Smart Grid 智能电网, 2015, 5, 93-99
Published Online June 2015 in Hans. http://www.hanspub.org/journal/sg
http://dx.doi.org/10.12677/sg.2015.53012

Hans汉斯

An Access Control Method Based on HABE Applying in Smart Grid

Yuanpeng Xie, Hong Wen

National Key Laboratory of Science and Technology on Communications, UESTC, Chengdu Sichuan
Email: 1334348030@qq.com

Received: May 29th, 2015; accepted: Jun. 8th, 2015; published: Jun. 12th, 2015

Abstract

There will be huge amount of real-time sensing data in the smart grid system, which would be a huge burden in storing and processing them for the data center, and the property of cloud computing could just fix it up, so the integration of cloud computing and smart grid makes sense. There is private and sensitive information which can't be known or falsified by a third party including the cloud servers in the data center, so the paper proposed an access control method that is based on the Hierarchical Attribute Based Encryption (HABE), which can control the access of the sensitive data storing on the cloud servers effectively.

Keywords

Smart Grid, Access Control, HABE, Encryption

应用于智能电网中的基于层次属性加密访问控制方法

谢远鹏，文　红

电子科技大学通信抗干扰国家级重点实验室，四川 成都
Email: 1334348030@qq.com

收稿日期：2015年5月29日；录用日期：2015年6月8日；发布日期：2015年6月12日

摘　要

智能电网系统拥有海量的实时采集数据，这会给电网数据中心带来巨大的存储和计算负担，而云计算的特点正是拥有强大的存储和计算能力，因此智能电网和云计算的结合能极大提高智能电网的数据存储能力和计算的有效性。由于电网数据中有隐私敏感信息，不能被包括云服务器在内的第三方窥伺和篡改。本文提出一种基于层次属性加密(HABE)的访问控制方法，能有效地实现对存放在云平台的敏感电网数据的访问控制。

关键词

智能电网，访问控制，层次属性，加密

1. 引言

随着智能电网[1]系统的迅速发展，智能电网设备的大量建成，实时采集的海量传感数据将涌入电网数据中心。对于数据中心，来自电网的数据量和对数据的计算量都过于庞大。而云计算作为一种具有超强存储能力和计算能力的典型范例，恰好能够解决这个问题。因此，将智能电网和云计算结合成为了一种合理的新型系统，我们称之为电力云系统。

但是，由于电网数据都存放在云平台上，如果不加以保护，一些敏感的信息如用户账户等将会被包括云服务器在内的第三方窥伺或篡改。隐私信息泄露将会对用户和电网企业造成严重后果。

而对智能电网，外部用户和电网内部对数据的访问和使用权限是不同的，在电网企业内部，各部门有其各自的工作职责和数据需求范围，根据不同部门的业务需求和职责权限，对其能访问的数据进行控制可以有效保护数据的隐私和防止恶意篡改。所以在电网数据的共享过程中不能一概而论，应该对数据进行分级访问控制和基于属性的访问控制。

本文针对存储于云平台的智能电网数据，设计了一种应用于智能电网的基于层次属性加密访问控制(Hierarchical Attribute Based Encryption Access Control)方法，该方法结合基于层次身份加密(Hierarchical Identity Based Encryption, HIBE)系统[2]和密文策略的基于属性加密(CP-ABE)系统[3]。基于层次属性的加密访问控制方法不仅能够同时支持基于精确身份的加密访问控制和基于属性的加密访问控制，而且具有常数级的解密开销，支持层次结构的密钥生成方式，实现细粒度的访问控制，适用于电力云环境下的数据多用户共享场景。

2. 相关内容

2.1. 基于层次的身份加密

1984 年，Shamir [4]提出了基于身份加密(Identity Based Encryption, IBE)的概念。与传统公钥加密体制不同，IBE 采用任意的、能够标识用户身份的字符串作为用户的公钥进行加密，例如，身份证号码、邮箱地址等。发送方无需在线查询权威认证中心(Certificate Authority, CA)关于接收方公钥的信息，解决了 CA 的性能瓶颈问题。

