一种面向云端辅助工业控制系统的安全机制

屠袁飞 [1,2] 杨 庚 [1] 张成真 [2]

摘 要 随着云计算、物联网等信息通信技术与数据采集与监控系统的整合, 工业控制系统面临新的安全问题, 其中数据的完整性、机密性保护和有效的身份认证问题受到了关注. 为了在这样一个多功能、分布式的环境中解决这些问题, 该文利用基于属性的加密方法, 构建访问控制策略, 为用户提供身份认证和授权服务, 保护用户与工业控制系统间的数据通信安全并实时检查存储数据的完整性. 方案从正确性、安全性及系统性能等方面做出分析, 并与常用的认证方法进行了对比.

关键词 工业控制系统, 访问控制, 身份认证, 完整性, 机密性

引用格式 屠袁飞, 杨庚, 张成真. 一种面向云端辅助工业控制系统的安全机制. 自动化学报, 2021, **47**(2): 432−441

DOI 10.16383/j.aas.c180142

开放科学 (资源服务) 标识码 (OSID):

A Security Scheme for Cloud-assisted Industrial Control System

TU Yuan-Fei [1,2] YANG Geng [1] ZHANG Cheng-Zhen [2]

Abstract With the integration of cloud computing, internet of things (IoT) and supervisory control and data acquisition (SCADA) system, industrial control system (ICS) is faced with new security issues. Among them, the issue of data integrity, confidentiality protection and effective authentication has drawn attention. To address these issues in such a versatile and distributed environment, attribute-based encryption is used to construct access control policies, provide authentication and authorization services, protect the data communication between users and ICS and check the integrity of stored data in real time. We prove the correctness of the scheme, analyze its security and evaluate its performance, also compare it with the commonly used methods.

Key words Industrial control system, access control, authentication, integrity, confidentiality

Citation Tu Yuan-Fei, Yang Geng, Zhang Cheng-Zhen. A security scheme for cloud-assisted industrial control system. *Acta Automatica Sinica*, 2021, **47**(2): 432−441

工业企业为了降低运营成本和相关费用, 不断寻求能够提供稳定性, 容错性和灵活性的工业系统解决方案. 云端辅助的工业控制系统[1] 随之出现, 即将云计算服务、物联网与传统的数据采集与监控 (Supervisory control and data acquisition, SCADA) 系统整合, 以感知真实世界中不断变化的状态, 通过云计算、大数据分析, 实现动态的优化控制, 甚至可以将其部署在实时闭环的控制回路中[2−5]. 在整合过程中, 新旧技术重叠使用, 除具有传统 SCADA 系统存在的安全问题外, 还面临其他来源多样的威胁, 包括敌对政府, 恐怖组织, 内部人士的恶意或意外行为, 恶意入侵者, 事故和自然灾害等. 依赖云通信使得 SCADA 系统更加开放, 但系统命令和信息也可能在通信过程中被修改, 嗅探或丢失. 即使一些工业云采用了传统的用户名密码的访问控制机制, 进入云中的用户面对系统全部的数据, 也可能破坏其他不可访问资源的隐私. 更重要的是, 在工业系统中执行的逻辑对物理世界有直接的影响, 被恶意攻击的系统会对人类的健康安全、环境、设备造成严重的破坏及损失, 最知名的莫过于 2010 年伊朗核系统遭受的 Stuxnet 病毒事件[6]. 近年来, 世界各国均提出了一些极具参考意义的指标和安全实践指南[7], 我国也颁布了《网络安全法》, 提出加强关键信息基础设施安全防护, 维护国家网络安全.

对此有学者提出通过加密方法来阻止信息泄露, 实现隐私保护[8]. 文献 [9] 基于稳定性判据设计了一种工业控制系统中加密传输机制的可行性评估模型.

文献 [10] 对 SCADA 网络安全已有的标准规范进行了综述, 并使用纵深防御理论对其分别进行了评估. 文献 [11] 采用粒子滤波算法, 建立工控系统

收稿日期 2018-03-12 录用日期 2018-07-15
Manuscript received March 12, 2018; accepted July 15, 2018
国家自然科学基金 (61572263, 61272084), 江苏省高校自然科学研究重大项目 (11KJA520002) 资助
Supported by National Natural Science Foundation of China (61572263, 61272084), the Major Project of Natural Science Research in Jiangsu University (11KJA520002)
本文责任编委 李乐飞
Recommended by Associate Editor LI Le-Fei
1. 南京邮电大学计算机学院 南京 210003 2. 南京工业大学计算机科学与技术学院 南京 211816
1. School of Computer Science & Technology, Nanjing University of Post & Telecommunication, Nanjing 210003 2. College of Computer Science & Technology, Nanjing Tech University, Nanjing 211816

网络态势感知模型, 判断系统是处于 "安全态势" 还是 "危险态势". 文献 [12] 针对 SCADA 系统使用的 DNP3 通信协议的安全问题, 使用密码学工具来防止数据在传输的过程中被窃听, 保护数据通信的安全, 并做了相关性能测试. 文献 [13] 针对工业无线传感器网络中无线介质的开放特性, 攻击者可以容易地窃听通信来收集关于传感器的隐私信息这一问题, 提出了一种能够支持网络身份验证的假名通信方案. 该方案利用代理服务器为每台传感器分配随机 ID 的方法来匿名通信, 但仅支持传感器的一跳范围之内的隐私保护. 文献 [14] 将主流加密算法应用在 PLC 中, 对其性能进行了仿真测试, 并在 PLC 网络中实测了网络吞吐量, 结果表明 AES 算法是目前最适合 PLC 的加密方法. 然而作为一种对称加密算法, 如何管理其密钥是必须考虑的问题.

通过上述安全控制措施的确能够检测恶意软件的引入, 减轻系统运行威胁, 但并没有将攻击者拒之门外. 文献 [15] 表明通过 APT 攻击, 攻击者能够在不引起数据被破坏的情况下, 长时间地潜伏在系统中窃取数据. 文献 [16] 指出用户的疏忽也是导致信息泄露的重要因素, 因此需要设计一种覆盖所有现场设备的细粒度访问控制方案, 防止任何未经授权的访问行为. 文献 [17] 提出应限制对打印机或共享磁盘等公共资源的访问, 访问者应包含在网络的已知用户中, 并通过认证方法来阻止隐蔽信道. 文献 [18] 针对关键基础设施资产保护问题, 采用可信计算方法来限制软件平台上的开放接口, 达到保护资产的目的, 但并不能提供细粒度的访问控制. 变电站安全标准 IEC/TS62351-8[19] 建议使用认证机制, 尤其是基于角色的访问控制 (Role-based access control, RBAC) 方法[20] 来降低整个 SCADA 网络的复杂性. 文献 [21] 则针对楼宇控制系统中各分布式子系统间的通信安全问题, 为用户分配预定访问权限策略的角色, 保护资源免受未经授权的访问. 文章缺点在于当主体和客体属性的数量变大时, 角色的数量呈指数增长.

