Incentive Techniques for the Internet of Things: A Survey

Praveen Kumar Reddy Maddikunta, Quoc-Viet Pham, *Member, IEEE*, Dinh C. Nguyen, *Member, IEEE*,
Thien Huynh-The, *Member, IEEE,* Ons Aouedi, *Member, IEEE*,
Gokul Yenduri, and Thippa Reddy Gadekallu, *Senior Member, IEEE*

***Abstract*—The Internet of Things (IoT) has remarkably evolved over the last few years to realize a wide range of newly emerging services and applications empowered by the unprecedented proliferation of smart devices. The quality of IoT networks heavily relies on the involvement of devices for undertaking functions from data sensing, computation to communication and IoT intelligence. Stimulating IoT devices to actively participate and contribute to the network is a practical challenge, where incentive techniques such as blockchain, game theory, and Artificial Intelligence (AI) are highly desirable to build a sustainable IoT ecosystem. In this article, we present a comprehensive survey on the incentive techniques for IoT, aiming to provide general readers with an overview of incentive-enabled IoT from background, motivations, and enabling techniques. Particularly, we provide an extensive review on the use of incentive techniques in a number of key IoT services, such as IoT data sharing, IoT data offloading and caching, IoT mobile crowdsensing, and IoT security and privacy. Subsequently, we explore the potential of incentives in important IoT applications, ranging from smart healthcare, smart transportation to smart city and smart industry. The research challenges are then highlighted, and potential directions are also discussed for future research of this important area.**

***Index Terms*—Incentives, Internet of Things, Game Theory, Blockchain, Artificial Intelligence, Smart Applications.**

I. Introduction

Recent years have witnessed the rapid growth of the Internet of Things (IoT) with the unprecedented proliferation of mobile devices such as smartphones, personal computers, and wearables. The advancement in this fundamental technology has empowered a wide range of applications, e.g., smart healthcare, smart transportation, and smart city, and thus effectively support our daily life [1]. In this context, IoT devices are employed to sense data from the physical environments via sensors for computation, storage, and training with machine learning (ML) integrated with smart devices [2]. For example, mobile crowd sensing (MCS) is an attractive solution for such IoT sensing platforms, where information can be recorded from sensors, e.g., camera and GPS modules, to serve end-users, such as human detection and localization. Moreover, IoT plays significant role in providing communication-related services such as data offloading with edge cloud servers for computation enhancement, user interconnection for global networking, and information exchange for collaborative IoT services [3].

Although IoT can provide significant services and applications, how to attract IoT devices to participate and contribute to the network is a practical challenge. Indeed, the quality of such networks and systems largely relies on the involvement of IoT devices to support end-users. However, IoT devices that undertake certain roles (e.g., data computation) in the system suffer extra resource consumption such as battery and memory. For instance, a smart IoT device needs to allocate part of its CPU resources to execute a data request from a user and also uses its memory to store data sensed from surrounding sensors. Due to such incurred operating expenses, certain IoT devices may be reluctant to share their resources which prevents the deployment of IoT platforms in practice. Furthermore, IoT devices may not be willing to share their data with others because of the lack of sufficient incentives. This is particularly true in real-world scenarios, for example, where patients do not want to send their health information to hospital doctors or insurance companies in the health IoT network if no benefits are given. Another challenge comes from the insufficient motivation of IoT nodes to participate in collaborative IoT services such as collaborative data training in intelligent IoT networks or cooperative data management in IoT storage platforms. For example, to realize federated data learning in IoT systems [4], the collaboration of devices is needed to address the common learning task, where each of them holds an important role in training its local data for building the global ML model. Without enough incentives, IoT devices may not be motivated to join the data training [5], [6].

Therefore, developing incentive solutions with fundamental technologies such as blockchain, Artificial Intelligence (AI), and game theory is highly needed for enabling sustainable IoT networks and systems. For example, blockchain can be used as an incentive platform for decentralized data sharing in IoT [7], where IoT users can retain control of the data sharing while earning incentives. In this regard, user-controlled privacy and data-sharing policies can be established using smart contracts [8] that support building up incentives for users

Praveen Kumar Reddy Maddikunta, Gokul Yenduri, andd Thippa Reddy Gadekallu are with the School of Information Technology, Vellore Institute of Technology, Tamil Nadu- 632014, India (email: {praveenkumarreddy, gokul.yenduri, thippareddy.g}@vit.ac.in).

