doi:10.3969/j.issn.1000-436x.2014.10.015

云环境数据服务的可信安全模型

熊礼治[1]，徐正全[1]，顾鑫[2]
（1. 武汉大学 测绘遥感信息工程国家重点实验室，湖北 武汉 430079；2. 湖北省标准化研究院，湖北 武汉 430061）

摘 要：针对云服务提供商的可信状态和云环境数据服务的安全需求，提出了云环境数据服务的可信重加密安全模型，即在云环境下的数据安全需要云服务提供商满足一定的可信程度，再结合有效的重加密算法才能得以保证。通过对重加密模型进行安全分析，并用密码算法对重加密模型进行验证，得到实现重加密算法的约束条件，同时提出可信评价模型，对云服务提供商的可信状态进行动态评价，为建立云环境数据服务的可信安全提供理论基础和实现依据。

关键词：云数据服务；重加密；数据安全；可信模型
中图分类号：TP393.08 **文献标识码**：A **文章编号**：1000-436X(2014)10-0127-11

Trusted secure model for data services in cloud computing

XIONG Li-zhi[1], XU Zheng-quan[1], GU Xin[2]
(1. State Key Laboratory of Information Engineering in Surveying, Mapping and Remote Sensing, Wuhan University, Wuhan 430079, China;
2. Hubei Institute of Standardization, Wuhan 430061, China)

Abstract: For trusted status of cloud service provider (CSP) and security requirements for data services in cloud computing, the trusted re-encryption secure model (TRSM) for cloud data services was proposed. Only with a certain trusted degree in CSP, cloud data security can be ensured by taking effective re-encryption schemes. The re-encryption secure model is verified by the classical cryptographic algorithms and analyzed by random oracles. Thus, the basic requirements of realizing re-encryption algorithm are got. Moreover, trusted evaluation model is proposed and used to dynamically evaluate CSP's trusted status, provides theoretical basis and realization for establishment of trusted secure data services in cloud computing.

Key words: cloud data services; re-encryption scheme; data security; trusted model

1 引言

信息化的加速和互联网络的发展，使数据服务在数据存储、数据处理模式上发生了改变，在传统的数据服务中，企业必须拥有大量的、高性能的服务设备来不断地增加数据存储空间和提高服务数据处理的性能，但随之而来的计算机硬件设备更新换代给企业带来不菲的服务基础成本，提高数据服务质量与降低企业服务成本之间的矛盾越来越明显。随着云计算的发展，具有海量数据访问、低成本、高性能计算的弹性云计算服务模式成为了当前研究的热点[1]。

云数据服务模式替代传统数据服务模式能大大降低企业数据服务的运营成本，同时企业可以利用云存储技术，将海量数据进行分类管理和数据分发，提高服务效率和服务质量，云数据服务模式如图 1 所示。然而在这样一个开放的环境下，安全问题成为了云数据服务发展的一个重要瓶颈[1]。现存的安全问题解决方案有利用防火墙技术防止黑客对数据的窃取，利用周期性安全检查维护基础设施的安全，利用访问策略

收稿日期：2013-05-27；**修回日期**：2013-09-09
基金项目：国家重点基础研究发展计划（“973”计划）基金资助项目（2011CB302306, 2011CB302204）；国家自然科学基金资助项目（41371402, 41101416）；国家教育部博士点基金资助项目（20110141110056）
Foundation Items: The National Basic Research Program of China (973 Program) (2011CB302306, 2011CB302204); The National Natural Science Foundation of China(41371402, 41101416); The Ph.D. Programs Foundation of Ministry of Education of China (20110141110056)

实现对数据用户的权限控制，利用单一加密手段防止数据内容外泄等。这些安全手段往往都基于一个前提，即云服务提供商（CSP, cloud service provider）本身是可信的，即能忠实按照用户的要求执行所分配工作任务且不破坏用户数据。而实际应用中，CSP 对于用户存储在云端的数据拥有特权，可以访问数据，甚至篡改、破坏用户数据。

针对 CSP 的特点，云数据服务中的 CSP 可信状态分为可信、不可信和不完全可信即半可信 3 种状态。可信状态下，CSP 能长期稳定提供服务且忠实执行用户设定的程序，对用户数据不产生任何兴趣；不可信状态下，CSP 会对敏感数据进行访问、复制和篡改、甚至破坏用户数据，使用户存储于云端的数据的机密性、安全性和合法访问受到安全威胁；半可信的状态下，CSP 是诚实的但对用户数据保持着好奇，它能忠实执行程序和设定相关访问协议，并有获取用户数据和访问控制策略的权利，并且云服务提供商的半可信状态在一定程度上是不可控的动态变化的。因此，针对 CSP 半可信状态及其动态变化性和云环境数据服务的安全，提出云环境数据服务的可信安全模型。

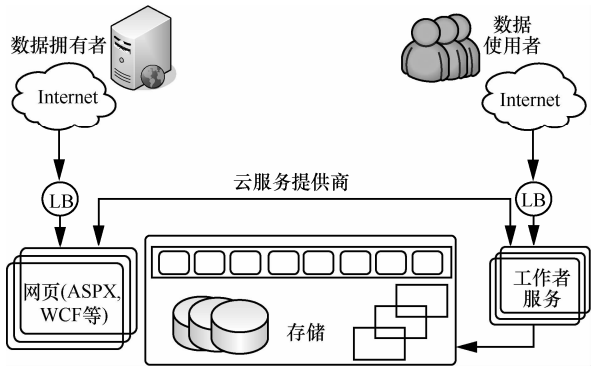

图 1 云数据服务模式

2 可信安全模型

2.1 可信安全模型定义

针对半可信状态，Matthew 等[2]在半可信的代理服务器的情况，提出用基于身份的代理重加密（IB-PRE, identity-based proxy re-encryption）来保证用户数据的安全。在 IB-PRE 框架中，代理服务器在不知道明文内容的情况下，能将数据拥有者（DO, data owner）加密后的密文转换成数据使用者（DU, data user）用自己的私钥能解开的密文。这样 DO 的明文数据不会泄露给代理服务器。Han 等[3]发现 IB-PRE 框架不能抵抗合谋攻击，不能直接应用于云环境下，随后对 IB-PRE 进行了改进，针对数据存储的应用环境，提出了基于身份的数据存储策略来抵抗合谋攻击。然而对于数据服务而言，IB-PRE 的模式并不适合云环境，因为代理服务器具有的极高的权利，一旦它被操控，可以为任何未授权的用户生成其可解的密文数据，无法保障数据拥有者的权利[4]。不过，利用重加密手段能生成中间密文版本的去屏蔽 CSP 对数据获取的方案是非常可取的。Yang 等[5]采用重加密手段专门对云环境下数据用户权限撤销问题进行研究，提出数据用户访问控制策略，将不同权限的用户进行区别，密钥管理时仅需对云端操作即可，并提到重加密可以使云端的用户数据保密，不同权限的用户能得到不同的内容。此外，Zhao 等[6]在半可信的 CSP 环境下，研究密文和加密方法之间的关系，利用云端对已加密数据再次加密，用户通过已有的公钥和私钥对重加密密文解密，提出了一种重加密方案。而此方案中 DO 的密钥并没有参与对明文进行保护，导致 DO 将过多的信息和权限置于 CSP 和 DU，易导致合谋攻击。针对上述问题和云环境下数据服务的特点，提出了一种可以抵制合谋攻击的重加密安全模型。

