cipher
CCP-CABE	Poor	Poor	Good	Good	Good	Key	Cipher
MA-ABE	Common	Good	Common	Good	Common	Cipher / key	Cipher / key
PRE	Poor	Poor	Common	Good	Common	Cipher/ key	Cipher / key
HIBE	Poor	Good	Good	Good	Good	Key	Cipher
HABE	Good	Common	Common	Good	Good	Key	Cipher
HASBE	Good	Common	Common	Good	Good	Key	Cipher

5 Research on a revocable CP-ABE mechanism that can identify user responsibility. Current research has realized the flexible CP-ABE mechanism with the standard assumption. However, this mechanism does not solve the responsibility identification of a user.

6 Hierarchical ABE. In a practical application, a hierarchical relationship between authorized institutions and attributes exist; so an investigation of hierarchical ABE is necessary.

7 The applicability and practicability of ABE: Due to the efficiency shortcomings, proposing a more practical ABE scheme in a cloud environment by combining PRE, anonymous authentication, access control, keyword search and other technical means has great significance.

8 Dual policy ABE. The policies in KP - ABE and CP - ABE can only control access to a user key or ciphertext. Improving the efficiency and flexibility of the double policy ABE mechanism, which can effectively protect privacy information, is an important direction.

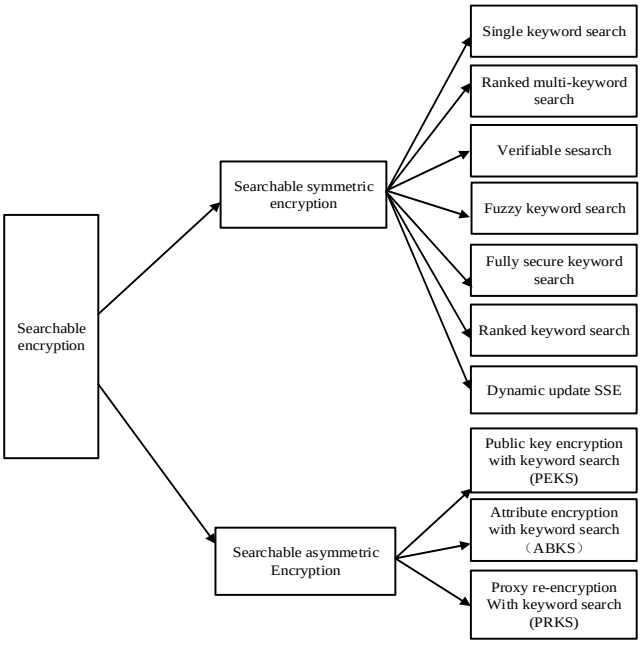


Fig. 20. Categories of searchable encryption

Searchable encryption schemes can be divided into two main types (Fig. 20): searchable symmetric encryption (SSE) and searchable asymmetric encryption (SAE), which mainly includes four algorithms: setup, token, index and query (Kamara and Papamanthou, 2012).

(1) Setup: In the SAE, the algorithm will generate the public key and private key according to the input security parameter; in the SSE, the algorithm will generate some private keys, such as the key of pseudo-random function.

(2) Trapdoor: According to the keywords of users, the algorithm generates the corresponding search credentials. The executor of algorithm is mainly determined by the application scenario and can be executed by the data owner, user or authority.

(3) Index: In this algorithm, the data owner will select the corresponding keyword set according to the file and use the searchable encryption mechanism to build the index table. In SAE, the data owner encrypts the file with the public key; in SSE, the data owner encrypts the key set with the symmetric key.

(4) Query: The algorithm is performed by the server. The server considers the search voucher and index table as input to calculate the protocol preset. The algorithm determines whether the file satisfies the search request by determining whether the output result is the same as the preset result. The server returns the search result.

5.1. Searchable symmetric encryption (SSE)

In the dictionary $D=\{\omega_1,\omega_2,\cdots\omega_d\}$, a symmetric searchable encryption algorithm can be described as a quintuple (Kamara and Papamanthou, 2013):

$SSE=(KeyGen, Encrypt, Trapdoor, Search, Decrypt)$

1) $K=KeyGen(\lambda)$: Input the security parameter λ, and output the key K.

2) $(I,C)=Encrypt(K,D)$: Input the symmetric key K and plaintext file set $D=(D_1,D_2,\cdots,D_n)$, $D_i\in 2^{\Delta}$, and the output index I and ciphertext file set $C=(C_1,C_2,\cdots C_n)$. If the SSE scheme is without index construction, $I=\varnothing$.

3) $T_\omega=Trapdoor(K,\omega)$: Input the symmetric key K and keyword ω and output the trapdoor T_ω;

4) $D(\omega)=Search(I,T_\omega)$: Input the index I and trapdoor T_ω and output the set $D(\omega)$, which is composed of the identifier of file ω;

5) $D_i=Decrypt(K,C_i)$: Input the symmetric key K and keyword ω_i, and output the corresponding plaintext file D_i.

If symmetric searchable encryption SSE is correct, then for $\forall n\in N,\omega\in\Delta,D=(D_1,D_2,\cdots D_n)$, $KeyGen(\lambda)$ and output K and (I,C) of $Encrypt(K,D)$, $Search(I,Trapdoor(K,\omega))=D(\omega)$ and $D_i=Decrypt(K,C_i)$, $C_i\in C,i=1,2,\cdots n$ exists.

Therefore, the symmetric searchable encryption process is described as follows: in the encryption process, the user executes the $KeyGen$ algorithm to generate the symmetric key K, encrypts plaintext D with K, and uploads the ciphertext to the server. In the retrieval process, the user executes the $Trapdoor$ algorithm to generate the trap T_ω of the keyword ω. The server uses T_ω to retrieve the file identifier $D(\omega)$ and extracts the secret according to $D(\omega)$. The user decrypts the returned files with K to obtain the target file.

5.1.1. Single-keyword search

Because of its simple and fast operation, a single keyword search is a common method of ciphertext retrieval.

To resist an attack of adaptive keyword selection, Kamara and Papamanthou (2012) proposed a dynamic SSE scheme, which not only supports dynamic update but also satisfies the sub-linear search time. Kamara and Papamanthou (2013) employed the data structure of a red black tree to search ciphertext, which did not need to access a series of memory locations and can be applied in multi-core architecture. Wang and Cao (2012) proposed a secure and efficient ranking keyword search method that is based on outsourcing cloud data. The scheme can calculate correlation scores but only supports a static single keyword search.

5.1.2. Ranked multi-keyword search

Due to the different frequencies of keywords, the keyword search scheme improves the applicability of the system based on the feedback results of the relevant ranking system.

Fu and Sun (2015) proposed a practical, efficient and flexible searchable encryption scheme, which supports both a multi-keyword ordered search and a parallel search. Xia and Wang (2015) proposed a secure, efficient and dynamic search scheme, which constructed a special keyword-balanced

binary tree as an index, and a greedy depth first search algorithm to achieve better efficiency.

Using semantic ontology, Fu and Ren (2016) investigated a multi-keyword search, and the user interest is expressed intelligently by the scoring mechanism. Based on the keyword weight, Fu and Wu (2016) proposed an efficient multi-keyword search scheme, developed a new keyword conversion method, and corrected several spelling errors.

5.1.3. Conjunctive keyword search

To overcome the shortcomings of a single keyword and multi-keyword search, a conjunctive keyword search scheme is proposed.

To improve the efficiency of searching encrypted data, Bösch and Brinkman (2011) provided a wildcard search scheme by the pseudo-random functions and filters. Cash et al. (2013) designed a searchable symmetric encryption protocol, which supported a joint search of symmetric encrypted data and a general Boolean query and provided a realistic and practical trade-off solution between performance and privacy in the databases. For extensive application, Jarecki and Jutla (2013) proposed a model to support Boolean queries and resist hostile non-collusive servers and arbitrary malicious clients.

5.1.4. Fuzzy keyword search

Based on the similar semantics of keywords, a fuzzy keyword search provides users with possible files, protects users' privacy information, and improves the efficiency of each search.

Li and Wang (2014) formalized the fuzzy keyword search problem of encrypted cloud data, effectively search the fuzzy keyword of encrypted cloud data, and greatly improve the availability of the system by returning matching files. Wang et al. (2013) proposed a new verifiable fuzzy keyword search scheme based on a symbol tree, which not only supports fuzzy keyword search but also has verifiability. Zhu and Liu (2017) proposed a dynamic fuzzy keyword search scheme to provide a secure fuzzy keyword search and verified the authenticity of the search results. To reduce the computation and storage space, GE and YU (2018) proposed an index vector for each fuzzy key set to verify the authenticity of the ciphertext. The results of these schemes are listed in Table 15.

