计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2021,30(8):104−110 [doi: 10.15888/j.cnki.csa.008005]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

面向新一代调控系统业务场景的权限管理①

季惠英[1,2], 彭　晖[1,2,3], 宋奇兵[1,2], 周　玲[1,2], 马　斌[4], 陈　云[1,2]

[1](南瑞集团有限公司 (国网电力科学研究院有限公司), 南京 211106)
[2](国电南瑞科技股份有限公司, 南京 211106)
[3](智能电网保护和运行控制国家重点实验室, 南京 211106)
[4](国网河北省电力有限公司, 石家庄 050021)
通讯作者: 季惠英, E-mail: jihuiying@sgepri.sgcc.com.cn

摘　要: 文中分析了新一代调控系统在系统架构、人机交互方式、业务组织方式等方面的变化, 梳理了新一代调控系统业务场景对权限管理的新需求, 提出了面向新一代调控系统业务场景的权限管理方案, 并对其关键技术如基于路径的全局受控资源标识定义、基于元数据的受控资源管理、基于规则引擎的多因素访问控制、基于上下级关系的跨域访问控制等进行了讨论, 最后结合新一代调控原型系统进行功能验证, 为上层各业务场景提供了立体式的受控资源安全访问控制手段.

关键词: 分布式系统; 资源管理; 跨域访问; 多因素约束; 访问控制

引用格式: 季惠英,彭晖,宋奇兵,周玲,马斌,陈云.面向新一代调控系统业务场景的权限管理.计算机系统应用,2021,30(8):104–110. http://www.c-s-a.org.cn/1003-3254/8005.html

Business Authority Management in New Generation Power Grid Dispatching and Control System

JI Hui-Ying[1,2], PENG Hui[1,2,3], SONG Qi-Bing[1,2], ZHOU Ling[1,2], MA Bin[4], CHEN Yun[1,2]

[1](NARI Group Corporation (State Grid Electric Power Research Institute), Nanjing 211106, China)
[2](NARI Technology Co. Ltd., Nanjing 211106, China)
[3](State Key Laboratory of Smart Grid Protection and Control, Nanjing 211106, China)
[4](State Grid Hebei Electric Power Corporation, Shijiazhuang 050021, China)

Abstract: This study analyzes the changes of the new generation power grid dispatching and control system in architecture, human-computer interaction modes, business organization modes, etc. It sorts out the new business-oriented requirements for authority management and proposes the business-oriented authority management solution with regard to this new system. The key technologies in this system are discussed, such as path-based global controlled resource identification and definition, metadata-based controlled resource management, multi-factor access control based on a rule engine, and cross-domain access control based on upper and lower organizational relationships. This solution is verified in a prototype system and provides a multi-dimensional secure access control method of controlled resources for business scenarios in the new generation power grid dispatching and control system.

Key words: distributed system; resource management; cross-domain access; multi-factor constraint; access control

2017 年初国家电网有限公司提出研发新一代电网调度控制系统[1]. 在继承现有电网调度自动化系统成果基础上, 新系统引入云计算、大数据及人工智能等新技术, 采用“物理分布、逻辑统一”的全新系统架构, 部

① 基金项目: 国家重点研发计划 (2017YFB0902600); 国家电网公司总部科技项目 (SGJS0000DKJS1900259)
Foundation item: National Key Research and Development Program of China (2017YFB0902600); Science and Technology Project of Headquater of State Grid (SGJS0000DKJS1900259)
收稿时间: 2020-11-11; 修改时间: 2020-12-12; 采用时间: 2020-12-18; csa 在线出版时间: 2021-07-31

署“位置无关、权限约束、同景展示”的人机云终端, 构建具备“全、快、准”特征的应用功能, 全面支撑新一代电力系统安全稳定运行[2−5]. 无论是系统架构、人机交互方式的变化, 还是新技术、新应用的引入, 对新一代调控系统安全防护提出了更高的要求, 而业务安全是其重要环节之一.

