# IBEXSec：一种面向工业互联网终端的通用安全服务框架

陈园，陈铁明，宋琪杰，马栋捷

（浙江工业大学计算机科学与技术学院，浙江 杭州 310023）

**摘　要：**随着工业互联网平台的应用发展，海量异构终端的安全隐患亟待解决。针对当前面临的工业互联网终端接入与数据传输的安全问题，提出一种基于身份公钥密码服务（IBE-XKMS）的终端安全通用服务框架——IBEXSec，支持工业互联网异构终端设备的安全接入、认证代理、跨域通信、隐私保护等安全功能。

**关键词：**工业互联网；终端设备；安全认证；身份公钥；密钥管理

**中图分类号：**TP309

**文献标识码：**A

**doi:** 10.11959/j.issn.1000−0801.2020069

# IBEXSec: a universal security framework for industrial internet terminal access

CHEN Yuan, CHEN Tieming, SONG Qijie, MA Dongjie

College of Computer Science and Technology, Zhejiang University of Technology, Hangzhou 310023, China

**Abstracts:** With the development and application of the industrial internet platform, the security risks of massive heterogeneous terminals need to be solved urgently. Aiming at the current industrial internet terminal access and data transmission security problems, a universal terminal security service framework called IBEXSec based on the identity public key cryptographic service (IBE-XKMS) was proposed to support security functions such as secure access, authentication agents, cross-domain communications and privacy protection of heterogeneous terminal devices on the industrial internet.

**Key words:** industrial internet, terminal device, security authentication, IBE, key management

## 1　引言

工业互联网终端设备为了实现智能化，集成越来越多的传感器，产生了大量的数据，伴随而来的是数据泄露等安全问题。海量终端异构设备接入工业互联网进行信息交换和数据通信，应用场景复杂，因此安全防护变得更复杂，传统的安全防护手段无法直接应用于工业互联网环境。

**收稿日期：**2020−02−10；**修回日期：**2020−03−04

**通信作者：**陈铁明，tmchen@zjut.edu.cn

**基金项目：**2019 年工业互联网创新发展工程-工业互联网网络安全公共服务平台项目（No.TC190H3WN）；国网浙江省电力有限公司科技项目（No.5211XT19006B）

**Foundation Items:** 2019 Industrial Internet Innovation and Development Project-Industrial Internet Cyber Security Public Service Platform Project (No.TC190H3WN), Science and Technology Project of State Grid Zhejiang Electric Power Co., Ltd. (No.5211XT19006B)

无线接入是工业互联网实现终端设备快速便捷接入的重要技术。随着4G的普及与5G的发展，无线接入能力大大提高，但传统的接入认证存在严重的安全问题。目前，学术界在设备安全接入认证问题上的研究成果大多围绕公钥认证。公钥基础设施（public key infrastructure，PKI）是目前使用最普遍的一种安全应用架构，然而PKI笨重的公钥证书管理和复杂的处理逻辑极大阻碍了PKI系统在工业互联网中的应用。由此无证书公钥技术成为研究热点，其中基于身份的公钥加密（identity based encryption，IBE）体制最为引人注目。陈铁明等[1]提出基于XML的IBE密钥管理服务体系——IBE-XKMS，解决传统IBE方案跨域通信的问题。本文结合工业互联网中终端计算能力有限、不支持或难以实现公钥计算的特性，针对设备数据安全传输、数据共享等问题，设计了基于IBE-XKMS的IBEXSec框架。框架中网关对本地设备进行代理，向IBE-XKMS请求公钥加密运算，减轻终端设备的计算压力。

## 2 研究现状

### 2.1 终端设备的安全认证

终端设备的接入认证是确保工业互联网安全的第一道屏障，是工业互联网安全中不容忽视的难题。随着科技的发展，终端设备的计算能力、存储能力不断提高，身份认证技术也从简单的用户名/口令，逐渐发展到智能卡、动态口令、数字证书、生物特征识别、动态密码以及多因素认证。终端身份认证的目的是防范非法接入和访问、假冒、抵赖、重放攻击等威胁，防止一切可能伪造和抵赖的因素。近几年，众多学者聚焦物联网系统的设备身份认证，提出了多种认证协议。这些协议可以分为两类：一类是基于计算成本低、消耗资源少的对称加密算法，该类协议迎合物联网终端设备资源有限和计算能力低的特性；另一类是基于计算量较大、安全性较高的非对称加密算法。

