文章编号:1671-4598(2017)10-0240-04 DOI:10.16526/j.cnki.11—4762/tp.2017.10.061 中图分类号:TP273 文献标识码:A

基于云存储的电力系统访问控制方案设计

陈 胜[1],刘晓放[1],张承模[2],王家军[3]
(1.贵州电网有限责任公司 电力调度控制中心,贵阳 550002;2.贵州电网有限责任公司 贵阳供电局,贵阳 550002;
3.贵州电网有限责任公司 兴义供电局,贵州 兴义 562400)

摘要:电力系统是一个由多个子系统构成的综合性系统,作为一个能够实现海量数据处理同时具有高实时性、高可靠性的管理控制平台,需要电力系统能够实现对所辖多个子系统进行复杂、细密、大范围的访问控制,这些条件要求能够设计出合理有效的访问控制模型;为了实现安全、可靠、高效的电力系统访问控制提出了将传统电力系统同云存储平台相结合的访问控制方案,通过云存储平台对数据进行存取可以达到大数据量、均衡负载、安全可靠的目的;通过添加可信度因子构建访问控制模型,根据不同用户的可行度计算值分配给以不同的权限,匹配其可操作的资源,实现了对于用户操作对象的细化识别。

关键词:云存储;电力系统;可信度;访问控制

Design of Access Control Scheme for Electric System Based on Cloud Storage

Chen Sheng[1], Liu Xiaofang[1], Zhang Chengmo[2], Wang Jiajun[3]
(1. Power Dispatching and Control Center, Guizhou Power Grid Co., Ltd, Guiyang 550002, China;
2. Guiyang Power Supply Bureau, Guizhou Power Grid Co., Ltd., Guiyang 556000, China
3. XingYi Power Supply Bureau, Guizhou Power Grid Co., Ltd., Xingyi 562400, China)

Abstract: Electric system is a comprehensive system which is composed of several subsystems, as to achieve a massive data processing control platform which has high real-time, high reliability, power system can realize complex, dense, large range of access control under the jurisdiction of a number of subsystems, these requirements can be designed a reasonable and effective access control model. In order to put forward the traditional access control power system with cloud storage platform combining access control scheme of power system security, reliability and efficiency, through the cloud storage platform for access to data can reach a large amount of data, load balancing, safe and reliable; through adding credibility factors to construct the access control model, according to the feasible degree the calculation of different users value assigned to a different authority, its operational resources, to achieve a detailed user operation object recognition.

Keywords: cloud storage; electric system; reliability; access control

0 引言

随着经济社会的高速发展,电网已经成为了国家能源产业链条上的一个重要环节,更是一个国家国力的重要体现。各行各业的生产运营都高度依赖电力的可靠供应,是否能够提高电网系统的供电可靠性以及供电质量显得至关重要。经过电力工作者们的不断研究探索,智能电网概念应运而生,其所具有的高效、安全、可靠、交互性强等特征为电网的发展指明了未来的方向。智能电网所具有的更强的信息流和业务流的融合能力大大提升了电网的坚强性同时具有更好的信息共享性与交互性。而能否构建一个有效可靠的智能电网的重要基础就是信息平台的搭建。

云存储和云计算作为一个全面的IT解决方案,以提供服务的方式为用户提供强大的存储和计算能力[1-3]。云存储技术在云计算的基础上,采用网络技术、文件分布式技术、集群技术、访问控制相结合的方法将数目庞大的下层存储设备进行集成,为上层提供透明可靠的数据存储服务。其可以解决海量数据的存储和维护问题,能够为系统提供实时、可靠、安全的数据存储服务[4]。为了提高电力系统的访问效率与容量,提出了基于云存储的电力系统访问控制方案。首先构建一个基于云存储的智能配电运营系统,提供了安全、可靠、高效、大容量的电力控制平台;随后引入可信度因子对每一个访问用户进行可行度计算,以确定其所拥有的权限,匹配相应资源。

本文的结构安排如下,首先介绍了云存储的结构模型,构建了基于云存储的智能配电运营系统,随后提出了可信度因子,通过计算不同用户可信度进行访问控制,紧接着提出了基于云存储的电力系统访问控制方案设计。最后通过实验进行了验证与分析并给出结论。

