Journal of Parallel and Distributed Computing 168 (2022) 1–16

Contents lists available at ScienceDirect

Journal of Parallel and Distributed Computing

www.elsevier.com/locate/jpdc

MB-MaaS: Mobile Blockchain-based Mining-as-a-Service for IIoT environments

Pronaya Bhattacharya [a], Farnazbanu Patel [a], Sudeep Tanwar [a,*], Neeraj Kumar [b], Ravi Sharma [c]

[a] *Department of Computer Science and Engineering, Institute of Technology, Nirma University, Ahmedabad, India*
[b] *Department of Computer Science and Engineering, Thapar Institute of Engineering and Technology, Deemed to be University, Patiala, Punjab, India*
[c] *Centre for Inter-Disciplinary Research and Innovation, University of Petroleum and Energy Studies, Dehradun, 248001, India*

A R T I C L E   I N F O

Article history:
Received 10 August 2021
Received in revised form 2 April 2022
Accepted 21 May 2022
Available online 30 May 2022

Keywords:
Mobile blockchain
Mobile edge computing
5G
Mining-as-a-Service
Data offloading

A B S T R A C T

In this paper, we propose a mobile blockchain (MB) based mining-as-a-service (MaaS) scheme, *MB-MaaS* for resource-constrained industrial internet-of-things (IIoT) environments. The scheme addresses the research gaps of fixed static allocation for miners to perform computationally intensive mining tasks through a multi-hop computational offloading (CO) scheme and addresses an auction mechanism for a fair bidding process among the miner nodes. The scheme operates in three phases. In the first phase, a multi-hop CO scheme with a fair incentive policy is formulated for miners. The CO schemes offer guaranteed offloading services to mobile devices from far-edge systems through a chain of neighbor nodes. Then, in the second phase, *MaaS* is proposed to leverage expensive mining tasks through 5G-enabled pico/femtocells. Integration of 5G allows massive end-to-end device and service connectivity. As IIoT ecosystems have limited memory and compute requirements, MaaS assures that the proposed consensus has a responsive validation and mining time. To make the data exchange in the consensus process lightweight, and allow a large number of sensors to share the data in a lightweight manner, an effective consensus mechanism Lightweight Proof-of-Proximity (LPoP), is proposed that forms group validations instead of single block validation. The data is exchanged through javascript object notation (JSON) format, maintaining a steady transaction rate. *MB-MaaS* is compared against the existing scheme for parameters bid thresholds and request servicing times, and mining and consensus formation. For example, the request serving time at 12 requests is improved by 56.78%, and a significant improvement of 26.47% is observed for processed blocks; parsing time on average is improved by 7.89%. The comparative analysis suggests that the scheme is more efficient than other competing approaches.

1. Introduction

Over the past decade, in the manufacturing sector, Internet of Things (IoT) ecosystems, including those in industrial IoT (IIoT) settings, have witnessed a significant increase in the deployment of sensors in low-powered IoT nodes. The sensor deployment is required to be planned judiciously, and recent schemes have suggested carrier-based deployment algorithms in IoT [6]. These (large number of) integrated sensor nodes generate significant data, which needs to be analyzed at nodes (e.g., edge nodes) with low storage and computing capabilities to enhance the user's quality of experience (QoE), for example, by reducing latency and delays. Mobile cloud computing infrastructures, for example, are deployed in IIoT ecosystems to support business analytics over open wireless channels. However, there are known limitations in this Mobile cloud computing-based infrastructure. Examples include inefficient load-balancing, service bottlenecks, centralized point-of-failures, end-user (EU) latency, and security attacks [27]. This necessitates the design of approaches to minimize computational overheads in IIoT settings without affecting security and privacy features.

There have been studies focusing on designing more efficient edge-based infrastructures over mobile edge computing (MEC), which enable seamless interaction with IoT sensors within cellular proximity of 1-2 hops [35], in an attempt to improve user experience and allow decentralization of service and network operations. However, in MEC infrastructures, data is forwarded to edge nodes (EN) over open wireless communications (e.g., using Zigbee, Blue-

* Corresponding author.
E-mail addresses: pronoya.bhattacharya@nirmauni.ac.in (P. Bhattacharya), 19mcei04@nirmauni.ac.in (F. Patel), sudeep.tanwar@nirmauni.ac.in (S. Tanwar), neeraj.kumar@thapar.edu (N. Kumar), ravisharmacidri@gmail.com (R. Sharma).

https://doi.org/10.1016/j.jpdc.2022.05.008
0743-7315/

tooth, and Z-Wave) that are power-hungry and resource-intensive. In other words, the open challenge is to design long-distance low-powered, energy-efficient, and space-constrained protocols for implementation in IIoT-based ecosystems. Moreover, sensor data spans heterogeneous autonomous systems through multiple IIoT stakeholders. Thus, there are also trust, and privacy considerations in such MEC-based constrained ecosystems.

There have been various solutions designed to facilitate privacy-preserving and trustworthy analytics, such as those using fifth-generation (5G) services and blockchain (BC). Also, owing to the shift of industrial operations towards massive customization and personalization, as presented with Industry 5.0 vision [23], a large amount of sensor integration and control is required. To enable seamless connectivity among devices, sixth-generation (6G) networks are also integrated with IoT solutions. A recent study by Lin et al. [19] has addressed the sensor integration with IoT underlying 6G communication channels. The scheme also addresses the security and privacy of data information through a proposed multi-objective problem. An ant colony optimization (ACO) algorithm is proposed that assures secure transfer of information and hides the sensitive attributes.

MEC simplifies the network functions at the 5G-radio access network (RAN) core units, which orchestrates virtual networking functions to allow seamless transfer of data, which can support a range of applications related to smart transportation, energy, unmanned aerial vehicles, healthcare, and others. 5G-MEC in IIoT setups would require low-powered resources, and thus to induce security and trust in such environments, BC is preferred. However, IIoT requires the support of lightweight validations, through effective consensus, that can be tailor-made to suit the particular application. A stripped-down version of BC, called mobile blockchain (MB), is more suitable that can be supported through low-powered hashing algorithms, which are perfectly suitable to edge environments [26]. The mining services would require low-energy consumption and, in case of heavy tasks, can be supported through an assisted Mining-as-a-Service (MaaS) ecosystem. However, while delegating tasks to MEC servers and validating transactions through MaaS, fair incentives for miner nodes are important. 5G-enabled MEC with MB in IIoT based ecosystems can be used to design a secure, trusted, scalable, responsive, and low-powered solution for data exchange among IIoT sensors. In BC-enabled MEC ecosystems, the EU can request real-time services based on effective pricing policies through EN, and data is offloaded through nearby edge devices [33]. To exploit the same, EN provides content-based caching services based on location and contextual queries of the EU. In case data is not present at the EN, a multi-hop offloading process is executed in the background to service EU request [13]. However, the data offloading process between EU and EN involves a transactional entry to be stored in a distributed ledger. In public BC, miners need to solve resource-intensive and complex Proof-of-Work (PoW) puzzles whose nonce value is smaller than the pre-specified target hash value. To solve the PoW puzzle, miners require high computational resources (CPU, memory, I/O, disk) and energy sources to solve PoW puzzles, which is not a scalable solution for energy-constrained IIoT applications. Thus, for IIoT applications, a consortium BC is a preferred approach. A consortium BC is permissioned and is managed through a group of collaborative entities that participate in the system. The participating entities manage the network policies, and consensus principles [7]. Research studies have suggested it as a viable choice to deploy a fast, resilient, and scalable BC. A permissioned network consumes less energy and power for block validation than public BC. However, a fair election process for validators (miners) is required to assure fairness in miner node selection.

To address the scalability issues of BC, a consensus mechanism for low-powered IIoT environments is proposed by Huang et al. [14]. The article discusses the limitations of centralized systems and how the systems are attack-prone owing to the single-point-of-contact. The authors proposed the integration of blockchain (BC) as a potential solution. To address the resource-intensive computation, they proposed a lightweight credit-based PoW mechanism based on direct acyclic graphs. In general, lightweight security mechanisms like elliptic-curve-cryptography (ECC)-based shared key, Diffie-Hellman (DH) signatures, and advanced encryption standard (AES)-128 in cipher block chaining modes are applicable in constrained IIoT [30]. Still, the systems are required to communicate data between nodes, where the behavior of a sensor node might be malicious. Thus, in distributed setups, to assure that the communicated data has not been tampered with, blockchain (BC) is the preferred choice. The only constraint is the expensive mining operation cost, which can be addressed by requesting the mining resources as services from edge nodes. Recently studies have suggested that integration of BC in IoT setups through lightweight consensus is a more preferred approach to assure reliable transfer [12]. Via 5G-MEC ecosystems, miners are granted mining resources as services, termed as MaaS from nearby stationed edge servers in dense pico/femtocells [10,32]. Deploying small cells improves bandwidth issues and provides high mobility to miners and the EU in BC. Computational offloading (CO) designed to expedite low-powered consensus and energy-efficient block formation is termed MB [34]. CO also needs a proper pricing scheme for providing resources to the miners by an EN. The pricing scheme is necessary to pay offloaded resources to the EN. Table 1 presents the lists of acronyms and notations used in the paper.

Table 1
Acronyms and notations.

Acronyms	Meaning
MB	Mobile Blockchain
EU	End User
EN	Edge Nodes
ES	Edge Server
BC	Blockchain
CO	Computational Offloading
ESP	Edge Service Provider
E	Entity set
E_x	Any entity x (Eg. E_{CS} is entity CS}
CS	Cloud Server
U_n	User n in User entity E_U
S_m	Sensor m in Sensor set
D_n	Data generated by user n
D_{S_m}	Data present at sensor node S_m
A_q	requested allocation by q^{th} miner
B_q	bidding price for the allocation by q^{th} Miner
C_{U_n}	Crypto currency available in Wallet W_{U_n}
Win_{ID}	Winner ID (=1, if resource is granted) of corresponding miner
W_{total}	Total number of winners decided by Entity E_{ES}
$W_{threshold}$	Maximum threshold number of winners
VM ID	Identity of Virtualization Model

1.1. Motivation

5G-enabled MEC infrastructures are deployed in constrained IIoT setups to address the challenges of EU latency and balance the overall loads on the nodes in the network. Resource-intensive tasks are offloaded to MEC nodes, and thus in such infrastructures, trust among the exchanged data is a prime concern. Thus, BC leverages a trusted chronology among the exchanged data. With BC inclusion, researchers have proposed MaaS with PoW to address the computational requirements and have proposed solutions where optimal scenarios of offloading and resource maximization are required. In such cases, the BC processes become lightweight, and MB is envisioned. However, another critical aspect is the fairness of PoW, which is often questioned on Byzantine security levels (network

Table 2
Relative comparison of existing state-of-the-art approaches.

Authors	Pico/Fe-mto Cells	MaaS	Energy-efficient consensus	Caching	Offlo-ading	Technique used	Environment
Liu et al. [20]	✗	✗	✗	✓	✓	Edge-based CO scheme based on stochastic geometry theory	Wireless Mobile BC networks
Bhattacharya et al. [2]	✓	✓	✗	✓	✓	Low-Latency content caching and offloading strategy in BC	BC-based MEC infrastructures
Liu et al. [21]	✗	✗	✗	✓	✓	D2D-caching and offloading strategy based on alternating direction method of multipliers (ADMM) model	BC-based MEC framework
Xiong et al. [31]	✗	✓	✗	✓	✓	Optimal pricing schemes for miners based on sub-game perfect equilibrium and Stackelberg Game	Cryptocurrency mining and pricing.
Jiao et al. [15]	✗	✗	✓	✗	✓	Auction-based edge computing in BC with low-powered resource allocation for miners based on social-welfare maximization strategies	Low-powered IoT
Li et al. [18]	✓	✓	✗	✗	✓	Parallel encrypted-offloading of tasks of mobile users to edge-servers	Encrypted IoT environments
Wang et al. [28]	✗	✗	✗	✓	✓	An optimal winning-bid model based on Vickrey- Clarke-Groves (VCG) based auction mechanism that achieves computational efficiency	Mobile-Device Clouds
Liu et al. [22]	✗	✓	✗	✗	✓	The smart contract based double auction mechanism to achieve the total utility of the auction participants	Wireless Mobile BC networks
Chen et al. [5]	✗	✓	✗	✗	✓	Multihop computational offloading for data processing and mining tasks	Blockchain empowered IIoT
Li et al. [17]	✗	✗	✓	✗	✗	Energy efficient consensus mechanism E-Raft for autonomous underwater vehicles	Blockchain based Multi-AUV system
T. et al. [1]	✗	✓	✓	✗	✗	A Machine learning Consensus based Light-weight Blockchain (MCLB) that is proposed for IoT environments, where edge nodes runs ML algorithm for consensus	Resource constrained IoT environment
MB-MaaS (The proposed approach)	✓	✓	✓	✓	✓	A CO scheme based on energy-efficient mining schemes based on fair incentive policy	Resource-constrained IIoT.

security in case an attacker holds less than 50% of power), and security of the algorithm in case the validator is malicious. PoW is tilted towards high computing machines and electric power and thus is not good for a fair economic model. Thus, to address the gap, the proposed scheme, *MB-MaaS* proposes a multi-hop offloading scheme coupled with a fair auction protocol that allows miners to get employ fair reward fees for mined transactions based on the distance of EN from the miner. This addresses the issue of delegating MaaS to far-away nodes, which was not addressed in earlier approaches.

