DOI：10.7652/xjtuxb201402005

云计算环境中的组合文档模型及其访问控制方案

熊金波[1,2]，姚志强[1,2]，马建峰[1]，刘西蒙[1]，马骏[1]
（1.西安电子科技大学计算机学院，710071，西安；2.福建师范大学软件学院，350108，福州）

摘要：针对云计算环境缺乏有效的组合文档模型及其元素分级安全保护的现状，结合多级安全思想和基于身份的加密(IBE)算法，提出了一种新的组合文档模型(ComDoc)及其访问控制方案(ICDAC)。ComDoc 包含组合文档的密文部分和密钥映射部分：前者保存具有安全等级的文档元素的密文；后者保存由 IBE 加密的密钥映射记录密文。ICDAC 依据授权用户的身份信息，利用 IBE 解密对应的记录后获得映射对，提取访问权限并解密授权的文档元素密文，实现组合文档元素分级安全保护的细粒度访问控制。实验结果表明：ComDoc 满足云计算环境中组合文档的特征以及安全需求；在加密相同组合文档的前提下，ICDAC 的密钥数量和计算开销明显优于已有方案。

关键词：云计算；组合文档；多级安全；身份加密；细粒度访问控制
中图分类号：TP309 **文献标志码**：A **文章编号**：0253-987X(2014)02-0025-07

A Composite Document Model and Its Access Control Scheme in Cloud Computing

XIONG Jinbo[1,2], YAO Zhiqiang[1,2], MA Jianfeng[1], LIU Ximeng[1], MA Jun[1]
(1. School of Computer Science and Technology, Xidian University, Xi'an 710071, China;
2. Faculty of Software, Fujian Normal University, Fuzhou 350108, China)

Abstract: A composite document model (ComDoc) and its fine-grained access control scheme (ICDAC) are proposed to address the actualities of lack of effective composite document model and multilevel security protection for document elements in cloud computing. The model combines the idea of multilevel security with an identity-based encryption (IBE) algorithm. In ComDoc composite document consists of a ciphertext part and a key-map part. The former stores the ciphertexts of document elements with security level. The element names and corresponding keys constitute map pairs and map records, and the records are then encrypted by the IBE and stored in the latter. The ICDAC achieves fine-grained access control with multilevel security protection for document elements by the following strategy. Authorized user decrypts the corresponding map records to get map pairs under the IBE in terms of the identity, and to extract the decryption keys to obtain the plaintext of the document elements. Comprehensive analysis shows that ComDoc satisfies the composite document characteristics and security requirements in cloud computing. Experimental results show that both the key numbers and the computational overheads of ICDAC are superior to existing scheme on the premise of encrypting the same composite documents.

收稿日期：2013-05-21。 作者简介：熊金波(1981—)，男，博士生；马建峰(通信作者)，男，教授，博士生导师。 基金项目：长江学者和创新团队发展计划资助项目(IRT1078)；国家自然科学基金重点资助项目(U1135002)；国家自然科学基金资助项目(61370078)；国家科技部重大专项资助项目(2011ZX03005-002)。
网络出版时间：2013-12-10 网络出版地址：http://www.cnki.net/kcms/detail/61.1069.T.20131210.1630.009.html

Keywords: cloud computing; composite document; multilevel security; identity encryption; fine-grained access control

云计算环境中云服务的发布、运行和组合等的实现均需要数据载体,而作为新型网络信息表现形式的组合文档是最合适的数据载体。云计算技术的快速发展促使这种载体的概念发生快速转变,传统单一格式、单个文件为中心的文档已经不再适应云服务对多样化格式、多类型结构化文档组合服务的新需求[1-2],如项目联合申报服务和医疗联合会诊服务等,都需要创建和管理复杂的组合文档。这类组合文档具有下列共性:①包含多个不同类型或格式的结构化文档元素,并被分属于不同安全域的多个参与者处理;②组合文档中不同的结构化文档元素携带不同程度的隐私信息,只授予具有相应安全等级的参与者处理[3];③组合文档在处理过程中,需跨越多个安全域,并在不安全的信道中传递。因此,需要建立适合云计算环境的组合文档模型及其细粒度访问控制机制,这对于保护组合文档存储和处理过程中的文档元素内容安全,建立组合文档安全体系具有重要的理论意义和实际价值。