Quoc-Viet Pham is with the Korean Southeast Center for the 4th Industrial Revolution Leader Education, Pusan National University, Busan 46241, Korea (e-mail: vietpq@pusan.ac.kr).

Dinh C. Nguyen is with the School of Engineering, Deakin University, Waurn Ponds, VIC 3216, Australia (e-mail: cdnguyen@deakin.edu.au).

Thien Huynh-The is with the ICT Convergence Research Center, Kumoh National Institute of Technology, Gumi, Gyeongsangbuk-do 39177, Korea (e-mail: thienht@kumoh.ac.kr).

Ons Aouedi is with the University of Nantes, France (e-mail: ons.aouedi@ls2n.fr

to share their profile data in terms of rewards (micro-payments or credits). Moreover, game theory can be exploited to develop incentive solutions for IoT data offloading [9], by encouraging more users to upload their data to the shared server for caching under a game-theoretic offloading formulation to ensure the benefits for all users in terms of latency minimization and coin earning. AI is also a powerful tool for building incentive mechanisms based on data learning and mining [10], which can encourage IoT users to participate in data training to obtain revenues as well as achieve their working objectives such as classification or regression in involved IoT applications. For instance, AI techniques are promising to train the energy trading policies via energy-related data training [10], aiming to support the service providers in the prediction of energy workloads and energy prices in a period of time, which in turn ensures the stability of smart grid systems. Incentive mechanisms are also necessary to promote the participation of distributed vehicles in sharing and computing data for vehicular services, such as traffic prediction and vehicular routing [11]. Moreover, smart homes can be stimulated to join the energy purchase process with electricity plants via incentive mechanisms enabled by blockchain that can offer credits (e.g., coins) for energy trading. The increasing significance of incentive techniques in IoT makes now the right time to draw attention to this prominent area of research.

A. Comparison and Our Key Contributions

Driven by the importance of incentive mechanisms and IoT, several related reviews have been conducted. For example, the study in [3] carried out a survey on incentive mechanisms for mobile crowdsensing, in which the incentive mechanisms are classified into two main categories: monetary and non-monetary. While the former motivates the IoT devices to perform sensing tasks with monetary benefits, the latter encourages the participants to contribute to sensing tasks to reduce their individual costs. Another survey on incentives for mobile crowdsensing was presented in [5], where the incentive techniques are divided into three branches, namely entertainment, service, and money. A survey was conducted in [6] to summarize the theoretical studies, applications, implementations, and experiments of incentive mechanisms in participatory sensing. Originated from economics, game theory has played an important role in designing distributed and incentive mechanisms for wireless and IoT networks. In [12], the importance of network effects was highlighted in crowdsensing services, and game theory was shown to be a promising tool to design incentive schemes for such services. Further, this work also developed an incentive algorithm that leverages the Bayesian Stackelberg game to model the interaction between services providers and users. The work in [13] reviewed the design of rewards in contract theory and demonstrated the use of contract theory-based incentive mechanisms for emerging scenarios in wireless networks, such as adverse selection, moral hazard, and spectrum trading. In [14], the coalition game was used to design two cooperative incentive approaches in ultra-dense heterogeneous networks. A review on game theory and multi-access edge computing (MEC) was presented in [15], where game theory can be used to design various incentive schemes for MEC systems.

The potential of AI and blockchain in designing incentive mechanisms have been explored, and thus there have been some surveys on this topic. For example, the works in [16], [17] revealed that game theory is a promising analytical tool for incentive mechanisms in blockchain consensus. Recent studies in [18], [19] showed that blockchain is a powerful concept to enhance the security of aerial access networks, and game theory has the potential to design incentive algorithms for such blockchain-enabled networks. The work in [20] explored the applicability of blockchain to design secure and incentive content delivery in autonomous vehicle systems. The use of blockchain to design incentive caching schemes in device-to-device (D2D) and MEC was studied in [21]. Recently, the use of AI techniques, such as deep reinforcement learning (DRL) and deep learning (DL) [22], along with game theory and blockchain for incentive design, has been extensively studied. For example, the work in [23] adopted blockchain and DRL to design an incentive and trust content sharing scheme in information-centric networks. The work in [24] identified incentive as an important design issue in FL and reviewed various incentive schemes in FL using blockchain and smart contract. Recent reviews in [25], [26] summarized incentive designs in FL according to different approaches, namely data contribution, FL client reputation, and resource allocation [26] and according to the incentive techniques, such as game theory, AI, and blockchain [25]. A summary table of related reviews on incentive mechanisms and our work is shown in Table I.