Table 15. Efficiency contrast of fuzzy keyword search

Properties	(Li and Wang, 2014)	(Wang et al.,2013)	(Zhu and Liu, 2017)	(GE and YU, 2018)
Index building cost	$O(nM)$	$O(nM)$	$O(m)$	$O(n)$
Trapdoor generation cost	$O(M)$	$O(M)$	$O(M)$	$O(1)$
Search cost	$O(M'h)$	$O(M'h)$	$O(M'h)$	$O(m)$
verification	—	$O(1)$	$O(1)$	$O(1)$

5.1.5. Verifiable searchable

Some SSE schemes also provide additional functions, such as detecting the behaviors of malicious servers (i.e., verifiability) and allowing the update of documents on servers. Kaoru and Yasuhiro (2013) showed you how to update (modify, delete, and add) documents in a verifiable way to enable the client to detect any cheating behavior of the malicious server. Chai and Gong (2012) proposed a verifiable SSE scheme, which effectively solves the conflict between data availability and data privacy. Liu and Yang (2018) proposed a multi-user verifiable scheme, which implemented the ideal features of verifiable SSE, that enables multiple users to perform a search. The contrasts of these schemes are listed in Table 16.

Table 16. Performance contrast

	Trapdoor	Index	Search	Verifiability
(Kaoru et al, 2013)	$O(1)$	$O(m)$	$O(1)$	$O(n)$
(Chai and Gong,2012)	$O(1)$	$O(\lvert\varepsilon\rvert^{l})$	$O(1)$	$O(R(w))+$
(Liu and Yang, 2018)	$O(1)$	$O(m^2)$	$O(1)$	$O(n)$

m is the number of all keywords, $R(w)$ is the number of documents that contain the keyword w, n is the number of stored documents, l is the word length of the keyword in the current search, and $|\varepsilon|$ is the size of the attribute set whose characters are organized to construct each word.

5.1.6. Fully secure keyword search

SSE has powerful and rich functions; it is always plagued by information disclosure. Recent literature has highlighted that the basic requirement of SSE is to allow update operations to disclose privacy.

After the formal definition of different types of backward privacy, Garg and Mohassel (2016) proposed a scheme to achieve both forward privacy and backward privacy and used some advanced encryption primitives for fine-grained control (Bost and Minaudy, 2017). From the point of view of computation and communication, Kim and Kim (2017) designed and implemented a forward security scheme with optimal search and update complexity, which can utilize both a reverse index and a forward index and greatly improve efficiency. Li and Huang (2019) extended the definition of forward privacy, proposed the concept of "forward search privacy", and developed a new SSE scheme by the concept of forward privacy. The contrasts of these SSE schemes are shown in Table 17.

Table 17. Contrast of several SSE schemes

K is the number of sub keywords, m is the number of sub keywords, D is the number of the documents in the database. n_w is the search result of keyword w, a_w is the total number of entries of keyword w, and d_w is the number of the cleared entries of w.

5.1.7. Dynamic update

Due to the dynamics of application in a search encryption scheme, when deleting or adding new ciphertext, data must be updated in time.

Emil and Charalampos (2014) proposed a dynamic searchable symmetric encryption scheme (DSSE), which can achieve small leakage and high efficiency, support a sub-linear time update in the worst case, and retain the data structure of only linear size. Using a very simple data structure, Asila and Jorge (2015) proposed a new decision support system to achieve low information disclosure and achieve an efficient and safe search/operation. Bost et al. (2016) proposed a new forward private SSE scheme, which only relied on a trapdoor arrangement. With the premise of security, it greatly improved the search efficiency. The contrasts of these DSSE schemes are listed in Table 18.

Scheme	Computation		Communication		Client storage
	Search	Update	Search	Update	
(Garg and Mohassel,2016)	$O(a_w \log N + \log^3 N)$	$O(\log^2 N)$	$O(n_w)$	$O(1)$	$O(K \log D)$
(Bost and Minaudy,2017)	$O(a_w)$	$O(1)$	$O(n_w)$	$O(1)$	$O(K \log D)$
(Kim and Kim, 2017)	$O(a_w - d_w)$	$O(1)$	$O(n_w)$	$O(1)$	$O(K \log D)$
(Li and Huang,2019)	$O(n_w)$	$O(1)$	$O(n_w)$	$O(1)$	$O(m \log D + D \log K)$

Table 18. Contrast of several DSSE schemes

The complexity is based on the keyword w or the unique keyword k. N is the total number of keyword pairs in the database, m is the number of times the queried keyword w was added to the database. n_w is the size of the search result set for the keyword w. a_w (resp. d_w) is the number of times the queried keyword w. N^+ is the total number of keyword pairs historically in the database $N^+ = \Sigma_w(a_w + d_w)$. The O hides the $\log\log N$ factors.

5.2. SAE (Searchable asymmetric encryption)

In this section, we will discuss public key encryption with keyword search (PEKS), attribute-based encryption with keyword search (ABKS), and proxy re-encryption with keyword search (PRKS) (Rhee and Park, 2010).

Paper	Data		Communication		Computation	
(Emil and Charalampos,2014)	$O(N^a), 0<a<1$	$O(N^+)$	$O(n_w + \log N^+)$	$O(\log N^+)$	$O(\min\{a_w + \log N^+, n_w \log^3 N^+\})$	$O(\log^2 N^+)$
(Asila and Jorg,2015)	$O(m+n)$	$O(m \times n)$	$O(N_w)$	$O(m \times n)$	$O(n)$	$O(m)$
(Bost et al, 2016)	$O(m)$	$O(N^+)$	$O(N_w)$	$O(k)$	$O(a_w + d_w)$	$O(k)$

5.2.1. PEKS

PEKS introduces the concept of attribute, in which users who satisfy the relevant properties can query the encrypted data. A public encryption key search algorithm consists of five polynomial time random algorithms (HU and LIU, 2019)

: Setup, KeyGen, PEKS, Trapdoor and Test:

(1) $Setup(1^\lambda) : (Pub, MK) \leftarrow Setup(1^\lambda)$, where λ is the system parameter, $Setup$ is the probability polynomial algorithm for generating the public parameter Pub and the master key MK.

(2) $KeyGen(MK, A) : \Pr iv_A \leftarrow KeyGen(MK, A)$. The key generation center KGC generates the user's private key $\Pr iv_A$ according to the access structure A and the system master key MK, where $KeyGen$ is a probability polynomial algorithm;

(3) $PEKS(Pub, \omega, \gamma) : C \leftarrow PEKS(Pub, \omega, \gamma)$. The sender encrypts the keyword ω to generate the ciphertext CT with the parameter Pub and attribute r. Only the user's attribute satisfies the access structure, who can decrypt the keyword ciphertext. $PEKS$ is the probability polynomial algorithm, which generates the ciphertext from the system public parameter Pub, keyword ω and attribute r.

(4) $Trapdoor(\Pr iv_A, \omega) : T_\omega \leftarrow Trapdoor(\Pr iv_A, \omega)$. The receiver uses the personal private key $\Pr iv_A$ to calculate the threshold value T_ω of the query key $\omega \in \{0,1\}^*$ and send it to the gateway server, $Trapdoor$ is the probability polynomial algorithm for the threshold T_ω of the private key $\Pr iv_A$ and the keyword ω.

(5) $Test(Pub, T_\omega, CT) : b \leftarrow Test(Pub, T_\omega, CT)$. In the public parameter Pub, the ciphertext $CT = PEKS(Pub, \omega', \gamma)$ of the keyword ω and the threshold $T_\omega = Trapdoor(\Pr iv_A, \omega)$ of the keyword ω. If $\omega' = \omega$, the output $b = 1$; otherwise $b = 0$, $Test$ is the probability polynomial algorithm to determine whether the CT corresponds to the ω of the threshold T_ω.

In this algorithm, $\lambda \in N$, for all attributes S and $\omega \in \{0,1\}^*$, query the same information.

Scheme	(Qiu and Liu,2017)	(Sun and Yu, 2016)	(Wan and Yu,2016)

and $\Pr[Test(Pub, Trapdoor(Priv_A, \omega), PEKS(Pub, \omega, \gamma)) = 1] = 1$.

The probability function considers all the public parameters Pub, master key MK, all the probability algorithms and the random oracle models. The key center generates the private key $Priv_A$ for the user by the algorithm $KeyGen$ according to the access structure A, and the user generates the threshold T_ω of the keyword ω by the private key $Priv_A$ and function $Trapdoor$. The server can obtain the ciphertext of the keyword ω according to the threshold T_ω.

The server uses the given threshold T_ω as the input of the algorithm $Test$ to determine whether the file contains the ciphertext of the keyword ω. Moreover, the server does not know the plaintext of the keyword ω, which hides the sensitivity of the query information. Because the key $Priv_S$ is related to the attribute, the user with the same attribute key can

Based on the existing security model, Rhee and Park (2010) introduced the concept of "trap door cannot distinguish", and constructed a secure searchable public key encryption scheme to prevent a keyword guessing attack. Fang and Susilo (2013) proposed two important security concepts: IND-CKCA and IND-KGA. The former is to capture an internal enemy, whereas the latter is to capture an external enemy.

Chen et al. (2015) and Huang and Li (2017) analyzed the weakness of public key encryption and keyword search and proposed a new public key encryption framework that is based on keyword search. The encrypted keyword can only be generated by the sender. Based on different input obfuscation, HU and LIU (2019) provided a simple contrast method to the cloud server to support the ciphertext search. The contrasts of these PEKS schemes are listed in Table 19.