与 RBAC 不同, 从分布式计算派生的基于属性的访问控制 (Attribute-based access control, ABAC) 方法为系统中的每个实体分配所谓的 "属性". 用属性描述的策略可以表达基于属性的逻辑语义, 灵活地描述访问控制策略[22]. 在基于密文策略 (Ciphertext-policy attribute-based encryption, CP-ABE) 的方案中[23], 密文中嵌入了访问控制结构, 即加密之后就确定了哪些用户能够对它进行解密而不需要借助可信服务器来实现这种控制.

本文利用基于属性的加密 (Attribute-based encryption, ABE) 算法能够有效实现细粒度非交互访问控制[24] 的特点, 为云端辅助的工业控制系统提出了安全高效的访问控制方案, 有效地控制了用户权限, 保护了数据隐私. 方案能够对云中存储数据进行实时动态地验证来识别损坏数据的行为, 确保数据的完整性. 并且为现场设备与用户建立了安全的通信连接, 通过对用户的严格认证, 保证现场控制器获得可信的数据. 最后, 文章分析了方案的安全性与性能开销, 并给出实验结果.

1 预备知识及系统模型

1.1 预备知识

1.1.1 双线性映射

设 G_1 和 G_2 是两个 p 阶循环群, 其中 p 为一大素数设 p 为 G_1 的生成元, 定义双线性映射 $e: G_1 \times G_1 \rightarrow G_2$ 满足如下条件:

1) 双线性性: 对任意的 $P,\ Q \in G_1, a, b \in \mathbf{Z}_p$, 满足 $e(P^a, Q^b) = e(P, Q)^{ab}$.

2) 非退化性: $e(P, P) \neq 1$.

3) 可计算性: 对任意 $P, Q \in G_1, a, b \in \mathbf{Z}_p$, 存在一个有效的多项式时间算法计算出 $e(P, Q)$.

1.1.2 线性秘密共享方案

一个基于成员集 P 的秘密共享方案 Π 在 $\mathbf{Z}_p$ 上是线性的需要满足一下两个条件:

1) 每个成员所分得秘密的一部分构成一个 $\mathbf{Z}_p$ 上的矩阵.

2) Π 中存在一个 $l \times (n+1)$ 秘密共享矩阵 M. 对于 $i = 1, \cdots, l$, M 的第 i 行表示第 i 个成员 $x_i \in P$. 设一个列向量 $\boldsymbol{v} = (s, r_2, \cdots, r_n)$, 其中 $s \in \mathbf{Z}_p$ 是待分享的秘密, 是随机的, 则 $M \cdot \boldsymbol{v}$ 把秘密 s 根据 Π 分成 l 个部分. $(M \cdot \boldsymbol{v})_i$ 属于成员 x_i.

1.2 系统模型

如图 1 所示, 云端辅助的工业控制系统一般包含四个实体: SCADA 系统、私有云 (Private cloud, PC)、公有云 (Public clouds, PubC) 以及数据用户 (Data consumers, DC).

1.2.1 SCADA 系统

SCADA 系统作为一个可以监控及控制所有设备的集中式系统, 一般包括以下的子系统: 人机界面系统, 远程终端控制系统 (Remote terminal unit, RTU), 可编程逻辑控制器 (Programmable logic controller, PLC), 分布式控制系统 (Distributed control system, DCS) 等. 对现场设备的控制及数据采集功能由 PLC 等控制系统进行, 包括启停电机, 读发送设备的状态报告等. SCADA 系统将采集到的数据发送到企业私有云平台, 并接收来自私有云的指令.

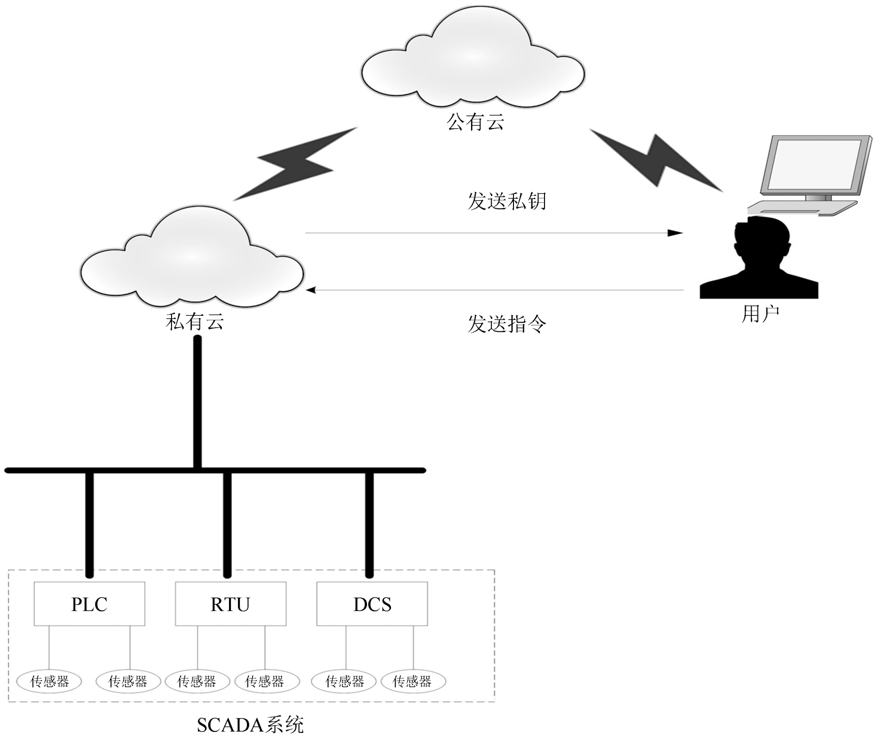


图 1 系统模型

Fig. 1 System model

1.2.2 私有云

私有云是为一个企业单独使用而构建的, 能够提供对数据、安全性和服务质量的最有效控制. 私有云具有相对安全的优势, 但不适合大规模存储. 企业在私有云部署授权中心 (Key generation center, KGC), 根据基于属性的加密方法, 生成公钥及主密钥, 管理系统中的属性, 构建访问策略并以此加密数据, 之后再把密文发送到公有云存储.

此外, 为防止由于软件错误或配置错误导致的数据损坏, 私有云对外包存储的数据进行完整性检查, 以确保数据是真实的, 或未被未经授权方修改过.

1.2.3 公有云

公有云由第三方提供商为企业提供, 包括位置独立的数据存储, 无处不在的数据访问, 按需的高质量服务, 成本低廉, 动态扩展性等优势. 企业在公有云上完成资源租用、应用托管和服务外包.

在本模型中, 我们假设公有云是诚实但又好奇, 且易受到攻击的. 因此由私有云对数据进行加密后再发送到公有云, 用户从公有云中获取密文. 由于访问控制策略包含在密文中, 只有具备相应属性的用户才能获得访问数据的权限, 因此公有云只能对密文进行存储、转发, 其自身也没有访问原始数据的权限. 此外, 公有云接受来自私有云的审核, 配合私有云完成存储数据的完整性检查.