由于 CSP 拥有对云端用户数据访问和控制的权利，在半可信的状态下，CSP 对用户数据保持着好奇，可能会发生篡改等行为。一旦 CSP 频繁地发生篡改，其可信状态应定义为不可信，应停止其继续进行服务。故 CSP 的半可信状态自身是一种变化的状态，它可能变化为可信状态和不可信状态，一旦变化为不可信状态，而数据服务安全方案又没有进行相应的调整，将带来不可挽回的损失，本文通过重加密数据服务安全协议来记录 CSP 发生的篡改等严重恶意行为。因此，为了确保云环境数据服务的安全，需要结合 CSP 数据服务的状况进行可信评价研究。

在当前的可信评价模型中，存在着主观评价和客观评价。王守信等[7]在信任云的基础上，提出一种基于云模型的主观信任量化评价方法。该方法使用主观信任云的期望和超熵对信任客体信用度进行定量评价，进而设计一种信任变化云刻画信任客体信用度的变化情况，为进一步的信任决策提供依据，但在 CSP 状态的变化上不是很可取。顾鑫等[8]提出将云理论与信任的概念相结合，从主观的角度讨论安全应用的可信度评价模型。孟祥怡等[9]针对开放网络中可信管理中的难点，提出了一种基于云

模型的主观信任管理方案。该方案利用云理论中的模糊性和不全定性，从主观的角度对可信进行分析，提出了主观信任评价模型。胡春华等[10]提出了基于概率密度函数来表征服务实体间的信任度客观评价模型，通过概率密度信任关系的计算、推理及合并的演化方法来实现。而对于云环境下，CSP 的可信状态是动态变化的，对其评价不能单独地采用主观或客观评价，需要提出一种综合时效、主观和客观考虑的可信评价方案，通过时效模型来动态地、准确地评价 CSP 的可信状态。

针对以上情况，本文提出云环境数据服务可信重加密安全模型（TRSM, trust re-encryption secure model），通过合理的重加密方法对数据进行保护，防止云端用户数据的内容泄露，通过有效的可信评估模型来判断 CSP 的可信状态，为安全重加密算法提供可信应用环境。只有在保证云服务提供商的可信程度在一定范围内，结合有效的安全手段才能保证数据服务在云环境下的安全性。

TRSM 包括重加密安全模型、重加密数据服务安全协议、可信评价模型。对于一个未知可信状态的 CSP，先假设它是半可信状态，生成重加密安全算法，按照重加密数据服务安全协议执行重加密安全模型，然后对运行的结果进行可信评价，确定 CSP 的可信状态，如果 CSP 符合完全可信状态的定义，则可以按照传统的数据服务安全进行处理；如果 CSP 符合不可信状态的定义，则建议停止其 CSP 服务；如果 CSP 符合半可信状态的定义，则可以按照可信重加密安全模型进行数据服务。

2.2　重加密模型定义

本文提出的重加密模型分为 3 个部分，分别是 DO 的第一次加密、CSP 端的第二次加密以及最终用户端的解密操作，形式化描述如下。

1) 系统建立 $Setup(K)\to\lambda_1,\lambda_2$，系统以 K 为安全参数生成公开参数 λ_1,λ_2。

2) DO 利用密钥生成算法生成密钥 $KeyGen(\lambda_1,\lambda_2)\to(k_1,k_1^{-1}),(k_2,k_2^{-1})$。DO 根据 λ_1,λ_2 生成用户的 2 组公私钥对 $(k_1,k_1^{-1}),(k_2,k_2^{-1})$。

3) DO 对数据明文 X 的第一次加密，其中，加密操作为 $Enc_1(\cdot,\cdot)$，加密密钥为 k_1，解密操作为 $Dec_1(\cdot,\cdot)$，解密密钥为 k_1^{-1}，产生的密文为 X_{e1}。

加密 $Enc_1(X,k_1)\to X_{e1}$；解密 $Dec_1(X_{e1},k_1^{-1})\to X$。

4) CSP 只得到公钥 k_2，在云端进行重加密，第二次加密操作为 $Enc_2(\cdot,\cdot)$，加密密钥为 k_2，产生的密文为 X_{e2}。

重加密 $Enc_2(X_{e1},k_2)\to X_{e2}$。

5) DU 对重加密密文进行解密得到明文 X，其解密密钥是由 DO 生成的。考虑到用户权限和数据安全等级，有以下定义。

定义 1　重加密模型中数据明文集 $X=\{x_1,x_2,x_3,\cdots,x_p\}$，即明文集拥有 p 个安全等级的数据明文；假设数据用户 DU 集合为 $U=\{u_1,u_2,u_3,\cdots,u_q\}$，即表示有 q 用户权限等级。访问权限等级为 i 的用户 u_i 对应的身份认证符为 ID_i，与之对应的重加密的解密密钥为 k_i^{-1}，且由 DO 在通信时刻生成，其中 $i\in b$。

定义 2　定义重加密密文解密密钥生成算法为 $f_{\text{rekey}}(\cdot,\cdot)$，则有 $f_{\text{rekey}}(k_1^{-1},k_2^{-1})=k_i^{-1}$。

定义 3　若已知重加密密文为 X_{e2}，定义其解密算法为 $Dec_0(\cdot,\cdot)$，则有重加密密文解密 $Dec_0(X_{e2},k_i^{-1})\to X$。

当 DO 分配给用户 u_i 的解密密钥为 k_i^{-1} 时，用户 u_i 从 CSP 得到重加密密文为 X_{e2i}，则解密过程可表示为 $Dec_0(X_{e2i},k_i^{-1})\to X_i$，其中 $i\in b$。

通过以上定义可以看出，DO 只需进行第一次加密，在改变第二层的加密密钥时，便可以实现密文版本转变和 DU 密钥权限的撤销。从上述分析中，可以得到重加密模型的 2 个基本性质，也是形成重加密算法的 2 个基本条件。

性质 1　重加密算法具有普适性，加密算法都可以通过 2 次加密获得重加密密文。

$$X_{e2i}=Enc_2(X_{e1i},k_2)=Enc_2(Enc_1(X_i,k_1),k_2)$$

性质 2　重加密密文不是逐级解密，在满足一定的条件下能实现对密文直接解密。

$X_i=Dec_0(X_{e2i},k_i^{-1})$，其中 $k_i^{-1}=f_{\text{rekey}}(k_1^{-1},k_2^{-1})$，$Dec_0(\cdot,\cdot)$ 为公开的标准解密算法。

其安全模型在第 3 节论述。

2.3　重加密数据服务安全协议定义

在重加密模型的步骤 4）中，DO 将密文数据操作权限委托给 CSP 来处理。而半可信 CSP 可以按照 DO 的指令将正确的重加密数据发送给 DU，同时也可以将经过篡改的错误数据进行发送，使 CSP 对发送 DU 的密文篡改成为可能。为了防止 CSP 发生篡改等严重恶意行为，并对其发生次数进行记录（该记录也是 CSP 可信评价中的一个指标），

本文设计重加密数据服务安全协议。

在 DO 授权时和 DU 在接收重加密密文之前，分别进行身份验证和数据验证，保证接收者和数据本身的正确性。协议中假设通信信道安全，2 次验证算法为 $Ver_{DO}(ID_i)$ 和 $Ver_{DU}((ID\oplus L)_{e1i},X_{e2i},k_i^{-1})$，其协议交互步骤如下。

初始状态为 DO 调用密钥生成算法产生 2 层加密密钥对 (k_1,k_1^{-1}) 和 (k_2,k_2^{-1})。

1) DO 调用第一层加密算法对消息 X_i 进行加密，$X_{e1i}\leftarrow Enc_1(X_i,k_1)$ 并存储于云端。

2) DU 向 DO 申请访问数据，并利用散列函数生成身份信息 ID_i 作为验证标识。

3) DO 调用验证算法 $Ver_{DO}(ID_i)$，$bool(Ver_{DO}(ID_i)==ID_i)$。

确认 DU 身份后对 $(ID_i\oplus L)$ 进行 k_1 加密，并调用 $f_{\text{rekey}}(\cdot,\cdot)$ 算法生成 $k_i^{-1}=f_{\text{rekey}}(k_1^{-1},k_2^{-1})$。同时令 CSP 利用密钥 k_2 对 $((ID\oplus L)_{e1i},X_{e1i})$ 进行重加密生成密文 X_{e2i}。此时密文中包括 2 部分信息，一部分为用户 DU 的身份 ID_i 和长度信息 L，另一部分为数据密文信息。

