

一种基于属性的去中心化访问控制模型

马星晨,朱建涛,邵 婧,刘明达

(江南计算技术研究所,江苏 无锡 214083)

摘 要:随着网络规模与开放程度的不断加大,传统的基于属性的访问控制模型(attribute-based access control, ABAC)在实际应用中存在着中心节点负担过大,决策过程安全风险较高等问题。为了更好地提升基于属性的访问控制模型的安全性,且满足大规模分布式网络环境下的应用条件,提出了一种基于属性的去中心化访问控制模型(decentralized attribute-based access control, DABAC)。在基于属性的访问控制模型的基础上对访问控制模型进行扩展,通过权益证明和证据链条的方式,实现了去中心化的决策方式,进一步提升了决策支持库和访问记录的安全性,增加了访问决策的可信性。相比于传统的访问控制模型,DABAC 模型具有更高的安全性、灵活性和容错性,通过更加安全的访问请求决策和更加详细的访问过程记录,更好地保护了客体资源。

关键词:访问控制;去中心化;安全决策;权益证明;证据链条

中图分类号:TP309

文献标识码:A

文章编号:1673-629X(2018)09-0118-05

doi:10.3969/j.issn.1673-629X.2018.09.024

A Decentralized Access Control Model Based on Attribute

MA Xing-chen, ZHU Jian-tao, SHAO Jing, LIU Ming-da

(Jiangnan Institute of Computing Technology, Wuxi 214083, China)

Abstract: With increasing of Internet scale and openness significantly, the traditional attribute-based access control model (ABAC) has many problems in practical application, such as excessive burden of central nodes and high security risk in decision-making process. In order to enhance the security of ABAC model and satisfy the conditions of applications in the large scale distributed network environment, we propose a decentralized attribute-based access control model (DABAC). The access control model is extended according to that based on attribute, through proof of stake and evidence chain to achieve decentralized decision, further improving the security of decision support libraries and access records, increasing the credibility of access decision. Compared with the traditional access control model, DABAC has better security, flexibility and fault tolerance. By providing more secure access decisions and more accurate access records, the object is protected better.

Key words: access control; decentralization; secure decision; proof of stake; chain of evidence

0 引 言

访问控制技术是保障信息安全的重要防护措施,用来检验主体是否有合法的权限来访问恰当的客体。传统的访问控制模型包括自主访问控制模型(DAC)、强制访问控制模型(MAC)以及基于角色的访问控制模型(RBAC)等^[1-2]。基于属性的访问控制模型(attribute-based access control, ABAC)于 2005 年由 Eric Yuan 和 Jin Tong 提出^[3]。通过不同的属性或属性组^[4]来描述真实场景中出现的实体,通过基于属性的逻辑语义描述复杂的访问控制策略。将传统访问控制模型中的身份、角色等信息,以属性的方式抽象出来,

以便更加细粒度地制定访问策略,贴近真实场景。

在 ABAC 模型的基础上,文献[5]使用本体一致性推理对现有 ABAC 授权框架进行扩展,即通过对本体知识库的一致性检测来判断策略的一致性,提升了策略的可信性及模型的自愈能力。文献[6]设计了一种具备通用性的 Web 服务访问控制模型,使用 Browser/Artifact 的身份认证授权方式,最终由认证服务器通过声明判断用户身份是否合法。文献[7-9]同样采用集中式决策或有中心的分布式决策支持系统对主体是否可以访问客体进行授权决策。

以上模型虽然都对基于属性的访问控制模型在效

收稿日期:2017-09-03

修回日期:2018-01-18

网络出版时间:2018-05-16

基金项目:国家核高基重大专项(2013ZX01029002-001);国家重点研发计划战略高技术重点专项(17-H863-01-ZT-004-009-01)