1.2.4 数据用户

数据用户一般为企业管理人员、工艺员、操作工、监管部门等. 用户向 KGC 声明其所拥有的属性, 获得属性私钥. 如果数据用户的属性满足密文中所定义的访问策略, 则用户可通过该私钥获得访问公有云中原始数据的权限, 对数据进行分析诊断, 再将优化后的参数或指令经私有云发送到底层 PLC、RTU 等设备.

2 系统方案

本文首先在文献 [25] 的加密算法基础上, 提出了一种面向云端辅助工业控制系统的保护用户隐私的访问控制方案. 一个支持细粒度属性撤销的 ABAC 方案由 6 种多项式时间算法组成: $Setup$, $KeyGen$, $Encrypt$, $Decrypt$, $ReEnc$, $ReKeyGen$. $Setup(1^\lambda) \rightarrow PK, PK', MK$: KGC 运行初始化算法, 输入安全参数 1^λ, 输出公钥 PK、PK' 和主密钥 MK. $KeyGen(MK, S) \rightarrow SK$: KGC 运行私钥生成算法, 输入主密钥 MK 和用户属性集合, 输出用户属性私钥 SK. $Encrypt(PK, K, \Lambda) \rightarrow CT$: 明文数据 K 的拥有者执行加密算法. 算法输入公钥 PK, 明文 K 和访问结构 Λ, 输出密文 CT. $Decrypt(SK, CT) \rightarrow K$: 数据用户执行解密算法. 算法输入该用户的属性私钥 SK 和密

文 CT, 若用户所持有的属性私钥 SK 满足密文 CT 中包含的访问结构 Λ, 算法能够正确输出明文 K. $ReKeyGen(SK,x')\rightarrow\widetilde{SK}$: KGC 执行私钥更新算法, 算法输入私钥 SK 的部分组件以及待撤销属性 x', 输出更新后的用户属性私钥 $\widetilde{SK}$. $ReEnc(CT,x')\rightarrow\widetilde{CT}$: 明文数据 K 的拥有者执行重加密算法. 算法输入密文 CT 的部分组件以及待撤销属性 x', 输出更新后的密文 $\widetilde{CT}$.

如图 2 所示, 某生产企业配方数据的访问策略规定只有工艺部门的技术员、主任或管理部门经理才可以看到其中的具体内容, 其逻辑表达式为: {[(工艺部门) AND (技术员 OR 主任)] OR [(管理部门) AND (经理)]}. 由于配方数据已按上述访问策略被加密, 因此其他部门人员就无法对该密文进行解密, 从而实现了灵活、细粒度的访问控制.

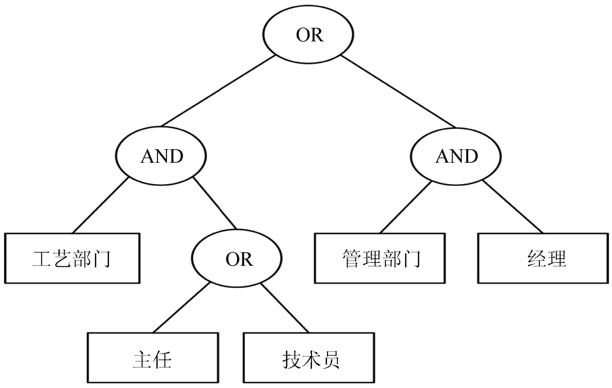


图 2　访问策略

Fig. 2　Access policy

随着时间的推移, 用户属性会发生变化, 相应的访问策略也要有变化, 此时需通过 $ReKeyGen$ 算法和 $ReEnc$ 算法对用户属性私钥及密文进行更新, 令被撤销属性的用户不能再访问密文.

2.1　访问控制方案构造

算法 1. 系统初始化 $Setup(1^\lambda)$

设 G, G_T 是两个阶为大素数 p 的乘法循环群, g 是 G 的一个生成元, 在 G 中随机选取辅助变量 u, 定义 $e:G\times G\rightarrow G_T$ 是一个双线性映射. KGC 随机选取 $\alpha,\beta,a\in\mathbf{Z}_p$. 哈希函数 $H:\{0,1\}^*\rightarrow G$ 作为散列到群 G 一个随机库.

生成系统公钥为:

$$PK=\{g,e(g,g)^\alpha,g^\alpha\},PK'=\{g^\beta\}\tag{1}$$

主密钥为:

$$MK=\{\alpha,g^\alpha,\beta\}\tag{2}$$

算法 2. 私钥生成算法 $KeyGen(MK,S)$

算法输入主密钥的组件 α,g^α 和用户属性集 S, 选取随机数 $t\in\mathbf{Z}_p$, 计算输出用户私钥为:

$$\begin{aligned}SK=&\{P,L,\forall x\in S,K_x\}=\\&\{g^\alpha g^{at},g^t,\forall x\in S:K_x=H(x)^t\}\end{aligned}\tag{3}$$

算法 3. 加密算法 $Encrypt(PK,K,(M,\rho))$

算法输入公共密钥 PK, 对称加密算法的密钥 K, 以及 LSSS 访问结构 (M,ρ). 令 M 为一个 $l\times n$ 阶的矩阵, l 为用户属性数, n 为访问策略中的属性数, 函数 ρ 将 M 中的每一行映射到一个用户属性. 在 $\mathbf{Z}_p$ 上随机选择一个矢量 $\boldsymbol{v}=(s,y_2,\cdots,y_n)\in\mathbf{Z}_p^n$ 用于分享加密元素 s, 对 $i=1,2,\cdots,l$, 计算 $\lambda_i=M_i\boldsymbol{v}$, 其中 M_i 为 M 的第 i 行, 再随机选取 $r_1,\cdots,r_l\in\mathbf{Z}_p$, 得到密文如下:

$$\begin{aligned}CT=&\{\widetilde{C},C,\{C_i,D_i\}_{i=1,\cdots,l}\}=\\&\{Ke(g,g)^{\alpha s},g^s,\{g^{a\lambda_i}H(\rho(i))^{r_i},g^{r_i}\}_{i=1,\cdots,l}\}\end{aligned}\tag{4}$$

算法 4. 解密算法 $Decrypt(SK,CT)$

算法以属性私钥以及密文为输入, 拥有的解密者试图解密, 假设用户的属性列表满足访问结构, 则存在使得, 其中 $I=\{i:\rho(i)\in S\}$ 解密算法首先计算:

$$A=\frac{\prod_{i\in I}e(C_iL)^{\omega_i}}{\prod_{i\in I}(e(D_i,K_{\rho(i)}))^{\omega_i}}=e(g,g)^{ats}\tag{5}$$

再计算输出明文:

$$K=\frac{\widetilde{C}\cdot A}{e\left(C,P\right)}\tag{6}$$

算法 5. 私钥更新算法 $ReKeyGen(SK,x')$

对任意待撤销属性 x', KGC 随机选取 $V_{x'}\in\mathbf{Z}_p$ 作为其更新值再选取私钥 SK 的部件 K_x 按如下公式与新的属性值 $V_{x'}$ 进行计算:

$$\begin{aligned}&x\neq x':\widetilde{K}_x=K_x=H(x)^t;\\&x=x':\widetilde{K}_x=K_{x'}^{v_{x'}}=H(x')^{t\cdot v_{x'}}\end{aligned}$$