4) 如果此时 CSP 将 X_{e2i} 改为 X'_{e2i}，并将 X_{e2i} 或 X'_{e2i} 重加密密文传输给 DU。

5) DU 接收到重加密密文后，根据调用 $Ver_{DU}((ID_i\oplus L)_{e1i},X_{e2i},k_i^{-1})$ 验证算法首先判断身份和长度信息是否为正确即 $bool(Ver_{DU}(X'_{e2i},k_i^{-1})==ID_i\,\|\,Ver_{DU}(X'_{e2i},k_i^{-1})==L)$。

如果重加密密文是 X'_{e2i}，则导致 DU 无法解析正确的 ID_i 和长度信息而拒绝接收数据，交互失败并记录 C。其重加密数据服务安全协议如图 2 所示。

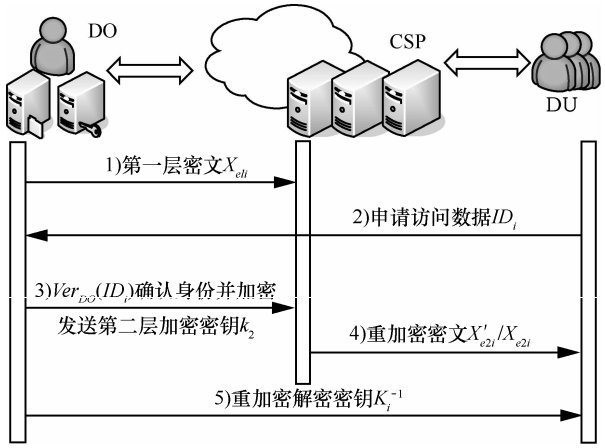

图 2 重加密数据服务安全协议

2.4 可信模型定义

本可信模型从客观评价和主观评价 2 个方面对 CSP 可信度进行评估。客观可信评价主要反映的是提供服务的 CSP 的基础设施的整体状态和性能，即对 CSP 中影响服务质量的因素的评价。它包括服务资源节点的服务时长、节点吞吐量、服务成功率、响应时间等。主观可信评价代表了用户对服务结果的满意程度，也是对服务的主观衡量，具有一定的模糊性。对于主观可信评价，需要从用户对服务注重的方面进行影响因子筛选，包括服务风险、服务满意度等，评价模型如图 3 所示。

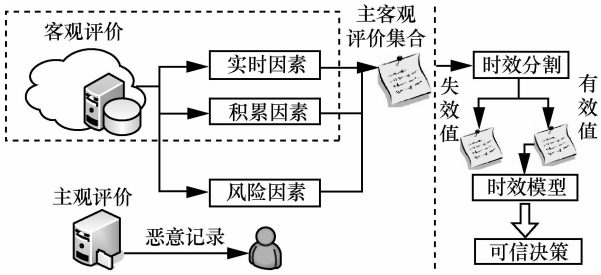

图 3 可信评价模型

为了方便描述，可以将这些评价因素定义为一系列的评价指标，确定评价指标论域 $U=\{u_1,u_2,u_3,\cdots,u_n\}$ 并归类主客观指标，有客观指标论域 $U_{obj}=\{u_1,u_2,u_3,\cdots,u_x\}$ 和主观指标论域 $U_{sub}=\{u_{x+1},u_{x+2},u_{x+3},\cdots,u_n\}$，通过以上分析，本文设计的云环境下可信评价模型可以表示为

$$T(t)=(1-\lambda)T_{\text{obj}}(t)+\lambda T_{\text{sub}}(t),\lambda\in[0,1] \qquad (1)$$

其中，$T(t)$ 为主客观可信评价结果；$T_{\text{obj}}(t)$ 为客观可信评价结果；$T_{\text{sub}}(t)$ 为主观可信评价结果；λ 为调整因子，调节主客观可信评价在最终可信评价中占有的比重；t 为当前评价时刻。另外，令式（1）中 λ 等于 0 时，则有 $T(t)=T_{\text{obj}}(t)$，此时可以将 $T_{\text{obj}}(t)$ 看作为 CSP 对加入陌生节点的可信性判断，评价指标的含义也会发生相应变化。

式(1)给出了可信评价应该考虑的主客观因素，同时定义可信等级论域 V 为 3 级{可信，不完全可信，不可信}，这 3 级分别描述了对服务质量的评价程度，对应着 CSP 的可信度。假设可信程度值在[0,1]中取值，则规定论域界限 $\eta\in[0,1]$（可根据需要调整）如下

$$V=\begin{cases} \text{可信} & , \quad 1 \\ \text{不完全可信} & , \quad \eta \leqslant T(t)<1 \\ \text{不可信} & , \quad 0 \leqslant T(t)<\eta \end{cases}$$

在主客观可信评价中，并不能对云环境下所有的影响因素全部分析，同时为了简化模型计算，本文在选择评价指标时先根据影响性质进行影响因素分类，选取每类影响因素中相对关键指标进行综合评价。

客观评价模型 $T_{\text{obj}}(t)$ 是对证据的收集分析后逻辑量化值，它主要包括实时因素模型和积累因素模型分别为 T_{real} 和 T_{history}。主观评价模型 $T_{\text{sub}}(t)$ 反映的是人类在日常活动中对证据的判断而形成的最终思维结果，主要包括风险因素模型为 T_{risk}。

其主客观可信时效模型在第 4 节进行论述。

3　重加密安全模型

3.1　复杂性假设

定义 4　（求解 RSA 困难假设）若给定大质数 q，p 满足 $\gcd(e,(p-1)(q-1))=1$，$N=pq$，对于任何概率多项式时间图灵机 T，有任意小正数 ε 满足

$$\Pr[T(N,e,m^e(\bmod N)=m]-\frac{1}{N}<\varepsilon \qquad (2)$$

即计算性 RSA 问题在多项式时间内不可解。

3.2　安全模型

利用随机预言机将重加密安全模型证明过程定义为一个游戏。在模型中存在一个攻击者和仿真者，仿真者拥有解答攻击者问题的所有困难知识，确保能对攻击者提出的所有问题能以一定正确概率的询问回应。首先由仿真者提出确定的挑战，如果仿真游戏挑战的成功概率为可忽略的值，那么挑战失败，同时也证明了该问题在符合实际情况条件下的不可计算性，反之则不困难，其中攻击者 T 能通过询问和自身能力获得存储在 CSP 端的数据密文对应的明文。安全模型描述如下。

1) 建立：重加密模型运行算法 $KeyGen(\cdot)$，$f_{\text{rekey}}(\cdot,\cdot)$ 以及安全参数 λ，得到 2 层密钥对 (k_1,k_1^{-1})，(k_2,k_2^{-1}) 和重加密解密密钥 k_i^{-1}。攻击者可得到系统参数，而重加密解密密钥 k_i^{-1} 只被重加密模型内的 DO 和 DU 所知。

攻击者可以进行下述动作。

2) 查询：攻击者可以根据自身的需求，适应性地做出一系列如下任何一种询问。

① 用户密钥对产生预言机 O_{KeyGen}：利用密钥产生算法获得密钥对 $(\hat{k},\ \hat{k}^{-1})\leftarrow KeyGen(\lambda)$。以一定正确概率返回密钥对 (k^*,k^{-1*})。