作者简介:马星晨(1988-),男,硕士研究生,研究方向为操作系统安全;朱建涛,硕士,高级工程师,CCF 会员(5600S),研究方向为操作系统。

网络出版地址: <http://kns.cnki.net/kcms/detail/61.1450.TP.20180515.1651.028.html>

率 and 安全性上做了提升,但仍然在一定程度上将决策的正确性和可信性寄托于决策中心或中心策略库是否安全,缺乏对策略库的保护以及无法保证在策略库进行更新时的安全问题;且没有考虑到不同节点间的个性化差异;在主体对客体的访问行为发生后,不能做到对访问记录的防伪造和防抵赖。

随着网络服务形态的多元化,去中心化网络模型越来越清晰^[10],而从比特币衍生出的区块链技术又将会去中心化的思想提升到了前所未有的高度。在去中心化的网络中,任何参与者均可提交内容,由整个网络的参与者共同进行内容协同创作和贡献。每个网络节点都可以自成中心或具有中心的一切功能,从而避免了由中心决定节点而带来的安全隐患。

基于上述分析,为了更好地提升基于属性的访问控制模型的安全性,且满足分布式网络环境下的应用条件^[11-12],文中提出了一种基于属性的去中心化访问控制模型(DABAC),并对该模型的设计思想、运行原理和性能进行了详细描述和分析。

1 基于属性的去中心化访问控制模型

1.1 模型设计思想

为满足现有复杂网络环境下的访问控制模型需要具有灵活配置、贴近真实应用等特点,文中研究的DABAC模型与同类别的访问控制模型相比,具有以下特点:

(1) 采用去中心化思想设计的DABAC访问控制模型,所有参与的节点都持有访问记录和策略的副本,并在网络中保持同步更新,即使有一定数量的节点受损,也不会影响整个系统的正常运行。同时,由于所有节点共同维护着相同的策略集和访问记录,使得所有节点都可以对整个系统中的操作进行监督。

(2) 采用基于权益证明^[13]的去中心化方式来保证群策结果的可信性。所有节点上主体对客体的访问请求都会在全网范围内进行表决。由于模型中权益与安全等级成正比,因此安全等级越高的节点的本地策略库的安全性和可信性也越高,从而该类节点所给出的决策的可信性也就越高。

(3) 访问主体在被授权访问时需要接受系统环境的验签名,并使用私钥对访问记录进行数字签名,通过叠加哈希的方法建立证据链条,以此杜绝其他访问主体的冒名访问,以及恶意访问主体通过伪造其访问记录以抵赖已经发生过的访问行为。

1.2 相关概念和定义

基于属性的去中心化访问控制模型的主要功能模块以及不同模块和节点之间的应用关系如图1所示。其主要功能模块有属性认证机构(attribute authorities,

AA)、策略执行点(policy decision point, PEP)、策略决策点(policy decision point, PDP)和策略及存储一致性检查点(policy & storage coherence point, P&SCP)。

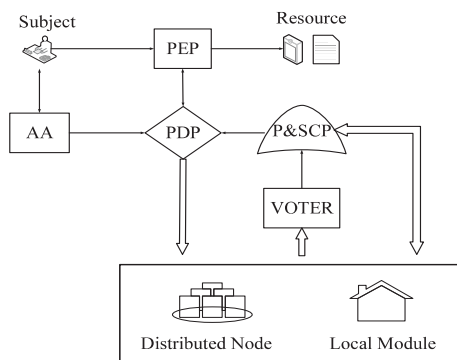


图1 基于属性的去中心化访问控制模型

1.2.1 模型基本元素定义

DABAC模型由访问主体、资源客体和操作三个对象组成,通过对访问主体属性、资源客体属性、系统环境属性集的构建,按照对客体访问的策略判定规则进行判定,决定对主体的操作授权。

