基于差分隐私的区块链工业物联网

唐珂盖，IEEE 成员，吴，刘烈煌朱，IEEE 成员，，IEEE 成员，邱，IEEE 高级成员

摘要——同时，两种新兴技术，区块链和边缘计算，正在推动物联网领域戏剧性的快速增长。应用边缘计算的好处是云计算可采用的互补性；区块链是为数据存储/治理构建透明安全环境的替代方案。本文提出了一种将物联网与边缘计算和区块链相结合的新方法，称为基于区块链的边缘互联网模型。该模型设计用于可扩展和可控的物联网系统，充分利用边缘计算和区块链的优势建立隐私保护机制，同时考虑其他约束，如能源成本。我们实现了在以太网上运行的实验评估。根据我们收集的数据，所提出的模型改善了隐私保护，而不会以节能的方式降低性能。

索引术语—物联网、区块链、隐私保护、差异隐私、边缘计算、任务分配

F

一 介绍

移动设备在当代社会的广泛应用已经显著推动了一个集成的网络环境，例如物联网(IoT)[1]–[5]。将云计算引入物联网被广泛认为是一种集中式计算解决方案，通过它可以交付繁重的计算任务或多功能。云部署有助于那些计算能力有限的设备扩大服务范围。在各个领域都产生了巨大的影响。远程医疗[6]、手机银行和手机租赁。可以观察到，云解决方案是集中式计算的一种表现形式，它通常简化了用户端的硬件/软件配置[7]。

尽管实施云计算有许多优点，但随着移动性中计算能力的增强，纯集中式服务部署不再是唯一的选择。例如，在终端用户和云服务器之间的通信过程中发生的能源浪费可能是不值得的，因为一些移动设备或本地附近的设备可以以更低的能源成本提供类似的服务。

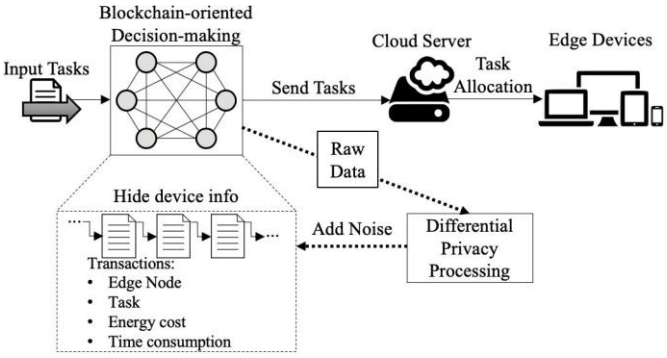
- *K. 盖(第一作者)，y。吴，l。朱和 z。张，北京理工大学计算机科学与技术学院，中国，北京，100081，，，。*
- *米（meter 的缩写））。邱，美国纽约州纽约市哥伦比亚大学电气工程系，邮编 10027。*
- *长度。朱是相应的作者(lie huanz @ bit . edu . cn)。*

- *这项工作得到了美国国家自然科学基金的资助中国(批准号。61972034)，北京理工大学青年学者研究基金项目(博士。唐珂.盖)。*

本地物联网部署的普及进一步加强了内部计算[8]。因此，作为一种新兴技术，边缘计算正在成为补充云系统的替代方法。在连接环境中，物联网系统中可以包含边缘设备，因此可以将任务迁移到空闲的边缘机器[9]，[10]。

此外，目前影响网络部署的另一个技术流行语是区块链。区块链的基因是保护隐私，因为使用别名可以掩盖区块链系统中所有参与者的真实身份。此外，区块链是一种分散的分类账存储系统，这决定了存储在链上的信息是不可改变的。实现区块链的其他特征主要来自于它的分散设置，例如容错、抗攻击和避免第三方风险。考虑到物联网的环境，区块链可以通过其分散的特性有效地发挥存储信息的作用。

尽管上述新兴技术得到了广泛应用，但构建物联网与边缘计算和区块链集成的蓝图仍不明确。这些机制之间的相互联系尚不可知。本文致力于开发一种隐私保护的可扩展任务分配策略，并考虑了实践中的其他约束。该方法被称为基于区块链的边缘互联网模型。图。1 展示了我们模型的架构，它展示了一个高层次的生物工程结构。如图所示，区块链正在扮演一个关键角色，负责信息保存和参与任务分配。在决策过程中可以应用一些参数，例如边缘节点，



图。1:提议模型的架构。

任务、能源成本或时间消耗。

这项工作的主要目的是利用区块链构建一个任务分配的隐私保护环境。我们将区块链带到现场来实现几个目标，包括增强边缘节点的可信度、确保通信安全以及实现最佳任务分配。被广泛接受的是，区块链可以为分散化应用和值得信赖的服务做出贡献[11]–[13]。然而，在能量相关的信息存储中直接使用区块链的缺点之一是泄露边缘节点的

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TII.2019.2948094, IEEE Transactions on Industrial Informatics

身份。在这项工作中，提出了一种差分隐私方法来保护身份，通过这种方法，噪声被添加到那些存储在块中的数据。

从任务分配的角度来看，分配的目标同时考虑了边缘设备和云服务器。区块链系统提供了一个决策平台，所有参与者都有公平的机会获得分配，这取决于优先级的设置。我们将网络中参与任务交付的所有设备视为参与者。我们的模型解决的关键问题是，它在云/边缘场景中的任务分配过程中自然隐藏了边缘设备的身份。在这项工作中，我们在配置策略优先级时考虑了一种类型的约束情况，它结合了能量和时间成本。提议模型的细节将在后续章节中介绍。

这项工作的主要贡献概述如下:

1) 这项工作提出了一种结合区块链、边缘计算和物联网的隐私保护方法。我们在区块链使用别名功能，因此由于分散设置，连接环境中的所有边缘设备都是可变和可扩展的。我们的方法是一种利用区块链特性解决边缘计算中任务分配问题的可追踪机制。为了改善/调整容差误差，每个块存储分配信息。
2) 这项工作探索了在区块链系统中实现差分隐私技术，以防止基于数据挖掘的攻击对块上的信息造成影响。

本文其余部分按以下顺序组织:第 2 节简要总结了最近的相关研究。接下来，第 3 节给出了提议模型的细节.此外，我们在第 4 节介绍了模型中的核心算法，在第 5 节展示和分析了从我们的评估中收集的部分实验结果.最后，第六节总结了本文的工作。

2 相关著作

2.1 任务分配中的隐私问题

许多先前的研究评估了强化学习(RL)技术在任务分配中的应用[14]–[16]。在这些尝试中，有代表性的方法是学习来自边缘节点的反馈/估计，以构造参数并产生奖励函数。通常需要持续的学习来实现最佳的奖励功能。尽管许多先前的研究已经探索将 RL 与任务分配相结合，但我们的研究站在考虑最佳任务分配以及隐私保护的观点上。

任务分配问题，在一些场景中被称为任务调度，是一个经典的研究课题，由于各种面向服务的部署的出现，最近吸引了更多的关注，例如云计算和物联网[17]，[18]。这一领域的探索大多集中在优化目标[19]上，如节约能源成本或提高效率。大多数优化研究很少考虑隐私保护问题。在这一部分，我们总结了以往在任务分配问题上有代表性的隐私驱动研究。

