基于区块链的属性分级访问控制方案

福州大学至诚学院
林庆新

2023.11.28

目录

网络安全是基础

没有网络安全
就没有国家安全

我国在IPv6规模部署取得明显成效，显著提升了我国互联网的承载能力和服务水平，有效支撑4G/5G、云计算、大数据、人工智能等新兴领域快速发展。

“十四五”时期是加快数字化发展、建设网络强国和数字中国的重要战略机遇期，我国IPv6发展处于攻坚克难、跨越拐点的关键阶段。

IPv6为建设网络强国、数字中国和智慧社会提供坚实支撑。

对IPv6规模部署的认识

- 对IPv6的认识要从海量地址能力提升到安全能力

  IPv6固定分配地址可实现地址与用户身份的绑定，源地址溯源有利于安全保障

- IPv6是增强互联网可靠性、可用性及业务多样性

  IPv6有可扩展的报头，提供很大的可编程空间

- IPv6是信息技术新时代的重要标志，将与新一代信息技术无缝融合互为支撑

  IPv6丰富的地址简化了网络协议，SRv6可以成为云网边端协同的统一承载协议

- IPv6是新一代互联网创新平台，是网络强国建设的战略支点

  我国在IPv6使用较早，率先在IETF标准化组织倡议并积极开发“IPv6+”新功能

福州大学至诚学院学校主页（域名：www.fdzcxy.edu.cn)和所有二级单位网站、OA系统、学工系统、人事系统等所有二级信息化应用系统全部完成IPv6升级，IPv6规模化部署。