Table 19. Contrast of several PEKS schemes

n denotes the number of files, and r denotes the number of the retrieving file

Scheme	Computation		Communication Cost	Functionality
	Trapdoor	Test		
(Rhee and Park, 2010)	$O(1)$	$O(n)$	$O(r)$	single
(Fang and Susilo, 2013)	$O(1)$	$O(n)$	$O(r)$	single
(Chen et al(2015)	$O(1)$	$O(n)$	$O(r)$	single
Huang and li (2017)	$O(1)$	$O(n)$	$O(r)$	single
HU and LIU (2019)	$O(1)$	$O(n)$	$O(r)$	Can extended

5.2.2. ABKS

ABKS encrypts the data by ABE. When the user's attributes satisfy the access policy, the technology enables the user to search the keywords used to encode cloud data.

Qiu and Liu (2017) proposed keyword search encryption that is based on hidden policy ciphertext. If the user's credentials cannot satisfy the access control policy of the data owner, they cannot search the encrypted data. Sun and Yu (2016) proposed a keyword search scheme, which can implement a fine-grained search and formalize the definition of security. Wan and Yu (2016) constructed an attribute encryption keyword search scheme that contains two independent attribute revocation lists. However, the calculation burden of the scheme is large. The contrasts of these ABKS schemes is presented in Tables 20 and 21.

Table 20. Contrast storage of ABKS schemes

scheme	(Qiu and Liu, 2017)	(Sun and Yu, 2016)	(Wan and Yu, 2016)
Setup	$(4+\sum_{i=1}^{n_a} n_i)\|G\|+(2+\sum_{i=1}^{n_a} n_i)\|Z_P\|$	$(2+3n_a)\|G\|+(1+3n_a)\|Z_P\|$	$(4+n_a)\|G\|+(2+3n_a)\|Z_P\|$
KeyGen	$(2+2n_a)\|G\|$	$(2+2n_a)\|G\|+\|Z_P\|$	$(1+3n_{a,u})\|G\|+\|Z_P\|$
IndexGen	$(2+2n_a)\|G\|$	$(2+n_{a,u})\|G\|$	$3\|G\|$
Encryption	--	--	$(2+2n_a)\|G\|$
Token	$(2+2n_a)\|G\|+\|Z_P\|$	$(1+2n_{a,u})\|G\|+\|Z_P\|$	$2\|G\|$

Table 21. Contrast calculation cost of ABKS schemes

Setup	$(2+\sum_{i=1}^{n_a} n_i)\mid E\mid$	$(1+3n_a)E+P$	$(2+2n_a)E+P$
Keygen	$(2+2n_a)E$	$(3+2n_a)E$	$(2+3n_{a,u})E$
Token	$(1+2n_a)E$	$(1+2n_{a,u})E$	$E+2P$
Search	$(1+2n_a)P+E$	$(1+n_a)P+E$	$E+2P$
Update	--	$(2+n_{a,u})E$	$n_x E$
Verification	--	--	--

5.2.3. PRKS

PRKS uses a proxy re-encryption system to search encrypted data, which enables authenticated data users to re-encrypt the source data and grant the search function to other users. Shao and Cao (2010) proposed proxy re-encryption with a keyword search and a new cipher primitive, which is proved to be secure in the random oracle model (wang and huang, 2012). Yau and Heng (2010) proposed a search agent re-encryption scheme and gave the specific construction of security and re-encryption scheme in the random oracle model.

Fang and susio (2012) proposed a new conditional proxy re encryption and keyword search, which combined PRE and PEKS, and resisted the chosen ciphertext attack. Yang and Ma (2016) introduced a new time-dependent scheme, which enabled patients to delegate part of their access rights in a limited time to search related records. The contrasts of these ABKS schemes are shown in Table 22

Table 22. Communication and computation overhead of PRKS schemes

l the size of keyword set, N the number of conjunctive keywords in the access structure, t_{EXP} : execution time for exponentiation operation, t_{Pair} : execution time for bilinear paring operation

Paper	Communication					Computation		
	Pub key	Pri key	CT	Tradpoor	Re-encryption	KeyGen	Encryption	Re-encryption
(Shao and cao, 2010)	1	1	7	1	7	t_{EXP}	$2t_{pair}+(2l+4)t_{EXP}$	t_{EXP}
(Yau and Hen, 2010)		1	2	2	2	t_{EXP}	$t_{pair}+3t_{EXP}$	t_{EXP}
(Fang and susilo, 2012)	5	5	7	4	4	$5t_{EXP}$	$3t_{pair}+3t_{EXP}$	$t_{pair}+2t_{EXP}$
(Wang and Huang, 2012)	$l+3$	3	$2l+4$	3	$l+3$	$(2l+3)t_{EXP}$	$(4l+3)t_{EXP}$	$2t_{pair}$
(Yang and Ma, 2016)	1	1	$l+3$	$l+3$	$l+6$	t_{EXP}	$(l+4)t_{EXP}$	$(l+5)t_{EXP}$

5.3. Discussion of SE

In this paper, we introduce the research mechanism of searchable encryption and analyze the research progress from two aspects: symmetric searchable encryption and asymmetric searchable encryption. The following problems in searchable encryption mechanism warrant further study:

1 Research on flexible and efficient query statement. In the existing searchable encryption scheme, the research focuses on fuzzy retrieval or conditional retrieval. Many shortcomings, such as keyword sorting, multi-keyword retrieval, and keyword retrieval results verifiability, exist.

2 Research on searchable encryption technology with semantic reservation. The encryption scheme will require that keywords have semantic relations that cannot be obtained by a server after encryption. The scheme can not only achieve accurate query but also accurately obtain the files of users.

3 Research on the expression ability of a ciphertext search sentence. A flexible ciphertext search statement can enable users to accurately locate the encrypted data files and increase the flexibility of expressing the search requirements.

4 Research on the efficiency of a searchable encryption scheme. To achieve a secure search, efficiency is a major factor in the process of ABE from theory to practice.

5 Research on an attribute-based encryption scheme with rich expression ability. This content is an important content of researching the searchable mechanism and the cornerstone of high efficiency and searchability for supporting any language and satisfying more expressive ability.

6 Research on search encryption keyword in a multi-server system model. Multi-party computing enables multiple entities to jointly calculate and obtain results. However, the application to multi-server keyword retrieval scenarios is difficult. Therefore, solving the keywords retrieval problem using the multi-server model is an urgent need.

7 Research on efficient decryption scheme and encryption outsourcing scheme. Pairing calculations will be time consuming; so reducing the use of pairing, which will improve the efficiency of encryption and decryption, and obtaining a fast decryption scheme are necessary.

8 Research on simple puzzle assumptions. For the condition of the same security level, this research is expected to have a very important role in promoting secure and searchable applications by seeking a simpler hypothesis.

9 Research on searchable encryption mechanism of relational operation (>, <, = etc.). Although some of the existing work can realize range and subset queries, they are not ideal regarding the effect of supporting the relational operation.

10 Research on potential key leakage in multi-user sharing mode. Although existing schemes have been capable of solving the keyword retrieval problem, they are based on higher system model assumptions or lower security objectives

or low efficiency due to server re encryption or other complex operations.

6. Combination technologies in cloud privacy

In the previous sections, we discussed and analyzed the research on cloud computing privacy protection based on access control, attribute encryption and search encryption. Due to the complex and changeable environment and massive information aggregation and advancements in research, ABE, trust, access control and many related technologies are integrated to achieve better privacy security protection in cloud computing (Eugenia and Maria,2013).

6. 1. Access control, encryption and trust

Trust, access control and encryption are important technical means of cloud computing. Many researchers have obtained important results from these aspects (Fig. 21).

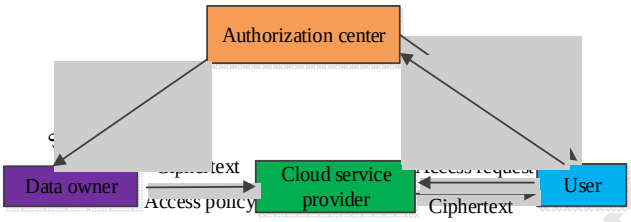


Fig. 21. Trust access control authority based on ABE

Eugenia and Maria (2013) introduced an access control model that is based on rich expression information, which can standardize context authorization policy and promote the realization of privacy protection by visualization technology. Lan and Vijay (2015) designed a cloud storage system that is based on encrypted RBAC and showed how to use trust assessment to reduce risk and improve the decision quality of data owners and cloud storage service roles. Xu and jiang (2019) proposed a trust-based mechanism to achieve collaborative privacy management, in which users can balance data sharing and privacy protection by adjusting the parameters of the proposed mechanism.

WANG and WANG (2019) proposed a framework of cloud storage security access control based on blockchain technology, in which the data owner can store the ciphertext of the data in the blockchain network via smart contract and establish an effective access period. Waqas et al. (2018) proposed a hybrid policy tree mechanism for dynamic attribute selection for security solutions and key management, which further utilized encryption and decryption service providers for complex operations.