我们观察到，许多先前的研究强调安全性/隐私性和性能之间的平衡。一般的研究方向是保证一个方面的性能(例如。隐私保护)，同时增加其他方面的保护，例如工作效率。因此，这类研究主要是抽象考虑两个或几个约束的优化问题。比如龚等人。[20]提出了一种方法，该方法支持移动设备与临时移动云共享资源，同时考虑地理信息保护。这种方法基于差别隐私，并平衡了一些变量，如隐私、效用和系统开销。

在嵌入式系统环境中，该工作[21]完成了对汽车电子系统控制器局域网通信安全的尝试。这项工作主要解决了一个同时满足安全性和安全性要求的映射问题。此外，该工作[22]将多处理器片上系统任务调度公式化为多维优化问题，考虑了安全约束。所提出的启发式算法也可以应用在云实现中。其他涉及类似研究主题的工作包括[23]，[24]。

与之前的工作不同，我们的工作引入了区块链的实现，以自然地保护分配基础设施的隐私。任务分配中隐私保护的核心之一是隐藏设备的身份。区块链体系中没有替代机制。在我们的方法中，系统优化可以很好地嵌入到构造块的操作中。下一节简要回顾了当代云/边缘系统中的区块链技术。

2.2 云/边缘计算中的区块链

区块链是一组使用区块进行透明、可追踪和防篡改操作的相关技术.如上所述，最近的许多研究强调了区块链的特点，以探索其潜在的实施方式。我们观察到，各种各样的领域都在试图利用这项技术来建立一个安全、公平和可审计的环境。

一个流行的领域是在基于云的医疗保健中使用区块链[25]，[26]。该领域的隐私泄露威胁来源于互联环境下的医疗信息共享。未知的医生或意想不到的服务提供者可能可以访问数据，尽管患者，即数据所有者，对服务界面背后的信息使用了解有限。这种类型的研究已经被许多最近的研究所探索[27]。

比如夏等人。[28]开发了一个基于区块链的医疗系统，用于监测医疗数据的使用情况。监控操作依赖于记录数据访问的所有活动，这是通过为每个活动构造一个块来实现的。这种方法利用了区块链的可追溯性，因此所有与数据访问相关的行为都以防篡改的方式记录下来。另一项工作[29]从不同的角度利用区块链提高了医疗数据的安全性。该作品从基于属性签名的角度使用了区块链；然而，其工作原理类似于谢等人的方法[28]，该方法也利用了的可追溯特性。在每个块中，通过记录数据用户的属性和多权限匹配的结果来存储访问动作。

在医疗数据共享中使用区块链只是研究方向的一个样本。事实上，实施区块链有许多领域，如数据存储、审计、金融服务等[30]–[32]。将云/边缘计算与区块链相结合是不切实际的，因为两个系统通常为不同的功能单元分别运行。云/边缘计算大多被认为是服务模式的媒介[33]；区块链在构建权力下放以实现某些功能方面发挥了作用[34]。然而，很少有人探索区块链和云/边缘计算的无缝集成。

此外，许多领域已经使用区块链技术来保证隐私保护。比如柯等人。[35]通过使用区块链和边缘计算构建了一个

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TII.2019.2948094, IEEE Transactions on Industrial Informatics

基于区块链的隐私保护移动众测系统。该系统提出了一种信誉管理方案，以保护用户隐私，抵御恶意用户。Axin 等人。[36]提出了一种高效且隐私保护的加密方案来追踪用户在数据共享领域的属性。该方案利用区块链的特点来保证数据的完整性和不可否认性，以保证数据的安全性和隐私性。

总之，我们的工作是尝试将边缘计算和区块链合并成一个新的合并形式。与之前的工作不同，我们的尝试是试图将区块链与边缘计算相结合，这使得区块链成为任务分配的技术组成部分。我们将在下一节详细介绍我们的模型。

3 提议的模型

3.1 威胁环境

由于存储在数据块中的所有数据对所有区块链用户都可用，因此我们模型的对手可以完全访问这些数据。基于数据挖掘的攻击方法被认为是主要的恶意活动。我们模型中定义的主要威胁是双重的。

第一个威胁是恶意用户发起恶意活动来映射边缘计算的基础设施。我们假设对手打算偷偷观察边缘系统的结构。尽管作为边缘节点的区块链的数据、任务、能量成本和时间消耗仅局限于记录要求，例如。分配计划，这些准确的信息可以作为发动联动攻击的参考。考虑到内部攻击，所有对手都有合法的角色来获得请求服务的授权，并且支持数据库是可访问的。边缘系统的基础设施可以通过单个/多个恶意用户发起的多次尝试进行映射。

此外，我们还考虑了恶意用户的其他威胁，但对抗行动的重点是窃取身份信息，如地理数据和能源成本信息，这将泄露边缘节点的身份信息，让对手知道边缘节点执行的特定任务。我们假设所有对手都与边缘节点有合法的通信协议，因此通信时间是可测量的。这会导致地理信息泄露，因为攻击者可以通过测量/比较延迟来估计物理距离。

3.2 模型设计

如前所述，我们的生物进化模型实现了一种差分隐私技术来筛选原始分配数据，并利用区块链来支持边缘计算中的任务分配。该模型中有许多关键组件，包括智能合约、边缘节点、优化服务器和块(用于记录执行任务的边缘节点的动作、能量成本和时间消耗)。我们为每个角色提供一个简短的总结，如下所示。

在我们的模型中，供应链的作用是将任务转移到运营部门，以便在运营部门之间处理它们，并记录相应的行动、能源成本和时间消耗。此外，ENs 需要执行任务并计算时间消耗和能量消耗，以获得即时奖励。此外，

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TII.2019.2948094, IEEE Transactions on Industrial Informatics

TABLE 1: Main notations used in this paper and the definitions.

Notations	Definitions
SC	Smart Contract, referring to a kind of computer trading protocol executing contract terms and plays a role of transferring tasks and recording data
ENs	Edge Nodes, referring to edge devices which compose industrial internet of things
W_j	Optimization Server which is used to Q-learning technique to achieve task allocation for ENs
N_i	Tasks which need to be distributed to ENs to execute, where $j \in m$, m is the amount of tasks Notation
E_{t+1}^{i/W_j}	for edge nodes, where $i \in k$, k is the amount of ENs
T_{t+1}^{i/W_j}	Energy cost for EN N_i executing task W_j at time t+1
r_{t+1}^{i}	Time consumption for EN N_i executing task W_j at time t+1
α	Referring to the reward function at time t+1 when EN N_i executes task W_j
ϵ	Balance factor between energy cost and time consumption for EN executing tasks which affects the weight of reward function
$n_{s,max}$	The parameter to decide greedy algorithm
$n_{s,t}$	The amount of state set for Q-learning algorithm
ϵ_{min}	The amount of states currently explored
ϵ_{max}	The minimum of exploration percentage of -greedy algorithm
$Q(s_t, a_t)$	The maximum of exploration percentage of -greedy algorithm
γ	Referring to the Q-value function for state s_t and action a_t at time t
$Q^*(s,a)$	Referring to a discount factor to instant reward
$\pi^*(s)$	The optimal Q-value function
$DP(E_i^{W_j})$	The optimal strategy
W_j	
N_i	
E_{t+1}^{i/W_j}	The energy cost for EN N_i executing task W_j which is processed by differential privacy algorithm
T_{t+1}^{i/W_j}	
r_{t+1}^{i}	
α	
ϵ	
$n_{s,max}$	
$n_{s,t}$	
ϵ_{min}	
ϵ_{max}	
$Q(s_t, a_t)$	
γ	
$Q^*(s,a)$	
$\pi^*(s)$	
$DP(E_i^{W_j})$	
OpS	

