

互联网细粒度云存储数据匿名可信访问控制方法

林锦添[†]

(中国电信国际公司,香港)

摘要:互联网细粒度云存储数据中的标签噪声,造成控制结果并发控制数较低,降低了匿名可信访问控制效果。因此,提出了互联网细粒度云存储数据匿名可信访问控制方法。分析互联网云存储数据在链路传输过程中的噪声变化规律,得出该噪声的偏差特性。基于分析结果划分数据的粒度,度量噪声特征去除噪声。为数据添加信息签名来匿名验证数据密文,由此分析形成的数字签名计算信用度,实现数据的匿名可信访问控制。实验结果表明:所提方法应用后得出的访问控制结果,表现出的并发控制数较高,控制效率较高,满足了互联网云存储数据的安全保密需求。

关键词:互联网数据;云存储数据;数据访问控制;匿名访问;可信访问;细粒度数据

中图分类号:TP309

文献标识码:A

An Anonymous and Trusted Access Control Method for Internet Fine Grained Cloud Storage Data

LIN Jintian[†]

(China Telecom Global Limited, Hong Kong, China)

Abstract: The label noise in fine-grained cloud storage data on the internet results in low concurrency control and reduces the effectiveness of anonymous trusted access control. Therefore, a method for anonymous and trustworthy access control of internet fine-grained cloud storage data is proposed. Analyze the noise variation pattern of internet cloud storage data during link transmission, and obtain the deviation characteristics of this noise. Based on the analysis results, divide the granularity of the data and measure the noise feature to remove noise. Add information signatures to the data to anonymously verify the ciphertext, and analyze the resulting digital signature to calculate credibility, achieving anonymous and trustworthy access control of the data. The experimental results show that the access control results obtained after the application of the proposed method exhibit a high number of concurrent controls and control efficiency, meeting the security and confidentiality requirements of internet cloud storage data.

Key words: internet data; cloud storage data; data access control; anonymous access; trusted access; fine grained data

在互联网的应用过程中,数据安全成为众多互联网用户的共同困扰。为了解决这一问题,对互联网数据进行基于某一属性的控制十分关键^[1]。基于数据安全与用户隐私保护的现实需求,验证访问互联网的用户身份数据成为领域内的重点研究方向^[2]。对此,很多研究人员提出了数据访问控制方

法。

文献[3]针对电子医疗系统中的数据访问控制方法进行研究。解析电子医疗系统数据从移动设备到云服务器端的上传路径,并基于该路径构建数据的安全共享模式。在该模式下分析数据属性的加密方法,并将该加密过程分为简易过程与复杂过

收稿日期:2024-02-23

作者简介:林锦添(1981—),男,福建福州人,本科,中级工程师,研究方向:云计算,云安全,数据隐私保护与合规。

[†]通信联系人,E-mail: linjintian1221@163.com

程。将后者的加密操作分配给系统云服务器端的边缘服务器。在该服务器中为数据添加对应的明文。引入零知识证明的方法为该数据明文连接相应的数据属性,通过对该属性的验证,实现数据访问控制过程。实验结果表明:该方法计算效率较低。文献[4]针对水利数据的访问控制方法进行研究。分析水利数据在存储服务器中的交互过程,并为其设置高级加密标准。将加密后的水利数据,以文件的形式上传至云端服务器中。利用数据链分析数据在服务器中的哈希值,并得出访问地址。制定数据在服务器中的安全服务策略,并为每种策略设置安全密钥,形成数据访问链。结合数据链与访问链,明确相应数据的所有权。查询水利数据在这一过程中的留痕状态,并将其作分隔处理,由此实现数据访问控制过程。实验结果表明:该方法普适性较差。文献[5]针对匿名共享的数据访问控制方法进行研究。基于数据在存储服务器中的公钥密码体制,分析数据在加密过程中的细粒度状态。以数据签名信息属性为基准,分析该数据的加密体制一致性程度。在区块链技术的支持下,构建不同等级的数据加密区块,并分发相应的密钥。设定安全访问的密钥等级阈值,从而动态扩展数据属性签名,并将其去中心化处理。由此解析数据的客体,并以此验证数据的来源,实现数据的访问控制过程。实验结果表明:该方法响应时间较长。

