基于数据信息技术的电力安全系统设计与实现

刘飞

（国网监利市供电公司　湖北省荆州市　433300）

摘要：随着现代化技术发展，电力能源应用日益广泛。为了实现电力安全、稳定供应需求，构建电力安全系统成为一项重要任务。传统模式下，我国电力行业多数企业采取中心化存储方式实现电力数据管理和数据共享，但随着电力系统迅速发展，该系统弊端日益明显。基于此，文章围绕现代研究成果，以区块链技术为基础，提出一种新的电力安全系统设计思路，借助区块链技术优势，提升电力数据存储安全性、电力数据访问效率。

关键词：数据信息技术；电力安全系统；设计思路；功能实现

引言：随着社会的不断发展，电力系统作为基础设施的一部分，对安全性的要求变得日益重要。传统的电力系统监测手段往往依赖于有限的传感器和人工操作，存在监测盲区和响应滞后的问题。为了提高电力系统的安全性，我们引入先进的数据信息技术，构建了一套全面的电力安全系统。提出的系统设计方案，以区块链技术为核心，发挥大数据分析等优势，实现对电力数据的深度挖掘、智能分析和安全存储，以及构建更为安全灵活的电力数据访问权限体系。通过本文的分析，对解决传统电力数据信息面临威胁有积极作用，可以进一步促进电力数据实现安全共享。

1 研究概述

1.1 研究背景

电力安全系统构建的主要目的是保证电力系统安全稳定运行，各设备得到高效监控，电力数据信息得到智能化管理和分析，有效识别故障信息，降低安全风险。该系统运行过程中，电力数据信息发挥重要支撑作用，因此，如何科学采集数据、智能处理数据、高效利用数据是关注重点。

区块链技术是一种分布式数据库技术，它以块的形式存储数据，并使用加密技术确保数据的安全性和透明性。其具备去中心化、支持智能合约、具备良好透明性和可追溯性等优势。区块链技术应用中，数据存储以区块为基本单位，每一个区块包含一定量的信息数据以及前一个区块的哈希值，最终各区块以链式结构为基础进行连接。除此之外，区块链技术依托密码学技术，可以显著提升数据机密性和完整性，并为信息安全性提供保障。但需要注意，由于特殊的“链式”结构，一旦受到攻击或者有人恶意篡改数据，会导致整个“链条”均受到影响。

基于区块链技术的优势和特殊结构特点，文章以该技术为基础，提出一种基于数据信息技术的电力安全系统设计方案，旨在为电力信息数据提供更为全面的保障。

1.2 系统设计概述

该方案主要从以下两个大方向进行思考，第一，提升电力数据安全存储性能；第二，强化电力数据访问权限。结合上述两大方向来看，数据安全存储方面侧重营造良好的存储环境。电力数据一般具备繁多、复杂特点，很多文件占据较大的存储空间，针对这一特点，结合区块链的区块存储特点，借助云存储平台对传统数据存储分布方式进行改造，以脱链存储方式提升数据处理效率和提升存储安全性。同时，为了降低数据泄密风险和恶意篡改风险，在方案中融入加密算法，对数据进行进一步加密处理。一般在上传云存储平台之前，先对数据进行加密，从而避免网络环境复杂，带来安全威胁。从数据访问权限和数据共享角度来看，借助区块链技术，可以借助存储地址差异和信息数据资源实现数据共享。但需要注意，为了保证信息安全，关于区块链的节点信息，一般以密文形式存在，或者只允许查看存储地址，如果想要深入访问或者想要查看具体某地址存储的电力数据信息，需要由管理人员向技术部门赋予访问权限，然后再由技术人员后台登录，才可以实现数据共享，另外，技术人员可以依据实际需求，在获得权限后向特定人员发起共享请求。通过严密的管控和访问权限设置，限定电力数据接触人员范围，可以有效保证数据信息安全[1]。

2 设计要点

基于上文对整体设计方案的阐述，文章提出的电力安全系统设计方案需要关注以下三方面内容。

2.1 数据储存

传统的数据存储方式由于技术局限性，在安全性方面面临挑战。尤其随着电力系统持续化发展，智能化技术应用日益广泛，产生的电力数据更为复杂、繁多，如果仍采用传统方式势必增大内部数据被篡改、遗失等风险。针对这一现象，文章从现代化技术研究成果角度入手，参照前人研究建议，应用云存储平台，规避数据安全风险。

应用云存储平台实现数据存储需求，具备以下几方面优势：第一，支持分布式存储。基于技术原理可以通过合理规划电力数据信息文件，将其分配到不同网络节点，这可以有效削弱数据安全风险。第二，有效预防篡改。电力信息数据中包含一部分极为重要且需要保密的信息，且这部分数据也较为庞大，因此在构建保密体系方面也面临挑战，借助云存储平台可以通过对存储地质进行对比，从而验证数据是否被篡改，这在降低恶意篡改威胁发生概率时有重要作用。第三，云存储平台可以通过智能化识别冗余数据、删除重复数据等缩短存储空间。

