IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received May 21, 2018, accepted June 24, 2018, date of publication June 29, 2018, date of current version July 30, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2851599

Accountable Privacy-Preserving Mechanism for Cloud Computing Based on Identity-Based Encryption

HONGBING CHENG[1,2], CHUNMING RONG[2], (Senior Member, IEEE), MANYUN QIAN[1], AND WEIHONG WANG[1]

[1]College of Computer Science and Technology, Zhejiang University of Technology, Hangzhou 310032, China
[2]Department of Electronic Engineering and Computer Science, University of Stavanger, 4036 Stavanger, Norway

Corresponding author: Hongbing Cheng (chenghb@zjut.edu.cn)

This work was supported in part by the National Nature Science Foundation of China under Grant 61402413 and Grant 61340058, in part by the Six Kinds Peak Talents Plan Project of Jiangsu Province under Grant 11-JY-009, in part by the European Research Project Accountability for Cloud and Other Future Internet Services, and in part by the National Nature Science Foundation of Zhejiang Province under Grant LY14F020019 and Grant LZ14F020001.

ABSTRACT Considering the openness and cross-domains of cloud computing, the traditional privacy-preserving technology cannot be applied in cloud computing efficiently. In this paper, inspired by the accountability idea, we proposed an accountable privacy-preserving mechanism based on identity-based encryption for cloud computing, which focuses on constraining the illegal network behavior by performing accountability to protect the privacy for cloud participants. First, based on the description logic, we defined the basic privacy concepts about the privacy guarantee, privacy request, privacy attribute, and privacy exposure condition for cloud system, and at the same time, the system architecture for the proposed accountable privacy-preserving mechanism is presented; second, combining the proposed accounting and auditing approaches, the integrated accountable privacy-preserving mechanism for cloud computing is proposed; and then, based on the possible two kinds adversary attacks against the proposed mechanism, the detailed security analysis and proof for the proposed mechanism are given; finally, we provide extensive experimental results and potential accountability implementation to demonstrate the efficiency of the proposed mechanism.

INDEX TERMS Privacy-preserving, accountability, trusted cloud computing, security, IBE.

I. INTRODUCTION

As a heart-stirring application paradigm, cloud computing [1] is becoming more and more popular, it has been dominant in many application areas. In order to attract the cloud users as many as possible, it has to provide the users with guaranteed quality of services which should be dynamic, reliable, secure and customizable. It is well known that, within the cloud environment, the users always can achieve adequate virtual resources, and no need to have a complete understanding of the system infrastructure and resource distribution. In such situation, cloud users are universally required to accept the underlying premise of privacy and security promise passively when they seek the services from cloud computing. Currently, many Internet users still hesitate to trust cloud computing because they think it cannot ensure the security of their data. Worst of all, the recent serious privacy problem [2] reported by NetworkWorld website make the cloud privacy issues more serious.

Till now, some related research on privacy-preserving for cloud computing have been performed, but most of the existing works red [3] mainly focused on the traditional privacy-preserving technology. Similar with the traditional web services, cloud computing are vulnerable to many types of network attacks as well, such as distributed denial of service attacks, worm attack, network sniffing and sinkhole attacks, especially, there exist some special security problem that only cloud computing must face to, and these are (1).Data integrity problem [4], [7], [10], [11]: cloud computing will delete data regularly to guarantee the continual storage service, and the data deletion may be undesirable from a user perspective, on the other side, extra copies of data are unavailable or cloud storage medias collapse will also lead to this problem. (2). Data protection problem [9], [12]: cloud computing poses several data protection risks on cloud users and providers. In some cases, it may be difficult for the cloud users to effectively check whether their data are processed in a legal way. (3). Lock in problem [6], [14]: currently, there is few efficient procedures or software which are available for could computing to protect data, application and service, and thus it is difficult for the cloud users to migrate their data among cloud service providers; and (4). Governance problem [18], [20], [23], [25]: In cloud computing infrastructures, the users are out of control to the Cloud Service Providers (CSP)and therefore some security threat will appear.

According to the above analysis, the urgent security issue about how to design the suitable technology to guarantee the privacy of cloud participants should be investigated. Inspired by the social accountability idea, we proposed the accountable privacy-preserving mechanism IBE-AC for cloud participants. In the proposed mechanism, each cloud participant registers in cloud system using their identity information, and generates private key using his/her identity information, then they can be authenticated each other based on the Auth-Encrypt and Auth-Decrypt procedures, which we redesigned from the corresponding procedure of IBE. Combining with the detailed privacy definition for cloud participants and system modeling, we proposed the accounting and auditing processes to deal with the network log files and judge whether one certain cloud participant has violated the privacy regulation. Finally, the cloud system will perform accountability on the related cloud participants according to the auditing privacy exposure results. The proposed privacy-preserving mechanism mainly focuses on regulating the network behavior of the participants in cloud computing to realize privacy-preserving. The main contribution of our paper can be summarized as follows:

- Different with the traditional privacy-preserving technology, we present the accountability system mechanism IBE-AC to protect the privacy for cloud tenants by constraining and regulating the network behavior of the cloud participants.
- Combining the IBE with the proposed accounting and auditing processes, we present the integrated accountable privacy-preserving mechanism for cloud computing. In the proposed mechanism, each registered cloud tenant associates with his/her identity information, private key and signature generated in IBE-AC system. For all modules of the proposed mechanism, the detailed processing procedures and related algorithms are designed as well. At the same time, we prove the security of the proposed mechanism under the two possible types of adversaries.
- We experimentally show that the proposed accountable mechanism performs efficiently and smoothly. In particular, the configurable function modules make the mechanism fit for different cloud application scenarios; at the same time, it is possible to achieve better performance and effectiveness through flexible distribution and agent mechanism for the function modules.

The rest of the paper is organized as follows. In Section II, related works is discussed and a systematic accountability mechanism is suggested. The preliminary, privacy and system modeling are given in Section III and Section IV respectively. In Section V, we propose the accountable privacy-preserving mechanism based on IBE, and prove the security of the mechanism under two possible adversaries attacks. An extensive experimental results and potential accountability implementation are presented in Section VI; and we conclude the paper in Section VII.

II. RELATED WORK

Recently, more and more individuals and enterprises have been inclined to place their data on the cloud platforms; accordingly, many privacy problems will also emerge. Some related privacy-preserving research in cloud computing were discussed in [3]. Most of the existing works mainly focus on the traditional privacy-preserving technology and schemes, meanwhile, some protocols, mechanisms, approach and schemes [4]–[7] are designed for privacy-preserving under different application scenarios. Pasupuleti *et al.* [4] use the probabilistic public key encryption algorithm to encrypt the cloud data before uploading, and then search the encrypted data based on some ranked keyword to retrieve the files from the cloud. In [5], to defense against the node compromise attacks in cloud computing, a novel threshold credit-based incentive mechanism (TCBI) is proposed based on the modified model of population dynamics, the difficulty of the mechanism lies in how to assess and set the credit value, which will affect the accuracy of the mechanism. Yan *et al.* [6] study a reputation mechanism to provide secure and privacy-aware communication process for the mobile cloud computing, which can identify and manage the adversary to protect the security and privacy against some attacks; and Xia *et al.* [7] proposed a privacy-preserving scheme to support content-based image retrieval (CBIR) over encrypted images, which no need to worry about leaking the sensitive information to the cloud servers, but accuracy and efficiency problem are the main drawback for the scheme.

For the privacy-preserving of cloud data, the works [8]–[11] mainly adopt related data protection technology to realize privacy-preserving in cloud computing, Yuan and Yu [8] focus on how to keep their respective data sets secretly in multi-party through conducting joint Back-Propagation neural network learning. References [9]–[12] study the topic of cloud privacy-preserving from the aspects of multi-keywords search, data sharing security and verifiable data aggregation respectively, all the schemes based on the traditional data information security technology. Considering the scale of cloud computing, these technology show lower efficiency in real cloud environment. To protect the personal health information among healthcare providers in distributed m-healthcare cloud computing system, Zhou *et al.* [14] propose a novel authorized accessible privacy model for patients to authorize physicians by setting an access tree, which can support flexible threshold predicates, in [15], a document retrieval framework was proposed to search the encrypted data which stored on the cloud, the frame can guarantee the confidentiality of the original data. And the deployed privacy-preserving n-keyword search scheme will protect the privacy of the data during searching and retrieving. In [16] and [17], encryption technology are designed to protect the cloud privacy, especially in [17], multi-key ensures the difficulty for adversary to decrypt the data encrypted by the owners, but evidently, the drawback of the scheme is that it will introduce more complexity to the cloud system. For the trusted cloud computing, Zhang *et al.* [18] present an online auction for cloud computing based on heterogeneous demands of cloud tenants, which mainly adopt some authenticated technology to guarantee the tenants privacy. At the same time, the references of [19]–[22] study the public auditing in cloud computing under different aspects. Actually, the public auditing always need public infrastructure to support and therefore sometimes is in low efficiency.

As a new computing paradigm, cloud computing is very different from the traditional network in system architecture and service deployment. Currently, there are some special security issues [23] in cloud computing except for some common security issues which are similar with the traditional internet technology, for example, in the security of boundary, cloud computing cannot be clearly defined boundaries to protect the device users, however, the traditional computing model can protect device users by dividing physical and logical security zones. In the service security aspect [24], the data, communications networks, services and other important resource are controlled by the cloud service providers. So, when the providers security is something wrong, how to ensure the available service and the data confidentiality are particularly important. Related to the protection of users data [25], we have to consider the stored location and approach for data; at the same time, data recovery, data encryption and data integrity protection are important topics as well. At the same time, in cloud computing model [25], the cloud service providers have too much privilege; however, the users rights may be difficult to ensure. Therefore, how to balance the rights between the cloud service providers and cloud users becomes a challenge.

From the above analysis of the related works, we can conclude that these existing security approaches always focus on the traditional security technology, and sometimes these approaches cannot efficiently solve the privacy-preserving problems in cloud computing. Inspired by the social accountability mechanism, in this paper, combining with Identity-based Encryption algorithm, we constructed a systematic accountable mechanism for cloud computing to make each cloud participant to act properly and legally. Actually, the concept of ''accountability'' in network security has emerged for a long time, the papers [26], [27] mentioned that the colorredaccountability will be an potential efficient approach to apply in privacy-preserving, and the authors suggested that accountability will be likely to become an efficient approach in cloud computing and which will help increase trust for it, at the same time, the accountability mechanism will make all cloud participants act properly during their network activities.