考虑到上述文献所提出的数据访问控制方法无法满足互联网领域中,细粒度的云存储数据的匿名访问可信度需求,本研究提出了一种互联网细粒度云存储数据匿名可信访问控制方法。该方法通过细粒度处理互联网云存储数据并去除数据标签中的噪声,在此基础上验证数据密文,由此计算信用度实现数据的匿名可信访问控制过程。

1 数据匿名可信访问控制方法设计

1.1 互联网细粒度云存储数据标签去噪

互联网的云存储数据的访问过程往往受到数据噪声的影响。基于这一干扰,本研究以细粒度的方式,将数据标签中的数据去除。

在数据访问的过程中^[6],数据在链路内传输,这使得数据标签的噪声处于动态变化的态势。分析数据在该过程中的变化规律,如图1所示。

如图1所示,互联网的云存储数据具备多个数据标签,由于数据标签在访问传输过程中的偏差特性,产生了标签噪声。基于这一规律,本研究对其进行细粒度标签去噪处理。

计算数据标签噪声的偏差概率向量值,如

式(1)所示^[7-8]。

$$p(x_i) = \frac{e^{h(x_i)}}{\sum_{x_i=1}^M e^c} \quad (1)$$

式中, $p(x_i)$ 表示相应数据的偏差概率向量值, x_i 表示互联网云存储数据, e 表示自然常数, $h(x_i)$ 表示数据的噪声值向量, M 表示数据的原始标签数量, c 表示交叉熵。

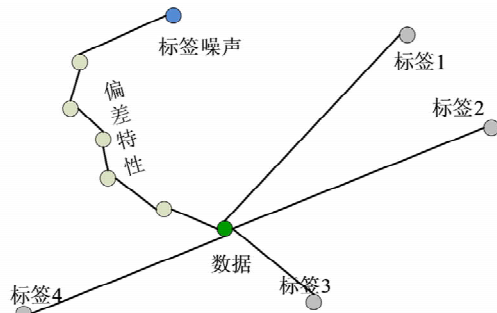


图1 数据噪声变化规律

基于式(1)的计算结果,将数据的噪声标签以细粒度划分,如式(2)所示。

$$T(x_i) = \sum_{c=1}^D p(x_i) \Theta \lg \frac{p(L)}{p(L)} \quad (2)$$

式中, $T(x_i)$ 表示数据噪声划分粒度, D 表示数据粒度细化值, Θ 表示隐变量, L 表示散度损失, $\tilde{y}$ 表示交叉熵在偏差变化过程中的损失值。

利用细粒度的数据噪声,度量互联网数据的噪声特征距离,以此筛选出需要去除的噪声部分。数据标签的噪声特征度量方法如式(3)所示^[9-11]。

$$W(x_i) = \frac{s \cos \theta}{\sum_{x_i=1}^M \|T(x_i)\| \|f(x_i)\|} \quad (3)$$

式中, $W(x_i)$ 表示互联网数据的标签噪声特征距离, $f(x_i)$ 表示数据的细粒度参数, s 表示超参数, θ 表示偏差特性夹角。

通过式(3)的计算,得到互联网云存储数据的噪声特征距值。基于这一结果,根据互联网数据访问管理的实际需求,为其设置早设定去除阈值。根据这一阈值筛选出数据标签噪声,完成去噪过程。

通过上述步骤,完成互联网细粒度云存储数据标签的去噪过程。

1.2 分层验证匿名数据密文

利用去噪后的数据,在数据层验证互联网云存储数据的密文。这一过程主要步骤为:

Step1:分匿名数据的初始密文。将互联网匿名访问数据作为主体,分析该数据认证消息与解密信息的关系,如式(4)所示。

$$S_{A \rightarrow B} = A \Big| \xrightarrow{x_w} B \quad (4)$$

式中, A 表示认证消息, B 表示解密信息,

$S_{A \rightarrow B}$ 表示两者的相关性关系, $\equiv$ 表示信任度, x_w 表示去噪后的互联网云存储数据。

Step2: 基于分析的数据认证关系, 为该数据添加信息签名^[12]。本研究根据非对称密钥的规则为数据添加信息签名, 如式(5)所示。

$$r = \frac{P \mid \xrightarrow{K} Q}{S_{A \rightarrow B} \sim X}$$

(5)

式中, r 表示添加的信息签名, P 和 Q 表示 A 和 B 之间的共享密文, K 表示公开密钥, $\sim$ 表示密钥的发送过程, X 表示密钥变量。

通过这一过程, 将数据与其密钥分离, 形成分层验证架构, 如图 2 所示。

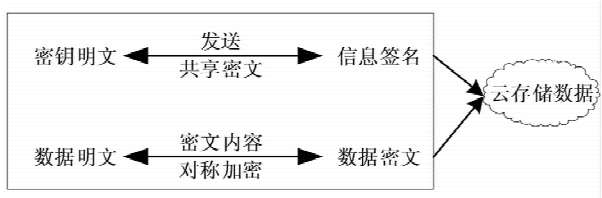


图 2 云存储数据分层验证架构

在如图 2 所示的架构中, 利用添加的信息签名, 验证互联网云存储数据的匿名密文。

Step3: 验证数据密文。本研究根据数据的信息签名接收规则对其进行验证。该接收规则表示为如式(6)所示的形式^[13]。

$$R = \frac{P \triangleleft (x_w, X)}{\kappa}$$

(6)

式中, R 表示信息签名接收规则, $\triangleleft$ 表示接收过程, κ 表示杂凑值。

基于这一接收规则, 验证匿名数据的身份信息。

通过上述步骤, 完成互联网云存储数据的匿名分层验证密文过程。

1.3 分析数字签名控制数据匿名可信访问

在互联网访问数据的匿名验证结果的基础上, 通过分析数据的数字签名, 计算数据的信用度, 基于该信用度的调控实现对互联网云存储数据的匿名可信访问控制过程。

分析通过信息签名验证后, 数据形成个体数字证书, 如图 3 所示^[14]。

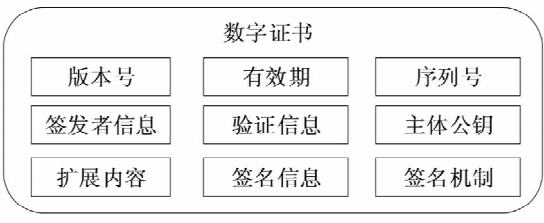


图 3 数据个体数字证书

如图 3 所示, 通过验证后的数据个体数字证书中包含签发者信息等验证内容。本研究基于该数字证书中的签名信息来分析计算该访问数据的信用度。

计算数据信用度, 如式(7)所示。

$$F(x_i) = \frac{q^r - q^{-r}}{q^r + q^{-r}}$$

(7)

式中, $F(x_i)$ 表示数据的访问信用度, q 表示数据的签名属性。

根据式(7)计算所得的数据信用度结果, 本研究引入判断矩阵分析每条访问数据的可信权重值。该判断矩阵中, 各数据访问信用度的比较规则如式(8)所示^[15]。

$$E_q = \begin{cases} 1, & q_{x_i} > q_{x_j} \\ 0.5, & q_{x_i} = q_{x_j} \\ 0, & q_{x_i} < q_{x_j} \end{cases}$$

(8)

