一种增强型 RBAC 智慧电厂动态控制权限方法研究及应用

韩晨辉 王涛 杜金刚 王毅 赵轩

西安热工研究院有限公司，陕西西安 710054

摘要：随着全球能源需求的增长和可再生能源技术的发展，智慧电厂作为电力系统的重要组成部分，其信息安全和权限管理尤为重要。传统 RBAC 模型在处理智慧电厂动态变化环境时存在局限，因此需要一种能够可动态配置的权限管理机制。本文研究了一种增强型 RBAC 方法，将权限控制中涉及到的数据逻辑控制与业务代码进行解耦，在系统运行期间进行数据逻辑的动态创建及修改，以适应智慧电厂中的动态权限管理需求，并通过实际智慧电厂场景应用，验证了模型的有效性和可行性。

关键词：RBAC，智慧电厂，动态权限配置

作者简介：韩晨辉（1999-），男，汉族，陕西咸阳，硕士研究生，助理工程师，能源电力信息化，西安热工研究院有限公司

1 绪论

随着全球能源需求的持续增长和可再生能源技术的快速发展，电力行业正迎来一场深刻的数字化和智能化转型[1]。智慧电厂[2]作为未来电力系统的重要组成部分，以其在能源管理、设备监控和运营优化等方面的显著优势，逐步成为行业发展的新趋势。在构建智慧电厂的过程中，信息安全和权限管理问题尤为重要[3]，为了确保电厂系统的安全、可靠和高效运行，迫切需要一种灵活且高效的权限控制方法。

基于角色的访问控制（Role-Based Access Control，RBAC）[4]作为一种广泛应用的权限管理方法，通过将用户与其角色相关联，并根据角色分配权限，简化了权限管理的复杂性。然而，传统的 RBAC 模型在应对智慧电厂中日益复杂和动态变化的环境时，显得力不从心[5]。例如，在电厂的实际运营中，人员的班组信息以及用户的具体任务需求可能会频繁变化。这些动态因素要求权限管理系统能够迅速调整用户权限，以适应实时的业务需求[6]。因此，需要一种增强型的 RBAC 模型来适应智慧电厂中的动态权限控制要求，以确保系统的安全性和灵活性。

本研究旨在提出一种增强型 RBAC 方法，以适应智慧电厂中的动态控制权限管理。具体来说，本研究将涵盖以下几个方面：

（1）分析传统 RBAC 模型的局限性：探讨传统 RBAC 模型在智慧电厂应用中的不足之处，特别是在处理动态变化时的限制。

（2）设计增强型 RBAC 模型：在传统 RBAC 模型的基础上，融入动态表达式控制，构建一个更加灵活和适应性的权限管理框架。

（3）验证与应用：构建一套动态权限控制系统。

本论文的结构安排如下：在第二章介绍传统 RBAC 模型的基本概念，介绍一种增强型 RBAC 动态控制权限方法，并介绍核心的表达式解析器。第三章将展示增强型 RBAC 模型在智慧电厂中的具体设计，探讨其实际效果和应用前景。

2 技术框架

2.1 RBAC 模型

在权限设计中，RBAC 权限模型使用角色解决了用户与权限点的关联，对于权限的控制则通过权限编码与相应的业务逻辑进行关联，在此模型中，权限只是一个标记，具体的数据验证逻辑需要在相关的业务代码中进行实现，基于数据逻辑的权限验证与业务代码混合在一起。例如：查询同一个业务功能的数据，根据需求可以按照组织机构字段进行隔离，也可以按照时间范围进行隔离。传统的实现方式将每种具体的数据隔离方式作为一个具体的权限，而数据的隔离则通

过逻辑代码或者数据库 SQL 进行实现，当有新的数据隔离需求或者现有的控制逻辑需要进行变更时，除了增加新的权限以外，还需要对业务代码进行修改、编译以及重新发布，极大增加了系统的开发量以及后期运维的成本。

2.2 一种增强型 RBAC 动态控制权限方法

本研究在传统 RBAC 模型的基础上进行了创新，提供一种全新的权限验证方法，包括操作权限和数据权限的详细定义和管理机制。将权限控制中涉及到的数据逻辑控制与业务代码进行解耦，在不影响程序运行的情况下，实现数据隔离逻辑的动态创建及修改。

操作权限是指用户在系统中能进行的具体操作。每一个操作权限通过权限编码与业务功能进行关联，确保用户只有在具备相应权限的情况下才能进入特定功能模块。

数据权限用于控制用户在执行操作时可以访问和操作的数据范围。通过数据表达式来定义，这些表达式可以包含常见的逻辑运算符和自定义函数，从而实现对数据的精确控制。数据表达式可以包含如“>”、“<”、“==”、“!=”等逻辑操作符，以及自定义的函数。表达式在系统运行时通过解析器动态解释和执行。为了便于权限的管理和灵活性，数据权限还支持将数据按照特定的规则进行分组。用户可以通过配置界面定义数据分组，并在数据权限表达式中引用这些分组。

用户同时具备多个数据权限时，这些权限之间可能存在包含关系，支持优先级机制，优先级高的数据权限会覆盖或简化优先级低的数据权限，确保权限验证的效率和准确性。

权限模型通过角色将用户与权限关联起来。用户与角色、角色与权限之间是多对多的关系。系统在设置权限时，先为角色分配操作权限，然后在权限的基础上进一步设置表达式，通过表达式解析器动态解析表达式，完成动态权限分配的过程。