III. PRELIMINARY

A. DESCRIPTION LOGIC

Description logic is a formal language for knowledge representation [28]. It is a set of stator belongs to first-order predicate logic. The basic components of the description logics are concepts, roles, and individuals. The concept describes the common attributes of an individual set, and the concept can be interpreted as an object set of a meta predicate, the role is the binary relation between objects.

Knowledge Representation can be divided into two categories: one is Logic-Based Knowledge Representation, another is non-Logic-Based Knowledge Representation. Logic-Based Knowledge Representation is usually a variation of the first order predicate logic. Reasoning is equivalent to proving logical inference. Non-Logic-Based Knowledge Representation: it is usually based on the use of a graphical interface. Knowledge is represented by a particular data structure, and reasoning can be done simply by processing the special process of the structure. The description logic knowledge representation system contains a knowledge base and its reasoning services. Knowledge base consists of two parts: Tbox and Abox. Tbox introduces the terminology of application; Abox includes instance assertion and role assertion.

In the description logic, the basic description language is ALC, which is a fundamental and special language, can be extended from Description logics(DL). Generally, we will let A and B denote the atomic concept, R denote the atomic relationship, C and D denote concept description, I is the explanation. The basic operations, syntax and semanticists of ALC are shown in Table 1.

TABLE 1. The grammar and semantics Of ALC.

Operation	Syntax	Semantics
Atomic concept	A	$A^I \subseteq \Delta^I$
Atomic relation	R	$R \subseteq \Delta^I \times \Delta^I$
Conjunction	$C \cap D$	$C^I \cap D^I$
Disjunction	$C \cup D$	$C^I \cup D^I$
Negation	$\neg C$	$\Delta^I \backslash C$
Existential Restrictions	$\exists R.C$	$\{x \vert \exists y.(x,y) \in R^I$, and $y \in C^I\}$
Global Restrictions	$\forall R.C$	$\{x \vert \forall y.(x,y) \in R^I$, then $y \in C^I\}$
Top	$\top$	Δ^I
Bottom	$\perp$	Ø

In ALC, syntax based on operation, atomic concept and atomic relation to construct complex concepts and relations. The basic operations include conjunction, disjunction, negation, existential restrictions and global restrictions. The semantics is a subset of a certain field, relation is the binary relation in the field set. Tbox contains the intentional knowledge of application. It usually describe the fact of concepts and tasks by terminological axioms. There are two forms of terminological axioms: Inclusion: C $\in$ D(R $\in$ S), e.g. Women $\in$ Human; Equality: C $\equiv$ D(R $\equiv$ S), e.g. Mother $\equiv$ Woman $\cap\exists$ hasChild.Person, C and D are the concept, R and S are the relation. An interpretation(I) consists of a non empty set (ΔI) and a function $(\cdot I)$, it can be denoted as $I = (\Delta I, \cdot I)$. For an interpretation I, if $C^I \subseteq D^I (C^I \equiv D^I)$, then I satisfies inclusion or equality, C ⊆ D(C ≡ D). If T is an axiom(a set of axioms), if and only if I satisfies every axiom in the set, then I satisfies T, and I is a pattern of the axiom(a set of axioms). More detail of the description logic can be referred in [28].

B. BILINEAR MAP AND THE IBE SCHEME

1) BILINEAR MAP

From here on, Zq is used to denote the group $\{0, \ldots, q-1\}$ under addition modulo q. For a group G of prime order we use G^* to denote the set $G^* = G|O$, where O is the identity element in the group G. We use Z and $Z+$ to denote the set of integers and positive integers respectively. We describe first some definitions [13] about bilinear map and then the IBE scheme.

Definition 1: An map $\hat{e}$:$G_1 \times G_1 \to G_2$ is called a bilinear pairing if, for all $x, y \in G_1$ and all $a, b \in Z$, we have $\hat{e}(x^a, y^b) = \hat{e}(x, y)^{ab}$.

Definition 2: The Bilinear-Diffie-Hellman problem (BDH) for a bilinear map $\hat{e}$:$G_1 \times G_1 \to G_2$ such that $|G_1| = |G_2| = q$ is prime can be defined as follows: given $g, g^a, g^b, g^c \in G_1$, compute $\hat{e}(g, g)^{abc}$, where g is a generator and $a, b, c \in Z$. An algorithm $\mathcal{A}$ is said to solve the BDH problem with advantage ε if $Pr[\mathcal{A}(g, g^a, g^b, g^c) = \hat{e}(g, g)^{abc)}] \geq \varepsilon$, Where the probability is over the random choice of a, b, c, g, and the random bits of $\mathcal{A}$.

Definition 3: A randomized algorithm $\mathcal{G}$ that takes a security parameter $k \in Z^+$ as input is a BDH parameter generator if it turns in time polynomial in k and outputs the description of two groups G_1, G_2 and a bilinear function $\hat{e}$:$G_1 \times G_1 \to G_2$, with $|G_1| = |G_2| = q$ for some prime q. The output of the algorithm is denoted by $\mathcal{G}(1^k) = \langle G_1, G_2, \hat{e}, q \rangle$.

2) IDENTITY-BASE ENCRYPTION(IBE)

The identity-based cryptography mainly includes four algorithm operations, Setup, Extract, Encrypt and Decrypt. It is worthwhile to mention that the identity-based cryptography is able to use any string as a public key, which is very convenient and practical in modern society. The four algorithm operations are specified as follows.

Setup(η): the algorithm takes a security parameter η as input and returns system parameters *SP* and master-key *MK*. *SP* includes the description of a finite message space M and a finite cipher text space *C*. The system parameters is public, while the master-key will be kept secretly at PKG.

KeyG(*SP*, *MK*, ID): the algorithm will input system parameters *SP*, master-key *MK*, and an arbitrary identity ID∈ $\{0, 1\}^*$, then outputs the corresponding private key *SK* for the input identity.

Encrypt(*SP*, ID, m): the encryption algorithm is run by sender, will take system parameters *SP*, receiver‘s identity ID and the plaintext m∈M as input. It returns the ciphertext c∈C.

Decrypt(*SP*, c, *SK*): Correspondingly, the decryption algorithm takes system parameters *SP*, the ciphertext c∈C, and the receivers private key *SK* as input. It output the plaintext m∈M or an error.

These algorithms in IBE scheme must satisfy the standard definition of consistency constraint, that is, when the algorithm KeyG generated a private key *SK* by the given ID which is the public key, then ∀m∈M: Decrypt (*SP*, c, *SK*) = m, where c = Encrypt(*SP*, ID, m).

IV. PRIVACY AND SYSTEM MODELING

A. PRIVACY MODELING

In this section, based on the description logic, we will define and model the privacy attribute, privacy request and privacy exposure condition for cloud participants. In order to describe and identify the privacy attribute of the cloud computing. In this paper, the cloud participants include cloud service providers and cloud tenants. Modeling and description of the cloud privacy consists of privacy guarantee of cloud service system (PG-CSS), Certificate Authority Statement(CAS), privacy attribute of providers or tenants(PA-P or PA-T), privacy request of providers or tenants(PR-P or PR-T), Privacy Guarantee of Providers(PG-P) and Privacy Exposure Condition of Providers or tenants(PEC-P or PEC-T). The relation of the privacy concepts is briefly shown in Fig.1.

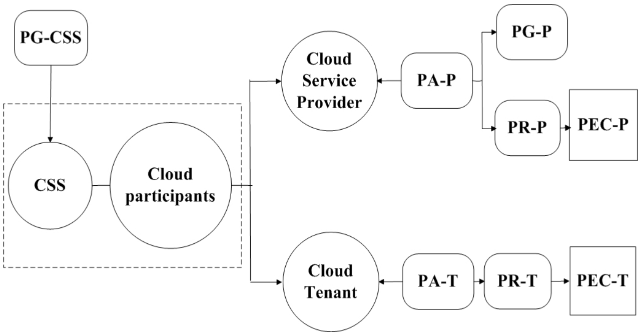


FIGURE 1. The modeling relation of the privacy for cloud participants.

Definition 4: Privacy Guarantee of Cloud Service System, PG-CSS. It is designed to protect the privacy of all users in the cloud system. And it can be described as follows:$PG\text{-}CSS = \langle Security, Result \rangle$.

Where, Security refers to the cloud service systems security, which can be denoted as:Security = {IBE-AC, Authentication}. Anyone must be authenticated when he/she joins in the cloud service system. Penalty refers to the punishment regulation what we will design for the proposed accountability system. It can be denoted as:Penalty = {0,1}, 0 means the participant has not violated the privacy regulation, but 1 means it has.

Definition 5: Privacy Attribute of Cloud Participants. Privacy Attribute of Cloud Service Providers(PA-P) is represented by a quaternion, $PA\text{-}P = \langle Pid, PEC\text{-}P, PG\text{-}P, Signature \rangle$. Where, Pid is the identity of privacy attribute owner, which will be used to identify the cloud service provider, PEC-P is the privacy exposure condition of cloud service provider, PG-P is privacy guarantee of cloud service provider, and Signature is the provider's digital signature.

Similarly, Privacy Attribute of Cloud Tenant(PA-T) can be represented by a triad as $PA\text{-}T = \langle Tid, PEC\text{-}T, Signature\rangle$, where, Tid represents the identity of the privacy owner, which will identify the cloud tenant. PEC-T denotes the privacy exposure condition of cloud tenant. And Signature is the digital signature of cloud tenants.

Definition 6: Certificate Authority Statement(CAS). Authorization is a part of the privacy exposure condition of the cloud service providers, that is, each privacy exposure must satisfy the CAS to verify that whether the cloud tenant owns this privacy.

CAS can be expressed as:$CAS = CA \xrightarrow{ServerJudge} user$

Where, CA refers to Certificate Authority, and usually is the trusted third party. ServerJudge is the operation of the Certificate Authority, according to its Signature, to judge whether a user is a legal participant in cloud service system.

Definition 7: Privacy Exposure Condition of Cloud Service Providers (PEC-P). $PEC\text{-}P = privacyConstr \wedge P - objectConstr$. The privacy exposure condition is a constraint on a cloud tenant to have a privacy attribute, where, privacyConstr represents the constraint on the content of the privacy requirement, and P-objectConstr represents the constraint on the private cloud tenant, when the object is legal, P-objectConstr can be noted as $P - objectConstr = CA \xrightarrow{ServerJudge} participant = CAS$.