式中, E_q 表示数据访问可信权重值, x_j 表示另一条互联网云存储的匿名访问数据, q_{x_i} 和 q_{x_j} 分别表示相应数据的签名属性。

在上述判断结果的基础上, 结合该数据的具体访问权限, 得出数据的匿名可信访问控制结果。该控制结果表示为式(9)的形式。

$$\omega = \frac{\sum_{x_i=1}^v E_q}{v(v-1)^\alpha}$$

(9)

式中, ω 表示数据访问控制结果, v 表示数据的同一 IP 请求数据量, α 表示数据请求访问端口。

在如式(9)所示的访问控制结果中, ω 仅包含两种计算结果, 负值表示该数据不允许访问, 正值则表示允许该数据访问请求的权限端口。

通过上述步骤, 完成互联网细粒度云存储数据匿名可信访问控制方法的设计。

2 实验与分析

2.1 实验准备

设计对比实验对本研究所提出的互联网细粒度云存储数据匿名可信访问控制方法的实践应用可行性进行测试, 通过实验结果, 对比分析该方法的应用有效性。

搭建本次数据访问控制实验的互联网云存储环境, 如图 4 所示。

如图 4 所示, 本次实验采用 Cinder 组件来搭建实验环境。该组件共包含五个模块, 如表 1 所示。

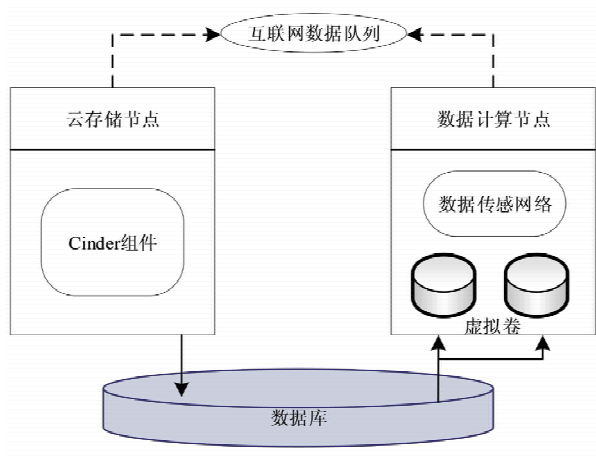


图 4 互联网云存储实验环境

表 1 Cinder 组件功能模块

模块	功能说明
cinder-scheduler	通过调度算法从多个存储节点服务器中,选择最合适的节点创建卷
cinder-api	外部接入入口、接收和响应外部请求
volume-provider	卷操作模块、驱动调用具体卷
cinder-volume	卷管理模块
volume-backup	备份服务器

基于如表 1 所示的功能,实现本次实验所需的基本参数调节功能。

将搭建的互联网云存储环境于实验测试硬件中运行。本次实验的硬件配置如表 2 所示。

表 2 实验硬件配置

序号	项目	参数
1	操作系统	Ubuntu 16.04
2	CPU	Intel(R) Core(TM) i7-7700
3	内存	8 GB
4	主频	3.60 GHz
5	运行框架	HyperLedger Fabric

本次实验全程于如表 2 所示的环境中开展。在上述环境中,模拟生成本次实验的互联网云存储数据,生成数据的格式如表 3 所示。

表 3 实验数据生成格式

数据属性	格式
访问数据 ID	ID_AMP
属性类型	a_ki
接收数据 ID	ID_DR
证明	Token_ID_DR
时间戳	T_AMP
有效期	T_e

基于上述过程,模拟生成若干个实验数据,并将上述模拟生成数据 ID 作匿名隐藏处理,测试在数据匿名访问情况下的访问控制效果,仅在结果分析阶段将其设置为可查询状态。

完成上述准备后,开展本次互联网细粒度云存储数据匿名可信访问控制实验。

2.2 互联网数据匿名访问可信控制

采用本研究所提出的互联网细粒度云存储数据匿名可信访问控制方法进行实验测试,根据实验结果分析本研究所提方法的实践应用可行性。

随机选用 10 条实验数据,测试每条实验数据的访问控制情况。经过实验,得到互联网数据匿名访问可信控制结果如表 4 所示。

表 4 互联网数据匿名访问可信控制

实验数据	上传权限访问	修改权限访问	删除权限访问	审核权限访问
49	√	×	×	×
105	√	√	√	√
138	×	√	×	√
462	√	√	√	×
677	√	×	√	√
943	√	√	×	√
1584	×	√	×	×
1996	√	×	√	×
2157	×	×	×	×
2834	×	√	√	√