1 云存储的结构模型

1.1 云存储基础构型

与经典的存储系统模型所不同,云存储技术是将存储数据与访问业务服务都基于虚拟的应用软件实现。一个标准的云存储系统的结构框架自上而下可以简化为:访问层、应用接口层、基础管理层和存储层。其基本的体系结构如图1所示[5-8]。

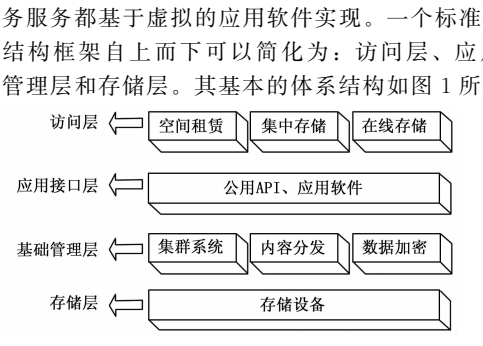

图1 云存储系统结构模型

其每一层都拥有不同的功能,在整个系统中分配着不同的作用:

收稿日期:2017-04-17; **修回日期**:2017-05-03。

作者简介:陈 胜(1986-),男,贵州贵阳人,硕士,工程师,主要从事电力系统调度自动化方向的研究。

1）访问层。该层给所有访问用户进行授权以登录云存储系统，并使用相应的云存储服务。

2）应用接口层。应用接口层是整个系统中适应性最强的部分，可以根据各类不同的具体业务需求进行应用接口开发，针对性地提供专业性的服务。

3）基础管理层。这一层是云存储系统中最为核心的部分，其技术实现也最为难办。这一层综合使用多种技术协调云端的各类不同设备之间的同步操作，使得 各类设备能够根据外部需求提供一致的对外服务。

4）存储层。作为云存储系统的根基，存储层是由各类具体的存储于通信设备所组成的，为了实现该层的基础功能需要搭建大量的计算机进行集群化计算实现虚拟管理。其中包含的大量存储设备是分散的，并不是传统模式的集中式，它们相互之间借助于网络进行连接传输。

1.2　基于 Hadoop 的云存储构型

该文章采用的云存储结构是以 Hadoop 为基础的，这是一个采用 Java 开发语言的分布式文件系统，其对于密集型的分布式应用具有很好的支持。该架构的关键技术是 HDFS，系统的各个节点的文件都存放在 HDFS 上[9-13]。Hadoop 具有很多非常优秀的特点：将需要计算的过程转移到离目标 数据最近的节点，减少了数据传输时间；采用“一次写多次读”模式，提高吞吐量；容错性非常高，即便出错后也能够迅速恢复，提高了存储的可靠性；易于拓展和移植。HDFS 的体系结构如图 2 所示。

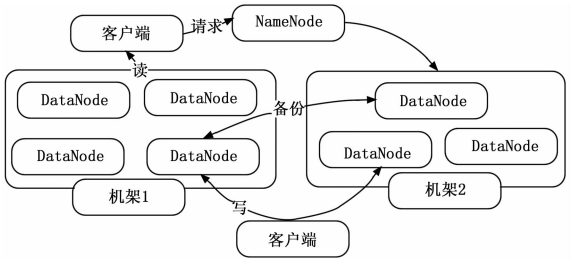

图 2　HDFS 体系结构示意图

2　基于可信度的访问控制模型

2.1　访问控制

访问控制技术是为了能够实现系统的安全可靠，有效地监控每一位用户对于目标资源的访问并授予相应的权限，防止非法用户对于系统资源的窃取与破坏[14]。访问控制由主体、客体以及访问控制策略这 3 个部分组成。主体指的是访问的主动发起者，由他提出访问或者使用目标系统中的特定资源，虽然他发起了访问但是并不是一定执行。客体则是指可以被除自身外其他实体所访问的目标对象，包括所有可悲操作的信息以及资源。访问策略并不是实体的设备，而是规则集合，规定了操作的方式和约束条件。

