面向工业物联网的无配对数据高效验证和聚合协议

马蓉，冯涛
（兰州理工大学计算机与通信学院，甘肃 兰州 730050）

摘　要：作为智能制造的支撑技术，工业物联网利用高效的数据共享驱动着工业生产的网络化、数字化、智能化，有助于制造企业降本增效，提升自身核心竞争力。然而因为工业生产现场设备自身资源的有限性使得维护系统安全的计算成本高昂且无法抵御各种攻击等缺陷极大地阻碍了其发展。因此，为了解决这些难题，提供工业系统稳健性、维护安全目标和提高效率，提出了一种无配对的数据高效验证和聚合（EUVA）协议。在基于椭圆加密算法的工业物联网环境中，使用同态加密技术提供数据隐私保护，并提供验证密钥管理方案，从而实现安全、高效的无配对验证。此外，通过安全性分析表明所提协议满足所提的安全目标。最后，通过MIRACL进行的性能分析表明，所提出的EUVA协议在计算通信成本和能源开销方面优于先前的类似机制。

关键词：工业物联网；无配对验证；数据聚合；密钥管理；安全分析
中图分类号：TP393.0
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2024215

Efficient unpaired data validation and aggregation protocol in industrial Internet of things

MA Rong, FENG Tao
School of Computer and Communication, Lanzhou University of Technology, Lanzhou 730050, China

Abstract: As a cornerstone technology of smart manufacturing, the industrial Internet of things (IIoT) harnesses efficient data sharing to propel the networking, digitization, and intellectualization of industrial production, thereby assisting manufacturing enterprises in cost reduction, efficiency enhancement, and bolstering their core competitiveness. Nevertheless, the limited resources inherent in industrial production field devices have posed significant hurdles to IIoT's development, primarily due to the high computational costs of maintaining system security and vulnerabilities that render it susceptible to various attacks. To address these challenges and enhance the robustness, security, and efficiency of industrial systems, an efficient unpaired verification and aggregation (EUVA) protocol was proposed. Within the context of an IIoT environment based on elliptic curve cryptography, homomorphic encryption was emploied to safeguard data privacy and a verification key management scheme was introduced, facilitating secure and efficient unpaired verification. Furthermore, security analysis demonstrates that the proposed protocol meets the outlined security objectives. Finally, performance analysis conducted using MIRACL reveals that the EUVA protocol outperforms previous similar mechanisms in terms of computational communication costs and energy consumption.

Keywords: industrial Internet of things, unpaired verification, data aggregation, key management, security analysis

收稿日期：2024–10–08
通信作者：冯涛，fengt@lut.edu.cn
基金项目：国家自然科学基金资助项目（No.61762060, No.62162039）；甘肃省重点研发基金资助项目（No.23YFGA0060）；甘肃省优秀博士生基金资助项目（No.23JRRA837）
Foundation Items: The National Natural Science Foundation of China (No.61762060, No.62162039), The Key Research and Development Program of Gansu Province (No. 23YFGA0060), The Foundation for Excellent Doctoral Program of Gansu Province (No.23JRRA837)

0 引言

工业物联网（IIoT, industrial Internet of things）融合了信息技术（IT，information technology）和运营技术（OT, operational technology）利用传感器、执行器、控制器、其他智能设备和网络连接来捕获和分析从整个工业生产过程中提取的海量数据[1]，利用数据蕴含的内在价值做出智能决策，优化了企业的制造资源配置和制造过程，提升了生产的效率、安全性和可靠性，降低了能耗、物耗与维护成本，增强了企业的核心竞争力。随着工业物联网中连接设备的数量呈指数级增长[2]，一天之内就有数十亿数据被交换，几乎所有通信都是通过开放渠道完成的[3]，其中包含了大量的敏感机密信息。因此，攻击者就很容易进行一些如窃听、删除、篡改或滥用企业工厂的机密记录等恶意行为[4]，例如，中间人攻击者修改机器生产参数将导致严重的生产事故，甚至可能造成生命损失。因此，在IIoT环境中，数据隐私、身份验证、消息完整性等安全问题将成为主要关注点，以防止中间人、冒名顶替、数据篡改等攻击，这些攻击与实体身份验证和密钥交换等问题相关[5-6]。

要实现安全高效的数据共享系统，利用大数据技术对海量的工业数据进行处理与分析，可以将数据信息转化为科学决策（如产品的设计方案、制造方案、物料供应方案等），要实现对复杂而不确定的工业制造环境的灵活应对，提高企业的制造效率、降低企业的维护成本，则必须有效防止对IIoT的攻击。改进的真实密钥协议机制是IIoT环境的必要条件，它能在连接节点之间提供适当的身份验证和密钥交换，以防止敌手的恶意活动[7]。数据聚合则用于消除工业传感器所收集数据的冗余，从而减少了节点的能源消耗和计算成本，它也面临着由于IIoT其特殊应用场景下所带来的各类安全问题。

在IIoT系统的基本架构中，许多工业传感器被设置在各类工业设备中，以观察工业生产的实时状况。这些生产记录与各种参数相关联。这些收集到的记录通过开放式互联网连接转发到云端服务器。云端服务器收到生产记录并进行存储，然后转发给相关的专业团队，如管理人员或设计人员等，他们可以根据数据的分析与处理结果改进产品的设计方案、制造方案、物料供应方案等，以及对潜在生产风险进行提前预警处理。

鉴于IIoT现阶段所面临的安全和隐私挑战，本文提出一种无配对的数据高效验证和聚合（EUVA）协议，在基于椭圆曲线加密（ECC, elliptic curve cryptography）算法的IIoT环境中，使用同态加密技术聚合受保护的数据，并提供验证密钥管理方案，从而实现安全、真实的验证。在数据各个阶段有效防止敌手攻击，同时还能降低计算和通信成本。本文贡献如下。