Xu and Fu (2017) designed a privacy protection model to ensure the security of encryption card dynamic scheduling and provided a series of security protocols to establish the trust chain between users and encryption card. Liu and Wang (2018) proposed a privacy protection framework to improve the willingness of data owners and untrusted enterprises to share data, which can effectively protect the private data of related participants. Yang and Li (2015) proposed a practical privacy protection and sharing scheme for medical records, which realized the consideration of differentmedical data.

6.2. Multi-tenant

Due to the sharing nature of cloud computing and application of virtualization technology, cloud computing service providers need to carefully address multi-tenant security and virtualization security threats.

Table 23. Contrast of several multi- tenant schemes

Literature	Classification	Scheme	Technical approach	Application	Scalability
(Eugenia and Maria, 2013)	Trust, access control and encryption	Access control model with rich expression policy	Visualization technology, policy	Privacy protection	Common
(Lan and Vijay (2015)		RBAC-based encryption for cloud storage	Trust, risk evaluation, encryption, RBAC	Cloud storage	Common
(WANG and WANG,2019)		Cloud storage security framework	Access control, blockchain technology	Blockchain network	Common
(Waqas et al.,2018)		Attribute selection for security solutions and key management	Hybrid policy tree, trust, encryption	Mobile cloud computing	Good
(Liu and Wang,2018)		Privacy protection framework	Trust, encryption	Internet of thing	Common
(Rémi and Guillaume, 2018)	Multi-tenant, virtualization	Robust solution to detect malicious activities	Virtualization safety	Cloud computing	Common
(LIU and SHAO, 2015)		Scheduling scheme of multiple directed acyclic graphs	Scheduling policy	Personal privacy security.	Good

Rémi and Guillaume (2018) proposed a robust and cost-effective solution to detect malicious activities in the public virtualization environment: 1) estimate the workload of virtual hosts; 2) provide a detection algorithm to distinguish the infected hosts, and evaluate the efficiency using a real data set. To solve the scheduling problem of multiple directed acyclic graphs in cloud computing, LIU and SHAO (2015) proposed a scheduling policy to satisfy the requirements of resources and protect privacy security.

Detecting attacks among tenants is a key security requirement. Mohamed and Chamseddine (2019) proposed a cross-tenant attack detection and prevention framework based on SQL

syntax analysis, which can satisfy the requirements of accuracy, portability and compatibility. Ghassan and Matthiasr (2017) analyzed the challenges of coordinating the security and functional requirements of an existing multi-tenant cloud and effectively improved the security of cloud storage services. The contrasts of these schemes are shown in Table 23.

6.3. Extension of access control privacy protection

Based on the characteristics of access control and cloud computing, many researchers have adopted extension ideas to protect privacy, and achieved many research results.

Qi and Ravi (2017) proposed a mechanism of mandatory content access control (MCAC), which is a distributed information flow control mechanism that enables content providers to control which network nodes cache content. Na and Kim (2016) proposed a macdroid, in which a platform can be controlled to access the installed applications and users can control the behaviors of the applications via policies. Fahim and Khan (2016) proposed a public key cryptography protocol for security entity authentication and to grant permission to an authorized person by the token in a smart card. Xin and Ram (2012) constructed an ABAC, which had the characteristics of "just enough", and can be configured as DAC, MAC and RBAC.

Michael and Gabriel (2012) proposed a new trust protocol framework, in which users provide role and location tokens and requests to service providers and service providers negotiate with role and location permissions to verify tokens and evaluate policies. Based on the rich algebraic structure of the elliptic curve, Zhu and Ahn (2013) proposed a unified role-based cryptosystem structure and implemented several functions, such as role revocation and anonymity, to verify the rationality and effectiveness. JASON et al. (2018) employed the smart contract and blockchain technology as general infrastructure to express the basic trust and identification relationship, realized the utilization of cross-organization, and implemented a challenge response authentication protocol to verify the ownership of user roles.

By order bilinear groups, Zhu and Huang (2015) proposed a practical construction method of ABE based on forward and backward derivative functions and provided a compact policy representation method to reduce the size of private key and ciphertext. In an information center network (ICN), Li and Huang (2018) proposed a privacy protection attribute management access control scheme, which can be compatible with the ICN architecture. Based on the combination of attribute and purpose, Morteza and Farnaz (2019) proposed a privacy protection access control framework. If the privacy preference of the requester is compatible with the privacy policy, the access request to the service is allowed. DING and CAO (2019) proposed an attribute-based access control scheme for the Internet of Things, which employed blockchain technology to record the distribution of attributes and satisfy the needs of efficient and lightweight computing. Authorization exceptions may occur during continuous reassessment. Arlindo and Altair (2014) proposed addressing the flexibility of continuous authorization reassessment by maintaining appropriate access control. The contrast results of these schemes are listed in Table 24.

Table 24. Contrast of several extension access control models

Literature	Classification	Scheme	Technical approach	Application	Scalability
(Qi and Ravi, 2017)	MAC	Mandatory content access control	Information flow	Network cache	Common
(Na and Kim, 2016)	MAC	Mandatory access control	Access policies	Android security	Common
Fahim and Khan (2016)	RBAC	Public key cryptography protocol	Encrypt, access control	Smart card.	Common
(Michael and Gabriel, 2012)	RBAC	New trust protocol framework	Privacy aware RBAC	Spatially privacy	Good
(JASON et al.,2018)	RBAC	Smart authentication protocol	Blockchain, trust	Blockchain	Common
(Li and Huang, 2018)	ABAC	Attribute management scheme	Access control policy	ICN	Good
(Morteza and Farnaz,2019)	RBAC	Purpose privacy access control	Purpose policy	Secure service	Good
(DING and CAO, 2019)	ABAC	Lightweight access control	Blockchain	Internet of things	Good
(Arlindo and Altair, 2014)	UCON	Authorization reassessment	Access control	Cloud computing	Good

6.4. Discussion and analysis

These privacy protection mechanisms cannot completely avoid privacy risks, such as access control, encryption, trust, and search encryption, which are some key issues to be explored.

1 With continuous changes in the application environment, a simple access structure has been unable to satisfy the security requirements of an access control system. The design of access structure with a rich expression ability is the future research focus of access control.

2 Integrating the trust model in ABE. When using the ABE mechanism for access control, the relationship among the data provider, cloud platform and user can be determined by the trust value. Further, complex key management and encryption and decryption calculations can be carried out on the cloud server, which not only ensures the security but also reduces the computing burden of the whole system.

3 Research of the multi-domain cooperation mechanism in access control. How to accurately understand the semantics of the original policy and overcome the differences of expression ability is an important guarantee of policy fusion and system security with multi-domain cooperation.

4 The combination of attribute encryption and other encryption mechanisms. The homomorphic encryption mechanism can realize ciphertext computation and protect outsourced privacy content. Both asymmetric encryption and symmetric encryption can realize the low-cost privacy

protection mechanism. Therefore, the combination of multiple encryption mechanisms is a controversial issue in future research.

7. Challenges and future directions

This paper focuses on the latest research results of cloud security privacy protection and introduces representative security threats and protection technologies, such as access control, ABE, and searchable encryption. Our analysis reveals some deficiencies in cloud security protection schemes. As a result, future research work should mitigate these deficiencies.

7.1. Challenges

Via analysis and contrast, we observe that cloud computing security protection work has achieved satisfactory research results. However, many problems remain, which prompt the consideration of a variety of security factors and continuous improvements in defense technology and security strategies.

1 All kinds of attacks are generally based on the defects of cloud infrastructure in a system management program. Different attack methods are adopted to enhance the operation authority or steal sensitive data.

2 To better defend cross-virtual machine side channel attacks, researchers should pay more attention to the forms of virtual machine attacks in the process of cloud migration, such as malicious theft of privacy information.

3 Design a security defense policy that can be independent of CSP to effectively limit the abuse of rights. In the process of security defense, researchers should also pay attention to the negative impact of defense schemes on the performance of public clouds.

4 The protection degree of sharing algorithms to a user's identity privacy needs improvement. The unidirectional and transitive characteristics of the proxy re-encryption algorithm need to be further investigated, while the efficiency of an attribute encryption algorithm in dynamic permission management is usually poor.

5 Recyclability proves that prevention of the illegal deletion of file level or block level cloud data and improved audit efficiency in the case of data updates are urgent.

6 Privacy requirements and service level agreements (SLAs). Hidden dangers of unintentional or malicious disclosure of user privacy exist in an SLA. Therefore, privacy modeling and verification, consistency detection, privacy description, and implementation are the key issues to be solved.

7 The privacy feedback mechanism contains risk of disclosure. In the privacy feedback mechanism, users can learn different privacy operations and understand potential risks that may damage confidentiality. The use of a third party to audit a privacy record is a key issue in the privacy feedback mechanism.

8 The conflict between the convenience and accountability of services and privacy protection. Risk assessment is not a new topic but privacy risk assessment remains an important challenge, which requires an evaluation of the trust level of cloud service providers and tenants.

7.2. Future directions

Many defense technologies and security mechanisms exist in cloud computing. We propose a future development framework, as shown in Fig. 22, which is divided into three parts: principle & model, methodology, and design &application. A cloud user can utilize various policies/technologies and quickly achieve target security and personalized privacy protection.