2.2　可信度访问控制

为了能够动态地控制与调整从用户发起请求到云存储系统进行授权的整个生态周期，该文设计了如图 3 所示的添加可信度的访问控制架构。

在该系统中引入可信度的概念对用户的访问接入进行控制，而可行度可以从两个方面进行度量：首先是基于用户身份和环境信息的可信度，这类似于信任管理中的直接信任概念，

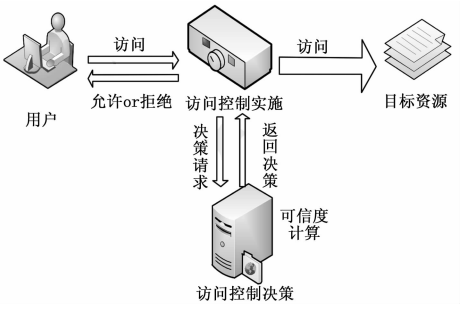

图 3　可信度访问控制框架示意图

将其定义为基本可信度；其次是用户行为的可信度，每次计算可信度时读取云端存储的用户访问历史文件根据不同权值计算其行为的安全性[15-16]。这两种可信度的取值都在［0，1］内，而由他们决定的用户可信度可以根据预设的加权权重计算得到。假定相应的权重为 ω_{AT}，ω_{BT}，其取值都在［0，1］内，且这两者之和为 1，即 $\omega_{AT}+\omega_{BT}=1$，对应的用户的可信度可以如下表示：

$$T(u)=\omega_{AT}AT(u)+\omega_{BT}BT(u) \tag{1}$$

而用户的基本可信度的关键因素与五个方面有关，分别是：静态属性、可信平台、系统、安全设备以及应用软件。假定这 5 个影响因子的权重分别为 $\omega_1,\omega_2,\omega_3,\omega_4,\omega_5$，进一步可以计算得出用户的基本可信度，计算公式如下：

$$AT(u)=\omega_1*t+\omega_2*(m_1\div n_1)+\omega_3*(m_2\div n_2)+\omega_4*(m_3\div n_3)+\omega_5*(m_4\div n_4)(4-2) \tag{2}$$

其中：n_1,n_2,n_3,n_4 分别表示平台、系统、安全控制设备以及应用的操作数数目，而 m_1,m_2,m_3,m_4 则分别表示这其中的可信操作数目，而静态可信度 t 由系统特性决定。

另一方面通过云存储系统记录并保存用户的访问行为，监控用户完成任务的情况。用户的访问行为与任务处理结果可以分为正面与负面两种情况，为了更加突出负面结果给系统造成的影响更大，在设计计算可信度时将正面结果的敏感值预定为 $v_i=1$，而另一方面将负面结果的敏感值预定为 $v_i=-2$，以体现出可信度的慢增骤降特性。由此，行为的可信度计算可以表示为：

$$BT(u)=\sum v_i\div\sum|v_i|(4-3) \tag{3}$$

3　基于云存储的电力系统访问控制方案

电力系统中的用户角色可以分成系统管理人员、智能微网、用电用户，当某一个用户想对系统存储于云端的资源发起访问时首先通过云存储端的可信度计算过程，通过计算得出的可信度与预设的阈值进行对比，根据相应的可信度分配以相应的操作权限。通过大量测试对比，可以假定系统管理人员的可信度阈值为 0.8，智能微网的可信度阈值为 0.7，而用电用户阈值设置为 0.6。

整个系统的访问控制方法如下：

1）合法用户 Alice 的访问控制：用户 Alice 进行登录系统操作，提出某一项具体的操作请求，具体步骤设计如下：

（1）控制系统对用户的身份进行确认，同时从云端搜集该用户存储于云端的操作记录日志，如果目标身份认证通过则进行下一步操作，否则拒绝用户登录系统；

（2）根据系统从云端搜集的用户操作记录，依次分类出属于平台、系统、安全设备以及应用程序的操作数目，将该次计

算操作转移到目标文件处，根据合理预设的权重值，计算出用户的最终可信度值；

（3）根据目标特征属性匹配其所属的用户组，确定其可使用的相关操作；

（4）在系统数据库中查询用户角色与所计算的可信度值，决定用户组操作；

（5）根据用户所属用户组与用户所请求的操作进行对比，以确定该用户是否可以进行相应操作；

（6）查询云端数据库，确定用户对于该操作所拥有的权限；

（7）确认操作合理后，进行操作，否则拒绝，并将该次操作记录的历史文件存储于云系统中。

2）非法用户 Bob 的访问控制：非法用户 Bob 伪装成合法用户登录系统，进行非法访问操作请求。同合法用户一样，首先系统进行身份确认，但是由于其进行了伪装，通过了系统认证，但是下一步计算用户可信度时，由于其存储于云端的操作记录可信操作数低，计算出的最终可信度值大大低于正常用户可信度，达不到其所属用户可信度值，系统根据这一可信度依据拒绝其进入系统，或者进入系统后不能达到高权限的操作。通过这种云端数据记录与对比的方式实现对目标用户的访问控制。