1) 基于ECC的工业物联网环境中，使用同态加密技术提供数据隐私保护，并提供验证密钥管理方案，从而实现安全、真实的无配对验证。

2) 对聚合数据设定优先级顺序，所提出的协议数据聚合过程基于信息优先级。将具有相似信息优先级的特定密码文本连接在一起，分类汇总计算输出满足IIoT实际场景需求。

3) 对所提出的认证和聚合协议的安全性进行分析，并进一步采用安全模型来说明协议的语义安全性。

4) 通过MIRACL进行仿真实验的性能分析表明，在IIoT环境下，所提协议在持续计算、通信存储和能源开销方面的表现优于其他相关方案。

1 相关研究工作

在物联网设施的支持下，可实现对工业生产状况的在线跟踪和监测，随着智能工业设备的不断增加，工业数据的保密性、完整性和设备身份验证等安全问题层出不穷，其传感器实体的身份验证和密钥交换等安全问题引起了相关研究人员的充分关注。为了缓解密钥托管和证书存储问题，Shamir[8]提出了基于ID的密码系统（IBC）这一新理念，其中用户身份可用作公钥。但后来发现，基于双线性配对的协议计算成本非常高[9]。因此，为了解决这些问题，基于免配对的协议应运而生[10]。例如，Das等[11]提出了一种远程用户与服务器的验证方案。该方案由于不注重对收集到的数据进行分类，因此计算成本很高。Othman等[6]和Gupta等[12-13]发现，每种智能设备都面临着能耗、计算和存储容量不足的挑战。因此，数据聚合被用于减少智能设备在网络上传输信息时的能耗。Song等[14]主要通过使用云辅助WBAN的多功能数据聚合器来维护数据隐私。在空间方面，需要聚合多个实体数据；在时间方面，只考虑单个实体一天内不同时段的记录，从而降低了计算成本，因此该方案既稳健又能

保护数据的安全和隐私。Islam 等[15]提出了一种不使用配对操作的安全高效通信方法，利用形式安全分析 BAN 逻辑证明了 AKA 协议攻击的安全性。Maria 等[16]介绍了一种基于边缘计算和双重签名技术的方案，该方案可保护数据隐私。

Sowjanya 等[17]发现，需要一种增强型轻量级协议来提供用户与服务器之间的安全通信。因此，他们提出了一种基于 ECC 的验证方案。Li 等[18]的主要目标是为计算、通信成本和空间找到最佳解决方案。因此，他们提出了一种轻量级的相互验证协议，该协议能保护传输记录的机密性。此外，Yao 等[19]提出了一种基于对称密钥的认证协议方案，针对现有的一些基于对称密钥的方案存在不完善的前向保密性等缺陷，该方案提供了完美的密钥保密性。Zhang 等[20]通过使用聚合器提出了一种轻量级无证书的隐私保护安全协议。他们重点关注保持数据的完整性和保密性，成功地防止了一些攻击。Vivek 等[21]主要关注如何减少通信节点之间的延迟，通过使用 ASCII 十六进制 ECC 方法来实现。Othman 等[22]提出了一种隐私保护方案，该方案能够减少聚合过程中高通信和高能耗，并维护用户数据的隐私和完整性、验证参与节点等。Cheng 等[23]通过利用同态签名概念，设计了一种无证书安全协议，不仅能够节省能源还有效解决了密钥托管问题，实现了保密性和身份验证。Hurtado 等[24]通过应用卷积神经网络方法，根据半监督技术对聚合数据进行了分类。Kishor 等[25]通过对基于物联网的健康记录用雾计算和机器学习来降低计算和通信的时延。Chaudhary 等[26]提出了一种识别二重身份攻击的技术，针对所有传感器都处于高风险区域的一种假冒攻击。Dang 等[27]使用基于身份的密码学进行数据安全聚合，但该方案不能抵御冒名攻击。

表 1 从不同角度概述了现有代表性方案，这些方案的核心目标是通过基于 IIoT 环境优先级的聚合机制，在工业传感器与服务器间构建身份验证的密钥协商协议。同时，表 1 展现了现有方案的优势和局限性。

上述方案聚焦于构建既安全又支持多实体间相互验证的密钥协议体系。然而，传统的公钥基础设施（PKI）由于依赖中央机构管理各节点的密钥对，常面临密钥管理复杂性的挑战。为解决此问题，私钥生成器（PKG）被引入以减轻密钥管理开销，通过为每位用户生成基于身份的私钥来实现。尽管如此，基于身份的双线性配对方案在计算上颇为昂贵，且部分协议在相互认证、授权机制及开放信道数据传输效率上表现不足。

经过分析现有方案，本文发现工业传感器在感知与数据聚合阶段缺乏对潜在攻击者的有效检测机制。此外，这些方案普遍面临计算与通信成本高昂的问题，难以充分保障数据的机密性与完整性。因此，进一步研究工作应聚焦于增强对攻击行为的监测能力，同时探索降低计算与通信成本、提升数据保护效能的新方法。针对上述 IIoT 现阶段所面临的安全和隐私挑战，本文提出了 EUVA 协议，提供安全、真实验证密钥管理方案，在数据各个阶段有效防止敌手攻击，同时还能降低计算和通信成本。

2　问题描述

本节将概述所提出的 IIoT 网络模型、敌手模型以及安全目标。

表 1　　**现有代表性方案的优势和局限性**

方案	冒充攻击	临时秘密	密码猜测	相互攻击	优势	局限性
Das 等[11]	×	×	×	√	设计一个身份验证的协议	未能防止冒名顶替攻击；隐私和身份验证安全目标受到损害
Song 等[14]	√	√	×	×	将用户数据记录进行了分类设计了 2 个多功能聚合函数	未能提供节点之间的相互认证；入侵者可以猜测密码以中断通信
Islam 等[15]	√	√	√	√	维护数据的安全性和隐私性	计算成本非常高；能量消耗大
Dang 等[27]	×	√	×	×	使用了基于身份的密码学	无法保持真实性；入侵者可以冒充参与节点
Gupta 等[12]	√	√	√	√	轻量级的认证协议方案；提供强大的安全通信	在协议阶段存在能量消耗
Ullah 等[10]	×	√	√	√	协议高效；可维护数据的机密性和隐私性	入侵者可以冒充参与节点
Cheng 等[23]	×	√	√	×	采用无证书方法解决了密钥托管问题	可以冒充盟友方；存在中间人攻击

2.1　IIoT网络模型

图1描述了IIoT网络模型，该模型由3个功能实体组成：工业传感器（IS）、聚合器（AG）和云端服务器（CS）。这些实体的作用如下所述。

工业传感器实时收集工业设备生产数据，用于检测关键变量，监控工业设备的运行状态和周围生产环境。感知位移、速度、压力、流速、温度、湿度、光强、浓度等传感设备都被集成到工业智能传感器中。这些工业智能传感器的任务是向聚合器报告所观察到的工业生产信息。

聚合器从工业传感器处收集数据，对数据进行聚合，就像工业传感器和云端服务器之间的网关。它是一个独特的智能点，具有更好的计算和通信能力。其存储的数据必须使用聚合程序来合并记录。为防止恶意单位访问网络，聚合器会积累工业传感器的生产记录，并验证工业传感器与云端服务器交互的真实性，然后对其进行聚合计算。