To address the gaps of responsive device caching and contextual service offloading [13,33], the paper proposes small femtocells for resource delegation so that pending tasks may be offloaded to neighboring EN based on available allocations. Finally, to address the gaps between resource-intensive and energy-efficient consensus [34], we have proposed a novel consensus *LPoP* that cyclically forms group block validations, with non-conformant nodes marked as invalid. Thus, the proposed scheme *MB-MaaS* leverages an efficient and scalable solution to address issues of EU latency, responsive caching, and energy-efficient consensus formation for constrained IIoT ecosystems.

1.2. Research contributions

Following are the research contributions of this paper.

- A fair reward and incentive policy for miner nodes through multi-hop CO chain structure in BC-enabled 5G-MEC with proximity-based content caching strategy based on EN geolocation.
- An algorithm for 5G-femtocell based MaaS is proposed, reducing EU latency constraints and expediting resource requirements through ES to miner nodes.
- An energy-efficient consensus *LPoP* is proposed as a lightweight and scalable solution for resource-constrained IIoT ecosystems.
- The limitations of the proposed scheme regarding security issues, BC node characteristics, collusive bidding, and femtocell design are discussed, with future work directions.

1.3. Layout

The rest of the paper is organized as follows. Section 2 presents the existing state-of-the-art schemes. Section 3 discusses the system model and the problem formulation. Section 4 discusses the proposed scheme that addresses the research gaps in existing schemes to leverage an efficient mining and consensus solution for low-powered IIoT sensor integration. Section 5 discusses the performance evaluation. Section 6 discusses the limitations of the proposed scheme and also discusses the future scope of the work. Finally, Section 7 concludes the paper.

2. State-of-the-art

This section presents the concise findings of the existing state-of-the-art approaches in a similar domain. Table 2 shows the relative comparison of the existing state-of-the-art approaches. For example, Liu et al. [20] proposed a wireless MB framework with edge devices connected to EN, and requests are offloaded to facilitate mining tasks based on stochastic geometry. To address issues of load-balancing and EU latency, Bhattacharya et al. [2] proposed an incentive MaaS strategy in MB through 5G Femto-cellular services to support CO. Authors in [21] proposed CO and content caching strategies to handle increased traffic in wireless BC through MEC support. To exploit the same, the authors have considered two offloading scenarios, one to a nearby access point (mode 0) and the other to a group of device-to-device (D2D) users (mode 1), and the decision of cache strategies are formulated. However, the limitation of this paper is that AP can fail to serve all the requests of the network. In addition, the D2D approach can increase the overhead in the system. Xiong et al. [31] proposed edge computing services in MB and proposed fair incentive schemes for miners based on a two-stage Stackelberg game that maximizes peer-profits of ES and miner entities. Nevertheless, they proposed a scheme limited to a single entity ESP, which can increase the overhead on the ESP. Also, ESP might not have sufficient resources to serve all the miners. Authors in [15] proposed an auction-based social welfare maximization scheme for resource allocation in MB through entities ES, BC-owner, and MB users, with polynomial time complexity. As a limitation, this scheme also depends on a single entity ESP. Li et al. [18], proposed *POEM+* pricing scheme for resource allocation for multi-buyer and seller environments. In the scheme, auction allocation is divided into discrete slot units, and the scheme's performance is compared to single allocation schemes. However, the scheme has not deployed any consensus mechanism between miners. MEC is also responsible for serving the requests, which can cause overhead on the edge server and system might lead to latency and efficiency issues. Authors in [28] [4] proposed improved versions of [18] scheme through *rRAND, MATCH* and multi-round auction algorithm *LNESTLE*. Authors in [22] have proposed the smart contact-based double auction mechanism long-term auction for mobile blockchain (LAMB) to achieve the total utility of the auction participators. The smart contract provides automatic execution and guarantees long-term performance as well. Lastly, they have simulated the results and compared them with the already existing algorithm WBD. However, this scheme uses the Proof-of-Stake (PoS) mechanism, which can be inefficient to build on mobile devices. As well as, the traditional consensus mechanism consumes more energy while deployed on mobile devices. To address the malicious behavior of sensor nodes, Djenouri et al. [8] proposed a deep learning scheme in Internet-of-Everything (IoE) setups. The authors proposed deep neural networks and integrated evolutionary algorithms to detect the outlier behavior of sensor nodes. The scheme evaluated the time series capture of sensor readings via a recurrent neural network and fine-tuned its performance through a genetic and bee-swarm evolutionary method that improves the training time. Authors in [9] proposed distributed knowledge graphs in 5G setups to propose that assures privacy-preservation in distributed network sites. They applied knowledge mining graphs to resolve the context and find the associative mapping. Chen et al. [5] have considered the multihop communication in the Blockchain environment for two tasks, one is a normal task which is the data processing task, and the mining task, which performs the PoW in the blockchain environment. They have developed an algorithm that considers both approaches in blockchain empowered IoT elements. As well as, they considered the offloading game to prove the Nash equilibrium (NE) in the game. Then authors have proposed the distributed message exchange to achieve NE for low computational complexity. But, the scheme is limited to LTE technology which can increase the latency in the system, while the use of 5G can eliminate the latency issues in the proposed scheme. To address the limitations of the above-mentioned research, we have considered the multiple entities (E_{ES}, E_{ESP}, and E_{CS}) to serve the offloading requests. Also, we have proposed the MaaS scheme and lightweight energy-efficient consensus mechanism (LPoP) for mobile blockchain and IoT environments, considering 5G technology.

3. System model and problem formulation

This section discusses the system model and problem formulation.

3.1. System model

A BC-envisioned 5G-MEC scheme *MB-MaaS* is proposed to address CO, EU latency, and energy-efficient consensus for mining schemes in constrained IIoT ecosystems. Fig. 1 depicts the proposed flow. The proposed scheme considers that the EU requests resources from ES, and if the request is not resolved at ES, it can be forwarded to an edge-service provider (ESP) that proposes an auction mechanism with ES to grant resources. Meanwhile, ESP can offload requests from Cloud Servers (CS), which are near to ESP through virtualization models (VM), and price fixation is communicated to ESP through CS. Based on the bidding pool, ESP forms a price-based auction with ES to maximize profit. To formulate the same, the scheme considers the EU entity E_U that requests resources from ES. In the scheme, we consider a total of n EU in the ecosystem. Any n^{th} EU U_n generates data D_n through IoT sensor nodes which are captured and sent via IoT aggregator A based on encrypted key-value mapping pairs through a shared session key S_k. The encrypted, stored data is forwarded to miner nodes E_M in Java-Script Object Notation (JSON) format to facilitate a lightweight exchange and scalable solution. The miner nodes execute mining application A_M through a proposed energy-efficient consensus scheme. Based on mined transaction list L_{T_U}, the EU requests are forwarded to 5G-femtocell and micro-cells in the radio access network (RAN). The base stations in 5G-RAN allocate communication frequency with ES-based EU request loads. Now, entity E_{ES} checks the E_U request and processes a local resolution through pre-fetched resources, if possible. Otherwise, the request list Req_q is forwarded to entity E_{ESP} that forms a local-auction process with E_{ES} based on the bidding pool. The auction scheme selects a winner from E_{ES} and serves Req_q based on the maximum winning threshold $Win_{threshold}$. So, if the miner decides the bidding amount is greater than the threshold value, the request of the respective miner will be granted, and mining resources will be allocated to that miner. Final allocation is done through resource request to entity E_{CS} that allocates virtual resources through distributed heterogeneous physical servers.

3.2. Problem formulation

As depicted in Section 3.1, in the proposed scheme *MB-MaaS*, we consider the entity set E as $E = \{E_U, E_M, E_{ES}, E_{ESP}, E_{CS}\}$. E_U consists of n users $\{U_1, U_2, \ldots, U_n\}$. Every n^{th} user has Wallet W_{U_n} as follows.

$$W_{U_n} = \{ID_{U_n}, (PU_n, PR_n), C_{U_n}, T_{U_n}\} \tag{1}$$

where ID_{U_n} is identity of n^{th} E_U, (PU_n, PR_n) are the public-private key pairs, C_{U_n} is the available cryptocurrency in wallet W_{U_n}, and T_{U_n} is the timestamp of wallet creation. Every n^{th} user U_n generates data D_n captured through m sensor nodes $S_m = \{S_1, S_2, \ldots, S_m\}$ in IIoT ecosystem through a channel C. The captured data of n^{th} user U_n is mapped to sensor S_m through a mapping function $M_1 : U_n \to S_m$ based on identifiers of U_n and S_m respectively. The collected data $\{D_1, D_2, \ldots, D_n\}$ of all n users mapped with $\{S_1, S_2, \ldots, S_m\}$. The uploading latency are subject to the following constraints.

$$\begin{aligned} C1 &: m > n \\ C2 &: \zeta(C) > 0 \end{aligned} \tag{2}$$

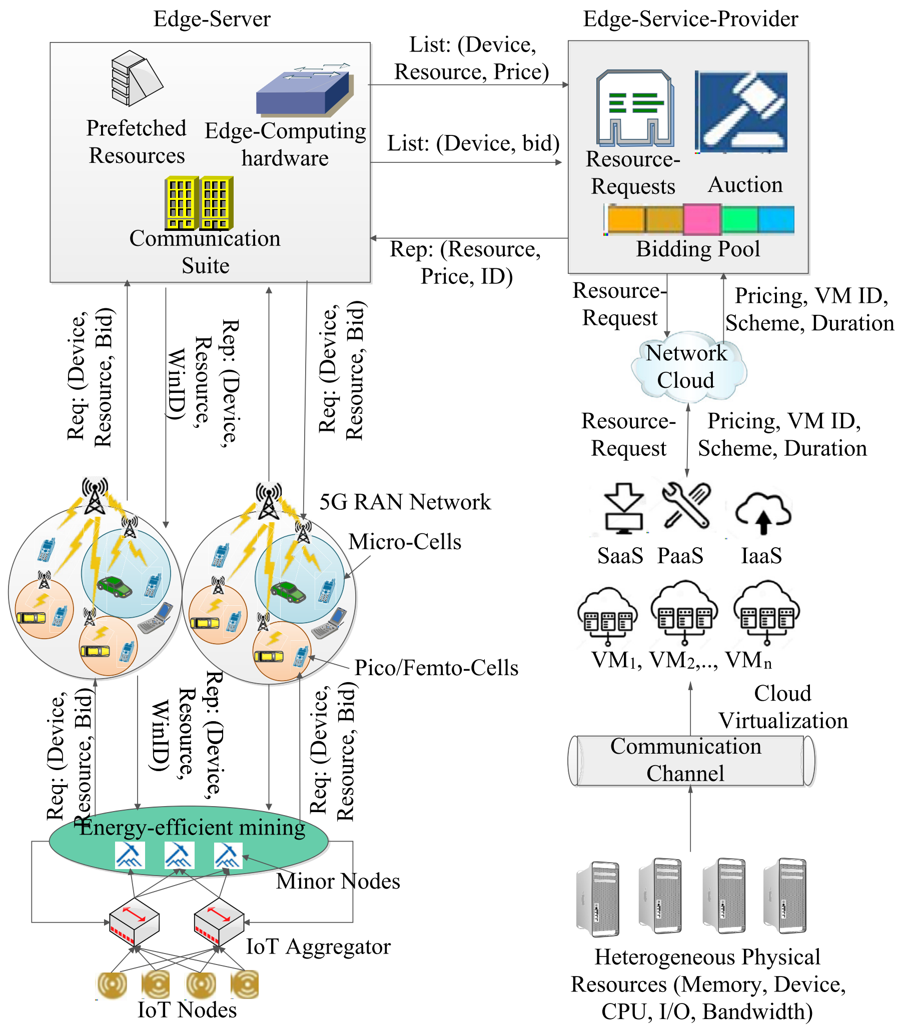


Fig. 1. *MB-MaaS*: The System model.

where $\zeta(C)$ denotes the channel bandwidth. The sent data S_m is collected through an IoT aggregator A that stores S_m based on key-value pair mapping $M_1 : A \rightarrow S_m$ and is defined as follows.

$$A = \{D_{S_1}, D_{S_2}, \ldots, D_{S_m}\} \tag{3}$$

where D_{S_m} is data generated by sensor node S_m. Here, a mapping of key-value pairs on A, between n^{th} E_U is done by,

$$A = \{(U_1, K_{D_1}), (U_2, K_{D_2}), \ldots, (U_n, K_{D_n})\} \tag{4}$$

where U_n is n^{th} user and K_{D_n} is the shared key for D_n. The stored data is now encrypted through shared key S_k as S_k=$\{S_{k_1}, S_{k_2}, \ldots, S_{k_m}\}$. For any m^{th} data D_{S_m} for sensor node S_m, a light weight key exchange S_{k_m} is facilitated as follows.