通过对云存储平台优势的阐述可知，合理应用云存储平台对提升数据存储安全性极为有利。具体来看，其应用流程如下：第一，发挥加密算法优势对数据进行加密处理，然后上传到云存储平台；第二，云存储平台对收到的数据进行统一化处理；第三，经过再加工的数据模块被科学分配到云存储平台不同节点存储；第四，所有数据存储完成后，云平台将经过加密的数据存储地址再提交给操作人员，便于其后续查阅、下载或者检索。

2.2 数据共享

现阶段，智慧电网建设过程中，数据共享是不可忽略的环节。一般情况下，采用可信共享模式实现目的，此种方法可以解决传统共享中流程复杂、效率低下问题。区块链技术的应用可以降低信息泄露风险[2]。

2.3 访问控制

数据共享过程中，如何提升数据安全性是重点。而访问控制权限设置是在保障安全性前提下，实现数据共享的可行方法。也就是通过访问权限设置，限制数据访问人员范围，只有获得授权的人员才能在平台中读取信息或者下载数据。

此种方式充分发挥优势的前提是制定科学的访问策略，策略具备针对性，对于获得权限的人员可以访问加密数据，如果没有得到权限，则只能读取普通数据、公开数据。

3 系统设计和功能实现

3.1 基于区块链的电力数据共享系统架构分析

围绕上文分析，文章提出如下图 1 所示的电力数据共享系统架构方案。该系统主要分为四大层级，分别是网络协议层、智能信息管理层、业务功能层和数据表现层。各层级具备不同功能，通过协同配合，为电力数据共享提供支撑。

结合图 1 来看，其中网络协议层主要包括分布式账本和共识机制等三大内容，主要作用是保证数据和数据库信息同步，并负责维护分布式账本，促使其发挥效用。进而保证云存储平台可以实现数据安全存储。与网络协议层相关联的数据库包括两种类型，其中 INFORMIX 数据库主要发挥数据查询，但需要注意该数据库支持简单查询，对于复杂的数据筛选任务无能为力；Redis 数据库适宜进行高级查询，实现两类数据库协同运行，可以最大限度实现电力数据安全传输、应用等功能[3]。智能信息管理层主要作用是对分布式账本进行读取和下载，这也是数据共享的前提。为了保证功能充分实现，按照系统管理和用户管理细化为两大模块，其中系统管理是通过区块链技术降低节点之间的通信成本，用户管理则为业务功能实现提供支持。业务功能层架构目的是支持系统后端服务功能实现。其包含用户信息注册、用户角色更改和用户信息注销等模块，可以后台对信息进行修正。数据表现层为用户提供区块链网络交互网页界面，该系统设计过程中，采用 SSM 框架为基础，借助 AI 技术等优势，确保各系统功能借助网络协议层支持，可以实现功能交互和信息流畅共享，例如数据表现层和数据业务层依靠 TCP 接口实现连接。

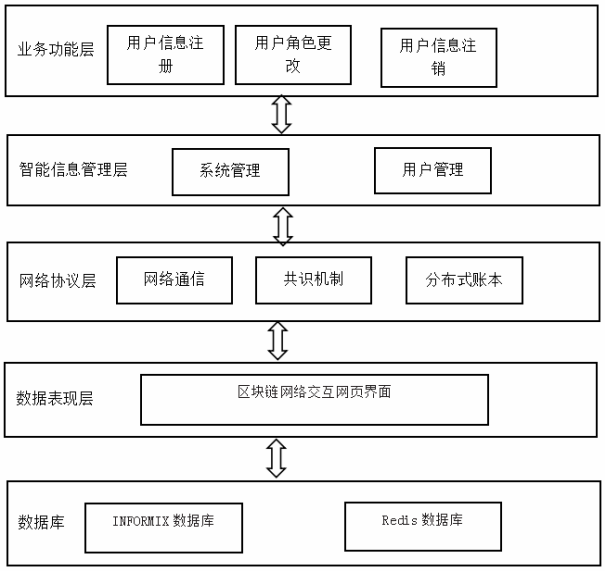

图 1 数据共享系统架构图示

3.2 功能实现

结合上文提出的系统架构，为了实现数据共享，以区块链技术为基础，借助开发链码和中间件云存储平台 SDK 两部分达成目标。其中开发链码区块链技术中的一项关键任务。链码是在区块链网络上运行的智能合约，它定义了网络中的业务逻辑[4]。