2.3 表达式解析器

本节实现了一个高度灵活且功能丰富的表达式解析器，专为处理复杂逻辑与数据操作而设计，尤其适用于需要在 Java 应用中动态解析和执行条件表达式、数学运算乃至生成 SQL 片段的场景。该解析器的核心能力在于其能够解析包含变量引用、算术运算、逻辑比较、自定义函数调用以及特定 SQL 操作符的复合表达式，并根据输入参数准确计算结果或构造 SQL 指令。如图 1 所述为表达式解析器流程图，用户登陆后查询用户所属权限编码和对应表达式，系统通过词法分析和语法分析解析表达式，并通过计算逻辑和 SQL 生成，得到最终的权限隔离结果，达到控制权限的目的。

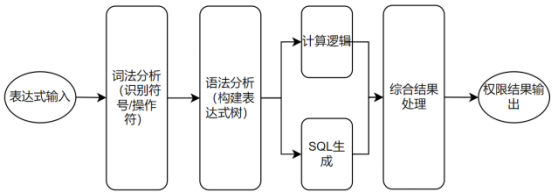

图 1 表达式解析器流程图

表达式用来定义用户在执行某个操作时的数据访问规则。例如，用户只能查看他自己录入的数据，表达式可以定义为，系统支持使用常见的逻辑操作符以及扩展函数来构建复杂的权限逻辑。

系统初始化阶段，通过 installOperators() 方法注册了一组预定义的运算符，涵盖基础的算术、比较、逻辑运算符及括号，允许用户根据需求扩展更多自定义运算符。为解析器提供了强大的表达式处理能力。

解析器的主要接口 eval() 和 getBooleanResult() 分别用于计算表达式的值和直接获取布尔结果，initSQL() 方法将表达式转换为 SQL 片段，用于动态构建查询语句，同时支持参数化查询。

表达式解析器的解析过程主要分为两部分：直接计算逻辑的 parse() 和面向 SQL 生成的 parse2Sql()。两者均采用了栈结构辅助解析，通过识别字符序列来分隔操作数与运算符，递归下降的方式遍历并构建表达式树，以此来处理运算符优先级与括号匹配问题。对于字符串、数字、布尔值等基本类型，解析器能准确识别并转换，同时支持变量值从外部映射中查找，增强了表达式的动态性。解析器通过 getFunctionResult() 方法执行用户定义的函数逻辑，扩展表达式的灵活性和实用性。

综上所述，表达式解析器是一个综合性的解决方案，实现高效解析和计算复杂表达式，适应动态 SQL 生成等特定需求，其在数据处理、业务逻辑动态配置

等领域具有应用价值。

3 系统设计

本文所述增强型 RBAC 智慧电厂动态控制权限方法，基于西安热工研究院自主知识产权的后端低代码平台 TPRI-DMP 作为技术实现，验证了此方法的可行性，本节以 TPRI-DMP 平台为实现依据，描述此方法的具体设计路径。

实现此套动态控制权限方法，需构建用户模块，角色模块，权限模块等。

用户维护模块主要负责用户信息的管理，包括用户的添加、修改、删除和查询功能。此外，用户维护模块还提供用户角色的分配和撤销操作，确保每个用户都能被正确地赋予相应的角色和权限。

角色维护模块负责管理系统中的角色信息。管理员可以通过该模块定义新的角色、修改现有角色的权限组合、删除不再需要的角色。同时，该模块还提供查询功能，能够显示某个特定角色下包含的所有用户信息，方便管理员进行角色管理和调整。

权限维护模块是整个系统的核心部分，负责定义和管理系统中的操作权限和数据权限。操作权限描述用户在系统中可以进行的具体操作，例如查询、修改、删除和审核等；数据权限则描述用户在执行这些操作时可以访问或操作的数据范围。定义权限时，根据表达式动态配置此权限编码对应权限，后端通过表达式引擎对其进行重新解析及预编译处理，从而实现数据逻辑控制的动态修改及扩展。权限维护模块通过灵活的配置和管理，实现了权限定义和业务逻辑的解耦，使系统具有较高的扩展性和灵活性。如图 2 所述，定义权限编码时，可灵活定义或修改多个表达式，通过权限编码将角色和表达式进行多对多关联，通过表达式解析器解析后，赋予角色相应权限，进而使对应人员具有相应权限。

图 2 权限配置界面

4 总结

本文提出的增强型 RBAC 方法有效解决了智慧电厂中动态权限控制的问题。通过分析传统 RBAC 模型的局限性，设计了一种新的权限模型，该模型包括了操作权限和数据权限的详细定义，通过角色将用户与权限关联，利用表达式解析器实现了权限的动态精确控制。设计数据库支持电厂系统的动态权限需求，用户登录权限设计采用了多因子身份验证，增强了安全性。该方法能够提高权限管理的效率和响应动态变化的能力，确保了系统的安全性和灵活性。

参考文献

[1] 王树东．保障国家能源安全推进绿色低碳转型高质量助力中国式现代化建设[N]．中国电力报，2024-06-27(001)．

[2] 王涛，单正涛，杜金刚，等．智能电厂生产管理开发平台研发[J]．热力发电，2019,48(09):115-119.DOI:10.19666/j.rlfd.201906129.

[3] 赵晋松，张朝阳，顾巍峰，等．基于工业互联网的智能电厂平台架构[J]．热力发电，2019,48(09):101-107.DOI:10.19666/j.rlfd.201906114.

[4] 余杨奎．基于角色的访问控制模型（RBAC）研究[J]．计算机技术与发展，2019,29(01):198-201.

[5] 孙恒一．一种扩展型 RBAC 电力交易系统权限模型设计与实现[J]．网络安全技术与应用，2018,(03):42-43.

[6] 胡文瑜，陈金波．面向访问过程的动态访问控制模型研究[J]．计算机技术与发展，2022,32(04):92-96+108.

作者简介：

韩晨辉（1999-），男，陕西咸阳，硕士研究生，助理工程师，能源电力信息化。