Computer Science and Application 计算机科学与应用, 2025, 15(4), 145-151
Published Online April 2025 in Hans. https://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2025.154087

Hans汉斯

云边端协同范式下的轻量级去中心化隐私认证方案

平雅娴，岳笑含

沈阳工业大学信息科学与工程学院，辽宁 沈阳

收稿日期：2025年3月8日；录用日期：2025年4月7日；发布日期：2025年4月15日

摘　要

随着工业4.0的快速发展，云边端协同范式(CET)通过整合云端、边缘节点与终端设备显著提升了计算资源利用效率，但其隐私认证机制面临中心化依赖与资源受限的双重挑战。本文提出一种面向工业CET的轻量级去中心化隐私认证方案，旨在实现低开销、高安全性的认证机制。通过区块链跨链架构建立去中心化信任连接，方案在消除传统权威机构(TA)依赖的同时，采用有限次双线性配对与模指数运算优化计算开销。实验结果表明，隐私认证的计算开销为毫秒级，通信代价保持在低字节位，满足工业场景的轻量化需求。方案进一步满足匿名性、不可伪造性、可追溯性等安全需求，为大规模工业设备接入场景提供了高效可靠的隐私认证解决方案。

关键词

云边端协同范式，隐私认证，去中心化，轻量级

Lightweight Decentralized Privacy-Preserving Authentication Scheme for Cloud-Edge-Terminal Collaborative Paradigm

Yaxian Ping, Xiaohan Yue

School of Information Science and Engineering, Shenyang University of Technology, Shenyang Liaoning

Received: Mar. 8th, 2025; accepted: Apr. 7th, 2025; published: Apr. 15th, 2025

Abstract

With the rapid advancement of Industry 4.0, the cloud-edge-terminal (CET) collaborative paradigm

文章引用: 平雅娴, 岳笑含. 云边端协同范式下的轻量级去中心化隐私认证方案[J]. 计算机科学与应用, 2025, 15(4): 145-151. DOI: 10.12677/csa.2025.154087

significantly enhances computational resource utilization through cloud-edge-terminal integration, yet its privacy authentication mechanisms face dual challenges of centralized dependencies and resource constraints. This paper proposes a lightweight decentralized privacy-preserving authentication scheme for industrial CET environments, aiming to achieve low-overhead and high-security authentication. By establishing decentralized trust connections via a blockchain cross-chain architecture, the scheme eliminates reliance on traditional trusted authorities (TAs) while optimizing computational costs through limited bilinear pairing operations and modular exponentiation optimizations. Experimental results demonstrate that the privacy authentication achieves millisecond-level computational latency and maintains communication costs within a low-byte range, fulfilling the lightweight requirements of industrial scenarios. The scheme further satisfies critical security properties including anonymity, unforgeability, and traceability, providing an efficient and reliable privacy authentication solution for large-scale industrial device deployment scenarios.

Keywords

Cloud-Edge-Terminal Collaborative Paradigm, Privacy-Preserving Authentication, Decentralized, Lightweight

1. 引言

自世界上首台计算机 ENIAC 开启数字文明序幕以来，计算机科技、互联网以及信息技术的迅猛进步，计算技术与信息通信技术的融合创新正驱动全球迈向第四次工业革命，将人类社会引领至一个前所未有的信息爆炸时代。随着工业 4.0 的快速发展，云边端协同范式(CET) [1] [2]通过整合云端、边缘节点与终端设备，显著提升了计算资源的利用效率。在图 1 所示的传统 CET 架构中，其通过任务卸载机制实现计算资源的立体化配置，云端(远程数据中心)提供全局性高算力资源，边缘节点(如 5G 基站、本地服务器)负责低延迟响应与局部数据处理，终端设备(如传感器、工业机器人)执行轻量化任务。三者通过动态任务卸载(Dynamic Task Offloading)实现资源互补，此外，CET 的全过程由一个备受信赖的权威机构(TA)进行统筹管理。