云端服务器是聚合的最终机构，其负责对最终的聚合结果解密并存储。一般而言，云端被假定为诚实而好奇的。云端服务器的用户是工业生产相关的专业团队，如管理人员或设计人员等，他们可以根据数据的分析与处理结果改进产品的设计方案、制造方案、物料供应方案等，以及对潜在生产风险进行提前预警处理。它拥有几乎无限的存储空间和强大的计算潜力。不过，本文假定只有授权实体和相关人员才能访问服务器。

2.2　敌手模型

本节为所提出的协议设计并定义了一个正式的敌手模型，该模型由参与节点组成，这些节点可以是网络中任意实体。其中任何2个参与节点都可以进行通信；其中一个参与节点发起对话，另一个参与节点做出反应。

假设$\mathcal{A}$为敌手，所提协议应该通过确保机密性、完整性和真实性来保证数据的安全聚合。

1) 保密性威胁。$\mathcal{A}$会选择以下攻击方式之一来获取密钥的可访问性：已知明文攻击、选择密文攻击或选择明文攻击。只要$\mathcal{A}$获得密钥的访问权限，就可以破译加密记录。

2) 完整性威胁。$\mathcal{A}$可能会破坏一个或多个聚合器或传感器，从而导致丢失一些重要的工业数据或聚合记录被修改，目的是向工业云端服务器发布错误的聚合（如重播命中）。

3) 真实性威胁。目前存在2种不同的威胁，它们会将真实性纳入风险范围。

①$\mathcal{A}$伪装成真实的工业传感器或聚合点，从而将虚假信息注入其网络。

②$\mathcal{A}$伪装成真正的工业云端服务器，在网络中注入虚假记录。

2.3　安全目标

所提面向IIoT的无配对数据验证和聚合协议应满足下列安全目标。

1) 相互认证：在生成会话密钥和传输数据之前，必须对所有实体的合法性进行认证。

2) 保密性：必须限制只有授权节点（如云端服务器）才能访问工业传感器的感知记录数据。

3) 完整性：所有数据必须具有适当的真实性和完整性，确保数据在传输过程中不会被篡改。

4) 保护节点匿名性：确保敌手永远不会获取

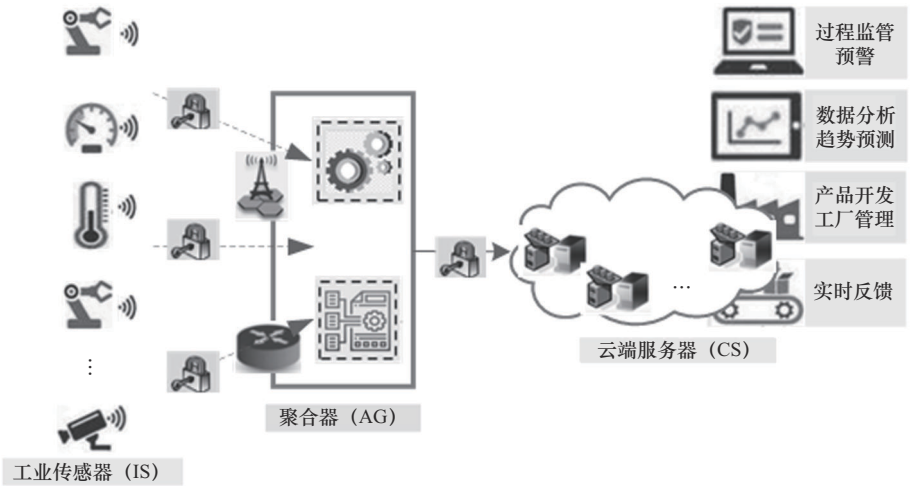

图1　IIoT网络模型

有关工业传感器或管理分析人员身份的任何信息。

5) 难解性：确保敌手无法追踪任何目标节点。

6) 能源消耗可持续性：工业物联网由资源受限的传感设备组成，因此所提协议的计算通信成本和能源开销应是可持续的。

3　EUVA 协议

本节主要详述了EUVA协议所应采取的所有步骤，包括：设置和注册，密钥生成，加密和验证，验证和聚合，验证和解密。表2列出了系统参数。

表2　　系统参数

参数	含义
x	PKG的主密钥
P	E/F_q的生成器
P_{Pub}	PKG的公钥
$H_i, i = 1,2$	安全哈希定义
q	素数模
a,b	随机数
s,r	临时密钥
ID_{IS}	工业传感器的身份
ID_{CS}	云端服务器的身份
ID_{AG}	聚合器的身份
$\lambda_{\text{IS}},\gamma_{\text{IS}}$	工业传感器节点的签名对
$\lambda_{\text{CS}},\gamma_{\text{CS}}$	云端服务器节点的签名对
$\lambda_{\text{AG}},\gamma_{\text{AG}}$	聚合器节点的签名对
K_{IS}	工业传感器节点计算得出的密钥
K_{CS}	云端服务器节点计算得出的密钥
K_{AG}	聚合器计算得出的密钥
SK_{ISCS}	工业传感器和云端服务器生成的会话密钥
SK_{AGCS}	聚合器和云端服务器生成的会话密钥

图2是EUVA协议流程。其中描述了首先为工业传感器与云端服务器配对以及为聚合器与云端服务器配对生成会话密钥。然后使用该密钥对收集到的感知数据类别进行加密，对聚合器进行验证，以检查其真实性。之后，聚合器生成一条信息S，转发给云端服务器进行验证。在对聚合器进行验证后，云端服务器发送一条许可信息，开始聚合加密数据并转发给云端服务器。服务器只有在验证后才会接受这些数据，否则就会丢弃。

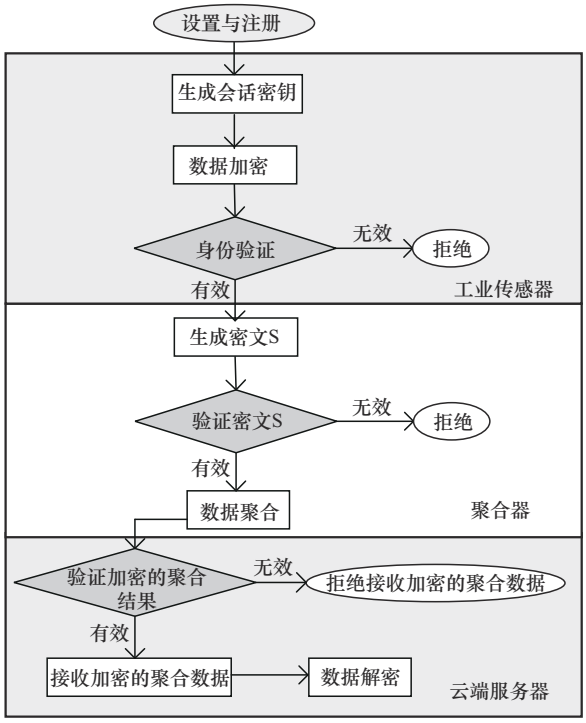

图2　EUVA协议流程

3.1　设置和注册阶段

据调查，大多数工厂管理都采用基于智能传感器的管理解决方案，而不是由工人对每个设备的运行状态进行登记。因此，不同的设备上配备着不同类型的传感器。此外，所有设备传感器和聚合器都必须在云服务器上注册。每当硬件设置完成后，云服务器就会监控每个传感器请求的密钥。从聚合器获取请求后，设备传感器就会开始响应请求。系统设置和注册过程的步骤如下。