Although incentive techniques have been reviewed in the literature, there is no comprehensive review that is dedicated to the use of incentive techniques in the IoT network and for key IoT applications and services. Applications of recent advances in game theory, blockchain, and AI for incentives in IoT have not been explored in [3], [5], [6]. Moreover, the use of game theory, blockchain, and AI in designing incentive mechanisms for IoT services and vertical applications has not been reviewed in the literature [12]–[21], [23]–[26]. This big gap motivates us to carry out this comprehensive survey on incentive mechanisms for IoT. The key contributions of this paper are extensive discussions on the use of incentive techniques for various IoT services (e.g., IoT data sharing, IoT data offloading and caching, mobile crowdsensing, and IoT privacy and security) and IoT applications (e.g., smart healthcare, smart transportation, smart city, and smart industry). From the extensive review, we also discuss several key challenges and highlight potential solutions and research direction in this interesting topic. In summary, the main contributions offered by this work can be summarized as follows.

1) Firstly, we present a comprehensive survey on incentive IoT and start by a preliminary to IoT data network and the fundamentals of important incentive techniques, including blockchain, game theory, and AI.
2) Secondly, we discuss the use of incentive techniques for key IoT services, namely IoT data sharing, IoT data offloading and caching, mobile crowdsensing, and IoT privacy and security. Moreover, we provide a summary

that summarizes the key contributions, lessons, and limitations of the reviewed literature.

3) Thirdly, we extensively review the use of incentive techniques for important vertical IoT domain applications: smart healthcare, smart transportation, smart city, and smart industry.
4) Finally, based on the reviewed literature on the use of incentive techniques for IoT services and vertical domain applications, we identify a number of key challenges and promising directions that may stimulate further studies on this topic.

B. Paper Organization

This paper is organized as follows. In Section II, we present the fundamentals of IoT and three main incentive techniques: blockchain, game theory, and AI. Next, in Section III, we discuss the use of incentive techniques for IoT services, including data sharing, data offloading and caching, mobile crowdsensing, and privacy and security. Then, applications of incentive techniques in vertical domain applications (e.g., smart healthcare, smart transportation, smart city, and smart industry) are discussed in Section IV. After that, key challenges and promising solutions are highlighted in Section V to drive further studies on IoT incentive mechanisms. Finally, we conclude the paper in Section VI.

II. Fundamental Incentive Techniques for IoT

In this section, the fundamentals of IoT data network infrastructure are discussed, followed by a discussion on several techniques that can be used in designing incentive mechanisms for IoT, such as blockchain, game theory, and AI.

A. IoT Data Network Infrastructure

In IoT networks, a full-life cycle of data infrastructure consists of sensing, collecting, and processing data from a large number of devices (e.g., mobile phones, wearable devices, smart vehicles, and others in wireless sensor networks) equipped with a rich set of sensors [27]. In general, IoT allows sharing data, extracting information, and perceiving knowledge between different users based on the collaboration of individuals within the same domain interest and across different domain interests, thus achieving context awareness more thoroughly. The popularity and innovation of smartphones and wearable devices having various built-in sensors are the crucial factors that drive the development and success of the IoT paradigm. For instance, the sensory data acquired from smartphone sensors (including accelerometer, gyroscope, GPS, barometer, compass, fingerprint, microphone, and camera) are being used for many mobile-aid applications in a wide range of domains, such as healthcare and wellness, geosciences, and transportation. Despite being similar to static nodes in terms of sensing, computing, and communicating, smartphones are more superior with portability and much more resources of battery supply, computing power, memory storage, connection range, and data transmission speed. Obviously, the IoT research aims to converge individual mobile technologies along with pervasive urban growth to enhance the quality of citizen's daily life.

Currently, most of the existing IoT systems are developed based on a general architecture, shown in Fig. 1, consisting of five layers: sensing, communication, data, information, and service/application, where several incentive techniques can be incorporated in different layers to encourage the development and the contribution of service providers and end users. Here the components with their functions of the layers are explored in brief as follows.