分布式环境下, 权限管理是保障系统业务安全的重要手段, 主要功能包括身份认证和访问控制. 身份认证通过密码、数字证书、生物特征等认证方式确认用户身份, 解决“你是谁”的问题, 避免非法用户进入系统[6,7]; 访问控制通过预定义的权限约束规则对用户访问系统的能力进行限制, 解决“你能做什么”的问题, 避免用户的非法操作[8,9].

近年来, 电网调度控制系统在安全防护方面已有较多研究, 主要集中在网络安全方面, 侧重于网络边界安全防护[10−13], 而在业务安全防护方面研究较少. 目前, 国网范围内智能电网调度技术支持系统基础平台 (简称 D5000 系统)[14] 使用广泛, 该平台提供基于角色访问控制模型和基于资源访问控制模型的权限管理子系统, 为上层业务提供统一权限管理服务, 功能包括用户管理、功能管理、角色管理、授权管理、权限鉴权等, 保证了系统内用户对系统内受控资源访问的安全性和可靠性. 但是, 该权限管理子系统存在以下不足:

(1) 受控资源类型以及受控资源实例数量支持有限, 类型只支持功能类、表域特殊属性类、报表文件类和图形文件类, 其中功能类实例数≤200;

(2) 受控资源定义维度单一, 只支持系统级定义, 没有与业务应用关联;

(3) 未解决跨域业务安全防控问题, 只适用于单系统内访问控制.

本文在深入分析新一代调控系统业务场景权限管理实际需求的基础上, 提出面向新一代调控系统业务场景的权限管理方案, 详细阐述了基于路径的全局受控资源标识定义方法、基于元数据的受控资源管理方法、基于规则引擎的多因素约束访问控制方法以及基于上下级关系的跨域访问控制方法关键技术, 研发实现了权限管理原型系统, 为保障新一代调控系统业务安全提供技术手段.

1 需求分析

新一代调控系统体系架构的核心特征是“物理分布、逻辑统一”[2], 建设方式如图 1 所示: 一是构建模型数据中心, 实现全网模型和数据的统一管理和按需使用, 为全局分析决策提供同源同质、时空多维的全局模型; 二是创新建设分析决策中心, 将原分散于各调控中心的分析决策功能相对集中部署; 三是升级新架构下的监控系统, 支持全局监视、作业自动导航和所辖电网实时就地控制; 四是构建位置无关、权限约束、同景展示的人机云终端, 支持调控人员本地、异地无差别监视控制.

图 1 新一代调控系统架构示意图

与传统智能电网调度控制系统相比, 新一代调控系统在系统架构、人机交互方式、业务组织方式、应用功能特性上存在明显的变化, 这种变化对权限管理提出了新的挑战.

(1) 系统架构变化

新一代调控系统打破了以往智能电网调度控制系统的地域限制, 由本地一套系统运行模式转变为地理位置广域分布的多套系统协同运行模式. 系统的这种广域特性, 要求用户可以方便快捷的登录其他异地系统, 或者在用户无感知情况下在本系统中进行跨域访问其他系统, 不受控的非法访问的影响范围将从单系统扩散到多系统中, 因此新一代调控系统访问控制范围需从单系统内扩大到多系统间.

(2) 人机交互方式变化

新一代调控系统启用了全新的云终端交互方式 (人机云终端具有地理位置无关性)[15], 这种方式打破了以往智能调度控制系统本地工作站模式, 新一代调控系统中的模型数据中心、分析决策中心、监控系统通过人机交互网在任意时刻、任意地点均可达, 这使得访问系统的用户在地域、时间、业务等多个维度上变

得不可控, 客户端环境因素变得复杂, 环境约束成为权限管理不可忽略的一个方面, 因此新一代调控系统访问控制维度需从业务维度扩展到环境维度.

(3) 业务组织方式的变化

新一代调控系统采用了全新的业务组织方式, 业务概念包括功能、子场景和场景. 功能是调控系统中包含数据输入输出和数据处理的过程; 场景由各功能根据业务逻辑灵活组合而成, 满足不同调控机构各业务的需求; 子场景是场景中逻辑紧密的功能子集. 复杂场景可包含多个子场景, 简单场景可只包含一个子场景; 功能及子场景均系统内部署, 场景可跨系统部署. 这种新的业务组织方式, 需要对系统受控资源的管理粒度更精细化, 因此新一代调控系统访问控制粒度需从系统级别细化到业务场景级别.