1 Secure search technology for protecting users' purposes. The mapping relationship is analyzed by frequent pattern mining to detect the privacy information hidden in the user's search intention and provide real-time warnings of behavior privacy, identity privacy and location privacy.

2 Integrate unified privacy metrics. From the life cycle of cloud data, the period includes multi-source data fusion, user behavior, and fine-grained access control in the search process. Because these privacy protection technologies have evaluation indicators, building an evaluation system that integrates multi-dimensional privacy protection, search accuracy and timeliness is necessary.

3 Information fusion and knowledge extraction technology for cloud computing big data. Given the multi-dimensional and multi-granularity characteristics of cloud data information and the diversity of users' search needs, extracting information to generate knowledge aggregates is necessary.

4 Coordinate the trust and interest relationship of multiple participants in cloud computing. The participation of different parties complicates the security/privacy issue in cloud computing because the security objectives of different parties may be very different and may even conflict with each other.

5 Big data and cloud computing. The real-time big data processing must continuously input, analyze and output the high-performance data stream in a short time. To ensure security and confidentiality, an efficient and lightweight cryptographic algorithm can reduce the computing cost.

6 Multiple cloud computing compatible integration. Because different cloud computing can be regarded as an independent field, these mechanisms are compatible. People should consider how to solve the compatibility problems in different countries.

7 Integration of various new network technology paradigms. The security layer among cloud computing, fog computing and Internet of Things devices can be built via blockchain. Cloud computing will become a reliable, credible and powerful architecture.

8 Privacy protection based on trusted cloud platform. Privacy protection in a trusted cloud platform involves the whole life cycle of data processing in a cloud.

9 Research on unified secure cross-platform mobile operating system. Different platforms and equipment of cloud providers

have similar functions and safety concepts, which can reduce costs and improve efficiency by multi-party unification.

10 Relevant government policies and regulations management. Cloud computing may sell the collected information to a third party without the permission of residents. Therefore, cloud computing requires new government policies to balance interests and privacy security risks.

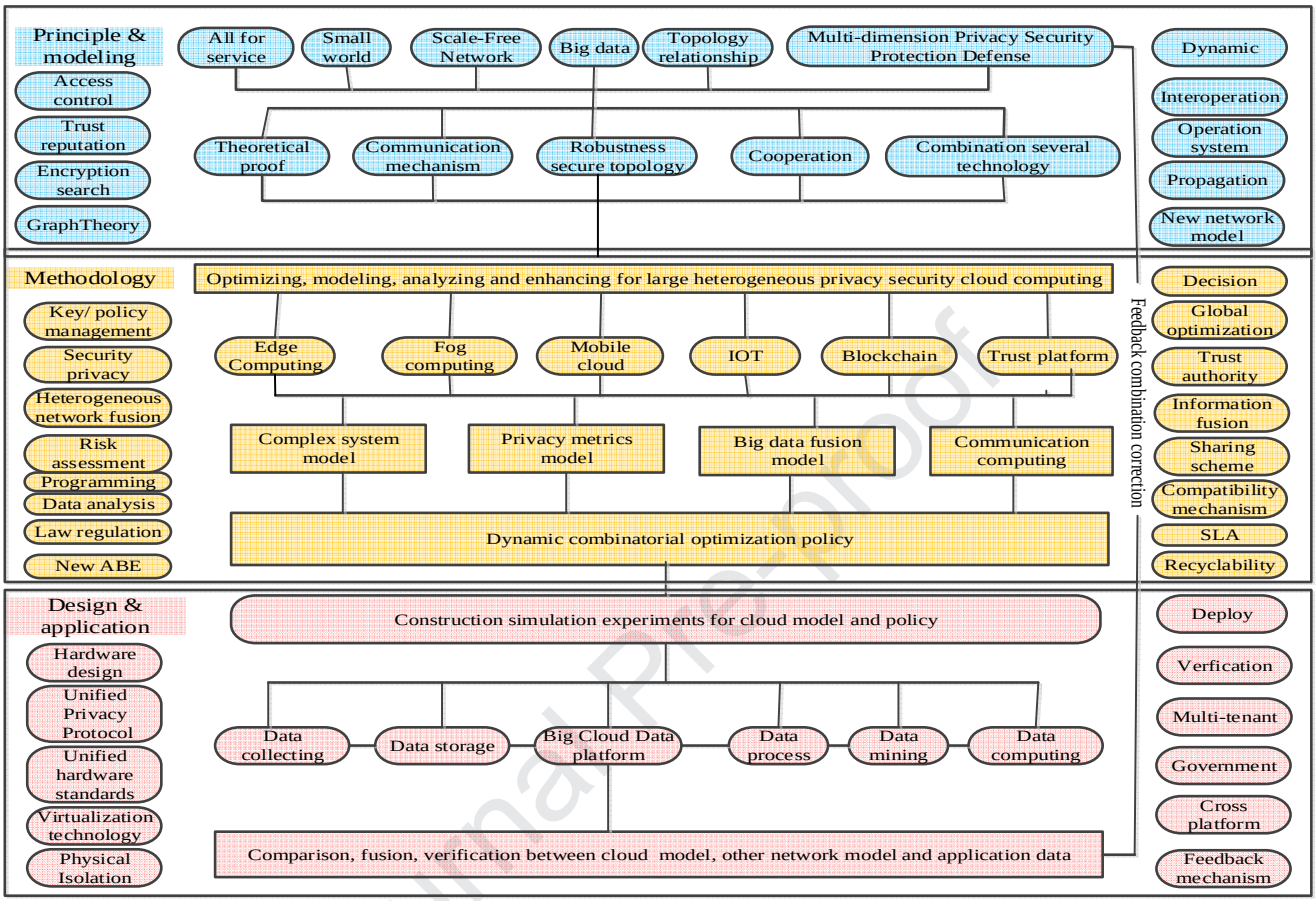


Fig. 22. Future development of cloud computing

8. Summary

Although cloud computing has a broad development prospect, it faces substantial privacy security challenges. We discuss and analyze the research progress of several technologies, such as access control, ABE and trust, and the associated challenges and research directions. Another problem that cannot be disregarded is that the security of network infrastructure has a key role, for example, the use of firewalls can protect the resources in the cloud from the bottom. Therefore, building a secure network infrastructure environment is the foundation of a cloud computing environment.

Note that the privacy protection and data security issues of cloud computing are not only technical issues but also involve standardization, laws and regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) (Greg Porter Heinz College, 2018) and Financial Agency Privacy Act (FAPA) (Karen and Bryan, 2016). In addition to the development of technology, academic, industrial and relevant management departments need to collaborate to create a secure efficient cloud environment.

References

Alexandra. Boldyreva, Vipul Goyal, Virendra Kumar. Identity-based encryption with efficient revocation. Proceedings of the 2008 ACM Conference on Computer and Communications Security, CCS 2008, Alexandria, Virginia, USA, October 27-31, 2008, pp. 417–426.

Allison. Lewko, Brent. Waters. Decentralizing attribute-based encryption. in Advances in Cryptology EUROCRYPT. Berlin, Germany: Springer, May 2011, pp. 568–588.

Amit Sahai, Hakan. Seyalioglu, Brent. Waters. Dynamic credentials and ciphertext delegation for attribute-based encryption. Advances in Cryptology. 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, August, 2012.

Amal Ghorbel, Mahmoud Ghorbel. Privacy in cloud computing environments: a survey and research challenges.The Journal of Supercomputing. June 2017, Volume 73, Issue 6, pp 2763–2800.

Amit Sahai, Brent Waters. Fuzzy Identity-Based Encryption. Annual EUROCRYPT 2005: Advances in Cryptology.

Amos Beimel, Aner Ben-Efraim. Multi-linear Secret-Sharing Schemes. International Association for Cryptologic Research 2014.LNCS, pp. 394–418.

An Liu; Weiqi Wang. A Privacy-Preserving Framework for Trust-Oriented Point-of-Interest Recommendation. IEEE Access,Year: 2018, Volume: 6.

Arlindo Luis Marcon Jr., Altair Olivo Santin. A UCONABC Resilient Authorization Evaluation for Cloud Computing.IEEE Transactions on Parallel and Distributed Systems, Vol. 25, No. 2, February 2014.

AŠila A. Yavuz, Jorge Guajardo. Dynamic searchable symmetric encryption with minimal leakage and efficient updates on commodity hardware. Selected Areas in Cryptography SAC 2015: 22nd International Conference, Sackville, Canada, August 12–14, 2015.

Baodong Qin, Hui Cui. Server-aided revocable attribute-based encryption resilient to decryption key exposure. Cryptology and Network Security - 16th International Conference, CANS 2017.

Beimel A. Secure schemes for secret sharing and key distribution [Ph.D. Thesis]. Technion: Israel Institute of Technology, 1996.

Bethencourt J, Sahai A, Waters B. Ciphertext Policy attribute-based encryption. 2007 IEEE Symp. on Security and Privacy. Washington; IEEE Computer Society, 2007. 321−334.

Bing Li, Dijiang Huang. Attribute-based Access Control for ICN Naming Scheme. IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 15, NO. 2, MARCH/APRIL 2018.