OpS 用于执行相应的 Q 学习算法，以实现最优 Q 值函数，该函数是未来的奖励和最优策略，用于将任务分配给 ENs 并与区块链上的智能合约进行通信。最后，区块链系统由记录相应数据的区块链组成。我们的模型设计功能块的目的是为了跟踪和调整。

在我们的模型中，SC 将这些需要由 ENs 处理的任务发送给 OpS。OpS 采用-贪婪算法和策略选择一个 EN 完成一个任务，实现 EN 完成相应任务的能量消耗和时间消耗。OpS 计算能量成本和时间消耗以获得即时奖励和 Q 值函数。此外，OpS 实现了最终的奖励和最终的最优 Q 值函数，以及决定某些 ENs 完成某些任务的最优策略。最后，OpS 会根据最优策略将相应的任务分配给 ENs。当 ENs 完成任务后，它们会将执行任务的 ENs 的动作、能量成本和时间消耗发送给 OpS，OpS 通过差分隐私技术处理能量成本数据。然后，供应链存储在区块链执行任务的能源消耗和能源消耗。

,,W_m}, ENs N = {N_1,N_2,…Wm}，*ENs N = {N1，N2，…,*。Nk}，SC on 区块链和 OpS，其中 m 是任务量，k 是 ENs 量。

在我们的模型中，OpS 是代理。我们模型的状态空间是不确定的 EN 执行不确定的任务。而动作空间 A 是 OpS 选择一个 EN 执行一个任务。(1).

$$r_{t+1}^{i} = \alpha E_{t+1}^{i/W_j} + (1-\alpha) T_{t+1}^{i/W_j}. \quad (1)$$

在 Eq。(1)α 是影响奖励函数权重的能量成本和时间消耗之间的平衡因子。E_{t+1}^{i/W_j}和T_{t+1}^{i/W_j}是 EN Ni 执行任务 Wj 的能源成本和时间消耗。α 越大，能量成本对奖励函数的影响越大。α 越小，时间消耗对奖励函数的影响越大。

对于任务分配，OpS 选择-贪婪算法选择 ENs 来处理任务。贪婪算法可以用等式表示。(2).

$$\epsilon = min(\epsilon_{max}, \epsilon_{min} + \mu(n_{s,max} - n_{s,t})/(n_{s,max}). \quad (2)$$

在 Eq。(2)，∏0，1]，ns，max 是状态集的数量，ns，t 是当前探索的状态的数量。ϵ_{min}和ϵ_{max}分别是贪婪算法的最小和最大探索百分比。

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TII.2019.2948094, IEEE Transactions on Industrial Informatics

我们的 Q 值函数由等式定义。(3).

$$Q(st，at) = Q(st，at)+\alpha(r+\gamma Q(st+1，at+1)Q(ST，at))。 \quad (3)$$

在等式中。(3)γ∏0，1]是折扣因子，对即时奖励很重要。γ 越大，Q 值函数越重要。γ 越小，奖励功能越重要。

OpS 将根据 Eq 的最优策略分配任务。(4).

$$\pi \sum(s)= ArgMaxQ\sum(s，a)。 \quad (4)$$

在 Eq。(4)Q∑(s，a)表示最优 Q 值函数。

在 OpS 达到最优策略 π∑(s)后，OpS 会将任务分配给相应的 ENs。我们设置一个四元组$\langle N_i, W_j, DP(E_i^{W_j}), T_i^{W_j}\rangle$来表示一个 EN Ni 执行一个任务 W_j 并产生能量成本 $DP(E_i^{W_j})$ 和时间消耗 Ti j，其中$DP(E_i^{W_j})$意味着 Ei j 由差分隐私算法处理。$\langle N_i, W_j, DP(E_i^{W_j}), T_i^{W_j}\rangle$供应链需要将四元组区块链存储在上，以便于追溯和调整任务分配。

差分隐私算法通过在查询结果中加入噪声来保护数据隐私。目前差分隐私算法主要采用拉普拉斯机制和指数机制两种方法。在我们的模型中，我们使用拉普拉斯机制[37]将噪声添加到能量成本集中。在[37]中，他们的差分隐私保护方法由等式表示。(5).

$$Pr[M(Q,D)=S] \propto exp(\frac{\epsilon}{\triangle Q}|S-Q(D)|_1). \quad (5)$$

在 Eq。(5)、它包括如下一些参数。*m()是基于拉普拉斯机制的差分隐私保护算法*。函数 Q 是数据集 d 的映射函数。集合 S 是由服从拉普拉斯分布和平均值的 M()产生的噪声集合。功能敏感度 4Q 和隐私保护级别，与隐私保护程度成正比，与数据可用性成反比。此外，他们的方法使用了由等式表示的概率密度函数。(6)使附加噪声服从拉普拉斯分布。

$$Pr(x,\lambda)=\frac{1}{2\lambda}e^{\frac{-|x|}{\lambda}}. \quad (6)$$

在 Eq。(6)、$\lambda = \frac{\triangle Q}{\epsilon}$和 x 是数据。他们使用差分隐私保护算法 M()向查询结果添加噪声，由等式表示。(7).

$$M(Q,D)=Q(D)+(Lap_1(\frac{\triangle Q}{\epsilon}) \\ (Lap_2(\frac{\triangle Q}{\epsilon}),\ldots,(Lap_m(\frac{\triangle Q}{\epsilon})) \quad (7)$$

在 Eq。(7)，$Lap_j(\frac{\triangle Q}{\epsilon}), i \in k$，是受拉普拉斯分布约束的查询数据的噪声。此外，4Q 是两个相邻数据集 D 和 D0 的两个查询结果的最大值，可以用等式表示。(8).