1) 系统设置

①加法群G与质数q可以生成曲线E/F_q，并且点P是G的生成元。

②选择$x \in Z_q^*$作为主私钥，以确定主公钥$P_{\text{Pub}} = xP$。

③安全散列函数定义为

$$H_1: \{0,1\}^* \times G \rightarrow Z_q^*$$

$$H_2: \{0,1\}^* \times \{0,1\}^* \times G \times G \times G \times G \times G \rightarrow Z_q^*$$

④param = $\{G,q,P,P_{\text{pub}},H_1,H_2\}$作为系统参数被公布，同时保持主密钥$x$的机密性。

2) 密钥提取：利用工业传感器的身份：$\text{ID}_{\text{IS}} \in 0,1^*$，PKG生成长期私钥。

①PKG选择一个随机数$a \in Z_q^*$，然后计算U_{IS}、h_{IS}和V_{IS}

$$U_{\text{IS}} = aP$$

$$h_{IS} = H_1[\mathrm{ID}_{IS} \| U_{IS}]$$
$$V_{IS} = a + h_{IS}x$$

②通过安全通道将元组$[V_{IS}, U_{IS}]$发送给工业传感器。

③ $(P_{IS} = U_{IS} + H_1[\mathrm{ID}_{IS} \| U_{IS}]P_{Pub} = V_{IS}P)$ 成立，PKG验证其私钥。同样，对于聚合器AG和CS，将收到

$$U_{AG} = bP, U_{CS} = cP$$
$$h_{AG} = H_1[\mathrm{ID}_{AG} \| U_{AG}], h_{CS} = H_1[\mathrm{ID}_{CS} \| U_{CS}]$$
$$V_{AG} = b + h_{AG}x, V_{CS} = c + h_{CS}x$$

3.2 会话密钥生成

首先计算工业传感器和云端服务器之间的协议密钥，双方相互验证。此外，生成的协议密钥将用于在工业传感器端点对传感器收集到的所有工业设备生产记录进行加密。之后，同样会在聚合器和云端服务器之间计算经过验证的协议密钥，以便安全地传输聚合数据。

3.2.1 工业传感器和云端服务器

1) 工业传感器端

选择一个临时密钥 $s \in Z_q^*$ 并计算 $T_{IS} = sP$，$\lambda_{IS} = [s + h_{IS}]^{-1}V_{IS}$，$\gamma_{IS} = V_{IS}P$。此外，发送元组集$\{\mathrm{ID}_{IS}, T_{IS}, \lambda_{IS}, \gamma_{IS}, U_{IS}\}$给云端服务器生成会话密钥。

2) 云端服务器

收到元组后，云端服务器需要验证工业传感器的真实性。云端服务器计算 $\lambda_{IS}[T_{IS} + H_1[\mathrm{ID}_{IS} \| U_{IS}]P]$并检查它是否等于$\gamma_{IS}$。若相等，则表示对工业传感器的验证成功，否则拒绝其生成协商密钥的请求。云端服务器再次选择一个临时密钥 $r \in Z_q^*$ 计算 $T_{CS} = rP$ 并生成 $\lambda_{CS} = [r + h_{CS}]^{-1}V_{CS}$和$\gamma_{CS} = V_{CS}P$。之后，云端服务器向经过身份验证的工业传感器发送元组$\{\mathrm{ID}_{CS}, T_{CS}, \lambda_{CS}, \gamma_{CS}, \mathrm{U}_{CS}\}$，同时计算密钥$K_{CS} = (r + V_{CS})(T_{IS} + U_{IS} + H_1[\mathrm{ID}_{IS} \| U_{IS}] \cdot P_{Pub})$，即 $H_1[\mathrm{ID}_{IS} \| U_{IS}] = h_{IS}$，并生成会话密钥$\mathrm{SK}_{CS} = H_2[\mathrm{ID}_{IS} \| \mathrm{ID}_{CS} \| T_{IS} \| T_{CS} \| \lambda_{IS} \| \lambda_{CS} \| \mathrm{K}_{CS}]$。

工业传感器接收数据后，通过计算表达式的值来验证云端服务器的身份，即 $\lambda_{CS}[T_{CS} + H_1[\mathrm{ID}_{CS} \| U_{CS}]P]$。若等于$\gamma_{CS}$，则身份验证成功；否则，由于身份验证失败，工业传感器拒绝生成会话密钥的请求。云端服务器的身份验证完成后，工业传感器密钥 $K_{IS} = (r + V_{IS})(T_{CS} + U_{CS} + H_1[\mathrm{ID}_{CS} \| U_{CS}]P_{Pub})$ 和生成 $\mathrm{SK}_{IS} = H_2[\mathrm{ID}_{IS} \| \mathrm{ID}_{CS} \| T_{IS} \| T_{CS} \| \lambda_{IS} \| \lambda_{CS} \| K_{IS}]$ 作为会话密钥，在 $H_1[\mathrm{ID}_{CS} \| U_{CS}] = h_{CS}$。工业传感器和云端服务器只有在两端成功完成身份验证时才开始计算会话密钥，否则它们会相应地拒绝对方的请求。

3.2.2 聚合器和云端服务器

本文同样在聚合器和云端服务器之间生成会话密钥，与3.2.1节中类似，即 $\mathrm{SK}_{AGCS} = \mathrm{SK}_{AG} = \mathrm{SK}_{CS} = H_2[\mathrm{ID}_{AG} \| \mathrm{ID}_{CS} \| T_{AG} \| T_{CS} \| \lambda_{AG} \| \lambda_{CS} \| K']$，$K' = K_{AG} = K_{CS} = (rtP + rV_{AG}P + tV_{CS}P + V_{CS}V_{AG}P)$。