- *Sensing layer:* At the bottom of the architecture, the sensing layer plays the role of *listening* to the world via sensors. Mobile devices with various built-in sensors (e.g., accelerometer, gyroscope, GPS, compass, microphone, and camera) allow acquiring raw signals from nature. These signals are transformed with analog-to-digital converter (ADC) modules for storage and processing hereafter. Some other specialized sensors, such as magnetometer, temperature, radiation, and air quality sensors, can be connected to mobile devices via sensor adapter. In addition to data acquisition, this layer takes other functionalities, including sensor configuration (e.g., sampling rate, frequency response, and range of value) and sourcing multimodality (e.g., time-series signal, high-dimensional signal, image, and video).
- *Communication layer:* This layer takes the responsibility for transmitting the data acquired from mobile devices to data center and cloud platform. Currently, mobile devices (such as smartphones and smartwatches) are equipped with several wireless connection and communication technologies (e.g., WiFi, Bluetooth, cellular, and satellite). Some advanced techniques can be exploited to enhance data transmission rate, reduce latency, and improve communication reliability.
- *Data layer:* In IoT systems, the sensory data can be stored in data center via centralized and decentralized storage systems. Relying on specific scenarios, e.g., the need of service providers and the support of mobile devices, data can also be located on cloud and fog servers. The data layer comprises some major components which perform data buffering, synchronization, maintenance, persistence, and exporting. Due to the high volume, variety, and velocity of multimodal sensory data from numerous devices, these processes can be complicated.
- *Information layer:* Processing data to attain meaningful information and knowledge is crucial in IoT systems, which is accomplished in the information layer. Various techniques and algorithms are exploited to process different types of data, which in turn acquire low-level and high-level information regarding concerning mobile services and applications. Notably, as the key technology to enhance performance, AI with pattern recognition should be applied to handle the large-scale heterogeneous data issue. In particular, supervised learning, unsupervised learning, semi-supervised learning, and RL with traditional machine learning (ML) algorithms and innovative DL architectures are exploited in data-driven and model-

TABLE I
SUMMARY OF RELATED REVIEWS ON INCENTIVE MECHANISMS.

References	**Contributions**	**Limitations**
[3]	A review of incentive mechanisms in mobile crowdsensing was presented.	The applicability of game theory, blockchain, and AI for incentive design was not explored.
[5], [6]	Comprehensive surveys on incentive mechanisms in mobile crowdsensing [5] and participatory sensing [6] were conducted.	The applicability of game theory, blockchain, and AI for incentive design was not explored.
[12]	Game theory was leveraged to design incentive mechanisms for crowdsensing services considering network effects.	The potential of incentives for IoT services and vertical applications was not studied.
[13], [14]	Game-theoretic approaches, such as Bayesian Stackelberg game and contract theory, were used to design incentive strategies in wireless networks.	These short papers were only limited to the applicability of game theory, while incentives for IoT were not studied.
[15]	Applications of various game-theoretic models for related scenarios in MEC systems (e.g., sensor networks, unmanned networks, heterogeneous networks, and vehicular networks) were reviewed.	This work did not focus on the potential of game theory for IoT services and IoT vertical applications, and the use of advanced blockchain and AI techniques.
[16], [17]	The importance of incentive designs in blockchain consensus protocols was emphasized.	This work focused mainly on blockchain but not incentives for IoT services and applications.
[18], [19]	Applications of blockchain for incentive designs in aerial access networks were studied.	These works did not focus on incentives for IoT services and applications.
[20], [21]	The applicability of blockchain to design secure and incentive mechanisms in future networks (e.g., autonomous vehicle systems and D2D communications) was investigated.	These short papers did not focus on incentives for IoT services and applications.
[23]	Blockchain and DRL were jointly used to design an incentive and trust content delivery scheme in information-centric networks.	This survey focused on a specific scenario in information-centric networks, while the review of incentives for IoT services and IoT applications were ignored.
[24]	This work highlighted incentives as an important design issue in FL and reviewed blockchain-based incentive solutions.	This work focused mainly on the use of blockchain for FL at mobile computing networks.
[25], [26]	Concise reviews on incentive mechanisms in FL.	Incentives for IoT services and IoT vertical applications were not the main focus of these papers.
This paper	A comprehensive survey on the use of blockchain, game theory, and AI for the design of incentive mechanisms for IoT services and IoT vertical domain applications. From the intensive survey, we also highlight a number of key challenges and potential solutions to stimulate further research on this interesting topic.	-

driven approaches for clustering, classification, and regression tasks. A pre-processing step can be examined to eliminate noise and remove outliers in a large-noisy-confusing dataset.