4Q =最大值{ | Q(D)–Q(D0)| 1 }。(8)

在我们的模型中，我们设置了隐私保护级别，并实现了数据集 E(能量成本集)。然后，我们生成噪声$Lap_j(\frac{\triangle Q}{\epsilon})$，以满足概率密度函数$Pr(E_i^{W_j},\lambda)$和

$$Pr(E_i^{W_j},\lambda)=\frac{1}{2\lambda}e\frac{-E_i^{W_j}}{\lambda}. \quad (9)$$

为了情商。(9)我们设$\lambda = \frac{\triangle Q}{\epsilon}$和$\triangle Q = E_i^{W_j}$ △。为了保护 ENs 的隐私，我们添加了$Lap_j(\frac{Q}{\epsilon})$代表的噪声情商。(10).

$$DP(E_i^{W_j}) = E_i^{W_j} + Lap_j(\frac{\triangle Q}{\epsilon}). \quad (10)$$

我们在下一节介绍主要算法。

算法 4.1 分配任务算法

要求:输入任务(W[m])、ENs (N(k))、折扣系数γ、平衡系数α

确保:最佳策略 π∑(s)

1: OpS 初始 Q(s，a) = 0，π(s)，s = s0

2:对于 t=1，2，... 做

3: OpS 确保其状态为 st

4: OpS 根据$\pi(s)$ and ϵ -贪婪算法选择一个 EN Ni 来处理任务 Wj

i/Wj

5: 镍产生能量成本 Et 和时间消耗

Tt 国际

法院

6: OpS 计算奖励函数 rti = αEti/Wj + (1)

i/Wj

α)Tt

7: OpS 计算 Q(st，at) = Q(st，at) + α(r + γQ(st+1，at+1)Q(ST，at))

8: OpS 计算策略 π(s) = argmaxQ(s，at+1)并设置 s = st

9:结束于

10:π∑(s)=π(s)11:返回

π∑(s)

四 算法

4.1 任务分配算法

分配任务算法是为在边缘节点之间分配任务而设计的。我们使用 RL 技术从迭代中构造近似最优解。实施 RL 技术的原因是为了提高在不断变化的应用场景中的可采用性。最近的一些研究[38]、[39]已经证明了 RL 在任务分配中的性能。算法 4.1 给出了分配任务算法的伪码。该算法的主要

输入包括一个输入任务，用 M[m]表示。一个输入 ENs，用 N(k)、折扣因子 γ 和平衡因子 α 表示，如伪码所示。分配任务算法的输出是最优策略 π∑。

我们将任务分配算法的主要阶段介绍如下:

1) 首先，OpS 需要初始化 Q(s，a) = 0，设置策略 π(s0)。然后，OpS 需要运行 t 次循环来实现最优策略 π∑(s)。
2) 在这个循环中，OpS 首先确保其状态 st，然后选择一个 EN

能源成本 Et 和时间消耗 Tt。然后 OpS 使用E_t^{i/W_j}和T_t^{i/W_j}计算奖励函数 RTI =αEtiWj+(1α)TtiWj。最后，OpS 计算策略 π(st) = argmaxQ(s，at+1)。

3) OpS 需要实现最优策略 π∑(s)来在 ENs 之间分配任务。所以，当 t 次循环结束，π∑(s)=π(s)时，可以得到 π∑(s)。

总之，这种算法使操作系统能够通过反向学习技术在进化网络之间分配任务。

算法 4.2 分配块创建算法

要求:输入任务(W[m])、en(N(k))和隐私保护级别
确保:四件套
1:供应链向运营部门发送任务
2: OpS 调用算法 4.1，以实现将 W[m]分配给 N[k]的最优策略 π∑(s)
3: OpS 成就集
4:对于 j = 0；j < m；j++ do
5: 操作系统产生噪音
$Lap_j(\frac{\triangle Q}{\epsilon})$
6:OpS 将噪音添加到查询结果中 sult 到
$DP(E_i^{W_j})$类别共计(E k
7:结束于
8: OpS 发送给$T_i^{W_j}$
9:SC storeset 类中区块链
10: returnsetset 这

3.6Biphasic assays

Reactions were performed with TOYF or PETNR under biphasic conditions to minimise water-mediated side reactions and improve substrate/product solubility (ESI Table S6). The solvents iso-octane, n-octanol and tert-butylmethyl ether (TBME) have been used previously in biphasic reactions with of a variety of OYEs. Experiments over 24 h involved seven oxidative substrates with either a photosensitizer ([Ru(bpz)2dClbpy)]Cl 50 mM TEA) or a NADPH

4.2 分配块创建算法

*分配块创建任务算法是为存储执行任务的实体的相应动作、能量成本和时间消耗而设计的。*算法的主要输入是任务 W[m]、ENs N(k)和隐私保护级别。该算法的输出是四元组$\langle N_i, W_j, DP(E_i^{W_j}), T_i^{W_j}\rangle$集。

我们将分配块创建任务算法的主要阶段介绍如下:

1) 首先，供应链向运营部发送任务。然后，OpS 调用算法 4.1 使用 Q 学习技术实现最优策略 π∑(s)将任务 W[m]分配给 ENs N[k]。OpS 选择某些 ENs 来执行某些任务，以实现能源成本和时间消耗。操作系统达到$\langle N_i, W_j, E_i^{W_j}, T_i^{W_j}\rangle$设定。
2) 为了确保系统的可追溯性，OpS 需要发送 SC $\langle N_i, W_j, E_i^{W_j}, T_i^{W_j}\rangle$集。但是，由于 ENs 的隐私性，SC 无法实现$E_i^{W_j}$。因此我们选择差分隐私保护方法拉普拉斯机制来给$E_i^{W_j}$添加噪声，以保证能量代价集的隐私性。我们生成满足概率密度函数$Lap_j(\frac{\triangle Q}{\epsilon})$的噪声$Pr(E_i^{W_j}, \lambda) =$

倪根据-贪婪算法处理任务 Wj。Ni 执行 Wj 并产生相应的

i/Wj i/Wj

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TII.2019.2948094, IEEE Transactions on Industrial Informatics

$\frac{1}{2\lambda}e\frac{-E_i^{W_j}}{\lambda}$，哪里 $\lambda=\frac{\triangle Q}{\epsilon}$和 $\triangle Q=E_i^{W_j}$. 然后，OpS 计算$DP(E_i^{W_j})=E_i^{W_j}+Lap_j(\frac{\triangle Q}{\epsilon})$。

3) 当作战部计算出$\langle N_i,W_j,DP(E_i^{W_j}),T_i^{W_j}\rangle$设置，操作系统将$\langle N_i,W_j,DP(E_{\dot{W}}^{W_j}),T_{\dot{W}}^{W_j}\rangle$设置发送到 SC。

SC 将把 hNi、Wj、DP(Ei j)、Ti ji 集存储在区块链上。

$\langle N_i,W_j,DP(E_i^{W_j}),T_i^{W_j}\rangle$总之，该算法使供应链能够将四元组区块链集存储在上，以确保任务分配的可追溯性和调整性。

5 评价和调查结果

我们实施了一项实验评估来评估我们的生物工程模型的性能。节能效率不是我们评估的重点，因为我们的方法在给定的标准(单位时间内的能源成本)下固有地具有最优解。在我们的评估中，我们从隐私保护的角度强调了可行性，从而衡量了差异化隐私保护处理的能源成本、时间消耗和能源成本。我们分别在第 5.1 节和第 5.2 节介绍了我们的实验配置和部分结果。同时，第 5.3 节显示了安全性分析，第 5.4 节讨论了局限性和未来的工作。