在非云计算环境中,关于文档模型及其访问控制的研究主要有以下 5 种类型:①文档相似性处理方法,如文献[4]分别从基于标记、路径、树和图结构 4 个方面综述了传统文档模型并提出异构结构化文档模型以解决相似内容的关联关系问题,文献[5-6]基于 XML 文档结构分别处理文档近似查询以及处理文档结构和语义相似性;②多结构文档模型,如文献[7]从物理、逻辑和语义 3 个方面分析结构化文档模型,并基于 Text 提出多结构文档模型,但该模型仅处理文本文件;③安全文档模型,如文献[8]提出一种保护机密文档的安全文档模型,该模型仅考虑文档的安全属性;④多媒体文档模型,如文献[9]提出一种支持多媒体内容重用和自适应改变的多媒体文档模型;⑤组合文档模型,如文献[2,10]提出一种公共网络环境中可公开传递的组合文档(Publicly Posted Composite Documents, PPCD)结构,以处理非安全信道中传递的复杂组合文档工作流安全访问问题。然而,前 4 种文档模型均以单文档为中心且单一格式的传统文档,其访问方式除了文献[8]以外均较少考虑安全因素,第 5 种文档模型未考虑组合文档的多安全等级的特征。在云计算环境中,仅有文献[11]研究这一主题,指出结构化文档应具有内容动态、多用户参与、多媒体交互等“活”文档特征,并形式化定义了一种能够满足以上“活”文档特征的结构化文档(Structured Document, SDoc)模型,但该文献未考虑文档组合及其安全访问方法。

本文针对云计算环境中缺乏合适的组合文档模型及其安全访问机制的现状,以 SDoc 模型[11]为基础,首先引入多级安全思想[3]和基于身份的加密算法(Identity-based Encryption, IBE)[12]建立适合云计算环境的组合文档(Composite Documents, ComDoc)模型;然后,在 ComDoc 模型的基础上构造基于 IBE 的组合文档访问控制(IBE-based Composite Document Access Control, ICDAC)方案以实现对组合文档元素的细粒度安全访问。

1 组合文档模型 ComDoc

1.1 组合文档特征

云计算环境中的组合文档从创建、传播、使用到最终销毁,整个生命周期都具有“活”文档特征。

(1)多参与者协同。组合文档由多个结构化文档元素组成,每个参与者可能操作不同文档元素的,或多个参与者协同处理同一个文档元素。

(2)多媒体交互。组合文档是真正意义的多媒体文档,而非传统多种媒体文档的混合。

(3)多样化呈现。组合文档元素针对不同的参与者具有不同的版式布局和呈现形式;对同一个参与者在不同时间和地点具有不同的呈现形式。

(4)多安全等级。不同的文档元素包含不同程度的隐私信息,具有不同的安全级别,应采用不同的密钥加密,并赋予不同的参与者处理,从而实现细粒度的安全访问。

1.2 ComDoc 概念模型

充分考虑以上组合文档的特征,在 SDoc 模型[11]的基础上构建 ComDoc。在 SDoc 中,文档由包含不同隐私程度的多个文档元素连接而成,需要定义不同的安全等级,本文将其划分为安全等级 1、安全等级 2 等,以便不同的组织依据需求自行定义。为了保护文档隐私,需要对其加密,通常情况下采用对称密钥 k 加密以提高效率和节省开销。如果每个文档元素分别采用一个 k 加密,则将带来庞大的密钥生成、分发和管理开销。因此,本文采用依据安全等级分配 k 的策略,如图 1 所示,同一参与者访问的具有相同安全等级的文档元素采用相同的 k 加密,

