云存储用户数据完整性保护与破坏的博弈分析

陈　洁，侯吉成

（北京信息科技大学理学院，北京　100192）

摘要：运用进化博弈的方法分析云存储中关于用户数据完整性保护与破坏的问题，并根据得益矩阵建立云存储中关于用户数据完整性保护与破坏的进化博弈模型，利用复制动态方程分析云存储用户及云存储服务提供商之间的进化稳定策略。分析结果显示：降低云存储用户检测数据完整性的投资和加剧云服务提供商恶意破坏用户数据完整性的损失，可以有效地保护云存储用户数据的完整性。

关键词：运筹学；博弈论；云存储；数据完整性；复制动态；进化稳定策略

中图分类号：O225　　**文献标识码**：A　　**文章编号**：1674-2850(2016)01-0081-07

Game analysis of the integrity protection and destruction of users' data in the cloud storage

CHEN Jie, HOU Jicheng

(*School of Science, Beijing Information Science & Technology University, Beijing*　100192, *China*)

Abstract: We used evolutionary game theory to analyze the integrity protection and destruction of users' data in the cloud storage. According to the benefit matrix, we established an evolutionary game model about the integrity protection and destruction of users' data in the cloud storage. Then, we used the replicator dynamic equation to analyze the evolutionary stable strategy of the users and the cloud storage service providers. The results show that it is of value for the integrity of users' data in cloud storage to reduce investment of users to detect their data and increase loss of vandalism data integrity of cloud service providers.

Key words: operational research; game theory; cloud storage; data integrity; replicator dynamics; evolutionary stable strategy

0　引言

随着大数据时代的到来，人们的生活、学习和思维均受到大数据信息风暴的冲击，大数据开启了一次重大的时代转型。发掘数据价值、征服数据海洋的“动力”是云计算。云存储[1]作为云计算中的一种基础设施，为用户提供着以互联网为基础的在线存储服务。云存储用户根据各自所需，向云服务提供商租用池内资源，从而节省本地存储硬件设施及管理人员的成本支出，专业的云服务提供商还能够为用户提供高效的管理技术及灾难性数据恢复功能[2]，为人们对信息的存储需求提供着日益剧增的便利。

随着云存储技术的日益完善，越来越多的用户运用云存储空间存放数据信息。然而，当用户把数据外包到云中之后，在物理上就失去了对数据的直接控制，这样便出现了安全隐患。数据的安全性与完整

基金项目：国家自然科学基金（11271178）

作者简介：陈洁（1990—），女，硕士研究生，主要研究方向：博弈论

通信联系人：侯吉成，教授，主要研究方向：经济博弈论、非线性分析. E-mail: houjc163@163.com

性面临威胁，云存储服务提供商是否会恶意删除用户数据以汲取更大的利润成了用户所担忧的问题[3]。

为保证用户数据完整性，通过设计云存储服务器与用户之间完成通信或服务所需遵循的规则和约定来检测数据的完整性，从而在技术层面进行保护。然而，一些协议中的算法只注重了高效性，在安全性方面却存在漏洞，使得云存储服务器通过伪造假证蒙混过关，破坏了用户数据的完整性。HAMILTON 指出，将博弈论应用于信息安全是未来很有前途的一个发展方向[4]。考虑到云存储服务提供商为汲取更大的经济利益很可能通过删除云存储用户的数据信息来节约池内资源，云存储用户为保护自身数据完整性，可通过可信的第三方对数据完整性进行检测。显然，云存储服务提供商与云存储用户之间存在着博弈关系，根据思维的有限理性特点，云存储用户通常需要多次向云存储服务提供商购买池内资源，因此云服务提供商和云存储用户之间的博弈是反复往返的长期过程，博弈双方不断学习和调整自己的策略，以适应博弈中的变化并获得收益[5]。这里考虑运用进化博弈复制动态[6]的方法分析云存储用户数据完整性保护与破坏问题。