该 IBE 系统的缺点是单一密钥生成器(Private Key Generator, PKG)负责为所有用户生成密钥，将成为系统效率的瓶颈。2002 年，Horwitz 等人[2]提出了基于层次身份加密(Hierarchical IBE, HIBE)的概念。在该方案中，一个处于较高层次的用户可以使用自己的私钥为处于较低层次的用户生成私钥。因此，PKG

只需为第一层次用户生成私钥，而更低层次用户的私钥可由其祖先节点上的用户进行管理，从而能够有效地减轻 PKG 的负担。同时，身份的认证和密钥的传输可以在局部完成，大大提高了系统效率。

2.2. 基于属性加密

基于属性的加密(Attribute Based Encryption, ABE)方案是近年来的公钥加密系统研究热点之一。

ABE [5]实质上可以看做 IBE 系统在用户的私钥中或者密文中引入了一个访问结构而构成的，这些结构定义了具备哪些属性的用户可以解密某个密文(授权集合)，哪些用户不能解密该密文(非授权访问集合)。

ABE 方案发展分为两个分支：密钥策略的 ABE(Key-Policy ABE, KP-ABE) [6]和密文策略的 ABE (Ciphertext-Policy ABE, CP-ABE) [3]。KP-ABE 和 CP-ABE 的区别在于访问结构部署的位置不同。KP-ABE 的访问结构部署在用户的私钥中。其中，用户的私钥是一个访问树结构；加密者为密文指定一系列需要满足的属性，当且仅当这些属性能够满足用户私钥的访问树结构时，用户才能够恢复出解密密钥，获取明文。

CP-ABE 的访问结构部署在密文中。由于访问控制部署在密文中，发送者具有更大的主动性，可以自己决定访问结构来加密一个密文。其中，用户由一个属性集合描述;加密者为密文指定一个树访问结构，当且仅当用户的属性集合能够满足密文的树访问结构时，才能够恢复解密密钥，获取明文。

3. 基于层次属性加密访问控制

云计算作为一种通过互联网为用户提供所需资源的新型计算模式，能给用户提供低成本、高质量的云计算服务。而智能电网系统由于拥有海量的传感数据和电网信息正好需要云服务提供的计算资源和存储资源，因此将云计算和智能电网系统结合形成新型的电力云模型将势在必行。

本文提出一种基于层次属性加密访问控制(HABEAC)的方法应用于电力云环境下多层次用户共享电力数据和信息的场景。

3.1. 方案简介

考虑以下场景：电网系统拥有敏感的电网传感数据如某地电压信息、某节点有安全隐患信息等，和隐私信息如用户身份、用户账户余额等，都需要先对其进行加密再上传到云平台上，但上传者对加密进行处理，以便授权让其他员工访问该数据。这些敏感隐私信息的访问控制列表如表 1 所示。

该访问结构特点如下：

(1) 同一加密数据的接收者为多个，例如对于用户身份，可以同时被项目总监和市场部用户科访问；

(2) 访问结构中不仅有精确的身份描述，还有用户属性的集合。例如对于账户余额，可以同时被项目总监、财务部员工和市场部用户科员工访问，其中项目总监为精确的身份描述，而财务部员工和市场部用户科员工为属性集合。