(4) 应用功能特性变化

新一代调控系统应用具备“全局”特征[5], 模型全、数据全、功能全, 这意味着系统将进入大规模信息共享时代, 信息急剧膨胀, 资源种类多、体量大且变化频繁. 这种应用特性, 使得受控资源管理的可扩展性要求更高, 因此新一代调控系统受控资源管理手段需要由静态配置方式转变为动态配置方式.

2 总体设计

根据新一代调控系统业务访问控制需求, 权限管理软件采用就地部署方式. 该方式要求在模型数据中心、分析决策中心、监控系统均独立部署权限管理软件, 使用图形化手段对系统内部用户、外部用户、受控资源以及权限策略进行管理, 同时为业务提供透明访问接口, 从业务角度为访问新一代调控系统关键资源提供安全保护机制.

2.1 功能架构

该软件功能架构如图 2 所示, 包括受控资源管理、用户权限配置以及用户权限验证.

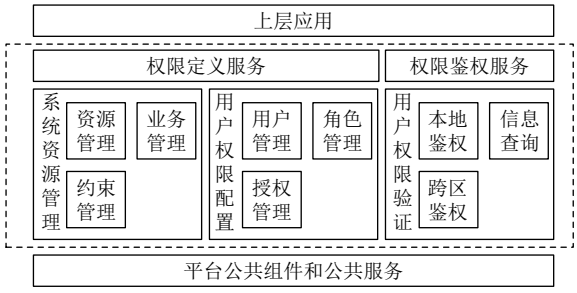

图 2 新一代调控系统权限软件功能模块示意图

(1) 受控资源管理

系统中任意需要访问控制的对象均可配置为受控资源, 例如操作、数据、文件等. 本文采用元数据管理方法, 通过类型、类型扩展属性、实例、实例扩展属性、业务资源来描述受控资源信息, 以适应不断新增的受控资源类型以及实例, 提高受控资源管理的灵活性和扩展性.

(2) 用户权限配置

用户权限配置采用基于角色访问控制模型和资源访问控制模型相结合的方法, 定义用户与角色的包含关系、用户对受控资源的控制策略、角色对受控资源的控制策略. 用户最终的受控资源控制策略是用户受控资源控制策略和用户所包含角色的受控资源控制策略的合集, 当两者存在冲突时, 以用户受控资源控制策略为优先. 本文中, 除考虑受控资源外, 对用户访问受控资源的时间特性和位置特性也进行了管理, 采用基于规则引擎方法定义权限生效的时间规则和位置规则并配置用户与规则的关系, 从而扩展了访问控制约束的维度.

(3) 用户权限验证

根据用户权限配置数据, 对每次用户受控资源访问操作进行权限验证, 判断给定的受控资源访问约束是否成立. 在新一代调控系统中, 用户权限验证包括本地验证和跨域验证. 本文采用基于上下级关系的跨域访问控制策略, 实现“上级访问”, “下级访问”、“同级访问”以及“访客访问”等多种跨域控制策略, 将访问控制范围从单系统扩展到多系统间.

2.2 部署架构

如图 3 所示, 权限管理模块在各系统均独立部署, 负责本系统受控资源的安全访问控制. 用户访问系统时首先通过安全认证中心进行身份认证, 然后通过被访问系统的权限管理模块进行安全访问控制. 权限的鉴权模块以当前系统的权限策略为判断依据进行内外访问鉴权和信息查询.

3 关键技术

3.1 基于路径的全局受控资源标识定义方法

全局受控资源标识定义需要考虑以下几个方面:

(1) 系统基于“物理分布、逻辑统一”的理念, 将分析决策中心、模型数据中心和监控系统通过高速通信网络连接起来, 形成逻辑上统一的大系统. 受控资源在逻辑上属于虚拟大系统, 但在跨域访问时需要区分受

控资源所属实际物理系统.