The judgment statement is:

$PEC\text{-}P = CAS?privacyConstr : refuse$

When the CAS has authenticated the users to be legal cloud participants, it will expose related privacy to the cloud participants based on the privacyConstr, otherwise it will reject the requests of the users. PrivacyConstr mainly involved the issues about whether the cloud tenants owned the privacy, and the constraints on the privacy privilege management for the cloud tenants. And privacyConstr can be noted as:

$$\begin{aligned} &privacyConstr \\ &= C(pn_1 : \{T_1, T_2, \ldots, T_m\}, \ldots, pn_i : \{T_1, T_2, \ldots, T_n\}) \\ &\quad \wedge C(pn_1 : T_1(am_1), \ldots, pn_i : T_s(am_q)) \end{aligned}$$

Where C is the class of privacy; pn_i are the name of privacy; pn_1:$\{T_1, T_2, \ldots, T_m\}$, ..., pn_i:$\{T_1, T_2, \ldots, T_n\}$ indicates which cloud tenants own the related privacy; pn_1:$T_1(am_1), \ldots, pn_i$:$T_s(am_q)$ denotes the management privilege on the related privacy for the cloud tenants.

For example, as the cloud tenant Tim, delivery company and the cloud service provider Taobao, we assume the tenant wants to sell his idle entity albums on Taobao, the privacy exposure condition to tenants address in Taobao is the seller, Tims address should only be exposed to the delivery company. Then Tims privacy exposure condition is shown as address:$dilivery\ company \wedge address$:$save(am)$. it means that the delivery company owns the privacy of address, at the same time, the delivery company has the management privilege to save the address.

Definition 8: Privacy Guarantee of Cloud Service Providers(PG-P). It refers to the cloud service providers guarantee to protect the privacy for other cloud participants, it can be denoted as: $PG\text{-}P = \langle QoS, SPS\rangle$.

Where, QoS refers to the quality of service of the cloud providers, for simplicity, in the proposed accountability system, we assume that Qos = {Availability,Sustainability}. Availability is the measure for the available resources that the cloud service providers can provide, Sustainability indicates the sustainable resource of the providers, and SPS refers to the security probability of service from the providers.

Definition 9: Privacy Attribute of Cloud Tenant(PA-T). Privacy attribute of cloud tenants can be represented by a triad as $PA - T = \langle Pid, PEC - T, Signature\rangle$.Where, Tid represents the identity of the privacy owner, which will identify the cloud tenant. PEC-T denotes the privacy exposure condition of cloud tenant. And Signature is the digital signature of cloud tenants.

Definition 10: Privacy Exposure Condition of Cloud Tenants(PEC-T). Different with PEC-P, PEC-T is the constraint of exposing privacy to the cloud service providers. In the proposed accountability system, the PEC-T will be denoted as: $PEC\text{-}T = DC \wedge privacyConstr$. There are two parts for the PEC-T, one is DC, which means the degree of confidence of cloud tenants to the service or the cloud service providers, another is the constraint of privacy request privacyConstr. We define DC = {Security,Qos}, where, Security denotes the security probability of cloud service, and QoS is the quality of cloud service, it represents the reliability and efficiency of the cloud service. At the same time, privacyConstr mainly involves the issues about whether the cloud service providers owned the privacy, and the constraints on the privacy privilege management for the cloud service providers, and privacyConstr can be noted as:

$$\begin{aligned} &privacyConstr \\ &= C(pn_1 : \{P_1, P_2, \ldots, P_x\}, \ldots, pn_i : \{P_1, P_2, \ldots, P_y\}) \\ &\quad \wedge C(pn_1 : P_1(am_1), \ldots, pn_i : P_r(am_t)) \end{aligned}$$

Where C is the class of privacy; pn_i are the name of privacy; pn_1: $\{P_1, P_2, \ldots, P_x\}$, ..., pn_i:$\{P_1, P_2, \ldots, P_y\}$ indicates which cloud service providers own the related privacy; pn_1:$P_1(am_1)$, ..., pn_i:$P_r(am_t)$ denotes the management privilege on the related privacy of the cloud service providers.

Definition 11: Privacy Request (PR), it represents a series of requirements to protect cloud participants privacy, and PR can be described by the list of PEC, we note it as $PR = (PEC)_1 \wedge (PEC)_2 \wedge \cdots \wedge (PEC)_x$. For example, the privacy request of cloud service providers can be described as: $PR\text{-}P = (PEC\text{-}P)_1 \wedge (PEC\text{-}P)_2 \wedge \cdots \wedge (PEC\text{-}P)_i$, and the privacy request of cloud tenants can be described as: $PR\text{-}T = (PEC\text{-}T)_1 \wedge (PEC\text{-}T)_2 \wedge \cdots \wedge (PEC\text{-}T)_j$.

B. SYSTEM MODEL

We present the model for accountable privacy-preserving mechanism in Fig 2, where, cloud participants include cloud users and cloud service providers, compared with the traditional cryptograph technology, the IBE scheme can generate the corresponding private key for any users when they input any random string as their public key. Accordingly, the functions of authentication and authorization are designed based on IBE scheme in the proposed accountability infrastructure, at the same time, auditing and accounting will be introduced to construct the entire accountability system. Actually, all cloud participants will register in the IBE-AC system and all of their network behavior will be storied in the network logs. When privacy accountability launched, the accountability system will perform the related function modules and make decisions according to the accounting results. Though there are many details about the deployment of the of accountability system, in this paper, we logically take it as cloud server, and mainly focus on the coordination and interaction agreements of the function modules for the accountability system.

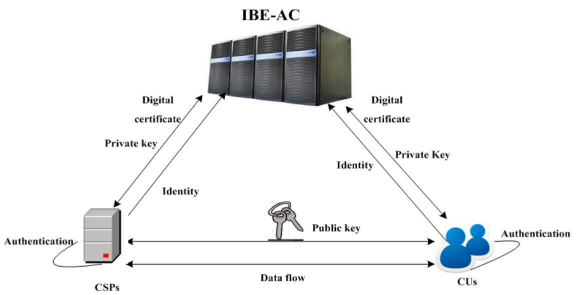


FIGURE 2. The IBE-AC system model.

In the proposed accountability system model, we will define the proposed accountable IBE scheme. Compared with the traditional IBE scheme, the Encrypt and Decrypt steps will be redefined to realize the authentication process for the accountability system between any two cloud participants.

- Auth-Encrypt(SP, ID_r, m, SK_s): The auth-encryption algorithm run by the sender will take system parameters SP, receiver‘s identity ID_r, sender‘s private key SK_s and the plaintext $m \in M$ as input. It returns the ciphertext $c \in C$.
- Auth-Decrypt(SP, c, SK_r, ID_s): The auth-decryption algorithm run by the receiver will take as input- system parameters SP, the ciphertext which generated in Auth-Encrypt under ID_r, the identity ID_s of the sender, the receiver‘s private key SK_r, it will output: the corresponding original plaintext $m \in M$.

According to the consistency constraint of IBE scheme, we also require the above two authenticated algorithms to satisfy the standard consistency constraint. Therefore, for the messages $m \in M$, for any pair cloud participants P1 and P2, their private keys SK_s, SK_r and with their corresponding identity ID_s and ID_r, it requires that: Authenticated-Encrypt (M, SK_s, ID_r)=Authenticated-Encrypt(M, ID_s, SK_r). Although the authenticated-encryption can perform authentication mechanism, it is faster than plain Encryption algorithm because it has less exponentiation and no point multiplication operations. In addition, we will introduce the signature algorithm based on IBE and another two operations which are introduced to realize the network behavior accounting and auditing for the proposed accountability system.

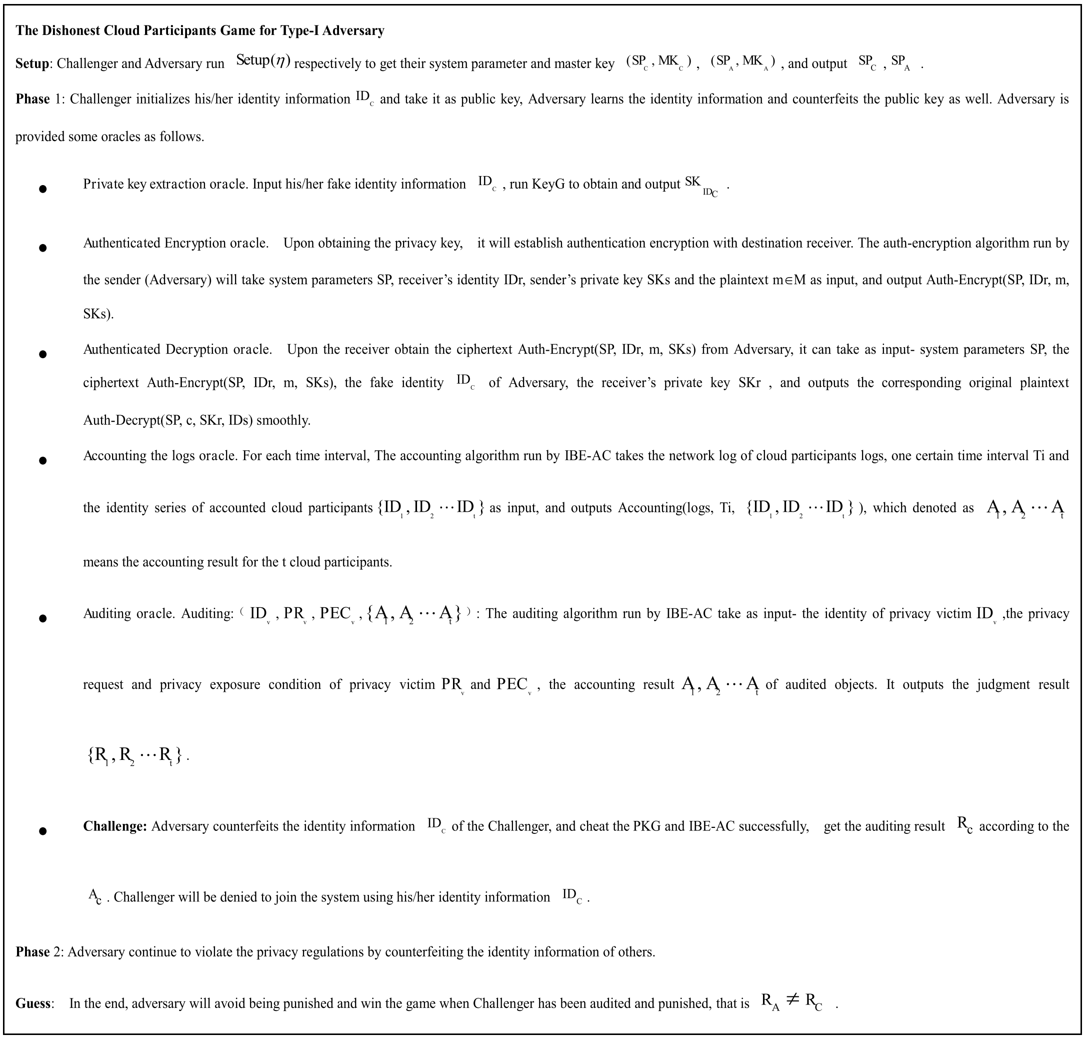
- Signature(SP, m, SK): The signature algorithm takes the system parameters SP, the private key SK of the signer and a message m as input, and outputs the signature associated with the message.
- Accounting(T_i, $\{Pri\text{-}log_{ID_1}, Pri\text{-}log_{ID_2} \cdots Pri\text{-}log_{ID_t}\}$): For simplicity, in this paper, we only consider the privacy-related logs for cloud participants, the accounting algorithm run by IBE-AC takes the privacy related network log set $\{Pri\text{-}log_{ID_1}, Pri\text{-}log_{ID_2}, \ldots, Pri\text{-}log_{ID_t}\}$ of cloud participants, one certain time interval T_i as input. For simplicity, in this paper, we only consider the privacy-related logs for cloud participants, the log format of cloud tenant and cloud service provider will be defined as $Pri\text{-}log_T = \{ID_T, Ti, PEC\text{-}T, PR\text{-}T, PA\text{-}T, PG\text{-}P\}$ and $Pri\text{-}log_P = \{ID_P, Ti, PEC\text{-}P, PR\text{-}P, PA\text{-}P, CAS\}$ respectively, and finally it will output the corresponding accounting result $A_1, A_2 \cdots A_t$ for the t cloud participants.
- Auditing:($ID_v, PR_v, PEC_v, \{A_1, A_2 \cdots A_t\}$): The auditing algorithm run by IBE-AC take as input- the identity of privacy victim ID_v,the privacy request and privacy exposure condition of privacy victim PR_v and PEC_v, the accounting result $\{A_1, A_2 \cdots A_t\}$ of audited objects. It outputs the judgement result $\{R_1, R_2 \cdots R_t\}$, for simplicity, in the paper, we define the value of R as 0 or 1, which means whether the corresponding cloud participant has violated the privacy regulation of the victim.