从而在一定程度上减小密钥管理开销。

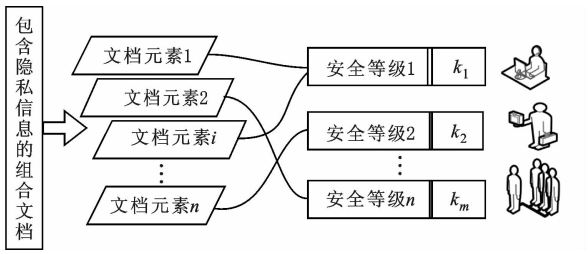

图 1　文档元素依据安全等级分配密钥

不同文档中的文档元素，如果具有相同的安全等级、或者相同或相似的文档属性，可以通过 SDoc 模型中定义的外部连接关系进行连接[11]。如将 A 文档中文档元素的绑定点连接到 B 文档另一元素的连接点，从而多个文档组合成一个组合文档 ComDoc。下面，给出 ComDoc 的形式化描述。

1.3　ComDoc 模型形式化描述

ComDoc 模型形式化描述为如下 2 部分：组合文档密文部分（CipherPart）和密钥映射部分（KeyMapPart）。

（1）CipherPart。该部分包含结构化文档 d_i 或文档元素 e_i 采用对称密钥 k_i 加密后的密文 C_{d_i} 或 C_{e_i} 的集合，即 $C_{\mathrm{CP}}=\{C_{d_i}\}\cup\{C_{e_i}\}$。

（2）KeyMapPart。该部分存储结构化文档名 n_d 或文档元素名 n_e 以及对应的 k_i 组成的$<n_{d_i}j,k_i>$映射对或$<n_{e_i},k_i>$映射对。每个参与者都拥有一条密钥映射记录 r_i，且 $r_i=\{<n_{d_i},k_i>\}\cup\{<n_{e_i},k_i>\}$，即该记录包含一个或多个映射对以实现细粒度访问控制。然后，该 r_i 的内容依据参与者身份 I_i 采用 IBE 加密后得到密文 $C_{\mathrm{IBE}-I_i}(r_i)$，则该部分为集合 $C_{\mathrm{KMP}}=\bigcup\{C_{\mathrm{IBE}-I_i}(r_i)\}$。

在此基础上，给出 ComDoc 的要领模型如图 2 所示。

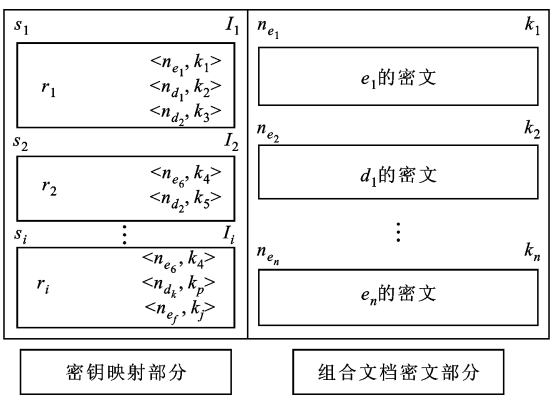

图 2　组合文档概念模型

2　ICDAC 方案

在 ComDoc 模型的基础上，利用 IBE 算法构造 ICDAC 方案。

IBE 是一种公钥密码算法，其公钥和私钥不在系统初始化时产生，而是基于用户的身份信息计算得到，且私钥可以延迟到需要解密的时候再申请计算，从而简化密钥的生成与管理。第一个实用且可证明安全的 IBE 方案是基于 Weil Pairing 构造的[12]。该方案中，用于计算公钥的是用户公开的身份标识符，如 email 地址，而私钥则由可信第三方的密钥产生中心（Key Generation Center，KGC）利用用户公钥计算得出[13]。

IBE 算法能够用于构造 ICDAC 方案的原因主要有以下 2 个方面：

（1）IBE 采用非对称加密算法，无需预先产生所有文档参与者的公/私钥和证书，从而简化了密钥管理；

（2）不同的参与者具有不同的安全级别，采用其身份加密安全等级相匹配的文档元素对应的 k，即可灵活实现对组合文档的细粒度访问控制。

ICDAC 方案的符号及其描述如表 1 所示。

表 1　ICDAC 符号及其描述

符号	描述
κ	足够大的安全参数
F	密钥生成函数
H	哈希函数
G_1，G_2	具有阶 q 的有限域群
g	G_1 的生成元
p	公共参数
$x\in\mathbf{Z}_q$	KGC 主私钥
$y=g^x$	系统主公钥
O_{CDO}	组合文档对象
k_{EIBE}	IBE 加密密钥
k_{DIBE}	IBE 解密密钥

