面向 Hadoop 的风险访问控制模型

李甲帅[1,2]， 彭长根[*2,3]，朱义杰[1,2]，马海峰[1,2]

（1.贵州大学 计算机科学与技术学院，贵州 贵阳 550025；2.贵州大学 密码学与数据安全研究所，贵州 贵阳 550025；3.贵州大学 理学院，贵州 贵阳 550025）

摘 要：传统的访问控制机制难以约束授权用户的恶意行为，从而采用这种访问控制机制的 Hadoop 平台面临着大数据隐私泄露风险。提出一种基于风险的访问控制模型，该模型通过对主体和客体标签的设定，根据用户的历史行为记录构造信息熵风险值计算函数，并进一步建立风险值波动的追踪链，通过风险值及其波动幅度动态调整用户的访问权限。将该模型应用于 Hadoop 的 Kerberos 认证协议的改进，结合访问令牌及风险监测实现大数据隐私保护风险访问控制机制。最后，针对医疗大数据进行应用仿真，实验表明该模型可以有效约束大数据应用平台中授权用户的访问行为。

关键词：风险访问控制；Hadoop；隐私保护；信息熵；大数据

中文分类号：TP309 **文献标识码：**A

A Risk Access Control Model for Hadoop

LI Jia-shuai[1,2],PENG Chang-gen[2,3],ZHU Yi-jie[1,2],MA Hai-feng[1,2]

(1. College of Computer Science & Information, Guizhou University, Guiyang 550025,China;

2. Institute of Cryptography & Data Security, Guizhou University, Guiyang 550025,China;

3.College of Science, Guizhou University, Guiyang 550025,China)

Abstract: Traditional access control models are hard to restrain the malicious behavior of authorized users. Accordingly, Hadoop platform with this access control model is difficult to prevent the risk of privacy disclosure. In this paper, a model of access control based on risk is proposed. A risk function of information entropy is designed from users' historical behavior based on setting the tag of subject and object. Furthermore, we present the tracking chain of risk and adjust the users' access authority dynamically according to the risk value and its volatility. Combining with access token and risk supervision, the risk access control mechanism for big data privacy protection is designed, which is applied to enhance the security of Hadoop Kerberos protocol. Finally, the experiment result shows the model can constrain the authorized users' access behavior effectively.

Key words: Risk Access Control; Hadoop; Privacy Protection; Information Entropy; Big Data

收稿日期：2015-11-xx；**修回日期：**2015-xx-xx

基金项目：国家自然科学基金资助项目(61262073)；全国统计科学研究计划基金资助项目(2013LZ46)；贵州省统计科学研究课题项目(201511)

Foundation Items: The Nation Natural Science Foundation of China(61262073); The Nation Statistical Scientific Research Projects(2013LZ46);The Guizhou Province Statistical Science Research Project(201511)

*通讯作者：peng_stud@163.com

1 引言

大数据时代，数据的增长给我们带来的迫切的分析需求，而 Hadoop 平台其快速的处理大量数据给我们带来的非常大的便利,它可以通过分布式计算提供高性能的并行数据计算，并基于分布式文件系统 Hdfs 来实现海量数据的可靠存储。然而，Hadoop 基于 Kerberos 的访问控制机制并不能有效的保护用户的隐私数据，和原有的访问控制模型类似，其基于访问令牌的访问控制模型是通过对用户身份进行验证，当用户的身份认证通过时，持系统颁发的访问令牌就可以对 Hadoop 集群进行访问，而其在集群中的操作便不受监管。针对此，刘莎[1]等人提出基于信任的访问控制模型，通过对用户的行为记录结合信任值计算算法用于 Hadoop 访问模型来限制用户的访问行为，其只考虑到了用户的操作行为，并没有对隐私数据的保护提供一种有效的保护措施。