$$D_{S_m} = E(S_{k_m}, D_m) \tag{5}$$

As it is an IoT environment, the lightweight exchange is done. So, the data is shared through JSON format. The encrypted data is not sent to miner entity E_M $\{M_1, M_2, \ldots, M_q\}$, with $q < n$. E_M runs a light-weight mining application A_M=$\{A_{M_1}, A_{M_2}, \ldots, A_{M_q}\}$ at local nodes. The miner application for any q^{th} miner is denoted as follows.

$$A_{M_q} = \{R_{M_q}, P_{M_q}, S_{M_q}, L_{T_U}\} \tag{6}$$

where R_{M_q}, P_{M_q}, and S_{M_q} denotes the resource, power and storage requirements of q^{th} miner. L_{T_U} is the list of unverified transactions for entity E_U. $R_{M_q}, P_{M_q}, S_{M_q}$ are now subject to following constraints.

$$\begin{aligned} C3 &: R_{M_q} \geq R_{min} \\ C4 &: P_{M_q} \geq P_{min} \\ C5 &: S_{M_q} \geq S_{min} \end{aligned} \tag{7}$$

where R_{min}, P_{min}, and S_{min} denotes the minimum requirements threshold for the resources. So, the system can limit the miner's demand, and the system does not allocate all the resources to the specific miner that requests higher resources along with higher bid value. To access the mining application A_{M_q}, a wallet W_{M_q} is created with attributes as follows.

$$W_{M_q} = \{MID_q, C_P, Q_{led}\} \tag{8}$$

where MID_q is the identity of q^{th} miner, C_P is the agreed consensus protocol among E_M, and Q_{led} is a public ledger where the transactional meta-information of all transactions appended to blocks are stored. The mining procedure requires less computational power due to the proposed energy-efficient consensus mechanism. Thus, the mining application becomes responsive that facilitates transactional storage in blocks through memory constrained and mobile devices. The notation here is referred to as

MB. In MB, CO services to mobile devices are performed through a q^{th} mining server. The request is forwarded to the edge server as follows.

$$Req_q = \{WID_q, MID_q, A_q, B_q\} \tag{9}$$

where, WID_q denotes the wallet identity of any q^{th} miner, A_q is the requested allocation by q^{th} miner, B_q denotes the bidding price for the allocation by q^{th} miner and is subjects to the following constraints

$$C6 : C_{U_q} \geq B_q \tag{10}$$

3.2.1. 5G-RAN network configuration

Req_q is forwarded through heterogeneous 5G-RAN network. To understand the network configuration in a better manner, we model the details for a specific femtocell only. The formulation remains same for all femtocells, denoted as $\{C_1, C_2, \ldots, C_l\}$. A dense femtocell unit is presented, with *INACTIVE* state options that facilitates low-powered transfer and co-channel interference mitigation. We consider in any l^{th} femtocell unit, a sniffer S_l with energy consumption to be close to 0.4 μW consumption. S_l forms a low-powered exchange unit with A through m^{th} base station as follows.

$$P(BS_m) = P_m + P_{R_A} + P_{T_A} + P(A) - P(S_l) \tag{11}$$

where $P(BS_m)$ denotes the overall required power for l^{th} femtocell unit, P_m denotes the required power by micro base antennas (MBS), P_{R_A}, and P_{T_A} denotes respectively the power computation from of transmitting and receiving antennas, $P(A)$ denotes the required power for IoT aggregator, and P_{S_l} is the power wasted due to small dense cells, and co-channel interference. In such co-channel operations, the femtocell power can be adjusted through a defined coverage range ω as follows.

$$A(BS_m) = min(P_m + \lambda - L_m(d) + L(\omega), BS_{max}) \tag{12}$$

where $A(BS_m)$ denotes the adjusted power, λ denotes the antenna gain, $L_m(d)$ denotes the path cell loss at a distance d, $L(\omega)$ denotes the path loss at coverage radius ω, and BS_{max} denotes the maximum threshold of power adjustment. Based on channel adjustment, we consider an interfering base station B' for any n^{th} user U_n with station B. To minimize interference, we consider the sub-carrier channel Γ. The signal-to-noise interference ratio (SINR) for femtocells is denoted as follows.

$$SINR_{U_n,\Gamma} = \frac{P_{B,\gamma} G_{U_n,B,\Gamma}}{N_0 \delta_f + \sum_{B'} P_{B',\Gamma} G_{U_n,B',\Gamma}} \tag{13}$$

where $P_{B,\gamma}$ denotes the transmitting power of U_n at B, at sub-carrier Γ, $G_{U_n,B,\Gamma}$ denotes the channel gain for U_n in B at Γ. Similarly, for B', $P_{B',\Gamma}$ and $G_{U_n,B',\Gamma}$ are defined as transmitting power of U_n an channel gain at co-channel station B', N_0 denotes the spectral density, and δ_f denotes the sub-carrier spacing. Based on $SINR_{U_n,\Gamma}$, U_n capacity on the sub-carrier Γ is computed as follows.

$$C_{B,\gamma} = \delta_f .log(1 + \alpha SINR_{U_n,\Gamma}) \tag{14}$$

where $C_{B,\gamma}$ depicts the user capacity on Γ, and α is defined as channel exponent. Based on $C_{B,\gamma}$, Req_q are forwarded to E_{ES}. E_{ES} pre-fetches resources from E_{ESP}, to satisfy bulk requests from femtocell users U_n.

3.2.2. Allocation of requests by E_{ES}

An edge server E_{ES} allocates requests of U_n based on the device configuration as follows.

$$E_{ES} = \{E_{PFR}, E_{ECH}, E_{CPS}, E_{TM}\} \tag{15}$$

The entity E_{ES} includes 4 modules. Where E_{PFR} denotes the pre-fetched module that denotes resources that are already offloaded at E_{ES} to serve requests by ES only. E_{ECH} is edge computing hardware to address EU latency, E_{CPS} is a communication protocol suite that provides basic communication standards for a given scheme, and E_{TM} is a transaction module where bidding prices are set. For any n^{th} user request Req_q, that is processing on and forwarded through q^{th} miner, E_{ES} partitions Req_q into two sub-requests Req_{q1} and Req_{q2} as follows.

$$\begin{aligned} Req_{q1} &= \{MID_q, A_q\} \\ Req_{q2} &= \{WID_q, B_q\} \end{aligned} \tag{16}$$

Req_{q1} is allocated to E_{PFR} where request allocation A_q is handled and Req_{q2} is allocated to E_{TM} where auction strategy is proposed between E_{ES} and E_{ESP} based on decided winner among E_M based on B_q. E_{ES} post allocation sends an acknowledgment piggybacked to E_M as follows.

$$Rep_q = \{WID_q, MID_q, A_q, Win_{ID_q}\} \tag{17}$$

s.t.

$$C7 : A_q \leq A_{ES} \tag{18}$$

where A_{ES} denotes the total available allocation at E_{ECH}, and Win_{ID_q} is winner ID of the q^{th} miner. Thus, based on boolean indicator $Win_{ID_q} = \{0, 1\}$, it checks whether the allocation is granted or revoked for the q^{th} miner. So, Win_{ID_q} denotes that the resources are allocated to q^{th} miner if its value is 0 and revoked if its value is 1.

3.2.3. Allocation by an edge service provider E_{ESP}

In case E_{ES} does not have sufficient resources to cater to Req_q, the requests are forwarded to E_{ESP} to initiate the process of CO. To formulate the same, E_{ESP} have the following entities.

$$E_{ESP} = \{E_{resource\_manager}, E_{auction\_protocol\_module}, E_{resource\_pool}\} \tag{19}$$

The $E_{resource\_manager}$ is resource manager, $E_{auction\_protocol\_module}$ is auction protocol module and $E_{resource\_pool}$ is resource pool. Two lists L_1 and L_2 are prepared by the E_{ES} before forwarding requests to the E_{ESP} as follows,

$$\begin{aligned} L_1 &= ((MID_1, A_1), (MID_2, A_2), \ldots, (MID_z, A_z)) \\ L_2 &= ((WID_1, B_1), (WID_2, A_2), \ldots, (WID_z, B_z), W_{total}) \end{aligned} \tag{20}$$

where L_1 is appended with W_{total} to indicate the total number of winners decided by E_{ES}. The need for W_{total} is that to maintain the total number of winners in the system. The system predetermines the $W_{threshold}$. So, E_{ES} must have to forward the parameter W total, otherwise, E_{ESP} can declare more number of winners than the $W_{threshold}$. L_2 is forwarded to $E_{resource\_manager}$ and $E_{auction\_protocol\_module}$ s.t. following constraints.

$$C8 : W_{total} < W_{threshold} \tag{21}$$

where $W_{threshold}$ is the maximum threshold of winners allocated by L_1. For any z^{th} miner, allocation A_z is completed by

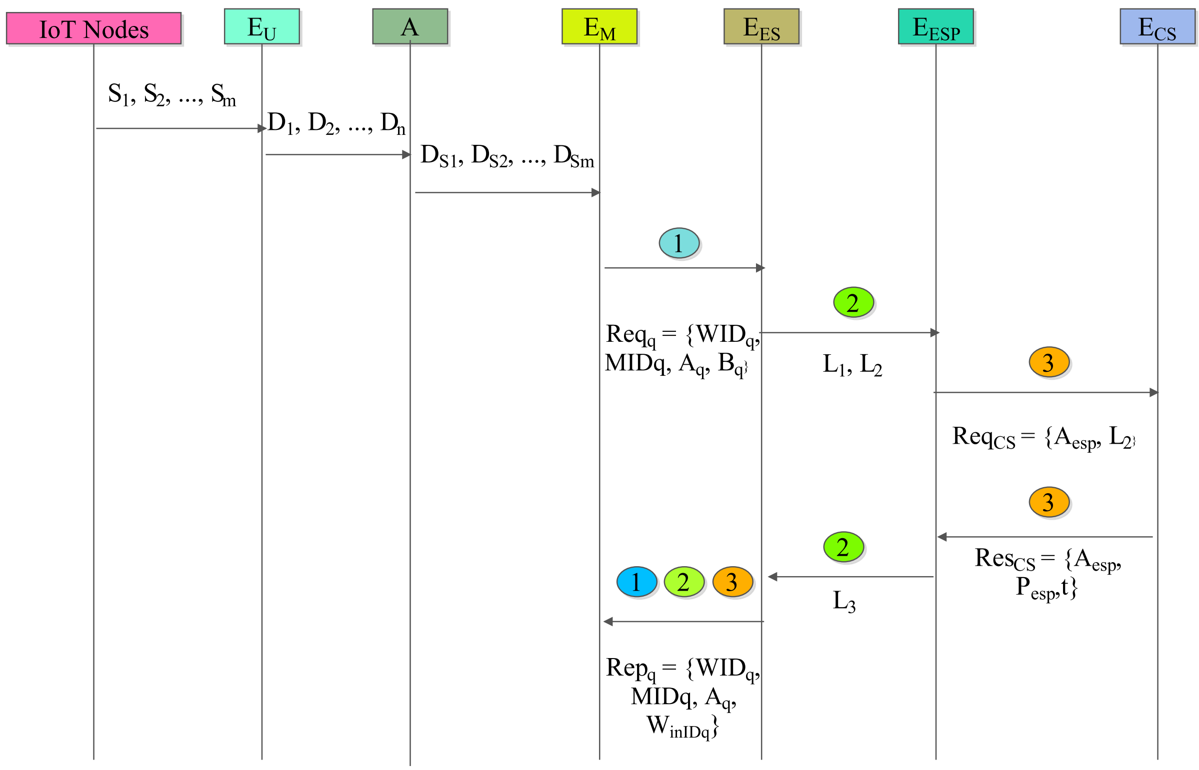


Fig. 2. The interaction handshake among different entities in the scheme.

$E_{resource\_manager}$ and $E_{auction\_protocol\_module}$ decides the winning status based on the bidding price B_z. E_{ESP} can place the request allocation s.t. the following constraints.

$$C9: A_z < A_{ESP} \tag{22}$$

where A_{ESP} is total allocation units available with E_{ESP}.