2.1　系统模型

ICDAC 的系统模型如图 3 所示，包含组合文档创建者、云服务器、可信 KGC 和组合文档参与者。

（1）组合文档创建者。依据参与者的身份 I_i、相应的访问权限和 ComDoc 模型创建组合文档，并将其封装成组合文档对象 O_{CDO} 后保存到云服务器中，将产生的$<s_i,I_i>$保存到 KGC 中。

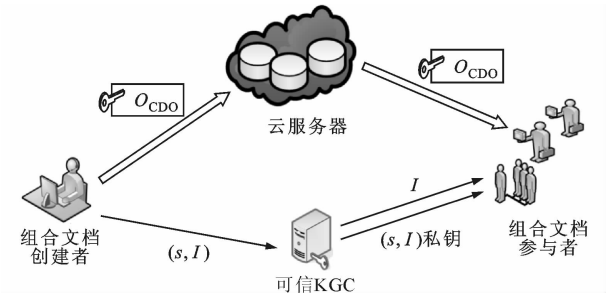

图 3 系统模型

(2)云服务器。保存创建者提交的 O_{CDO},并只允许授权的参与者访问。

(3)可信 KGC。产生公共参数,支持 IBE 加密并为授权用户产生私钥,并负责保存$<s_i,I_i>$。

(4)组合文档参与者。参与组合文档的处理,需向可信 KGC 提交 I_i 并认证通过后,从 KGC 获得对应的$<s_i,I_i>$和私钥;然后从云服务器获得相应的 O_{CDO},解封装 O_{CDO}并解密其中的密文最终获得需要访问的组合文档明文。

在系统模型中,本文假设 KGC 是可信服务器,可以由组织内部或可信第三方提供;组合文档创建者和参与者可信,且与可信 KGC 之间存在安全的通信信道,如 IPSec 或 SSL 等。下面分别从系统层面和算法层面构建 ICDAC 方案。

2.2 ICDAC 方案系统描述

系统层面描述方案中高级操作的功能实现,主要包括以下 3 个阶段。

(1)系统建立。该阶段主要由 KGC 执行。给定系统安全参数 κ,调用算法层面的系统建立算法能产生系统参数 p 和 IBE 公钥和私钥参数。

(2)组合文档创建。该阶段主要由创建者执行。创建者首先为 d_i 或 e_i 划分安全等级,同一参与者访问的相同安全等级的 d_i 或 e_i 选用相同的 k,并调用文档加密算法对其加密后将密文 C_{CP}存储在 CipherPart 中;然后,创建者获得所有参与者的身份 I_i,依据 I_i 调用密钥生成算法计算各参与者的 IBE 加密密钥 k_{EIBE};再依据各参与者的角色组织其 r_i 中的映射对$<n_{d_i},k_i>$或$<n_{e_i},k_l>$,从而不同参与者访问不同文档元素,实现文档元素级细粒度访问。组织好 r_i 后,调用 IBE 加密算法加密 r_i 得到密文 C_{KMP}并存储在 KeyMapPart 中,之后由系统为该记录产生一个随机序列 s_i,s_i 和参与者 I_i 组成元组$<s_i,I_i>$,创建者将其保存到 KGC 中;最后,调用封装算法将密文 C_{CP}和 C_{KMP}封装成 O_{CDO},然后保存到云端服务器中。

(3)组合文档安全访问。该阶段主要由参与者执行。首先,向 KGC 提交身份 I_i,认证通过后,KGC 找到匹配的$<s_i,I_i>$并计算该参与者的 IBE 私钥 $k_{I_i}=H(I_i)^x\in G_1$,一起通过安全信道发送给参与者,参与者再调用密钥生成算法计算得到 IBE 解密密钥 k_{DIBE};然后,从云服务器获得相应的 O_{CDO},调用解封装算法将 O_{CDO}还原为密文 C_{CP}和 C_{KMP};最后,依据获得的$<s_i,I_i>$从 KeyMapPart 中找到对应的 r_i,调用 IBE 解密算法解密出相应记录 r_i,获得权限范围内的映射对$<n_{d_i},k_i>$或$<n_{e_i},k_l>$,即可提取相应的 k 并调用解密算法获得 d_i 或 e_i 的明文,实现对组合文档的安全访问。