(2) 系统采用“场景”、“子场景”新的业务概念, 需考虑不同业务对同类资源差异化的访问控制需求, 受控资源标识需要明确资源所属业务实例.

(3) 受控资源是系统中需要受控访问的实体的统称, 常见类型包括: 操作、数据、文件等. 不同受控资源类型实例描述方式不同, 例如操作类通过操作名称定义、文件类通过路径和文件名定义等, 因此, 在受控资源标识中需要明确资源的类型, 从而确定该类型实例的描述方法.

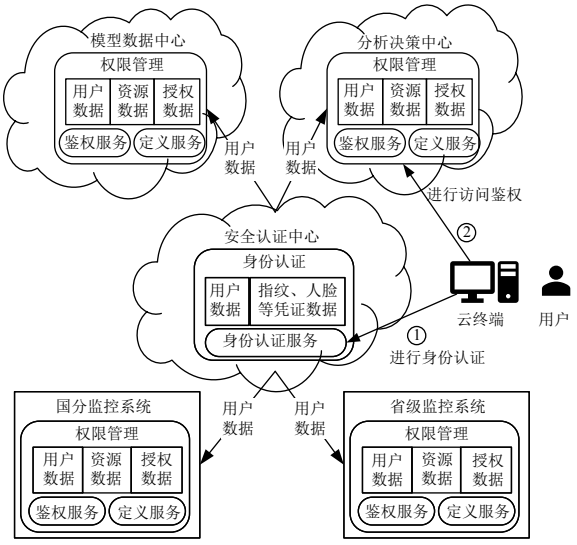

图 3 新一代调控系统权限软件部署示意图

本文提出基于路径的全局受控资源标识定义方法, 按系统属性、业务属性、类型属性以及实例描述的层次组织, 在不同的属性间以“:”分隔, 格式如下所示:

<domainObj>:<scnObj>:<resourceTypeCode>:<resourceInstance >

其中, domainObj 表示物理系统属性; scnObj 表示业务属性; resourceTypeCode 表示受控资源类型; resourceInstance 表示受控资源实例.

根据上述定义方法, 以某监控系统公共服务业务下表域资源的节点信息表 node_info) 节点名 (name) 为例进行说明:

格式: FXJC1:realtime/public:RESTYPE_TABCOL:node_info/name

其中, FXJC1 为某监控系统全局系统名, realtime/public 为业务实例, RESTYPE_TABCOL 为表域类型标识, node_info/name 为具体的表域类型实例. 对于<domainObj>和<scnObj>关键字可使用“-”标识其默认属性, 分别指代被访问系统以及系统全业务.

3.2 基于元数据的受控资源管理方法

新一代调控系统打破了以往智能电网调度控制系统的地域限制, 由本地一套系统运行模式转变为地理位置广域分布的多套系统协同运行模式, 系统间交互以及信息资源的共享变的更加频繁, 这意味着受控访问的资源信息将急剧膨胀. 如何有效管理庞大的受控资源, 是权限管理解决的核心问题之一. 本文提出了基于元数据的受控资源管理方法, 通过对已知受控资源类型抽象建模, 满足受控资源持续更新、灵活定义需求, 有效提升受控资源管理的可扩展性.

受控资源元数据包括资源类型、资源类型扩展属性、资源实例、资源实例扩展属性、业务资源, 表结构原型设计如图 4 所示.