3.2.4. Requesting resources from the E_{CS}

In case A_z is greater than A_{ESP}, a request Req_{CS} is forwarded to E_{CS} to grant resources. For the same, E_{CS} places a price P_{esp} that includes pricing for resource access. Here, E_{ESP} itself will request the resources rather than forwarding resources to E_{CS}. So, E_{CS} will give the resources to ESP as per the requirement of E_{ESP}. Here, E_{ESP} can request any amount of resources irrespective of the demands of the miners.

$$Req_{CS} = \{A_{esp}\, \iota_2\} \tag{23}$$

where A_{esp} is a constant resource allocation required by E_{ESP} from E_{CS}, and ι_2 denotes the network timestamp. Based on the request allocations by E_{CS} a price is levied on E_{ESP}, which is denoted as follows.

$$Rep_{CS} = \{A_{esp}, P_{esp}, t\} \tag{24}$$

where P_{esp} is the per unit prices based on allocation units to E_{ESP} and t is the time duration for allocation of services, denoted as A_{esp}. The resource allocation A_{esp} is stored in $E_{resource\_pool}$ and subsequently allocation requests by E_{ES} are handled by E_{ESP}. The reply list L_3 to E_{ES} is depicted as follows.

$$L_3 = ((D_1, P_1, W_{ID_1}), (D_2, P_2, W_{ID_2}), \ldots (D_z, A_z, W_{ID_z}), W_{total}). \tag{25}$$

Based on L_3, E_{ESP} generates reply to E_{ES} based on each winner will be allocated with requested resources by them. Thus, based on above discussions, the problem formulation P_f of *MB-MaaS* scheme is defined as follows.

$$P_f : max_{Req_q}\{E_M, R_{M_q}, P_{M_q}, S_{M_q}\} \tag{26}$$

s.t.

$$\begin{aligned} &c_1 : L(\omega) < P_{B,\gamma} \\ &c_2 : WIN_q > W_{threshold} \\ &c_3 : Req_q < R_d \\ &c_4 : L_{T_U} > 0 \end{aligned} \tag{27}$$

Constraint c_1 dictates that path losses are less than transmitting power of U_n, that mitigates co-channel interference, c_2 specifies winner ID of q^{th} miner must be less than maximum threshold of winner allocations, c_3 specifies request time for resource allocation must be less than acceptable delay R_d, to minimize round-trip-times (RTT), and improve throughput. Finally, c_4 indicates simple constraint of non-empty unverified transactions in the channel.

Fig. 2 shows the handshake diagram of the given scheme. Total of seven entities are present in the system, IoT Nodes, E_U, A, E_M, E_{ES}, E_{ESP}, and E_{CS}. In the first step, m IoT nodes generate the data $\{S_1, S_2, \ldots, S_m\}$, that data is then sent to the E_U and E_U generates the data $\{D_1, D_2, \ldots, D_m\}$. Then A aggregates data as per the eq. (3). This aggregated data is sent to the E_M for further processing. The E_M will require the resources from the E_{ES}, so it requests the resources by sending Req_q as per eq. (9). If the available resources are not enough to serve all the requests, another two lists L_1 and L_2 are sent to the E_{ESP} as per the eq. (20). Moreover, if E_{ESP} is not capable to fulfill the requests, then E_{ESP} requests to E_{CS} to provide resources by sending Req_{CS}. Accordingly, Rep_{CS}, L_3 (as per eq. (25)), and Rep_q are generated. These replies are forwarded to the E_M and the demands of miners are served.

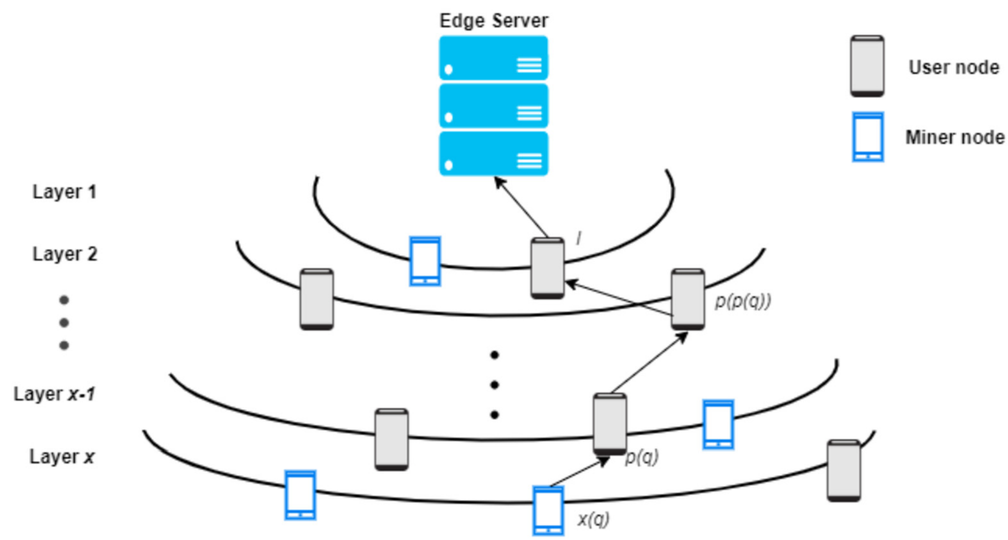


Fig. 3. Multihop CO.

4. *MB-MaaS*: the proposed scheme

As indicated in section 3.2, miner nodes collect resource requests from U_n as A_{M_q} and forward the same to E_{ES} through a 5G-femtocell network. E_{ES} allocates resources, if available, or CO the same to E_{ESP}. For the same, an auction pricing mechanism is present between E_{ES} and E_{ESP}. The details of the same are now presented as follows.

4.1. Multi-hop computational offloading chain for E_M

Here, a Layer architecture is proposed for passing the requests of miners to E_{ES}. A hop-to-hop forwarding is considered where miners act as source and E_{ES} is the destination. Also, the normal users in the environment will act as the carrier of the requests made by the corresponding miner. Here, E_M forms a CO path $\{1, p(q), p(p(q)), \ldots, l\}$ to reach E_{ES}. The CO scheme is based on the following assumptions.

1. *One user node U_n can help only one miner E_M.*
2. *$\forall U_n : U_n \neq E_M$ i.e. U_n cannot participate as miner node.*
3. *$\forall E_M : Req_q = \delta$ i.e. Req_q by E_M is fixed during connection state.*

The following is depicted in Fig. 3. In the proposed multi-hop CO scheme, we consider the edge server E_{ES} is located at *Layer 0* of the offloading chain [5]. Proximity of E_M nodes from E_{ES} might be different, where some miner nodes are nearer (single-hop) and some are far (multi-hop) from E_{ES}. We consider any q^{th} E_M not at *Layer 0*, and hence, direct CO is not possible. In such cases, we consider the q^{th} miner at *Layer x*, denoted as $x(q)$. $x(q)$ sends the CO request to immediate user node U_{x-1} at *Layer* $x-1$. In such case, we consider U_{x-1} as parent node of $x(q)$ with the CO request edge e, denoted as $p(q)$. In case of disconnection of $p(q)$, or timeouts, the node is marked as *UNAVILABLE*, and the request is forwarded to upper layer i.e. *Layer* $x-2$, or $p(p(q))$. The recursion is continued until E_M is serviced through E_{ES}. The recursion chain is depicted as follows.

$$P = \{p(q), p(p(q)), \ldots, l\} \tag{28}$$

where, P denotes the path to reach E_{ES} and l is the chain length.

4.2. Auction-based strategy for fair reward pricing of E_M

As stated above, any user node U_n can service only one miner node. Thus, the cost of relaying mining task of user n to its parent $p(n)$, denoted as $C^{rel}_{(n,p(n))}$ is depicted as follows.

$$C^{rel}_{(n,p(n))} = (s_q/v_{(n,p(n))}).w_n.p^e \tag{29}$$

where s_q denotes the mining task size of q^{th} miner, $v_{(n,p(n))}$ is the transmission rate of CO through U_n, and p^e is the price per-unit of energy to support CO by miner. Any user U_n can help a miner node E_M to offload tasks from E_{ES}, and in return, gets a certain share of reward depicted as follows.

$$C^{rel}_n = C^{rel}_{(n,p(n))} - p_n \tag{30}$$

where, p_n is forwarding reward of user node n.

A fair incentive policy is presented that addresses the latency issues in CO over multiple devices, as nodes nearby of E_{ES} get serviced first. Nodes at *Layer 1* are serviced first than *Layer x*, and hence miners at *Layer 1* gets access to resources first. These nodes can start the mining task earlier than miner nodes at *Layer x*. To address the same, we consider a fair incentive policy for all miner nodes stationed at different layers by setting different bidding amounts $\{B_1, B_2, \ldots, B_x\}$ layer-wise. We set a bid threshold of B_{min} to indicate the minimum service bid for all miners. Now, miner nodes that are stationed near E_{ES} have higher prices than miners at lower layers. Thus, at *Layer x*, the bid threshold B_x depends on computed distance d_x from E_{ES} and is depicted as follows.

$$B_x \propto 1/d_x \tag{31}$$

As the distance d_x increases w.r.t. E_{ES} the bidding threshold value B_x decreases. Similar to the bid threshold, at each layer, we consider the winning threshold of the bidding process, depicted as W^x_{min} for any x^{th} layer. As miners close to E_{ES} pay a higher price due to less EU latency of CO, this policy also attracts $x(q)$ to participate in the mining process. As d_x increases, more computational resources are required by q^{th} miner, and hence more rewards are applicable. The details of the proposed scheme are presented in Algorithm 1. For the *ALLOCATION* sub-procedure, bids B are sorted based on $Win^k_{threshold}$. The same is depicted in Lines 1-30. Lines 31-43 depicts the request allocation from E_{ESP} based on auction

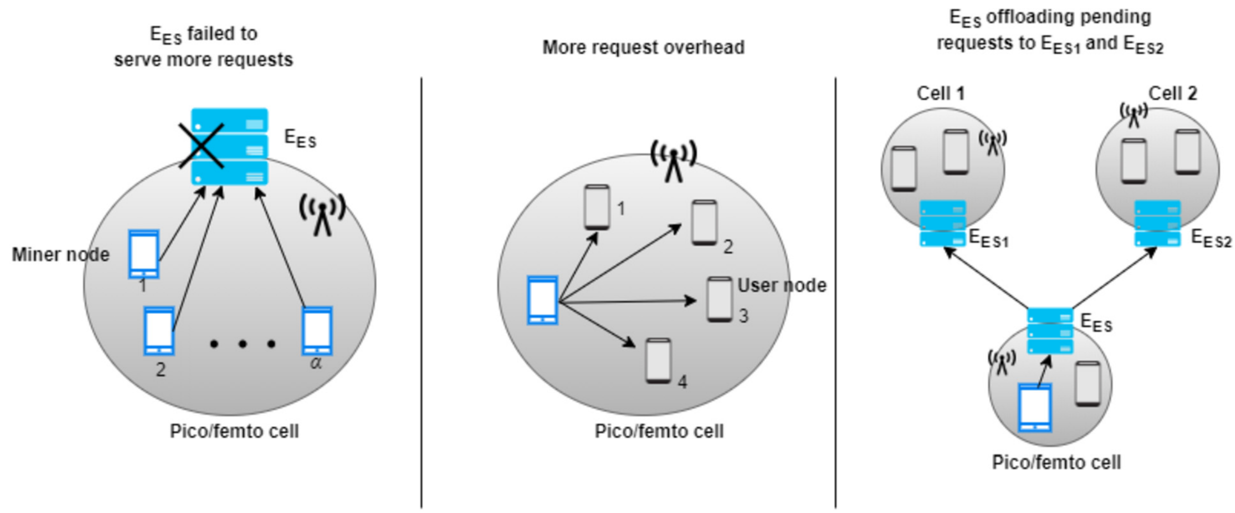


Fig. 4. Offered scenarios of CO in *MaaS*.

Algorithm 1 Auction-based strategy for fair reward pricing of miners.

Input: Number of layer x, Threshold amount of every layer $B_{min}^{1\_to\_x}$, threshold value of winners at each layer $Win_{threshold}^{1\_to\_k}$, Number of miners q for x layers, Wallet W_U of each miner.
Output: Win_{ID} of each miner.

procedure ALLOCATION_E_{ES}(x)
  for $k \leftarrow 1$ to x **do**
    for $i \leftarrow 1$ to q **do**
      Sort bids B in descending order;
    end for
  end for
  for $k \leftarrow 1$ to x **do**
    $Win_{total}^{k} \leftarrow 0$;
    for $i \leftarrow 1$ to q **do**
      if ($Win_{total}^{k} \leq Win_{threshold}^{k}$) **then**
        if ($B_i \leq C_{U_i}$) **then**
          if ($B_i \geq B_{min}^{k}$) **then**
            if ($A_i \leq A_{ES}$) **then**
              $Win_{ID_i} \leftarrow 0$; $A_{ES} \leftarrow A_{ES} - A_i$;
              $C_{U_i} \leftarrow C_{U_i} - B_i$; $Win_{total}^{k} \leftarrow Win_{total}^{k} + 1$;
            else
              $z = q - (i - 1)$;
              Call procedure ALLOCATION_ E_{ESP}(z,Win_{total}^{k});
            end if
          else
            $Win_{ID_i} \leftarrow 0$;
          end if
        else
          invalid bidding;
        end if
      end if
      return Win_{ID_i}.
    end for
  end for
end procedure
procedure ALLOCATION_ E_{ESP}(z,Win_{total}^{k})
  for $j \leftarrow 1$ to z **do**
    if ($Win_{total}^{k} \leq Win_{threshold}^{k}$) **then**
      if ($A_j \leq A_{ESP}$) **then**
        $Win_{ID_i} \leftarrow 0$; $A_{ESP} \leftarrow A_{ESP} - A_j$;
        $C_{U_j} \leftarrow C_{U_j} - B_j$; $Win_{total}^{k} \leftarrow Win_{total}^{k} + 1$;
      else
        $j \leftarrow j - 1$;
        Call procedure REQUEST_$E_{CS}(A_{esp})$;
      end if
    end if
  end for
end procedure
procedure REQUEST_$E_{CS}(A_{esp})$
  $A_{CS} \leftarrow A_{CS} - A_{esp}$;
  return A_{esp}.
end procedure

A_j. Finally, sub-procedure *REQUEST* allocates the request to miner nodes that are offloaded from E_{ESP}. The time-complexity of Algorithm 1 is $O(x.qlogq)$ due to comparative bid sort, and space complexity is $O(xq + z)$. Constraint c_1 is satisfied path loss $L(\omega)$ is minimized due to local edge service in cell C from E_{ES}. Constraint c_2 is satisfied as winner ID of q^{th} miner is less than the bidding threshold.