V. THE PROPOSED ACCOUNTABLE SCHEME

A. SECURITY DEFINITIONS

In the proposed accountable privacy-preserving model, IBE-AC is assumed to be semi-trusted, and it will be attacked by dishonest cloud participants which will try to avoid being punished. Therefore, according to the motivation and possibility, two types of adversaries may emerge in the accountable privacy-preserving scheme, which can be described as follow.

- *Type − I adversary*. This kind adversary as the dishonest cloud participants which always deliberately aim to violate the privacy regulations. Therefore, an easy way they can utilize is to counterfeit the identities of others, such adversaries will try to obtain the useful private information from others before being audited. Thus, by counterfeiting others information, the adversary will avoid being punished even having violated the privacy regulations.
- *Type − II adversary*. This kind adversary as the dishonest cloud participants which have violated the



The Dishonest Cloud Participants Game for Type-I Adversary

Setup: Challenger and Adversary run $\mathrm{Setup}(\eta)$ respectively to get their system parameter and master key (SP_c, MK_c), (SP_A, MK_A), and output SP_C, SP_A .

Phase 1: Challenger initializes his/her identity information ID_c and take it as public key, Adversary learns the identity information and counterfeits the public key as well. Adversary is provided some oracles as follows.

- Private key extraction oracle. Input his/her fake identity information ID_c , run KeyG to obtain and output SK_{ID_C} .
- Authenticated Encryption oracle. Upon obtaining the privacy key, it will establish authentication encryption with destination receiver. The auth-encryption algorithm run by the sender (Adversary) will take system parameters SP, receiver's identity IDr, sender's private key SKs and the plaintext m∈M as input, and output Auth-Encrypt(SP, IDr, m, SKs).
- Authenticated Decryption oracle. Upon the receiver obtain the ciphertext Auth-Encrypt(SP, IDr, m, SKs) from Adversary, it can take as input- system parameters SP, the ciphertext Auth-Encrypt(SP, IDr, m, SKs), the fake identity ID_c of Adversary, the receiver's private key SKr , and outputs the corresponding original plaintext Auth-Decrypt(SP, c, SKr, IDs) smoothly.
- Accounting the logs oracle. For each time interval, The accounting algorithm run by IBE-AC takes the network log of cloud participants logs, one certain time interval Ti and the identity series of accounted cloud participants $\{ID_1, ID_2 \cdots ID_t\}$ as input, and outputs Accounting(logs, Ti, $\{ID_1, ID_2 \cdots ID_t\}$), which denoted as $A_1, A_2 \cdots A_t$ means the accounting result for the t cloud participants.
- Auditing oracle. Auditing: (ID_v , PR_v , PEC_v , $\{A_1, A_2 \cdots A_t\}$) : The auditing algorithm run by IBE-AC take as input- the identity of privacy victim ID_v ,the privacy request and privacy exposure condition of privacy victim PR_v and PEC_v , the accounting result $A_1, A_2 \cdots A_t$ of audited objects. It outputs the judgment result $\{R_1, R_2 \cdots R_t\}$.
- **Challenge:** Adversary counterfeits the identity information ID_c of the Challenger, and cheat the PKG and IBE-AC successfully, get the auditing result R_c according to the A_c . Challenger will be denied to join the system using his/her identity information ID_C .

Phase 2: Adversary continue to violate the privacy regulations by counterfeiting the identity information of others.

Guess: In the end, adversary will avoid being punished and win the game when Challenger has been audited and punished, that is $R_A \neq R_C$.

FIGURE 3. **The dishonest cloud participants game for type-I adversary.**

privacy regulations. To avoid being punished, one or more of the dishonest cloud participants will launch collusion attack to the system. Such attack may collapse the IBE-AC or counterfeit the identity of the legal cloud participants. Generally, considering the robustness and security mechanism, IBE-AC failure is a small probability affair. Therefore, in order to avoid such attack, we must restrict when $ID_i \neq ID_j$ when $i \neq j$.

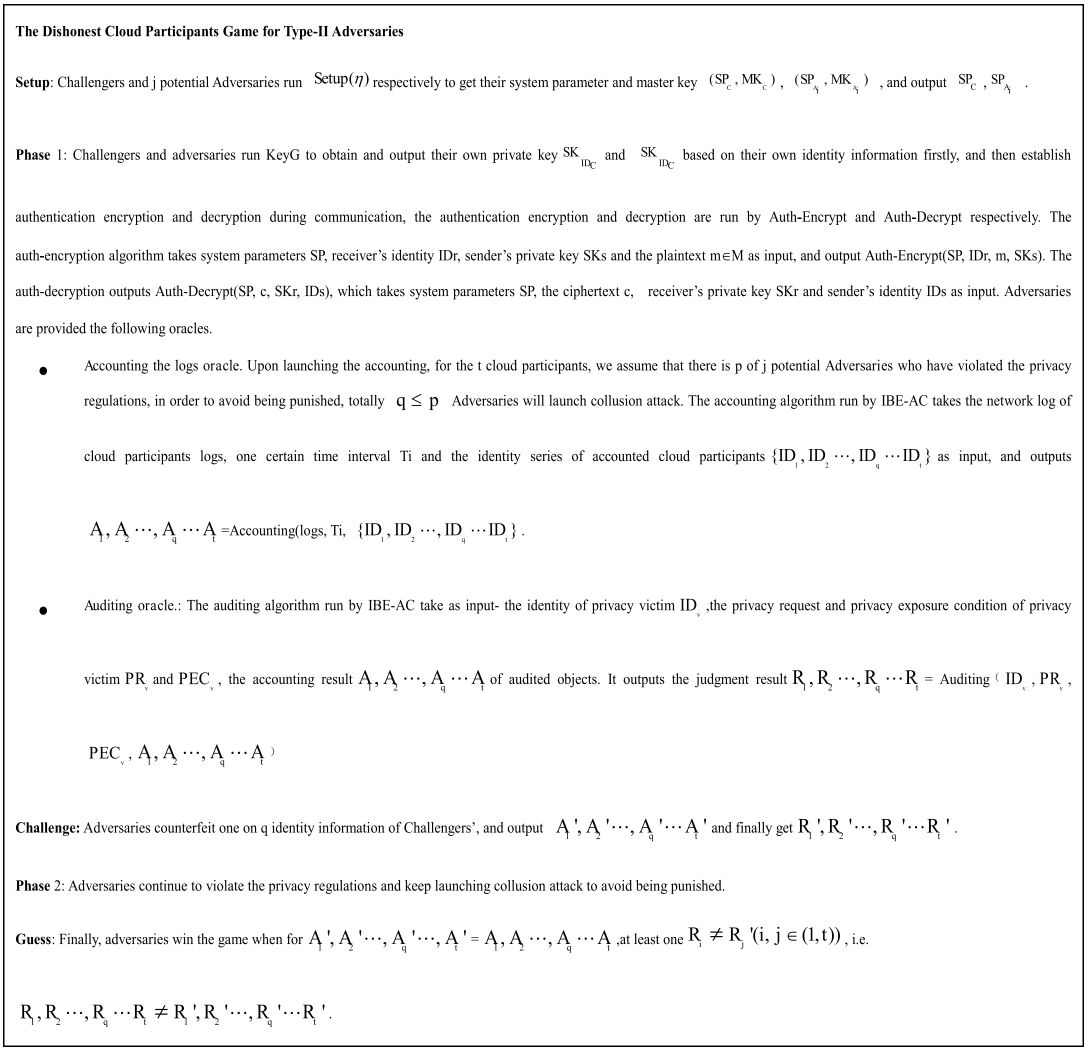
Based on the above intuitions, we will define the dishonest cloud participants game for type-I and type-II adversaries for the game story in Fig 3 and Fig 4 respectively. Suppose $\mathcal{R_I}$ and $\mathcal{R_{II}}$ represent the type-I and type-II adversary, and their advantage in attacking the accountable privacy-preserving scheme based on IBE ε can be defined as $Adv_{\varepsilon,\mathcal{R_I}}(\eta) = |Pr[R_A \neq R_C]$-$\frac{1}{2}|$ and $Adv_{\varepsilon,\mathcal{R_{II}}}(\eta) = |Pr[R_1, R_2 \cdots R_q \cdots R_t \neq R'_1, R'_2 \cdots R'_q \cdots R'_t]$-$\frac{1}{2}|$ respectively.