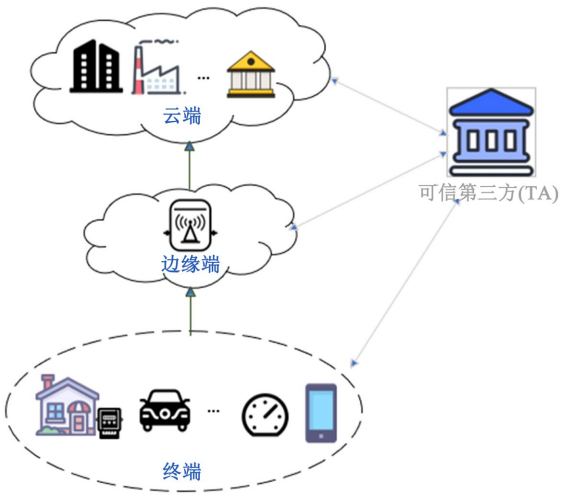

Figure 1. CET system architecture
图 1. CET 系统架构图

传统隐私认证体系[3]-[6]的认证过程中，均需要如图 1 描述的 TA 参与，这种中心化信任模型存在三重潜在风险，包括信任锚点单一化导致系统性信任危机、操作透明度不足可能引发权力滥用以及中心化架构引发单点失效瓶颈。集中式架构固有的缺陷在大规模工业设备接入场景下更易显现出来，当 TA 需处理或参与爆炸式的认证请求时，容易出现响应延迟等性能瓶颈，危急系统可靠性[4]。此外，资源受限终端设备(如低功耗智能传感器、嵌入式 PLC 控制器)的算力与存储约束对隐私认证机制提出特殊挑战，例如计算密集型密码操作超出设备处理能力、存储空间限制阻碍复杂证书链或动态凭证的本地存储等，严重影响工业现场设备的可持续运行。

综上所述，CET 架构中终端节点的隐私认证面临中心化依赖、资源受限挑战。为应对这两方面挑战，本文提出一种面向工业 CET 的轻量级去中心化隐私认证方案，文章贡献如下：

1) 去中心化架构：在基于工业 CET 框架的基础上，利用区块链跨链架构构建云端与边缘端的信任连接，并参考指定验证者签名的特定属性，消除对 TA 的依赖。

2) 轻量化设计：方案设计中采用有限次双线性配对与模指数运算，实现毫秒级认证开销。

3) 安全需求分析：围绕工业 CET 场景下的特点及上述两点挑战，分析了方案的安全及隐私需求，包括匿名性、不可伪造性、正确性、可追溯性等。

2. 相关工作

随着工业 CET 的提出与应用，基于此场景的传统隐私认证方法可分为伪名认证和基于零知识证明(ZKP)的认证两类。2019 年 Wang J 等人[7]采用异或运算与哈希算法等技术为基于边缘计算的智能电网系统引入了一种基于区块链的相互认证和密钥协议，该方案提供访问控制功能，并依赖于 TA 实现不可追溯。在 2023 年，Mohammed B A 等人[8]提出了一种基于车载雾计算的名为 Anaa-fog 的伪名认证方案，每个参与车辆用于验证数字签名的临时密钥由雾服务器生成，能够抵御伪造攻击、重放攻击、中间人攻击等攻击。最近在 2024 年，Junfeng Tian [5]等人为应对现有基于身份的 MEC 匿名认证和密钥协议(ID-AAKA)存在的局限性，提出了一种通过一次性伪名与公私钥实现的新 ID-AAKA 方案，同时引入了并行处理机制减少总时间消耗。

除了上述方案之外，2020 年 Pravin Mundhe [9]等人提出了一种基于环签名的轻型条件隐私保护认证方案，而对于可追溯性来说，只有 TA 可以显示车辆的原始身份。2022 年，Yanping Wang [10]等人提出了一种基于群签名的边缘辅助智能交通系统(ITS)匿名认证方案，允许经过认证的终端向边缘节点报告无限的不可链接消息，而无需大量的伪名下载和存储成本。2023 年，Wenhua Huang [11]等人基于匿名认证并采用无证书机制和非线性对的聚合签名，提出了一种基于可信雾计算的动态匿名认证方案，同时设计了一个金融服务机构之间的协同信任评估模型。上述方案对于可追溯性，不是缺乏就是依赖 TA。

此外，一些新颖的隐私认证方案相继被提出，在 2018 年，Cui J 等人[4]就为车辆自组网的消息认证过程中引入了一种新的边缘计算概念，为车辆添加边缘 TPD(防篡改设备)，并且该边缘不会被攻击。在 2022 年，Wu F [12]等人提出了一个应用于车联网的保持所有安全特性的伪名认证方案，并且可由 TP 对需要的车辆身份进行披露。随后在 2023 年，Tanveer M [13]等人为无人机互联网(IoD)提出了一个称为 SAAF-IoD 的安全匿名身份认证框架，方案构建利用混沌映射、对称加密和哈希函数，可以抵抗特权内部攻击和地面站服务器(GS)旁路攻击。上述方案具有的共同点是对于责任追溯功能均依赖于 TA。