5.1 实验配置

配置我们实验的原则是模拟基于边缘的物联网应用。在物联网系统中应用边缘计算通常由有限数量的边缘设备(节点)组成，这些设备主要是为特定目的/系统而部署的。因此，我们提出的模型具有较小范围的边缘节点，这与面向公众的区块链系统不同。

软件配置包括在计算机(MacBook Pro 2017 版)上运行的 Ethereum 客户端 Geth(1 . 8 . 3-稳定版)以及 Ethereum Wallet 0.10.0.硬件配置包括一个 macOS 10.13.4 操作系统，一个 2.3GHz 的 CPU，一个 i5 版本的英特尔酷睿，一个 8 GB 的 2133 MHz LPDDR3 内存。任务分配和差分隐私保护算法的确定性编程是由运行在 py charm CE 2017 . 3 . 1 版本上的 python 计算语言编写的。

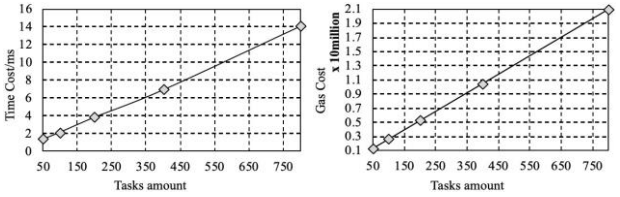
在实验评估中，主要测量目标包括数据打包时间、打包数据的气体成本、执行任务的能量成本、差分隐私保护处理的时间消耗和能量成本。我们在下一节介绍了一些评估结果。

5.2 实验结果

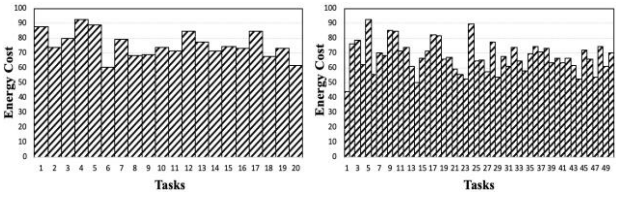
由于页面长度限制，我们展示了从本节实验中收集的部分评估结果。我们选择了一些有代表性的案例，这些案例有不同数量的任务来描述被检查变量的变化趋势，它们是 20、50、100 和 200。

图。2 显示了将配对参数打包到块的时间长度的结果，这些参数是 ENs Ni 设置的任务 *Wj 集、差分隐私保护处理的能量成本*$DP(E_i^{W_j})$*集和时间消耗*$T_i^{W_j}$*集*。根据我们的数据收集，打包这些数据的块创建时间范围在 1-15 秒内。数据打包到区块链的趋势是线性增长，这表明时间成本与任务数量呈正相关。

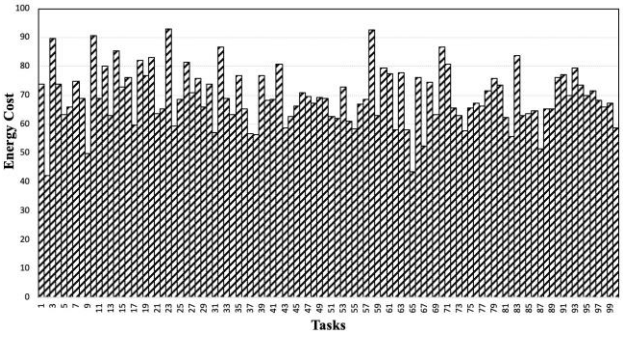
此外，图。图 3 显示了将上述数据打包到区块的天然气成本结果。根据图。3、瓦斯范围



图。2:包装的时间成本-图。3:打包四元组集到将四元组集打包到区块链的汽油成本。区块链。



图。4:欧洲标准图的能源成本。5:当任务数量为 20 时，一个工程师处理一项任务的能源成本.任务量为 50。



图。6:当任务数量为 100 时，EN 处理任务的能源成本。

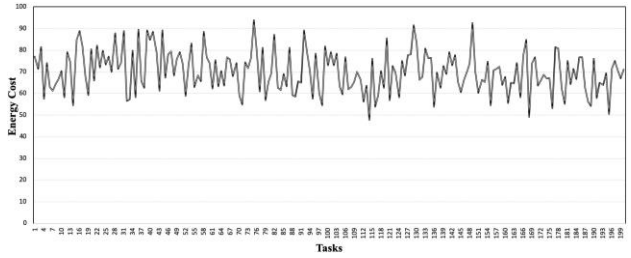
将数据打包到区块链的时间在 1×105 gas-21×105 gas 范围内。此外，将数据打包到区块链的天然气成本与任务量成线性关系。

图 4 -7 显示了一个执行某一任务的环境网络的能量成本，该任务遵循最优策略 π∑。不同的是任务数量的多样性:20、50、100 和 200.能源成本的多少与 ENs 的性能和完成任务的难易程度有关。类似地，从图。图 8。11，他们显示了

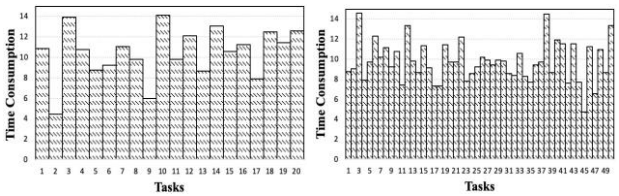
This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TII.2019.2948094, IEEE Transactions on Industrial Informatics

一个 EN 在任务数量为 20、50、100 和 200 的情况下执行某个任务的时间消耗。此外，时间消耗的数量与 ENs 的性能和完成任务的难度有关。

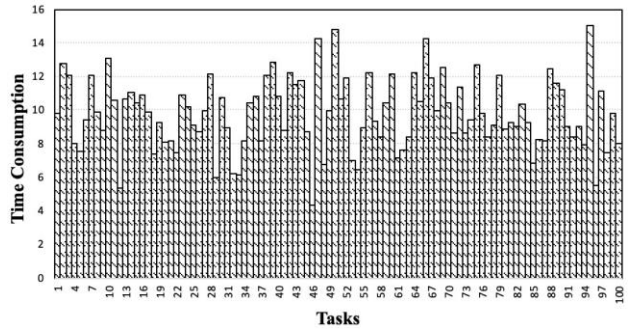
图。图 12。图 13。图 14 和。15 表示$DP(E_i^{W_j})$集，它是通过使用与图 1 相关的拉普拉斯机制的差分隐私保护的能量成本集。图 4。图 5。图 6 和图 7。7.从这些数字中可以看出，$DP(E_i^{W_j})$不是