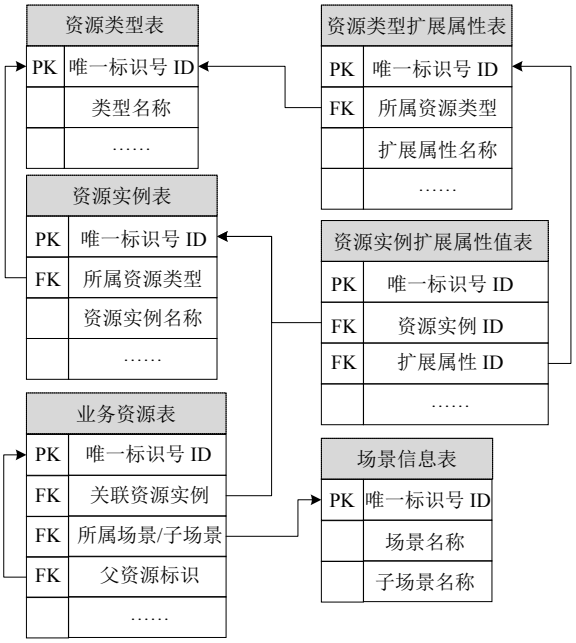

图 4 基于元数据受控资源管理表结构原型

(1) 资源类型用于定义资源类型标识以及该资源类型对应的权限效力, 例如操作资源, 其类型标识为 RESTYPE_OP, 其权限效力包括允许、禁止; 文件资源, 其类型标识为 RESTYPE_FILE, 其权限效力包括可读、可写、可删除、禁止读、禁止写、禁止删除.

(2) 资源类型扩展属性用于描述该资源类型的特征属性, 例如操作类具有操作名属性、文件类具有根路径及文件名属性.

(3) 资源实例和资源实例扩展属性用于描述具体的资源实例, 例如图形文件、报表文件是文件类资源实例.

(4) 业务资源是与具体业务场景绑定的资源实例. 新一代调控系统业务场景间存在大量属性相同的资源, 为避免在各场景下重复定义, 先将其定义为业务场景无关的资源实例, 再与需要的业务场景进行关联.

下面以表数据资源为例说明元数据定义方法, 步骤如下:

(1) 定义资源类型及权限效力. 表数据资源类型为 RESTYPE_DATA, 其权限效力包括可读、可写、可删除、禁止读、禁止写、禁止删除.

(2) 定义资源类型扩展属性. 表数据资源类型扩展属性包括: 表名、主键域、显示域、检索域、过滤条件等.

(3) 定义表数据资源实例. 如需定义图形信息表表数据资源实例, 表 1 显示了一种可能的资源实例扩展属性填写样例.

表 1 图形信息表表数据资源实例定义示例

属性	属性值
表名	SYS_GRAPH_B
主键域	ID
显示域	NAME
检索域	GRAPH_TYPE

3.3 基于规则引擎的多因素约束访问控制方法

新一代调控系统启用全新人机云终端交互方式, 与以往智能电网调度控制系统人机相比, 人机云终端具有开放性、访问透明性和位置无关性的特点[4,9]. 针对人机云终端的特点, 提出基于规则引擎的多因素约束访问控制方法, 定义用户在时间维度、位置维度的访问约束, 使得用户在不同时间、不同地理位置具有不同的受控资源访问权限, 提升新一代调控系统受控资源安全防护的全面性.

如图 5 所示, 在位置维度方面, 按云终端 IP 地址设置约束. 在约束管理中创建 IP 地址约束实例, 例如配置 IP 网段 192.168.*.*为本地云终端网段, 约束为“权限生效”. 将该位置约束作用到某权限规则上, 例如权限规则为“用户登陆监控系统 A 允许”, 则实际含义为用户只有通过 192.168.*.*网段的人机云终端才能访问监控系统 A, 用户在其他网段云终端上禁止访问监控系统 A.

如图 6 所示, 在时间维度方面, 支持时刻约束和时段约束. 在约束管理中创建时段约束实例, 例如配置时段每天 8:00～17:00 为工作时间, 约束为“权限生效”. 将该时间约束作用到某权限规则上, 例如权限规则为“用户登陆监控系统 A 允许”, 则实际含义为用户只有在每天 8:00～17:00 才能通过人机云终端访问监控系统 A, 在该时间段外用户无法访问监控系统 A.