(3) 如同企业内部等级一样，用户的密钥也有等级关系。例如，电网企业为不同等级的部门生成密钥，同样的，部门为内部员工生成不同的密钥。

由上面的描述可知，要能够实现这些需求，该访问控制方法需要满足一下特点：

(1) 一个密文可以同时被多个，密钥解密；

(2) 访问控制结构能够同时支持精确的身份和属性集合；

(3) 密钥的生成具有和电网企业内部一样的层次性。

为了实现上述要求，本文结合了 G-HIBE [7]方案中的层次密钥生成思想和 DNF 形式[8]的访问结构，提出了应用于智能电网的基于层次属性加密访问控制方法。

3.2. 方案概述

本文提出的基于层次属性加密访问控制方案整体结构如图 1 所示。

该方案总体上由电网企业内部、可信第三方和云服务器三大部分构成。其中云服务器由云服务提供商提供，主要作用为存储或计算来自电网企业的数据；可信第三方主要负责产生、发布系统参数和电网企业密钥；电网企业由第一层内部实体和下层内部可信实体，其中第一层内部可信实体用于管理用户，为用户生成用户私钥，相当于电网企业的人事部，下层内部可信实体负责管理用户属性并为用户生成用户身份密钥和用户属性密钥(用于解密)；图中每个用户拥有唯一的 *ID* 和系列属性集合，每个内部可信实体(包括第一层和下层)和用户属性也拥有唯一的 *ID*。*ID* 是描述系统中实体特征的字符串。如果一个用户的 *ID* 位于访问结构中的精确用户身份 *ID* 集合内，或者用户的用户属性在访问结构中属性集合内，则可以对加密数据进行解密。

3.3. 方案密钥

本 HABE 方案中涉及了非对称加密技术，因此该方案拥有若干密钥，表 2 总结了该方案中使用的主要密钥。

根密钥 MK_0 为可信第三方所拥有，作用是为第一层的内部可信实体产生主密钥。

每一个下层内部可信实体都拥有一个拥有公钥 PK_i 和主密钥 MK_i，其中公钥 PK_i 由下层可信实体的 *ID* 组成，其形式为 $\left(PK_{i-1}, ID_i\right)$，其中，$PK_{i-1}$ 是该内部可信实体的父亲节点的公钥，ID_i 是该实体的 *ID*。特别地，第一层内部可信实体的公钥 PK_* 由其 *ID* 组成，形式为 ID_*。第一层内部可信实体的作用是管理

Table 1. The list of the access control method based on HABE
表 1. HABE 方案访问控制列表

信息类型	访问结构
电压信息	项目总监，负责电压监控的技术人员
安全隐患	项目总监，安全部负责安全技术人员
用户身份	项目总监，市场部用户科员工
账户余额	项目总监，财务部员工，市场部用户科员工

Table 2. The list of major keys in HABE
表 2. HABE 方案主要密钥列表

密钥名称	密钥含义
MK_0	根密钥
MK_*	第一层内部可信实体的主密钥
PK_*	第一层内部可信实体的公钥
PK_i	下层可信实体的公钥
MK_i	下层可信实体的主密钥
PK_u	用户 *u* 的公钥
SK_u	用户 *u* 的私钥
$SK_{i,u}$	用户 *u* 的身份密钥
$SK_{i,u,a}$	用户 *u* 的关于属性 *a* 的密钥
PK_a	属性 *a* 的公钥