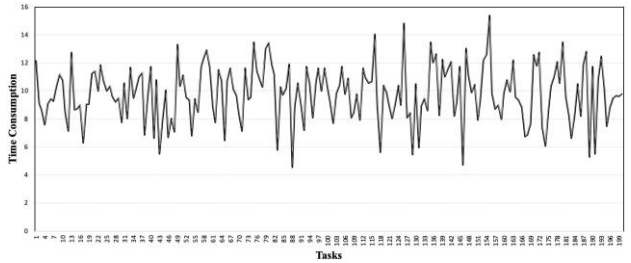
图。7:当任务数量为 200 时，EN 处理任务的能源成本。



图。8:图的时间消耗。9:当任务数量为 20 时，当一个 en 处理一个任务时，该 EN 处理一个任务的时间消耗.任务数量是 50。



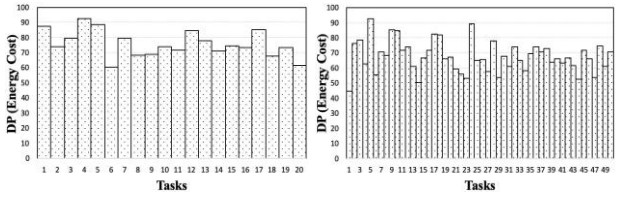
图。10:当任务数量为 100 时，EN 处理任务的时间消耗。



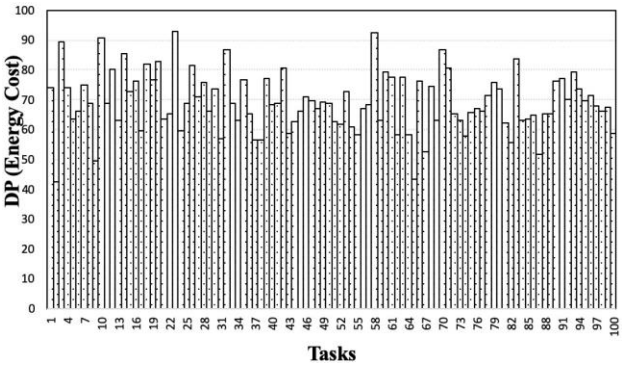
图。11:当任务数量为 200 时，EN 处理任务的时间消耗。

与$E_i^{W_j}$在能源成本设置的可用性方面有很大不同，$DP(E_i^{W_j})$保护了环境网络的隐私。

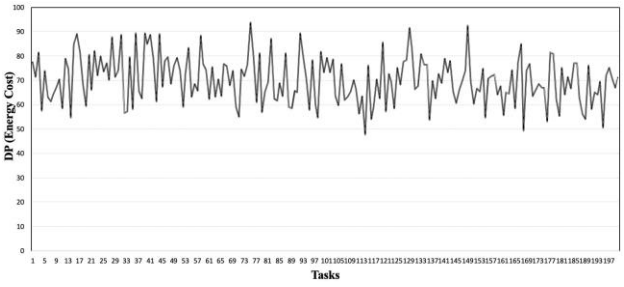
图 16 - 19 显示了原始的



图。12:能源成本保护图。13:当任务数量为 20 时，当 en 处理一个任务时，EN 处理一个任务的差分隐私保护的能量成本.任务数量是 50。



图。14:当任务数量为 100 时，处理任务的 EN 受差异隐私保护的能量成本。



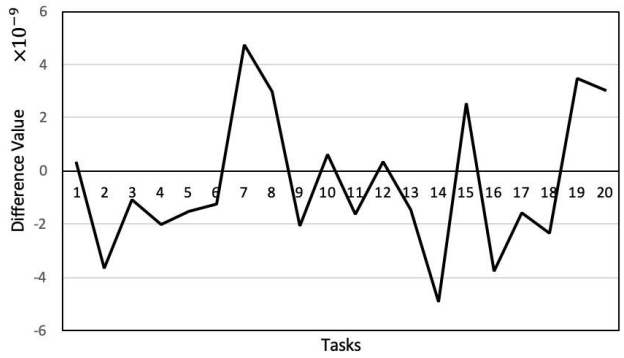
图。15:当任务数量为 200 时，处理任务的 EN 受差异隐私保护的能量成本。

能源成本数据和 DP-ed(能源成本)数据，通过差分隐私技术进行处理。在这些图中，我们可以了解到，能源成本和 DP(能源成本)之间的差值在 6∫10-9∨6∫10-9 之间.这些差

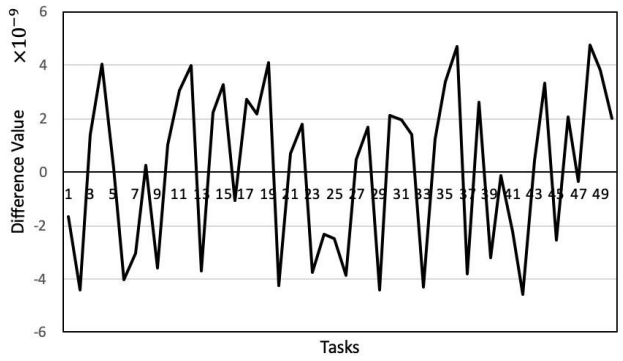
This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TII.2019.2948094, IEEE Transactions on Industrial Informatics

值并不显著，但它们可以有效地防止恶意用户获取原始数据和分析边缘节点的位置。

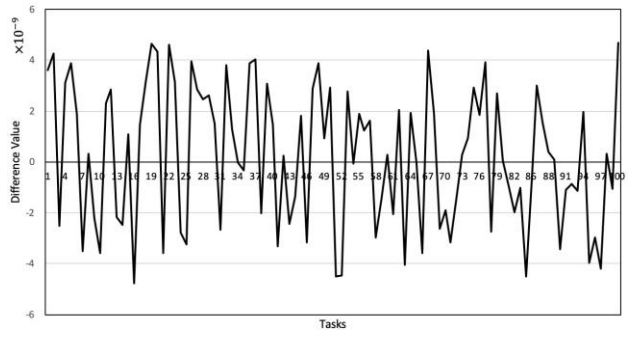
总之，我们评估的主要发现包括:(1)系统中的任务量与区块创建时间长度和天然气成本呈正相关；(2)能量成本和时间消耗与 ENs 性能和完成任务难度相关(3)差别隐私保护方法对数据可用性没有影响。



图。16:任务量为 20 时能源成本与 DP(能源成本)的比较)。



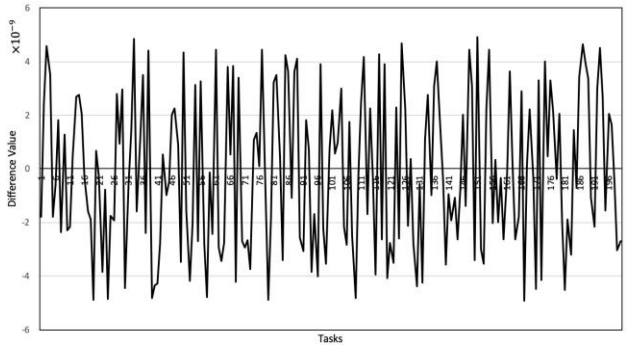
图。17:任务量为 50 时能源成本与 DP(能源成本)的比较)。



图。18:任务量为 100 时，能源成本与 DP(能源成本)的比较)。

5.3 证券分析

我们对提议的基于隐私的差分区块链系统进行了安全分析，该系统与第 3.1 节中给出的预定义威胁环境相关联。基于威胁假设，对手可以完全访问存储在数据块中的所有数据。两种类型的威胁，恶意用户发起恶意活动来映射基础架构