3. 方案构建

本章节以工业 CET 为依托，围绕第 1 章提出的挑战问题，首先设计提出方案的系统模型，对模型中涉及的实体进行描述，并给出相关算法定义；其次，基于方案架构与工业 CET 面临的实际问题给出方案应具备的安全及隐私需求。

3.1. 方案系统模型

关于终端隐私认证方案的系统模型如图 2 所示。模型共包括三类实体，包括终端节点、边缘节点、云端节点。

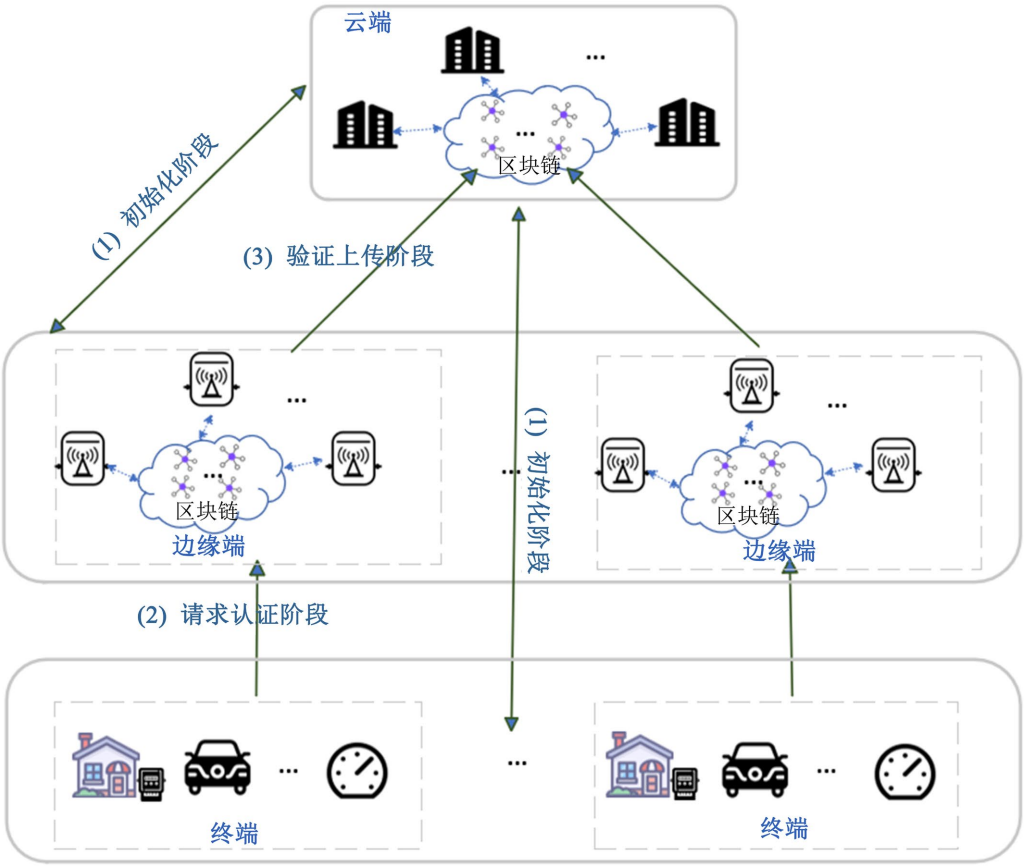

Figure 2. System model
图 2. 系统模型图

终端节点(TN)：TN 是半可信的实体，可以是无人机、传感器、手机等各种接入设备，负责数据采集、传感、输入输出操作，并依赖边缘或云端进行复杂计算和存储。

边缘节点(EN)：EN 是半可信的实体，可以是网络交换机、路由器、基站等各种部署在终端节点较近的地方的节点。EN 被添加到区块链侧脸上以提供本地服务，它们从终端节点收集数据并进行验证，之后将验证结果与数据上传到云端，若 EN 对收集到的信息质疑，则将内容发送到云端管理中心进行处理。

云端节点(CN)：CN 被添加到区块链主链上，是提供指定范围内监控、存储和集中控制服务的实体，它们存储利用来自 EN 的信息并处理 EN 无法处理的数据。CN 可以组成去中心化自治组织(DAO)实施控制，因此可以被定义为不可信的实体。CN 还负责生成公共参数以及追踪数据来源。