如表 4 所示,在对上述 10 条实验数据的访问控制实验结果中,每条数据对于不同的权限有着不同的访问控制结果。将这一结果与该数据所具备的实际访问权限对比可知,本研究所提方法得出的数据访问控制结果与该数据拥有的实际访问权限完全一致,控制结果具备可信度,具备应用可行性。

2.3 结果评价指标

为了更加直观地体现出本次互联网细粒度云存储数据匿名可信访问控制方法实验结果的有效性,设置定量指标评价实验结果。基于互联网云存储数据的网络安全保护需求,将本次实验的定量评价指标设定为并发控制数,其计算方法如式(10)所示。

$$\bar{\lambda} = \left(\frac{N_t s_t p_t}{t_{\bar{\lambda}}} \right)^{\iota} + C_{\max}$$

(10)

式中, $\bar{\lambda}$ 表示并发控制数, N_t 表示导入的互联网云存储数据量, s_t 表示单条数据发生的访问请求数量, p_t 表示单条数据的访问请求时间, $t_{\bar{\lambda}}$ 表示实验时长, ι 表示调节因子, $C_{\max}$ 表示单条互联网数据的最大控制时间。

根据并发控制数指标的计算,分析同一时间内,所能够处理的数据访问请求控制的数据帧。计算所得的并发控制数结果数值越高,表明该方法在

互联网云存储数据的匿名可信访问控制实践中,表现出的访问请求控制处理能力越强,控制结果有着更高的可信度,具备更高的实践应用有效性。

2.4 结果分析与讨论

为了保证本次实验结果的有效性,采用对比分析的方法对本次实验结果进行评价。分别采用文献[3]、文献[4]以及文献[5]所提出的数据访问控制方法作为本次实验的对照组。基于设定的结果评价指标,分析并讨论不同控制方法的应用性能。

经过实验,得到不同方法下的互联网云存储数据的匿名可信访问控制结果如图 5 所示。

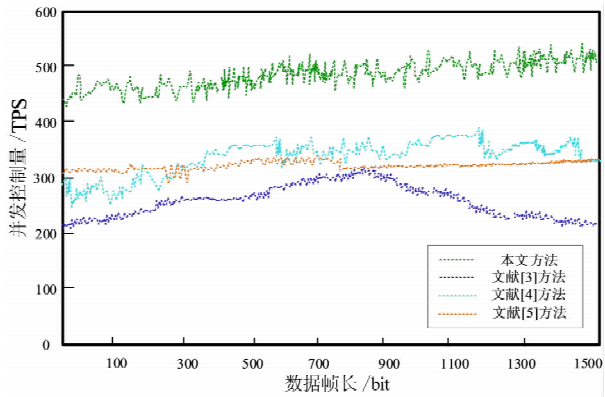


图 5 不同方法数据匿名访问控制结果

由图 5 可知,在不同的数据访问控制方法中,文献[4]和文献[5]所提方法的并发控制数据结果数值较为接近,在不同的数据帧长中,并发控制数的结果均值均在 300 TPS 左右,而文献[3]所提方法表现出的并发控制数与前两者有着较大的差距,在数据帧长为 900 bits 的区间内时,其并发控制数呈现稳步提升的态势,而当数据帧长大于 900 bits 后,其指标数值呈现较大幅度的下跌趋势,控制效果大大降低。而本研究所提方法在数据帧长的变化下,并发控制数的结果数值十分稳定,且比较高,稳步控制在 400~500 TPS 的范围内,较其他三种控制方法相比,控制效果有着十分明显地提升,展现出了更高的实践应用有效性。