云存储平台的软件开发工具包（SDK）是开发者用来与特定云存储服务进行交互的一组工具和库。这些 SDK 简化了与云存储服务的通信，提供了易于使用的接口，以便在应用程序中轻松集成云存储功能。文章提出的方案中，应用 SDK 功能的主要目的是当系统应用程序

接收发出的命令后，可以调用开发链码进行区卢埃连划分，从而为分布式账本之间信息交互奠定基础。

基于文章提出的方案设计思路，文章选择以包括 C# 语言、JAVA、Python 语言等在内的编程语言，促使系统程序实现运行。

4 系统测试

4.1 测试环境营造

为了验证基于数据信息技术的电力安全系统设计方案能否满足需求以及功能能否充分实现，在此按照表 1 所示参数，设置系统环境。

表 1　系统环境配置参数总结表

环境组成部分	具体项	参数
系统主要开发工具	Docker 18.09.5	18.09.5
	Docker Compose	1.27.3
	Golang	1.14.6
	Fabric	2.3
虚拟机	CPU	4 核
硬件部分	内存	8G
	硬盘	30g

文章提出的系统设计思路，以区块链技术为基础，需要在 Linux 系统下才能正常运行，因此，测试环境在 Linux 平台基础上营造。

4.2 区块链网络搭建

该系统主要服务对象为电力系统数据技术人员和数据管理人员两类，因此，在营造测试环境中，需要基于实际应用需求，按照数据技术人员和数据管理人员两类特点，构建区块链网络系统，也就是保证搭建的系统可以容量两种不同类型网络发挥效用。同时需要保证两个网络系统之间存在流畅通信渠道，便于技术人员和管理人员实现交流。

4.3 功能测试

测试过程中，功能测试包括三大项内容：第一，验证用户管理模块各功能可以正常发挥运转，如用户注册、注销等功能均可以按照预期发挥作用；第二，验证管理人员登录系统后，系统界面可以自动对信息进行验证；第三，设置访问权限，为所有数据管理人员授予注册账户和秘密，将权限开放范围设定在所有管理人员，角色定位分配为数据所有者。测试过程中，预设用户账号为 admin，用户密码为 passwor123，然后验证其访问权限是否按照预设发挥作用[5]。

4.4 数据共享测试

数据共享是不可忽略的内容之一，其可以细化为电力数据资源分布、数据资源检索、数据共享和共享复审四大模块。在此对上述四大模块功能实现情况进行测试。

（1）数据资源分布。将电力系统所有电力资源数据实现统一管理，且登录者的信息系统均用于数据资源发布，并将测试的数据资源溯源码、数据名称、存储地址等进行设置，然后对其数据发布功能、信息更改功能等进行测试[6]。

（2）数据资源检索。在对应的数据资源模块中输入关键词，从而验证该系统的数据资源检索功能效果。

（3）数据共享。主要验证数据能否在技术人员和管理人员之间实现智能共享。

（4）共享复审。为了保证数据安全性，设置共享复审环节。在测试过程中，模拟数据管理人员登录电力系统，并向技术部门提交共享复审申请。此时验证该环节的应用性能[7]。

4.5 测试结果概述

经过系统化测试，设计的系统各功能可以按照预期发挥效用，以用户管理模块为例，结果表明，各项功能均可以按照预期发挥效用。对数据共享性能进行测试，结果表明，可以按照预期达成目标。综上可知，文章提出的设计思路具有实用价值。

结语

综上所述，由于传统电力数据信息存在被恶意篡改、泄密等风险，为了有效缓解上述问题，文章以电力数据为基础，引用区块链技术，设计了基于数据信息技术的电力安全系统，该系统以云存储平台为基础架构，在其上构建电力数据安全共享系统，并通过测试，验证功能实用性。最终结果证明，该设计思路可以进一步保证电力数据安全。

参考文献：

[1]肖靖,曾锦松,许佳庆,等.基于云边端协同技术的电力安全管控系统设计[J].供用电,2023,40(5):44-52.

[2]张明.基于“互联网+”的电力安全事故管理系统设计[J].信息与电脑(理论版),2023,35(5):50-53.

[3]黄杰韬,王泽涌.数据实时分析的电力安全生产监测系统设计[J].能源与环保,2022,44(12):256-261.

[4]常帅.电力安全生产管理信息系统设计分析[J].中国新通信,2022,24(18):122-124.

[5]赵子源,邢宏伟.基于大数据的电力监控系统网络安全监测系统设计[J].能源与环保,2022,44(1):242-247+255.

[6]常政威,彭倩,张泰,等.电力作业现场可穿戴安全保障系统设计与实现[J].四川电力技术,2020,43(3):43-47.

[7]邓成俊,谭世海,汪超.基于 3D 虚拟仿真技术的电力安全实验培训系统设计与实现[J].实验室研究与探索,2019,38(8):114-118.