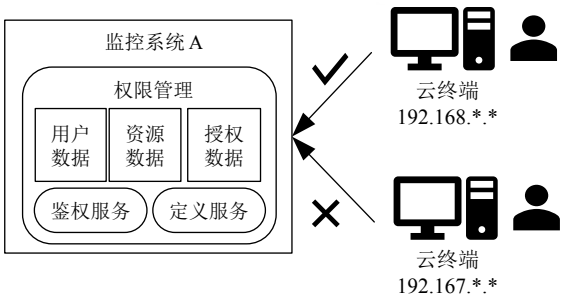

图 5 权限管理位置约束示意图

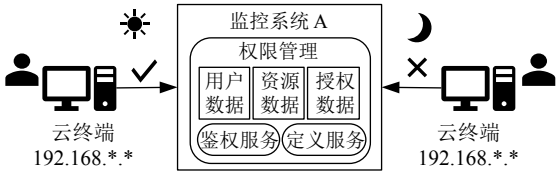

图 6 权限管理时间约束示意图

3.4 基于上下级关系的跨域访问控制方法

与以往智能电网调度控制系统相比, 新一代调控系统的广域特性以及数据共享特性, 使得系统间跨域访问成为一种常规操作, 如何有效控制跨域访问的安全性以及方便配置跨域访问约束是需要解决的一个难题. 本文提出了基于上下级关系的跨域访问控制方法, 通过用户所属组织机构与被访问系统所属组织机构的等级关系, 确定用户扮演的跨域访问角色——跨域访问角色包括“上级访问”、“下级访问”、“同级访问”以及“默认访问”, 然后使用跨域访问角色所配置的权限规则进行鉴权.

如图 7 所示, 用户在安全认证中心进行身份认证, 返回身份认证信息 (包含用户所属组织机构信息); 用户访问某系统时进行访问控制, 首先根据用户所属组织机构和系统所属组织机构关系进行访问模式判断, 然后根据访问模式进行对应处理. 本地访问模式, 即用户和被访问系统所属组织机构一致, 则根据用户获取其权限规则进行判断; 跨域访问模式, 即用户和被访问

系统所属组织机构不同, 则根据所属组织机构的上下级关系确定用户扮演的跨域访问角色, 然后根据对应的跨域访问角色获取其权限规则进行判断. 在图 7 中, 步骤①、②示意了身份认证过程; 步骤③~⑤示意了本地访问模式过程; 步骤⑥~⑧示意了跨域访问模式过程.

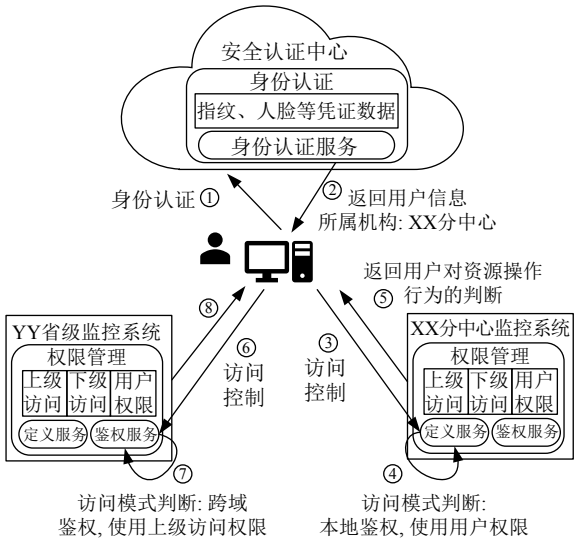

图 7 跨域鉴权示意图

4 验证及应用

开发团队搭建实验验证环境, 用于验证面向新一代调控系统业务场景的权限管理方案, 重点验证了基于规则引擎的多因素约束访问控制功能以及基于上下级关系的跨域访问控制功能.

4.1 实验验证环境

实验验证环境如图 8 所示, 由 2 个监控系统、2 个人机云终端组成. 监控系统 A 所属组织机构为 ORG-HD, 监控系统 B 所属组织机构为 ORG-JS, 其中 ORG-HD 的等级高于 ORG-JS. 配置云终端 IP 地址分别为 10.85.166.18、10.85.63.122. 运行在人机云终端的软件通过人机交互网访问监控系统.

4.2 验证内容

在监控系统 A 定义用户权限规则、时间约束和位置约束, 如表 2、表 3 所示; 在监控系统 B 定义上级访问角色权限规则, 如表 4 所示. 在本地鉴权模式下, 验证无约束条件和有约束条件下用户操作资源鉴权情况; 在跨域鉴权模式下, 验证上级访问下级时文件资源鉴权情况.