② 重加密解密密钥产生预言机 O_{rekey}：攻击者输入 2 个密钥对 $(\hat{k}_1,\hat{k}_1^{-1})$ 和 $(\hat{k}_2,\hat{k}_2^{-1})$，该预言机以一定正确概率返回攻击者 k_i^{-1*}，且 $k_i^{-1*}=f_{\text{rekey}}(\hat{k}_1^{-1},\hat{k}_2^{-1})$。

针对不同的攻击者，存在如下 4 种攻击。

攻击游戏 1　外部攻击者（除 DO、DU、CSP 外）攻击重加密模型中第一层的加解密过程。

在重加密模型公开系统参数后，攻击者利用公开的加密密钥 k_1 和 k_2，不断尝试获取重加密数据密文，最后利用公开的解密算法的构成来解密重加密密文。而重加密模型仅公开加密公钥，攻击者只能靠猜想密文的方式来对重加密模型进行攻击。所以对于任意概率多项式时间敌手 T，$\hat{X}_{e1}$ 为攻击者猜测的重加密密文，$\frac{1}{|F|}$ 是攻击成功的概率，对任意小的正数 ε 有

$$\Pr[T(\hat{X}_{e1})=X\,|\,T(k_1,k_2)=k_1^{-1}]-\frac{1}{|F|}<\varepsilon \qquad (3)$$

即攻击者时间敌手 T 由密文求出明文的概率等于猜测概率。对于外部攻击者，在没有足够信息的情况下对重加密模型进行攻击的成功率几乎可以忽略不计。所以重加密模型在应对外部威胁上是比较可靠的。

攻击游戏 2　DU 作为攻击者的情况下，拥有 CSP 发送的重加密密文和重加密解密算法，且同时拥有从 DO 端发送的重加密解密密钥。

假设攻击者 DU 获得 k_i^{-1}，由于 $k_i^{-1}=f_{\text{rekey}}(k_1^{-1},k_2^{-1})$，从 k_i^{-1} 直接推出 (k_1^{-1},k_2^{-1}) 的可能性取决于算法 DO 的密钥生成算法 $f_{\text{rekey}}(\cdot,\cdot)$。而 $f_{\text{rekey}}(\cdot,\cdot)$ 只由 DO 掌握，所以 DU 只能靠自身能力逆推出算法中的参数 k_1^{-1}。即使假设攻击者 DU 拥有逆推出 k_1^{-1} 的能力，则 DU 还需要获取 CSP 端存储的所有密文内容 X_{e1}。对于 DU，其只拥有对 X_{e1i} 的访问权限，而 $X_{e1i}\not\subset X_{e1}$，所以 DU 对全部密文的攻击也只能属于猜测攻击。因此 DU 攻击者攻击的重点放在如何通过 k_i^{-1} 获取全部重加密密文和对应的解密密钥上。

同理，跟攻击游戏 1 有同样的分析。重加密模型仅公开加密公钥，攻击者只能靠猜想密文的方式来对重加密模型进行攻击。所以对于任意概率多项式时间敌手 T，$\hat{X}_{e1}$ 为攻击者猜测的重加密密文，$\hat{k}_2^{-1}$ 为猜测密钥第二层解密密钥，对任意小的正数 ε 有

$$\Pr[T(\hat{X}_{e1})=X \mid T(k_i,\hat{k}_2^{-1})=k_1^{-1}]-\frac{1}{|F|}<\varepsilon \quad (4)$$

式(4)表示攻击者时间敌手由密文求出明文的概率接近猜测概率。

攻击游戏 3 攻击者 CSP 拥有第一层密文且同时拥有重加密的第二层加密密钥，其最理想的攻击方式是直接攻击 DO 第一层的加密密钥。CSP 作为攻击者利用公开的加密算法、公开的加密密钥 k_1 以及第一层加密数据 X_{e1}，对第一层的解密密钥进行攻击。攻击游戏过程如下。

① 获取公开的加密算法、公开的加密密钥 k_1 以及第一层加密数据 X_{e1}

② 假设攻击者 CSP 在拥有 k_1 的情况下对上述预言机 O_{KeyGen} 提出询问，上述预言机以一定概率返回可能的 k_1^{-1*}。

③ 攻击者 CSP 结合自身能力求解密钥生成算法的求逆问题，最终通过第一层加密密文 X_{e1} 和 k_1^{-1*} 获得明文消息合集 X。

当且仅当对于系统参数 $n\in \text{deploy}(\lambda)$，任何一个非零的数 n 和所有的概率多项式时间（PPT）算法，下面的概率是可以忽略的，则重加密模型在攻击游戏 3 中具有安全性。

$$\Pr[(\hat{k}_j,\ \hat{k}_j^{-1})\leftarrow KeyGen(\lambda)_{j\in[0,n]},(t,X,k_1^{-1}) \leftarrow T^{O_{KeyGen}}(X_{e1},k_1,\hat{k}_j^{-1})] \quad (5)$$

式(5)前半部分的含义是攻击者通过的系统安全参数产生所有可能的 n 对公私钥。后半部分的预言机 O_{KeyGen} 输入的系统参数 λ，该预言机输出为可能的第一层解密密钥 k^{-1*}；最后由概率多项式时间算法输出所用时间开销与全部明文信息 X。

同理，在以上的假设条件约束下，重加密模型仅公开加密公钥，攻击者只能靠猜想密文的方式来对重加密模型进行攻击。所以对于任意概率多项式时间敌手 T，对任意小的正数 ε 有

$$\Pr[(\hat{k}_j,\ \hat{k}_j^{-1})\leftarrow KeyGen(\lambda)_{j\in[0,n]},(t,X,k_1^{-1}) \leftarrow T^{O_{KeyGen}}(X_{e1},k_1,k^{-1*})]$$

$$=\Pr[T(X_{e1})=X \mid T(k_1,k_2)=k_1^{-1}]-\frac{1}{|F|}<\varepsilon \quad (6)$$

即攻击者通过公钥求私钥的概率可以忽略不计，攻击者时间敌手 T 由密文求出明文的概率接近猜测概率。

通过以上分析可知，不论是外部攻击者还是单独的 DU、CSP 攻击，对于 DO 的明文获取的概率都接近于猜测攻击，而猜测攻击的成功率几乎可以忽略不计。所以，该重加密模型对于单一角色攻击具有较高的安全性。

攻击游戏 4 CSP 和 DU 合谋攻击 DO，试图获取 DO 的第一层加密密文的解密密钥，从而通过公开的解密算法获取 DO 的所有明文数据。

CSP 和 DU 作为攻击者 T 的攻击过程如下。

① 合谋获取第一层加密密文 X_{e1} 以及 DU 重加密解密密钥 k_i^{-1}。

② 由于攻击者获知 $k_i^{-1}=f_{\text{rekey}}(k_1^{-1},k_2^{-1})$，而在攻击游戏 3 中，攻击者对预言机 O_{KeyGen} 提问找出 k_1^{-1*} 的概率已被证明可以忽略。所以攻击者在游戏 4 中直接对预言机 O_{rekey} 提出 k_i^{-1*} 的询问，并将满足 $k_i^{-1*}=f_{\text{rekey}}(\hat{k}_1^{-1},\ \hat{k}_2^{-1})$ 条件的 $\hat{k}_1^{-1}$ 和 $\hat{k}_2^{-1}$ 进行记录。

③ 仿真者给出任意密文 X_e（对应的明文为 X），攻击者利用获得的 $\hat{k}_1^{-1}$ 和公开的解密算法求出 $Dec_1(X_e,\hat{k}_1^{-1})\rightarrow\hat{X}$，若 $\hat{X}=X$，则挑战成功；否则挑战失败。