1　用户数据完整性保护与破坏博弈模型的建立及基本假设

云存储服务在运行过程中主要有云存储服务提供商和用户 2 个参与者。由云存储服务提供商和用户之间的策略依存性，可以利用得益矩阵建立数据完整性防护的进化博弈模型。

令 a 为云存储服务提供商的正常收益；b 为云存储服务提供商恶意删除用户数据的额外收益；c 为云存储服务商被发现其恶意删除数据所承担的赔偿；d 为用户数据完整情况下的收益；e 为用户检测数据付给第三方的费用；f 为用户数据不完整带来的直接损失；g_1 为云存储用户的信誉价值；g_2 为云存储服务器的信誉价值。建立数据完整性防护的策略型模型，如表 1 所示。

表 1　云存储服务提供商与用户的得益矩阵

Tab. 1　Benefit matrix of the users and the cloud storage service providers

用户	云存储服务提供商	
	删除数据	不删除数据
检测	$d+c-e,\ a+b-c-g_2$	$d-e,\ a$
不检测	$d-f-g_1,\ a+b-g_2$	$d-g_1,\ a$

2　云存储数据完整性保护与破坏的进化博弈分析

复制动态方程是进化博弈中最具应用价值的动态方程。云存储服务提供商和用户在数据完整性保护与破坏问题中表现出的理性程度较低，云存储用户的数据完整性保护与破坏问题中，策略学习和动态调整的速度不快，因而可采用描述生物进化的复制动态对云存储用户数据保护与破坏进行有限理性博弈分析。

2.1　进化博弈的复制动态

假设云存储用户采用检测数据完整性的概率为 x，则不检测数据完整性的概率为 $1-x$. 同时，假设云存储服务提供商恶意删除用户数据的概率为 y，则云存储服务提供商诚信保护用户数据的概率为 $1-y$，其中，$x,y\in[0,1]$.

云存储用户“检测”策略的期望得益为

$$u_{1e}=y(d+c-e)+(1-y)(d-e)=cy+d-e,$$

“不检测”策略的期望收益为

$$u_{1n}=y\cdot(d-f-g_1)+(1-y)(d-g_1)=-fy+d-g_1,$$

混合策略，“检测”与“不检测”策略的平均得益为

$$\overline{u}_1 = x\cdot u_{1e} + (1-x)u_{1n} = (c+f)xy + (g_1 - e)x - fy + d - g_1 .$$

云存储服务提供商“删除”策略的期望得益为

$$u_{2e} = x(a+b-c-g_2) + (1-x)(a+b-g_2) = -cx + a + b - g_2 ,$$

“不删除”策略的期望得益为

$$u_{2n} = x\cdot a + (1-x)a = a ,$$

混合策略，“删除”与“不删除”策略平均得益为

$$\overline{u}_2 = y\cdot u_{2e} + (1-y)u_{2n} = -cxy + (b-g_2)y + a .$$

分别将复制动态方程用于云存储用户和云存储服务提供商，得到云存储用户复制动态方程为

$$\frac{\mathrm{d}x}{\mathrm{d}t} = x(u_{1e} - \overline{u}_1) = x(1-x)\left[(c+f)y + g_1 - e\right],$$

云存储服务提供商的复制动态方程为

$$\frac{\mathrm{d}y}{\mathrm{d}t} = y(u_{2e} - \overline{u}_2) = y(1-y)(b - g_2 - cx) .$$

令 $\frac{\mathrm{d}x}{\mathrm{d}t}=0$, $\frac{\mathrm{d}y}{\mathrm{d}t}=0$, 得到云存储用户和云存储服务提供商间博弈的动态系统 5 个平衡点：$(0,0)$, $(0,1)$, $(1,1)$, $(1,0)$, $\left(\frac{b-g_2}{c}, \frac{e-g_1}{c+f}\right)$.

2.2 策略的进化稳定性分析

进化稳定策略是进化博弈论中具有真正稳定性和较强预测能力的均衡，它本身是一种均衡状态并且对微小扰动具有稳健性，即如果某些博弈方由于偶然的错误而产生偏离，复制动态仍然会使其恢复到进化稳定策略。因而，研究云存储用户数据完整性的保护与破坏问题的进化稳定策略具有较强的实际意义。

2.2.1 云存储用户策略进化稳定性分析

令 $F_1(x) = \frac{\mathrm{d}x}{\mathrm{d}t}$，根据微分方程的稳定性定理和进化稳定策略的性质，当 $F_1(x^*) < 0$ 时，x^* 为进化稳定策略。