近年来，有学者提出了基于风险访问控制方法，即在在无法准确为用户指定其所可以访问的数据下又能保持数据流通程度最大。2007 年，IBM 研究中心的 Cheng 等[2]就模糊多层次的风险访问控制进行了理论研究；2010 年，美国普渡大学的 Ni 等[3]在 Cheng 等的工作上分析了模糊风险访问控制的最优模糊策略；2012 年，Kirkpatrick 等[4]针对访问控制过程中服务器作为访问评估的角色进行了研究；同年，Pashalidis 等[5]通过模糊策略的风险访问控制实现隐私和效用的平衡；2014 年，冯登国等[6]指出风险的访问控制可以用于大数据隐私保护，在此方面 Wang 等[7]做了有益探索，利用风险访问控制应用于医疗数据的隐私保护。本文在此基础上，建立一种面向 Hadoop 平台的风险访问控制模型，先对访问主体和客体进行访问标签的设定，通过历史行为记录的收集，并通过比较用户信息量和平均信息量之差来建立风险值计算函数；其次，建立追踪链来对风险值的波动幅度进行检测；最终实现基于风险的访问控制模型。

本文在结构基础上首先介绍了所要引入的风险访问控制模型；并基于现有的 Hadoop 访问控制模型的不足，将风险访问控制模型用于 Hadoop 大数据平台中来实行更加有效的隐私数据的保护；最后，结合医疗数据和授权医生诚实和恶意度的定义，通过风险值得比较表明改进后的模型可以有效约束授权医生对平台的访问行为。

2 风险访问控制模型

传统的访问控制模型都是基于关口的访问控制模型，对于授予权限的用户其后期行为并没有进行有效的监管，从而导致系统中隐私数据的泄露。

在本访问控制模型中，基于历史访问行为记录，引进信息熵的方法计算用户访问系统得到的信息量，以及系统中所有用户因为相同目的访问得到的平均信息量，进而计算风险值，并对风险值进行存储，通过追踪链对风险值变化波动幅度进行周期性的跟踪。以下是本文的风险访问控制模型生成的详细步骤：

1) 对访问主体和客体进行标签的设定；

2) 基于信息熵计算风险值；

3) 风险值追踪链的建立。

2.1 访问主体和客体设定标签

对于用户的每一次访问，都会对访问主体即用户设定一定的标签，在医疗系统中，可以对医生的访问目的等信息来作为其访问的标签；对于访问客体也要设定标签，如对病人的敏感数据，就可以通过国际疾病分类 ICD-10 来设定标签。

2.2 风险值计算

系统中会定期的对用户的访问行为记录进行分析，并计算风险值。在对用户 u_i 的访问行为进行分析时，将每一个用户相同的访问目标签下的数据进行整合，记为 $S(u_i, g_j)$，其中 g_j 为用户的访问目的，并且 $g_j \in G_i$，G_i 表示用户 u_i 的一段周期内的一系列访问目的。在系统的数据中，根据访问客体的标签进行设定，用 l_k 表示其中某一类数据的标签，$l_k \in L$，L 表示系统中所有的数据标签的分类，用 $f_{u_i}(g_j, l_k)$ 表示访问目的为 g_j 且数据标签为 l_k 的数据出现的次数，通过该次数我们就可以算出用户因为该目的 g_j 访问数据标签 l_k 的概率 $p_{u_i}(l_k \mid g_j)$，其中 $p_{u_i}(l_k \mid g_j) = f_{u_i}(g_j, l_k) / \sum_{l_b \in L} f_{u_i}(g_j, l_b)$，$l_b$ 表示在该访问目的下所有的数据标签，基于信息熵的计算公式，就可以得出用户 u_i 在访问目的 h_i 下得到的信息量

$$H_{u_i}(g_j) = -\sum_{k=1}^{|L|} p_{u_i}(l_k \mid g_j) \ln p_{u_i}(l_k \mid g_j) \tag{1}$$

同样，我们也可以在系统的历史数据行为记录中，得到相同的访问目的 g_i 的所有用户 u_{all} 的访问记录，并得到 u_{all} 的平均信息量 $\overline{H}(g_j) = H_{all}(g_j) / C(u_{all})$，$H_{all}(g_j)$ 表示 u_{all} 的信息量总和，$C(u_{all})$ 表示系统中这些用户的数量，通过比较用户 u_i 和 u_{all} 的信息量，就可以得到在相同访问目的 h_i 之下的差值，即风险值

$$risk(u_i, g_j) = \max(H_{u_i}(g_j) - \overline{H}(g_j), 0)$$

在系统中周期性的对用户的所有的访问目的进行求和，就可以得到用户的风险值为

$$risk_{u_i} = \sum_{g_b \in G_i} risk(u_i, g_b)$$

从中可以看出，在相同的访问目的之下，当用户得到的信息量相比系统中所有的用户得到的信息量偏大时，则用户的风险值也会随之增加，因而通过这种方式，系统就可以对已经授权访问数据用户的访问行为通过风险值进行约束，当其风险值大于系统设定的阀值时，系统就会限制其访问，从而可以防止一些恶意访问等带来的隐私数据的泄露。