定义1(访问主体 subject):访问主体即对资源和被保护数据进行访问的实体。

定义2(资源客体 resource):资源客体为被动实体,在整个访问流程中处于被动位置。

定义3(操作 operate):操作是指访问主体对于资源客体的访问行为,定义了主体对客体的具体访问行为以及访问类型。

定义4(访问主体属性 SA):在DABAC模型中,访问主体属性主要由用户ID、访问权限、生命周期和访问历史等组成。

定义5(客体资源属性 RA):资源客体属性主要由资源ID(文件名称)、当前状态和安全等级组成。

定义6(系统环境属性 EA):系统环境属性主要由时间、安全等级和历史记录组成。

定义7(权益 security_level):节点所具有的安全等级即为该节点拥有的权益。

1.2.2 访问策略规范

DABAC模型中使用去中心的方式进行决策,其主要目的是通过提升模型决策的准确性和可信性,保护资源客体的安全,防止其被非法访问和使用。

利用SA、RA和EA分别表示访问主体S、资源客体R和环境E的属性赋值关系,且各个对象的属性以集合的方式存在:

$$ATT(S) \subseteq SA_1 \times SA_2 \times \cdots \times SA_n, 1 \leq n \leq N$$

$$ATT(R) \subseteq RA_1 \times RA_2 \times \cdots \times RA_k, 1 \leq k \leq K$$

$$ATT(E) \subseteq EA_1 \times EA_2 \times \cdots \times EA_m, 1 \leq m \leq M$$

基于DABAC模型构建的访问控制系统可以根据不同的应用场景和访问模式设定具体规则。其规则的

POS 模式是以节点的安全等级和可靠性为基础,通过竞争表决机会和正确性,获得奖励,用以进一步提高节点的可靠性。奖励方程如下:

$$\text{Reward} = \text{Reliability} \times \frac{\text{security_level}}{\text{Target}}$$

$$\text{New_Reliability} = \text{Reliability} + \text{Reward}$$

其中,Target 可以根据模型的实际应用情况做灵活调整。

在 POS 竞争过程中,随着该节点正确表决结果的次数不断增多,节点获得的表决奖励将不断累积,自身可靠性也将不断提高,完成权益证明的时间也将越快。

群策模块 VOTER 负责收集发出决策请求的节点在其关门时间内收到的所有表决结果,通过表决函数来得到最终的结果:

$$f_{\text{vote}} = f(\text{LD}, \text{ND}_1, \text{ND}_2, \dots, \text{ND}_n)$$

其中

$$f(x_0, x_1, \dots, x_n) = \text{BOOL}(x_0 + x_1 + \dots + x_n - n/2)$$

当结果为 1 时,访问主体的访问请求被允许;当结果为 0 时,访问主体的访问请求被拒绝。如图 3 所示。

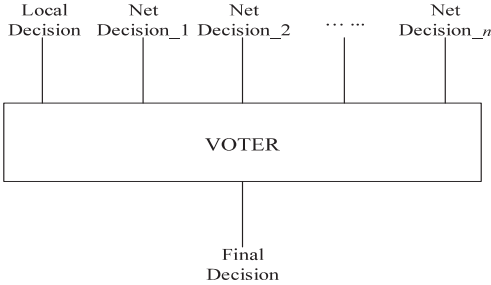


图 3 基于去中心化的群策模块

1.5 分布式策略和证据链条机制

通过 DABAC 模型中的 P&SCP 来保证使用 DABAC 模型构建的访问控制系统的分布式策略库和访问记录的一致性。

P&SCP 接收来自网络节点和本地节点的所有访问记录和策略更新,而后根据不同的类别和需求,将收到的信息分发至不同的功能模块。在分布式存储的基础上,使用数据存证技术对策略进行更新和修改,使用证据链条技术保存访问记录,以保证全网节点的策略库和访问记录的一致性。

(1) 基于分布式辅助的身份征信机制。

策略的更新由具有管理员权限的用户执行,根据节点的安全等级不同,只能自上而下地更新策略,即高安全等级的节点可以更新低安全级节点的策略,反之不行。

所有不同安全等级的管理员身份信息在基于 DABAC 模型的系统建立之初就被广播全网并存储于各个节点的 PAP 内,在进行策略更新时,该节点必须将更新后的策略、更新后策略库的哈希值、执行本次更