目录

数据访问控制方法

RBAC

基于角色的访问控制（RBAC）：对系统操作的各种权限不是直接授予具体的用户，而是在用户集合与权限集合之间建立一个角色集合。

DAC

自主访问控制（DAC）：由客体的属主对自己的客体进行管理，由属主自己决定是否将自己的客体访问权或部分访问权授予其他主体，这种控制方式是自主的。

ABAC

基于属性的访问控制（ABAC）：ABAC是一种逻辑访问控制方法，在这种方法中，对执行操作的授权是通过评估与主体、客体、申请操作相关联的属性来确定的。

存在问题与解决方案

- 传统的访问控制方式 存在问题：

  权限管理效率不高、访问控制中心化、灵活性差、难溯源等。

- 解决方案：一种区块链上属性分级的访问控制机制：

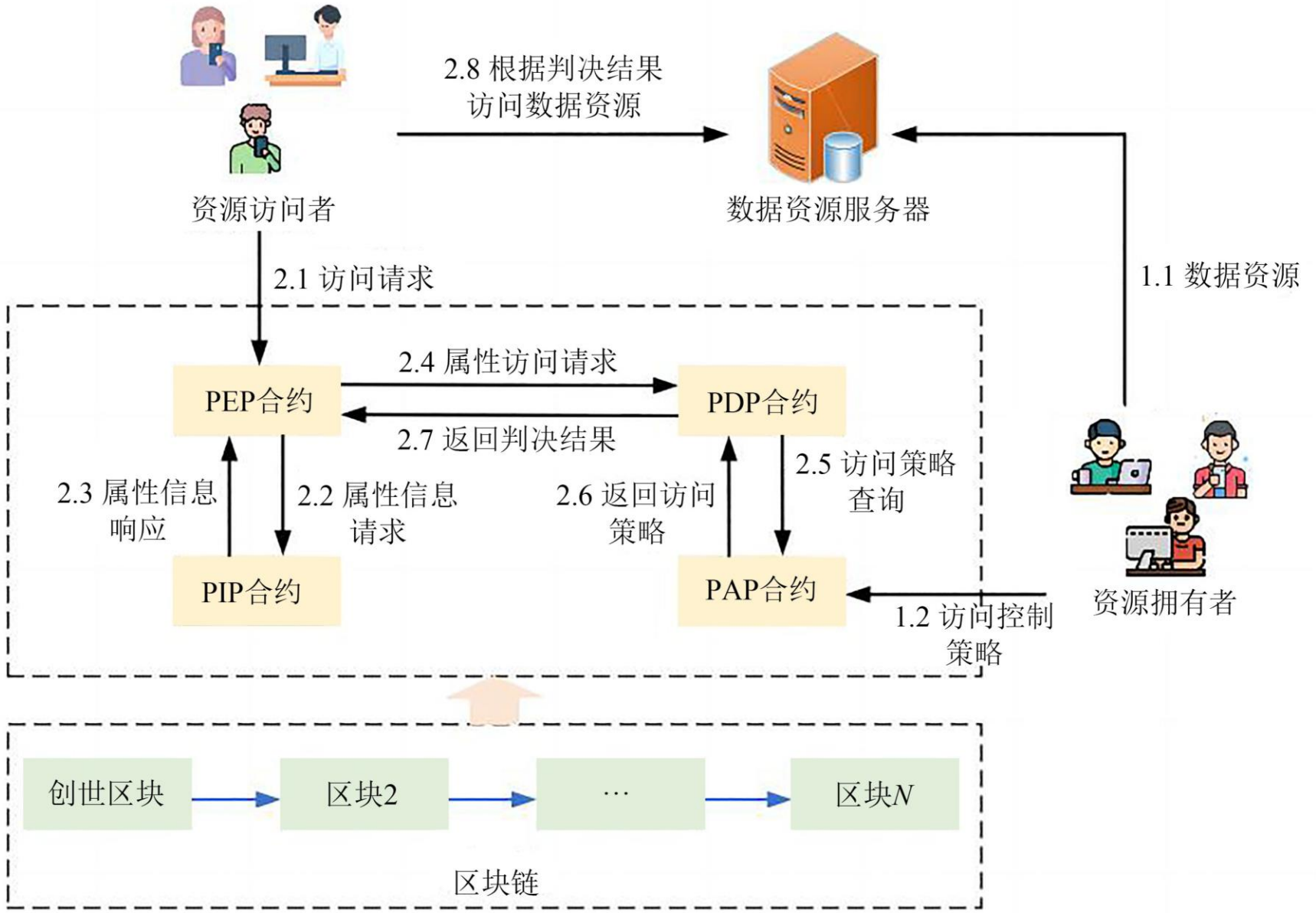
  升权限管理的灵活性和效率

  实现访问控制的去中心化

  实现精细的访问控制对属性进行分级处理

目录

系统设计


2.8 根据判决结果
访问数据资源
资源访问者
数据资源服务器
2.1 访问请求
1.1 数据资源
2.4 属性访问请求
PEP合约
PDP合约
2.7 返回判决结果
2.3 属性信息
响应
2.2 属性信息
请求
2.6 返回访问
策略
2.5 访问策略
查询
PIP合约
PAP合约
资源拥有者
1.2 访问控制
策略
创世区块
区块2
…
区块N
区块链

数据资源分级

数据资源拥有者根据数据资源的敏感度(Sensitivity,S)、关键度(Criticalness，C)、改动影响(Alter，A)三个维度对所拥有的数据资源进行分级。

高敏感(S3)、中敏感(S2)、弱敏感(S1）；严重(C3)、较重(C2)、一般(C1)；重大影响(A3)、较大影响(A2)，一般影响(A1)。

根据上述 3 种维度，将数据隐私等级从高到低划分为 5 级(Ｌ 5)、４级(Ｌ４)、３级(Ｌ３)、２级(Ｌ２)、１级(Ｌ１)

算法 1　数据等级划分算法

输入：数据 data={S，C，A}

输出：数据等级 Data_Level

```
1:if (S=S3&&C=C3&&A=A3) then
2:      Data_Level=5;
3:else if ((S=S3&&C=C3)||(S=S3&& A=A3)||
   (C=C3&&A=A3)) then
4:      Data_Level=4;
5:else if(S=S3||C=C3||A=A3) then
6:      Data_Level=3;
7:else if(S=S2||C=C2||A=A2) then
8:      Data_Level=2;
9: else
10:     Data_Level=1;
11:end if
12:returnData_Level;
```

用户信誉值评估

初始信誉值：$$R_{Cre}=\sum_{i=1}^{m}(\alpha_i \bullet S_i+\beta_i \bullet F_i)/m$$

历史信誉值：$$R_{History}=\frac{\sum_{i=1}^{n}(R_{Current} \bullet t_i)}{\sum_{i=1}^{n} t_i}$$

信誉值	信誉等级
(90, 100]	C5
(80, 90]	C4
(70, 80]	C3
(60, 70]	C2
(0, 60]	C1

综合信誉值：$$R_{Final}=a*R_{Cre}+b*R_{History}$$

属性访问控制智能合约设计

■智能合约的控制过程依赖于策略的决策点（PDP）和执行点（PEP），通过去中心化保证过程的安全、可靠、可信和可追溯。

具体实现过程如下：由数据资源拥有者设置资源隐私等级和访问控制策略并上传到策略管理点（PAP）；其次访问控制处理过程由策略信息点（PIP）提供属性查询服务；最后根据查询到用户信誉等级和数据隐私等级进行策略判决，得到授权结果。