最后，设定系统中会周期性根据每一个用户的身份信息等设定一定的风险阀值 Φ_{u_i}，并且风险阀值会在用户访问时由于用户的风险值的增加而减小，其 $\Phi_{u_i} = \Phi_{u_i} - risk_{u_i}$，从而得到风险访问控制的判断函数 $AccessCheck(u_i)$ 如下所示

$$AccessCheck(u_i)=\begin{cases}1 & if\ \Phi_{u_i}\geq 0\\ 0 & if\ \Phi_{u_i}<0\end{cases}$$

2.3 风险值追踪链

在本文中，考虑到风险是根据用户的历史访问行为记录进行计算的，因而在风险值的产生和访问过程中有可能存在一定的窗口期，在此期间，用户有可能会一次性的将分配给他的风险阀值用完，继而产生一定程度的隐私泄露，为了将此隐私泄露的程度降到可控的范围之内，通过对风险值的波动程度进行追踪，并最后设定系统的波动可以容忍的波动阀值，如果用户的波动范围超过该阀值，则系统禁止其访问。

首先，建立一个追踪链 S 用来存储系统中所有访问用户的风险值，$s_{u_i}\in S$ 表示用户 u_i 一段时间内的风险值，且 $s_{u_i}=\{r_{t_1},r_{t_2},\cdots,r_{t_n}\}$，其中 r_{t_n} 表示用户在 t_n 时间的风险值波动幅度，且其值为 $r_{t_n}=(\Phi_{u_i}-risk_{u_i})_{t_n}$，用 $\mathrm{w}_{\mathrm{u_i}}$ 表示用户这段时间的波动幅度，则

$$w_{u_i}=(\sum_{i=1}^{n}r_{t_i})/n$$

其次，规定系统可以容忍的波动幅度为 θ，得到用户和系统容忍度的一个判断函数

$$RiskCheck(u_i)=\begin{cases}1 & if\ w_{u_i}\leq\theta\\ 0 & if\ w_{u_i}>\theta\end{cases}$$

通过比较用户 u_i 的一段时间内的风险值和波动幅度 $\mathrm{w}_{\mathrm{u_i}}$ 和 θ，当 $\mathrm{w}_{\mathrm{u_i}}$ 大于 θ 时，则超过了系统允许的波动范围，即而比较函数中返回的值是 0，从而有效的限制用户访问系统中的敏感数据。

2.4 风险访问控制模型

结合风险值的计算以及风险值的波动范围来对系统中的敏感数据进行保护，当用户的风险阀值 Φ_{u_i} 小于 0 时，则系统会禁止其访问系统中的数据，其次，由于风险值的计算中系统中会存在一定的窗口期，因而会定时的跟踪风险值的波动幅度，当其超过系统规定的幅度时，系统同样也会禁止其访问，从中可以看出，当用户访问系统时，

$$access=(AccessCheck(u_i)+RiskCheck(u_i))$$

当 $access=2$ 时，系统才会允许其访问系统中的数据，当 $access<2$ 时，可以判断出用户可能是风险阀值小于 0 或者其风险值的波动范围超过了系统容忍范围之内从而导致其小于 2，因而对于这些授权用户的访问行为要进行约束。具体的风险访问控制模型如下图 1 所示：