Bo Qin, Qianhong Wu, Lei Zhang. Provably secure threshold public-key encryption with adaptive security and short ciphertexts. Information Sciences 210 (2012) 67–80.

Boneh Dan, Franklin Matt. Identity-Based encryption from the weil pairing. CRYPTO 2001. LNCS 2139, Berlin, Heidelberg: Springer-Verlag, 2001. 213−229.

Brent Waters. Realization. International Association for Cryptologic Research 2011. LNCS 6571, pp. 53–70.

Christoph. Bösch, Brinkman. Brinkman, P. Hartel, and W. Jonker. Conjunctive Wildcard Search over Encrypted Data. Secure Data Management, Springer Berlin Heidelberg, 2011, pp. 114-127.

Cong Wang, Ning. Cao, K. Ren. Enabling secure and efficient ranked keyword search over outsourced cloud data. IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 8, pp. 1467-1479, Dec. 2012.

CHENGYU HU, PENGTAO LIU. Public-Key Encryption with Keyword Search via Obfuscation. IEEE ACCESS, VOLUME 7, 2019.10.19.

Cloud Security Alliance, 2017. “Security Guidance for Critical Areas of Focus in Cloud Computing V4.0,” http://www.cloudsecurityalliance.org/.

David. Cash, Stanislaw Jarecki. Highly-Scalable Searchable Symmetric Encryption with Support for Boolean Queries. Advances in Cryptology – CRYPTO 2013, Springer Berlin Heidelberg, 2013, pp. 353-373.

Dan Liu, Zheng Yan. A Survey on Secure Data Analytics in Edge Computing. IEEE INTERNET OF THINGS JOURNAL, VOL. 6, NO. 3, JUNE 2019.

De liang Xu, Cai Fu, Guohui Li.Virtualization of the Encryption Card for Trust Access in Cloud Computing. IEEE ACCESS: 2017, Volume: 5.

De Sourya Joyee，Ruj, Sushmita. Efficient decentralized attribute-based access control for mobile clouds. IEEE Trans. Cloud Computing. Doi: 10.1109/TCC.2017.2754255.

Ducas Léo. Anonymity from asymmetry: new constructions for anonymous HIBE. In: Pieprzyk J. CT-RSA. Lecture Notes in Computer Science, vol. 5985, pp. 148–164. Springer, Heidelberg (2010).

Eugenia I. Papagiannakopoulou, Maria N. Koukovini. A privacy-aware access control model for distributed network monitoring. Computers and Electrical Engineering 39 (2013) 2263–2281.

Ferraiolo DF, Sandhu R, Gavrila S. Proposed NIST standard for role-based access control. ACM Trans. on Information and System Security, 2001, 4(3); 224-274.

Ghassan Karame, Matthias Neugschwandtner, Hubert Ritzdorf. Reconciling Security and Functional Requirements in Multi-tenant Clouds. SCC '17 Proceedings of the Fifth ACM International Workshop on Security in Cloud Computing Pages 11-18.

Goyal V, Pandey O, Sahai A, Waters B. Attribute-Based encryption for fine-grained access control of encrypted data. In: Proc. of the 13th ACM Conf. on Computer and Communications Security 2006.

Greg Porter Heinz College, Carnegie Mellon University. A Mapping of the Health Insurance Portability and Accountability Act (HIPAA) Security Rule to the Cyber Resilience Review (CRR). 2018.

Hui Cui, Robert H. Deng.Server-aided revocable attribute-based encryption. Computer Security - ESORICS 2016 - 21st European Symposium on Research in Computer Security, Heraklion, Greece, 2016, Proceedings, Part II, 2016, pp. 570–587.

Hui Guo，Zhenfeng Zhang. Proxy re-encryption with unforgeable re-encryption keys. Cryptology Netw. Secur., vol. 8813, pp. 20–33, 2014.

Hyun Sook Rhee, Jong Hwan Park. Trapdoor security in a searchable public-key encryption scheme with a designated tester. J. Syst. Softw., Vol. 83, no. 5, pp. 763–771, 2010.

Heng He; Ruixuan Li. Secure, Efficient and Fine-Grained Data Access Control Mechanism for P2P Storage Cloud. IEEE Transactions on Cloud Computing: 2014, Volume: 2, Issue: 4.

Hua Deng, Qianhong Wu. Ciphertext-policy hierarchical attribute-based encryption with short ciphertexts. Information Sciences 275 (2014) 370–384.

Hui Ma, Rui Zhang, Guomin Yang. Efficient Fine-Grained Data Sharing Mechanism for Electronic Medical Record Systems with Mobile Devices.DOI 10.1109/TDSC.2018.2844814, IEEE Transactions on Dependable and Secure Computing.

Hui Ma, Rui Zhang, Shuzhou Sun. Server-Aided Fine-Grained Access Control Mechanism with Robust Revocation in Cloud Computing.IEEE Transactions on Services Computing, VOL. 14, NO. 8, AUGUST 2015.

Jin Li，Qian Wang，Cong Wang. Fuzzy keyword search over encrypted data in cloud computing. Int. J. Eng. Res. Appl, vol. 4, no. 7, pp. 197–202, 2014.

Jinguang. Han, W. Susilo. Improving privacy and security in decentralized CP-ABE. IEEE Trans. Inf. Forensics Security, vol. 10, no. 3, pp. 665–678, 2015.

Li, Jingwei，Huang, Xinyi. Securely outsourcing attribute-based encryption with checkability. IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 8, pp. 2201–2210, 2014.

Ning Jianting, Dong Xiaolei. Wei. White-box traceable ciphertext-policy attribute-based encryption supporting flexible attributes. IEEE Trans. Inf. Forensics Secur, vol. 10, No. 6, pp. 1274–1288, Jun. 2015.

Jianting Ning, Zhenfu Cao, Xiaolei Dong. Large universe ciphertext-policy attribute-based encryption with white-box traceability.in Computer Security. Berlin, Germany: Springer, 2014, pp. 55–72.

Jun Shao, Zhenfu Cao. CCA-secure proxy re-encryption without pairings. Proc. Public Key Cryptography, vol. 5443, pp. 357–376, 2009.

Jun Shao, Rongxing Lu. Fine-grained data sharing in cloud computing for mobile devices. 2015 IEEE Conference on Computer Communications, INFOCOM, Kowloon, Hong Kong, May 1, 2015, pp. 2677–2685.

Jun Shao, Zhenfu Cao. Proxy re-encryption with keyword search. Inf. Sci., vol. 180, no. 13, pp. 2576–2587, 2010.

Jianfeng, Wang et al. Efficient verifiable fuzzy keyword search over encrypted data in cloud computing. ComSIS Vol. 10, No. 2, Special Issue, April 2013.

Jason Paul Cruz, Yuichi Kaji. RBAC-SC: Role-Based Access Control Using Smart Contract. IEEE ACCESS, VOLUME 6, 2018.

Jianbing Ni, Kuan Zhang. Securing Fog Computing for Internet of Things Applications: Challenges and Solutions. IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 20, NO. 1, 2018.

Jianting Ning, Zhenfu Cao.White-Box Traceable CP-ABE for Cloud Storage Service: How to Catch People Leaking Their Access Credentials Effectively. IEEE Transactions on Dependable and Secure Computing, Vol. 15, No. 5, September/October 2018.

Jiguo Li, Ningyu Chen. Extended File Hierarchy Access Control Scheme with Attribute Based Encryption in Cloud Computing.DOI 10.1109/TETC.2019.2904637, IEEE Transactions on Emerging Topics in Computing.

Jiguo Li, Qihong Yu. Hierarchical attribute based encryption with continuous leakage-resilience. Information Sciences 484 (2019) 113–134.

Ji Jiang Yang, Jian Qiang Li. A hybrid solution for privacy preserving medical data sharing in the cloud environment. Future Generation Computer Systems 43–44 (2015) 74–86.

Jin Li, Yanyu Huang, Yu Wei. Searchable Symmetric Encryption with Forward Search Privacy. IEEE Transactions on Dependable and Secure Computing. DOI10.1109/TDSC.2019.2894411.

Johanna Ullrich, Tanja Zseby. Network-Based Secret Communication in Clouds: A Survey. IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 19, NO. 2, SECOND QUARTER 2017.

Joonsang Baek, Willy Susilo. New Constructions of Fuzzy Identity-Based Encryption. 2007 ACM symposium on Information, computer and communications security, 368-370.

Kan Yang, Xiaohua Jia, Kui Ren. DAC-MACS: Effective data access control for multi-authority cloud storage systems. IEEE Trans. Inf. Forensics Security, vol. 8, no. 11, pp. 1790–1801, Nov. 2013.

Kee Sung Kim, Minkyu. Kim. Forward Secure Dynamic Searchable Symmetric Encryption with Efficient Updates. In CCS, ACM, pages 1449-1463, 2017.

Kaoru Kurosawa. Yasuhiro Ohtaki. How to update documents verifiably in searchable symmetric encryption. in Cryptology and Network Security - 12th International Conference, CANS 2013, Paraty, Brazil, November 20-22. 2013, pp. 309–328.