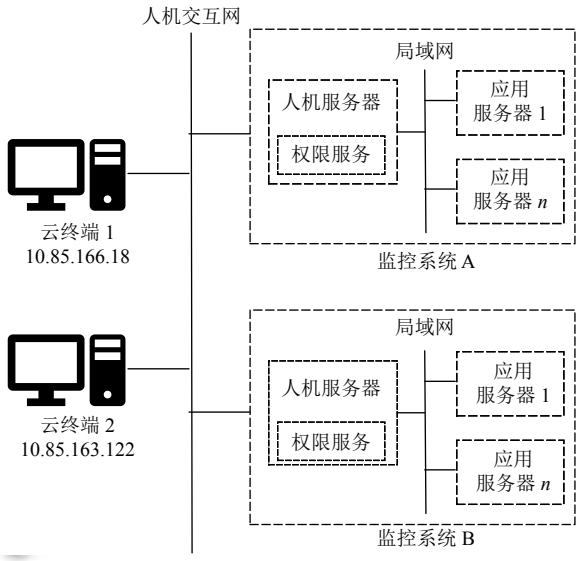

图 8 权限管理验证环境示意图

表 2 监控系统 A 约束配置示例

规则名	约束条件规则	约束效力是否生效
时间1	10:00～12:00	是
位置1	10.85.166.*	是

表 3 监控系统 A 用户权限配置示例

用户	资源URL	权限效力
hd1	-:-:RESTYPE_OP:MODEL_MODIFY	允许
hd2	-:-:RESTYPE_OP:MODEL_MODIFY	禁止
hd3	-:-:RESTYPE_OP:MODEL_MODIFY 时间1 位置1	允许

表 4 监控系统 B 角色权限配置示例

角色	资源URL	约束效力
上级访问	-:-:RESTYPE_FILE:fileA.g	可读
	-:-:RESTYPE_FILE:fileB.g	禁读

4.3 验证结果

根据上述权限配置情况, 验证 (1) 本地验证无约束条件下用户操作资源鉴权情况; (2) 本地验证有约束条件下用户操作资源鉴权情况; (3) 跨域验证上级访问下级文件资源鉴权情况.

(1) 通过用户 hd1 访问监控系统 A 验证本地无约束条件下用户操作资源鉴权情况, 鉴权结果见表 5, 验证结果符合预期.

(2) 通过用户 hd3 访问监控系统 A, 验证本地有约束条件下用户操作资源鉴权情况, 鉴权结果见表 6, 验证结果符合预期.

表 5 验证内容 (1) 的结论

用户	环境情况	被访系统	资源简称	权限效力	鉴权结果	结论
hd1	终端1全天 终端2全天	A	MODEL_ MODIFY	允许	通过	正确
hd2	终端1全天 终端2全天	A	MODEL_ MODIFY	允许	不通过	正确

表 6 验证内容 (2) 的结论

用户	环境情况	被访系统	资源简称	权限效力	鉴权结果	结论
hd3	终端1时间1内 终端2时间1内	A	MODEL_ MODIFY	允许	通过 不通过	正确
	终端1时间1外 终端2时间1外	A	MODEL_ MODIFY	允许	不通过	正确

(3) 通过用户 hd1 访问监控系统 B 验证上级访问下级的跨域文件资源鉴权情况, 鉴权结果见表 7, 验证结果符合预期.

表 7 验证内容 (3) 的结论

用户	环境情况	被访系统	资源简称	权限效力	鉴权结果	结论
hd1	终端1全天 终端2全天	B	fileA.g	允许	通过	正确
	终端1全天 终端2全天	B	FileB.g	允许	不通过	正确

4.4 应用情况

目前新一代调控系统已陆续在华东、西北、江苏、上海等调控中心建设示范工程并进行试运行. 权限管理作为新一代调控系统重要公共服务组件之一, 为图形、云桌面、应用商店等业务应用提供了业务安全访问控制, 满足业务多维度、细粒度的权限控制需求. 在图形应用中, 通过权限管理实现了不同用户对图形文件、图形操作的受控访问; 在云桌面应用中, 通过权限管理实现了不同用户可登录系统的受控访问; 在应用商店中, 通过权限管理实现了不同用户在应用全生命周期管理流程中不同操作的受控访问.