PIP合约

算法 2　PIP 合约算法

输入：原始访问请求 NAR；区块链节点存储数据 BlockData

输出：相关属性访问请求 AAR

```
1:  attrTuple=parserNAR(NAR);
2:   for i=1 to BlockData.length do;
3:     for j=1 to attr_BlockData.length do;
4:      if (attrTuple.match(attr_blockdata[j])) then;
5:  {AAR.add(this.blockdata.transaction.attribute); continue;}
6:    end for;
7:  end for;
8:  return AAR
9: final;
```

- PIP负责管理存储客体属性、操作属性、主体属性和环境属性，以及属性值之间的关系，将其存储到区块链中，并提供属性信息查询。
- 首先，原始属性访问请求(NAR)将被发往PIP合约。其次，属性类事务区块将会被PIP合约遍历，从而获取特定属性信息，这些信息与原始属性访问请求匹配。如果成功，属性信息将被PIP合约组成属性访问请求(AAR)，并返回结果。

PAP合约

算法 3　PAP 合约算法

输入：属性访问请求 AAR；区块链节点存储数据 BlockData

输出：策略集 policy_set

```
1:data_level=parserAttr(AAR);
2: for i=1 to BlockData.length do;
3:    for j=1 topolicy_BlockData.length do
4:       if (data_level=this.data_level) then;
5: {policy_set.add(policy_BlockData[j]);}
6:    end for;
7: end for;
8: returnpolicy_set
9: final;
```

- 数据拥有者在发布数据资源时，会根据数据隐私等级制定相应的访问控制策略并存储到区块链中。策略管理合约负责管理数据资源的访问控制策略。

- 首先，属性访问请求（AAR）被发送给策略管理合约，策略管理合约解析AAR，并从搜索访问控制策略中获取相关属性信息。其次，访问控制策略区块将被策略管理合约遍历，并得到数据等级相应的访问控制策略，然后在策略集（policy_Set）中进行添加。最后，策略管理合约在遍历结束后给策略判断合约（PDP）返回策略集，以此判决访问控制策略。

PDP合约

算法 4　PDP 合约算法

输入：属性访问请求 AAR；访问控制策略集 policy_set

输出：permit or deny or unknown

```
1:permit_set=null; deny_set=null; unknown_set=null;
2: for i=1 to policy_set.length do;
3:decide_result=PolicyDecide(policy_set[i]);
4:    if (decide_result=permit) then;
5:    {permit_set.add(policy_set[i]);}
6:    else if (decide_result=deny) then
7:     {deny_set.add(policy_set[i]);}
8:    else
9: {unknown_set.add(policy_set[i]);}
10: end for;
11:if (permit_set! =null&&deny_set=null)then
12:       return permit;
13: else if
     (permit_set=null&&deny_set! =null) then
14:       return deny;
15:else if
     (permit_set! =null&&deny_set! =null) then
16:       returnerrorHandle();
17: else
18:       return unknown
19: final;
```

- 根据访问控制策略集和属性访问请求来进行的。例如，策略判决合约允许访问请求同时授予访问权限，当且仅当访问控制策略与数据访问者的属性信息相符；否则，策略判决合约拒绝本次访问请求。
- 策略判决合约的执行过程如下：第一，输入访问控制策略集policy_set和属性访问请求AAR。
- 第二，遍历访问控制策略集，先后判断属性访问请求（AAR）与访问控制策略是否配：如果匹配，则在许可策略集（permit_set）中添加访问控制策略；如果不匹配，访问控制策略添加到拒绝策略集（deny_set）中;否则添加到未知策略集（unknown_set）中。
- 第三，根据策略判决结果集可以得到判决结果。如果permit_set不为空且deny_set为空，则表示允许访问；如果permit_set为空且deny_set不为空，则表示拒绝访问；如果permit_set和deny_set都不为空，则表示判决结果有冲突，需要进行冲突处理；如果上述情况均未发生，则返回unknown。