4.3. Mining-as-a-Service (MaaS) for mobile blockchain in IoT elements

To support multi-hop CO from E_{ESP}, we consider 5G-femtocells, with E_{ES} deployed in each cell C that acts as nearest edge-resource, that facilitates the expensive mining operations [13]. To support the same, we consider block mining applications offload tasks from nearby devices. Consider an offloaded task $\mathbb{T}$ from nearby device set D_n. D_n consists of set of nearby nodes, depicted as $\{N_1, N_2, \ldots, N_l\}$ to support parallel mining operations. To exploit the same, $\mathbb{T}$ is divided into smaller tasks $\{T_1, T_2 \ldots, T_l\}$, which are then mapped to D_n. A mapping function $M_D^T : T_l \leftarrow N_l$ is formed. However, with more devices, parallel requests needs to be addressed, that increases the EU latency.

Thus, to address overhead issues, one E_{ES} is issued in each cell C and device D_n can offload $\mathbb{T}$ by sending a request to E_{ES}. Fig. 4 presents the different CO scenarios. In the first scenario, a single E_{ES} is placed in cell C to address miner node requests. This approach has overhead and scalability drawbacks. As the number of users increases, then the capacity of E_{ES}, the E_{ES} can fail to serve all the requests. In the second scenario, a nearby edge device D_n is selected instead of E_{ES} to address mining requests. This solves the issues of E_{ES} overhead, but as D_n is resource-constrained, not all requests can be serviced. As well as, if the number of requests increases in the cell, more requests overhead get generated. In third scenario, sub-edge-servers E_{ES1} and E_{ES2} are placed in cell $C1$ and $C2$ respectively. So, if E_{ES} fails to serve all the requests of its cell, it can offload those requests to nearby ES E_{ES1} and E_{ES2}. So, in case of dense users, sub edge-servers are serviced through main E_{ES}. Based on framed scenarios of CO for E_M, we now present the *MaaS* scheme. The details are presented in Fig. 5. We consider S micro-cell units within a cell structure. Each cell is serviced through deployed E_{ES}. We consider α miners present in S micro-cells, with $A_M = \{M_1, M_2, \ldots, M_\alpha\}$. To offload tasks, every E_{ES} present in S has resource allocation from E_{ES}. The allocation

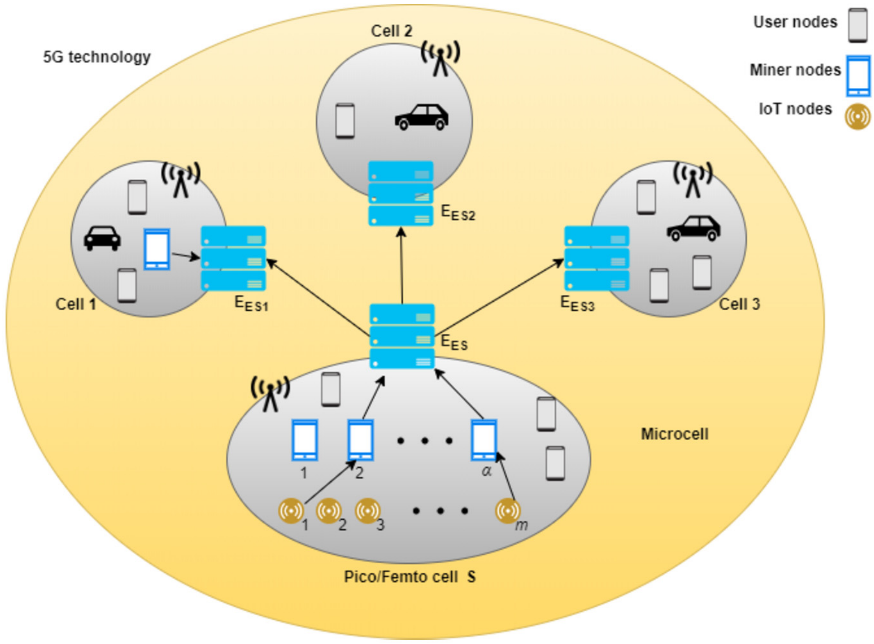


Fig. 5. Mining-as-a-Service (MaaS) for mobile blockchain in IoT elements.

Algorithm 2 Mining-as-a-Service (MaaS) for mobile blockchain in IoT elements.

Input: Number of small cells S, IoT nodes m, User nodes n, Miner nodes α.
Output: Resulting hash of miner node E_M.

1: **procedure** MAAS(S, m, n, α)
2: **for** $i \leftarrow 1$ to m **do**
3: **for** $j \leftarrow 1$ to n **do**
4: **if** $(i \in U_j)$ **then**
5: $D_{s_i} \leftarrow E(S_{k_i}, D_i)$;
6: Send D_{s_i} to IoT aggregator A;
7: $D_j \leftarrow D_j + D_{s_i}$;
8: **else**
9: Data does not belong to any user;
10: **end if**
11: **end for**
12: **end for**
13: **for** $(j \leftarrow 1$ to $n)$ **do**
14: Send D_j to U_j.
15: **for** $(k \leftarrow 1$ to $\alpha)$ **do**
16: **if** $k == j$ **then**
17: Send D_j to Mining application A_{M_k};
18: **else**
19: User is not participated as miner;
20: **end if**
21: **end for**
22: **end for**
23: **for** $(\gamma \leftarrow 1$ to $\alpha)$ **do**
24: sum= sum + R_{M_γ}
25: **end for**
26: **if** $(sum > A_{ES})$ **then**
27: $result = sum - A_{ES}$;
28: **for** $(k \leftarrow 1$ to $S)$ **do**
29: request k^{th} Edge server to know the allocation left;
30: **end for**
31: According to left allocation divide the *result* into small tasks s;
32: **for** $(k \leftarrow 1$ to $S)$ **do**
33: Allocate s_k;
34: **end for**
35: **else**
36: **for** $(\gamma \leftarrow 1$ to $\alpha)$ **do**
37: **if** $(R_{M_\gamma} < R_{min})$ **then**
38: Request E_{ES} for A_{ES_γ} ;
39: $R_{M_\gamma} \leftarrow R_{M_\gamma} + A_{ES_\gamma}$;
40: Perform *LPoP* with R_{M_γ};
41: Return hash $H(B)$.
42: **end if**
43: **end for**
44: **end if**
45: **end procedure**

is denoted as A_{ES}. Thus, the total requested allocation can exceed the available allocation, depicted as follows.

$$\sum_{\gamma=1}^{\alpha} A_\gamma > A_{ES} \tag{32}$$

In such cases, E_{ES} offloads the pending tasks to neighboring micro-cells. For the same, E_{ES} sends a request R to other micro-cells for available allocation post allocation to miners in that current cell. The remaining allocation units from A_{ES} are equally divided into remaining micro-cells to balance loads and requests. The details of the proposed algorithm are now presented in Algorithm 2. In the algorithm, lines 1-12 presents the condition where D_{s_i} forwards sensor data to A to perform mining operations by application A_k. The mining process is depicted in lines 13-22. In case resources are not available at A_k, *MaaS* is invoked by sending a request to k^{th} E_{ES}. The same is depicted in lines 23-45. The mining application facilitates m sensor nodes for n users. Thus, time complexity of Algorithm 2 is $O(nm)$. As the allocation requests are placed as a queue, the space complexity is $(\alpha.D_j)$. Constraint c_3 is satisfied as mining application A_{M_k} allocates cumulative A_{ES} through small task sets s that minimizes latency R_d at q^{th} miner node.

4.4. Lightweight Proof-of-Proximity: a light-weight and scalable solution for constrained IoT nodes

In this section, we present the details of the Lightweight Proof-of-Proximity (LPoP) scheme, which is based on the basic delegated PoP consensus protocol [16]. In PoP consensus, a neighbor discovery mechanism is executed during data transmission. The node selection is based on a standard voting-based consensus scheme, in which a voting node is selected based on the node distance from the transaction event. However, this does not assure fairness too far away nodes, as there is a low probability of such nodes being elected. Thus, we modify the PoP consensus with a fair incentive policy for the far-away nodes, which is not addressed in previous approaches. The modified consensus is renamed lightweight PoP (LPoP).

Algorithm 3 *LPoP*: Energy-efficient mining in *MB-MaaS*.

Input: Sequence of input transactions $\{T_1, T_2, \ldots, T_n\}$
Output: Count C of valid v and invalid iv transactions.
Initialization: v=0, iv=0.

```
procedure VERIFY_TX(T)
    for (i ← 1 to PN-1) do
        if (U_n==NN) then
            if (iv ≥ v) then
                R ← Request_Server(G, PN, B);
                verify T in ledger;
                if (T == v) then
                    v ← v+1;
                else
                    iv ← iv+1;
                end if
            else
                v ← v+1;
            end if
        else
            i ← Verify_Ledger(T)
            if (T == v) then;
                v ← v+1;
            else
                iv ← iv+1;
            end if
        end if
    end for
    return v, iv.
end procedure
```

LPoP assumes that miner nodes are allocated A_{ES} from nearest E_{ES} in the micro-cell unit. We assume a multi-hop offloading scheme, where the nodes at the first layer are serviced before the next layer, and subsequently, the general layer x. However, since Layer 1 nodes are stationed near E_{ES}, they would get the resource first and thus are applicable to start the mining process. This process is similar to PoP, where the voted node is closer to the edge node. However, to address the fair incentive policy, we present an auction-based mechanism, that introduces a bid threshold value B_x for any Layer x.

The details of the consensus scheme are presented in Fig. 6. We assume each sensor device S_m is associated with a user node U_n in cell C. The block validation process V_b is carried out by U_n, instead of S_m, as IoT devices are constrained by power and storage requirements. The data is delivered to U_n through IoT aggregator A, which converts and serializes the data in concise binary object representation (CBOR), or JSON format, increasing transaction throughput with less computational and storage overheads. To address huge influx of data at U_n, *LPoP* forms group validations.

To exploit the same, we consider a group $\mathbb{G}$ of user nodes U_n, with a chosen proposer node (PN) in the proximity of $\mathbb{G}$. PN connects to S_m to gather data D_{S_m} from the m^{th} sensor node. Nodes in a common group $\mathbb{G}$ form a cycle with a start as PN. Along with PN, two other nodes are present- normal user nodes (NN) and ledger copy node (LN). NN serves required resource allocations to miner nodes, and LN keeps track of validated transactions in a cycle.