用 $\tilde{K}_x$ 替代原私钥部件中相对应的 K_x 算法输出重定义的用户私钥为:

$$\widetilde{SK}=\{P,L,\forall x\in S,\widetilde{K}_x\}\tag{7}$$

算法 6. 重加密算法 $ReEnc(CT,x')$

算法选取密文 CT 的部件 D_i, 及算法 5 中为待撤销的属性 x' 选取的值 $V_{x'}$ 按如下公式计算:

$$\begin{aligned}&\forall i=1,2,\cdots,l;\\&\rho(i)\neq x';\widetilde{D}_i=D_i=g^{r_i};\\&\rho(i)=x';\widetilde{D}_i=D_i^{1/V_{p(i)}}=(g^{r_i})^{\frac{1}{V_{p(i)}}}\end{aligned}$$

此时重加密之后的密文为

$$\widetilde{CT}=\{\widetilde{C},C,\{C_i,\widetilde{D}_i\}_{i=1,\cdots,l}\} \tag{8}$$

2.2 用户读取数据

ABE 算法作为一种公钥加密算法, 本身较复杂, 不适合对大型文件进行加密, 而对称加密算法又必须解决安全传递对称密钥的问题, 因此本文采用混合加密的方式, 首先私有云从密钥空间中随机选取一个对称密钥 K, 利用对称加密算法 $AES(K,D)$ 对现场采集数据 D 进行加密. 之后根据 ABE 算法, 定义该文件的访问结构, 调用加密算法 3 加密上述对称密钥 K, 得到密钥密文 CT, 再按照图 3 的存储格式发送至公有云.

$$(Encrypt(K),AES(K,D))\,|_{PC\rightarrow PubC} \tag{9}$$

其中 $PC \rightarrow PubC$ 表示由私有云至公有云的数据传输.

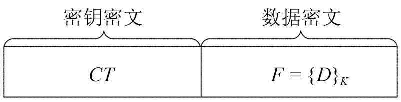


图 3 数据文件的密文格式

Fig. 3 Format of ciphertext

用户向 KGC 声明其所拥有的属性, 根据算法 2 获得属性私钥. 之后从公有云获取加密数据, 利用算法 4 得到会话密钥 K. 最后利用会话密钥 K 解密 $AES(K,D)$ 得到原始数据 D.

2.3 数据完整性检查

用户可以在将数据发送到云端之前对数据进行加密来保护数据, 但是它不能防止由于软件错误或配置错误导致的数据损坏或恶意用户的篡改. 这就需要对云中存储数据进行完整性检查, 以确保租户存储的数据是完整可获取的. 通过密码学的挑战应答方式, 企业在私有云上部署完整性检查服务, 由其对公有云发送挑战信息, 通过对公有云响应的严格认证, 获得其政策合规性的技术保证. 认证过程分为 2 个阶段: 初始化阶段和挑战阶段, 以下将详细描述 2 阶段的过程.

2.3.1 初始化阶段

步骤 1. 私有云根据算法 1 生成密钥对 $\{g^{\beta},\beta\}$.

步骤 2. 私有云对密文 F 进行分块, 将其分为 $F=\{b_1,b_2,\cdots,b_n\}$, 随机选择 $m_i\in\mathbf{Z}_p$, 为上述每一数据块生成认证元数据集合 $\Phi=\{\sigma_1,\sigma_2,\cdots,\sigma_n\}$, 这里 $\sigma_i=(H(i)\cdot u^{m_i})^{\beta}$, $H(i)$ 为 i 对应的哈希运算.

步骤 3. 私有云将 $\{m_i\}$ 和 $\{\sigma_i\}$ 附在密文之后发送到公有云中存储.

2.3.2 挑战阶段

步骤 1. 私有云作为验证者, 周期性地发起完整性验证. 从文件 F 分块中随机选取 t 个索引编号, 并为每一个编号选取一个随机数 $v_i\in\mathbf{Z}_p$, 将二者组合形成挑战请求 $\{i,v_i\}_{i\in[1,n]}$, 并将 v_i 发送到公有云作为挑战.

步骤 2. 公有云利用其存储的 v_i 做以下运算

$$\begin{aligned}\mu&=\sum_{i=i_1}^{i_t}v_i\cdot m_i\\ \sigma&=\prod_{i=i_1}^{i_t}\sigma_i^{v_i}\end{aligned} \tag{10}$$

然后将 $\{\mu,\sigma\}$ 发送给私有云进行验证.

步骤 3. 私有云接收到 $\{\mu,\sigma\}$ 后, 判断如下等式是否成立

$$e(\sigma,g)=e(\prod_{i=i_1}^{i_t}H(i)^{v_i}\cdot u^{\mu},v) \tag{11}$$

若等式成立, 则认为公有云中存储的数据是完整的.

2.4 用户与私有云的直接通信

通过公有云的分析、优化服务, 用户可以更好地掌控生产全局, 提供个性化产品的关键参数, 优化生产工艺. 用户将关键信息提交给私有云, 私有云解析产品数据和关键参数, 再将数据传输给底层的工业机器人、PLC、RTU 控制器开展生产流程. 在这一过程中, 私有云需对用户进行身份认证, 防止恶意用户的攻击, 保证系统的安全运行. 为此本文提出一种简单且安全的数据通信方案, 为 Internet 上传输的数据提供可互操作的、基于密码学的安全保证, 保护了传输数据的机密性、完整性. 详细步骤如下:

步骤 1. 系统根据算法 1 进行初始化, 用户获得 KGC 发布的属性私钥.

步骤 2. 用户向私有云提出更新参数 $Para$ 的请求. 私有云从密钥空间中随机选取一个密钥 K_1, 利用算法 3 加密 $K_{Tdate}=K_1||datetime$, 并将加密后的标记发送到用户, 并保存 $H(K_{Tdate})$ 运算值.

$$(Encrypt(K_{Tdate}))|_{PC\rightarrow DC} \tag{12}$$

$H(\cdot)$ 表示发送端与接收端协议预先约定的哈希函数, $datetime$ 为当前时间.

步骤 3. 用户得 $(Encrypt(K_{Tdate}))|_{PC\rightarrow DC}$ 后, 通过算法 4 解密密文, 并做哈希运算, 再发回私有云, 供其读取验证: $H'=H\,(K_{Tdate})\,|_{DC\rightarrow PC}$.

步骤 4. 私有云读取用户返回的信息后, 比较 H' 与 H 是否相等. 如果相等, 私有云和用户便可将标记 K_1 作为双方直接通信的会话密钥进行安全的加密通信.