Sathyadevan等[2]针对户外极端受限的终端设备，提出一种轻量级的动态密钥认证方案（Protean），该方案使用对称加密算法，设备每次和网关进行认证时，都会发送下一次通信的加密密钥，但是该方案基于特定安全硬件，无法适配大部分应用场景；杨力等[3]提出一种可信的匿名无线认证协议，该协议使用对称加密算法，在认证过程中，每阶段使用临时身份和不同的一次性密钥，确保安全性，但认证过程中需要进行多次加/解密运算，计算代价大，不适合用于无线网络；谌双双等[4]提出基于PKI的通用无线认证协议（GWAP），引入可信证书验证代理和证书有效性凭据，该协议通过证书有效性凭据完成证书的有效性检查及公钥的传递，降低通信开销；周彦伟等[5]提出一种基于身份哈希证明系统的抵抗泄露攻击的可撤销IBE机制，进一步增强安全性和抗泄露能力；鲁阳[6]设计一种终端设备的身份标识，并提出一种基于身份标识的轻量化认证算法，降低终端设备认证过程中的计算量；张鑫等[7]提出了一种移动异步可信接入认证协议，传感器节点和移动宿节点经过身份验证后，便实现相互身份验证和密钥协商。这些认证协议都旨在降低通信开销、降低计算量、缩短认证时间或提高安全性，但还是无法兼顾安全性和高效性。

### 2.2 IBE-XKMS密码服务

IBE公钥密码体制以唯一标识用户身份的信息作为用户的公钥，无需数字证书。在IBE系统中，用户的公钥从用户的身份信息中得到，其相应的私钥由可信第三方密钥服务器产生。1984年，Shamir[8]最早提出由基于身份加密（IBE）和基于身份签名（IBS）组成的基于身份的公钥密码体制（IBC），并证明该方案对于选择密文攻击（chosen ciphertext attack，CCA）是安全的。随后，Tananka[9]为了解决不抵抗合谋攻击的问题，引入了门限的概念，提出基于离散对数难题和大整数分解难题的改善IBE方案。2001年，Boneh等[10]提出基于

双线性映射、Weil 配对原理的 BF-IBE 方案，这是第一个真正实用的 IBE 方案。此后，大量使用双线性映射函数构造的 IBE 方案被提出。

2010 年，陈铁明等[1]针对 IBE 方案存在的 PKG 集中式密钥托管风险和跨域通信问题，研究提出基于 XML 的 IBE 密钥管理服务体系：IBE-XKMS 服务。IBE-XKMS 将 IBE 的密钥管理扩展到 Web services，该系统可支持不同域、不同参数的分布式 PKG 和各类基于 IBE 的安全应用开发所需的密钥安全管理服务，实现更灵活、更便捷的 IBE 安全服务。

## 3　IBEXSec 框架

PKI 利用可信第三方 CA 颁布公钥证书来绑定公钥和身份信息，然而 PKI 需要搭建复杂的 CA 系统，且证书的生成、分发、撤销、验证和存储均需占用较多资源。而 IBE 不依赖于数字证书，认证效率较高，占用资源少，显然比 PKI 更适合用于工业互联网的设备认证。基于 XML 的 IBE 密钥管理服务体系——IBE-XKMS 解决了 IBE 方案中 PKG 集中式密钥托管风险的问题，并集成了跨域通信功能，但没有考虑设备信息泄露的问题。基于现有的 IBE-XKMS 服务，结合隐私保护技术，本文构建一种名为 IBEXSec 的面向工业互联网终端安全服务框架。IBEXSec 框架结构如图 1 所示。

第一层为工业互联网终端设备层，主要为海量异构工业设备；第二层为接入层，主要是网关，通过支持异构协议以接入各种工业互联网终端设备，并负责请求 IBE-XKMS 服务和管理设备私钥；第三层为云平台层，支持存储、计算、分析、管理等一系列云服务。在终端设备层，传感器、电表等设备资源有限，不适合执行复杂的公钥加密运算，因此 IBEXSec 框架提出网关对本地设备进行代理，向 IBE-XKMS 请求公钥加密运算的方案，将复杂的加密运算迁移到 IBE-XKMS，减轻终端设备的计算压力，同时也确保设备数据从网关到云端的安全传输。