However, the LPoP scheme still requires a MaaS scheme, similar to PoW, as the data sharing has become lightweight, but the agreement process requires the voting round. The scheme focuses on making the data transmission lightweight, but the consensus's general agreement and voting process still require resources from ES. A MaaS scheme resolves the limitations of heavy computational requirements of miners during the auction and the voting process. Once the auction is complete, the data should be transmitted to the other nodes at low latency. Thus, the security of the consensus remains intact, and data exchange becomes responsive as the propagation is in the form of CBOR or JSON, which reduces the transmission overheads of the system. Also, when every node maintains a copy of the ledger, storage constraints can arise in MB. So, this scheme is lightweight in the form of storage because the ledger's replica is not maintained by every node in

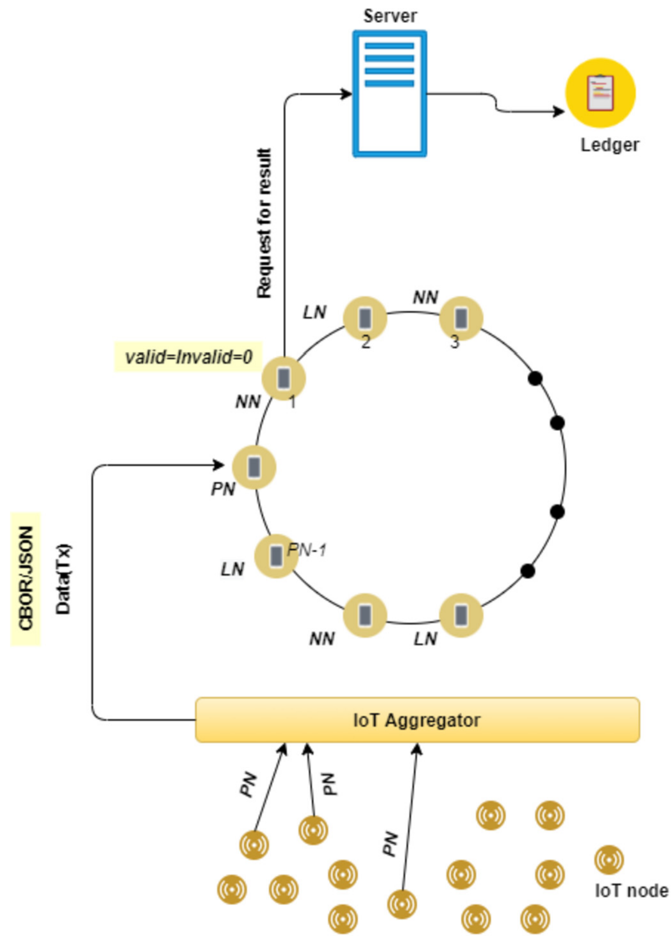
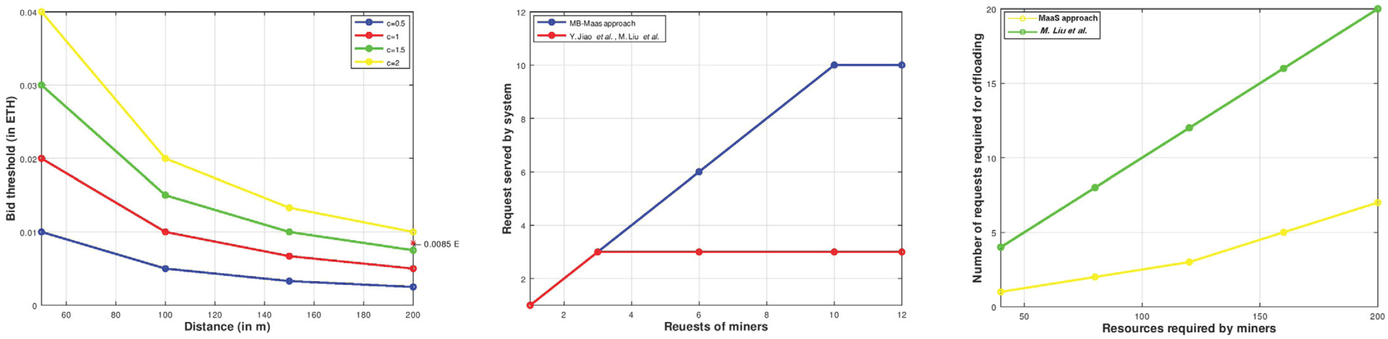


Fig. 6. *LPoP*: Lightweight Proof-of-Proximity for energy-efficient mining in *MB-MaaS*.

the system but by some specific nodes. This replica is kept by only ledger nodes LN and edge server ES. Even nodes are placed as LN except the starting PN node, and an odd number of nodes will be NN. The server of the cell also maintains a copy of the ledger. PN propagates appended transactions $\{T_1, T_2, \ldots, T_m\}$ in group $\mathbb{G}$, with counts as *valid* or *invalid*, based on consensus state in group $\mathbb{G}$. For each node, the count values are incremented, with final consensus based on majority of count results. The result is then propagated to LN to propagate block formations in B. Algorithm 3 presents the details of the proposed scheme. As we consider m sensor nodes associated with n^{th} user, the time-complexity of Algorithm 3 is $\mathbf{O}(m.PN)$. To present the group cycle, a circular queue $\mathbb{Q}$ is considered, and hence, space complexity is $\mathbf{O}(PN)$. Constraint c_4 is satisfied as transactions are validated in block groups $\mathbb{G}$, and count of v and iv are updated in real-time. Hence, no unverified transactions L_{T_U} are present in channel state CS.

5. Performance evaluation of *MB-MaaS*

In this section, we evaluate the performance of *MB-MaaS* auction and CO against traditional schemes based on request-serving time [15], [20], and D2D approach [21]. Based on offloaded requests from E_{ES}, network parameters- latency [2], D2D-caching time [21], [18], and energy-dissipation in consensus formation [29], in which we compare our proposed *LPoP* against other lightweight consensus scheme like Proof-of-Elapsed Time, and Lightweight Proof-of-Stake, based on selected parameters.



(a) Bid price based on distance. (b) Request Serving Time (c) Offloaded Requests to E_M.

Fig. 7. *MB-MaaS*: Bid-Thresholds and CO of Requests against traditional approaches.

Table 3
Simulation parameters.

Parameters	Value
Area of cell	300 m x 300 m
Number of miner nodes	12
Number of user nodes	40
Distribution of miner nodes	uniform, 3 at each layer
Distribution of user nodes	uniform, 10 at each layer
Number of layers in cell	4
Distance between two layers	50 m
Distance between layer 0 (E_{ES}) and layer 1	50 m
Fixed resource demand of each miner	40
Available allocation A_{ES} at E_{ES}	120
Available allocation A_{ESP} at E_{ESP}	120
Allocation A_{CS} cloud E_{CS} can provide	160
Minimum price E_{ES} charge to serve request	0.0085 ETH

5.1. Experimental setup

In *MB-MaaS*, we recorded different temperature, motion, and touch sensor readings through Raspberry PI 3 through wireless connectivity. The recorded readings are serialized in JSON format over cell area 300 m x 300 m for node distributions. 52 nodes are distributed in the network, where 40 nodes are normal mobile nodes and 12 are miner nodes. Miner nodes are installed with MB client application and connected to E_{ES} deploying ethereum blockchain platform [32]. To plot the simulation results, we use *Octave v4.4.1* and *Matlab v9.3*. The details of the simulation parameters are presented in Table 3. Here, the area of our experiment is 300 m x 300 m. Therefore, the selection of simulation values are made based on the constrained area. Moreover, most of the values are kept static to reduce the complexity of the result. For example, the resource capacity of E_{ES}, E_{ESP} and E_{CS} is decided to bypass the fractional resource blocks. However, the given algorithms can also handle the fractional capacity. The same reason applies to the number of miner nodes at each layer. As the user nodes are used to make the paths, the value of the user nodes can be changed per layer, considering assumptions that are mentioned in sub-section 4.1. Here, the minimum required users must be 9 in layer 1 (based on assumption 1). To avoid the case of a node failure, we kept it 10. The value of the threshold price is decided as 0.0085 ETH by considering the current value of Ethers. This value can be dynamic and can be decided by the ESP.

5.2. Simulation results

This subsection presents the simulation results based on considered simulation parameters. In addition, we consider auction-based results for bid thresholds to justify the fair incentive allocation and the effectiveness of *MaaS* and the *LPoP* consensus scheme. The details are presented as follows.

5.2.1. Auction-based strategy and CO requests to E_M

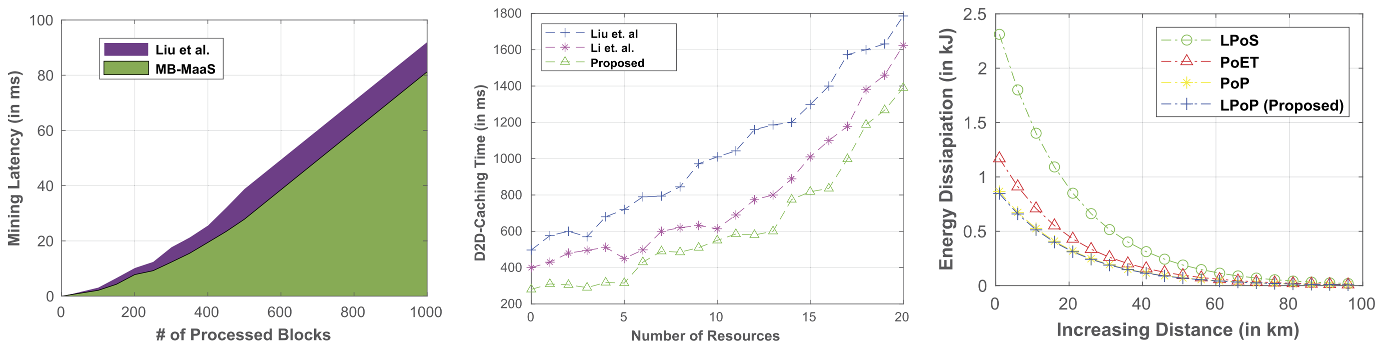
To simulate the same, we consider E_{ESP} runs the local ethereum blockchain to serve pending requests. We assume a permissioned BC approach, where the nodes are authenticated to participate in the auction process. E_{ESP} is also connected to cloud servers to request resources and maintain a resource pool. Fig. 7 depicts the results. For fair bid threshold, we consider a 4-hop layered network, with a minimum threshold at each layer as $B_{min}^{1\_to\_4}$. Fig. 7a depicts the same. For x^{th} layer, we consider $B_{min}^{x} = c.(1/d_x)$, where c is constant value. We plot for different values of c, with a minimum incentive charged at 0.0085 ETH for E_M. The fair bid threshold can be calculated at $c = 2$. As evident as the distance of E_{ES} from x increases, the price decreases to allow a fair incentive policy for q^{th} far-away miner.

Next, we formulate the number of requests served by miner E_M node, denoted as Request serving ratio (RSR). The following is depicted in Fig. 7b. As per the simulation parameters, the resource demand for each miner is 40. In other systems, these demands can be served by edge servers only. So, according to the capacity of E_{ES}, which is 120, it can serve only 3 requests $(40 * 3)$. So, the graph becomes steady after 3 requests. Whereas, in the MB-Maas scheme, 3 requests will be served by E_{ES}. In addition, the capacity of E_{ESP} is also 120, making the total served requests equal to 6. Moreover, the capacity of E_{CS} is 140, which can serve 4 more requests, resulting in a total of 10 requests served by the system. So, as a result, traditional systems can serve only 3 requests, while MB-Maas serves a total of 10 requests. As evident, from a total of 12 requests, 10 requests will be served in *MB-MaaS* due to multi-hop CO. The computed RSR is 0.83, as compared to traditional schemes [20], [15], with RSR of 0.25. This is because requests are pre-fetched and stored at E_{ES}, which minimizes the service response time.

Fig. 7c shows the number of parallel requests required to support CO. as evident, at 200 resources, the number of generated requests is 5.43, compared to 20.12 in the proposed scheme.

5.2.2. Efficiency of MaaS and energy-efficient consensus mechanism LPoP

We consider an edge device D_n with α miners present in 5G-microcell units. To simulate the same, we assume each E_{ES} are serving requests from two different cells E_M of own cell. The following is depicted in Fig. 8. For Fig. 8a, the mining latency is measured against processed blocks by E_M. At $n = 812$ blocks, the latency is close to 61.2 milliseconds (ms) in *MB-MaaS*, compared to 77.4 ms in traditional scheme (Liu et al. [21]), which shows a significant improvement of 26.47% in the proposed work. This is

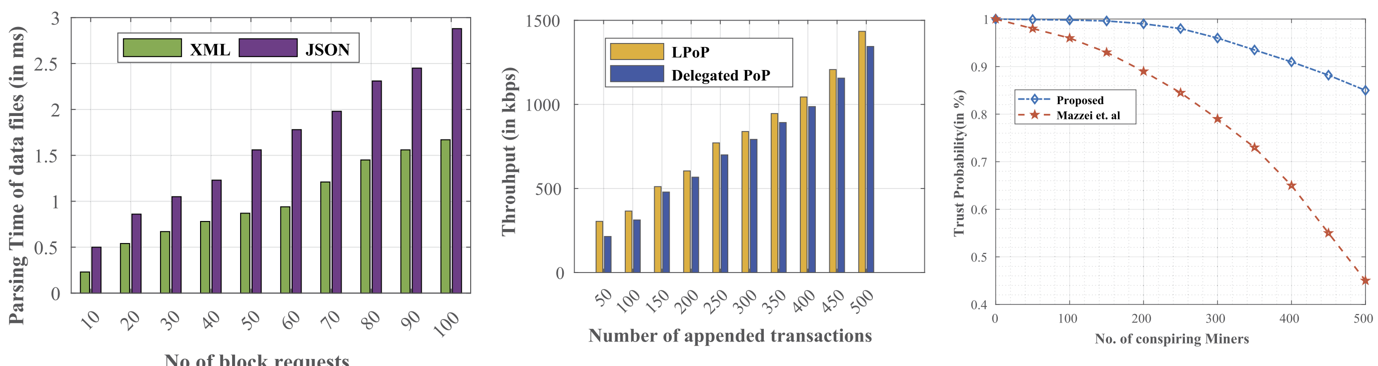


(a) Mining latency of processed blocks in *MaaS*.