图。19:任务量为 200 时能源成本与 DP(能源成本)的比较)。

边缘计算和恶意用户窃取边缘节点的身份信息，我们的模型需要面对和解决。

$\langle N_i, W_j, DP(E_i^{W_j}), T_i^{W_j} \rangle$在我们的生物进化模型中，我们使用一个操作系统将任务分配给进化者和进化者来存储区块链上的四元组。对于第一类威胁，在不增加噪声的情况下，对手可以通过从开源访问支持数据库，从挖掘分配信息或发起链接攻击来映射边缘计算基础设施，从而轻松获得真实身份和行为隐私。幸运的是，我们的生物进化模型使用一种差分隐私保护方法(拉普拉斯分布机制)将噪声添加到能量成本集中，从而在保护目标集上产生失真。我们的观察是，利用拉普拉斯机制可以在考虑迭代需求的同时成功地筛选出 ENs 的真实分配信息。对于基于数据挖掘的攻击，从对手的角度来看，噪声会增加特征提取和信息检索的复杂性。此外，还可以采用附加噪声来保护用户身份，以避免第二类威胁，因为存储在区块链和其他支持已处理数据的数据库上的数据之间很难进行数据匹配操作。因此，实现我们的生物进化模型可以有效地增强隐私保护能力。

5.4 讨论

我们工作的新颖性是显而易见的。我们创造性地融合了一些新兴技术，包括边缘计算、物联网和区块链。该模型充分利用了每种技术的优势，在保证隐私保护和智能控制的同时，保证了任务分配的可操作性。尽管我们的模型很新颖，但在未来的工作中仍有一些限制/挑战需要解决。在这一部分，我们强调了在我们的研究中发现的一些可研究的问题。

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TII.2019.2948094, IEEE Transactions on Industrial Informatics

我们注意到供应链与任务分配的关系有限，因为任务分配大多由运营部完成。$\langle N_i, W_j, DP(E_i^{W_j}), T_i^{W_j} \rangle$ SC 的功能是将四元组区块链存储在上。由于上述问题，我们假设 OpS 是安全的。潜在的风险是当操作系统不安全时，任务可能会泄露给攻击者。

我们发现的另一个问题是，添加到能量成本集的噪声对能量成本集的数据可用性没有太大影响。我们的模型旨在保证数据的可用性，我们设置的噪声对能源成本设置的影响很小。由于我们设置的噪声，ENs 的隐私可能会受到失真程度对能量成本设置不大的影响。针对上述问题，我们的研究将在未来的工作中从这些角度不断探索我们的模型。

6 结论

本文重点设计了一种在物联网中实现边缘计算的隐私保护方案。所提出的方法被称为生物进化模型，它在任务分配中利用了区块链技术。实现了三个设计目标，使基于边缘的物联网系统具有任务分配功能、隐私保护和防篡改功能。我们的评估表明，我们的模型能够达到设计意图。

确认

本工作得到了国家自然科学基金(批准号。61972034)，北京理工大学青年学者研究基金项目(博士。唐珂·盖)。

参考

[1] 问。杨，b。朱，和s。吴。车载网络中云辅助信息传播的架构。*IEEE 接入，4:2764–2770，2016*。

[2] Z. 王 h。宋，d。沃特金斯，k。昂，p。薛，问。杨，还有 X. 石。水可持续性的网络物理系统:挑战与机遇。*IEEE 通信杂志，53(5):216–222，2015*。

[3] H. Mahdikhani 和 r。鲁。在雾计算增强物联网中实现隐私保护的多点积查询。2017 年 IEEE 全球通信大会，第 1-6 页，新加坡滨海湾金沙，2017 年.IEEE。

[4] T. 王，j。Y. 周，a。F. 刘，男。Z. A. 布伊扬，g。J. 王和 w。J. 贾。物联网中基于 Fog 的数据同步计算和存储卸载。*IEEE 物联网杂志，6(3):4272–4282，2019*。

[5] T. 王，l。邱，g。徐，a。K. 桑加亚，和 a。刘。物联网中基于移动雾计算的节能可信数据采集协议。*IEEE 工业信息学交易，第 1-1 页，2019 年*。

[6] C. 张，l。朱，c。徐和 r。鲁。PPDP:基于云的电子医疗系统中一种高效且隐私保护的疾病预测方案。*未来一代计算机系统，79:16–25，2018*。

[7] 米（meter 的缩写））。迪亚斯，c。沃尔玛和 b。卢比奥。物联网和云计算集成中的最新技术、挑战和开放问题。*网络和计算机应用杂志，67:99–117，2016*。

[8] J. 林，w。于，n。张，x。杨 h。张和 w。赵。物联网调查:架构、使能技术、安全和隐私以及应用。*IEEE 物联网杂志，4(5):1125–1142，2017*。

[9] 长度。雷 h。徐，x。熊 k。郑，和 w。项。nb-iot 边缘计算系统中基于近似动态规划的联合计算卸载和多用户调度。*IEEE 物联网杂志，6(3):5345–5362，2019*。

[10] T. 王 h。罗，j。X. 郑，和 m。谢。基于智能移动边缘计算的 CPC 信任评估众包机制。*智能系统与技术学术会议，第 1-1 页，2019 年*。

[11] J. A. Jaroodi 和 n。穆罕默德。工业中的区块链:一项调查。*IEEE 接入，7:36500–36515，2019*。

[12] 南。比斯瓦斯，k。谢里夫，f。李，b。努尔和 y。王。物联网安全交易的可扩展区块链框架。*IEEE 物联网杂志，6(3):4650–4659，2019*。

[13] 米（meter 的缩写））。Dabbagh。苏克和 n。南。萨法。区块链的演变:一项文献计量研究。*IEEE 接入，7:19212–19221，2019*。

[14] 南。鲁。Tessier 和 w。页（page 的缩写）。伯利森。热感知多核任务分配的强化学习。在第 25 版大湖超大规模集成电路研讨会上，第 379-384 页，2015 年。

[15] D. B. 努尔丁，a。加尔比和 s。B. 艾哈迈德。动态环境下任务分配的多智能体深度强化学习。在 2017 年第 12 届软件技术国际会议上，第 17-26 页。

[16] J. 姚和 n。安萨里。基于在线强化学习的移动物联网能量感知任务分配。2019 年 IEEE 国际通信会议，第 1-6 页，2019 年。

[17] C. Giovanelli。基尔基，s。西埃拉，我。塞罗宁和 v。维亚特金。提供频率遏制储备的能量资源任务分配算法。*工业信息学的 IEEE 交易，PP(99):1，2018*。

[18] J. 王，y。王，d。张，女。王 h。熊，c。陈问。吕，还有 z。邱。具有个体任务质量保证的移动人群感知多任务分配。*IEEE 移动计算交易，第(99)页:1，2018*。

[19] J. 米（meter 的缩写））。露娜，c。T. 阿卜杜拉和 g。长度。海尔曼。云中数据存储资源分配和加密的概率优化。*IEEE 云计算事务，6(2):428–439，2018*。