设备在首次接入网关后，需要进行身份注册，由网关负责将设备身份信息发送至 IBE-XKMS 请求 Register 服务，生成设备私钥。为防止终端设备存在的克隆攻击等安全隐患，设备私钥存储在安全性等级更高的网关。出于对工业互联网部分终端设备功能设定和云服务器存储压力的考虑，部分终端设备并不一直保持连接传输数据（例如烟雾报警器，当烟雾的浓度超过阈值时，才会连接网关上传异常数据），还有些设备为了节能会频

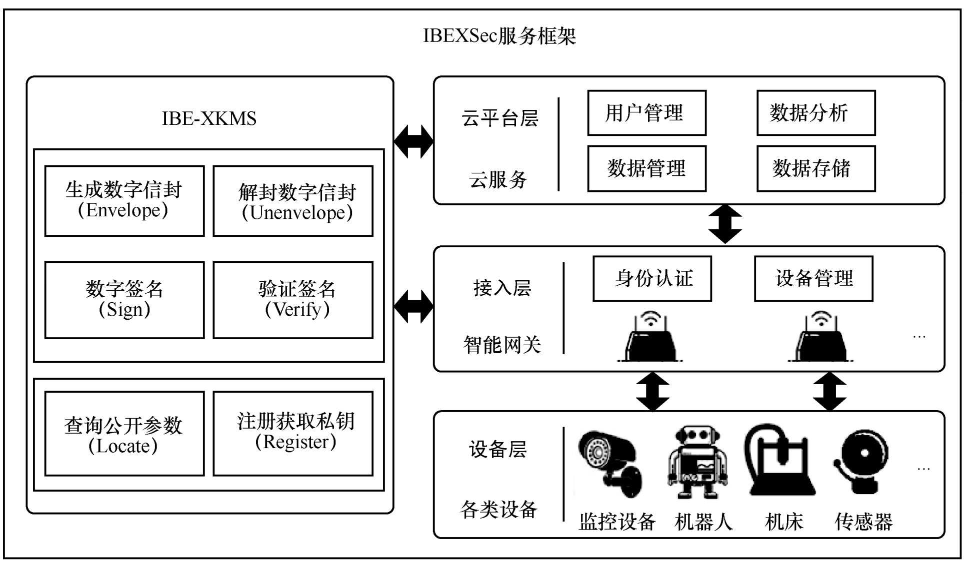



图 1　IBEXSec 框架结构

繁进入休眠状态。当设备每次连接网关时，都需要进行身份认证。本框架假设设备与网关之间的所有通信都是安全的，安全隐患主要存在于网关与云平台层的交互中。

IBEXSec 框架支持设备跨域通信，利用网关向 IBE-XKMS 请求数字信封服务和解封数字信封服务，以完成复杂的数据加密与解密，不仅大大降低了设备的运算压力，也减少了低安全等级设备与设备之间通信潜在的安全问题。考虑大数据时代数据的价值，IBEXSec 框架设计了数据共享功能，支持用户请求共享设备存储在云端的数据，挖掘数据价值。

部分设备存在隐私泄露的安全风险，IBEXSec 框架设计了别名机制，支持设备利用别名发送数据。别名能有效隐藏真实设备身份信息，防止物理攻击，同时由于别名机制不用替换传统工业设备，大大降低了成本。

### 3.1 设备注册

在 IBEXSec 框架中，设备层终端首次接入网关后，需要进行身份注册，网关收集终端设备的身份信息后，需要请求 IBE-XKMS 服务，生成设备的私钥。IBEXSec 框架的符号描述见表 1。