Definition 12: An identity-based authenticated encryption with accountable privacy-preserving scheme is semantically secure against adaptive chosen-plaintext attack (IND-ID-CPA) if no polynomially bounded adversary (adversaries) has(have) a non-negligible advantage against challenger in dishonest cloud participants game for both type-I and type-II adversaries.

For the proposed scheme, beyond the CPA security, it can be specified that 1) An identity-based authenticated encryption with accountable privacy-preserving scheme is IND-ID-CPA (semantically secure against adaptive chosen-plaintext attack) secure if no polynomial time adversary (adversaries) has(have) non-negligible advantage in the modified games for both type-I and type-II adversaries, in type-II adversaries, the encryption and decryption oracle in both phases are removed; 2) An identity-based authenticated encryption with accountable privacy-preserving scheme is secure in any model for type-I adversary, but in selective model for type-II adversaries, in which the challenge identities is submitted before setup.

B. THE PROPOSED ACCOUNTABLE SCHEME

Before joining in the cloud system, the users will register in the IBE-AC system, and they will be authenticated each other during communication. When accountability launched,



The Dishonest Cloud Participants Game for Type-II Adversaries

Setup: Challengers and j potential Adversaries run $\mathrm{Setup}(\eta)$ respectively to get their system parameter and master key (SP_c, MK_c), (SP_{A_i}, MK_{A_i}), and output SP_C, SP_{A_i}.

Phase 1: Challengers and adversaries run KeyG to obtain and output their own private key SK_{ID_C} and SK_{ID_C} based on their own identity information firstly, and then establish authentication encryption and decryption during communication, the authentication encryption and decryption are run by Auth-Encrypt and Auth-Decrypt respectively. The auth-encryption algorithm takes system parameters SP, receiver's identity IDr, sender's private key SKs and the plaintext m∈M as input, and output Auth-Encrypt(SP, IDr, m, SKs). The auth-decryption outputs Auth-Decrypt(SP, c, SKr, IDs), which takes system parameters SP, the ciphertext c, receiver's private key SKr and sender's identity IDs as input. Adversaries are provided the following oracles.

- Accounting the logs oracle. Upon launching the accounting, for the t cloud participants, we assume that there is p of j potential Adversaries who have violated the privacy regulations, in order to avoid being punished, totally $q \le p$ Adversaries will launch collusion attack. The accounting algorithm run by IBE-AC takes the network log of cloud participants logs, one certain time interval Ti and the identity series of accounted cloud participants $\{ID_1, ID_2 \cdots, ID_q \cdots ID_t\}$ as input, and outputs

  $A_1, A_2 \cdots, A_q \cdots A_t$ =Accounting(logs, Ti, $\{ID_1, ID_2 \cdots, ID_q \cdots ID_t\}$.

- Auditing oracle.: The auditing algorithm run by IBE-AC take as input- the identity of privacy victim ID_v ,the privacy request and privacy exposure condition of privacy victim PR_v and PEC_v, the accounting result $A_1, A_2 \cdots, A_q \cdots A_t$ of audited objects. It outputs the judgment result $R_1, R_2 \cdots, R_q \cdots R_t$ = Auditing (ID_v, PR_v,

  PEC_v, $A_1, A_2 \cdots, A_q \cdots A_t$)

Challenge: Adversaries counterfeit one on q identity information of Challengers', and output $A_1', A_2' \cdots, A_q' \cdots A_t'$ and finally get $R_1', R_2' \cdots, R_q' \cdots R_t'$.

Phase 2: Adversaries continue to violate the privacy regulations and keep launching collusion attack to avoid being punished.

Guess: Finally, adversaries win the game when for $A_1', A_2' \cdots, A_q' \cdots, A_t' = A_1, A_2 \cdots, A_q \cdots A_t$,at least one $R_i \ne R_j'(i, j \in (1,t))$, i.e.

$R_1, R_2 \cdots, R_q \cdots R_t \ne R_1', R_2' \cdots, R_q' \cdots R_t'$.

FIGURE 4. The dishonest cloud participants game for type-II adversaries.

the accounting and auditing processes will be executed. The detailed accountable privacy-preserving scheme is described as follows.

- Setup(η): Taking η as input, the setup algorithm is run by PKG to generate a prime q, two groups G_1, G_2 of order q, and an admissible bilinear map $\hat{e}$:$G_1 \times G_1 \to G_2$. It selects a random $\alpha \in G_1$ as well as two random integer s and x, $s, x \in Z_q^*$ and set $\beta = \alpha^s$. Then, PKG choose cryptographic hash functions for some n, H_1:$\{0, 1\}^* \times G_2 \to G_1^*$, H_2:$G_2 \to \{0, 1\}^n$, H_3:$\{0, 1\}^n \times \{0, 1\}^n \to Z_q^*$, H_4:$\{0, 1\}^n \to \{0, 1\}^n$. Finally, the output system parameters are $SP = \{q, G_1, G_2, \hat{e}, n, \alpha, \beta, H_1, H_2, H_3, H_4\}$. The master key is $MK = s$.
- KeyG(SP, MK, ID): For each cloud participant's private key request on identity $ID \in 0, 1^*$, the KeyG algorithm computes $Q_{ID} = H_2(ID) \in G_1^*$ and outputs the private key SK to be $SK_{ID} = x + x_i + (Q_{ID})^S = x + x_i + (H_2(ID))^S$, where, x is a random number generated in Setup algorithm, x_i is a random parameter for the private key of cloud participant, which is generated by and kept secretly in the IBE-AC.
- Auth-Encrypt(SP, ID_r, m, SK_s): Suppose a cloud participant wants to encrypt the message m under his/her own private key SK_s, the receiver's identity ID_r. He/She chooses a random $\mu \overset{R}{\leftarrow} \{0, 1\}^n$, and then computes $r = H_3(\mu, m)$ and $v = \hat{e}(SK_s, H_2(ID_r))$,finally, outputs the ciphertext

$$\begin{aligned} c &= \langle r, \mu \oplus H_1(r, v), H_4(\mu) \oplus m \rangle \\ &= \langle H_3(\mu, m), \mu \oplus H_1(r, v), H_4(\mu) \oplus m \rangle \\ &= \langle H_3(u, m), \mu \oplus H_1(H_3(u, m), \\ &\quad \times \hat{e}(SK_s, H_2(ID_r))), H_4(\mu) \oplus m \rangle \end{aligned}$$

- Auth-Decrypt(SP, c, SK_r, ID_s): Let c follow the $\langle U, V, W \rangle$ style, for the above ciphertext c, $U = H_3(\mu, m)$, $V = \mu \oplus H_1(H_3(\mu, m)), \hat{e}(SK_s, H_2(ID_r)))$ and $W = H_4(\mu) \oplus m$. Suppose that the ciphertext c is encrypted using the sender's SK_s and the receiver's identity ID_r, the receiver has his/her own private key SK_r. Firstly, he/she will compute $s = \hat{e}(H_2(ID_s), SK_r)$, $\sigma = H_1(U, s)$, and then recover the plaintext as follows:

$$\begin{aligned}
m &= \langle W \oplus H_4(\sigma)\rangle \\
&= \langle W \oplus H_4(V \oplus H_1(U, s))\rangle \\
&= \langle W \oplus H_4(V \oplus H_1(U, \hat{e}(H_2(ID_s)), SK_r))\rangle \\
&= \langle H_4(\mu) \oplus m \oplus H_4(\mu \oplus H_1(H_3(\mu, m), \\
&\quad \times \hat{e}(SK_s, H_2(ID_r))) \oplus H_1(H_3(\mu, m), \\
&\quad \times \hat{e}(H_2(ID_s), SK_r))\rangle \\
&= m
\end{aligned}$$

Check that $U = H_3(\sigma, m)$, if not, reject the ciphertext and its sender, otherwise, outputs the plaintext m and authenticates the sender.

- Accounting(Ti, $\{Pri\text{-}log_{ID_1},\ Pri\text{-}log_{ID_2} \cdots Pri\text{-}log_{ID_t}\}$): Before launching accountability, the IBE-AC runs accounting algorithm to collect and process the privacy involved network log of cloud participants during one certain period Ti. For simplicity, in this paper, we only consider the privacy-related records for cloud participants, According the cloud privacy definition in Section 4.1, the privacy-related format of cloud tenant is defined as:

$$\begin{aligned}
&Pri - log_T \\
&= \{ID_T, Ti, PEC\text{-}T, PR\text{-}T, PA\text{-}T, PG\text{-}P\} \\
&= \{ID_T, Ti, DC \wedge privacyConstr, \\
&= (PEC\text{-}T)_1 \wedge (PEC\text{-}T)_2 \cdots \wedge (PEC\text{-}T)_j, \\
&= \langle ID_T, PEC\text{-}T, Signature\rangle, PG\text{-}P\} \\
&= \{ID_T, Ti, DC \wedge privacyConstr, \\
&\quad \times (PEC\text{-}T)_1 \wedge (PEC\text{-}T)_2 \cdots \wedge (PEC\text{-}T)_j, \\
&\quad \times \langle ID_T, DC \wedge privacyConstr, Signature\rangle, \\
&\quad \times \langle Qos, SPS\rangle\} \\
&= \{ID_T, Ti, DC \wedge privacyConstr, \\
&\quad \times (PEC\text{-}T)_1 \wedge (PEC\text{-}T)_2 \cdots (PEC\text{-}T)_j, \\
&\quad \times Signature, \langle Qos, SPS\rangle\} \\
&= \{ID_T, Ti, DC \wedge privacyConstr, \\
&\quad \times (DC \wedge privacyConstr)_1 \wedge \\
&\quad \times (DC \wedge privacyConstr)_2 \cdots \wedge \\
&\quad \times (DC \wedge privacyConstr)_j, Signature, \\
&\quad \times \langle Qos, SPS\rangle\}
\end{aligned}$$

where

$$\begin{aligned}
&privacyConstr \\
&\ = C(pn_1 : \{P_1, P_2, \ldots, P_x\} \ldots pn_i : \{P_1, P_2, \ldots, P_y\}) \\
&\quad \wedge C(pn_1 : P_1(am_1), \ldots, pn_i : P_r(am_t))
\end{aligned}$$

and the privacy-related format of cloud service provider will be defined as:

$$\begin{aligned}
&Pri - log_P \\
&\ = \{ID_P, T_i, PEC\text{-}P, PR\text{-}P, PA\text{-}P, CAS\} \\
&\ = \{ID_P, T_i, PEC\text{-}P, \\
&\quad \times (PEC\text{-}P)_1 \wedge (PEC\text{-}P)_2 \cdots \wedge (PEC\text{-}P)_i, \\
&\quad \times \langle Pid, PEC\text{-}P, PG\text{-}P, Signature\rangle, CAS\} \\
&\ = \{ID_P, T_i, PEC\text{-}P, \\
&\quad \times (PEC\text{-}P)_1 \wedge (PEC\text{-}P)_2 \cdots \wedge (PEC\text{-}P)_i, \\
&\quad \times PG\text{-}P, Signature, CAS\} \\
&\ = \{ID_P, T_i, privacyConstr \wedge P - objectConstr, \\
&\quad \times (PEC\text{-}P)_1 \wedge (PEC\text{-}P)_2 \cdots \wedge (PEC\text{-}P)_i, \\
&\quad \times PG - P, Signature, CAS\} \\
&\ = \{ID_P, T_i, privacyConstr \wedge P - objectConstr, \\
&\quad \times (privacyConstr \wedge P - objecConstr)_1 \wedge \\
&\quad \times (privacyConstr \wedge P - objecConstr)_2 \cdots \wedge \\
&\quad \times (privacyConstr \wedge P - objecConstr)_i, \\
&\quad \times PG - P, Signature, CAS\} \\
&\ = \{ID_P, T_i, privacyConstr \wedge CAS, \\
&\quad \times (privacyConstr \wedge CAS)_1 \wedge \\
&\quad \times (privacyConstr \wedge CAS)_2 \cdots \wedge \\
&\quad \times (privacyConstr \wedge CAS)_i, \\
&\quad \times \langle Qos, SPS\rangle, Signature, CAS\} \\
&\ = \{ID_P, T_i, privacyConstr, \\
&\quad \times privacyConstr_1 \wedge privacyConstr_2 \cdots \wedge \\
&\quad \times privacyConstr_i, \langle Qos, SPS\rangle, \\
&\quad \times Signature, CAS\}
\end{aligned}$$

where

$$\begin{aligned}
&privacyConstr \\
&\ = C(pn_1 : \{T_1, T_2, \ldots, T_m\} \ldots pn_i : \{T_1, T_2, \ldots, T_n\}) \\
&\quad \wedge C(pn_1 : T_1(am_1), \ldots, pn_i : T_s(am_q))
\end{aligned}$$

for the t accounted cloud participants, takes one certain time period Ti and logs set $\{Pri\text{-}log_{ID_1}, Pri\text{-}log_{ID_2}, \cdots, Pri\text{-}log_{ID_t}\}$ as input. It will output the corresponding accounting result $\{A_{ID_1}, A_{ID_2}, \cdots, A_{ID_t}\}$ for the t cloud participants, where, $A_{ID_i} = ((pi_1(am_1), t_1), (pi_2(am_2), t_2), \cdots, (pi_u(am_v), t_u))$, pi denotes the privacy it access, am is the operation on the privacy and t is the timestamp.

- Auditing(ID_v, PR_v, PEC_v, $\{A_{ID_1}, A_{ID_2}, \cdots, A_{ID_t}\}$): In the step, the auditing algorithm run by IBE-CSP take as input- the identity of privacy victim ID_v,the privacy request and privacy exposure condition of privacy victim PR_v and PEC_v,the accounting result $\{A_{ID_1}, A_{ID_2}, \cdots, A_{ID_t}\}$ of audited objects. It outputs the judgement result $\{R_{ID_1}, R_{ID_2}, \cdots, R_{ID_t}\}$, for simplicity, in the paper, we define the value of R_{ID_i} as 0 or 1, which means whether the corresponding cloud participant has violated the privacy regulation of the victim.

C. SECURITY ANALYSIS

Firstly, we prove the IND-ID-CPA secure of the proposed mechanism under the type-I adversary attack.

Theorem 1: Any IND-ID-CPA adversary (dishonest cloud participants) against the proposed accountable privacy-preserving scheme implies an IND-ID-CPA attacker against IBE [13] scheme.

Proof: For the IBE scheme, it has been proved to be IND-ID-CPA secure [13]. Let $\Im$ is an IND-ID-CPA adversary in the type-I adversary definition described above, we show that $\Im$ gives rise to an IND-ID-CPA adversary $\aleph$ against IBE scheme.

Without loss of generality, let the Identity information in the IBE scheme is not unique, so the dishonest cloud participant can counterfeit the ID information randomly in the IBE-AC system. We assume the adversary $\aleph$ run $Setup(\eta)$ to get their system parameter and master key $SP = \{q, G_1, G_2, \hat{e}, n, \alpha, \beta, H_1, H_2, H_3, H_4\}$.The master key is $MK = s$. From his/her challenger (SP_C, MK_C), (SP_A, MK_A),and output SP_C, SP_A, when input a master public key from his/her challenger of the others ID receiving. When the adversary $\Im$ launches a key generation request for an identity ID, $\aleph$ will query his/her own challenger to generate a private key $SK_{ID} = (H_2(ID))^s$ and begins executing the key generation protocol in interaction with $\Im$. The $\aleph$ adversary will supply a commitment $\Phi = g^{-Ti}(g^a \cdot g^{-ID})^{\omega}$ and an interactive Weil pairing proof of knowledge of the pair (Ti, ω), based on the extractor of the proof of knowledge, $\aleph$ extracts the pair by backtracking $\Im$ and $SK_ID = (H_2(ID))^s$.

In the challenge stage, $\Im$ randomly selects a victim identity ID_v and message m, which $\aleph$ forwards to his/her own challenger. Afterwards, the challenger will provide $\aleph$ with the corresponding ciphertext C which will relayed to $\Im$, and after key generation queries, $\Im$ and $\aleph$ will output the same bit, 0 or 1. So, if $\Im$ won the game, $\aleph$ has won as well.

Secondly, collusion attack is another possible attack for the proposed scheme, which is launched by the dishonest cloud participants who have violated the privacy regulations. To avoid punishment, more than one of the dishonest cloud participants will launch collusion attack to the proposed accountable scheme.

We will introduce some definitions of the collusion attack firstly and then prove the security of the proposed scheme against the collusion attack, that is the type-II adversary attack.

Definition 13: Bilinear-Diffie-Hellman problem inversion (BDHI) assumption [13]: We say that satisfies the BDHI assumption if no probabilistic polynomial algorithm A can solve BDHI with non-negligible advantage.

Definition 14: k-collusion attack algorithm assumption [29]: for random integers $(x, y, r_i) \in Z_q$, given k different inputs $g^{1/(x+y+r_1 H(ID_1))}$, $g^{1/(x+y+r_2 H(ID_2))}$, $\ldots$, $g^{1/(x+y+r_k H(ID_k))}$, $(1 \leq i \leq k)$, it do not exist a probabilistic polynomial algorithm Θ can calculate $g^{1/(x+y+r_0 H(ID_0))} \in G_1$ with non-negligible probability.

Based on the above definitions and assumption. From now on, we will show that the proposed accountable privacy-preserving scheme is always secure under the type-II adversary attack,

Lemma 1: Under k Bilinear Diffie-Hellman Inversion (k-BDHI) assumption, it do not exist a k-collusion attack algorithm $(k - CAA)$ to make k legal cloud participants to learn the secret successfully through collusion with non-negligible probability.

Proof: we assume that there exist a k-collusion attack algorithm and $g^{t^i} \in (G_1^*)^k$, $(i = 0 \cdots k)$, g and g_1 are generated by group G_1. We know that $x + x_i + (H_2(ID_i))^s$ is the private key of the cloud participants created from the identity ID_i in IBE-AC system. Generally, the private keys of cloud participants are kept secretly by themselves and will not let other cloud participants or adversaries know easily. In order to prove the security of the proposed scheme. We will consider the worst case that k legal nodes are compromised by adversaries and become the collusive attackers. In such case, the private keys of the k legal cloud participants are disclosed and they will launch collusion attack on the proposed system. According to the proposed scheme, the private key of the k legal cloud participants are $x + x_i + (H_2(ID_i))^s$, $i = 1 \cdots k$, we can compute $g_1^{x+x_i+(H_2(ID_i))^s}$. For simplicity, we note $F(ID_i) = x_i + (H_2(ID_i))^s$, at the same time, let $x = t\text{-}F(ID_0)$, $g_1 = g^{\coprod_{i=1}^{k}(x+F(ID_i))}$, we can get equations as follows:

$$g_1^{1/(x+F(ID_j))} = g^{\coprod_{i=1,i\neq j}^{k}(x+F(ID_i))} = g^{\coprod_{i=1,i\neq j}^{k} t}, \quad i = 1 \cdots k.$$

From the k-collusion attack algorithm $k-CAA$ assumption, we assume that there exists a k-collusion attack algorithm we can compute to get $g_1^{1/(x+F(ID_j))}$, and an equation can be described as follows:

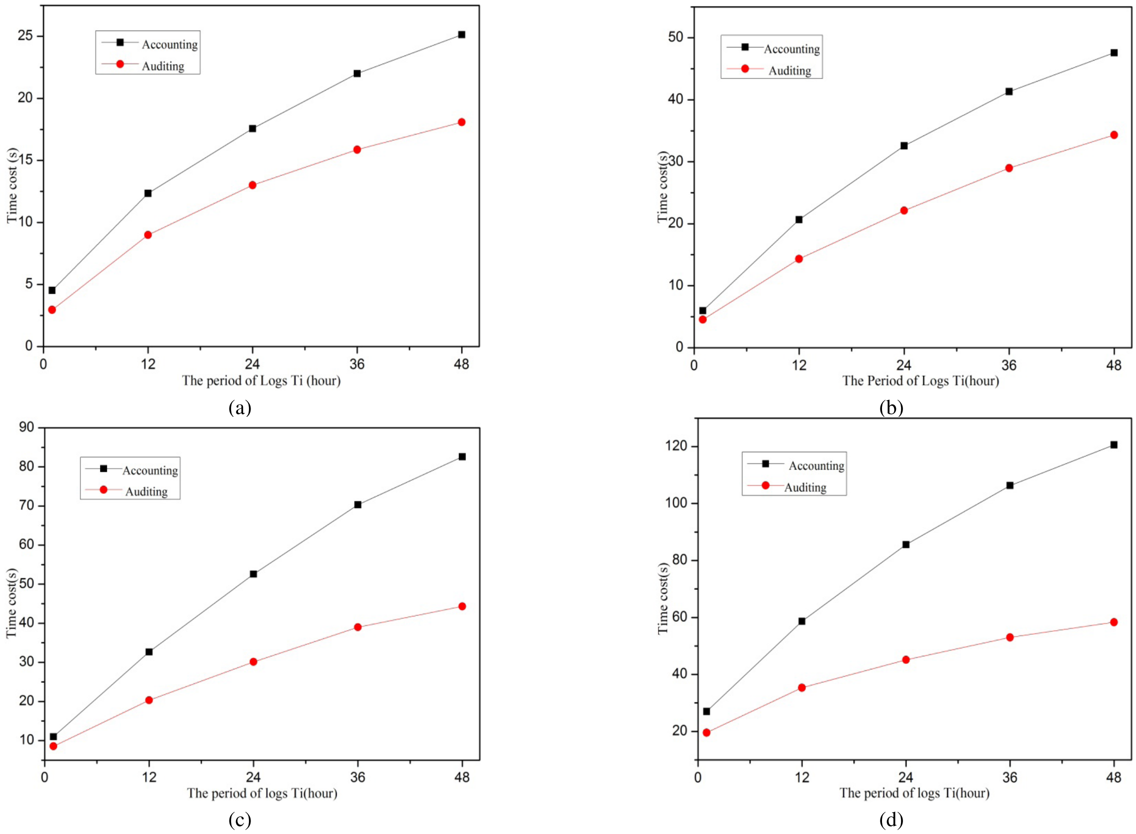
$$g^{\frac{1}{t}} = \left(\frac{g_1^{1/(x+F(ID_0))}}{g^{\sum_{i=0}^{k} a_i t^i}}\right)^{\frac{1}{a_0}}, \quad a_0 \neq 0$$