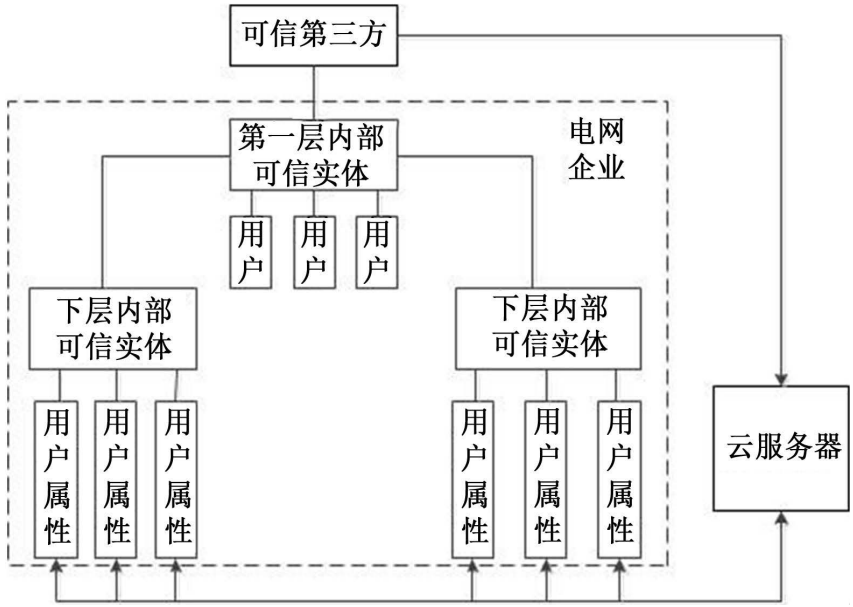

Figure 1. The general structure of HABE
图 1. HABE 整体结构

用户，为用户生成用户私钥，其他下层内部可信实体管理一系列属性集合，并为用户生成用户身份密钥和用户属性密钥。

用户 u 由精确的身份 ID 以及系列属性集合组成。其中用户的 ID 表示为 ID_u，其属性集合表示为 $\{a\}$。

每个用户 u 都拥有一个用户公钥 PK_u，一个用户私钥 SK_u，一系列用户身份密钥 $\{SK_{i,u}\}$ 和一系列用户属性密钥 $\{SK_{i,u,a}\}$。其中用户公钥 PK_u 的形式为 (PK_*, ID_u)，这里 PK_* 为第一层内部可信实体的公钥。

用户属性 a 由一个精确的 ID 描述，表示为 ID_a。属性 a 拥有一个公钥，其形式为 (PK_i, ID_a)，其中 PK_i 为管理该属性的下层内部可信实体的公钥。

3.4. 方案模块

本方案的具体算法由如下各模块组成：

(1) **初始化模块**：输入一个足够大的安全参数 K，由可信第三方输出系统参数 params 和根密钥 MK_0；

(2) **主密钥生成模块**：可信第三方或者内部可信实体利用系统参数 params 和自己的主密钥为下层可信实体生成主密钥。

(3) **私钥生成模块**：第一层内部可信实体首先确定用户 u 的公钥是否为 PK_u。如果是，则利用其主密钥 PK_* 和系统参数 params 为用户生成私钥 SK_u；否则输出为“空”。

(4) **用户身份属性生成模块**：下层内部可信实体首先确定用户 u 是否满足属于自己管理的属性 a。如果是，则为该用户生成用户身份密钥 $SK_{i,u}$，和用户属性密钥 $SK_{i,u,a}$；否则，输出为“空”。

(5) **加密模块**：为了加密电网数据 D，数据加密用户 u 首先确定拥有该电网数据访问权限的接收者的精确 ID 集合 R，和 DNF 形式的基于属性访问结构 A。该用户以位于 R 中所有用户的公钥，以及位于 A 中的所有属性公钥作为输入，输出则为加密后的密文 CT。

(6) **身份解密模块**：为了解密密文 CT，如果某用户 u 的 ID 属于集合 R，则能够利用系统参数 params 和该用户私钥 SK_u 恢复电网数据 F。

(7) **属性解密模块**：为了解密密文 CT，如果用户 u 的属性满足访问结构 A，则能够利用系统参数 params，

用户身份密钥 $SK_{i,u}$，以及该用户的属性密钥 $SK_{i,u,a}$ 恢复电网数据 F。

3.5. 性能分析

本方案涉及了一些加密算法，其中计算开销从大到小依次为双线性对操作、乘幂操作、点乘操作。而由于点乘操作的时间开销相对于前两者可以忽略。因此，本节性能分析中只考虑双线性对操作和乘幂操作带来的时间开销。

初始化算法中计算一次乘幂操作为系统生成固定长度的系统参数。主密钥生成算法中计算两次乘幂操作为下层内部可信实体生成长度为 $O(L)$ 的主密钥，其中 L 为下层内部可信实体所处层次。密钥生成算法中计算一次乘幂操作为用户生成固定长度的用户私钥。用户身份属性生成算法中计算一次乘幂操作为用户生成长度为 $O(L+M)$ 的用户身份密钥和用户属性密钥，其中 L 为管理用户属性的内部可信实体所处层次，M 是用户拥有的属性数目。