则重加密模型在攻击游戏 4 下具有安全性，当且仅当对于系统参数 $n\in \text{deploy}(\lambda)$，任何一个非零的数 n 和所有的概率多项式时间（PPT）算法，下面的概率是可以忽略的。

$$\Pr[\hat{k}_{j\in[0,n]}^{-1},\ \hat{k}_{z\in[0,n]}^{-1},(t,X,k_1^{-1})\leftarrow T^{O_{\text{rekey}}}(X_{e1},k_i^{-1},\hat{k}_z^{-1},\ \hat{k}_j^{-1})] \quad (7)$$

式(7)前半部分的含义是攻击者通过的参数产生可能的 n 个密钥。后半部分的预言机 O_{rekey} 输入是 2 个密钥，分别代表第一层加密密钥和第二层加密密钥，该预言机输出为 k_i^{-1*}，k_i^{-1} 用于输出密钥的正确性对比。最后由概率多项式时间算法输出所用时间开销，全部明文信息 X 及正确的 k_1^{-1}。

综合以上几种攻击游戏来看，重加密模型在抵抗单一角色攻击方面有着比较突出的优势，其主要原因是重加密方案利用了密码学中解决数学困难

的复杂性。攻击者在只知道密文、公钥任意一者的情况下去求解 DO 数据明文的可能性往往接近或者等于猜测攻击。而在合谋攻击的情况下，重加密方案的安全性的决定因素则发生了改变。通过攻击游戏 4 分析可知，攻击者在对重加密模型进行攻击时，可以通过合谋攻击绕过对已知的数学困难进行求解，而直接通过分析 $f_{\text{rekey}}(\cdot,\cdot)$ 就有可能获得 DO 的第一层加密密钥。此时，DO 的第一层密钥是否安全取决于 DO 的重加密密钥生成算法 $\hat{k}_i^{-1} = f_{\text{rekey}}(\hat{k}_1^{-1}, \hat{k}_2^{-1})$ 是否能通过 $\hat{k}_i^{-1}$ 和已知信息逆向推导出 $\hat{k}_1^{-1}$。

DO 所拥有的重加密密钥算法 $f_{\text{rekey}}(\cdot,\cdot)$ 并没有固定的形式，在本文提出的重加密模型下，密钥算法随着选择的加密算法改变而改变。为了进一步说明重加密模型对数据的安全保护作用以及得到重加密密钥算法 $f_{\text{rekey}}(\cdot,\cdot)$ 对合谋攻击有抵抗性的约束条件，本文将 2 种经典的加密算法代入重加密模型进行验证，根据定义的重加密模型，设计合适的重加密密钥算法 $f_{\text{rekey}}(\cdot,\cdot)$ 并对抗合谋攻击的安全性进行讨论。

3.3　重加密模型算法验证

针对现今密钥体制的分类，分别进行对称密钥和公钥密钥算法进行算法验证。序列密码属于对称密钥体制采用典型的序列密码算法，公钥体制采用典型的 EIGamal 密码算法。

3.3.1　基于序列密码的重加密算法

根据重加密模型的定义，需要找到合适的 $f_{\text{rekey}}(\cdot,\cdot)$ 和 $Dec_0(\cdot,\cdot)$ 使重加密方案成立。假设权限 i 用户 u_i 对 DO 请求的数据为 X_i，于是基于序列密码的重加密过程为

$$X_{e1i} = Enc_1(X_i, k_1) = X_i \oplus k_1$$

$$X_{e2i} = Enc_2(X_{e1i}, k_2) = X_{e1i} \oplus k_1 = X_i \oplus k_1 \oplus k_2$$

其中，$\oplus$ 表示加密操作。

从重加密密文的解密过程进行分析，对应的逐级解密过程如下。

$$X_i = Dec_1(X_{e1i}, k_1^{-1}) = Dec_1(Dec_2(X_{e2i}, k_2^{-1}), k_1^{-1})$$

$$= X_{e2i} \oplus k_2^{-1} \oplus k_1^{-1} = Dec_0(X_{e2i}, k_i^{-1}) \quad (8)$$

通过简单分析式(8)，当且仅当 $k_i^{-1} = f_{\text{rekey}}(k_1^{-1}, k_2^{-1}) = k_2^{-1} \oplus k_1^{-1}$ 时（利用异或操作的自反性质），存在解密算法 $Dec_0(\cdot,\cdot)$ 满足性质 2，且为标准的使序列密码解密算法。此时，重加密的存在性得到了证明，同时也找出了相应的解密密钥算法 $f_{\text{rekey}}(\cdot,\cdot)$。

对合谋攻击进行分析，若 CSP 与 DU 合谋攻击，则攻击者已知的信息有 DU 的 k_i^{-1}、第一层密文 X_{e1} 以及第二层加密密钥 k_2。由于采用的是对称加密体制，所以有 $k_2 = k_2^{-1}$。由于序列密码重加密的整个过程比较简单，假设攻击者有能力推导解密密钥算法 $k_i^{-1} = f_{\text{rekey}}(k_1^{-1}, k_2^{-1}) = k_2^{-1} \oplus k_1^{-1}$。

由异或操作的自反性质可知，$k_i^{-1} = k_2^{-1} \oplus k_1^{-1} \rightarrow k_1^{-1} = k_i^{-1} \oplus k_2^{-1}$。

攻击者在获得 k_1^{-1} 后，可以利用公开的解密算法 $X \leftarrow Dec_1(X_{e1}, k_i^{-1})$。

对于序列密码而言，攻击者通过分析解密密钥算法 $f_{\text{rekey}}(\cdot,\cdot)$ 非法获取了 DO 存储在云端的全部明文数据。所以在采用对称加密体制的序列加密作为加密算法的情况下，重加密模型并不能安全地抵挡 CSP 和 DU 的合谋攻击，数据的机密性不能得到保证，所以该算法不适合于重加密安全模型。

3.3.2　基于 ElGamal 密码的重加密算法

根据重加密模型的定义，需要找到合适的 $f_{\text{rekey}}(\cdot,\cdot)$ 和 $Dec_0(\cdot,\cdot)$ 使重加密方案成立。在参数生成阶段，选取大素数 p 和本原元 $\alpha \in F_p^*$。由于采用公钥密钥体制产生公私钥对 (k, k^{-1})，令第一层 ElGamal 算法的公私钥对为 (k_1, k_1^{-1})，第二层加密算法的公私钥对为 (k_2, k_2^{-1})，公开的系统参数为 k_1、k_2 和 p_1、p_2、α_1 和 α_2。则对于任意明文 $X_i \in Z_p$，重加密方案中有如下加密过程

$$X_{e1i}\{C_{1i}, C_{2i}\} = Enc_1(X_i, k_1); C_{1i} \equiv \alpha_1^{d_1} \bmod p_1;$$

$$C_{2i} \equiv X_i k_1^{d_1} \bmod p_1 \quad (9)$$

由于第一层加密返回 2 个密文 C_{1i} 和 C_{2i}，此时的重加密可以选择对 2 个密文同时进行重加密，或者仅对存在明文的信息 C_{2i}。在不损失安全性能的情况下，简化加密的复杂度，对含有明文信息的密文 C_{2i} 进行第 2 次加密处理。其过程可以表示为

$$X_{e2i}\{C_{1i}, C_{21i}, C_{22i}\} = Enc_2(C_{2i}, k_2); C_{1i} \equiv \alpha_1^{d_1} \bmod p_2,$$

$$C_{21i} \equiv \alpha_2^{d_2} \bmod p_2 \; C_{22i} \equiv C_{2i} k_2^{d_2} \bmod p_2 \quad (10)$$