步骤 5. 用户按如下格式将参数 $Para$、目标控制器编号 ID_s、用户编号 ID_c, 当前时间 $datetime$ 串联并按如下格式发送到私有云.

$$(ID_s, ID_c, AES(K_1, ID_s||ID_c||datetime||Para),\\ H(ID_s||ID_c||datetime||Para))_{DC\to PC} \tag{13}$$

步骤 6. 私有云解密消息得到新的参数 $Para$, 然后比较 $(H' = H(ID_s||ID_c||Para))$ 是否与 H 相等, 如果相等, 则证明消息的真实性、完整性.

步骤 7. 私有云将新的参数 $Para$ 传送到目标控制器中, 执行指令.

2.5　对称密钥的有效期

作为一种非对称加密算法, ABE 的加解密时间长、速度慢, 计算复杂度高. 因此在第 2.2 节用户读取数据一节中, 采用 ABE 算法加密对称密钥, 再用对称密钥完成对现场采集数据的加密. 由于访问控制策略包含在密文中, 只有具备相应属性的用户才能得到对称密钥, 从而获得现场数据. 在实际使用中, 为保证通信的安全, 对称密钥在使用一段时间后就应被撤销. 私有云可定时更新对称密钥, 用户需重新通过 KGC 的身份认证后才能获得新密钥. 在此过程中, 密钥的有效期越短, 系统的安全性越高, 但是系统开销也会增大.

在第 2.4 节用户与私有云的直接通信一节中, 也采用了上述的混合加密方法. 在用户发往私有云的参数密文中, 包含了当前的传送时间. 因此通信双方可约定用户指令的有效时间, 当私有云接收用户指令达到约定时间后, 即可撤销用于该直接通信的密钥 K_1.

3　方案分析

3.1　正确性分析

以下对算法 4 解密过程的正确性进行验证: 在没有属性撤销情况下:

$$A = \frac{\prod_{i\in I} e(C_i, L)^{\omega_i}}{\prod_{i\in I} e(D_i, K_{\rho(i)})^{\omega_i}} =$$

$$\frac{\prod_{i\in I} e(g^{a\lambda_i} H(\rho(i))^{r_i}, g^t)^{\omega_i}}{\prod_{i\in I} e(g^{r_i}, H(\rho(i))^t)^{\omega_i}} = \\ \prod_{i\in I} e(g,g)^{at\lambda_i\omega_i} = e(g,g)^{ats}$$

当需对某用户的属性 x' 进行撤销时, 算法 4 求解 A 的过程将分为如下两部分:

若 $\rho(i) \neq x'$:

$$B_i = \frac{e(C_i, L)^{\omega_i}}{e(D_i, K_{\rho(i)})^{\omega_i}} = \\ \frac{e(g^{a\lambda_i} H(\rho(i))^{r_i}, g^t)^{\omega_i}}{e(g^{r_i}, H(\rho(i))^t)^{\omega_i}} = e(g,g)^{at\lambda_i\omega_i}$$

若 $\rho(i) = x'$:

$$B_i = \frac{e(C_i, L)^{\omega_i}}{e(\widetilde{D}_i, \widetilde{K}_{\rho(i)})^{\omega_i}} = \\ \frac{e(g^{a\lambda_i} H(\rho(i))^{r_i}, g^t)^{\omega_i}}{e((g^{r_i})^{1/v_{\rho(i)}}, H(\rho(i))^{tv_{\rho(i)}})^{\omega_i}} = \\ e(g,g)^{at\lambda_i\omega_i}$$

此时:

$$A = \prod\nolimits_{i\in I} B_i = \prod\nolimits_{i\in I} e(g,g)^{at\lambda_i\omega_i} = e(g,g)^{ats}$$

然后求解下式:

$$\frac{\widetilde{C}\cdot A}{e(C,P)} = \frac{Ke(g,g)^{\alpha s}\cdot e(g,g)^{ats}}{e(g^s, g^\alpha g^{at})} = K$$

以下对数据完整性验证的式 (11) 进行证明:

$$\begin{aligned} e(\sigma, g) = & e(\prod_{i=i_1}^{i_t} \sigma_i^{v_i}, g) = \\ & e((\prod_{i=i_1}^{i_t} [h(i)\cdot u^{m_i}]^{\beta})^{v_i}, g) = \\ & e((\prod_{i=i_1}^{i_t} [h(i)\cdot u^{m_i}]^{v_i})^{\beta}, g) = \\ & e(\prod_{i=i_1}^{i_t} [h(i)\cdot u^{m_i}]^{v_i}, g^{\beta}) = \\ & e(\prod_{i=i_1}^{i_t} h(i)^{v_i}\cdot \prod_{i=i_1}^{i_t} u^{m_i\cdot v_i}, g^{\beta}) = \\ & e(\prod_{i=i_1}^{i_t} h(i)^{v_i}\cdot u^{\sum_{i=i_1}^{i_t} m_i\cdot v_i}, g^{\beta}) = \\ & e(\prod_{i=i_1}^{i_t} h(i)^{v_i}\cdot u^{\mu}, v) \end{aligned}$$

□

3.2　安全性分析

3.2.1　数据的机密性

本方案中, 数据文件的机密性取决于对称加密算法 (AES), 而对称加密算法的机密性则主要取决

于对称密钥 K 的安全性. 密钥 K 的加密采用了 ABE 算法, 该算法已被证明是安全的, 未认证用户 (如攻击者) 的属性集不满足访问策略, 无法在解密过程中恢复 $e(g,g)^{ast}$ 的值, 从而不能访问数据文件. 同理, 撤销属性的用户所拥有的属性私钥已无法与重加密密文中的组件进行匹配运算, 因此也不能成功解密.

本方案利用公有云存储密文数据, 一方面它对所存文件的内容是好奇的, 另一方面它也会诚实地执行企业私有云安排的任务. 公有云除存储密文外, 仅负责接受私有云的完整性检查挑战, 返回相应的密文数据块, 不参与任何与加密相关的行为, 也不会获得任何有效的属性私钥, 因此其无法解密密文.

3.2.2 抗合谋攻击

基于属性的加密算法最大的挑战是防止合谋用户的攻击. 在 CP-ABE 中, 秘密共享值 s 嵌入在密文中. 为了解开密文, 用户或者合谋攻击者需要将 $e(g,g)^{ast}$ 恢复出来. 合谋攻击者必须利用密文中的组件 C_l, D_l 和其他合谋用户的私钥组件 L, $K_{\rho(i)}$ 做相应的双线性配对运算. 但是, 每一个用户的私钥都通过一个随机数 t 唯一生成, 每个用户的 t 不同, 因此即使用户合谋, $e(P,P)^{ast}$ 的值也不会被恢复. 只有当该用户具有的属性满足访问策略时 $e(P,P)^{ast}$ 值才会被恢复.

3.2.3 数据的完整性

在云存储环境中, 由于用户失去了对外包数据的本地控制, 会担心数据是否一直正确地存储在云中. 为了检测甚至防止这种情况发生, 需要定期审核云数据的完整性. 因此用户如何验证云数据的完整性成为了云存储中一个关键问题.

该方案通过数据分块、分别编码及抽查文件随机子集技术来确保云服务系统中数据的持有性和可恢复性, 能够进行无限多次完整性验证, 同时有效地确保了数据的内容不被验证者察知, 用户甚至可以将繁琐的数据审计任务交由可信的第三方管理者来完成.