3.3 加密和验证

机密性和匿名性是有效数据聚合的基本要求，可确保互联网的信息不会被未经授权的实体查看。因此，为了保证点对点数据的机密性，本文方案采用了同态加密技术。使用同态加密技术的优势是，它可以对密文进行复杂的数学计算，而不会泄露初始明文数据的细节。由于所有计算都是在加密的明文上进行的，因此保密性和匿名性得以保留。工业传感器和云端服务器之间的所有通信都是安全可靠的，不会受到任何恶意修改或未经授权的访问。

算法1描述了使用会话密钥SK_{ISCS}执行的加密过程，该密钥是根据分类数据为工业传感器和云端服务器生成的。相应地，使用随机数来检索数据的新鲜度信息。同时，计算MACh值为$h_i(C_i \| M_i)$，分别用于验证所有传输数据类别的完整性。在向聚合器传输加密后的$(C_i \| h_i)$之前，需要检查其真实性。因此，本文使用基于密码的身份验证或基于生物特征的相互授权技术。检查完聚合器的真实性后，就将所有加密数据$(C_i \| h_i)$发送给聚合器。

算法1 加密算法

使用会话密钥SK_{ISCS}对收集到的工业数据进行加密，输入M_i、N_i、SK_{ISCS}。

1) 将所有M_i映射到椭圆曲线上的点P_i。

①对于紧急状况（EC, emergency condition）：

计算$C_i^{EC} = E_{\mathrm{SK}_{ISCS}}(P_i \| N_i)$。

计算哈希值$h_i^{EC} = h(C_i \| M_i)$。

②对于重要状况（VC, vital condition）：

计算$C_i^{VC} = E_{\mathrm{SK}_{ISCS}}(P_i \| N_i)$。

计算哈希值$h_i^{VC} = \mathrm{h}(C_i \| M_i)$。

③对于常规状况（RC, regular condition）：

计算 $C_i^{\mathrm{RC}} = E_{\mathrm{SK_{ISCS}}}(P_i \| N_i)$。

计算哈希值 $h_i^{\mathrm{RC}} = h(C_i \| M_i)$。

2) 将 $(C_i^{\mathrm{EC}} \| h_i^{\mathrm{EC}})$、$(C_i^{\mathrm{VC}} \| h_i^{\mathrm{VC}})$ 和 $(C_i^{\mathrm{RC}} \| h_i^{\mathrm{RC}})$ 发送给聚合器。

3.4　验证和聚合

只有在工业传感器和聚合器之间完成相互验证后，聚合器才会向云端服务器发送信息 $S = E_{\mathrm{SK_{AGCS}}}(\mathrm{ID_{AG}})$。该信息 S 一般使用协议密钥 $\mathrm{SK_{AGCS}}$ 生成，以验证聚合器与云端服务器之间的关系，具体说明如下。

接下来，云端服务器使用聚合器 $\mathrm{ID_{AG}}$ 和会话密钥 $\mathrm{SK_{AGCS}}$ 计算 S'。用接收到的 S 值检查它，如果两者不匹配，那么云端服务器将阻止聚合器访问网络，无论它是恶意的还是未经身份验证的。接下来，若计算值匹配云端服务器，则将授权消息导向聚合器，聚合器一旦收到同一云端服务器的许可通知，就会开始其信息聚合过程。建议方案的数据聚合过程基于信息优先级。工业现场的生产记录分为三大类，其中，将紧急数据设定为最高优先级，以便紧急从工业传感器传输到云端服务器，并立即采取紧急处理措施；有些关键的工业设备的运行状况需要根据管理者的要求进行日常观察，这类数据属于重要数据；不属于紧急和重要类别的工业数据将归入常规类别，这些常规数据定期在云端服务器上更新。

事实上，必须将具有相似信息优先级的特定密码文本连接在一起，而不是将所有基于不同优先级的数据连接在一起。最后，分类汇总计算输出 $(C_{\mathrm{AG}}^{\mathrm{EC}}, h_{\mathrm{AG}}^{\mathrm{EC}})$、$(C_{\mathrm{AG}}^{\mathrm{VC}}, h_{\mathrm{AG}}^{\mathrm{VC}})$ 和 $(C_{\mathrm{AG}}^{\mathrm{RC}}, h_{\mathrm{AG}}^{\mathrm{RC}})$ 应通过安全通道传输到云端服务器。只有在聚合器验证过程结束后，聚合器才会开始根据优先级聚合工业传感器收到的所有数据。因此，在传输任何重要的工业信息之前，工业传感器、聚合器和云端服务器都要在整个过程中相互验证。

3.5　验证和解密

云端服务器在获得汇总信息后启动解密和验证流程。首先，云端服务器对收到的加密汇总数据进行解密，然后验证点对点的完整性。所有涉及的计算都通过以下步骤进行。

步骤 1　对接收到的聚合数据 $(C_{\mathrm{AG}}^{\mathrm{EC}}, h_{\mathrm{AG}}^{\mathrm{EC}})$、$(C_{\mathrm{AG}}^{\mathrm{VC}}, h_{\mathrm{AG}}^{\mathrm{VC}})$ 和 $(C_{\mathrm{AG}}^{\mathrm{RC}}, h_{\mathrm{AG}}^{\mathrm{RC}})$ 使用会话密钥 $\mathrm{SK_{ISCS}}$，该密钥为工业传感器和云端服务器生成，并计算 $M' = D_{\mathrm{SK_{ISCS}}}(C_{\mathrm{AG}})$。

步骤 2　计算 $h' = h(M_i \| C_i)$，并与接收到的 h_{AG} 进行验证。检查 $h' = h_{\mathrm{AG}}$ 是否成立，只有在验证成功的情况下，汇总数据才会被批准；否则，云端服务器将丢弃该数据。之后，管理人员或设计人员等相关的专业团队都可以访问这些通过审核的记录。

4　安全性分析

1) 中间人攻击。在所提 EUVA 协议中，IS 节点向 CS 发送一组元组 $\{\mathrm{ID_{IS}}, T_{\mathrm{IS}}, \lambda_{\mathrm{IS}}, \gamma_{\mathrm{IS}}, U_{\mathrm{IS}}\}$。假设在它们之间存在一个攻击者 $\mathcal{A}$。攻击者计算 $T'_{\mathrm{IS}} = uP$ 并发送修改后的元组 $\{\mathrm{ID_{IS}}, T'_{\mathrm{IS}}, \lambda_{\mathrm{IS}}, \gamma_{\mathrm{IS}}, U_{\mathrm{IS}}\}$ 给 CS。CS 在从任何节点接收元组时，需要验证发送节点的身份。但此时，服务器无法认证攻击者节点 $\mathcal{A}$ 身份，拒绝使用由攻击者节点转发的接收到的元组来计算会话密钥，并向攻击者节点发送认证失败的消息。