5 结语

本文在分析新一代调控系统业务场景的权限管理需求基础上, 提出了面向新一代调控系统业场景的权限管理方案以及相关关键技术. 基于路径的全局受控资源标识定义方法, 解决了受控资源全局描述问题; 基于元数据的受控资源管理方法, 解决了受控资源的动态扩展问题; 基于规则引擎的多因素约束访问控制方法, 解决了多维度权限约束问题; 基于上下级关系的跨域访问控制方法, 解决了跨域访问控制问题. 实验验证及应用情况表明, 相关技术满足新一代调控系统业务场景的权限管理需求, 为新一代调控系统安全运行奠定了基础. 后续随着业务发展的需要, 将继续对业务场景访问控制需求进行分析和功能研发.

参考文献

1 许洪强, 姚建国. “大电网智能调度与安全预警”特约主编寄语. 电力系统自动化, 2019, 43(22): 1–2. [doi: 10.7500/AEPS20190928006]

2 姚建国, 杨胜春, 单茂华. 面向未来互联电网的调度技术支持系统架构思考. 电力系统自动化, 2013, 37(21): 52–59. [doi: 10.7500/AEPS20130714014]

3 许洪强, 姚建国, 於益军, 等. 支撑一体化大电网的调度控制系统架构及关键技术. 电力系统自动化, 2018, 42(6): 1–8. [doi: 10.7500/AEPS20170617001]

4 黄昆, 赵昆, 杨立波, 等. 电网调控系统轻量化人机交互体系架构及关键技术. 电力系统自动化, 2019, 43(7): 159–165. [doi: 10.7500/AEPS20180525001]

5 许洪强, 姚建国, 南贵林, 等. 未来电网调度控制系统应用功能的新特征. 电力系统自动化, 2018, 42(1): 1–7. [doi: 10.7500/AEPS20170518001]

6 王平, 汪定, 黄欣沂. 口令安全研究进展. 计算机研究与发展, 2016, 53(10): 2173–2188. [doi: 10.7544/issn1000-1239.2016.20160483]

7 毛俊杰, 刘鹏, 李昌锋. 基于人脸识别和生物特征的学生身份安全认证系统. 电子设计工程, 2020, 28(12): 30–34.

8 王于丁, 杨家海, 徐聪, 等. 云计算访问控制技术研究综述. 软件学报, 2015, 26(5): 1129–1150.

9 冯朝胜, 秦志光, 袁丁, 等. 云计算环境下访问控制关键技术. 电子学报, 2015, 43(2): 312–319. [doi: 10.3969/j.issn.0372-2112.2015.02.017]

10 高昆仑, 辛耀中, 李钊, 等. 智能电网调度控制系统安全防护技术及发展. 电力系统自动化, 2015, 39(1): 48–52. [doi: 10.7500/AEPS20141014013]

11 王栋, 陈传鹏, 颜佳, 等. 新一代电力信息网络安全架构的思考. 电力系统自动化, 2016, 40(2): 6–11. [doi: 10.7500/AEPS20150117004]

12 苏盛, 李田. 电力信息物理系统网络安全防护中的底线思维. 电力系统自动化, 2017, 41(22): 162–167. [doi: 10.7500/AEPS20170806003]

13 李志强, 苏盛, 曾祥君, 等. 基于虚构诱骗陷阱的电力调度系统针对性攻击主动安全防护. 电力系统自动化, 2016, 40(17): 106–112. [doi: 10.7500/AEPS20160109005]

14 辛耀中, 石俊杰, 周京阳, 等. 智能电网调度控制系统现状与技术展望. 电力系统自动化, 2015, 39(1): 2–8. [doi: 10.7500/AEPS20141008024]

15 许洪强, 赵林, 景沈艳, 等. 面向大电网的人机云终端设计. 电力系统自动化, 2019, 43(22): 130–136. [doi: 10.7500/AEPS20180822003]