新任务的管理人员的身份信息一起打包,并广播全网。任何收到策略更新信息的节点都会对发送信息的管理员身份进行校验,校验成功后再对本地策略库进行更新。

(2) 基于证据链条的访问记录一致性机制。

通过使用时间戳技术以及访问主体私钥签名的方式并建立访问流程的前后关联关系,实现了将访问主体的访问行为以时间序列串联成为数据证据链条。该证据链条从访问主体接入系统起就将相关数据加盖时间戳并用其私钥进行签名,之后,将包含时间戳和私钥签名的数据通过特定加密算法生成唯一对应的数据 Hash 值;之后每一步新数据的产生都会被立即加盖时间戳并使用私钥进行签名,并且基于前一步已经产生的 Hash 值生成一个新的唯一的 Hash 值。最后生产的哈希值会被全网广播,并被保存在全网所有节点的数据库中。证据链条工作原理如图 4 所示。

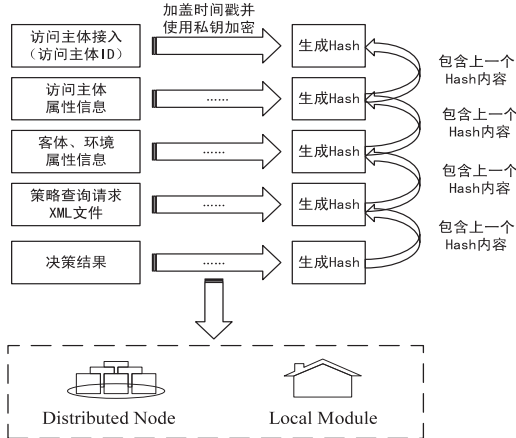


图 4 证据链条生成过程

2 安全性分析

2.1 DABAC 模型安全性分析

(1) 最小特权原则。

最小特权原则是指每个访问主体只能拥有刚好完成工作的最小权限^[14]。在基于 DABAC 模型构建的访问控制系统中,不是根据访问主体的职责进行简单的一次性权限划分,而是通过收集访问主体、资源客体和系统环境的属性,访策略库中进行查询,得出最终决策。该方式不仅考察访问主体本身,还根据访问主体的任务性质进行综合决策,从而对最终分配给访问主体的权限做到最大控制。

(2) 职责分离原则。

职责分离是指将不同的权限许可分派给不同的模块用以互相牵制,使得单个模块的功能必须与其他模块的工作相一致或相联系,并受到监督和制约,防止出现一个模块完成两项不相容的工作的情况^[15]。在 DABAC 模型中,在为访问主体分配属性时,相互冲突

的两个或多个属性不能分配给同一个访问主体,以避免拥有足够权限的恶意访问客体在缺少监督和制约的情况下危害系统安全。

(3) 多人负责原则。

通过授权分散化,即对于关键任务必须在功能上进行划分,使得该任务由多人共同承担,保证任何个体无法拥有完成该任务的全部权限。DABAC 模型通过去中心化的策略库使得整个网络中的任意一个节点只能基于自身的策略库做出表决,而无法做出最终决策。最终决策需要由发出策略查询请求的节点上的 P&SCP 模块汇总所有节点的表决后作出最终决策。由于最终决策是综合了全网节点上的所有策略库的表决而确定的,想要对最终决策进行攻击需要控制全网过半的节点,随着网络规模的不断增大,攻击成本也将大大提升。

2.2 与相关模型比较

相比于传统访问控制模型,ABAC 模型具有很好的灵活性和可扩展性。本节从决策方式和策略及访问记录更新方式两方面对 DABAC 模型和 ABAC 模型进行比较。

(1) 决策方式。

传统 ABAC 模型多采用集中式策略库的形式进行决策,其安全性依托于整个网络的可靠程度和策略库的自身安全。DABAC 模型采用分布式决策,通过模型的全网一致性特点来保证整个系统网络内的所有节点共同维护一个策略库。该模型得出的决策是由全网所有节点共同表决的结果,若攻击者想要对该结果做出更改,则需要监听大于百分之五十的网络流量,或控制超过一半的网络节点,才有可能对最终的决策结果做出修改。