2.3 ICDAC 方案算法描述

算法层面主要执行由系统层面调用的具体算法实现,主要包括如下 9 个算法。

(1)系统建立算法。可信 KGC 根据系统安全参数 κ 运行系统建立算法,生成并且输出一个哈希函数 $H:\{0,1\}^*\rightarrow G_1$、随机密钥 k 和一个对称加密算法 T、一个双线性对函数 $e:G_1\times G_1\rightarrow G_2$(加法循环群 G_1 和乘法循环群 G_2 均为大素数阶 q 的有限域群,且 G_1 的生成元为 g)和密钥生成算法 $F:G_3\rightarrow\{0,1\}^m$(这里 m 为密钥长度),则系统参数 $p=(H,T,e,F,G_1,G_2,y)$。此外,KGC 生成私钥 $x\in\mathbf{Z}_q$ 与公钥$(g,y=g^x)\in G_1^2$。

(2)文档加密算法。创建者将系统参数 p、对称密钥 k、文档 d_i 或文档元素 e_i 输进文档加密算法(如 AES),采用 k_i 加密 d_i 或 e_i,得到密文 C_{d_i} 或 C_{e_i},将汇总的密文 $C_{CP}=\{C_{d_i}\}\cup\{C_{e_i}\}$存储在 CipherPart 中。

(3)加密密钥生成算法。创建者依据参与者身份 I_i 随机选择一个伪私钥 α 并计算 $H(I_i)^\alpha$,又从 KGC 获得系统公钥 y,运行双线性对函数 $e(H(I_i)^\alpha,y)$,并将其输进加密密钥生成算法。该算法计算并输出该参与者的 IBE 加密密钥 $k_{EIBE_i}=F(e(H(I_i)^\alpha,y))$,同时输出一个伪公钥 $z=g^\alpha$ 并安全发布给参与者。

(4)IBE 加密算法。创建者将 IBE 加密密钥 k_{EIBE_i}和密钥映射记录 r_i 输进 IBE 加密算法,采用 k_{EIBE_i}加密 r_i 并输出为该记录的密文 $C_{IBE-I_i}(r_i)$,其汇总的密文 $C_{KMP}=\bigcup\{C_{IBE-I_i}(r_i)\}$存储在 KeyMapPart 中。

(5)封装算法。创建者将公开参数 p 和组合文档的密文 $C=C_{CP}+C_{KMP}$输进封装算法中,输出组合文档对象 O_{CDO},并将其存储在云服务器中。

(6)解密密钥生成算法。参与者将身份 I_i 提交给 KGC，KGC 认证参与者身份后，计算其私钥 $k_{I_i}=H(I_i)^x\in G_1$，并将该私钥安全发送给参与者。参与者还可以从 KGC 处获得伪公钥 $z=g^r$ 并将其与 k_{I_i} 一起输入解密密钥生成算法，该算法计算并输出参与者的 IBE 解密密钥 $k_{\mathrm{DIBE}_i}=F(e(k_{I_i},z))$。

(7)解封装算法。参与者从云服务器获得 O_{CDO} 并与系统参数 p 一起输入解封装算法，将 O_{CDO} 解封装并输出为组合文档的两部分密文 C_{CP} 和 C_{KMP}。

(8)IBE 解密算法。参与者从 KGC 获得 IBE 解密密钥 k_{DIBE_i}。由于对函数 e 具有双线性性质，即下面等式成立 $e(k_{I_i},z)=e(H(I_i)^x,g^\alpha)=e(H(I_i)^\alpha,g^x)=e(H(I_i)^\alpha,y)$，即得到 $k_{\mathrm{DIBE}_i}=k_{\mathrm{EIBE}_i}$。参与者将 k_{DIBE_i} 和 $C_{\mathrm{IBE}-I_i}(r_i)$ 输入 IBE 解密算法，解密 $C_{\mathrm{IBE}-I_i}(r_i)$ 后得到并输出 r_i 的映射对 $<n_{d_i},k_i>$ 或 $<n_{e_i},k_l>$。