表 1 IBEXSec 框架的符号描述

| 符号 | 描述 |
|---|---|
| ID_Device | 设备身份信息 |
| $SK_G$ | 网关私钥 |
| $PK_G$ | 网关公钥 |
| $SK_D$ | 设备私钥 |
| Exp | 密钥有效期 |
| $T$ | 时间戳 |
| PP | PKG 公开参数 |
| DN_ID | ID 所在域的域名 |
| Sign ($M$) | 表示对消息哈希 $H(M)$的 XML 数字签名 |
| $Enc_K(M)$ | 表示用密钥 $K$ 对消息 $M$ 加密 |
| Register | 身份注册服务，获取私钥 |
| Locate | 查询 ID 所在域的公开参数 |
| Envelope | 生成数字信封服务 |
| Unenvelope | 解封数字信封服务 |
| Verify | 验证签名服务 |

设备身份注册过程如图 2 所示，在身份注册阶段，网关获取设备信息后，提供相应的设备身份信息给 PKG，PKG 生成公钥，随后 PKG 使用私钥提取算法计算该设备的私钥，并生成一条利用网关公钥加密的信息（设备身份信息、设备私钥、PKG 公开参数）发送给网关，网关收到后用网关私钥解密，最后存储在网关安全存储区域。

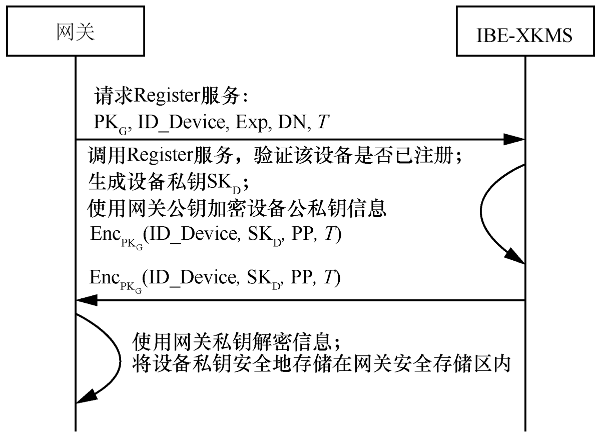



图 2 设备身份注册过程

### 3.2 跨域设备通信

IBEXSec 框架考虑设备间通信的需求，比如报警系统集成多个分布在不同区域的传感器，传感器采集到异常数据时需要触发报警，此时存在跨域通信的可能性。IBEXSec 框架中不同域设备间的通信过程如图 3 所示，设备 A、设备 B 分别属于不同域，有不同的 PKG 公开参数，设备 A 属于域 M，设备 B 属于域 N，设备 A 向设备 B 发送数据。假设在设备 A 和设备 B 传输数据之前，都已经完成身份认证，并且设备与网关之间的通信是安全的。设备 B 一侧的网关在接收到信息之后，也可以选择用存储在网关的设备 B 私钥解密使用设备 B 公钥加密的对称加密密钥 $K$，再向 IBE-XKMS 请求签名验证服务。