其中，d_1 和 d_2 为随机选取的整数。

与序列密码步骤同样分析，ElGamal 加密算法的逐级解密过程如下

$$X_i \equiv Dec_1(X_{e1i},k_1^{-1}) \equiv Dec_1(Dec_2(X_{e2i},k_2^{-1}),k_1^{-1})$$
$$\equiv C_{22i} \times (\alpha_2^{d_2} \bmod p_2)^{-k_2^{-1}} \times (\alpha_1^{d_1} \bmod p_1)^{-k_1^{-1}}$$
$$\equiv Dec_0(X_{e2i},k_i^{-1}) \tag{11}$$

为了方便寻找可行的重加密密文的解密算法，不妨假设 2 次加密的密钥都基于同样的系统参数生成（等同于在同系统参数下生成两对公私钥），即有 $p_1 = p_2 = p$、$\alpha_1 = \alpha_2 = \alpha$，则将式(11)变为

$$X_i \equiv X_{e2i} \times \alpha^{-d_2 sk_2 - d_1 sk_1} \bmod p \tag{12}$$

注意：随机数 d_1 和 d_2 必须不同，这是因为采用相同随机数，通过 2 次明文和密文的对比会导致明文泄露。假设 $d_1 = d_2$ 加密了 2 个消息 m 和 m' 得到对应的密文为 (c_1,c_2) 和 (c_1',c_2')，则有 $\frac{c_2}{c_2'} \equiv \frac{m}{m'} \bmod p$ 成立。当 m 已知时，则很容易求出 m'，导致第 2 次的信息明文泄露。

为了标准化重加密密文解密算法 $Dec_0(\cdot,\cdot)$，对式(12)进行 ElGamal 算法标准重定义，可将其简化为

$$X_i \equiv C_2' \times C_1'^{k'^{-1}} \tag{13}$$

其中，前半部为 $C_2' \equiv X_i(k_1^{d_1} \times k_2^{d_2})^{d'} \bmod p$，后半部为 $C_1' \equiv \alpha^{d'} \bmod p$，解密密钥为 $k'^{-1} = -d_2 sk_2 - d_1 sk_1$，随机整数 $d' \neq d_1 \neq d_2 \in [1, p-2]$。

经过重新定义后，需要在 CSP 端的对加密处理做出相应调整，将原来形式的 $X_{e2i}\{C_{1i},C_{21i},C_{22i}\}$ 变为 $X_{e2i}\{C_1',C_2'\}$ 且 DO 加密端也需要同时约定随机数 d'，加密过程更新为

$$X_{e1i}\{C_{1i},C_{2i}\} = E_1(X_i,k_1);\ C_{1i} \equiv \alpha_1^{d_1 d'} \bmod p_1;$$
$$C_{2i} \equiv X_i k_1^{d_1 d'} \bmod p_1 \tag{14}$$

通过上述调整，最终可以找到重加密解密密钥生成算法

$$k_i^{-1} = f_{\text{rekey}}(k_1^{-1},k_2^{-1}) = -d_2 k_2^{-1} - d_1 k_1^{-1}$$

且 $Dec_0(\cdot,\cdot)$ 满足性质 2，符合标准的 ElGamal 算法标准。

其合谋攻击分析如下。

若 CSP 与 DU 合谋攻击，结合以上找到的解密算法进行安全分析。假设攻击者能根据自身能力推导出 $f_{\text{rekey}}(k_1^{-1},k_2^{-1})$，而且能合法获得 k_1、k_2、X_{e1} 和 k_i^{-1} 的情况下，则攻击者将攻击数据明文 X 问题转化为通过 $k_i^{-1} = f_{\text{rekey}}(k_1^{-1},k_2^{-1}) = -d_2 k_2^{-1} - d_1 k_1^{-1}$ 求解 k_1^{-1} 的问题。

在 ElGamal 算法中，安全密钥的长度为 1 024 bit，那么 k_1 和 k_2 的长度都应为 1 024 bit 或者更长。根据密钥生成算法 $k_i^{-1} = f_{\text{rekey}}(k_1^{-1},k_2^{-1}) = -d_2 k_2^{-1} - d_1 k_1^{-1}$ 可知，DO 得到的密钥 k_i^{-1} 的长度至少为 1 024 bit。证明此式安全的最直接的方式就是证明符合算法公式的 k_1 和 k_2 的解大于 $2^{1\,024}$ 对。因为攻击者若对密钥进行猜测攻击，完成整个过程最多需要 $2^{1\,024}$ 次。如果 k_1 和 k_2 的组合变化大于对密钥猜测的次数，则 $k_i^{-1} = f_{\text{rekey}}(k_1^{-1},k_2^{-1}) = -d_2 k_2^{-1} - d_1 k_1^{-1}$ 能抵抗合谋攻击。由于该式从数学无法求出 k_1 和 k_2 的组合变化，所以不妨假设存在相同的随机数,且都为 p−2，那么 $k_i^{-1} = f_{\text{rekey}}(k_1^{-1},k_2^{-1}) = -d_2 k_2^{-1} - d_1 k_1^{-1}$ 可以简化为 $k_i^{-1} = -(p-2)(k_2^{-1} + k_1^{-1})$。

由于 $(k_2^{-1} + k_1^{-1})$ 的长度必然超过 1 024 bit，所以只要 p 足够大，上式求解的困难则可以转化为对大数分解问题的求解。又因为大数分解问题是 RSA 密码所基于的数学困难，根据定义 4 可知，对于大数分解成功的概率是可以忽略不计的；再者即使攻击者能成功分解出 p−2 和 $(k_2^{-1} + k_1^{-1})$，还需要对 $(k_2^{-1} + k_1^{-1})$ 的组合进行确定。所以在 p 足够大的情况下，对于系统参数 $n \in \text{deploy}(\lambda)$，任何一个非零的数 n 和所有的概率多项式时间（PPT）算法，成功概率可以转化为

$$\Pr[\hat{k}_{j\in[0,n]}^{-1},\ \hat{k}_{z\in[0,n]}^{-1},(t,X,k_1^{-1}) \leftarrow T^{O_{\text{rekey}}}(X_{e1},k_i^{-1},\ \hat{k}_z^{-1},$$
$$\hat{k}_j^{-1})] < \Pr[T(N,e,m^e(\bmod N) = m] - \frac{1}{N} < \varepsilon \tag{15}$$

即攻击者的成功概率是可以忽略的。且 CSP 与多 DU 合谋时也无法获取 k_1^{-1}，根据算式 $k_i^{-1} = f_{\text{rekey}}(k_1^{-1},k_2^{-1}) = -d_2 k_2^{-1} - d_1 k_1^{-1}$，当增加了一个已知量时，同时增加 3 个未知量。所以在此种情况下，ElGamal 算法的重加密方案具有抗合谋攻击的能力。

3.4 算法约束条件

通过以上分析，可以得出以下 4 点重加密模型的加密算法选择条件。

1) $\forall E_1 = E_2$，$\exists f_{\text{rekey}}(\cdot,\cdot), Dec_0 \rightarrow Dec_0(X_{e2i},\ f_{\text{rekey}}(k_1^{-1},\ k_2^{-1})) = X_i$

以上约束条件表明 2 层加密方式相同的重加密模型下，选择的加密方法必须保证解密算法和解密生成密钥算法的存在，且需要一次解出密文。此要

求是建立重加密模型的基础，不相同的 2 层加密会给寻找带来很高的复杂度，如果复杂度过高使得无法找出合适的解密算法和解密生成密钥算法，那么重加密模型便无法实现。通常来讲，能找到的 2 层加密方式不同的重加密算法一般为多级解密方式，在解析密文过程很容易暴露第一层解密密钥的关键信息，CSP 通过合谋便能解开所有存于云端数据，这是要求能一次解密的根本原因。