为了加密电网数据 D，用户 u 运行加密算法。给定精确的 ID 集合 $R=\{ID_{u_1},\cdots,ID_{u_m}\}$ 和基于属性的 DNF 形式访问结构 $A=\vee_{i=1}^{N}(CC_i)=\vee_{i=1}^{N}\left(\wedge_{j=1}^{n_i}a_{ij}\right)$，该算法计算一次双线性对 $\hat{e}(Q_0,n_A rP_*)$，以及 $O(m+NT)$ 次乘幂操作输出长度为 $O(m+NT)$ 的密文，其中 m 是 R 中电网数据用户的数目，N 是 A 中精确属性的数目，T 是管理 A 中属性的内部可信实体中的最深层次。其中，双线性对 $\hat{e}(Q_0,P_*)$ 的计算只需要一次，因为该双线性对与电网数据内容无关的。

在解密模块中，ID 属于 R 中的用户为了恢复电网数据 D 而计算一次双线性对的时间开销为 $O(1)$，属性满足访问结构 A 的用户。

表 3 比较了本方案与 CP-ABE 方案和 G-HIBE 方案的性能。在该表中表，M 是与电网数据用户相关的属性数目，L 是管理用户属性内部可信实体所处的最深层次，S 是访问结构中的属性数目，N 是访问结构中的精确属性的数目，T 是管理访问结构中属性内部可信实体所在的最深层次，m 是精确 ID 集合中用户的数目，P 是访问结构中与用户属性匹配的属性数目。

由于 HABE 方案支持层次结构的密钥生成方式的优点以及支持精确身份加密的优点，那么变量 L,T,m 均可设置为常数。此时，HABE 方案的性能为最优。

4. 总结

随着智能电网的发展，实时采集的海量传感数据将涌入电网数据中心，按需购买云计算资源用于存储和计算电网数据将成为未来的趋势。为了保护电网中的隐私数据和敏感数据，本文提出一种基于层次属性加密访问控制的方法应用于电力云环境下多层次用户共享电力数据和信息的场景，并与其他方案进行了性能比较。

该方法结合了基于层次身份加密系统[2]和密文策略的基于属性加密系统[3]。基于层次属性的加密访问控制方法不仅能够同时支持基于精确身份的加密访问控制和基于属性的加密访问控制，而且具有常数

Table 3. Comparison of the cost between three methods
表 3. 三种方案性能比较

对象	CP-ABE [6]	G-HIBE [7]	HABE
用户密钥长度	$O(2M)$	$(2M)$	$O(L+M)$
密文长度	$O(2S)$	$O(3N)$	$O(NT+m)$
加密	$O(2N)$	$O(3N)$	$O(NT+m)$
解密	$O(2P)$	$O(1)$	$O(1)$

级的解密开销，支持层次结构的密钥生成方式，实现细粒度的访问控制，适用于电力云环境下的数据多用户共享场景。

参考文献 (References)

[1] 余贻鑫, 栾文鹏 (2009) 智能电网. *电网与清洁能源*, **1**, 7-11.

[2] Horwitz, J. and Lynn, B. (2002) Toward hierarchical identity-based encryption. *Advances in Cryptology—EUROCRYPT* 2002, Springer Berlin Heidelberg, 466-481.

[3] Bethencourt, J., Sahai, A. and Waters, B. (2007) Ciphertext-policy attribute-based encryption. *IEEE Symposium on Security and Privacy*, 2007. SP'07, IEEE, 321-334.

[4] Shamir, A. (1985) Identity-based cryptosystems and signature schemes. *Advances in Cryptology*, Springer Berlin Heidelberg, 47-53.

[5] 王小明, 付红, 张立臣 (2010) 基于属性的访问控制研究进展. *电子学报*, **7**, 1660-1667.

[6] Goyal, V., Pandey, O., Sahai, A., et al. (2006) Attribute-based encryption for fine-grained access control of encrypted data. *Proceedings of the* 13*th ACM conference on Computer and Communications Security*. ACM, 89-98.

[7] Gentry, C. and Silverberg, A. (2002) Hierarchical ID-based cryptography. *Advances in Cryptology—ASIACRYPT* 2002, Springer Berlin Heidelberg, 548-566.

[8] Müller, S., Katzenbeisser, S. and Eckert, C. (2009) Distributed attribute-based encryption. *Information Security and Cryptology—ICISC* 2008, Springer Berlin Heidelberg, 20-36.