4 实验与分析

4.1 方案验证与分析

由于采用了云存储来实现海量数据的存储以及通过可信度对目标用户的访问进行控制，实验部分分别对系统的大数据存储能力、吞吐量以及是否可有效进行访问控制进行验证分析。

首先搭建一个 Hadoop 集群以充分利用整个电力系统中的闲置资源，该实验使用 8 台计算机采用相同的配置构建了一个完全分布式的 Hadoop 集群。平台一共由 8 个物理节点组成，其中一个作为 Namenode，剩余 7 个作为 Datanode，每一个节点的配置都是 Intel（R）Core（TM）i3CPU，主频 2.27 GHz，内存大小 4 G，使用的网络带宽 100 Mbps。

由于 Linux 是唯一支持 Hadoop 的系统平台，因此实验采用 Linux 作为操作系统，所用 Linux 版本为 Ubuntun12.04，JDK1.6 版本。

在系统配置完成后，首先测试验证了系统对于访问数据的吞吐能力，插入一条大小为 1 KB 的数据，设置不同的数据量，测试其存储速率。结果如图 4 所示。

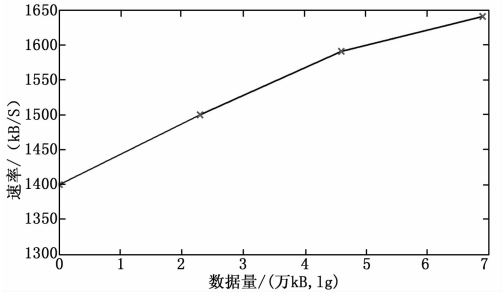

图 4 吞吐速率验证结果

由图 4 可以看出该系统具有很好的数据吞吐能力，同时随着数据量的不断提高其吞吐速率也随着不断增加，体现了云存储方案集群化后的数据处理优势。

由于系统需要从云存储系统中读取用户存储的访问数据进行可信度的计算以对用户的访问行为进行控制，另一方面测试系统对于数据的读取速率。结果如下图 5 所示。

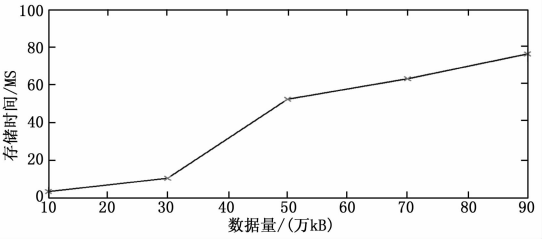

图 5 存储速率验证结果图

由图 5 可以看出该系统对于数据的读取具有非常好的支持，其对于数据的读取所花费的时间一直维持在一个较低的水平之下，但是随着数据量的不断增大其数据读取时间也相应增加。

随后我们对于系统是否可以进行用户的访问控制进行仿真验证，首先通过仿真从云端读取出用户的访问数据，通过计算后得出其可信度，反馈给访问控制模块。最终实现的系统会促进可信用户的可信度不断提升，而对于非法用户其每次非法操作都会对其 后续可信度造成影响。在不同身份用户进行访问时其所对应的可信度如图 6 所示。

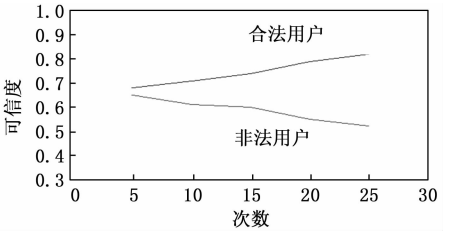

图 6 不同用户访问可信度值

如图 6 所示，在合法的用户访问电力系统时，根据其所计算出的可信度高于非法用户的可信度值，且随着访问次数的增加，其每次的访问记录都会被存储到云端，随后的可信度计算会根据这些操作记录进行判定。可以看出随着操作次数的不断增加，合法用户的可信度不断增加，而相反的对于非法用户其可信度受其非法操作的影响可信度一直下降。结果表明系统有效实现了对于用户访问行为的控制管理目标。