若 $y = \frac{e-g_1}{c+f}$，则 $\frac{\mathrm{d}x}{\mathrm{d}t} = x(u_{1e} - \overline{u}_1) = x(1-x)\left[(c+f)y + g_1 - e\right] = 0$，那么所有的 x 都是稳定状态，如图 1 所示。

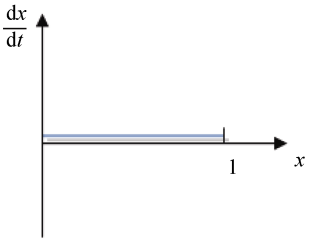

图 1 $y = \frac{e-g_1}{c+f}$ 时的相位图

Fig. 1 Phase diagram when $y = \frac{e-g_1}{c+f}$

因为 $c+f>0$ 恒成立，讨论当 $e-c<f+g_1$，即 $0<\frac{e-g_1}{c+f}<1$ 成立时，用户检测数据完整性的额外花销（即检测费用除去云存储服务所给的赔偿部分）低于用户由于数据不完整带来的损失（直接经济损失与间接声誉损失），若 $y>\frac{e-g_1}{c+f}$，则 $F_1'(1)<0$，因而 $x^*=1$ 为进化稳定策略，如图 2 所示。

博弈结果为：当云存储服务器选择删除用户数据策略的概率大于$\frac{e-g_1}{c+f}$时，有限理性的云存储用户最终会选择检测数据完整性。若$y<\frac{e-g_1}{c+f}$，$F_1'(0)<0$，因而$x^*=0$为进化稳定策略，如图3所示。博弈结果为：当云存储服务器选择删除用户数据策略的概率小于$\frac{e-g_1}{c+f}$时，有限理性的云存储用户最终会选择不检测数据完整性。

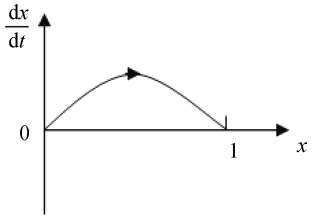

图2 $y>\frac{e-g_1}{c+f}$时的相位图

Fig. 2 Phase diagram when $y>\frac{e-g_1}{c+f}$

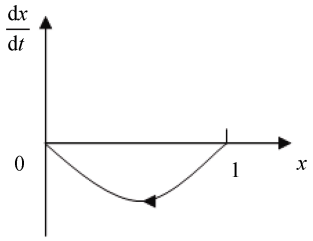

图3 $y<\frac{e-g_1}{c+f}$时的相位图

Fig. 3 Phase diagram when $y<\frac{e-g_1}{c+f}$

当$e-c>f+g_1$，即$\frac{e-g_1}{c+f}>1$成立时，用户检测数据完整性的花费与云存储服务所给的赔偿之差高于用户由于数据不完整带来的损失（直接经济损失与间接信誉损失），总有$F_1'(0)<0$，因而$x^*=0$为进化稳定策略，如图4所示。博弈结果为：当用户检测数据是否完整的费用很高而得到的赔偿较少时，无论云存储服务器是否删除用户数据，云存储用户都会选择不对数据的完整性进行检测。

当$e<g_1$，即$\frac{e-g_1}{c+f}<0$成立时，用户检测数据是否完整的费用损失小于用户因数据不完整带来的信誉损失，$F_1'(1)<0$恒成立，因而$x^*=1$为进化稳定策略，如图5所示。博弈结果为：用户检测数据的费用损失小于用户因数据不完整带来的信誉损失时，无论云存储服务器是否删除用户数据，云存储用户都会选择对数据的完整性进行检测。

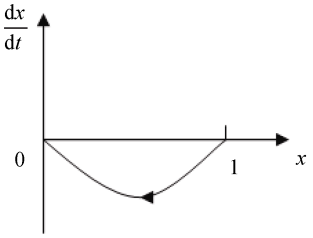

图4 $\frac{e-g_1}{c+f}>1$时的相位图

Fig. 4 Phase diagram when $\frac{e-g_1}{c+f}>1$

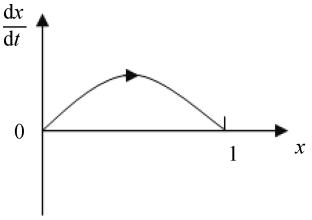

图5 $\frac{e-g_1}{c+f}<0$时的相位图

Fig. 5 Phase diagram when $\frac{e-g_1}{c+f}<0$

2.2.2 云存储服务提供商策略进化稳定性分析

令$F_2(y)=\frac{\mathrm{d}y}{\mathrm{d}t}$，根据微分方程稳定性定理和进化稳定策略的性质，当$F_2(y^*)<0$时，$y^*$为进化稳定策略。