(b) Effect on D2D-caching time with increasing E_M requests.

(c) Energy dissipation of *LPoP* against traditional IoT-based schemes.

Fig. 8. *MB-MaaS*: Efficiency of *MaaS* and low-powered consensus *LPoP* against traditional schemes.



(a) Parsing time analysis of JSON vs XML.

(b) Analysis of throughput of LPoP vs delagted PoP scheme.

(c) Trust Probability analysis against Public BC scheme

Fig. 9. *MB-MaaS*: Analysis of *LPoP* consensus in terms of lightweight transactional exchange.

due to the fact that E_{ES} service a smaller cell area, and divides $\mathbb{T}$ into sub-tasks, hence mining latency is improved.

Fig. 8b now presents the D2D-caching time at E_{ES}, while requesting resources from E_{ESP}. We assume that to demand of 1 miner node requires caching from 4 user nodes and 2 requests from server. At 15 requests, the D2D caching time is 784.34 ms, compared to 1195.14 ms in Liu et al. [21], and 912.32 ms in Li et al. [18], This is due to the fact that in each cell, a sub edge-node E_{ES1} is present in each cell C, that fetches data from main E_{ES} in close vicinity of itself.

In the proposed *LPoP* scheme, the data exchange is through concise representation protocols like CBOR or JSON, and user nodes are differentiated as normal and ledger nodes, where normal nodes provide the required resource allocation to ledger nodes. In such cases, mining power is not externally derived from other nodes. The dissipation is governed by the following equation $D_c = \gamma \times e^{-pt}$, where D_c is the dissipation constant, and γ is the external power requirement, and p denotes the mining power consumption, and t denotes the time window. Based on D_c, $E_d = D_c \times e^{-\alpha t}$ is the dissipated energy in time t. Thus, the value of γ decreases and D_C values are lower. Experimentally, the value of D_c is computed to be 3.95 for PoS, 2.43 for LPoS, and 0.91 for standard Proof-of-Proximity (PoP) consensus. The modified Lightweight PoP D_c value of 0.89, and thus the energy requirements are significantly lower. Moreover, PN groups validation requests V_b and aggregates the sensor data, verified by LN, with a simple count scheme.

Fig. 8c depicts the energy dissipation of proposed *LPoP*. As evident, at 20 hops, the dissipated energy is close to 0.37 kJ compared to other consensus schemes. We considered a mining window of the fixed time interval of 360 seconds and computed the required power to simulate the same. Now the energy dissipation is measured as the product of power and time.

5.3. Analysis of LPoP consensus in terms of lightweight transactional exchange

In this subsection, we formulate the efficacy of *LPoP* scheme for lightweight transfer of data. We evaluate the performance in terms of the parsing time of data. We compare the data transfer, the node throughput, and the scheme's performance in the event of collusive bidders, where the overall trust of the consensus is validated. The details are presented as follows.

Fig. 9a depicts the improvement in parsing time in data exchange through JSON format. We compare our data exchange against XML format, which takes a high parsing time. FOr 50 block requests, our scheme has a parsing time of 0.87 ms, compared to 1.56 ms. Please note that we have considered the scenario where normal nodes provide the resource allocation to miner nodes to derive the parsing time. On average, an improvement of $\approx$ 31.45% is achieved. The reason is that JSON serially processes the data and can be manipulated with the eval() method. In the case of compressed and serialized JSON through CBOR, the parsing time is further reduced by 7.89%. Thus, in our scheme, we make the data transfer lightweight, which also improves the energy efficiency of the *LPoP* consensus, as depicted in Fig. 8c. Moreover, XML is prone to attacks when the document definitions are validated, and JSON transfer is highly secure. In such case, cross-site request forgery (CSRF) attacks are mitigated.

Table 4
Experimental results of LPoP.

Node	Condition	Result from server	Result by node
NN(1)(faulty)	valid=invalid	valid	valid=0, invalid=1
LN(2)	NA	NA	valid=1, invalid=1
NN(3)	valid<invalid	valid	valid=2, invalid=1
LN(4)(faulty)	NA	NA	valid=2, invalid=2
NN(5)	valid=invalid	valid	valid=3, invalid=2
LN(6)	NA	NA	valid=4, invalid=2
NN(7)	valid>invalid	NA	valid=5, invalid=2
LN(8)	NA	NA	valid=6, invalid=2
NN(9)(faulty)	valid>invalid	NA	valid=6, invalid=3

Fig. 9b presents the throughput analysis of the appended transactions. In the delegated PoP scheme [16], the consensus voting selection is based on the distance of the mining node from the resource event, and thus for far-away nodes, the transactional incentives are lower. Due to the fair incentive policy of *LPoP*, we assume that miner nodes are allocated A_{ES} from the nearest E_{ES} in the micro-cell unit. An auction mechanism breaks the serial voting process of the node, which is close to E_{ES}, and thus all the miner nodes are motivated to participate in the consensus formation. In this way, the consensus also breaks the monopoly of certain nodes to participate in the election, which could lead to a collusion attack. As evident, at 300 transactions, the scheme has a high throughput of 1338.857373 kbps against 383.9344646 kbps, as only selective nodes participate in the mining process.

Fig. 9c presents the trust probability as depicted in Mazzei et al. [24]. We assume the *LPoP* setup in a permissioned BC, where the nodes are authorized to view the transactional data. We compare the trust probability, which is presented as follows.

$$T_p = V_t/T_t \tag{33}$$

where T_p denotes the trust probability, V_t denotes the valid transaction proposed by node *x*, and T_t denotes the overall number of transactions proposed by *x*. In case the proposed transaction is invalid, T_p decreases, and thus nodes with more valid transaction proposals are more trusted. In such cases, the miners who are compromised would have a lower T_p value. Specifically, we have set a low threshold of $T_p = 0.3$ to increase compromised miners in the system randomly. In a public chain, there are high chances of collusion as more than 50% of miners in the network generate more hash power from the same community, which reduces the trust and invalidates the newly added block. It allows malicious entities to grow the side-way chain. The network will accept the longest growing chain, so a private chain that uses the *LPoP* consensus mechanism will refrain our network from intruders.

Table 4 presents the result received from E_{ES} for random use nodes U_r. To formulate the same, a total of 10 nodes are selected, with a node elected as PN. In $\mathbb{G}$, we elect 5 NN nodes and 4 LN nodes. Each NN node sends a request to E_{ES} that also maintains a copy of the public ledger. Through *LPoP*, the consensus is achieved based on the majority principle by considering 2 NN and 1 LN faulty, as evident from the table. As nodes are added as faulty and non-faulty, the count of valid and invalid bits is incremented, as proposed in Algorithm 3. The successful valid transactions are appended to the chain in a final iteration.

6. Limitations of the proposed work and future scope

In this section, we present the technical limitations of the proposed work and the future scope of the work. The purpose of presenting the section is to motivate the researchers toward potential future studies that can be carried out in a similar domain. The limitations are presented as follows.

- *Security Limitation*- In the proposed scheme, we consider that Mining-as-a-Service (MaaS) is supported via the multihop CO from E_{ESP}, where E_{ES} serves as the edge server to satisfy the request. The nodes $\{N_1, N_2, \ldots, N_l\}$ offload their respective tasks to E_{ES}. The computational offloading chain is considered for fair incentive allocation. However, in case any link on the path P from *Layer 1* to *Layer (x-1)* is broken, then a real-time coordinated path setup is required to establish the connectivity back to E_{ES}. During the time of disconnection, any malicious intruder might form a replay attack where it can present a path with a lower cost to reach E_{ES}. In such cases, the nodes consider that triggered updates modify their path accordingly, leading to potential grey-hole selective attack conditions. The nodes would delete the previous paths and add the path given by the adversary, and thus, the adversary might selectively access the resources through the compromised nodes. A way to prevent such an attack is to record every possible path from *Layer 1* to *Layer x*. However, such a case would require the nodes to possibly download the entire topology states, which would increase the complexity of the scheme. Thus, as part of the future scope, an optimization and trade-off are required between active path setup versus predefined path selections to minimize costs.
- *Block size and Response Time*- In the proposed scheme, the scalability of the BC node would depend on the block size. If many transactions are added to the network, the proposed scheme becomes time-intensive to execute the transaction sets. However, miners are leveraged with computational resources, but we consider MB with limited storage and power. In such cases, many transactions might have to wait in a long queue for validation during peak transfers. A possible solution is to store the transactions in decentralized file systems, like interplanetary file systems (IPFS), and only store the content hash in the main MB. As the length of the content hash would be 32 bytes, more transactions are appended to the same block length, which improves the system's response time.
- *Collusive bidding*- The scheme *MB-MaaS* presents an auction-based strategy for fair reward pricing for E_M that depends on the amount of mining task allocated to q^{th} miner node. As nodes in *Layer 1* are closer to E_{ES}, there is more probability for E_M at *Layer 1* to mine the block. However, the proposed incentive for E_M at *Layer 1* is less and would increase with each miner at lower layers, but the miners at the last layer *x* might hardly get a chance for mining the blocks. In such cases, the miner at *Layer x* might collude with the miner at layer *Layer 1* to share his incentives if given a chance to mine the blocks. In such cases, the miners *p* and *q*, respectively at *Layer 1*, and *Layer x*, might form a collusive bidding to allow miner at *Layer x* win the election every time. Thus, as rewards are higher with increased distance d_x, the shared profits would be higher. Shyamsukha et al. [25] proposed a fair block scheme, *PoRF*, that addresses the issue by addition of a reputation score R_m with every miner E_m who takes part in the bidding process. The score R_m should increase only if the miner has proposed a fair block proposal and should be penalized (or decreased) for incorrect block proposals. However, the proposed scheme considers a sharded BC that can be costumed or tailor-made with selective chains. Thus, a generic scheme that can be integrated with sharding with fair incentives and block proposals is an open issue.
- *Interference management of 5G femtocell design*- In the scheme, in the 5G-RAN network, we consider dense femtocell units and present the analysis of power for m^{th} BS over a defined coverage range. However, in femtocell design, a crucial problem is interference management. Researchers have proposed solutions that focus on increasing the power of base cell units,

but in such cases, the setup and maintenance expense also increases [11]. Thus, in such cases, several possible solutions have focused on spectrum management and clustering femtocells with fractional frequency reuse. However, a possible direction is to form a joint channel allocation and power-aware cognitive non-orthogonal multiple access (NOMA) strategy for femtocells that maximizes the overall sum rate of nodes in the femtocell [3]. In such cases, choosing an effective pairing of strong and weak users in femtocell units to observe significant channel gain is a challenge. Thus, an effective choice of algorithms that can satisfy the pairing request of strong and weak users to maximize the sum rate is a potential future scope.

7. Conclusion

IIoT ecosystems are resource-constrained but require resilient and trusted computing infrastructures. Recently, 5G-enabled MEC has shown tremendous potential in IIoT due to flexible networking services that can be customized depending on application requirements. However, low-powered MB is applicable to secure the data exchange among sensors and induce trust in such an ecosystem. The proposed scheme, *MB-MaaS*, demonstrated the potential of the integration of MB and 5G-MEC and proposed *MaaS* to facilitate expensive mining operations in energy-constrained IIoT setups. Via fair incentive policy for miners, based on a layered multihop CO algorithm, a responsive edge-caching D2D policy is formulated for local resource allocations in a femtocellular infrastructure. Through femtocells, EN presents real-time *MaaS* to miners in case of high CO latency from distant EN. Thus, mining and EU latency are significantly reduced, increasing transaction throughput. Once mining resources are allocated, the scheme uses our proposed energy-efficient consensus mechanism *LPoP* that forms a cyclic group block validation through PN. The simulation results demonstrated that the proposed scheme outperforms other competing approaches.

Future research includes extending the scheme to include resilience to a broader range of attacks and to prove the enhanced security formally.

Declaration of competing interest

There is no Conflict of Interest.

References

[1] Abhiroop T., S. Babu, B.S. Manoj, A machine learning consensus based lightweight blockchain architecture for Internet of things, in: 2022 14th International Conference on COMmunication Systems NETworkS (COMSNETS), Banglore, India, 2022, pp. 1–6.

[2] P. Bhattacharya, S. Tanwar, R. Shah, A. Ladha, Mobile edge computing-enabled blockchain framework-a survey, in: P.K. Singh, A.K. Kar, Y. Singh, M.H. Kolekar, S. Tanwar (Eds.), Proceedings of ICRIC 2019, Springer International Publishing, Cham, 2020, pp. 797–809.

[3] I. Budhiraja, S. Tyagi, S. Tanwar, N. Kumar, M. Guizani, Cross layer noma interference mitigation for femtocell users in 5g environment, IEEE Trans. Veh. Technol. 68 (5) (2019) 4721–4733, https://doi.org/10.1109/TVT.2019.2900922.

[4] L. Chen, J. Wu, X.-X. Zhang, G. Zhou, Tarco: two-stage auction for d2d relay aided computation resource allocation in hetnet, IEEE Trans. Serv. Comput. 14 (2021) 286–299, https://doi.org/10.1109/TSC.2018.2792024.