4.2 方案不足

虽然该方案有效实现了对用户访问行为的控制管理并获得了较高的吞吐量与速率，但是依然存在一些欠缺之处：

1）可信度计算依赖于权值的设置，只有设定合理的权值才能保证系统的稳定有效运行，兼容性不强；

2）云存储系统的复杂度高、架构难度大，对于平台迁移所产生的问题需要进一步研究。

5 结论

本文基于云存储的高数据量处理能力，吞吐量快，读取时间短的优势结合可信度计算设计了基于云存储的电力系统访问控制方案。通过云存储的方式将用户的访问记录进行保存并在用户访问时进行提取以进行可信度计算，云存储架构通过集群方式大大提高了系统的数据吞吐速率并降低了数据读取时间，提高了系统效率。另一方面通过对用户的特征并结合其过往操作记录的可信度分析计算得出用户的可信度，根据可信度进行

相应的授权操作，有效实现了对不同用户的访问行为进行控制的目的。总结而言，该方案不但可以有效实现访问控制，同时能够极大提高系统效率，具有很好的发展前景。

参考文献：

[1] 赵雪良. 电力云存储中基于属性和策略的访问控制研究 [D]. 保定：华北电力大学，2014.

[2] 甘玉芳. 面向智能电网云存储的基于属性角色的访问控制研究 [D]. 保定：华北电力大学，2015.

[3] 罗　超. 基于云存储的智能配用电系统及其访问控制方法研究 [D]. 保定：华北电力大学，2014.

[4] 张鸿辉，刘　伟，李永强. 应用于电网企业的云存储访问控制增强策略 [J]. 计算机应用与软件，2014 (2)：17－20.

[5] 冉　军. 基于云存储的智能电网访问控制研究 [D]. 保定：华北电力大学，2014.

[6] 关志涛，杨亭亭，徐茹枝，等. 面向云存储的基于属性加密的多授权中心访问控制方案 [J]. 通信学报，2015，36 (6)：116－126.

[7] 明　镜. 智能配电网云存储中基于属性的访问控制研究 [D]. 保定：华北电力大学，2015.

[8] 厉优栋. 基于电力系统统一平台的访问控制机制的研究与实现 [D]. 上海：上海交通大学，2012.

[9] 王保义，王蓝婧. 电力信息系统中基于属性的访问控制模型的设计 [J]. 电力系统自动化，2007，31 (7)：81－84.

[10] 王保义，邱素改，张少敏. 电力调度自动化系统中基于可信度的访问控制模型 [J]. 电力系统自动化，2012，36 (12)：76－81.

[11] 张　强，刘雪艳，王维洲，等. 基于 CP－ABE 的智能电网访问控制研究 [J]. 计算机工程，2014，40 (12)：83－88.

[12] 夏明超，吴俊勇，吴命利. 基于角色访问控制在电力监控系统中的应用 [J]. 电力系统及其自动化学报，2008，20 (2)：46－50.

[13] 孙中伟，张荣刚. 智能配电网通信系统访问控制研究 [J]. 电力系统保护与控制，2010，38 (21)：118－121.

[14] 宋燕敏，杨争林，曹荣章，等. 电力市场运营系统中的安全访问控制 [J]. 电力系统自动化，2006，30 (7)：80－84.

[15] 孙中伟，张荣刚. 智能配电网通信系统访问控制研究 [J]. 电力系统保护与控制，2010，38 (21)：118－121.

[16] 丁　杰，奚后玮，韩海韵，等. 面向智能电网的数据密集型云存储策略 [J]. 电力系统自动化，2012，36 (12)：66－70.