3.2.4 通信认证

大多数 SCADA 元件不认证发给他们的命令, 无论命令是否合法, 它们仍将执行发送给他们的任何命令. 本方案中, 当用户发送指令到现场控制器时, 需先通过私有云的认证, 才能完成指令更新. 在这一过程中, 考虑到密钥 K_1 可能会被用户泄露或者被攻击者离线破解来获得, 因此随机选取了密钥 K_1 并加入失效时间来保证通信安全.

在 SCADA 系统中, 拒绝服务攻击是最常见的攻击方式. 这种攻击一般不能对系统进行控制, 但会降低整个系统的性能, 甚至令其故障. 攻击者利用大量合理的服务请求来占用过多的服务资源, 或频繁发送命令来限制各种 SCADA 系统所需的资源, 从而导致系统无法执行预定的任务[26]. 本方案不用实时在线检测用户身份, 且采用了随机密钥和失效时间的设置, 如果攻击者不能在规定的时间内提交会话密钥, 则不能访问系统. 对于频繁提交认证请求的攻击者, 也可撤销其属性, 拒绝访问请求.

3.3 性能分析

3.3.1 通信消息长度

用户访问公有云获取数据时, 需首先利用式 (9) 获取对称加密密钥 K, 根据式 (4) 和式 (9), 可以计算出密钥密文总长度为:

$$Size = |Encrypt\,(K)| = \left|\widetilde{C}\right| + |C| + |C_1| + \cdots + |C_l| + |D_1| + \cdots + |D_l| = (2l+2)\,|p| \tag{14}$$

在实际应用场景中, 为达到足够的访问属性数目与较低的计算开销, 令访问属性数 $l=10$.

式 (14) 中的每个参数长度是可变的, 本方案的评估中, 双线性映射 e 采用基于椭圆曲线上的 Tate 对, 椭圆曲线定义在有限域 F_p 上, G 和 G_T 的阶 p 是一个 20 Byte 的素数. 为了达到 1 024-bit RSA 的安全等级, p 应为一个 64 Byte 的素数, 其中 G_T 是一个定义在有限域 $F^*_{p^2}$ 上的乘法群的 p 阶子群.

设定 p 为有限域 $F^*_{p^3}$ 上长度为 42.5 Byte 的素数, 以及有限域 $F^*_{p^6}$ 上长度为 20 Byte 的素数. 因此, 式 (14) 计算出的总密文长度可表示为 $22\,|p|$ Byte, 大小范围为 440 Byte 到 1 408 Byte.

信道建立后, 在下次会话生成之间的通信, 由于用户拥有了对称密钥, 其通信密文长度可表示为:

$$Size = |AES\,(K, D)| \tag{15}$$

其长度为 16 Byte.

当用户需与私有云进行通信时, 同理根据式 (3) 和式 (11) 可计算出私有云与用户之间通信时的密文长度如下:

$$Size = |Encrypt\,((K_{Tdate}))| + |Hash(K_{Tdate})| = (2l+2)\,|p| + 16 \tag{16}$$

按照相同的分析方法, 从式 (16) 以计算出总密文长度为 $22\,|p| + 16$ Byte, 大小范围为 456 Byte 到 1 424 Byte.

数据用户成功建立链接之后, 其发送到私有云

的密文长度为:

$$\begin{aligned}Size =& |ID_s| + |ID_c| + \\ & |AES(K_1, ID_s \parallel ID_c \parallel datetime \parallel Para)| + \\ & |H(ID_s \parallel ID_c \parallel datetime \parallel Para)| = \\ & 1 + 1 + 16 + 16 = 34\end{aligned} \tag{17}$$

此处将 IDs 和 IDc 的长度分别设为 1 Byte, 这已能满足实际使用. 从以上分析可见, 在用户与公有云建立链接完成认证这一过程中, 通信的密文长度为 $22|p|$ Byte, 建立安全链接后, 二者之间通信的密文长度为 16 Byte. 而在用户与私有云建立链接完成认证的过程中, 通信的密文长度为 $22|p| + 16$ Byte, 建立安全链接后, 二者之间通信的密文长度为 34 Byte.

各通信阶段的消息长度如表 1 所示, 为了建立安全的通信连接, 本方案会形成一个较大的消息密文, 但当连接建立之后, 用户和云之间通信的消息密文长度会大大缩短.

表 1　密文长度

Table 1　Length of ciphertext

实体之间	加密 (Byte)	解密
用户 – 公有云建立连接	$22\|p\|$	1
用户 – 公有云数据传输	16	1
用户 – 私有云建立连接	$22\|p\|+16$	1
用户 – 私有云数据传输	34	1

密文长度与不同安全强度的关系如图 4 所示, 可以看出, 在建立通信链接进行认证时, 密文长度与安全强度成线性关系, 安全强度越高, 密文越长当用户完成认证进行数据传输时, 密文长度不依赖于安全强度.

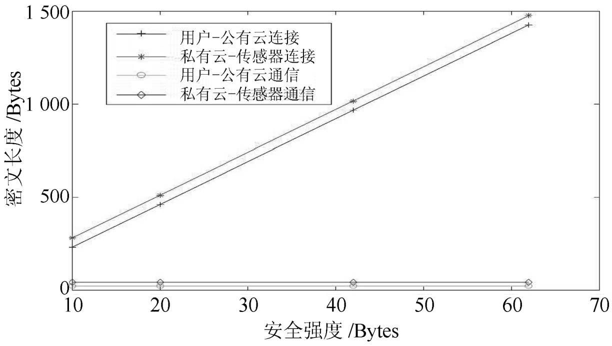


图 4　密文长度与安全强度关系图

Fig. 4　Relationship between the ciphertext size and the security level

3.3.2　通信消耗

该方案的通信消耗主要集中在用户从公有云获取密文的通信及用户发送指令到私有云的通信, 因此密文长度直接影响了通信消耗.

表 1 可以看出, 为了建立安全的通信连接, 本方案会形成一个较大的密文长度, 但当连接建立之后, 用户和公有云之间的通信密文长度会大大缩短, 由于密文长度直接决定了通信能量损耗与计算开销, 因此在通信相对频繁时, 本方案较短的密文长度能够保证更低的能量损耗与更小的计算开销.

3.3.3　计算开销

该节将本方案与传统的基于证书的认证、基于默克尔树的认证和基于身份的认证方法进行比较, 分析计算开销. 根据文献 [27], 在主频 400 MHz 的 32 位微处理器上计算 Tate 对大约需要 62.04 ms, 校验一次 ECDSA-160 签名需要耗时 18.48 ms, 由于哈希算法和对称加密算法有着极低的计算开销, 此处忽略了哈希算法和对称加密算法的开销.