[20] Y. 龚，c。张，y。方，和j。星期日。移动云计算中任务分配的位置隐私保护。*《计算领域新兴主题的 IEEE 交易》，6(1):110–121，2018*。

[21] C. 林，问。朱，c。冯和甲。桑吉奥瓦尼-文森特利。基于 CAN 的实时分布式汽车系统的安全软件映射。《国际计算机辅助设计会议录》，第 115-121 页.IEEE 出版社，2013。

[22] C. 刘，j。拉金德兰，c。杨和 r。凯里。通过安全驱动的任务调度，保护异构 MPSoCs 免受不可信的 3p 的攻击。*《计算领域新兴主题的 IEEE 交易》，2(4):461–472，2014*。

[23] 南 。Basu。Karuppiah。Selvakumar。C. 李 。H. 伊斯兰，m。米（meter 的缩写））。哈桑和 m。Z. A. 布彦。云计算环境下物联网应用任务调度的智能/认知模型。*未来一代计算机系统，88:254–261，2018*。

[24] 长度。曾，b。维拉瓦利和 x。李。SABA:一种安全感知和预算感知的云工作流调度策略。*并行和分布式计算杂志，75:141–151，2015*。

[25] X. 李，p。江，t。陈，x。罗和阿 q。文。区块链系统安全性调查。*未来一代计算机系统，第 1-1 页，2017 年*。

[26] H. 田，j。他，还有 y。丁。区块链隐私医疗数据管理。*J. 医疗系统，43(2):26:1–26:6，2019*。

[27] C. 埃斯波西托 a。德森蒂斯峰。托尔托拉，h。常和周克瑞。区块链:医疗云数据安全和隐私的灵丹妙药？*IEEE 云计算，5(1):31–37，2018*。

[28] 问。夏，鄂。赛法，k。j .阿萨莫阿。高，x。杜，还有 m。吉扎尼。医疗共享:云服务提供商之间通过区块链实现无信任的医疗数据共享。*IEEE 接入，5:14757–14767，2017*。

[29] R. 郭，h。石，问。赵，和马超。郑。电子健康记录系统中基于属性的区块链多重安全签名方案。*IEEE 接入，776(99):1–12，2018*。

[30] J. r .康。于，x。黄，s。纽约马哈尔詹。张和 e。侯赛因。使用区块链财团实现插电式混合动力汽车之间的本地化点对点电力交易。*IEEE 工业信息学杂志，13(6):3154–3164，2017*。

[31] A. 雷 h。纽约克鲁克申克。曹，p。Asuquo，c。Ogah，和 z。星期日。基于区块链的异构智能交通系统动态密钥管理。*IEEE 物联网杂志，4(6):1832–1843，2017*。

[32] K. 克里斯蒂斯和 m。德弗茨基奥蒂斯。区块链和物联网智能合同。*IEEE 接入，4:2292–2303，2016*。

[33] X. 陈，l。焦，w。李，和 x。傅。面向移动边缘云计算的高效多用户计算卸载。*IEEE/ACM 网络交易，24(5):2795–2808，2016*。

[34] 南。安德伍德。比特币以外的区块链。*澳大利亚竞争管理委员会通讯，59(11):15-17，2016*。

[35] K. 赵，s。唐，b。赵，和 y。吴。基于区块链的移动众测的动态隐私保护信誉管理。*IEEE 接入，7:74694–74710，2019*。

[36] A. 吴，y。张，x。r .郑。郭，问。赵，和马超。郑。区块链高效且保护隐私的可追踪属性加密。*电信年鉴，74(7):401–411，2019 年 8 月*。

[37] C. Dwork，f。McSherry。尼西姆和 a。史密斯。校准私人数据分析中的噪声灵敏度。《密码学理论》，2006 年，第 265-284 页。

[38] J. 杨，x。你，g。吴，m。米（meter 的缩写））。哈桑，a。阿尔莫格伦和 j。古纳。强化学习在无人机集群任务调度中的应用。*未来一代计算机系统，95:140–148，2019*。

[39] 南。Mostafavi。艾哈迈迪，和 m。A. 萨拉姆。云计算中基于强化学习的前瞻任务调度。*CoRR，abs/1810.04718，2018*。

唐珂盖[M 17'-S 13']收到了英国国旗。自动化专业学位，中国南京南京科技大学，2004 年，加拿大不列颠哥伦比亚省温哥华市不列颠哥伦比亚大学教育技术硕士学位，2010 年，工商管理硕士学位，2009 年，信息技术硕士学位，2014 年，美国麻省理工学院南菲尔德劳伦斯理工大学，博士学位。美国纽约佩斯大学计算机科学学位。

他目前是计算机学院的副教授北京理工大学科学与技术学院，北京，中国。他出版了 3 本书和 100 多篇同行评议的期刊/会议论文，包括 6 篇 ESI 高被引论文。他获得了 5 项电气和电子工程师协会最佳论文奖(例如。TrustCom 18 '和 HPCC 18 ')和近 5 年的 2 个 IEEE 最佳学生论文奖。他的研究兴趣包括网络安全、区块链、边缘计算、云计算和强化学习。

吴，现任北京理工大学计算机科学与技术学院计算机科学专业硕士研究生。她的研究兴趣包括网络安全、区块链和云计算。

朱烈煌获得博士学位。2004 年获得中国北京北京理工大学计算机科学学位，工程硕士学位
分别于 2001 年和 1998 年获得中国武汉大学工学学士学位。

现任中国北京理工大学计算机科学与技术学院教授。他发表了 100 多篇同行评议的期刊或会议论文，包括 10+篇 IEEE/ACM Transactions 论文(IEEE TIFS、IEEE TII、IEEE TVT、IEEE TSG、信息科学、IEEE 网络、计算机与安全等)。他获得了多项 IEEE 最佳论文奖，包括 IWQoS 17′、TrustCom 18′。他的研究兴趣包括安全协议分析和设计、无线传感器网络和云计算。

张子健，现任北京理工大学计算机科学与技术学院副教授。他是布法罗纽约州立大学无处不在的安全和隐私研究实验室的访问学者。他在著名期刊和杂志上发表了 40 多篇论文，。TPSC、TCC、INS。他的论文被 2017 年 IEEE/ACM 服务质量国际研讨会授予 IEEE 最佳论文奖。他的研究兴趣包括认证和密钥协商协议、实体识别和行为识别。

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TII.2019.2948094, IEEE Transactions on Industrial Informatics

邱[SM 07']分别于 1992 年和 1998 年获得中国上海交通大学工学学士和硕士学位，2003 年获得计算机科学硕士学位，并获得博士学位。2007 年获得美国得克萨斯州达拉斯大学计算机科学学位。

现任美国纽约哥伦比亚大学兼职教授，中国深圳深圳大学计算机科学特聘教授。他出版了 15 本书，400 篇同行评议的期刊/会议论文，以及 3 项注册专利。他的研究兴趣包括网络安全、机器学习、大数据、云计算、异构系统和嵌入式系统。