And finally we will get $\hat{e}(g, g)^{\frac{1}{t}} = \hat{e}(g, g^{\frac{1}{t}})$, so, there exists a k-collusion attack algorithm $(k - CAA)$ to solve the Bilinear Diffie-Hellman Inversion $(k - BDHI)$ problem, actually, this is not true according to the above k Bilinear Diffie-Hellman Inversion $(k - BDHI)$ assumption, so Lemma 2 is true.

END proof

VI. PERFORMANCE EVALUATION AND POTENTIAL IMPLEMENTATION

In order to evaluate the efficiency and effectiveness of the proposed accountable privacy-preserving mechanism, in the section, we will perform a thorough and detailed experimental evaluation for the proposed scheme in Section 5. We construct the testbed by using 64-bit M2 High memory double extra large Linux servers on Amazon EC2 platform. At the same time, we set 42 computers with Federal 10.0, Intel core i5-2400 CPU processor and 4G DDR memories to construct virtual private servers(VPS) [30], considering the computer capacity and network bandwidth, in the experiment,



(a)

(b)

(c)

(d)

FIGURE 5. The time cost of accounting and auditing under different experimental scenarios. (a) 42*1 simulated cloud users. (b) 42*5 simulated cloud users. (c) 42*15 simulated cloud users. (d) 42*25 simulated cloud users.

each computer will be split into 1, 5, 15 and 25 virtual private server, which will provide different number virtual computer units to simulate the cloud users. By combining the privacy concepts and definitions with the test log files based on the BSD syslog protocol [31], we pre-process the collected logs file using the data clean mechanism [32] firstly, and then simulate the accountability effectiveness when huge cloud users are available. For all evaluation in this section, we set group G_1 as 160-bit, G_2 as 512-bit and all communication in the evaluation based on TCP/IP protocol network.

A. PERFORMANCE EVALUATION FOR ACCOUNTABILITY

1) PERFORMANCE EVALUATION FOR ACCOUNTING AND AUDITING

In this section, we will test the accounting and auditing modules of the accountability under different scenarios. As described in the above experimental setup. The accounting and auditing stages will be tested under four different cases based on the virtual private servers technology [33]. In the simulation, each computer will be split into1, 5, 15 and 25 virtual private server, which can totally provide 42, 210, 630 and 1050 cloud users for simulation respectively. In Fig.5(a), for the 42 simulated cloud users, we set different network access mechanisms for them and collected 5 periods(1hour, 12 hours, 24 hours, 36 hours and 48 hours) network logs for accounting and auditing algorithm. From the test result in Fig.5(a), it is not hard to conclude that as the collected logs volume increase, the time overhead of the accounting step increases faster than the auditing step because the accounting need more time to pre-process the original logs file. (Note: for the time cost in Fig.5 and Fig.6, we only calculated the real process time of the Accounting and Auditing algorithm, not including the time overhead of data collection and transmission.)

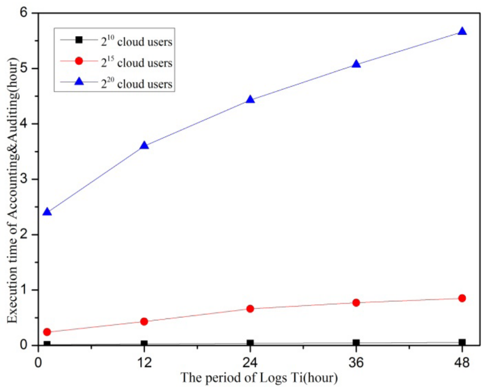


FIGURE 6. The execution time of accountability under different simulation scenarios.

Correspondingly, similar with the simulated setup of Fig.5(a), the test results of another three cases with 210, 630 and 1050 cloud users are shown in Fig.5(b), Fig.5(c) and Fig.5(d) respectively. From the experiment results, we can find that although the time overhead has increased as the increment of the period Ti and the accounted cloud users, the efficiency of the accounting and auditing processes are still perfect because the execution time of the proposed scheme is still within minutes level.

In the real cloud environment, the number of cloud users will be always larger than those we have evaluated above. Based on the average logs file volume created by per cloud user per hour in Fig.5(d), we evaluate the execution time of both accounting and auditing for different number of simulated cloud users under different periods Ti. The number of simulated cloud users are 2^{10}, 2^{15} and 2^{20} for three situations. For the experimental results in Fig.6, although the number of simulated cloud users reached to 2^{20}, the time overhead of the accounting and auditing modules run on one single Linux server only needs several hours to deal with the collected log files. Actually, in the real cloud application environment, we can distribute some agents for accounting and auditing modules to process the collected log files in a parallel mode, which will enhance the efficiency of accounting and auditing to some extent.

2) EFFECTIVENESS EVALUATION FOR ACCOUNTABILITY

In order to evaluate the accountability effectiveness of the proposed mechanism, we take the privacy-preserving of Taobao customers as the test examples, and set three popular privacy attributes for the victim cloud user, the address privacy address: $address : dilivery\ company \wedge address : save(am)$, the credit card information privacy $card\_info : Taobao \wedge card\_info : save(am)$, and the shopping order information privacy $order\_info : customer \wedge order\_info : all(am)$. For the shopping order privacy, it means that only the customer himself/herself owns the privacy of his/her shopping order information, at the same time, only the customer himself/herself has the all management privilege on the privacy. If any other customers attempt to abuse or access the constrained privacy illegally, then they violated the cloud privacy regulations.

In this experiment, after retrieving the 48 hours' simulated logs file based on the 2^{10}, 2^{15} and 2^{20} simulated cloud users scenario of Fig.6, we randomly insert 100,1000 and 10000 access records which violated the above three privacy constraint in the logs for the corresponding number of cloud users. When auditing algorithm runs, it will judges whether the cloud user has violated the privacy regulations according the accounting logs, the PR and PEC of the privacy victim. As described in the proposed mechanism, the judgment result R_i will be set as 1 if cloud user CUi has violated the privacy regulations. Table 2 shows the statistical results of how many cloud users have violated the privacy regulations for each period Ti under the three different scenarios.

Besides the better performance in efficiency, from the detected results of the cloud users who have violated the privacy regulation in Table 2, we can conclude that the proposed accountable privacy-preserving mechanism has detected 100% "illegal cloud user" for all evaluated scenarios. Therefore, in practical cloud situation, when the accounted cloud users are determined, the proposed accountable mechanism can perform accounting and auditing for one selected period Ti flexibly.

TABLE 2. Statistical results of detected violated cloud users for different period Ti.

Ti	1 hour	12 hours	24 hours	36 hours	48 hours
Detected-Num (User=2^{10})	3	27	48	76	100
Detected-Num (User=2^{15})	21	263	514	743	1000
Detected-Num (User=2^{20})	245	2472	5013	7629	10000

B. POTENTIAL ACCOUNTABILITY IMPLEMENTATION ON CLOUD PARTICIPANTS

In the proposed accountable mechanism, besides some special privacy concepts that mentioned above, we have defined some basic data protection and privacy control policies of the Service-Level Agreement for its implementation. In our proposed system, there exists a module to manage the Service-Level Agreement for all cloud services, which formulates rules of the obligations and rights for all cloud participants. In the implementation, we will define the security and privacy of the Service-Level Agreement for the proposed accountability system as Formula(1).

$$SLA_{S_i} = \{Price_{S_i}, Security_{S_i}, Privacy_{S_i}, Penalty_{S_i}\} \quad (1)$$

Where S_i denotes the i'th cloud service, $Price_{S_i}$ means the rent fee the cloud service providers should charge when they meet the requirement of the Service-Level Agreement. $Security_{S_i}$ defines some mechanisms which make it extremely difficult or uneconomical for an unauthorized person to access the private data information. $Privacy_{S_i}$ denotes the protection against the exposure or leakage of confidential data; and finally, the $Penalty_{S_i}$ denotes the penalty the cloud service providers should pay when their Service-Level Agreements violate the promised services. Without loss of generality, in real implementation, we define some polices for the four components $Price_{S_i}$, $Security_{S_i}$, $Privacy_{S_i}$ and $Penalty_{S_i}$ of the Service-Level Agreement in Formula (2-5).

$$\begin{aligned} Price_{S_i} &= \{rent_{fee\ x\ time}\} && (2)\\ Security &= \{Authentication, certificate, Anthority, \\ &\quad\ Authorization, Encrpytion\} && (3)\\ Privacy &= \{Audting, Accounting\} && (4)\\ Penalty_{S_i} &= \begin{cases} cccyellow\ card\ penalty \\ money\ penalty \\ red\ card\ penalty \end{cases} && (5)\end{aligned}$$

The definition of each policy in $Security_{S_i}$ and $Privacy_{S_i}$ of the Service-Level Agreement can be referred in the privacy model and the system model IBE-AC in Section 4.

In the proposed accountability system, we will penalize the cloud service providers if their Service-Level Agreements violate the promised services, we regard that Service-Level Agreement fulfilled when it has met all the requirements of the privacy service, otherwise it violated.

$$T(SLA_{S_i}) = \begin{cases} ccc1, SLA\ fulfiiled \\ 0, SLA\ voilated \end{cases} \tag{6}$$

According to Formula (6), if Service-Level Agreement fulfilled, the corresponding cloud service providers should charge from cloud users based on the policy of $Prices_{S_i}$; on the contrary, if Service-Level Agreement violated, the cloud service providers should be punished based on the policy of $Penaltys_{S_i}$. In the practical cloud application environment, we can formulate detailed penalties and compensation strategies for the proposed accountable privacy-preserving mechanism according to real requirement and circumstance.