同样地，如果攻击者向 IS 节点发送类似 $\{\mathrm{ID_{CS}}, T'_{\mathrm{CS}}, \lambda_{\mathrm{CS}}, \gamma_{\mathrm{CS}}, U_{\mathrm{CS}}\}$ 的元组，IS 也会拒绝这些元组，因为 IS 也无法验证发送者节点 $\mathcal{A}$ 的身份。对于聚合器和服务器的情况也类似。因此，不存在中间人攻击的可能性。

2) 临时已知信息攻击。根据所提 EUVA 协议中 $\mathrm{SK} = H_2[\mathrm{ID_{IS}} \| \mathrm{ID_{CS}} \| T_{\mathrm{IS}} \| T_{\mathrm{CS}} \| \lambda_{\mathrm{IS}} \| \lambda_{\mathrm{CS}} \| K]$，其中 $K = rsP + rV_{\mathrm{IS}}P + sV_{\mathrm{CS}}P + V_{\mathrm{CS}}V_{\mathrm{IS}}P$ 的机密性对于保持会话密钥 SK 的机密性起着主要作用。然而，即使攻击者获得了当前会话的临时密钥 r 和 s，也无法确定会话密钥 SK。攻击者 $\mathcal{A}$ 只有在确定了 $V_{\mathrm{CS}}V_{\mathrm{IS}}P$ 的值之后，才能获得会话密钥 SK。即使知道了 $(P_{\mathrm{IS}}, P_{\mathrm{CS}}) = (V_{\mathrm{IS}}P, V_{\mathrm{CS}}P)$，计算 $V_{\mathrm{CS}}V_{\mathrm{IS}}P$ 也属于解决 CDHP 问题的困难假设范畴。对于聚合器和云端服务器的情况也类似。因此，所提协议能够在临时证据泄露给攻击者的情况下防止攻击。

3) 已知密钥攻击。所提协议的会话密钥计算依赖于 2 个临时值 r 和 s。这样，由于 $T_{\mathrm{IS}} = rP$ 和 $T_{\mathrm{CS}} = sP$ 的计算基于 ECDL 问题的计算难题假设，因此处于风险区域的任何会话密钥 SK 都不会影响新的会话密钥 SK 的计算。对于 AG 和 CS 也是如此。因此，如果现有会话密钥发生泄露，攻击者 $\mathcal{A}$ 无法获取关于其他会话密钥的信息。

4) 完美前向安全性。即使节点的私钥被泄露，

攻击者$\mathcal{A}$也无法获得之前的会话密钥。攻击者$\mathcal{A}$可能想要确定SK，因此它首先需要计算$K = rsP + rV_{IS}P + sV_{CS}P + V_{CS}V_{IS}P$，以及知道$\lambda_{IS} = [s + h_{IS}]^{-1}V_{IS}$和$\lambda_{CS} = [r + h_{CS}]^{-1}V_{CS}$。一旦$V_{IS}$和$V_{CS}$被公布，$\mathcal{A}$就可以计算出$V_{CS}V_{IS}P$，但无法计算出$rsP$、$rV_{IS}P$和$sV_{CS}P$，因为$r$和$s$对$\mathcal{A}$是未知的。由于严格假设在多项式时间内解决ECDL问题将是困难的，因此攻击者无法从T_{IS}和T_{CS}中获得r和s的值。$\mathcal{A}$还可试图$(T_{IS},P_{CS}) = (sP,V_{CS}P)$和$(T_{CS},P_{IS}) = (rP,V_{IS}P)$中推导出$rsP$、$rV_{IS}P$和$sV_{CS}P$，并计算$K = rsP + rV_{IS}P + sV_{CS}P + V_{CS}V_{IS}P$、$\lambda_{IS} = [s + h_{IS}]^{-1}V_{IS}$和$\lambda_{CS} = [r + h_{CS}]^{-1}$。然而，由于解开CDHP问题的困难假设，这也是不可能的。对于AG和CS也是类似的。因此，EUVA协议成功地保持了完美前向安全性。

5) PKG前向安全性。本文已经在上文中证明，由于解决CDH和ECDL问题的困难假设，$\mathcal{A}$总是无法利用之前的会话密钥来获得会话密钥信息。然而，所有参与者的私钥都将因PKG主密钥的泄露而受到影响，但可以说当前和先前的密钥信息将始终保持安全。因此，在所提协议中保留了PKG前向安全性。

6) 非密钥主导性。在所提协议中，会话密钥同样依赖于IS和CS或AG和CS的输入。因此，任何一方都无法主导会话密钥的计算。因此，无论是IS和CS还是AG和CS，都无法相互主导。

7) 保密性。IS使用会话密钥SK_{ISCS}传输所有记录的工业感知数据的加密形式。由于已经证明了密钥SK的强大性质，并且由于CDH和ECDL问题的困难假设，$\mathcal{A}$无法计算或访问它。因此，数据在通过信道传输时保持了其保密性。只有拥有相同密钥的授权节点（如CS）才能解密数据并获得原始消息。假设在AG端对传输的信息进行了窃听，但这将是徒劳的，因为AG用于聚合数据而不进行解密。因此，所提协议成功地保持了数据的保密性。

8) 完整性。在所提协议中，还关注了节点的完整性。假设$\mathcal{A}$对加密数据进行修改，而不是出于各种目的访问数据。为了防止这种情况，服务器CS检查$h'_{AG} = h_{AG}$是否匹配，如果不匹配，则丢弃数据；否则，接收数据，所以它成功地保持了端到端的数据完整性。

5 性能分析

本节概述了所提协议在计算和通信成本方面的有效性评估。此外，为了执行所提协议，本文使用MIRACL来进行相关的计算[28]。本文在配置有Intel core i7 9700 CPU@3.0 GHz和8 GB RAM处理器的64位Ubuntu 20.04.4 LTS操作系统上进行了模拟工作。平均对每个加密功能进行了100次操作，通过计算这些迭代的平均值来确定运行时间，并与现有相似协议（文献[6-7, 22, 27, 29-30]）进行对比实验分析。

表3给出了各种加密操作的执行时间。一般来说，哈希运算（T_H）和点加运算（T_A）操作的执行成本将被忽略，因为这些操作相对于其他操作（如$T_H \approx 0.000\ 1$ ms和$T_A \approx 0.000\ 3$ ms）所需的计算量非常小。