(2) 策略及访问记录更新方式。

对于访问策略和访问历史记录,传统 ABAC 模型通过在网络中建立中心数据库节点的方式进行存储,其安全保障完全依赖于中心数据库的自身安全。基于 DABAC 模型架构的访问控制系统使用基于分布式辅助的身份征信和证据链条的方式,分别保证了策略更新和访问记录的一致性。需要更新策略库的节点必须按照模型规则,证明进行策略更新操作人员的身份合法性;使用时间戳技术以及访问主体私钥签名的方式并建立访问流程的前后关联关系,并且叠加之前记录的哈希值,确保了访问主体的访问请求和决策结果的记录不被篡改。

3 结束语

针对现有 ABAC 模型在大型分布式环境下进行应用所存在的弊端,提出了一种基于属性的去中心化

访问控制模型。在基于属性的访问控制模型的基础上对访问控制模型进行扩展,引入了去中心化的概念,提升了策略库和访问记录的安全性,增加了访问决策的可信性。同时对 DABAC 模型的安全性进行了详细分析,相比于传统访问控制模型,该模型具有更高的安全性、灵活性和容错性,通过更加全面地对访问请求进行决策,使得客体资源受到更好的保护。

参考文献:

- [1] 赵明斌,姚志强. 基于 RBAC 的云计算访问控制模型[J]. 计算机应用,2013,32(S2):267-270.
- [2] 李凤华,苏 铨,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.
- [3] YUAN E, TONG Jin. Attributed-based access control (A-BAC) for web services[C]//IEEE international conference on web services. Orlando, FL, USA; IEEE, 2005.
- [4] 李晓峰,冯登国,陈朝武,等. 基于属性的访问控制模型[J]. 通信学报,2008,29(4):90-98.
- [5] 倪 川,黄志球,王珊珊,等. 基于属性的支持策略本体推理的访问控制方法研究[J]. 计算机科学,2015,42(3):96-101.
- [6] 展宗思. 基于属性的跨域访问控制模型设计[J]. 网络安全技术与应用,2013,13(3):32-34.
- [7] 夏春涛,杨艳丽,曹利峰. 基于 ABAC 的 Web Services 访问控制研究[J]. 计算机应用与软件,2012,29(2):83-85.
- [8] JIN Xin, KRISHNAN R, SANDHU R. A unified attribute-based access control model covering DAC, MAC and RBAC [C]//Proceedings of the 26th Annual IFIP WG 11.3 conference on data and applications security and privacy. Paris, France; Springer, 2012:41-55.
- [9] 刘 江,张红旗,代向东,等. 一种 ABAC 静态策略冲突检测算法[J]. 计算机工程,2013,39(6):200-204.
- [10] 朱国库,蒋文保. 一种去中心化的网络域名服务系统模型[J]. 网络空间安全,2017(1):14-18.
- [11] 叶春晓,钟 将,冯 永. 基于属性的访问控制策略描述语言[J]. 东南大学学报:英文版,2008,24(3):260-263.
- [12] ZHANG Xinwen, LI Yingjiu, NALLA D. An attribute-based access matrix model [C]//Proceedings of the 2005 ACM symposium on applied computing. Santa Fe, New Mexico; ACM, 2005:359-363.
- [13] LI Wenting, ANDREINA S, BOHLI J M, et al. Securing proof-of-stake blockchain protocols [C]//Data privacy management, cryptocurrencies and blockchain technology. [s. l.]:[s. n.], 2017:297-315.
- [14] 王 瑞,杨震晖. 论网络环境下最小特权原则与隐私权的法律保护[J]. 北方工业大学学报,2014,26(2):13-17.
- [15] BOTH A R A, ELOFF J H P. Separation of duties for access control enforcement in workflow environments[J]. IBM Systems Journal, 2001, 40(3):666-682.