- *Service/Application layer:* On the top of the architecture, the service/application layer receives the meaningful information derived from the information layer to provide to users who can access through open and secure application programming interfaces (APIs). Although the components in this layer can vary along with requested services, typically, they are responsible for the following basic functions: service orchestration, authoring, and analytic with visualization. Furthermore, user interface and user experience play human-machine responsiveness and interactivity. Many existing applications in IoT systems can be divided into the task-wise category (with scheduling, assignment, and execution) and the user-wise category (with use type, recruitment, and selection).

In the rest of this section, we present the most important techniques used in current IoT networks, including game theory, blockchain, and AI.

B. Blockchain

Blockchain has gained popularity in recent years since the inception of bitcoin. Blockchain is a distributed ledger in which the transactions are stored in blocks, and they are distributed and duplicated across millions of devices in the network [28], [29]. Whenever a new transaction is executed, it is updated in the ledger of all the blocks in the blockchain network. The transactions are recorded with hash functions. The data in the blockchain can be modified only if the data in more than 50% of the blocks is updated, which makes it nearly impossible to cheat, hack, or change the data [30]. One of the key enabling technologies of blockchain is a smart contract, which executes automatically when a record is updated or whenever a new block is added to the blockchain. Through smart contracts, the trustability of the nodes/blocks in the blockchain can be ensured. Apart from immutability and trustability, blockchain is also known for traceability. As all the transactions are stored in an immutable manner, the products can be easily traced throughout their lifecycle. These properties of blockchain, namely, security, traceability, trustability, and immutability, are the main reasons for increased usage of blockchains across the industry domains such as supply chain,