假设每个数据用户进行 N 次数据交互, 在基于证书的算法中, 计算开销主要由两次 ECDSA 签名认证产生, 总开销为 $2 \times 18.48N = 36.96N$ ms; 在基于默克尔树的认证方法中, 计算开销主要是一次 ECDSA 签名认证, 因此开销为 $18.48N$ ms; 基于身份的认证方法中, 计算开销主要为两次 Tate 对计算, 总计算开销为 $2 \times 62.04N = 124.08N$ ms. 本文提出的算法中, 数据用户与公有云或私有云通信进行身份认证的计算开销主要为 22 次 Tate 对, 总开销为 $22 \times 62.04N = 1\,364.88N$ ms, 认证完成后, 在会话密钥更新之前, 用户无需再计算 Tate 对表 2 展示了计算开销对比.

从表 2 可以得出以下结论: 在数据传输次数较少时, 本方案由于注重安全性认证, 因此产生较大的计算开销, 在认证完成后, 无需再进行重复认证, 因此随着数据传输次数的增加 ($N > 11$), 在相同传输次数条件下, 本文方案计算开销低的优势逐步体现.

表 2　计算开销

Table 2　Computation overhead

方案	计算开销 (ms)
基于证书的认证	$36.96N$
基于默克尔树的认证	$18.48N$
基于身份的认证	$124.08N$
数据用户与公有云或私有云的通信	$1\,364.88N$

3.4　实验仿真

本节通过仿真实验验证算法整体的计算开销. 实验采用斯坦福大学开发的基于 JAVA 的双线性对密码库 (PBC Library), 椭圆曲线采用 Type A: $y^2 = x^3 + x$. 实验环境为 Inter (R) Core (TM) i5-3230M 2.60 GHz CPU, 12.00 GB 内存, Windows7 64 bit 操作系统. 实验中对称加密采用 128 bit AES 加密算法, 不计实际应用中的数据传输延时. 实验对

算法最关键的初始化、私钥生成、加密、解密这 4 个步骤进行仿真, 结果如图 5～8 所示. 算法在属性个数不断增加的情况下, 消耗时间也随之增加. 这是因为随着属性个数增多, 算法需生成的属性值、密文组件及需解密的组件均随之增多.

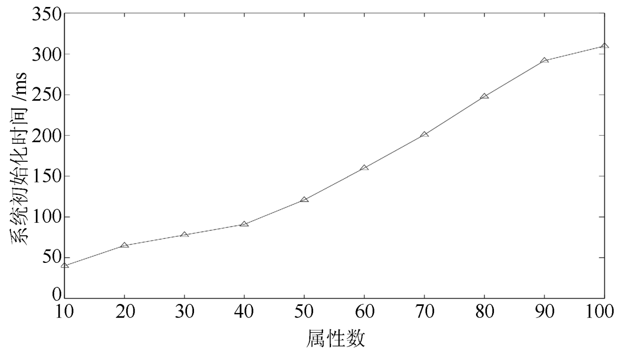


图 5　系统初始化时间

Fig. 5　Setup time

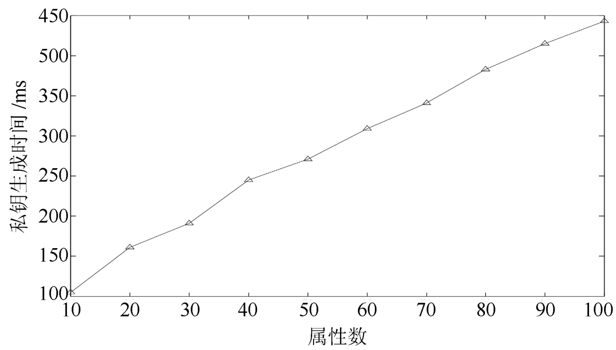


图 6　私钥生成时间

Fig. 6　Private key generation time

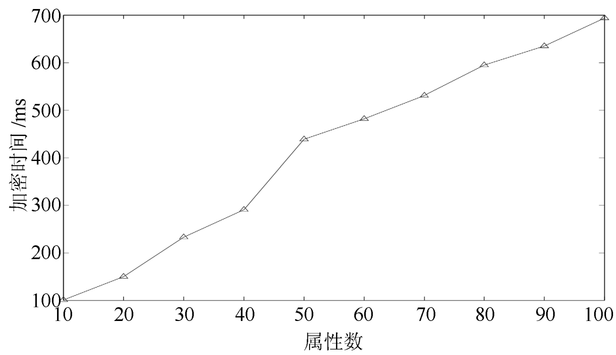


图 7　加密时间

Fig. 7　Encryption time

从以上仿真可见, 当属性个数达到 100, 系统仍能够保持一个较短的运行时间, 在实际应用中, 数据属主可灵活设定访问策略, 实现细粒度的访问控制.

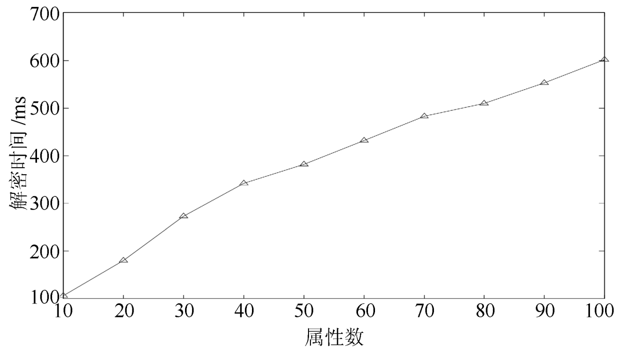


图 8　解密时间

Fig. 8　Decryption time

4　结束语

本文为面向云端辅助的工业控制系统的数据传输、存储、访问设计了一种安全机制, 利用基于属性的访问控制方法, 对用户进行身份授权及认证, 为其与控制系统之间建立安全的通信连接, 并对存储数据进行完整性检查, 解决了数据的机密性、完整性保护问题. 通过性能分析并与已有方案的比较, 本方案的性能随着数据传输次数的增加 (N >11), 其优势逐步体现.

References

1 Sajid A, Abbas H, Saleem K. Cloud-assisted IoT-based SCADA systems security: A review of the state of the art and future challenges. *IEEE Access*, 2016, **4**: 1375−1384

2 Langmann R, Rojas-Peña L F. A PLC as an industry 4.0 component. In: Proceedings of the 13th International Conference on Remote Engineering and Virtual Instrumentation (REV). Madrid, Spain: IEEE, 2016. 10−15

3 Wan J F, Tang S L, Shu Z G, Li D, Wang S Y, Imran M, et al. Software-defined industrial internet of things in the context of industry 4.0. *IEEE Sensors Journal*, 2016, **16**(20): 7373−7380

4 Goldin E, Feldman D, Georgoulas G, Castano M, Nikolakopoulos G. Cloud computing for big data analytics in the process control industry. In: Proceedings of the 25th Mediterranean Conference on Control and Automation (MED). Valletta, Malta: IEEE, 2017. 1373−1378

5 Xia Yuan-Qing. Cloud control systems and their challenges. *Acta Automatica Sinica*, 2016, **42**(1): 1−12
(夏元清. 云控制系统及其面临的挑战. 自动化学报, 2016, **42**(1): 1−12)