(9)文档解密算法。参与者获得映射对 $<n_{d_i},k_i>$ 或 $<n_{e_i},k_l>$ 后，即可提取出相应的密文 C_{d_i} 或 C_{e_i} 以及对应的密钥 k，并与系统参数 p 一起输入文档解密算法，解密 C_{d_i} 或 C_{e_i} 后获得并输出组合文档明文 d_i 或文档元素明文 e_i。

3　安全性证明与综合分析

3.1　文档模型的分析与比较

将 ComDoc 模型与已有最新文档模型的效能对比分析汇总于表 2。

表 2　ComDoc 与其他文档模型的特征比较

文档模型	动态性自适应性	多用户性	多媒体性	安全等级	安全访问
PPCD 模型[2,10]	√	√	√	×	○
语义文档模型[4]	√	×	√	×	×
XML 文档模型[6]	√	×	√	×	×
安全文档模型[8]	×	×	○	√	○
本文 ComDoc 模型	√	√	√	√	√

注：√表示满足该特征；×表示不满足该特征；○表示部分满足该特征。

文献[2,10]提出的 PPCD 模型是最新的组合文档模型，具有自适应性、多用户性和多媒体特征，但该模型没有对文档和文档元素划分安全等级，不具备多级安全特征；文献[4]提供语义建模结构化文档，能够自适应表达不同类型文档的语义信息，但不具备组合文档其他特征；文献[6]基于 XML 建立文档结构比较框架，基于标签语义处理文档结构和语义相似性，并未考虑多用户参与、多安全等级等文档特征；文献[8]为保护企事业单位和政府机密文档而提出安全机密文档模型，该模型能够灵活地实现多级安全的控制与分发，但是并不具备组合文档的其他特征。

综上所述，以上最新研究成果均在某种程度上满足云计算环境中组合文档的“活”文档特征，然而均存在不同程度的局限性。ComDoc 模型通过分割文档元素并赋予安全等级，能够满足组合文档的特征需求：①不同用户具有不同的安全等级，能够访问和处理不同的文档元素，体现多安全等级和多用户性；②同一用户在不同上下文环境中也具有不同安全等级，其能访问的文档元素也会发生变化，体现自适应性；③每个文档元素都可以是多媒体文档，体现多媒体性；④结合 IBE 算法能够实现对文档元素的细粒度访问控制。因此，ComDoc 模型符合云计算环境中服务共享与传播的数据媒介特征与要求，适合云计算环境。

3.2　访问控制机制的分析与比较

文献[2,10]构建的 PPCD 组合文档着重考虑组合文档的访问控制方案，其中文献[2]基于 PKI 实现对组合文档的安全访问，其主要优势是已有基础设施完善，方案实现简单。存在的局限性主要体现在：①系统初始化时，需要为所有文档参与者预先产生公/私钥对并发布证书，假设有 n 个参与者，组合文档共 m 个元素，因需要为每个参与者每个不同的元素分配不同的密钥，因此，密钥和证书的管理开销为 $(n+2nm)$，其复杂度为 $O(nm)$；②在文档创建之初，创建者需要收集所有参与者的公钥，缺少一个便不能正常生成组合文档。文献[10]基于 IBE 实现对组合文档的安全访问，主要优势是引入 IBE 机制后不需要在系统初始化时为参与者产生公/私钥对并发布证书，只需要管理参与者的身份信息。此外，该方案亦没有对文档元素划分安全等级，仍然需要为每个参与者每个不同的元素分配不同的密钥，因此，密钥管理开销为 (nm)，其复杂度为 $O(nm)$，与文献[2]相比，并未明显改善。

本文提出的 ICDAC 方案在 ComDoc 模型的基础上引入 IBE 机制，相比文献[10]，本文方案的优势主要为：①对组合文档元素划分安全等级，能够分等级保护文档内容隐私；②同一参与者访问的相同安全等级的文档元素选用同一密钥加密，比如将文档元素划分为 4 个安全等级，则密钥数量为 $(4n)$，其

复杂度为 $O(n)$，从而简化了密钥管理；③结构简单，只有 CipherPart 和 KeyMapPart 两部分，而 PPCD 模型还包含进入表部分，共有 4 个字段，因此，ComDoc 模型具有较小的存储开销；④根据参与者身份设置密钥映射记录，再利用 IBE 加密该记录内容，方便实现细粒度访问控制。将以上 3 种访问控制方案的比较汇总于表 3。