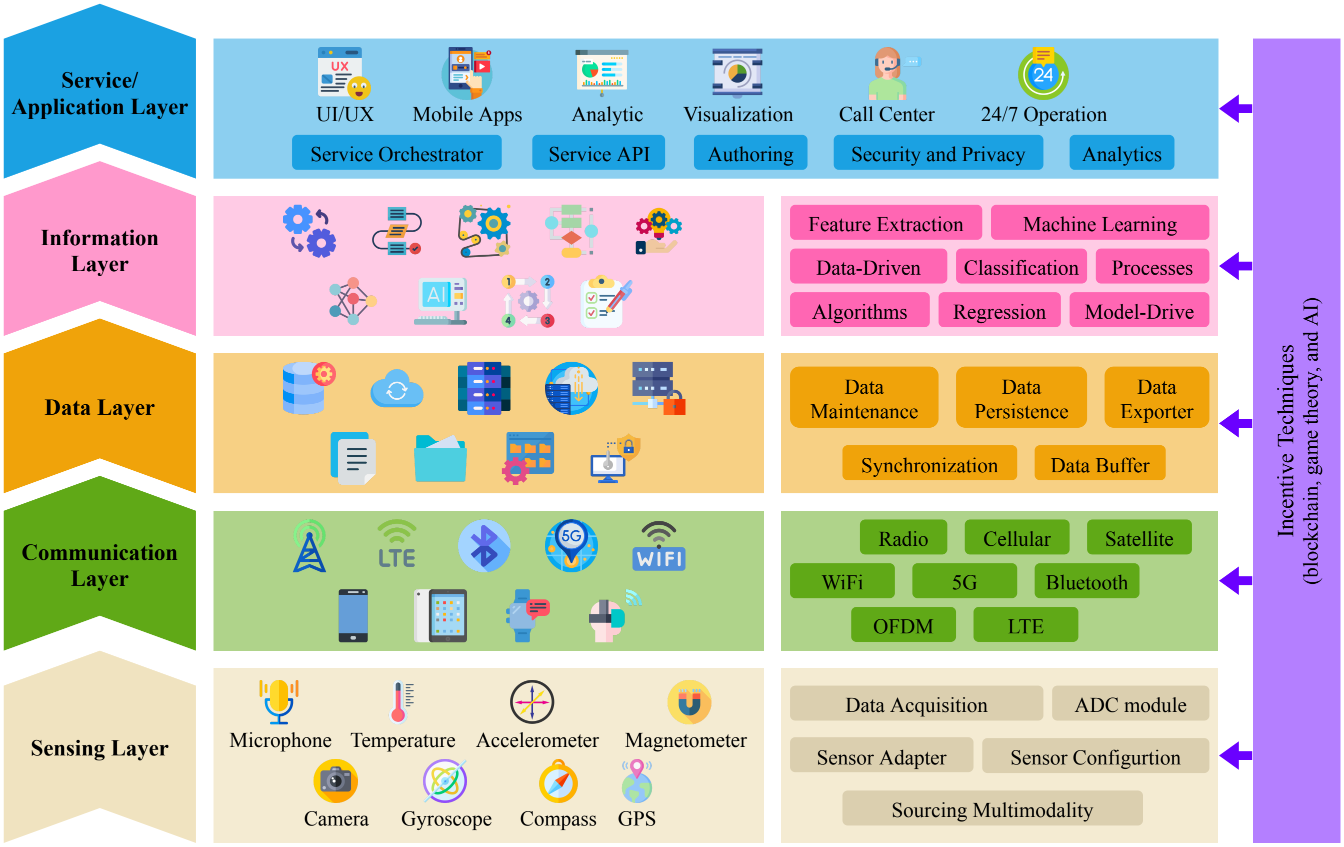

Fig. 1. IoT data network infrastructure.

healthcare, insurance, smart cities, etc [31], [32].

Blockchain has immense potential in incentive mechanisms in IoT. Blockchain can ensure transparency of incentives calculated, secure the data generated by the volunteer nodes in crowd-sourcing, preserve the privacy of the participants who sense the data from the environment as requested by the requesters [33]. In this context, edge servers compute tasks from IoT devices that receive a reward given by the blockchain each time they purchase more computational resources. To ensure security, the authors in [34] proposed an incentive mechanism based on the blockchain platform to motivate IoT devices to purchase more computational resources when they participate in the mining process. Clients get unfair rewards from service providers (SP) when they participate in collaborative tasks. Even though the reward payment seems low, the SPs should provide accurate and secure services to lightweight clients (LC). Therefore, [35] implemented a fair payment system where the clients send requests to the SPs through blockchain. The SP provides the service codes in an off-chain method. The client validates the service codes received and pays the price of the service to the SP. The originality of the proposed incentive mechanism enhanced the reputation of the SPs; consequently, clients send more requests to the SP as they get affordable incentives from the SPs .

C. Game Theory

Game theory is an important branch in applied mathematics, in which tools are provided to analyze the situations where the players have to make decisions based on the actions/decisions taken by other players in the game, i.e., the decisions made by the players are interdependent. The players in the game may have opposed, similar, or mixed interests. A solution to a game depends on the outcomes from the optimal decisions of the players. Game theory has applications in several situations where the players' interactions affect the outcome of the game. For example, game theory can be used to determine what business conglomerates or political coalitions can be formed, the optimal selling price of a product/service in the competition, which voter or group of voters have power, selection of personnel for the jury, best possible location for a manufacturing plant, etc [36], [37].

Game theory can play a very important role in calculating incentives in IoT-based applications as they involve many participants who work in a cooperative or independent manner to provide the necessary data to the requesters. Some of the recent works on incentive mechanisms using game theory are discussed below.

To enhance the performance of physical layer security (PLS), extra devices generate artificial jamming voluntarily by enabling jammers to consume their own power. To force jammers to voluntarily participate in the cooperation, the work in [38] introduced an incentive mechanism into the routing design, aiming to satisfy rewards for jammers who generate jamming signals to guarantee PLS performance. To enhance the performance evaluation, a two-stage Stackelberg game was designed to work in two stages. In the first stage, the source aims at maximizing its utility by determining the optimal rewards; in the second stage, each jammer independently focuses on its jamming consumption power while competing for the rewards based on how its contribution to the PLS is enhanced, which is formulated as a non-cooperative game [38].