Karen Colorafi1, Bryan Bailey. It’s Time for Innovation in the Health Insurance Portability and Accountability Act (HIPAA). JMIR Med Inform

2016.
Kwangsu Lee, Jong Hwan Park. Anonymous HIBE with short ciphertexts: full security in prime order groups. Des. Codes Cryptogr. (2015) 74:395–425.
Liming Fang, Willy. Susilo. Chosen-ciphertext secure anonymous conditional proxy re-encryption with keyword search. Theoretical Comput. Sci., vol. 462, pp. 39–58, Nov. 2012.
Liming. Fang, Willy. Susilo. Public key encryption with keyword search secure against keyword guessing attacks without random Oracle. Inf. Sci., vol. 238, pp. 221–241, Jul. 2013.
Lan Zhou, Vijay Varadharajan. Trust Enhanced Cryptographic Role-Based Access Control for Secure Cloud Data Storage. IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 10, NO. 11, NOVEMBER 2015.
Lei Xu, Chunxiao Jiang. Trust-Based Collaborative Privacy Management in Online Social Networks. IEEE Transactions on in Formation Forensics and Security, Vol. 14, No. 1, January 2019.
Lewko A, Sahai A, Waters B. Revocation systems with very small private keys. In: Proc. of the IEEE Symp. on Security and Privacy. Washington: IEEE Computer Society, 2010. 273−285.
Li Ping Chen, Yi Hui.Research on the Cloud Computing Storage Privacy Preserving Based on MB-Tree Dynamic Access Model. Applied Mechanics & Materials;2014, Issue 513-517, p2350.
Liu Yaqiu, Shao Hongrun. Multi-DAGs Scheduling Integrating with Security and Availability in Cloud Environment. Chinese Journal of Electronics Vol.24, No.4, Oct. 2015.
M. Fahim Ferdous Khan, Ken Sakamura. A Discretionary Delegation Framework for Access Control Systems. OTM 2016 Conferences, LNCS 10033, pp. 865–882, 2016.
Michael S. Kirkpatrick, Gabriel Ghinita. Privacy-Preserving Enforcement of Spatially Aware RBAC.IEEE Transactions on Dependable and Secure Computing, Vol. 9, No. 5, September/October 2012.
Mihir Bellare, Dennis Hofheinz. Subtleties in the Definition of IND-CCA: When and How Should Challenge Decryption Be Disallowed? Cryptol. (2015) 28: 29–48.
Mohamed Yassina, Chamseddine Talhi. ITADP: An inter-tenant attack detection and prevention framework for multi-tenant SaaS.Journal of Information Security and Applications 49 (2019) 102395.
Morteza Amini, Farnaz Osanloo. Purpose-Based Privacy Preserving Access Control for Secure Service Provision and Composition. IEEE TRANSACTIONS ON SERVICES COMPUTING, VOL. 12, NO. 4, JULY/AUGUST 2019.
Muhammad Baqer Mollaha, Md. Abul Kalam Azad. Security and privacy challenges in mobile cloud computing: Survey and way ahead. Journal of Network and Computer Applications 84 (2017) 38–54.
Nuttapong Attrapadung, H. Imai. Attribute-based encryption supporting direct/indirect revocation modes.in Cryptography and Coding, 12th IMA International Conference, Cryptography and Coding 2009, Cirencester, UK, December 15-17, 2009.
Na June-sung; Kim Do-Yun. Mandatory Access Control for Android Application Security. Journal of KIISE, Volume 43 Issue 3, Pages.275-288, 2016.
Ning Shang, Elisa Bertino. Privacy-Preserving Policy Based Content Sharing in Public Clouds. IEEE Transactionn on Knowledge and Data Engineering, Vol. 25, No. 11, November 2013.
Okamoto T., Takashima K. Achieving short ciphertexts or short secret-keys for adaptively secure general inner-product encryption. In: Lin D., Tsudik G., Wang X. (eds.) CANS. Lecture Notes in Computer Science, vol. 7092, pp. 138–159. Springer, Heidelberg (2011).
Okamoto T., Takashima K.: Adaptively attribute-hiding (hierarchical) inner product encryption. EUROCRYPT. Lecture Notes in Computer Science, vol. 7237, pp.591–608. Springer, Heidelberg (2012).
PAN JUN SUN. Privacy Protection and Data Security in Cloud Computing: A Survey, Challenges, and Solutions.VOLUME 7, 2019, IEEE ACCESS. Digital Object Identifier 10.1109/ACCESS.2019.2946185
PAN JUN SUN. Research on the Tradeoff Between Privacy and Trust in Cloud Computing. VOLUME 7, 2019, IEEE ACCESS.Digital Object Identifier 10.1109/ACCESS.2019.2891589.
Peng Zhang, Joseph K. Liu.A Survey on Access Control in Fog Computing. IEEE Communications Magazine • February 2018. Digital Object Identifier: 10.1109/MCOM.2018.1700333.
Qi Chai, Guang Gong. Verifiable symmetric searchable encryption for semi-honest-but-curious cloud servers. Proceedings of IEEE International Conference on Communications, ICC 2012, Ottawa, ON, Canada, June 10-15, 2012, 2012, pp. 917–922.
Qiong. Huang, Hongbo. Li. An efficient public-key searchable encryption scheme secure against inside keyword guessing attacks. Inf. Sci., vols. pp.1–14, 2017.
Qi Li, Ravi Sandhu. Mandatory Content Access Control for Privacy Protection in Information Centric Networks. IEEE Transactions on Dependable and Secure Computing, Vol. 14, No. 5, September 2017.
QIAN XU, CHENGXIANG TAN. Secure Multi-Authority Data Access Control Scheme in Cloud Storage System Based on Attribute-Based Signcryption. IEEE Access, VOLUME 6, 2018.
Qinlong Huang; Yixian Yang; Licheng Wang. Secure Data Access Control With Ciphertext Update and Computation Outsourcing in Fog Computing for Internet of Things. IEEE Access: 2017, Volume: 5.
Raphael Bost, Brice Minaudy. Forward and Backward Private Searchable Encryption from Constrained Cryptographic Primitives. In CCS, ACM, pages 1465-1482, 2017.
Raphael Bost. $\Sigma o\phi o\varsigma$: Forward secure searchable encryption. Proc. SIGSAC Conf. Comput. Commun. Secur., Vienna, Austria, 2016, pp. 1143–1154.
Rui. Jiang, Xianglong. Wu, Bharat. Bhargava. SDSS-MAC: Secure data sharing scheme in multi-authority cloud storage systems. Comput. Secur., vol. 62, pp. 193–212, Sep. 2016.
Rui. Zhang, Hui. Ma, and Y. Lu. Fine-grained access control system based on fully outsourced attribute-based encryption. Journal of Systems and Software, vol. 125, pp. 344–353, 2017.
RajaniKanth Aluvalu,Lakshmi Muddana. A Survey on Access Control Models in Cloud Computing. Proceedings of the 49th Annual Convention of the Computer Society of India, Volume 1 pp 653-664, 2015.
Rémi Cogranne, Guillaume Doyen. Detecting Botclouds at Large Scale: A Decentralized and Robust Detection Method for Multi-Tenant Virtualized Environments. IEEE Transactions on Network and Service Management, Vol. 15, No. 1, March 2018.
Reza Tourani; Satyajayant Misra. Security, Privacy, and Access Control in Information-Centric Networking: A Survey. IEEE Communications Surveys & Tutorials, Vol. 20, No. 1, First Quarter 2018.
Rui Zhang, Rui Xue. Searchable Encryption for Healthcare Clouds: A Survey. IEEE TRANSACTIONS ON SERVICES COMPUTING, VOL. 11, NO. 6, NOVEMBER/DECEMBER 2018.
Sanjam. Garg, Payman. Mohassel. TWORAM: Efficient oblivious RAM in two rounds with applications to searchable encryption. In CRYPTO pages 563-592, 2016.
Stanislaw Jarecki, Charanjit Jutla. Out sourced symmetric private information retrieval. 2013 ACM SIGSAC Conference on Computer and Communications Security, Berlin, Germany, pp. 875-888.
Sanjam Kamara, Charalampos. Papamanthou. Parallel and Dynamic Search able Symmetric Encryption. Financial Cryptography and Data Se curity, Springer Berlin Heidelberg, 2013, pp. 258-274.
Seny. Kamara, Charalampos Papamanthou. Dynamic Searchable Symmetric Encryption. 2012 ACM Conference on Computer and Communications Security, Raleigh, North Carolina, USA, 2012, pp. 965-976.
Shuo Qiu, Jiqiang. Liu. Hidden policy ciphertext-policy attribute-based encryption with keyword search against keyword guessing attack. Sci. China Inf. Sci., vol. 60, May 2017, Art. no. 052105. doi: 10.1007/s11432-015-5449-9.
Sushmita Ruj, Milos Stojmenovic. Decentralized access control with anonymous authentication of data stored in clouds. IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 2, pp. 384–394, Feb. 2014.
Shulan Wang, Junwei Zhou. An efficient file hierarchy attribute-based encryption scheme in cloud computing. IEEE Transactions on Information Forensics and Security, vol. 11, no. 6, pp. 1265-1277, Jun. 2016.
Shangping. Wang, Xiaojuan. Yu. Revocable key-policy attribute-based encryption scheme with two revocation lists. J. Electron. Inf. Technol,vol. 38, no. 6, pp. 1406–1411, 2016. doi: 10.11999/JEIT150845.
Shamir A. How to share a secret. Communications of the ACM, 1979, 22(11):612−613.
SHANGPING WANG, XU WANG. A Secure Cloud Storage Framework with Access Control Based on Blockchain. VOLUME 7, 2019, IEEE ACCESS.
Shareeful Islam, Moussa Ouedraogo. Assurance of Security and Privacy Requirements for Cloud Deployment Models. IEEE Transactions on Cloud Computing, Vol. 6, No. 2, April-June 2018.
SHEKHA CHENTHARA, KHANDAKAR AHMED. Security and Privacy-Preserving Challenges of e-Health Solutions in Cloud Computing. VOLUME 7, 2019, IEEE ACCESS.
SHENG DING, JIN CAO. A Novel Attribute-Based Access Control Scheme