(上接第 220 页)

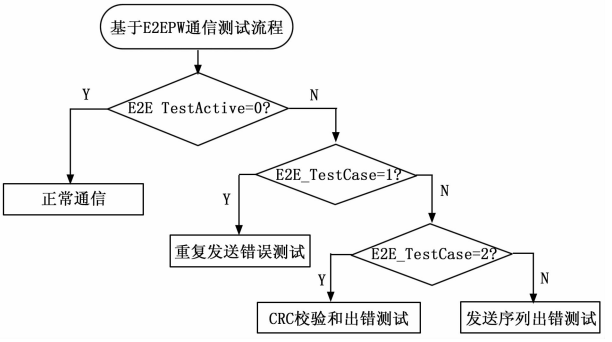

图 12　基于 E2EPW 的 E2E 通信的测试流程图

4.2　基于 COM E2E Callout 实现跨 ECU 通信测试

由于条件限制，本文通过开发工具模拟一个节点，捕捉开发板发送出来的 CAN 报文，修改 CAN 报文的 ID，然后重新发给开发板。通过这样的方式，模拟跨 ECU 之间的通信。

4.2.1　E2E 跨 ECU 通信测试

1）常通信测试：在 TRACE32 中添加观测量 E2E _ P02ReceiverState _ msg _ RxCycle500 _ 20，这是 COM 层上 E2E 通信的状态结构体，其内部保存对最新接收到的 PDU 的校验结果。用 CANoe 和开发板配合构造一个闭环的通信过程来测试 E2E 跨 ECU 通信是否正常工作。此时接收端状态结构体中 Status 为 E2E _ P02STATUS _ OK，表示接收端校验正常，Rte _ ImplicitBufs 会跟随 CAN 报文内容动态变化。

2）异常通信测试：本文通过构造一个开环的通信过程测试 E2E 的检错能力，将 CAN 卡和开发板连接，此时上位机不对接收到的报文做处理，而是将我们自定义的报文发给开发板。发送端的 Counter 是 0－15 循环，如果我们通过 E2E 保护的数据没有动态改变，则 CAN 报文在每个循环中只要 Counter 相同，那 CAN 报文的内容完全一致。首先保证接收端校验正常，再人为的在报文中注入我们想要的错误来测试不同的错误。连续发送两帧 Counter 为 2 的 CAN 报文来测试重复发送错误，此时接收端状态结构体中 Status 为 E2E _ P02STATUS _ REPEATED。改变 Counter 为 2 的 CAN 报文的内容，使其 CRC 校验和出错，然后发送给开发板，此时接收端状态结构体中 Status 为 E2E _ P02STATUS _ WRONGCRC。改变发送序列，在本应该发 Counter 为 3 的时候，发送 Counter 为 4 的给开发板，接收端状态结构体中 Status 为 E2E _ P02STATUS _ OKSOMELOST。

5　结论

本文在 AUTOSAR 架构下，采用 E2E Profile 2 实现了 E2E 安全通信。介绍了基于 E2E Profile 2 实现 E2E 安全通信的原理。在 ECU 内部通信采用 E2E Protection Wrapper 的通信模式，在 ECU 跨核通信采用 COM E2E Callout 的通信模式，描述了这两种通信模式的搭建过程，并搭建实验来模拟在这两种模式下的通信错误，实验表明，该方法能快速有效的检测通信过程中的重复发送错误、CRC 校验和错误及发送序列错误等问题，保障汽车的通信安全。

参考文献：

[1] 魏学哲，戴海峰，孙泽昌. 汽车嵌入式系统开发方法、体系架构和流程 [J]. 同济大学学报（自然科学版），2012，40 (7)：1064－1070.

[2] 高焕吉. 基于 AUTOSAR 的汽车电子控制系统嵌入式软件开发 [J]. 汽车电器，2010 (05)：11－14.

[3] AUTOSAR Administration. Specification of SW－C End to－End Communication Protection Library V4.2.2 [EB/OL]. http：//www.autosar.org/.

[4] AUTOSAR Administration. Specification of Module E2E Transformer V4.2.2 [EB/OL]. http：//www.autosar.org/.

[5] AUTOSAR Administration. Specification of Communication V4.2.1 [EB/OL]. http：//www.autosar.org/.

[6] Moessinger J. AUTOSAR－The Standard for Global Cooperation in Automotive SW Development [Z]. 2008.

[7] Voget S. AUTOSAR and the Automotive Tool Chain [C]. 2010.

[8] AUTOSAR Administration. Specification of Operating System V5.0.0 [EB/OL]. http：//www.autosar.org/.

[9] ETAS GmbH. RTA－OS User Guide [Z]. 2014.

[10] AUTOSAR 基础软件介绍 [Z]. 2013.

[11] 秦美峰. AUTOSAR 软件构件运行实体映射模型的研究与设计 [D]. 成都：电子科技大学，2012.