表3 各种加密操作的执行时间

操作	描述	执行时间/ms
T_{PM}	在ECC中，对于标量点乘法操作的执行时间	2.001 5
T_{MP}	哈希函数映射操作的执行时间	2.005 8
T_{BM}	双线性乘法配对操作的执行时间	4.002 6
T_M	标量乘法操作的执行时间	0.780 0
T_E	指数运算操作的执行时间	8.023 9

表4显示了现有协议和本文所提EUVA协议所使用的操作及各个方案的通信开销和计算成本开销。图3清楚地显示了不同协议使用各运算操作的次数。相较于其他协议，EUVA协议在计算次数和复杂性上都有着显著的优势。

表4 相关方案对比

协议	通信开销	计算开销	困难问题假设
文献[6]	$2\lvert G_q\rvert$	$7T_{PM} + 4T_{MP} + 3T_M$	CDH、ECDH
文献[7]	$2\lvert G_q\rvert$	$4T_{PM} + 1T_{MP} + 1T_M$	CDH
文献[22]	$2\lvert G_q\rvert$	$3T_{PM} + 2T_{BM}$	CDH、BDH
文献[27]	$2\lvert G_q\rvert$	$6T_{PM}$	CDH
文献[29]	$2\lvert G_q\rvert$	$6T_{PM} + 4T_{MP}$	CDH、OGDH
文献[30]	$2\lvert G_q\rvert$	$5T_{PM} + 3T_{MP} + 2T_E$	CDH、ECDL
EUVA	$2\lvert G_q\rvert$	$4T_{PM}$	CDH、ECDH

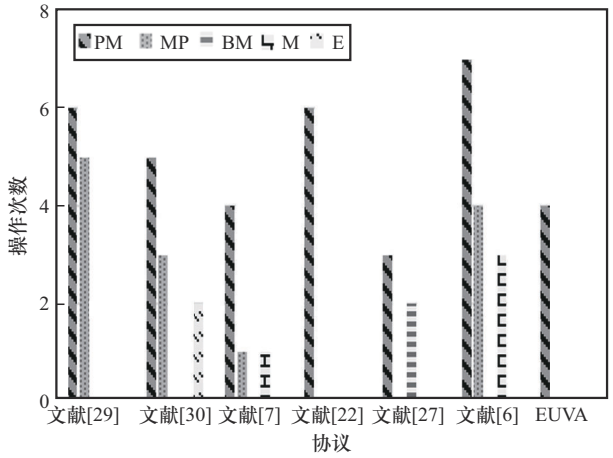

图3　不同协议使用各运算操作的次数

图4将现有协议的系统设置、PKG和会话密钥协议等每个阶段的计算开销进行比较分析。对比于其他工作，EUVA协议在会话密钥阶段的计算开销最低。无配对的会话密钥验证管理在效率上有着明显优势，可有效地降低计算-通信成本。

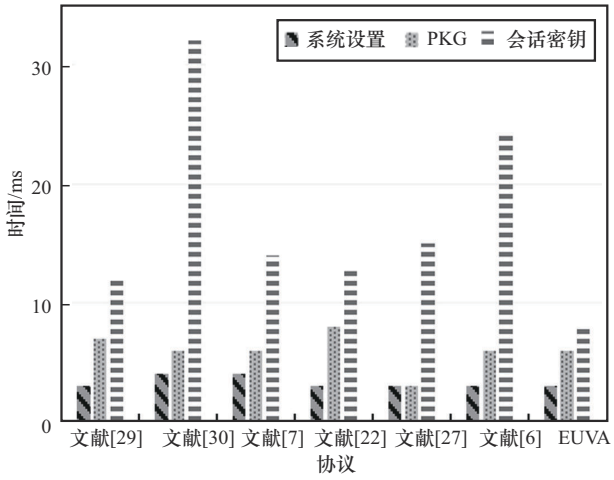

图4　计算开销

在智能传感器系统中，能耗是重点关注问题，因此需要尽可能地减少所提协议的存储和能耗开销。能耗估算使用能耗=功率×时间公式计算。在EUVA中，IS需要1.00 mJ，PKG需要20.36 mJ，CS根据其参与的不同阶段（如设置、私钥生成和相互认证阶段）需要6.004 5 mJ。同样，对于其他现有协议，本文也计算了它们的传感器、服务器和授权第三方的能耗记录，并通过图5展示了能耗开销的比较。从图5中可以看到，EUVA最小化了两端的能耗开销，以提高IIoT系统的性能。

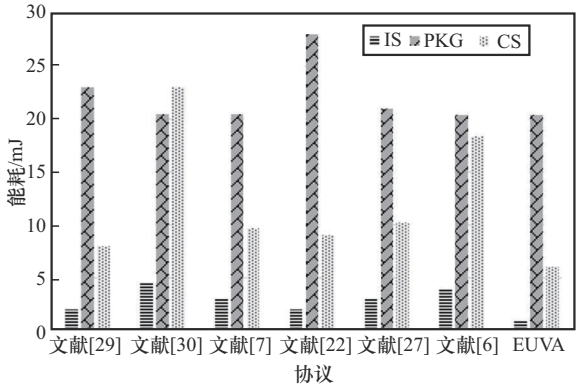

图5　能耗开销

6　结束语

针对在IIoT智能环境中现场设备自身资源的有限性导致计算成本高昂且无法抵御各种攻击、设备和数据的低安全性等缺陷，本文根据IIoT环境下的网络模型及其安全要求，提出了一种针对IIoT网络模型及其特定安全需求的高效无配对数据验证与聚合协议。该协议巧妙融合了ECC的强健性与同态加密技术的数据隐私保护能力，构建了一个既安全又真实的无配对验证框架。在此基础上，本文还设计了相应的验证密钥管理方案，进一步增强了系统的整体安全性与可信度。此外，性能评估结果表明，与现有协议相比，所提协议降低了通信开销和计算成本，并最大限度地减少了能源开销。在未来研究中，将进一步验证所提协议在实际工业物联网环境中的性能和可扩展性，尤其是对于大规模网络中的节点故障和网络时延等现实问题。

参考文献：

[1] MA R, FENG T, XIONG J B, et al. DScPA: a dynamic subcluster privacy-preserving aggregation scheme for mobile crowdsourcing in industrial IoT[J]. IEEE Internet of Things Journal, 2024, 11(2): 1880-1892.

[2] WU D P, WU S E, RAWAT D B, et al. Special issue on knowledge- and service-oriented industrial Internet of Things: architectures, challenges, and methodologies[J]. IEEE Internet of Things Journal, 2022, 9(18): 16738-16741.