### 3.3 数据传输与共享

在大数据和云计算时代，数据拥有巨大的价值，数据开放共享是一种趋势。但目前大数据产业存在资源开放共享程度低、数据价值难以被有

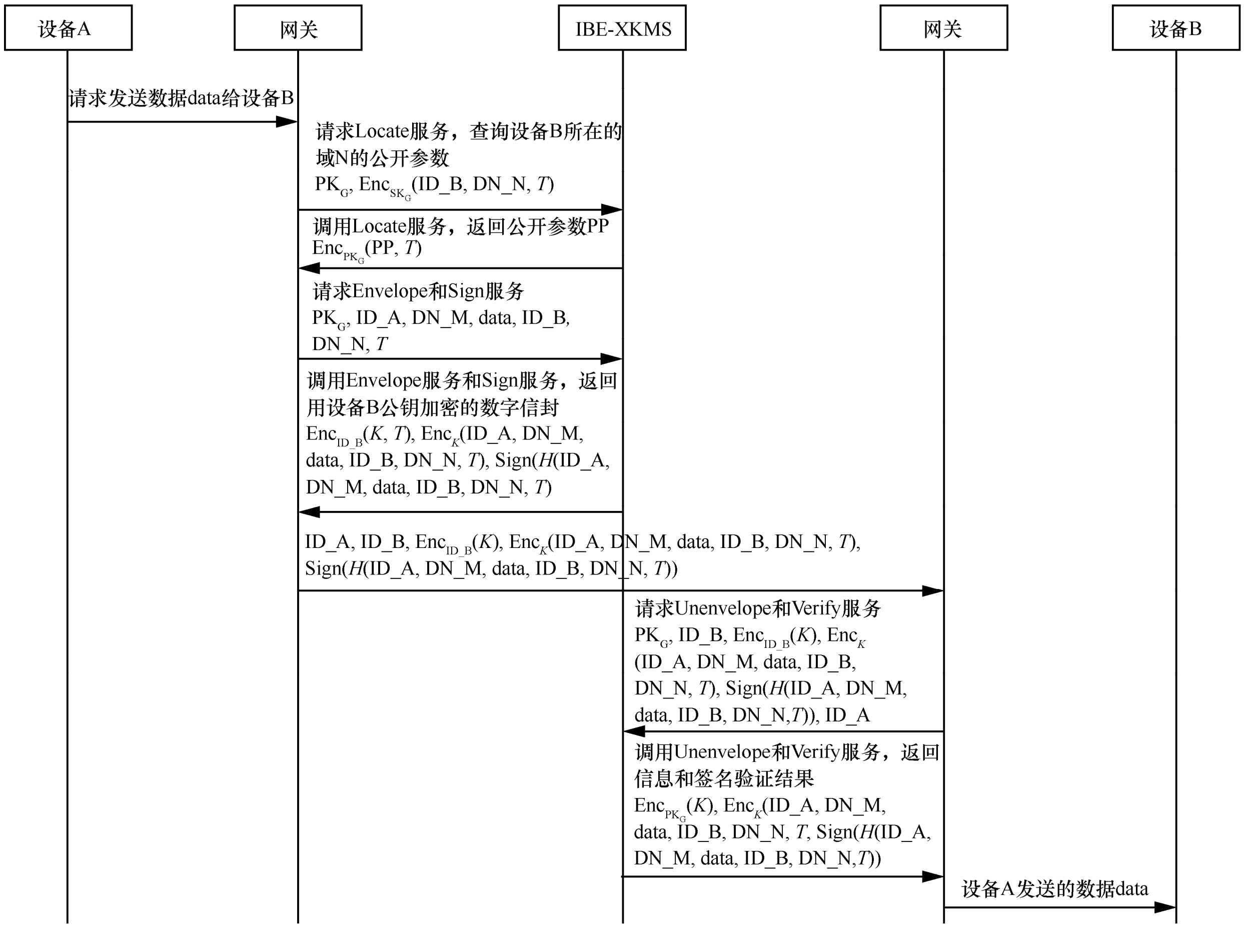



图 3　IBEXSec 框架中不同域设备间的通信过程

效地挖掘利用、安全性有待加强等问题。因此，IBEXSec 框架考虑数据开放共享的需求，设计数据安全传输和共享模块。

设备和网关建立连接后，需要将数据上传至云平台层。由于数据的传输量较大，安全性要求不高，因此使用加密速度较快、性能较高的对称加密算法。用户请求数据共享过程如图 4 所示，设备请求数据存储服务，上传数据，网关向 IBE-XKMS 请求数字信封服务，生成使用设备公钥加密的对称加密密钥和使用对称加密密钥加密的数据。存储在云服务器的数据可调用管理服务设置数据查看权限与有效期限。若用户取得权限并在有效期内，云平台向 IBE-XKMS 请求解封数字信封服务，获得解密数据后调用数据管理服务，将数据安全地发送给用户。

由于每次使用的对称加密密钥都不相同，即使攻击者窃取一部分数据，也不影响其他数据的安全。

## 3.4　隐私保护

传统的网络边界瓦解，工业大数据开放共享，设备内置越来越多的传感器，短时期内传统的、有安全隐患的工业终端设备不会被替换，这给攻击者提供了攻击途径。因此，在进行设备认证和数据传输的时候，保护设备信息是一种有效手段，可以不用替换传统设备，成本较低。

未来的终端设备是传感器高度融合的，由多个传感器组成，每个传感器的功能可能不尽相同，多个传感器共同协作。一种情况是在数据共享中，用户请求的数据可能只是某一类数据，比如一个设备同时内置了温度传感器、湿度传感器、重力