从实验结果可知,本研究所提方法在互联网云存储数据的匿名访问控制实践中,表现出的并发控制数结果较为优秀,控制后得到的信息有着更高的可信度,具备较高的实践应用价值。

3 结 论

随着人们在互联网使用过程中信息安全意识的逐渐增强,为了防止未经授权的用户数据的匿名访问非法操作,对数据的匿名访问控制是一个关键。对此,提出了一种互联网细粒度云存储数据匿

名可信访问控制方法。经过实验可知,依据所提方法得出的数据访问控制结果,表现出了较高的并发控制数。该方法在互联网云存储数据管理工作中的应用,不仅能够通过细粒度操作将互联网数据的访问控制过程提升到更细致的控制水平,还能够通过更高的并发控制数,提高互联网云存储数据的访问控制效率,有效降低了数据匿名可信访问过程中的安全风险。基于这样的应用优势,该方法在互联网数据安全防范工作中,具备较高的推广应用价值。

参考文献

[1] 郭政,吴武清,刘源,等. 基于多任务支持向量机的能源互联网数据深度融合方法[J]. 计算机应用与软件, 2023, 40(3): 22—27.

[2] 杨杉,谭博,郭静波. 基于压缩感知的新一代能源互联网的数据采集方法[J]. 可再生能源, 2022, 40(7): 952—958.

[3] 张晓旭,石润华. EHR 系统中一种验证外包加密数据正确性的访问控制方案[J]. 信息安全, 2023, 23(5): 85—94.

[4] 刘秋明,许泽峒,姚哲鑫,等. 融合属性基加密和信用度的水利数据访问控制模型[J]. 科学技术与工程, 2023, 23(1): 263—273.

[5] 王静怡,刘百祥,方宁,等. 基于区块链与属性密码体制的匿名数据共享访问控制[J]. 计算机工程, 2023, 49(10): 41—52.

[6] 杜瑞忠,张添赫,石朋亮. 基于区块链且支持数据共享的密文策略隐藏访问控制方案[J]. 通信学报, 2022, 43(6): 168—178.

[7] 李俊,唐智灵. 复杂网络中链上数据安全访问控制仿真[J]. 计算机仿真, 2023, 40(4): 382—385, 513.

[8] 叶进,庞承杰,李晓欢,等. 基于区块链的供应链数据分级访问控制机制[J]. 电子科技大学学报, 2022, 51(3): 408—415.

[9] 蒋家昊,张璇,邓宏镜,等. 基于区块链的多部门数据共享访问控制流程建模[J]. 计算机集成制造系统, 2022, 28(10): 3202—3211.

[10] 张亚兵,王健,邢饒. 工业互联网中增强安全的云存储数据访问控制方案[J]. 计算机应用研究, 2021, 38(12): 3765—3770.

[11] 夏喆,罗宾,徐桂彬,等. 智能电网中支持细粒度访问控制的隐私保护数据聚合方案[J]. 信息安全, 2021, 21(11): 28—39.

[12] 张悦,田秀霞,颜赞成,等. 一种基于分级策略的电力营销大数据访问控制方案[J]. 华东师范大学学报(自然科学版), 2021(5): 169—184.

[13] 张晓均,王鑫,廖文才,等. 支持条件身份匿名的云存储医疗数据轻量级完整性验证方案[J]. 电子与信息学报, 2022, 44(12): 4348—4356.

[14] 孙二华,胡云冰. 5G 车载网络电力注入的大数据匿名批量验证[J]. 计算机应用与软件, 2021, 38(9): 328—332+349.

[15] 刘子杰,王凯,王亚刚,等. 工业互联网端边云协同数据同步方案设计与实现[J]. 计算机应用研究, 2022, 39(3): 821—825.