表 3 组合文档访问控制方案对比分析

访问控制方案	管理对象	分级保护	密钥管理复杂度	存储开销	访问粒度
PPCD-PKI[2]	公/私钥和证书	不支持	$O(nm)$	较大	粗粒度
PPCD-IBE[10]	身份信息	不支持	$O(nm)$	较大	粗粒度
本文 ICDAC	身份信息	支持	$O(n)$	较小	细粒度

从表 3 可以看出，相比最新研究成果，本文 ICDAC 方案具有明显优势。然而，在组合文档创建之初，创建者需要知道所有参与者的身份信息，当创建者不可信时将泄露参与者的身份隐私。为了解决此问题，下一步将引入权重属性基加密机制[14]，将 ComDoc 多级安全和权重属性相关联，建立 ComDoc 权重属性加密方案，以实现多级安全和支持身份隐私保护的细粒度访问控制。

3.3 访问控制方案计算开销的分析与比较

通过加密不同大小的组合文档分别比较 ICDAC 方案和 PPCD-IBE 方案[10]的计算开销。实验环境为基础平台：CPU 为 Intel Core i5 2450 MB，RAM 为 2 GB，DDR III 1 600 MHz，OS 为 Ubuntu 12.04；密码平台：Pairing-Based Cryptography Library[15]，160 bit 椭圆曲线构造的 Type A 双线性对，标准的 128 bit AES 对称加密算法和 48 bit Hash 函数。实验测试了 2 种方案的计算开销，循环执行 200 次取平均值。

实验随机选取 4 个不同大小的组合文档 A(183.2 kB)、B(3.70 MB)、C(20.8 MB) 和 D(267.4 MB)，均分为 3 个元素且其中有 2 个元素为相同安全等级，2 个参与者参与访问。PPCD-IBE 方案采用 AES 算法加密文档(每个用户每个元素都需要 1 个密钥，共需要 6 个密钥)，采用 IBE 算法加密进入表；ICDAC 方案采用 AES 加密文档(每个用户只能访问与之安全等级匹配的文档元素，共需要 2 个密钥)，采用 IBE 算法加密密钥映射记录。实验测量计算开销(单位 ms)的结果如表 4 所示。由表 4 可知，ICDAC 方案的计算开销要明显优于 PPCD-IBE 方案，主要原因是 PPCD 的进入表部分多 2 次对称加密的计算开销。另外，由于 ICDAC 方案没有进入表部分，相比 PPCD 要节省存储开销；ICDAC 方案的对称密钥数量要远低于 PPCD-IBE 方案。

4 结 论

组合文档是云计算环境中新型的网络信息表现形式，在信息交换与传播中扮演关键角色。在云计算环境中，组合文档具有多用户参与、多媒体交互和多安全等级等“活”文档特征。从而，满足这种“活”文档特征的组合文档模型及其安全相关研究对于云计算环境中安全信息交互、服务协同等具有重要的理论和实际意义，对于加快云计算产业发展具有积极的推动作用。

本文的主要贡献为以下 2 个方面：

(1)引入多级安全思想建立 ComDoc 模型，满足了云计算环境中组合文档的特殊特征，可为实现复杂的组合文档及其工作流服务提供实现机制；

表 4 访问控制方案计算开销的比较 ms

方案	加密组合文档的计算开销				加密映射记录的计算开销			
	A	B	C	D	A	B	C	D
PPCD[10]	1.71	27.55	160.02	2 068.24	0	0	0	0
ICDAC	1.71	27.55	160.02	2 068.24	16.28	16.28	16.28	16.28
方案	加密进入表的计算开销				总的计算开销			
	A	B	C	D	A	B	C	D
PPCD[10]	17.29	17.55	20.37	42.01	19.00	45.10	180.39	2 110.25
ICDAC	0	0	0	0	17.99	43.83	176.30	2 084.52

(2)将 IBE 算法融入到 ComDoc 模型中，提出基于 IBE 的组合文档细粒度访问控制方案 ICDAC，可实现云计算环境中对组合文档的细粒度安全访问。

综合分析比较与实验结果表明，本文提出的 ICDAC 方案要明显优于已有方案。

参考文献：

[1] BALINKSY H, SIMSKE S J. Secure document engineering [C]// Proceedings of the 11th ACM Symposium on Document Engineering. New York, USA: ACM, 2011: 269-272.