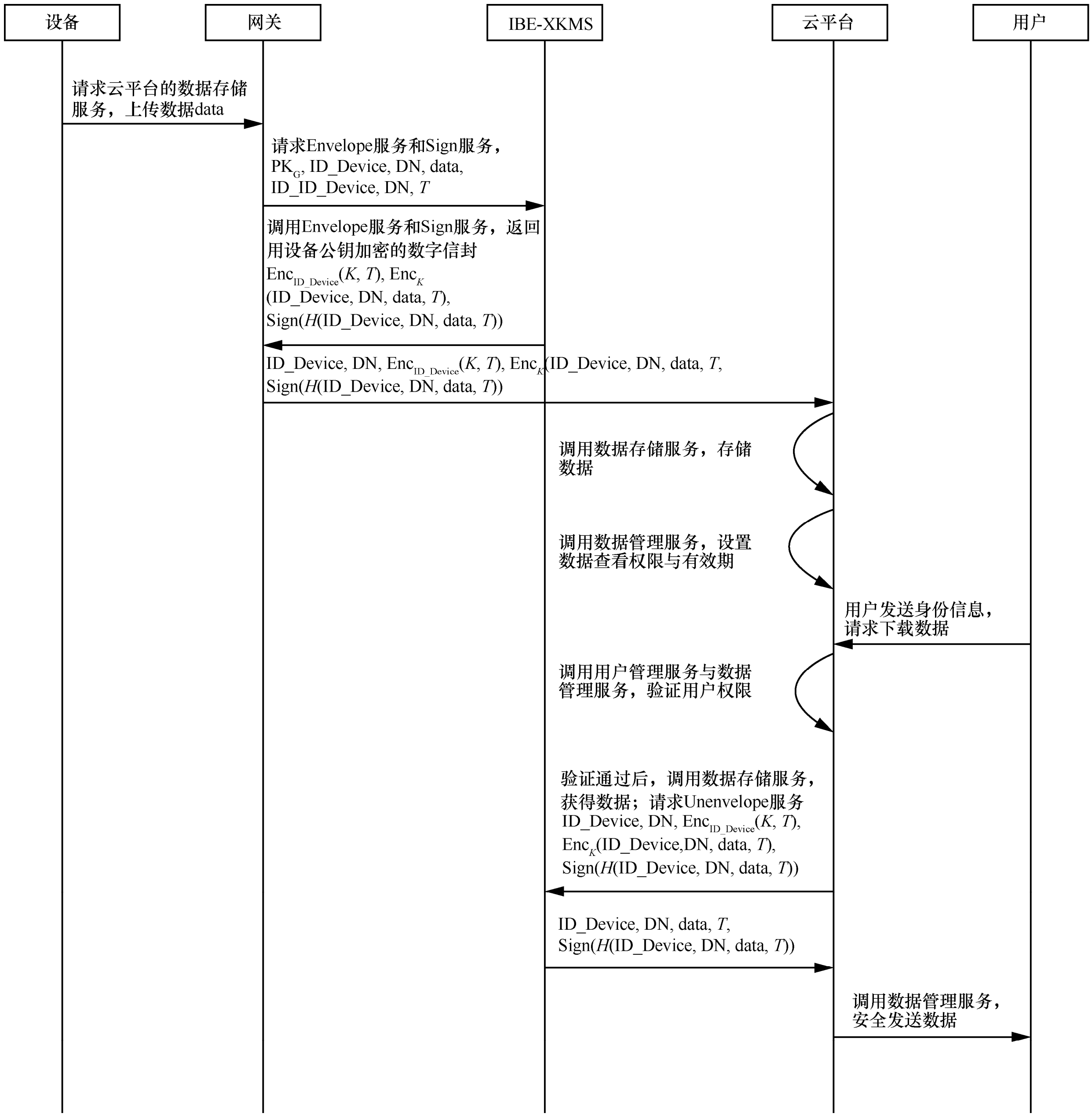



图 4　用户请求数据共享过程

传感器、光电传感器、压力传感器等，然而用户只需要其中的温度数据；另一种情况是为保护设备隐私，隐藏设备真实信息，此时可申请设备的别名，别名与设备无关，基于第一种情况，别名的设置可与传感器有关。网关为别名请求 IBE-XKMS 服务申请公私钥时，会在网关维护的别名表中增加一条记录，别名表格式如图 5 所示，其中 $PK_S$ 表示传感器公钥，$SK_S$ 表示传感器私钥，$Exp_S$ 表示传感器公钥有效期，ID_Device 表示设备身份信息，Exp 表示设备公钥有效期。当超过设备公钥或者传感器公钥的有效期时，删除此条记录。