[3] SAHA R, KUMAR G, CONTI M, et al. DHACS: smart contract-based decentralized hybrid access control for industrial Internet-of-things[J]. IEEE Transactions on Industrial Informatics, 2022, 18(5): 3452-3461.

[4] MA R, FENG T, TIAN Y L, et al. EPMA: edge-assisted hierarchical privacy-preserving multidimensional data aggregation mechanism[J]. Mobile Networks and Applications, 2023, 28(5): 1831-1841.

[5] BI R W, GUO D L, ZHANG Y Y, et al. Outsourced and privacy-preserving collaborative k-prototype clustering for mixed data via addi-

tive secret sharing[J]. IEEE Internet of Things Journal, 2023, 10(18): 15810-15821.

[6] OTHMAN S B, BAHATTAB A A, TRAD A, et al. Confidentiality and integrity for data aggregation in WSN using homomorphic encryption [J]. Wireless Personal Communications, 2015, 80(2): 867-889.

[7] ALIJUMAIE G S, ALZEER G, ALGHAMDI R, et al. Modern study on internet of medical things (IOMT) security[J]. International Journal of Computer Science and Network Security, 2021, 21(8): 254-266.

[8] ADI S. Identity-based cryptosystems and signature schemes[C]// Workshop on the Theory and Application of Cryptographic Techniques. Berlin: Springer, 1985: 47-53.

[9] GUPTA D S, ISLAM S H, OBAIDAT M S, et al. A provably secure and lightweight identity-based two-party authenticated key agreement protocol for IIoT environments[J]. IEEE Systems Journal, 2021, 15(2): 1732-1741.

[10] ULLAH I, AMIN N U, KHAN M A, et al. An efficient and provable secure certificate-based combined signature, encryption and signcryption scheme for Internet of Things (IoT) in mobile health (M-health) system[J]. Journal of Medical Systems, 2020, 45(1): 4.

[11] DAS A K, GOSWAMI A. A secure and efficient uniqueness-and-anonymity-preserving remote user authentication scheme for connected health care[J]. Journal of Medical Systems, 2013, 37(3): 9948.

[12] GUPTA D S, ISLAM S H, OBAIDAT M S, et al. LAAC: lightweight lattice-based authentication and access control protocol for E-health systems in IoT environments[J]. IEEE Systems Journal, 2021, 15(3): 3620-3627.

[13] GUPTA D S, BISWAS G P. Secure computation on cloud storage[J]. Journal of Cases on Information Technology, 2015, 17(3): 22-29.

[14] HAN S, ZHAO S, LI Q H, et al. PPM-HDA: privacy-preserving and multifunctional health data aggregation with fault tolerance[J]. IEEE Transactions on Information Forensics and Security, 2016, 11(9): 1940-1955.

[15] ISLAM S H, BISWAS G P. A pairing-free identity-based two-party authenticated key agreement protocol for secure and efficient communication[J]. Journal of King Saud University - Computer and Information Sciences, 2017, 29(1): 63-73.

[16] CANO M D, CAÑAVATE-SANCHEZ A. Preserving data privacy in the Internet of medical things using dual signature ECDSA[J]. Security and Communication Networks, 2020, 2020: 4960964.

[17] SOWJANYA K, DASGUPTA M, RAY S. Elliptic Curve Cryptography based authentication scheme for Internet of Medical Things[J]. Journal of Information Security and Applications, 2021, 58: 102761.

[18] LI J L, SU Z, GUO D K, et al. PSL-MAAKA: provably secure and lightweight mutual authentication and key agreement protocol for fully public channels in Internet of medical things[J]. IEEE Internet of Things Journal, 2021, 8(17): 13183-13195.

[19] YAO H L, YAN Q, FU X B, et al. ECC-based lightweight authentication and access control scheme for IoT E-healthcare[J]. Soft Computing, 2022, 26(9): 4441-4461.

[20] ZHANG B. A lightweight data aggregation protocol with privacy-preserving for healthcare wireless sensor networks[J]. IEEE Systems Journal, 2021, 15(2): 1705-1716.

[21] KUMAR V, RAY S, DASGUPTA M, et al. A pairing free identity based two party authenticated key agreement protocol using hexadecimal extended ASCII elliptic curve cryptography[J]. Wireless Personal Communications, 2021, 118(4): 3045-3061.

[22] BEN OTHMAN S, ALMALKI F A, CHAKRABORTY C, et al. Privacy-preserving aware data aggregation for IoT-based healthcare with green computing technologies[J]. Computers and Electrical Engineering, 2022, 101: 108025.

[23] CHENG Q F, LI Y T, SHI W B, et al. A certificateless authentication and key agreement scheme for secure cloud-assisted wireless body area network[J]. Mobile Networks and Applications, 2022, 27(1): 346-356.

[24] HURTADO S, GARCÍA-NIETO J, POPOV A, et al. Human activity recognition from sensorised patient's data in healthcare: a streaming deep learning-based approach[J]. International Journal of Interactive Multimedia and Artificial Intelligence, 2023, 8(1): 23.

[25] KISHOR A, CHAKRABORTY C, JEBERSON W. A novel fog computing approach for minimization of latency in healthcare using machine learning[J]. International Journal of Interactive Multimedia and Artificial Intelligence, 2021, 6(7): 7.

[26] CHOUDHARY D, PAHUJA R. Improvement in quality of service against doppelganger attacks for connected network[J]. International Journal of Interactive Multimedia and Artificial Intelligence, 2022, 7 (5): 51.

[27] DANG L J, XU J, CAO X F, et al. Efficient identity-based authenticated key agreement protocol with provable security for vehicular ad hoc networks[J]. International Journal of Distributed Sensor Networks, 2018, 14(4): 155014771877254.

[28] ZHANG X Y, THAKUR N, OGUNDEPO O, et al. MIRACL: a multilingual retrieval dataset covering 18 diverse languages[J]. Transactions of the Association for Computational Linguistics, 2023, 11: 1114-1131.

[29] AMAN M N, BASHEER M H, DASH S, et al. HAtt: hybrid remote attestation for the Internet of Things with high availability[J]. IEEE Internet of Things Journal, 2020, 7(8): 7220-7233.

[30] DHILLON P K, KALRA S. Multi-factor user authentication scheme for IoT-based healthcare services[J]. Journal of Reliable Intelligent Environments, 2018, 4(3): 141-160.

[作者简介]

马蓉（1992– ），女，甘肃兰州人，兰州理工大学博士生，主要研究方向为数据安全与隐私保护。

冯涛（1970– ），男，甘肃临洮人，博士，兰州理工大学研究员、博士生导师，主要研究方向为网络与信息安全、区块链、工业互联网安全等。