[2] BALINKSY H, SIMSKE S J. Differential access for publicly-posted composite documents with multiple workflow participants [C]// Proceedings of the 10th ACM Symposium on Document Engineering. New York, USA: ACM, 2010: 115-124.

[3] 熊金波，姚志强，马建峰，等. 基于行为的结构化文档多级访问控制 [J]. 计算机研究与发展，2013，50(7)：1399-1408.
XIONG Jinbo, YAO Zhiqiang, MA Jianfeng, et al. Action-based multilevel access control for structured document [J]. Journal of Computer Research and Development, 2013, 50(7): 1399-1408.

[4] TAN S S, TANG E K, RANAIVO M B, et al. Modeling semantic correspondence in heterogeneous structured document collection [C]// Proceedings of the 2011 International Conference on Semantic Technology and Information Retrieval. Los Alamitos, CA: IEEE Computer Society, 2011: 189-196.

[5] 衡星辰，罗俊颉，郭俊文，等. 八邻域网格聚类的多样性 XML 文档近似查询算法 [J]. 西安交通大学学报，2007，41(8)：907-911.
HENG Xingchen, LUO Junjie, GUO Junwen, et al. Approximate query algorithm based on eight neighbor grid clustering for heterogeneous XML documents [J]. Journal of Xi'an Jiaotong University, 2007, 41(8): 907-911.

[6] TEKLI J, CHBEIR R. A novel XML document structure comparison framework based on sub-tree commonalities and label semantics [J]. Web Semantics: Science, Services and Agents on the World Wide Web, 2012, 11(3): 14-40.

[7] PORTIER P E, CHATTI N, CALABRETTO S, et al. Modeling, encoding and querying multi-structured documents [J]. Information Processing & Management, 2012, 48(5): 931-955.

[8] ZHENG S, LIU J. A secure confidential document model and its application [C]// Proceedings of the International Conference on Multimedia Information Networking and Security. Piscataway, NJ, USA: IEEE Computer Society, 2010: 526-529.

[9] BOLL S, KLAS W. ZYX: a multimedia document model for reuse and adaptation of multimedia content [J]. IEEE Transactions on Knowledge and Data Engineering, 2001, 13(3): 361-382.

[10] BALINSKY H, CHEN L, SIMSKE S J. Publicly posted composite documents with identity based encryption [C]// Proceedings of the 11th ACM Symposium on Document Engineering. New York, USA: ACM, 2011: 239-248.

[11] 熊金波，姚志强，金彪. 云计算环境中结构化文档形式化建模 [J]. 计算机应用，2013，33(5)：1267-1270.
XIONG Jinbo, YAO Zhiqiang, JIN Biao. Formal modeling for structured document in cloud computing [J]. Journal of Computer Applications, 2013, 33(5): 1267-1270.

[12] BONEH D, FRANKLIN M. Identity-based encryption from the Weil pairing [J]. SIAM Journal on Computing, 2003, 32(3): 586-615.

[13] XIONG J B, YAO Z Q, MA J F, et al. A secure document self-destruction scheme with identity based encryption [C]// Proceedings of the 5th International Conference on Intelligent Networking and Collaborative Systems, IEEE INCoS'13. Los Alamitos, CA, USA: IEEE CS, 2013: 239-243.

[14] 刘西蒙，马建峰，熊金波，等. 密文策略的权重属性基加密方案 [J]. 西安交通大学学报，2013，47(8)：44-48.
LIU Ximeng, MA Jianfeng, XIONG Jinbo, et al. Ciphertext policy weighted attribute based encryption scheme [J]. Journal of Xi'an Jiaotong University, 2013, 47(8): 44-48.

[15] LYNN B. The Pairing-based cryptography library [EB/OL]. [2013-04-20]. http://www.crypto.stanford.edu/pbc/dounload.html.

（编辑　刘杨　武红江）