2) $\forall E_1 = E_2$， $k \neq k^{-1} \mid k_1 \neq k_2$

上述条件约束了加密算法的加解密密钥的关系，要求加密解密密钥不同，同时第一层加密密钥不能同于第二层加密密钥。通过上文的分析可知，如果加密密钥等于解密密钥的话，那么 CSP 在处理数据的过程中就已经掌握了存储在云端密文的解密密钥，从序列密码重加密算法安全分析可知，对称密钥体制的重加密模型无法抵抗的 CSP 与 DU 的合谋攻击。另外，如果 2 层加密密钥 $k_1 \neq k_2$，这将导致 $f_{\text{rekey}}(\cdot,\cdot)$ 的抗合谋攻击性大大降低，攻击者很容易从推导出的 $f_{\text{rekey}}(\cdot,\cdot)$ 获得 DO 数据明文，使得 CSP 端数据隐私受到威胁。

3) $\forall f_{\text{rekey}}(\cdot,\cdot)$， $f_{\text{rekey}}(\cdot,\cdot)^{-1},(k_i^{-1}) \not\rightarrow k_1^{-1}$

这条约束可以理解为重加密模型下存在的解密密钥生成算法必须具有抗攻击性或为单向门限函数，即攻击者 CSP 在获得 $k_i^{-1} = f_{\text{rekey}}(k_1^{-1},k_2^{-1})$ 的情况下，极难求逆获得 k_1^{-1}。由于 $f_{\text{rekey}}(\cdot,\cdot)$ 算法是由 DO 自定义生成，而 $f_{\text{rekey}}(\cdot,\cdot)$ 的抗逆推特性保护了 DO 解密密钥的安全，同时也是抗合谋攻击的关键所在。在利用公钥密码体制寻找 $f_{\text{rekey}}(\cdot,\cdot)$ 时，可以适当将此抗逆推性转化为公钥密码学所基于的数学困难，这也是公钥密码体制易用于重加密模型的原因之一。

4) 对于多个 DU 的 k_i^{-1}，不能推导出 k_1^{-1}

这条约束主要是考虑到 DO 密钥的安全性。对于多个 DU 进行合谋攻击，能推导出 DO 的 k_1^{-1}，那么该重加密算法也不能满足保密性要求，DU 可以利用 DO 的加解密钥对 (k_1,k_1^{-1}) 对其他用户进行伪装攻击。

通过以上 4 个条件的约束分析，将文献[2,3,6,11]中的重加方案进行对比分析，文献[6]中是 2 次同样类型的加密，符合本文提出的模型设定要求。但由于不符合第 3)条，CSP 能轻易地根据密钥的分配信息推导出重密文的解密密钥，导致 CSP 端的密文得以解密，所以该方案并不能具备抗合谋攻击的能力。而文献[2,3,11]中，分别对比第 1)条、第 2)条可以发现，文献[2,3]找到了 2 层不同加密方式下的重加密算法，但在解密时采用的是分级解密方式，导致了第一层密文的关键密钥信息泄露，而第二层加密操作只是对密钥处理进行变化，根据条件 2)要求，对称密钥体制暂时无法很好保护解密密钥而导致合谋攻击。在文献[11]中只能保证主密钥的安全，而不能保证合谋攻击下云端存储数据的安全。因此，以上的重加密框架都不能很好适应于云环境数据服务的安全要求。

4　主客观可信时效模型

根据可信重加密安全模型定义，云服务提供商的可信性是安全的前提，对云服务提供商的可信程度的有效评价和监测是实现可信重加密安全不可或缺的基础。在开放的云环境下，云服务提供商的可信状态在一定程度上是不可控的动态变化的，如果不能有效认定或者辨别云服务提供商的可信状态，数据服务的安全性就不能得到有效保证。所以建立合适的可信评价模型，全面真实地评价云服务提供商的可信状态及其变化是非常必要的。建立主客观可信时效模型，一方面是借鉴已有的主客观可信评价机制，以实现对可信程度的评估，另一方面则通过时效模型，以准确反映可信状态的变化。

从客观可信评价的角度来讲，实时因素指标反映的是评价时刻的参数特性，而积累量反映的只是历史的经验积累，所以积累因素模型是要根据历史的积累量反映当前评价时刻的值，利用已知量来预测未知量。

对于实时因素的计算，采用对实时量进行一定时间的采样，然后对时间段内的采样样本进行分析。在较短的时间窗口 Δt 内的变化并不频繁，所以本文简单地利用加权平均法进行处理。有以下评价计算式

$$T_{\text{real}} = \sum_{j=1}^{m}\sum_{i=1}^{n} y_j(i)/mn \tag{16}$$

其中，$y_j(i)$ 是不同时间段 j 内不同指标 u_i 的采样值。

对于积累因素的计算，将积累量计算同化到统一的模型当中。如果有 i 个积累参量参与了评价，则有

$$T_{\text{history}}=\frac{T_{ht\_1}+T_{ht\_2}+\ldots+T_{ht\_i}}{i} \tag{17}$$

其中，T_{ht_i} 是每个指标 u_i 积累参量的值，可以根据实际的应用情况进行计算。

对于主观评价中的风险因素计算，在云环境下，构成风险的因素很多，比如数据灾难恢复风险、基础设备维护风险、信息泄露风险等。而从用户的角度来看，以上风险在云环境下都可以利用有效的机制规避，数据灾难风险可以采用数据多备份机制控制；信息泄露的风险可以利用加密手段对数据进行保护；并且部分措施和机制在云环境下 CSP 已经具备且实施，所以对于用户来讲，云环境中最大的风险为用户所需要的服务是否能被 CSP 安全有效的完成。

简单来看，用户利用云服务完成相关任务相当于用户与 CSP 之间发生交易，对于未知交易对象的可信衡量莫过于直接查看其交易的成功率，成功率高的拥有较高的可信度，反之则可信度较低。在利有效用机制规避其他风险的情况下，用户对云服务的风险判断主要取决于云服务历史服务成功率高低，所以本文在研究云服务成功率的基础上，设计云环境下计算风险因素模型。

在 CSP 提供云数据服务时，如果与部分 DU 合谋则可能获得用户 DU 对密文的验证方式，从而对其他 DU 进行篡改攻击。受到此类篡改攻击的 DU 是可以通过身份验证但会接收错误密文。此时的 CSP 行为属于恶意攻击，攻击次数用参数 C 表示。

假设至评价时刻 t 时，云服务的 m 次交互中，有 n 次成功交互，则有风险因素 T_{risk} 可以通过式(18)计算。

$$T_{\text{risk}}=\frac{n}{m+\sigma C} \tag{18}$$

其中，σ 为风险调节因子，C 为 CSP 恶意行为次数。

此处的参数 C 是由重加密数据服务安全协议记录的 CSP 严重恶意行为次数，普通的交互失败只表现在失败次数 $m-n$ 中。当 $C\geqslant 1$ 时，便表明 CSP 发动过篡改攻击，所以风险调节因子 σ 应相应地赋予较大的数值，使发动过篡改攻击的 CSP 的风险率大幅度提高。这里的 T_{risk} 与实际数值表示的含义相反，T_{risk} 越大表明风险越小，反之越大。

通过以上实时因素、积累因素和风险因素的模型设计可知，当主客观评价模型中对某类特性特别看重时，可以利用式(16)和式(17)进行主客观可信评价模型的求解。如果评价过程对各指标的权重没特殊要求，可以利用加权平均将式(1)转化为式(19)。

$$\begin{aligned}T(t)&=(1-\lambda)T_{obj}(t)+\lambda T_{sub}(t)\\&=\frac{(1-\lambda)}{2}(T_{\text{real}}+T_{\text{history}})+\lambda T_{\text{risk}}\end{aligned} \tag{19}$$