6 Farwell J P, Rohozinski R. Stuxnet and the future of cyber war. *Survival*, 2011, **53**(1): 23−40

7 Zhou Xiao-Feng, Chen Xiu-Zhen. Gray analytical hierarchical assessment model for industry control system security. *Netinfo Security*, 2014, (1): 15−20
(周小峰, 陈秀真. 面向工业控制系统的灰色层次信息安全评估模型. 信息网络安全, 2014, (1): 15−20)

8 Singh A, Prasad A, Talwar Y. SCADA security issues and FPGA implementation of AES — A review. In: Proceedings of the 2nd International Conference on Next Generation Computing Technologies (NGCT). Dehradun, India: IEEE, 2016. 899−904

9 Liang Yao, Feng Dong-Qin, Xu Shan-Shan, Chen Si-Yuan, Gao Meng-Zhou. Feasibility analysis of encrypted transmission on security of industrial control systems. *Acta Automatica Sinica*, 2018, **44**(3): 434−442
(梁耀, 冯冬芹, 徐珊珊, 陈思媛, 高梦州. 加密传输在工控系统安全中的可行性研究. 自动化学报, 2018, **44**(3): 434−442)

10 Zhou X J, Xu Z, Wang L M, Chen K. What should we do? A structured review of scada system cyber security standards. In: Proceedings of the 4th International Conference on Control, Decision and Information Technologies (CoDIT). Barcelona, Spain: IEEE, 2017. 605−614

11 Lu Geng-Hong, Feng Dong-Qin. Modeling of the industrial control network situation awareness based on particle Filtering. Acta Automatica Sinica, 2018, **44**(8): 1405−1412
(陆耿虹, 冯冬芹. 基于粒子滤波的工业控制网络态势感知建模. 自动化学报, 2018, **44**(8): 1405−1412)

12 Shahzad A, Musa S, Aborujilah A, Irfan M. Industrial control systems (ICSs) vulnerabilities analysis and SCADA security enhancement using testbed encryption. In: Proceedings of the 8th International Conference on Ubiquitous Information Management and Communication. Siem Reap, Cambodia: Elsevier, 2014. 1−7

13 Oualha N, Olivereau A, Boudguiga A. Pseudonymous communications in secure industrial wireless sensor networks. In: Proceedings of the 11th Annual Conference on Privacy, Security and Trust. Tarragona, Spain: IEEE, 2013. 98−102

14 Halas M, Bestak I, Orgon M, Kovac A. Performance measurement of encryption algorithms and their effect on real running in PLC networks. In: Proceedings of the 35th International Conference on Telecommunications and Signal Processing (TSP). Prague, Czech Republic: IEEE, 2012. 161−164

15 Bere M, Muyingi H. Initial investigation of industrial control system (ICS) security using artificial immune system (AIS). In: Proceedings of the 2015 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC). Windhoek, Namibia: IEEE, 2015. 79−84

16 Morrow B. BYOD security challenges: control and protect your most sensitive data. *Network Security*, 2012, **2012**(12): 5−8

17 Cazorla L, Alcaraz C, Lopez J. Cyber stealth attacks in critical information infrastructures. *IEEE Systems Journal*, 2018, **12**(2): 1778−1792

18 Jenkins J, Burmester M. Protecting infrastructure assets from real-time and run-time threats. In: Proceedings of the 7th International Conference on Critical Infrastructure Protection VII. Washington, USA: Springer, 2013. 97−110

19 Ding Xin-Zhi, Li Hui-Jie, Yang Hui-Xia, Zhang Xi-Ling, Liu Zhu-Kui. Present situation analysis and prospect for international standards system based on IEC/TC 57. *Power System Protection and Control*, 2014, **42**(21): 145−154
(丁心志, 李慧杰, 杨慧霞, 张喜玲, 刘柱揆. 基于 IEC/TC57 国际标准体系现状分析研究与展望. 电力系统保护与控制, 2014, **42**(21): 145−154)

20 Sandhu R S, Coyne E J, Feinstein H L, Youman C E. Role-based access control models. *Computer*, 1996, **29**(2): 38−47

21 Soni A, Keoh S L, Kumar S S, Garcia-Morchon O. Hada: hybrid access decision architecture for building automation and control systems. In: Proceedings of the 1st International Symposium on ICS & SCADA Cyber Security Research 2013. Swindon, UK: BCS, 2013. 1−11

22 Zhang Ting, Yang Geng, Teng Wei, Wang Dong-Yang. Access control method based on attribute and constant-size ciphertext in cloud computing. *Computer Technology and Development*, 2013, **23**(11): 128−132
(张婷, 杨庚, 滕玮, 王东阳. 云计算中基于属性和定长密文的访问控制方法. 计算机技术与发展, 2013, **23**(11): 128−132)

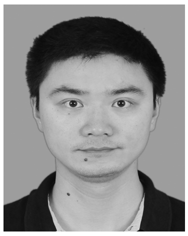
23 Feng Deng-Guo, Chen Cheng. Research on attribute-based cryptography. *Journal of Cryptologic Research*, 2014, **1**(1): 1−12
(冯登国, 陈成. 属性密码学研究. 密码学报, 2014, **1**(1): 1−12)

24 Yu S C, Wang C, Ren K, Lou W J. Attribute based data sharing with attribute revocation. In: Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security. Beijing, China: IEEE, 2010. 261−270

25 Zu L H, Liu Z H, Li J J. New ciphertext-policy attribute-based encryption with efficient revocation. In: Proceedings of the 4th International Conference on Computer and Information Technology. Xi′an, China: IEEE, 2014. 281−287

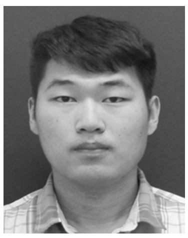
26 Colbert E J M, Kott A. *Cyber-Security of SCADA and Other Industrial Control Systems*. Switzerland: Springer International Publishing, 2016.

27 Hu C Q, Li H J, Huo Y, Xiang T, Liao X F. Secure and efficient data communication protocol for wireless body area networks. *IEEE Transactions on Multi-Scale Computing Systems*, 2016, **2**(2): 94−107



屠袁飞 南京邮电大学计算机学院博士研究生. 主要研究方向为网络安全, 云计算与访问控制. 本文通信作者.
E-mail: yuanfeitu@163.com.
(**TU Yuan-Fei** Ph. D. candidate at School of Computer Science, Nanjing University of Post & Telecommunication. His research interest covers network security, cloud computing and access control. Corresponding author of this paper.)

杨 庚 南京邮电大学计算机学院教授, 会员. 主要研究方向为网络安全, 分布与并行计算. E-mail: yangg@njupt.edu.cn
(**YANG Geng** Professor at the School of Computer Science, Nanjing University of Post & Telecommunication. His research interest covers network security, parallel & distributed computing.)



张成真 南京工业大学计算机科学与技术学院硕士研究生. 主要研究方向为云计算与信息安全.
E-mail: ddream-zhang@163.com
(**ZHANG Cheng-Zhen** Master student at the School of Computer Science, Nanjing Tech University. His research interest covers cloud computing and information security.)