VII. CONCLUSION

In this paper, focusing on the critical issue of cloud privacy-preserving, we proposed an accountable privacy-preserving mechanism based on IBE scheme. Firstly, we model and define the detailed privacy attribute for cloud participants based on description logic, and then introduced two algorithms to realize accountability combined with the modified IBE scheme in the IBE-AC model.

Furthermore, we consider the possible adversary attacks to the proposed accountable privacy-preserving mechanism, we describe the two types adversaries launched by the dishonest cloud participants, type-I and type-II adversaries for the game story. From the theory level, we proved the proposed mechanism is secure against the attacks launched by them.

Finally, we evaluated the proposed privacy-preserving mechanism through extensive simulation and experimental test, at the same time, we discuss the potential implementation of the proposed accountable privacy-preserving mechanism.

REFERENCES

[1] P. Mell and T. Grance, "The NIST definition of cloud computing," *Nat. Inst. Standards Technol.*, vol. 53, no. 6, p. 50, 2011.

[2] *Serious Privacy Problems in Cloud Computing*. Accessed: Mar. 26, 2018. [Online]. Available: http://www.networkworld.com/article/2185187/security/15-worst-internet-privacy-scandals-of-all-time.html

[3] D. Zou, Y. Xiang, and G. Min, "Privacy preserving in cloud computing environment," *Secur. Commun. Netw.*, vol. 9, no. 15, pp. 2752–2753, 2016.

[4] S. K. Pasupuleti, S. Ramalingam, and R. Buyya, "An efficient and secure privacy-preserving approach for outsourced data of resource constrained mobile devices in cloud computing," *J. Netw. Comput. Appl.*, vol. 64, pp. 12–22, Apr. 2016.

[5] J. Zhou, X. Dong, Z. Cao, and A. V. Vasilakos, "Secure and privacy preserving protocol for cloud-based vehicular DTNs," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 6, pp. 1299–1314, Jun. 2015.

[6] Z. Yan, X. Li, M. Wang, and A. V. Vasilakos, "Flexible data access control based on trust and reputation in cloud computing," *IEEE Trans. Cloud Comput.*, vol. 5, no. 3, pp. 485–498, Jul./Sep. 2017.

[7] Z. Xia, X. Wang, L. Zhang, Z. Qin, X. Sun, and K. Ren, "A privacy-preserving and copy-deterrence content-based image retrieval scheme in cloud computing," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 11, pp. 2594–2608, Nov. 2016.

[8] J. Yuan and S. Yu, "Privacy preserving back-propagation neural network learning made practical with cloud computing," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 1, pp. 212–221, Jan. 2014.

[9] X. Yao, Y. Lin, Q. Liu, and J. Zhang, "Privacy-preserving search over encrypted personal health record in multi-source cloud," *IEEE Access*, vol. 6, pp. 3809–3823, 2018.

[10] K. Prasad, J. Poonam, K. Gauri, and N. C. Thoutam, "Data sharing security and privacy preservation in cloud computing," in *Proc. Int. Conf. Green Comput. Internet Things (ICGCIoT)*, Oct. 2015, pp. 1070–1075.

[11] G. Zhuo, Q. Jia, L. Guo, M. Li, and P. Li, "Privacy-preserving verifiable data aggregation and analysis for cloud-assisted mobile crowdsourcing," in *Proc. IEEE INFOCOM*, Apr. 2016, pp. 1–9.

[12] H. Ma *et al.*, "Verifiable and exculpable outsourced attribute-based encryption for access control in cloud computing," *IEEE Trans. Dependable Secure Comput.*, vol. 14, no. 6, pp. 679–692, Nov./Dec. 2017.

[13] D. Boneh, M. Franklin, "Identity-based encryption from the weil pairing," *SIAM J. Comput.*, vol. 32, no. 3, pp. 586–615, 2003.

[14] J. Zhou, X. Lin, X. Dong, and Z. Cao, "PSMPA: Patient self-controllable and multi-level privacy-preserving cooperative authentication in distributedm-healthcare cloud computing system," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 6, pp. 1693–1703, Jun. 2015.

[15] G. Raghuraman *et al.*, "Cloud based privacy preserving efficient document storage and retrieval framework," in *Proc. IEEE Int. Conf. Intell. Comput. Commun. Process. (ICCP)*, Sep. 2015, pp. 519–525.

[16] B. Feng, X. Ma, C. Guo, H. Shi, Z. Fu, and T. Qiu, "An efficient protocol with bidirectional verification for storage security in cloud computing," *IEEE Access*, vol. 4, pp. 7899–7911, 2017.

[17] H. Rong *et al.*, "Privacy-preserving scalar product computation in cloud environments under multiple keys," in *Proc. Int. Conf. Intell. Data Eng. Automated Learn.* Berlin, Germany: Springer, 2016, pp. 248–258.

[18] H. Zhang, B. Li, H. Jiang, F. Liu, A. V. Vasilakos, and J. Liu, "A framework for truthful online auctions in cloud computing with heterogeneous user demands," *IEEE Trans. Comput.*, vol. 65, no. 3, pp. 805–818, Mar. 2016.

[19] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for secure cloud storage," *IEEE Trans. Comput.*, vol. 62, no. 2, pp. 362–375, Feb. 2013.

[20] Y. Gong, C. Zhang, Y. Fang, and J. Sun, "Protecting location privacy for task allocation in ad hoc mobile cloud computing," *IEEE Trans. Emerg. Topics Comput.*, vol. 6, no. 1, pp. 110–121, Jan./Mar. 2018.

[21] B. Wang, B. Li, and H. Li, "Oruta: Privacy-preserving public auditing for shared data in the cloud," *IEEE Trans. Cloud Comput.*, vol. 2, no. 1, pp. 43–56, Jan./Mar. 2014.

[22] J. Li, L. Zhang, J. K. Liu, H. Qian, and Z. Dong, "Privacy-preserving public auditing protocol for low-performance end devices in cloud," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 11, pp. 2572–2583, Nov. 2016.

[23] J. Ward and J. Peppard, *The Strategic Management of Information Systems: Building a Digital Strategy*. Hoboken, NJ, USA: Wiley, 2016.

[24] J. Baek, Q. H. Vu, J. K. Liu, X. Huang, and Y. Xiang, "A secure cloud computing based framework for big data information management of smart grid," *IEEE Trans. Cloud Comput.*, vol. 3, no. 2, pp. 233–244, Apr./Jun. 2015.

[25] A. Almutairi, M. I. Sarfraz, and A. Ghafoor, "Risk-aware management of virtual resources in access controlled service-oriented cloud datacenters," *IEEE Trans. Cloud Comput.*, vol. 6, no. 1, pp. 168–181, Jan./Mar. 2018.

[26] S. Pearson *et al.*, "Accountability for cloud and other future Internet services," in *Proc. IEEE 4th Int. Conf. Cloud Comput. Technol. Sci. (CloudCom)*, Dec. 2012, pp. 629–632.

[27] F. Xhafa, J. Feng, Y. Zhang, X. Chen, and J. Li, "Privacy-aware attribute-based PHR sharing with user accountability in cloud computing," *J. Supercomputing*, vol. 71, no. 5, pp. 1607–1619, 2015.

[28] J.-L. Tsai and N.-W. Lo, "Secure anonymous key distribution scheme for smart grid," *IEEE Trans. Smart Grid*, vol. 7, no. 2, pp. 906–914, Mar. 2016.

[29] M. Krötzsch, F. Simancik, and I. Horrocks. (2012). "A description logic primer." [Online]. Available: https://arxiv.org/abs/1201.4089

[30] P. Lu, "Construction of computer encrypted secure communication environment based on private virtual network technology," *Int. J. Simul.-Syst., Sci. Technol.*, vol. 16, no. 4B, pp. 2.1–2.6, 2015.

[31] C. Lonvick, *The BSD Syslog Protocol*, document RFC 3164, Internet Engineering Task Force, Network Working Group, Aug. 2001.

[32] G. Zhang and M. Zhang, "The Algorithm of Data Preprocessing in Web Log Mining Based on Cloud Computing," in *Proc. Int. Conf. Inf. Technol. Manage. Sci. (ICITMS)*. Berlin, Germany: Springer, 2013, pp. 467–474.

[33] P. Emelyanov *et al.*, "Common file caching for virtual private servers," U.S. Patent 9 286 310 B1, Mar. 15, 2016.

HONGBING CHENG received the Ph.D. degree in network and information security from the Nanjing University of Posts and Telecommunications in 2008. He was a Research Fellow with Nanjing University, China, the University of Stavanger, Norway, and Manchester University, England, from 2010 to 2013. He is currently an Associate Professor with the College of Computer and Software, Zhejiang University of Technology, Hangzhou, China. He has authored over 50 refereed journals and conference papers. His research interests include cloud computing, information and network security, big data security, and wireless sensor networks. He has served as the symposium chair and the session chair for several international conferences. He is an Associate Editor of the *Journal of Network and Information Security*.

CHUNMING RONG (SM'12) is currently the Head of the Center for IP-based Service Innovation, University of Stavanger, and also an adjunct Chief Scientist leading Big-Data Initiative at IRIS. He has extensive experience in managing large-scale research and development projects funded by both industry and funding agencies, both in Norway and EU. He has extensive contact network and projects in both the industry and academics. His research work focuses on data science, cloud computing, security, and privacy. He has been a member of the Norwegian Academy of Technological Sciences since 2011. He was the Vice President of CSA Norway Chapter from 2015 to 2016. He is the Co-Chair of the IEEE Blockchain and the Chair of the IEEE Cloud Computing. He is also the Founder and the Steering Chair of the IEEE CloudCom Conference and Workshop Series. He is also the Steering Chair and an Associate Editor of the IEEE Transactions on Cloud Computing and the Co-Editor-in-Chief of the *Journal of Cloud Computing* (Springer).

MANYUN QIAN received the bachelor's degree from the College of Computer, Central China Normal University, Wuhan, China. She is a postgraduate Student with the College of Computer and Software, Zhejiang University of Technology, Hangzhou, China. Her research interests include cloud computing and information and network security.

WEIHONG WANG received the M.Sc. degree in computer science from Zhejiang University in 1999. He currently serves as a Professor with the Zhejiang University of Technology. His research interests include cloud computing, big data analytics, and information security.