3.2. 方案形式化定义

1) 初始化阶段

这一阶段是由云端组成 DAO 的 CN 生成全局公共参数的算法，生成的公共参数广播给其他实体，包括终端节点与边缘节点，这些实体使用公共参数生成相关参数。

$Setup\left(1^{\lambda}\right)\rightarrow pp$：本算法由 DAO 执行，输入安全参数 λ，输出全局公共参数 pp。

$KeyGen_{TN}\left(pp\right)\rightarrow\left(sk_{TN}, pk_{TN}\right)$：本算法由 TN 执行，以 pp 为输入，输出密钥对 $\left(sk_{TN}, pk_{TN}\right)$。

$KeyGen_{EN}\left(pp\right)\rightarrow\left(sk_{EN}, pk_{EN}\right)$：本算法由 EN 执行，以 pp 为输入，输出密钥对 $\left(sk_{EN}, pk_{EN}\right)$。

2) 请求认证阶段

这一阶段是由 TN 执行生成，使用自己私钥与连接 EN 的公钥对于要传输的数据生成认证消息，并为该消息生成零知识证明。

$AuthSend\left(pp, msg_{TN}, sk_{TN}, pk_{EN}\right)\rightarrow\sigma_{TN}=\left(\sigma, \pi_{TN}\right)$：由 TN 来执行，以公共参数 pp、数据 msg_{TN}、私钥 sk_{TN}、连接 EN 的公钥 pk_{EN} 为输入最终生成的认证请求消息为 $\sigma_{TN}=\left(\sigma_{j}, \pi_{TN}\right)$，其中内部包含的每个算法描述如下：

$TN.SingleSign\left(pp, msg_{TN}, sk_{TN}, pk_{EN}\right)\rightarrow\sigma$：TN 使用 pp、自己的私钥 sk_{TN}、连接 EN 的公钥 pk_{EN} 以及数据 msg_{TN} 作为输入，生成部分认证消息 σ。

$TN.Proof\left(pp, x, w, msg_{TN}\right)\rightarrow\pi_{TN}$：TN 使用私钥 sk_{TN} 与随机数 r_{TN} 作为证据 w，以 pp、陈述 x、证据 w 与数据 msg_{TN} 作为输入，生成消息证明 π_{TN}，其中 $x=\left(\sigma, pk_{TN}, pk_{EN}\right)$。

3) 验证上传阶段

在该阶段，算法由 EN 执行验证，并借助区块链执行相应上传操作。

$AuthVerify\left(pp, \sigma_{TN}, msg_{TN}, pk_{TN}, pk_{EN}, sk_{EN}\right)\rightarrow \mathrm{d}=0/1$：如果最终验证消息有效则输出结果 1，否则输出结果 0。其中内部包含的每个算法描述如下：

$EN.Verfproof\left(pp, \pi_{TN}, x, msg_{TN}\right)\rightarrow d_{\pi}=0/1$：首先对消息证明进行验证并输出验证结果，EN 以 pp、π_{TN}、x 与数据 msg_{TN} 作为输入，输出验证结果 d_{π}，如果验证通过则输出为 1，否则输出结果为 0，其中 $x=\left(\sigma, pk_{TN}, pk_{EN}\right)$。

$EN.SingleVerify\left(pp, \sigma, msg_{TN}, pk_{TN}, sk_{EN}\right)\wedge d_{\pi}\rightarrow d=0/1$：EN 对认证消息的部分内容 σ 进行验证，以 pp、部分消息 σ、数据 msg_{TN}、TN 公钥 pk_{TN} 与 EN 私钥 sk_{EN} 作为输入，并与 d_{π} 求交集，得出认证结果 d。最后将认证结果及相关数据生成签名，打包发送至云端。

$CN.SigVerify$：CN 对接收到的候选区块进行验证，若验证成功，则将区块上链，若验证失败，则由 DAO 进行后续处理。

3.3. 安全及隐私需求

正确性：任何合法的 EN 都能够正确验证认证消息 σ_{TN} 的真实性和有效性。若 σ_{TN} 有效，EN 与 CN 应当接受；若 σ_{TN} 无效，则应当拒绝。

不可伪造性：只有合法的 TN 可以生成有效的认证消息，即在不知道 TN 的私钥 sk_{TN} 时，未经授权的第三方(包括 EN 本身)均不能伪造出有效的、可被所有 EN 成功验证的消息，即使他们知道其他合法消息 σ_{TN} 的内容。