若 $x=\frac{b-g_2}{c}$，则 $\frac{\mathrm{d}y}{\mathrm{d}t}=y\left(u_{2\mathrm{e}}-\bar{u}_2\right)=y(1-y)(b-g_2-cx)=0$，那么所有的 y 都是稳定状态，如图 6 所示。

当 $g_2<b<g_2+c$，即 $0<\frac{b-g_2}{c}<1$ 成立时，云存储服务器删除用户数据的额外收入低于删除用户数据的损失（信誉损失和赔偿费），若 $x<\frac{b-g_2}{c}$，$F_2'(1)<0$，因而 $y^*=1$ 为进化稳定策略，如图 7 所示。博弈结果为：当云存储用户选择检测数据完整性策略的概率小于 $\frac{b-g_2}{c}$ 时，有限理性的云存储服务提供商最终会选择删除用户数据的策略。若 $x>\frac{b-g_2}{c}$，$F_2'(0)<0$，因而 $y^*=0$ 为进化稳定策略，如图 8 所示。博弈结果为：当云存储用户选择检测数据策略的概率大于 $\frac{b-g_2}{c}$ 时，有限理性的云存储服务提供商最终会选择不删除用户数据。

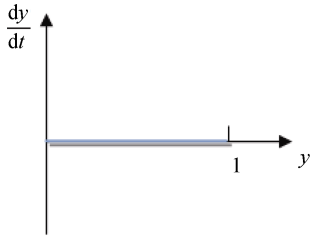

图 6 $x=\frac{b-g_2}{c}$ 时的相位图

Fig. 6 Phase diagram when $x=\frac{b-g_2}{c}$

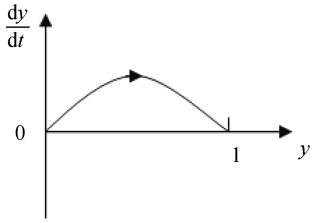

图 7 $x<\frac{b-g_2}{c}$ 时的相位图

Fig. 7 Phase diagram when $x<\frac{b-g_2}{c}$

当 $b>g_2+c$，即 $\frac{b-g_2}{c}>1$ 成立时，云存储服务器删除用户数据的额外收入高于删除用户数据的损失（信誉损失和赔偿费），此时总有 $F_2'(1)<0$，因而 $y^*=1$ 为进化稳定策略，如图 9 所示。博弈结果为：当云存储服务器删除用户数据所得到的额外收入高于删除用户数据的损失（信誉损失和赔偿费）时，无论云存储用户是否通过第三方来检测数据的完整性，云存储服务提供商都会选择删除用户数据。

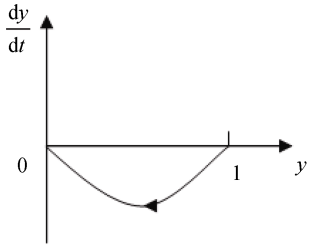

图 8 $x>\frac{b-g_2}{c}$ 时的相位图

Fig. 8 Phase diagram when $x>\frac{b-g_2}{c}$

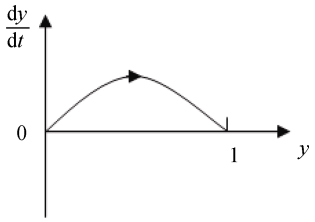

图 9 $\frac{b-g_2}{c}>1$ 时的相位图

Fig. 9 Phase diagram when $\frac{b-g_2}{c}>1$

当 $b<g_2$，即 $\frac{b-g_2}{c}<0$ 成立时，云存储服务器删除用户数据的额外收入低于删除用户数据的信誉损失，恒有 $F_2'(0)<0$ 成立，因而 $y^*=0$ 为进化稳定策略，如图 10 所示。博弈结果为：当云存储服务器删除用户数据的额外收入低于删除用户数据的信誉损失时，无论云存储用户是否通过第三方来检测数据的完