| | | | | |
|---|---|---|---|---|
| $PK_S$ | $SK_S$ | $Exp_S$ | ID_Device | Exp |

图 5　网关维护的别名表

终端设备在本地也会维护一张别名表，格式如图 6 所示，其中，ID_Sensor 表示传感器信息，

当设备需要匿名时，可用别名发送数据，外部人员将无法找到该真实设备，故无法实施攻击。别名表存储在设备的安全数据和程序存储区。

| | | |
|---|---|---|
| $PK_s$ | $Exp_s$ | ID_Sensor |

图 6　设备维护的别名表

## 4　安全性分析

在分析过程中，假设每个设备的私钥只被其对应的网关代理拥有，其他设备拥有公钥，并且私钥被窃取的可能性非常低；假设终端设备与网关之间的通信是安全的。

### 4.1　重放攻击

重放攻击（replay attack）是一种常见的网络攻击方式，主要由攻击者通过恶意地重传或重放以前发送的信息来实现。重放攻击可分为两种情况：一种是模仿网关，另一种是模仿云端服务器。由于网关和云端服务器的通信信息都是通过 IBE-XKMS 服务生成的 XML 数字信封，且都包含时间戳，若信息超时则丢弃该信息，所以无论攻击者模仿网关还是云端服务器，重放攻击都会失败。综上所述，IBEXSec 框架可以抵抗重放攻击。

### 4.2　中间人攻击

中间人攻击（man-in-the-middle attack，MITM 攻击）是一种常见的网络攻击方式，主要通过拦截正常的网络通信数据并进行数据篡改和嗅探，而通信双方毫不知情。攻击者可以接收两个受害者之间交换的所有信息，并可以篡改信息再重新发送。在 IBEXSec 框架中，跨域设备在通信之前都会先进行身份认证，网关对本地设备进行代理，向可靠第三方密钥管理中心 IBE-XKMS 请求服务之前也要进行身份认证，并且对于重要的通信信息，设备的网关代理会请求 Sign 签名服务和加密服务，而攻击者无法获取设备私钥，即使获取了信息也无法篡改签名信息，攻击者无法获取设备私钥就无法解密信息。因此，IBEXSec 框架可以抵抗中间人攻击。

### 4.3　前向保密性

前向保密性确保一个密钥泄露，其他密钥也不会被破解。因为每当设备传输数据，网关都会请求数字信封服务，会生成新的加密密钥，所以即使攻击者破解了当前的加密密钥，也无法破解其他的加密密钥。而且每个密钥都是独立生成的，即使攻击者破解了之前使用过的加密密钥，也不会增加成功破解其他加密密钥的概率。因此，IBEXSec 框架拥有前向保密性，即使泄露了一个密钥，也无法影响以前和未来的数据传输的安全性。

### 4.4　设备匿名性

设备可以选择用别名发送数据来对设备匿名处理，由于别名的设置与设备无关、与传感器有关，但是在工业互联网中，传感器的种类和数量都有很大规模，所以攻击者无法识别真实的设备，保证设备的匿名性。

## 5　结束语

针对工业互联网终端设备安全通信、数据传输与共享、保护设备信息的需求，本文提出一种面向工业互联网终端的安全服务框架——IBEXSec 框架。该服务框架以 IBE-XKMS 技术为基础，结合隐私保护技术，实现对终端设备的身份注册、数据安全传输与共享，并提供设备匿名的功能，同时将复杂的加解密运算交给网关代理和 IBE-XKMS 服务，大大减轻了资源受限终端设备的计算压力。

IBEXSec 框架仍然可以在移动终端设备认证、设备多级管理等方面进行改进，如跨域后设备的身份认证问题与数据传输问题。下一步，笔者将重点研究 IBEXSec 框架的新功能以健全该框架功能的多样性与全面性以及利用机器学习对接入设备的智能识别与认证方法，提高身份认证的效率。

## 参考文献：


[1] 陈铁明, 李伟, 蔡家楣, 等. IBE-XKMS: 一个基于 XML 的 IBE 密钥管理服务体系[J]. 电信科学, 2010, 26(7): 22-31.
CHEN T M, LI W, CAI J M, et al. IBE-XKMS: XML-based IBE key management service infrastructure[J]. Telecommunications Science, 2010, 26(7): 22-31.