[5] W. Chen, Z. Zhang, Z. Hong, C. Chen, J. Wu, S. Maharjan, Z. Zheng, Y. Zhang, Cooperative and distributed computation offloading for blockchain-empowered industrial Internet of things, IEEE Int. Things J. 6 (5) (2019) 8433–8446.

[6] C.-F. Cheng, Y.-C. Chen, J.C.-W. Lin, A carrier-based sensor deployment algorithm for perception layer in the iot architecture, IEEE Sens. J. 20 (17) (2020) 10295–10305.

[7] C. Del-Valle-Soto, G. Durán-Aguilar, F. Cortes-Chavez, A. Rossa-Sierra, Energy-efficient analysis in wireless sensor networks applied to routing techniques for Internet of things, in: International Conference on Applied Human Factors and Ergonomics, Springer, 2019, pp. 312–321.

[8] Y. Djenouri, D. Djenouri, A. Belhadi, G. Srivastava, J.C.-W. Lin, Emergent deep learning for anomaly detection in Internet of everything, IEEE Int. Things J. (2021), https://doi.org/10.1109/JIOT.2021.3134932, 1–9.

[9] Y. Djenouri, G. Srivastava, A. Belhadi, J.C.-W. Lin, Intelligent blockchain management for distributed knowledge graphs in iot 5g environments, Trans. Emerg. Telecommun. Technol. (2021) e4332, https://doi.org/10.1002/ett.4332https://onlinelibrary.wiley.com/doi/abs/10.1002/ett.4332 .

[10] S. Guo, Y. Dai, S. Guo, X. Qiu, F. Qi, Blockchain meets edge computing: Stackelberg game and double auction based task offloading for mobile blockchain, IEEE Trans. Veh. Technol. 69 (5) (2020) 5549–5561.

[11] R. Gupta, T. Rathod, D. Reebadiya, S. Tanwar, P. Bhattacharya, E. Pricop, Faith: trusted chain network for non-cooperative d2d communication underlying hetnet, in: 2021 13th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), 2021, pp. 1–6.

[12] D. Hanggoro, R.F. Sari, A review of lightweight blockchain technology implementation to the Internet of things, in: 2019 IEEE R10 Humanitarian Technology Conference (R10-HTC)(47129), Depok, West Java, Indonesia, 2019, pp. 275–280.

[13] Z. Hong, W. Chen, H. Huang, S. Guo, Z. Zheng, Multi-hop cooperative computation offloading for industrial iot–edge–cloud computing environments, IEEE Trans. Parallel Distrib. Syst. 30 (12) (2019) 2759–2774.

[14] J. Huang, L. Kong, G. Chen, M.-Y. Wu, X. Liu, P. Zeng, Towards secure industrial iot: blockchain system with credit-based consensus mechanism, IEEE Trans. Ind. Inform. 15 (6) (2019) 3680–3689, https://doi.org/10.1109/TII.2019.2903342.

[15] Y. Jiao, P. Wang, D. Niyato, Z. Xiong, Social welfare maximization auction in edge computing resource allocation for mobile blockchain, in: 2018 IEEE International Conference on Communications (ICC), Kansas City, MO, USA, 2018, pp. 1–6.

[16] L.P. Ledwaba, G.P. Hancke, A. Mitrokotsa, S.J. Isaac, A delegated proof of proximity scheme for industrial Internet of things consensus, in: IECON 2020 the 46th Annual Conference of the IEEE, Industrial Electronics Society, Singapore, 2020, pp. 4441–4446.

[17] X. Li, Y. Guo, L. Yan, X. Xu, Energy-aware blockchain for multiple autonomous underwater vehicles cooperative operation, in: 2021 40th Chinese Control Conference (CCC), 2021, pp. 3005–3010.

[18] Y. Li, J. Wu, L. Chen, Poem+: pricing longer for mobile blockchain computation offloading with edge computing, in: 2019 IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on Data Science and Systems (HPCC/SmartCity/DSS), Zhangjiajie, China, 2019, pp. 162–167.

[19] J.C.-W. Lin, G. Srivastava, Y. Zhang, Y. Djenouri, M. Aloqaily, Privacy-preserving multiobjective sanitization model in 6g iot environments, IEEE Int. Things J. 8 (7) (2021) 5340–5349, https://doi.org/10.1109/JIOT.2020.3032896.

[20] M. Liu, F.R. Yu, Y. Teng, V.C.M. Leung, M. Song, Computation offloading and content caching in wireless blockchain networks with mobile edge computing, IEEE Trans. Veh. Technol. 67 (11) (2018) 11008–11021, https://doi.org/10.1109/TVT.2018.2866365.

[21] M. Liu, F.R. Yu, Y. Teng, V.C.M. Leung, M. Song, Joint computation offloading and content caching for wireless blockchain networks, in: IEEE INFOCOM 2018 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Honolulu, HI, USA, 2018, pp. 517–522.

[22] T. Liu, J. Wu, L. Chen, Y. Wu, Y. Li, Smart contract-based long-term auction for mobile blockchain computation offloading, IEEE Access 8 (2020) 36029–36042, https://doi.org/10.1109/ACCESS.2020.2974750.

[23] P.K.R. Maddikunta, Q.-V. Pham, B. Prabhadevi, N. Deepa, K. Dev, T.R. Gadekallu, R. Ruby, M. Liyanage, Industry 5.0: a survey on enabling technologies and potential applications, J. Ind. Inf. Integr. 26 (2022) 100257, https://doi.org/10.1016/j.jii.2021.100257.

[24] D. Mazzei, G. Baldi, G. Fantoni, G. Montelisciani, A. Pitasi, L. Ricci, L. Rizzello, A blockchain tokenizer for industrial iot trustless applications, Future Gener. Comput. Syst. 105 (2020) 432–445.

[25] S. Shyamsukha, P. Bhattacharya, F. Patel, S. Tanwar, R. Gupta, E. Pricop, Porf: proof-of-reputation-based consensus scheme for fair transaction ordering, in: 2021 13th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), 2021, pp. 1–6.

[26] K. Suankaewmanee, D.T. Hoang, D. Niyato, S. Sawadsitang, P. Wang, Z. Han, Performance analysis and application of mobile blockchain, in: 2018 International Conference on Computing, Networking and Communications (ICNC), 2018, pp. 642–646.

[27] V. Sundararaj, Optimal task assignment in mobile cloud computing by queue based ant-bee algorithm, Wirel. Pers. Commun. 104 (1) (2019) 173–197.

[28] X. Wang, X. Chen, W. Wu, Towards truthful auction mechanisms for task assignment in mobile device clouds, in: IEEE INFOCOM 2017 - IEEE Conference on Computer Communications, Atlanta, GA, USA, 2017, pp. 1–9.

[29] M. Wu, K. Wang, X. Cai, S. Guo, M. Guo, C. Rong, A comprehensive survey of blockchain: from theory to iot applications and beyond, IEEE Int. Things J. 6 (5) (2019) 8114–8154, https://doi.org/10.1109/JIOT.2019.2922538.

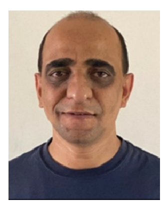
[30] X.-W. Wu, E.-H. Yang, J. Wang, Lightweight security protocols for the Internet of things, in: 2017 IEEE 28th Annual International Symposium on Personal, In-

door, and Mobile Radio Communications (PIMRC), Montreal, QC, Canada, 2017, pp. 1–7.
[31] Z. Xiong, S. Feng, D. Niyato, P. Wang, Z. Han, Optimal pricing-based edge computing resource management in mobile blockchain, in: 2018 IEEE International Conference on Communications (ICC), Kansas City, MO, USA, 2018, pp. 1–6.
[32] Z. Xiong, Y. Zhang, D. Niyato, P. Wang, Z. Han, When mobile blockchain meets edge computing, IEEE Commun. Mag. 56 (8) (2018) 33–39, https://doi.org/10.1109/MCOM.2018.1701095.
[33] C. You, Y. Mao, J. Zhang, K. Huang, Energy-efficient offloading for mobile edge computing, in: Wiley 5G Ref: The Essential 5G Reference Online, 2019, pp. 1–18.
[34] Y. Yu, Mobile edge computing towards 5g: vision, recent progress, and open challenges, China Commun. 13 (Supplement2) (2016) 89–99, https://doi.org/10.1109/CC.2016.7833463.
[35] W. Zhan, C. Luo, G. Min, C. Wang, Q. Zhu, H. Duan, Mobility-aware multi-user offloading optimization for mobile edge computing, IEEE Trans. Veh. Technol. 69 (3) (2020) 3341–3356.

Pronaya Bhattacharya is currently employed as an Assistant Professor with the Computer Science and Engineering Department, Institute of Technology, Nirma University, Ahmedabad, India. He has over eight years of teaching experience. He has authored or coauthored more than 60 research papers in leading SCI journals and top core IEEE COMSOC A* conferences. Some of his top-notch findings are published in reputed SCI journals, like IEEE JOURNAL OF BIOMEDICAL AND HEALTH INFORMATICS, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, IEEE INTERNET OF THINGS JOURNAL, IEEE TRANSACTIONS ON NETWORK SCIENCE AND ENGINEERING, IEEE ACCESS, ETT (Wiley), Expert Systems (Wiley), FGCS (Elsevier), OQEL (Springer), WPC (Springer), ACM-MOBICOM, IEEE-INFOCOM, IEEE-ICC, IEEECITS, IEEE-ICIEM, IEEE-CCCI, and IEEE-ECAI. He has 786 citations to his credit with an H-index of 15 and an i10-index of 18. His research interests include healthcare analytics, optical switching and networking, federated learning, blockchain, and the IoT. He has been appointed as a technical committee member and the session chair across the globe. He is a Lifetime Member of professional societies, like ISTE and IAENG. He was awarded the seven Best Paper Awards in Springer ICRIC-2019, IEEE-ICIEM-2021, IEEE-ECAI-2021, and Springer COMS2-2021. He is a Reviewer of 17 reputed SCI journals, like IEEE INTERNET OF THINGS JOURNAL, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE ACCESS, IEEE Network, ETT (Wiley), IJCS (Wiley), MTAP (Springer), OSN (Elsevier), WPC (Springer), and others.

Farnazbanu Patel is a Post graduate student of Nirma University, batch of 2021. Her research interests lie in the area of integration of 5G and Blockchain Technology, focused to solve real-world problems.

Sudeep Tanwar (Senior Member, IEEE) is currently working as a Professor with the Computer Science and Engineering Department, Institute of Technology, Nirma University, India. He is a Visiting Professor at Jan Wyzykowski University, Polkowice, Poland; and the University of Pitesti, Pitesti, Romania. He has authored two books, edited 13 books, and more than 270 technical papers, including top journals and top conferences, such as IEEE TRANSACTIONS ON NETWORK SCIENCE AND ENGINEERING, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE WIRELESS COMMUNICATIONS, IEEE Network, ICC, GLOBECOM, and INFOCOM. He initiated the research field of blockchain technology adoption in various verticals, in 2017. His H-index is 50. He actively serves his research communities in various roles. His research interests include blockchain technology, wireless sensor networks, fog computing, smart grid, and the IoT. He is a member of the Technical Committee on Tactile Internet of the IEEE Communication Society. He is a Senior Member of CSI, IAENG, ISTE, and CSTA. He has been awarded the Best Research Paper Awards from IEEE GLOBECOM 2018, IEEE ICC 2019, and Springer ICRIC-2019. He has served many international conferences as a member of the organizing committee, such as the Publication Chair for FTNCT-2020, ICCIC 2020, and WiMob2019; a member of the Advisory Board for ICACCT-2021 and ICACI 2020; the Workshop Co-Chair for CIS 2021; and the General Chair for IC4S 2019 and 2020 and ICCSDF 2020. He is serving on the editorial boards for Frontiers of Blockchain, Cyber Security and Applications, Computer Communications, the International Journal of Communication Systems, and Security and Privacy.



Neeraj Kumar is a professor at Thapar Institute of Engineering and Technology, Deemed to be University, India. He received his Ph.D. from SMVD University, India, in CSE and was a postdoctoral research fellow at Coventry University, United Kingdom. He has more than 400 research papers in leading journals and conferences of repute. He is an Associate Editor/Technical Editor of IEEE Communications Magazine, IEEE Network, IJCS (Wiley), JNCA (Elsevier), ComCom (Elsevier), Security and Privacy (Wiley), the IEEE Systems Journal, and ACM Computing Surveys.

Ravi Sharma is working as a Professor in the Centre for Inter-Disciplinary Research and Innovation, University of Petroleum and Energy Studies, Dehradun, India. Dr Sharma is passionate in the field of Business analytics and worked in various MNC's as a leader of various software development groups. Dr Sharma has contributed various articles in the area of business analytics, prototype building for startup, and artificial intelligence. Dr Sharma leading academic institutions as a consultant to uplift research activities in inter-disciplinary domains.