将主客观评价的集合进行时效处理，根据顾鑫[12]等提出的时效策略，得出针对云环境下重加密安全模型具有时效的可信评价方案如下

$$H_{\text{Trust}}=\begin{cases}\sum_{i=1}^{k}[(1-\lambda)T_{\text{obj}}(i)+\lambda T_{\text{sub}}(i)]*f_{\omega}(Time(T_i))-\\ \varepsilon\Delta x\otimes F(t-L), & 1\leqslant i\leqslant k\\ T(0), & i=0\end{cases} \tag{20}$$

其中，k 代表历史评价中有效评价个数，$f_{\omega}(Time(T_i))$ 表示时效权值，$\Delta x\otimes F(t-L)$ 表示时间衰减项，采用 Gumbel 估计，那么刻度参数 $\hat{\delta}>0$，当满足 $0\leqslant L+1/\gamma$ 时（在实际情况中可以实现），可以求得 $\partial H_{\text{Trust}}/\partial L<0$，即表示 H_{Trust} 是关于评价间隔时长 L 是单调递减的。如果采用逐级衰减法来计算，H_{Trust} 也是关于评价间隔时长 L 是单调递减的。当 L 足够长时，H_{Trust} 会减小到 0，这是符合信任随时间衰减的自然特点的。又因为规定 H_{Trust} 的取值范围在[0,1]之间，所以当 H_{Trust} 小于 0 时，取值仍为 0。

5 存在的问题与展望

通过上述的研究，形成了云环境数据服务可信安全模型，可以满足云环境数据服务的安全需求，篇幅所限，本文就理论方案的安全性及约束条件进行讨论，暂不考虑具体实现中的效率差异。但还有以下两点不足。

1) DO 和 DU 之间密钥通信量的问题。本文提出的方案中，为了防止合谋攻击，避免 CSP 将不属于 DU 访问权限的数据进行重加密操作发送到 DU 解密，所以在 DO 加密阶段，将数据分成按权限划分的最小数据单元进行不同密钥的第一次加密操作。若此时 DU 访问权限包括了 n 个最小数据单元，则在解密过程中需要收到对应的 n 个密钥的密钥组，这种方式无形中增加了 DO 和 DU 之间的密钥通信量。

实际上，在云环境下的数据服务重加密方案中，该问题核心矛盾在于选择密文的权限和重加密权限不能同时置于 CSP 端。如果采用协商密钥的方式规定 DU 的解密密钥，那么 DO 需要自身保管明文，在每次发送时自行选择 DU 访问权限的明文进

行一次重加密工作。这种方式完全没有利用到云代理大容量、高性能的特点，所有操作都由 DO 自身完成，可以直接忽略云代理的存在，将密文直接发给 DU 解密。因此，本文的方案虽然增加了密钥通信量，但能很好地利用云计算平台的特性，将存储和加密开销转移到云端。

2) 加密效率的问题。本文提出的方案虽然能保证云环境下的数据服务安全，但多采用基于公钥加密体制的密码算法。对于有良好处理能力的对称密码体制，公钥体制密码的加密计算开销大于对称密钥体制密码。根据上文的分析，采用对称密码又不能很好保护数据服务的安全性，如何解决安全保护和高效计算的矛盾需要进一步研究。

对于有高计算性能的云计算平台来讲，如果假设云平台的计算能力近似于无限，那么本方案在数据服务安全保护方面是具有优势的。若在计算能力有限的情况下，本方案局限于有高安全需求的云环境下的数据服务。

6　结束语

本文针对云环境数据服务半可信的云服务提供商，提出了可信重加密安全模型，对重加密模型进行了安全分析，并利用重加密安全模型找出适合重加密算法的约束条件，为构造云环境数据服务的适应不同安全程度的重加密算法提供理论基础，并针对 CSP 变化的可信状态进行了可信时效评估，使云环境数据服务更安全。基于可信重加密安全模型，按照文中的构建验证方法，不难得出目前基于公钥体制的 RSA 密码、椭圆双曲线密码的重加密方案，也满足可信模型的需要，用户可以根据不同的应用场景和需求去构建不同安全性级别、复杂度和效率的重加密算法。相对于已有的云环境数据服务安全方案，本模型有以下几个优势。

1) 将数据存储和加密计算开销都转移到云端，通过选择合适的重加密算法来抵抗合谋攻击，通过安全协议对数据进行验证，保证了云环境数据服务的安全。

2) 设计的会话密钥方式的重加密模型简单可行，通过改变第二层密钥便可改变密文版本和实现密钥权限的撤销。同时该模型对密码算法具有普适性，并通过安全模型给出重加密算法的选择约束，为选择合适的抗合谋攻击算法提供思路。

3) 对于数据请求者 DU，不增加解密操作和难度，仅需密钥和密文就能通过公开的密码算法实现一次解密，同时避免了多级解密带来的 DO 密钥泄露问题。

4) 将可信因素融入方案中，通过数据安全协议的数据验证过程，记录 CSP 恶意篡改行为，形成可信证据反馈，为验证可信前提提供参考依据。

参考文献：

[1] 冯登国, 张敏, 张妍等. 云计算安全研究[J]. 软件学报, 2011,22(1):71-83.
FENG D G, ZHANG M, ZHANG Y, *et al*. Study on cloud computing security[J]. Journal of Software, 2011, 22(1):71-83.

[2] GREEN M, ATENIESE G. Identity-based proxy re-encryption[A]. Applied Cryptography and Network Security[C]. Springer Berlin Heidelberg, 2007.

[3] HAN J G, SUSILO W, MU Y. Identity-based data storage in cloud computing[J]. Future Generation Computer Systems, 2013, 29(3): 673-681.

[4] WANG X A, YANG X Y. On the insecurity of an identity based proxy re-encryption scheme[J]. Fundamenta Informaticae, 2010, 98(2-3): 277-281.

[5] YANG Y J, ZHANG Y C. A generic scheme for secure data sharing in cloud[A]. IEEE Parallel Processing Workshops (ICPPW), 2011 40th International Conference[C]. 2011.

[6] ZHAO G S, RONG C, LI J, *et al*. Trusted data sharing over untrusted cloud storage providers[A]. 2010 IEEE Second International Conference on Cloud Computing Technology and Science (CloudCom)[C]. 2010.

[7] 王守信, 张莉, 李鹤松. 一种基于云模型的主观信任评价方法[J]. 软件学报, 2010,21(6):1341-1352.
WNAG S X, ZHANG L, LI H S. Evaluation approach of subjective trust based on cloud model[J]. Journal of Software, 2010,21(6): 1341-1352.

[8] 顾鑫, 徐正全, 刘进. 基于云理论的可信研究及展望[J]. 通信学报, 2011,30(7):176-181.
GU X, XU Z Q, LIU J. Review of cloud based trust model[J]. Journal of Communications, 2011,29(7):176-181.

[9] 孟祥怡, 张光卫, 刘常昱等. 基于云模型的主观信任管理模型研究[J]. 系统仿真学报, 2007,(14):3310-3317.
MENG X Y, ZHANG G W, LIU C Y, *et al*. Research on subjective trust management model based on cloud model[J]. Journal of System Simulation, 2007,(14):3310-3317.

[10] 胡春华, 罗新星, 王四春等. 云计算环境下基于信任推理的服务评价方法[J]. 通信学报, 2011,30(12):72-81.
HU C H, LU X X, WANG S C, *et al*. Approach of service evaluation based on trust reasoning for cloud computing[J]. Journal on Communications, 2011,30(12):72-81.

[11] 赵菁, 冯登国, 杨林等. 一个高效的选择密文安全的分类代理重加密方案[J]. 电子学报, 2011,(11):2513-2519.

（下转第 144 页）