[2] SATHYADEVAN S, ACHUTHAN K, DOSS R, et al. Protean authentication scheme–a time-bound dynamic KeyGen authentication technique for IoT edge nodes in outdoor deployments[J]. IEEE Access, 2019: 92419-92435.

[3] 杨力, 马建峰, 朱建明. 可信的匿名无线认证协议[J]. 通信学报, 2009, 30(9): 29-35.
YANG L, MA J F, ZHU J M. Trusted and anonymous authentication scheme for wireless networks[J]. Journal on Communications, 2009, 30(9): 29-35.

[4] 谌双双, 陈泽茂, 王浩. 基于 PKI 的通用无线认证协议研究[J]. 计算机科学, 2012, 39(7): 74-77.
CHEN S S, CHEN Z M, WANG H. Research on general wireless authentication protocol based on PKI[J]. Computer Science, 2012, 39(7): 74-77.

[5] 周彦伟, 杨波, 夏喆, 等. 抵抗泄露攻击的可撤销 IBE 机制[J]. 计算机学报, 2020: 1-28.
ZHOU Y W, YANG B, XIA Z, et al. Revocable identity-based encryption scheme with leakage-resilience[J]. Chinese Journal of Computers, 2020: 1-28.

[6] 鲁阳. 物联网终端可信认证与自动接入技术研究与实现[D]. 南京: 南京邮电大学, 2019.
LU Y. Research and implementation of terminal authentication and automatic access technology in IoT[D]. Nanjing: Nanjing University of Posts and Telecommunications, 2019.

[7] 张鑫, 杨晓元, 朱率率, 等. 物联网环境下移动节点可信接入认证协议[J]. 计算机应用, 2016, 36(11): 3108-3112.
ZHANG X, YANG X Y, ZHU S S, et al. Trusted access authentication protocol for mobile nodes in internet of things[J]. Journal of Computer Applications, 2016, 36(11): 3108-3112.

[8] SHAMIR A. Identity-based cryptosystems and signature schemes[C]//Proceedings of Annual International Cryptology CRYOTO 1984: Conference Advances in Cryptology. Berlin: Springer, 1984: 47-53.

[9] TANAKA H. A realization scheme for the identity-based cryptosystem[C]//Proceedings of Conference on the Theory and Applications of Cryptographic Techniques, Advances in Cryptology-CRYPTO 1987. Berlin: Springer, 1987: 340-349.

[10] BONEH D, FRANKLIN M. Identity-based encryption from the weil pairing[C]//Proceedings of Annual International Cryptology Conference, Advances in Cryptology—CRYPTO 2001. Berlin: Springer, 2001: 213-229.

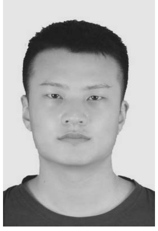
[11] COCKS C. An identity based encryption scheme based on quadratic residues[C]//Proceedings of IMA International Conference on Cryptography and Coding, Cryptography and Coding 2001. Berlin: Springer, 2001: 360-363.



[作者简介]

**陈园**（1994− ），女，浙江工业大学计算机科学与技术学院硕士生，主要研究方向为物联网安全。

**陈铁明**（1978− ），男，博士，浙江工业大学计算机科学与技术学院教授、博士生导师，主要研究方向为网络空间安全、大数据分析。



**宋琪杰**（1994− ），男，浙江工业大学计算机科学与技术学院硕士生，主要研究方向为区块链和物联网安全。

**马栋捷**（1994− ），男，浙江工业大学计算机科学与技术学院硕士生，主要研究方向为信息安全。