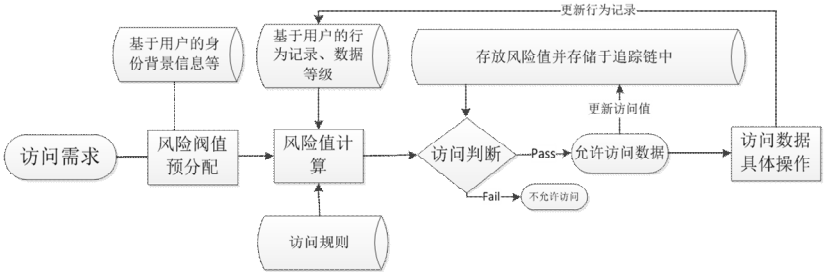


图 1 风险访问控制模型

3 基于风险访问控制模型用于 Hadoop 平台

当前基于 Kerberos 认证协议的 Hadoop 访问控制模型是一种关口式的访问控制，根据用户的身份，系统中会颁发票据，用户持有此票据便可以访问 Hadoop 集群中，并对集群中的数据进行分布式读取和计算，而对于用户在集群中的操作行为并没有进行监控，这样就会导致授权的用户在集群中的操作不受约束，本文基于此，将风险的访问控制模型结合 Kerberos 协议用于 Hadoop 的访问控制模型中，来实现对已经授权用户的访问行为进行约束，进而达到平台中隐私数据的进一步的保护。

3.1 基于 Kerberos 认证协议的 Hadoop 访问控制模型

Hadoop1.0.0 版本之后，才在其中加入了基于 Kerberos 认证的访问控制，在集群运行时，集群内的节点使用密钥进行认证，只有通过认证之后才能正常的访问节点，这种认证确保了 Hadoop 集群的可靠安全。

Kerberos 机制解决了客户端到服务器和服务器到服务器端的认证，在其 KDC 上会产生客户算、主节点和子节点之间相互通信的密钥 Keytab，通过这些 Keytab，节点之间就可以进行互相的认证，并提供相应的服务，防止了被冒充的可能性。其具体的访问控制分为两级，其中 ServicelLevel Authorization（访问令牌）为系统级，用于控制用户是否可以访问集群，另一级包括 Acess Control on Job Queues 和 DFSPermmision，分别用于控制 Hadoop 平台中的 mapreduce 计算和文件的读取权限。在 Hadoop 平台中，包括 master 节点和 slave 节点，master 节点根据用户的访问令牌完成身份的验证工作；slave 节点分为 Datanode 和 Jobtarcker 节点，分别完成分布式计算和分布式读取数据的验证，在 Datanode，用户持有 Block access token 访问令牌来对数据进行数据的读取等操作，如果 DFSPermmision 验证通过，则可以进行数据的读取操作，在 Jobtarcker 节点，用户持有 Job token 进行数据的计算等操作，如果 Access Control on Job Queues 验证通过，则允许用户的计算任务放入到计算序列中，等待 Mapreduce 的计算，图 2 是具体的访问控制流程。

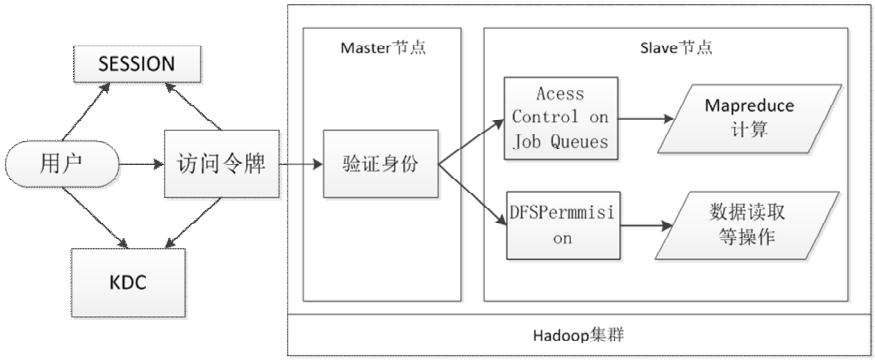


图 2 基于 Kerberos 的 Hadoop 访问控制模型

3.2 Hadoop 平台加入风险的访问控制新模型

基于原有的 Hadoop 访问控制模型，结合本论文讲述的风险访问控制模型用于其中，当用户访问集群时，持访问令牌访问集群，Master 节点不再仅仅充当验证身份的作用，其还可以通过信任值数据库计算用户的风险值，并结合追踪链中的风险值的波动幅度，来判断用户是否可以访问系统中的数据，由于对风险值的计算是根据用户的历史访问行为，因而可以充

分利用 Hadoop 的心跳机制来实现对用户操作行为的收集。其中关于标签的设定以及相关的算法定义如下：

定义 **1** s_{u_i} 为用户 u_i 在每一次访问过程中访问主体标签的设定，$s_{u_i}=\{clientID,role\}$，其中 *clientID* 表示该标签属于哪个用户，*role* 表示用户的所属的角色，即主体标签的设定，*time_start* 表示使用该标签的开始时间，本文在访问主体的标签设定中，就根据用户所属的角色来定。