匿名性：给定 σ_{TN}，EN 无法让任何外部人员相信 σ_{TN} 是来自发送者 TN 的认证消息。

可认证性：系统内部的实体可以确保消息确实由声明的 TN 生成，能够验证消息的来源确实是拥有公钥 pk_{TN} 的 TN 生成的，并且该属性能够保证消息 msg_{TN} 在传输的过程中没有被篡改。

可追溯性：确保在 EN 提出质疑时，云端 DAO 能够追溯到具体的 TN 或 EN。

4. 性能分析

本章节对文中方案的各个算法进行仿真实验与性能分析。首先对核心算法性能进行理论分析，分析

过程中对不同实体进行不同配置，即分别采用智能手机和基于 Windows 平台的 Ubuntu 系统对 TN 和 EN 的性能进行评估，具体配置如表 1 所示。针对区块链，由于暂不涉及对 CN 的分析，本研究目前采用 Hyperledger Fabric 框架[14]进行评估，通过部署同一局域网的互联节点，表明验证事务平均耗时 3.06 ms。

Table 1. Entity platform configuration information
表 1. 各实体平台配置信息

实体名称	平台信息	测试算法
TN	CPU：第二代骁龙®8 移动平台八核最高 3.19 GHz MEM：12.0 GB	$KeyGen_{TN}$，$TN.SingleSign$，$TN.Proof$
EN	CPU： Intel(R) Core(TM) i5-7300HQ CPU @ 2.50GHz 2.50 GHz RAM：200 GB OS：Ubuntu 22.04	$KeyGen_{EN}$，$EN.Verfproof$，$EN.SingleVerify$
SC (Fabric 链码)	平台配置信息 CPU： Intel(R) Core(TM) i5-7300HQ CPU @ 2.50GHz 2.50 GHz 内存：200 GB 操作系统：Ubuntu 22.04	$CN.SigVerify$

算法开销理论分析结果如表 1 所示。在本节的分析中，鉴于群加法运算、整数运算、哈希运算等基础操作的计算开销较小，故本方案在性能评估模型中予以合理省略，其中 T_{G_1}，T_{G_2} 表示在 G_1，G_2 中完成指数运算的时间，T_e 表示完成一次配对操作的时间。对于在验证上传阶段 EN 对验证结果生成的签名采用基础 BLS 签名，因此最终 EN 的验证时间表示为表 1 所示内容。

Table 2. Theoretical calculation cost table
表 2. 理论计算代价表

实体	EN	TN	CN
初始化	T_{G_2}	T_{G_1}	-
请求认证	$3T_{G_1}$	-	-
验证上传	-	$3T_e + 6T_{G_1}$	$2T_e$

为定量评估多安全级别椭圆曲线下的算法效率差异，本文选取 MCL 密码学库[15]下的四大主椭圆曲线构建基准测试集：100-bit 安全级别的 BN254，126-bit 安全级别的 BN381_1，128-bit 安全级别的 BLS12_381，134-bit 安全级别的 BN462。其相关群运算理论基准测试的测试结果具体数据如表 2 所示，从而得出本文方案中每阶段的理论计算代价如表 3 所示，根据表中数据计算出每阶段的计算开销均为毫秒级。

针对通信代价方面，TN 在请求认证阶段生成的认证消息 $\sigma_{TN} = (\sigma, \pi_{TN})$ 与发送数据 msg_{TN} 的理论大小为 $3|G_1| + 2|Z_q| + |msg_{TN}|$，即为 3 个 G_1 群元素、2 个 Z_q 群元素以及数据字符串。以椭圆曲线 BLS12_381 为基准，优化后的代数结构元素尺寸为 $|G_1|$ =48bytes 与 $|Z_q|$ =48bytes，由此得出最终发送一条认证消息的大小为 240 字节+$|msg_{TN}|$，足够在工业 CET 场景中快速传输。

Table 3. Benchmarking results of group operations theory for elliptic curve cryptography
表 3. 各椭圆曲线相关群运算理论基准测试结果

	BN254		BN381_1		BLS12_381		BN462	
	Android	PC	Android	PC	Android	PC	Android	PC
T_{G_1} (ms)	0.4874	0.0764	1.2568	0.197	1.186	0.186	5.461	0.856
T_{G_2} (ms)	1.341	0.183	3.533	0.482	3.408	0.465	12.395	1.691
T_e (ms)	4.9057	0.361	12.922m	0.949	9.205	0.676	35.3224	2.594

致　谢

将扰扰，付悠悠。感谢一切参与本文撰写工作的作者。

参考文献

[1] Zhou, X.K., Xu, X.S., Liang, W., *et al*. (2021) Intelligent Small Object Detection Based on Digital Twinning for Smart Manufacturing in Industrial CPS. *IEEE Transactions on Industrial Informatics*, **18**, 1377-1386.