整性，云存储服务提供商都会选择不删除用户数据。

2.2.3　云存储用户与云存储服务提供商复制动态的关系分析

考虑，当$0<\frac{e-g_1}{c+f}<1,\ 0<\frac{b-g_2}{c}<1$时，即用户检测数据完整性的花销较少而得到的赔偿较大，云存储服务提供商删除用户的额外收益较少而付出的代价较大的情况下，这与社会现状十分相似，得到相位图如图11所示。

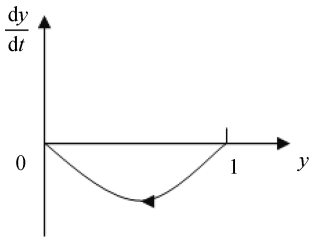

图10　$\frac{b-g_2}{c}<0$时的相位图

Fig. 10　Phase diagram when $\frac{b-g_2}{c}<0$

由图11可以看出，云存储服务提供商与云存储用户的决策处于不良的循环状态，这与现实社会的状况相吻合。这种情况对双方都是不利的，对云存储用户来说尤为不利。但在双方博弈的过程中，有利于提高云服务提供商对删除数据进行伪装的技术和提高可信第三方的检测技术水平。因此，云存储用户和云存储服务提供商两博弈方的复制动态关系给客观现实世界中的云存储用户数据完整性的安全问题提供了合理解释。

下面对其他状态下两博弈方的得益情况进行分析，为解决不良循环状态提供良好的办法。

当$\frac{e-g_1}{c+f}<0,\ \frac{b-g_2}{c}<0$时，即云存储用户检测数据完整性的花销比因数据不完整对公司形象带来的损失小，云服务提供商删除用户数据获得的额外收益低于服务信誉受损带来的损失时，进化稳定策略为$x^*=1$，$y^*=0$，得到相位图如图12所示。

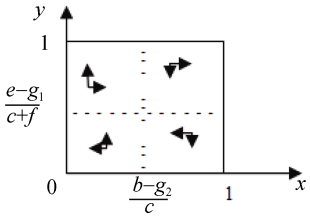

图11　$0<\frac{e-g_1}{c+f}<1,\ 0<\frac{b-g_2}{c}<1$时的相位图

Fig. 11　Phase diagram when $0<\frac{e-g_1}{c+f}<1,\ 0<\frac{b-g_2}{c}<1$

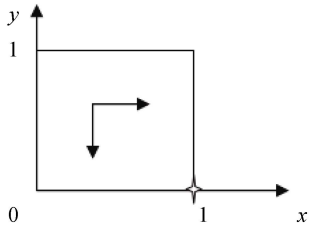

图12　$\frac{e-g_1}{c+f}<0,\ \frac{b-g_2}{c}<0$时的相位图

Fig. 12　Phase diagram when $\frac{e-g_1}{c+f}<0,\ \frac{b-g_2}{c}<0$

在这种情况下，云存储用户为保护数据完整性的花销低于数据不完整给公司带来的损失，使得所有用户都会通过可信第三方对数据完整性进行检测；而云服务提供商恶意删除用户信息带来的损失远远超出了删除用户数据所带来的额外收益，导致所有云服务提供商都不再恶意删除用户数据。因而，为保证云存储数据的完整性，降低云存储用户检测数据完整性的投入和加大云服务提供商的损失都是可行的方法。

当$\frac{e-g_1}{c+f}>0,\ \frac{b-g_2}{c}<0$时，即当云存储用户通过可信第三方检测数据完整性的花销大于因数据不完整对公司形象带来的损失，且云服务提供商恶意删除用户数据获得的额外收益低于服务信誉受损带来的损失时，进化稳定策略为$x^*=0$，$y^*=0$．当$0<\frac{e-g_1}{c+f}<1,\ \frac{b-g_2}{c}<0$时，如图13所示；当$\frac{e-g_1}{c+f}<1,\ \frac{b-g_2}{c}<0$时，如图14所示。