定义 **2** O_i 为系统中对数据标签的设定，$O_i=\{tag_{num},main_{tag},sub_{tag}\}$，其中 tag_{num} 表示该数据标签的具体数值，$main_{tag}$ 表示该标签的数据是属于哪个主类，sub_{tag} 表示该标签的数据是属于哪个子类，这里主类和子类的定义主要是为了下一步的实验而做的准备。

定义 **3** $behavior_{u_i}$ 为 u_i 用户的访问行为记录，$behavior_{u_i}=\{s_{u_i},o_i,time\_start,time\_finish\}$，其中 s_{u_i} 和 o_i 分别表示了此次访问行为过程中的主体和客体的标签的设定，*time_start* 表示访问的开始时间，*time_finish* 表示访问的结束时间。

算法一 用户的访问行为记录收集算法 behaviorcollecting

输入： s_{u_i} ， o_i

输出：TRUE 或 FALSE

```
For Hadoop 集群运行 to Hadoop 集群终止 DO
  If(clientID==NULL)
    return FALSE ;即此时没有用户访问集群
  Else
    {
      behavior_ui =SetBehavior(s,u)；//根据用户和数据的标签结合系统的时间等信息生成用户的访问行为记录
      SendBehavior(behavior_ui)；//将此访问行为记录通过 Hadoop 特有的心跳机制传送到 master 节点，实现用户历史行为记录的收集
      WirteBehavior(behavior_ui)；//master 节点写入到信任值数据库
    return TRUE
    }
  ENDIF
  ENDFOR
```

该算法首先会判断有没有用户访问集群，有用户访问集群，根据访问目的和访问数据的标签，结合系统中时间，会在 Hadoop 集群中的相关的 slave 节点生成一条访问记录，继而通过心跳机制，可以将这些访问记录周期性的传送到 master 节点，master 节点在收集到这些信息后，会将其写入到信任值数据库。

定义 **4** 风险值的定义为 $risk=\{clientID,number,time\}$，其中 *clientID* 为用户的标识，*number* 为用户的风险值，*time* 为风险值产生的时间。

定义 **5** 风险险阀值的定义为，$threshold=\{clientID,value\}$，其中 *clientID* 为用户的表示，

value 为用户的风险阀值，初始值可以根据用户的身份信息进行分配。

定义 **6**　追踪链的定义为 $s=\{clientID, risk_t, threshold_t, time\}$，其中 *clientID* 为用户的表示，$risk_t$ 表示时间 t 时刻用户的风险值，$threshold_t$ 表示时间 t 时刻用户的风险阀值，*time* 表示 t 时刻的时间。

算法二　风险访问判断算法 $risk_{computing}$

输入：clientID

输出：TRUE 或 FLASE

```
For hadoop 集群运行 to hadoop 集群终止 DO
 If(clientID==NULL)
  return FALSE ;//即此时没有用户访问集群，所以也没必要计算风险值
  Else
 If(traverseBehavior(clientID)==NULL)//用户是第一次访问集群
  InitialiseRisk(clientID，threshold) //初始化风险阀值
  risk=RiskBehavior(client)//计算出用户的风险值
  threshold=threshold-risk；
  s=WirteRisk(risk,threshold)//将风险值和阀值写入到追踪链 s 中
If(AccessCheck(risk)+RiskCheck(clientID)==2)
Then return TRUE
Else FALSE
ENDIF
ENDFOR
```

该算法首先是从信任值数据库中遍历用户的访问行为，如果是第一次访问集群，则对用户的风险阀值进行初始化，如果不是，则计算用户的风险值，更新风险阀值，并将此次访问中的风险阀值和风险值存储到追踪链 s 中，最后，通过 *AccessCheck(risk)* 和 *RiskCheck(clientID)* 两个判断函数分别对用户的风险值和其波动幅度进行检验，如果验证通过，则用户可以继续访问集群。下图 3 是风险访问控制模型用于 Hadoop 现有的访问控制机制中。