Using Blockchain for IoT. IEEE ACCESS.VOLUME 7, 2019.
Shengmin Xu, Guomin Yang. Secure Fine-Grained Access Control and Data Sharing for Dynamic Groups in the Cloud. IEEE Transactions on Information Forensics and Security, Vol. 13, No. 8, August 2018.
Shulan Wang, Kaitai Liang. Attribute-Based Data Sharing Scheme Revisited in Cloud Computing. IEEE Transactions on Information Forensics and Security, Vol. 11, No. 8, August 2016.
Stefanov, Charalampos Papamanthou. 2014. Practical dynamic searchable encryption with small leakage. In Proceedings of the 2014 Network and Distributed System Security (NDSS) Symposium. Internet Society, Reston, VA, U.S.A.
Susan Hohenberger, Brent Waters. Attribute-Based Encryption with Fast Decryption. PKC 2013, LNCS 7778, pp. 162–179, 2013.
Tara Salman, Maede Zolanvari. Security Services Using Blockchains: A State-of-the-Art Survey. IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 21, NO. 1, 2019.
Wei chuen Yau, Swee.Huay Heng. Proxy re-encryption with keyword search: New definitions and algorithms. in Proc. Int. Conf. Security Technol., vol. 122. Jeju Island, Korea, Dec. 2010, pp. 149–160.
Wenhai Sun, Shucheng. Yu. 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.
Waqas Ahmad, Shengling Wang. Reputation-Aware Trust and Privacy-Preservation for Mobile Cloud Computing.IEEE Access: 2018,Volume: 6.
Xu anWang, Xinyi. Huang. Further observation on proxy re-encryption with keyword search. J. Syst. Softw., vol. 85, no. 3, pp. 643–654, 2012.
Xiaodong Lin, Rongxing Lu. Proxy re-encryption with delegatable verifiability. in Proc. Australia. Conf. Inf. Secur. Privacy, 2016, vol. 9723, pp. 120–133.
Xiaoyu. Zhu, Qin Liu. A novel verifiable and dynamic fuzzy keyword search scheme over encrypted data in cloud computing. Proc. IEEE Trustcom/BigDataSE/ISPA, Aug. 2017, pp. 845–851.
Xin Jin, Ram Krishnan. A Unified Attribute-Based Access Control Model Covering DAC, MAC and RBAC. DBSec 2012, LNCS 7371, pp. 41–55.
Xinrui Ge, Jia Yu, Chengyu Hu. Enabling Efficient Verifiable Fuzzy Keyword Search Over Encrypted Data in Cloud Computing. IEEE ACCESS, VOLUME 6, 2018.
Xueqiao Liu, Guomin Yang. Multi-user Verifiable Searchable Symmetric Encryption for Cloud Storage. IEEE Transactions on Dependable and Secure Computing, 2018.DOI: 10.1109/TDSC.2018.2876831.
Yanjiang Yang, Joseph K Liu, Kaitai Liang. Extended proxy-assisted approach: Achieving revocable fine-grained encryption of cloud data," in Computer Security - ESORICS 2015 - 20th European Symposium on Research in Computer Security, Vienna, Austria, September 21-25, 2015.
Yu Chi Chen. SPEKS: Secure server-designation public key encryption with keyword search against keyword guessing attacks. Comput. J., vol. 58, no. 4, pp. 922–933, Apr. 2015.
Yan Zhu, Gail-Joon Ahn. Role-Based Cryptosystem: A New Cryptographic RBAC System Based on Role-Key Hierarchy. IEEE Transactions on Information Forensics and Security, Vol. 8, No. 12, December 2013.
Yan Zhu,Dijiang Huang. From RBAC to ABAC: Constructing Flexible Data Access Control for Cloud Storage Services. IEEE TRANSACTIONS ON SERVICES COMPUTING, VOL. 8, NO. 4, JULY/AUGUST 2015.
Yang Yang, Maode Ma. Conjunctive Keyword Search with Designated Tester and Timing Enabled Proxy Re-Encryption Function for E-Health Clouds. IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 11, NO. 4, APRIL 2016.
Yu Zhan, Baocang Wang. Improved Proxy Re-Encryption with Delegatable Verifiability. IEEE SYSTEMS JOURNAL. Digital Object Identifier 10.1109/JSYST.2019.2911556.
Zhangjie. Fu, Kui. Ren. Enabling Personalized Search over Encrypted Outsourced Data with Efficiency Improvement. IEEE Transactions on Parallel and Distribut ed Systems, vol. 27, no. 9, pp. 2546-2559, Sep. 2016.
Zhang Jie. Fu, Xinle. Wu. Toward Efficient Multi-keyword Fuzzy Search over Encrypted Out sourced Data with Accuracy Improvement. IEEE Transactions on Information Forensics and Security, vol. 11, no. 12, pp. 2706-2716, Dec. 2016.
Zhangjie,Fu, Xing Ming. Sun. Achieving Efficient Cloud Search Services: Multi-keyword Ranked Search over Encrypted Cloud Data Supporting Parallel Computing. IEICE Transactions on Communications, vol. E98-B, No. 1, pp.190-200, Jan. 2015.
Zhen Liu, Zhenfu Cao. White-box traceable ciphertextpolicy attribute-based encryption supporting any monotone access structures. IEEE Trans. Inf. Forensics Secur, vol. 8, no. 1, pp. 76–88, Jan. 2013.
Zhen. Liu, Zhenfu. Cao. Blackbox traceable CP-ABE: How to catch people leaking their keys by selling decryption devices on ebay. ACM SIGSAC Conf. Comput. Commun. Secur., 2013, pp. 475–486.
Zhihua Xia, Xinhui Wang. A Secure and Dynamic Multi-Keyword Ranked Search Scheme over Encrypted Cloud Data. IEEE Transactions on Parallel and Distributed Systems, vol. 27, no. 2, pp. 340-352, 2015.
Zhifeng Xiao, Yang Xiao. Security and Privacy in Cloud Computing. IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 15, NO. 2, SECOND QUARTER 2013.
Zuhua Shao. Improvement of identity-based proxy multi-signature scheme.The Journal of Systems and Software 82 (2009) 794–800.

Highlights

- We discuss the privacy security risks of cloud computing and propose a comprehensive privacy protection framework.
- We analyze the characteristics of several access control models and highlight their advantages and disadvantages based on various factors.
- We summarize the algorithm flow and development of ABE, and discuss several important achievements in cloud privacy protection, such as fine-grained, revocation mechanism, multi-authority, trace mechanism, proxy re-encryption and hierarchical encryption.
- We discuss and compare two searchable encryption schemes, such as searchable asymmetric encryption (SAE) and searchable symmetric encryption (SSE).
- We discuss and analyze the integration technology scheme of access control, trust and encryption and discuss the challenges and future research directions.

Pan Jun Sun is a PhD in information and communion system of Shanghai Jiao Tong University. He received MS degree in control theory and application from Taiyuan University of Science and Technology in 2010. His research focus on cloud computing, privacy preservation, access control and trust management. Email is “sunpanjun2008@163.com.

Declaration of interests

Dear Editors:

I would like to submit the manuscript " Security and Privacy Protection in Cloud Computing: Discussions and Challenges " to "JOURNAL OF NETWORK AND COMPUTER APPLICATIONS ". No conflict of interest exits in the submission of this manuscript, and manuscript is approved by all authors for publication. I would like to declare that the work described was original research that has not been published previously, and not under consideration for publication elsewhere, in whole or in part.

In order to better service for my article，I authorize "JOURNAL OF NETWORK AND COMPUTER APPLICATIONS " to assign the same or different reviewers. Last, thanks for the workers of editing group!

Pan jun sun, 3, 21, 2020.

Dear Editors:

I am sure to submit the manuscript “Security and Privacy Protection in Cloud Computing: Discussions and Challenges ” to “JOURNAL OF NETWORK AND COMPUTER APPLICATIONS ”. There is no conflict of interest in my submission, which has been approved and published by all authors. I state that the work described is original research that has not been published before, and that it has not been considered to be published in whole or in part elsewhere.

In order to better service for my article，I authorize “JOURNAL OF NETWORK AND COMPUTER APPLICATIONS ” to assign the same or different reviewers. Last, thanks for the workers of editing group!