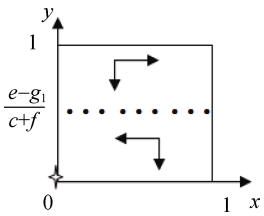

图 13 $0<\frac{e-g_1}{c+f}<1,\ \frac{b-g_2}{c}<0$ 时的相位图

Fig. 13 Phase diagram when $0<\frac{e-g_1}{c+f}<1,\ \frac{b-g_2}{c}<0$

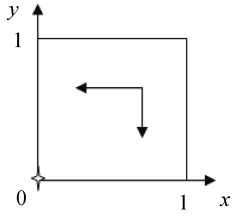

图 14 $\frac{e-g_1}{c+f}<1,\ \frac{b-g_2}{c}<0$ 时的相位图

Fig. 14 Phase diagram when $\frac{e-g_1}{c+f}<1,\ \frac{b-g_2}{c}<0$

此时，云存储用户检测数据完整性的投资超过了因数据不完整对公司形象带来的损失，使得所有用户都不通过可信第三方对数据完整性进行检测；而云服务提供商恶意删除用户信息带来的损失高出其通过恶意删除用户数据获得的额外收益，导致所有云服务提供商都不再恶意删除用户数据，双方都放弃主动行为，达到最佳理想状态。但这种状况会使得可信第三方检测数据完整性的投资无限增长，要保证数据的完整性，那么对于数据完整性的投资就要保证在一定的范围内，这种情况不符合实际。

3 结论

根据上述分析，给出了保护用户数据完整性问题的关键：降低云存储用户检测数据完整性的投资成本和加大云服务提供商恶意删除用户数据的损失。如果用户通过可信第三方检测数据完整性的投资成本足够小，那么所有的云存储用户都会选择对数据的完整性进行检测，云存储服务器考虑到损失的惨重也就不会采取恶意删除用户数据的策略来获取额外的利润。现给出几点具体解决措施：首先，为降低云存储用户检测数据完整性的投资成本，国家应在政策上提倡鼓励云存储技术的发展；在技术上，加大数据完整性检测技术投资，激励检测技术的高效进步以减少硬件设施的投资；在思想上，加强思想道德教育，提高第三方检测者的可信性。同时，为加大云服务提供商恶意删除用户数据的损失，相关部门应完善相应法律法规，加大管理力度，对不法分子侵害云存储用户权益的行为严惩不怠。

研究运用进化博弈方法，对云存储用户数据完整性保护与破坏问题进行了分析，为现如今大数据时代信息飞速发展带来的云存储服务的数据安全问题中数据完整性问题提供了可行的解决措施。

[参考文献] (References)

[1] HAMILTON S N, MILLER W L, OTT A, et al. The role of game theory in information warfare[C]//Proceedings of the 4th Information Survivability Workshop. Vancouver: IEEE Computer Society Press, 2002: 45-46.

[2] 孙薇，孔祥维，何德全，等. 基于演化博弈论的信息安全攻防问题研究[J]. 情报科学，2008，26（9）：1408-1412.
SUN W, KONG X W, HE D Q, et al. Research on attack and deference in information security based on evolutionary game[J]. Information Science, 2008, 26(9): 1408-1412. (in Chinese)

[3] 朱建明, RAGHUNATHAN S. 基于博弈论的信息安全技术评价模型[J]. 计算机学报，2009，32（4）：828-834.
ZHU J M, RAGHUNATHAN S. Evaluation model of information security technologies based on game theoretic[J]. Chinese Journal of Computers, 2009, 32(4): 828-834. (in Chinese)

[4] 安宝宇. 云存储中数据完整性保护关键技术研究[D]. 北京：北京邮电大学，2012.
AN B Y. Research on the key technologies of data integrity protection in cloud storage[D]. Beijing: Beijing University of Posts and Telecommunications, 2012. (in Chinese)

[5] 谢识予. 经济博弈论[M]. 3 版. 上海：复旦大学出版社，2012.
XIE S Y. Economic game theory[M]. 3th ed. Shanghai: Fudan University Press, 2012. (in Chinese)

[6] YANG K, JIA X H. Security for cloud storage systems[M]. Berlin: Springer, 2013.