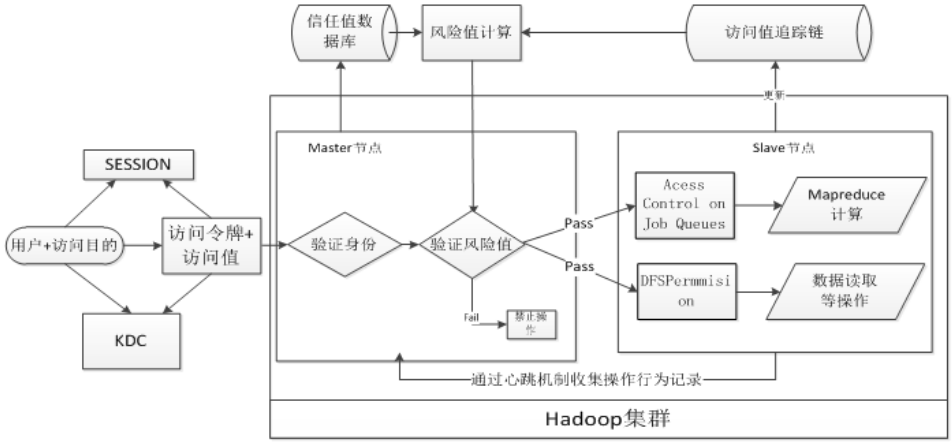


图 3　加入风险之后的 Hadoop 访问控制模型

4 仿真实验

4.1 实验设置

在我们的实验中，以医疗数据用于 Hadoop 平台中，来实现对医疗数据的隐私保护，这里我们的数据来源于真实的医疗数据，包括对 1500 病人的访问事件，在本实验中，对于医生，会分为诚实者和恶意者，对 Hadoop 平台中，信任值数据库中储存的是每一个医生的访问记录，对于每一个访问记录，包括用户的信息，以及访问主体标签(通过医生所在的科室)和数据标签，对于每一个访问主体标签的产生，都会对应一系列的数据标签，病人的数据标签可以通过 ICD-10 疾病编码进行设定，在这里设定医生u_i表示因为某一个访问目的访问数据的疾病编码d_i，另外用D_i^1和D_i^2来表示d_i在疾病代码中属于的主类和子类，因而$c_i \in D_i^2 \in D_i^1$，并且$D_i^1 \in D$，D表示所有的疾病代码集合，其下表 1 所示。

表 1　　疾病代码及医生科室关系表

科室	ICD10 主类编码	ICD10 子类编码	ICD10 疾病编码	ICD10 名称	拼音助剂码
神经科	G	70	1	重症肌无力	ZZJWL
神经科	G	70	101	中毒性肌神经疾患	ZDXJSJJH
神经科	G	70	201	先天性肌弛缓	XTXJCH
神经科	G	71	1	肌营养不良	JYYBL
眼科	H	02	506	眼睑闭锁	YJBS
眼科	H	02	601	眼睑黄斑瘤	YJHBL
眼科	H	04	505	泪道阻塞	LDZS
眼科	H	04	506	泪小管阻塞	LXGZS
眼科	H	04	601	泪囊瘘	LNL

在分布式存储系统 Hdfs 中，对于数据标签d_i其和D_i^2的关联度应该大于和D_i^1 - D_i^2的关联度，在本文中，通过机器学习得知，一个诚实医生，根据医生所属于的科室，其应该有68%的概率访问数据的标签应该属于D_i^2，并且有 95%的概率其数据标签是属于D_i^1；另外，系统中允许每一个医生以 5%的概率来访问系统中不属于该主类的数据，即系统容忍的无意间泄露的概率是 5%。

最后，我们根据医生的访问记录通过风险访问控制模型来对风险值进行计算，每一个用户的风险值即根据用户所属的科室(访问目的)和 ICD10(数据标签)之间的关系结合信息量来进行确定。

4.2 实验结果

在试验中，我们设置了 500 个医生，对于 500 个医生，其都可以授权访问集群，即每一个医生都持有合法的访问令牌访问集群，并设定其中的 10%的医生为恶意医生，这些恶意医生的定义以超过 5%的概率来访问系统中不属于自己主类的数据，通过对平台中的信任值数据库进行风险值的计算，我们可以得出其中诚实医生和恶意医生的平均风险值表如下表 2 所示：