Radio frequency energy harvesting (RFEH) based IoT system consisting of a data access point (DAP), and several energy access points (EAPs) has been recently proposed to collect information [39]. In an RFEH-based IoT system, EAPs support sensors by providing wireless charging services via the radio frequency (RF) energy transfer technique. DAP collects data from sensors. Since the DAP and EAPs may be operated by different operators, the way to motivate them to carry out the task of collecting data is required to motivate self-interested EAPs to help charge the sensors. To motivate the third party, [40] proposed an effective incentive mechanisms to improve the payoff of the DAP as well as those of EAPs. The proposed scheme considered the complete information that the EAPs will truthfully report to the DAP, e.g., their channel gains between EAPs and sensors and their energy costs. To evaluate the performance caused by information asymmetry, the existing Stackelberg game-based approach with complete information has been considered due to the lack of complete information. As a result, the expected utility function of the DAP is defined and optimized in the Stackelberg game. In addition, the authors applied contract theory to determine an optimal contract that aims at motivating the EAPs under asymmetric information. The monopoly labor market in economics helps in modeling the contract for the RFEH-based IoT, where the DAP is modeled as the employer who offers an agreement contract to each EAP. The agreement contract is composed of contract items, which are considered as combinations of energy-reward pairs.

D. Artificial Intelligence

AI is a branch of computer science in which machines are trained to think and act like humans. It leverages machines and computers to mimic the decision-making and problem-solving capabilities of the mind of humans [41]. AI is widely used in computer vision, healthcare systems, automotive vehicles, speech recognition, and natural language processing. Among many branches of AI, machine learning (ML) and deep learning (DL) are two important approaches. ML addresses the question of how to build a computer system that improves automatically through experience [42], [43]. It tries to automate the process of knowledge extraction from training data to make predictions on unseen data. For example, historical traffic data are used to improve traffic classification and reduce congestion. In other words, the main idea of ML is to generalize beyond the examples in the training set and hence can be thought of as "programming by example". However, building models using conventional ML models is bottlenecked by the amount of features engineering required [44]. In the meanwhile, DL-based models are able to learn hidden features through multiple non-linear processing units (i.e., neurons) in deep architecture.

Although these ML/DL-based models have been successfully used to classify the participant users/devices based on the value of the information provided or on their performance so that they can be incentivized accordingly, they require a central entity to process the data collected from all users in the network. Data transmission to a central entity may cause a direct breach of privacy, be time-consuming, and can introduce network congestion [45]. To solve these issues, distributed learning such as federated learning (FL) has been proposed [46]. Unlike the traditional ML/DL, the learning process with the distributed learning concept occurs locally at each device. Some of the recent works using distributed DL models for incentive mechanisms are discussed below.

Preserving the privacy of users participating in collecting training data requires secure mechanisms. In the case of distributed deep learning, an incentive mechanism based on blockchain is discussed in [47]. The authors proposed a secure and decentralized framework based on a blockchain incentive mechanism. This mechanism used cryptographic primitives for privacy-preserving distributed deep learning, which can deliver data confidentiality, computation auditability, and incentives for parties who participate in collaborative training. Also, an incentive mechanism has recently been used with FL [45] to motivate high-reputation clients (e.g., high-quality data, high computation resource) to participate in the training process [48], and without a reward mechanism, the data owners (e.g., clients) will be reluctant to join the learning [26]. It may improve the final model quality, lead to faster local training, and hence fewer communication rounds needed between the server and the clients [49]. Therefore, considering an FL setting that consists of a central server and a set of clients, it is essential for the server to develop an incentive mechanism to encourage more clients participation. In this context, several contributions have been proposed. For example, the work in [50] used an incentive mechanism by combining contract theory with reputation and blockchain [51] in order to motivate the clients with high-quality data to join the FL process.

III. Applications of Incentive Techniques for IoT Services

In this section, the applications of incentive techniques for IoT services such as data sharing, data offloading and caching, mobile crowdsensing, privacy and security are discussed along with recent state of the art.

A. Incentives for IoT Data Sharing

The accelerated advancement of cloud technology has increased the number of businesses and enterprises intending to keep their secure information on cloud platforms. Cloud services facilitate firms and organizations to use their services, hardware, and resources effectively and efficiently. Various devices being used extensively in and around us generate massive volumes of information that are often maintained by cloud servers [52]. Apart from storage and management, there is also a need to distribute the required data to legitimate data owners. In the present day and age, data sharing, information sharing, disclosure has become extremely predominant at all levels of society. It is evident from various studies that data sharing and reuse are extremely helpful in the processes involved in