[2] Tan, T., Zhao, M. and Zeng, Z. (2022) Joint Offloading and Resource Allocation Based on UAV-Assisted Mobile Edge Computing. *ACM Transactions on Sensor Networks*, **18**, 1-21. https://doi.org/10.1145/3476512

[3] Tian, J. and Ni, R. (2024) An Identity Authentication and Key Agreement Protocol for the Internet of Vehicles Based on Trusted Cloud-Edge-Terminal Architecture. *Vehicular Communications*, **49**, Article ID: 100825. https://doi.org/10.1016/j.vehcom.2024.100825

[4] Cui, J., Wei, L., Zhang, J., Xu, Y. and Zhong, H. (2019) An Efficient Message-Authentication Scheme Based on Edge Computing for Vehicular Ad Hoc Networks. *IEEE Transactions on Intelligent Transportation Systems*, **20**, 1621-1632. https://doi.org/10.1109/tits.2018.2827460

[5] Tian, J., Wang, Y. and Shen, Y. (2024) An Identity-Based Authentication Scheme with Full Anonymity and Unlinkability for Mobile Edge Computing. *IEEE Internet of Things Journal*, **11**, 23561-23576. https://doi.org/10.1109/jiot.2024.3385095

[6] 解可旺. 基于区块链的智能电网可追溯匿名认证[J]. 软件导刊, 2024, 23(12): 174-180.

[7] Wang, J., Wu, L., Choo, K.R. and He, D. (2020) Blockchain-Based Anonymous Authentication with Key Management for Smart Grid Edge Computing Infrastructure. *IEEE Transactions on Industrial Informatics*, **16**, 1984-1992. https://doi.org/10.1109/tii.2019.2936278

[8] Mohammed, B.A., Al-Shareeda, M.A., Manickam, S., Al-Mekhlafi, Z.G., Alayba, A.M. and Sallam, A.A. (2023) Anaa-fog: A Novel Anonymous Authentication Scheme for 5g-Enabled Vehicular Fog Computing. *Mathematics*, **11**, Article No. 1446. https://doi.org/10.3390/math11061446

[9] Mundhe, P., Yadav, V.K., Singh, A., Verma, S. and Venkatesan, S. (2020) Ring Signature-Based Conditional Privacy-Preserving Authentication in VANETs. *Wireless Personal Communications*, **114**, 853-881. https://doi.org/10.1007/s11277-020-07396-x

[10] Wang, Y., Wang, X., Dai, H., Zhang, X. and Imran, M. (2023) A Data Reporting Protocol with Revocable Anonymous Authentication for Edge-Assisted Intelligent Transport Systems. *IEEE Transactions on Industrial Informatics*, **19**, 7835-7847. https://doi.org/10.1109/tii.2022.3226244

[11] Huang, W., Du, H., Feng, J., Han, G. and Zhang, W. (2023) A Dynamic Anonymous Authentication Scheme with Trusted Fog Computing in V2G Networks. *Journal of Information Security and Applications*, **79**, Article ID: 103648. https://doi.org/10.1016/j.jisa.2023.103648

[12] Wu, F., Li, X., Luo, X. and Gu, K. (2022) A Novel Authentication Scheme for Edge Computing-Enabled Internet of Vehicles Providing Anonymity and Identity Tracing with Drone-Assistance. *Journal of Systems Architecture*, **132**, Article ID: 102737. https://doi.org/10.1016/j.sysarc.2022.102737

[13] Tanveer, M., Kumar, N., *et al*. (2023) SAAF-IoD: Secure and Anonymous Authentication Framework for the Internet of Drones. *IEEE Transactions on Vehicular Technology*, **73**, 232-244.

[14] (2023) Hyperledger Fabric. https://www.hyperledger.org/blog/2023/02/16/benchmarking-hyperledger-fabric-2-5-performance

[15] Jyothilakshmi, K.B., Robins, V. and Mahesh, A.S. (2022) A Comparative Analysis between Hyperledger Fabric and Ethereum in Medical Sector: A Systematic Review. In: Karrupusamy, P., Balas, V.E. and Shi, Y., Eds., *Sustainable Communication Networks and Application*, Springer, 67-86. https://doi.org/10.1007/978-981-16-6605-6_5