表 2　　诚实与恶意医生的平均风险值

医生比例	5%	10%	15%	20%
诚实医生平均风险值	0.23	0.19	0.17	0.13
恶意医生平均风险值	1.04	1.08	1.14	1.61

从图中可以看出，诚实医生比恶意医生的风险值明显要低 6~8 倍，即在系统允许所有医生访问集群的情况下，通过风险值得计算，可以发现恶意医生平均的风险值明显大于诚实的医生，即将风险的访问控制用于 Hadoop 大数据平台，可以有效的降低授权用户进行不合法的操作。

5　结束语

本文提出了一种基于风险的访问控制模型，并将其用于现有的 Hadoop 平台的访问控制框架中，其优点在于：

1) 通过设置访问控制中主体和客体的标签，并基于用于的历史行为操作记录为基础，利用信息熵的计算方法，来计算出用户的风险值，使得该访问控制模型不再是一个“关口模式”，而是一种动态、更加细粒度的模型。

2) 在用户允许访问的同时，系统会通过风险值追踪链来实时记录风险值的变化幅度，使得用户在访问系统和风险值计算的窗口期期间，有效的降低系统中数据隐私泄露。

3) 基于 Hadoop 原有的访问控制模型，以及 master 节点通过心跳机制实时收集每一个 slave 节点的信息，可以有效的收集用户的操作记录，实现了将基于风险的访问控制模型用于 Hadoop 大数据平台中，在 master 节点验证完身份之后，基于风险值的计算及风险值幅度的变化，验证用户的访问风险，从而在合法的用户可以进入到 Hadoop 集群的前提下，能对授权用户的访问行为进行进一步的约束，继而可以保护平台中的隐私数据。

本文由于实验数据所限，因而对实验误差会有一定的影响；另外，在风险访问控制模型的基础上，如何对风险阀值和风险值波动容忍度进行合理的设定是下一步研究重点。

参考文献：

[1] 刘莎, 谭良. Hadoop 云平台中基于信任的访问控制模型[J]. 计算机科学, 2014, 41(5): 155-163.

[2] Cheng P C, Rohatgi P, Keser C, et al. Fuzzy multi-level security: An experiment on quantified risk-adaptive access control[C]. Security and Privacy, 2007. SP'07. IEEE Symposium on. IEEE, 2007: 222-230.

[3] Ni Q, Bertino E, Lobo J. Risk-based access control systems built on fuzzy inferences[C]. Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security. ACM, 2010: 250-260.

[4] Kirkpatrick M S, Ghinita G, Bertino E. Privacy-preserving enforcement of spatially aware RBAC[J]. Dependable and Secure Computing, IEEE Transactions on, 2012, 9(5): 627-640.

[5] Pashalidis A, Preneel B. Evaluating tag-based preference obfuscation systems[J]. Knowledge and Data Engineering, IEEE Transactions on, 2012, 24(9): 1613-1623.

[6] 冯登国, 张敏, 李昊. 大数据安全与隐私保护[J]. 计算机学报, 2014, 37(1): 246-258.

[7] Wang Q, Jin H. Quantified risk-adaptive access control for patient privacy protection in health information systems[C]. Proceedings of the 6th ACM Symposium on Information,

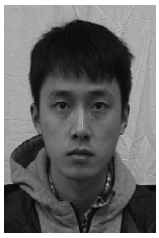
Computer and Communications Security. ACM, 2011: 406-410.
[8] 李凤华, 苏锦, 史国振, 等. 访问控制模型研究进展及发展趋势[J]. 电子学报, 2012, 40(4): 805-813.
[9] 刘逸敏, 周浩峰, 王智慧, 等. Purpose 融合: 基于风险 purpose 的隐私查询访问控制[J]. 计算机学报, 2010 (8): 1339-1348.

作者简介：

李甲帅（1989-），男，山西运城人，硕士，贵州大学，主要研究方向为密码学与可信计算

彭长根[通信作者]，(1963-)，男，侗族，贵州锦屏人，博士，贵州大学教授、博士生导师，主要研究方向为密码学、信息安全。
E-mail:peng_stud@163.com

朱义杰（1989-），男，山东临沂人，硕士，贵州大学，主要研究方向为密码学与可信计算



马海峰（1990-），男，四川乐山人，硕士，贵州大学，主要研究方向为密码学与可信计算