目录

实验结果和分析

随着数据隐私等级的降低，访问控制时延也在降低。这是因为数据隐私等级越高，访问控制策略越复杂，策略检索时间和判决时间就越长

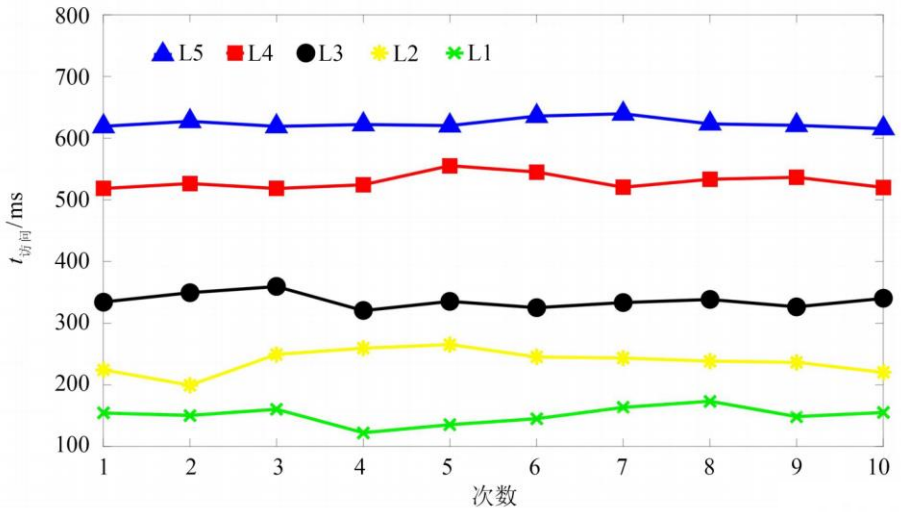


图 2　访问控制时延比较

策略判决时延($t_{判决}$)随着访问请求的增加而增加。这是因为随着访问策略的增加，不仅增加遍历空间，而且也增加策略判决复杂度。

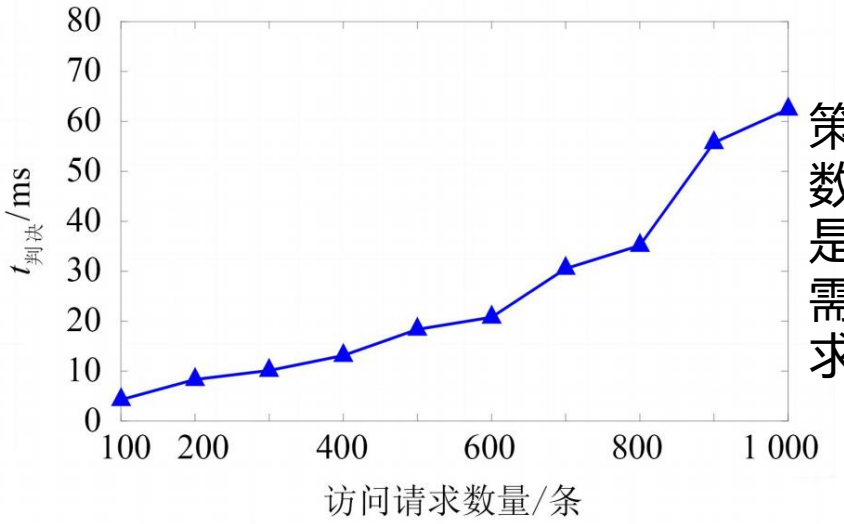


图 3　策略检索时长

策略检索时间随着访问请求数量的增长而线性增长。这是因为随着请求数量的增多，需要排队等待合约处理的请求时长增加。

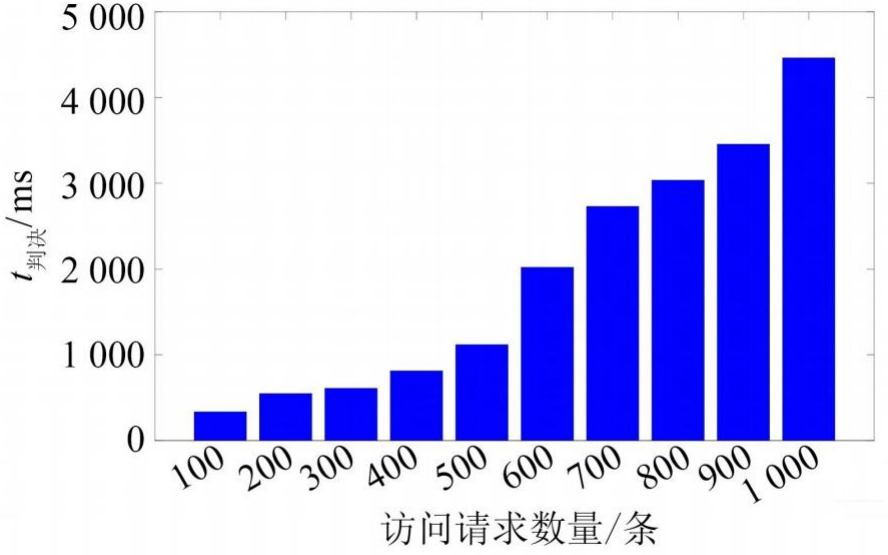


图 4　策略判决时延

实验结果和分析2

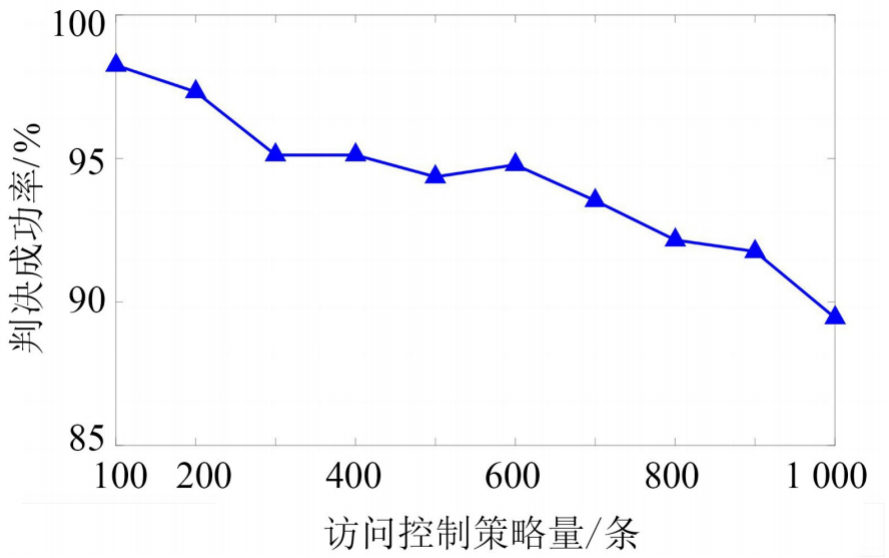


图 5　策略判决成功率

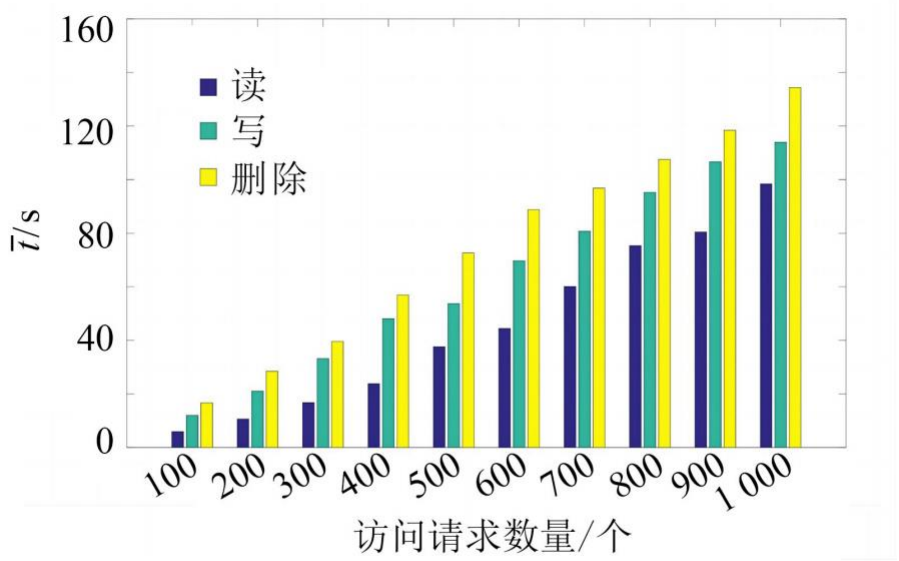


图 6　不同数量策略请求下的处理时间

如图 5 所示. 因为访问控制策略增多， 出现策略发生冲突的现象， 从而导致合约策略判决失败。

如图 6 所示. 同一时间内对访问策略执行不同操作所需要的平均时延(t)，读、写、删除的平均时延。

总结

- 针对访问控制存在中心化和数据共享效率低下的问题，基于属性访问控制机制与区块链技术结合提出了一种新型的属性分级访问控制机制。
- 新机制基于智能合约技术实现控制去中心化、访问可追溯和可审计的访问控制过程，不但提高访问控制的可信度而且实现了数据共享的安全性；通过设置数据隐私等级和访问用户当前信誉等级实现访问控制策略，提高用户的访问效率。
- 实验结果表明该方案能够实现控制去中心化、提高访问效率，实现访问控制可靠、可追溯，保证数据的安全与共享。

福州大学至诚学院
FUZHOU UNIVERSITY ZHICHENG COLLEGE

谢谢，请您批评指正！

林庆新：13860642501

2023.11.28