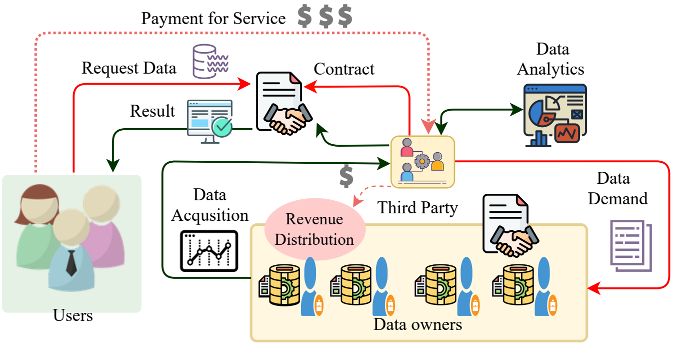

Fig. 2. Reward distribution for IoT data sharing between data owners and third parties.

sharing of data resources which also contributes to enhancing the efficiency and quality of work guiding innovation as well. Efficient data sharing techniques eliminate redundancies and repetition of work. This is the era of big data and digital technologies that have grown enormously and have become a critical strategic resources. In spite of all its positivity, the big data industry has been facing a major challenge pertinent to “data islands,” resulting in an acute dilemma in decision making [53], [54]. The best possible solution to this issue is to develop a reasonable and efficient data-sharing model. Since there exist limitations relevant to data volume and diversity among individual data owners, the idea of data sharing across several cloud platforms will assist third-party participants in using diverse big data analytical methodologies. This would enable the incorporation of value-added services by offering healthcare services to customers by collecting medical data from various hospitals. Data sharing, apart from its varied applications, renders significant contributions to the present human lives. There are three major obstacles related to data sharing: refusal to share, worry of sharing, and difficulty to share data. Although immense efforts are still being directed, the issues relevant to mutual-trust relationships and increase in user participation are yet to be resolved. It is also difficult to provide incentives that allow both reliable and collaborative data exchange across numerous cloud platforms. The present solution to such challenges would be to use the third party as trusted organizations enabling data sharing. However, there is no dynamic incentive scheme to guarantee data sharing across a large number of users. There are issues relevant to slow response speed, data tampering, and unsecured transmissions in the classical data-sharing model.

Fig. 2 depicts the reward distribution mechanism used for data sharing between data owners and third parties in IoT-based systems. The existing cloud-based data sharing models are also vulnerable due to centralized storage problems wherein users requesting data often get perplexed regarding privacy, data leakage, and data tampering issues. The revenue distribution, on the other side, tends to become more reasonable encouraging participants to improve the quality of service (QoS), data reliability in order to generate a high level of profits. Efficient incentive mechanisms should be promoted and exploited to attract more cloud stakeholders involved in data sharing to participate in coalition ensuring data sharing actively that maintains the quality and revenue of services.

In order to overcome the aforementioned challenges of data sharing, the study in [55] proposed a secure framework with three different categories of participants: data owners, miners, and third parties, wherein data is transferred through blockchain, which authorizes various participants using blockchain and guarantees data security. The primary objective of this research is to provide data sharing in multiple clouds incorporating incentive schemes. The proposed model employs Shapley value to create a fair incentive arrangement for data sharing, and the revenue distribution is performed through verification and analysis. The study results would motivate more collaborative effort in data contribution, improvement in data authenticity at an optimized level. The study by [56] proposed an incentive model using blockchain-based data sharing in IoT systems using an evolutionary game theory approach. The main objective of the evolutionary game theory using the incentive model was to dynamically adjust the incentive or participation cost facilitating active user participation in data sharing. It is mentioned in the study that When the number of users engaging in data exchange tends to decline, the involvement of users is likely to be lower in the lack of an incentive adjustment system, ultimately leading to the downfall of the data-sharing network. The implementation suggests incentive adjustment mechanism enhances the participation of distributed users by offering incentives, maintains the scalability of the sharing system, ensuring the balance between the user participation level of the data sharing network and the network maintenance cost. The study in [7] discussed another application of blockchain-based platform for sharing user profile data, enabling users to keep control over the sharing and receiving of rewards, was suggested. The main contribution of this proposed model is based on user-defined privacy and data sharing regulations that are encapsulated in smart contracts. Additionally, it facilitates establishing financial incentives for users to provide their personal data (micro-payments or credits). The sharing of user profile data in a distributed fashion is implemented using MultiChain. This has been done by performing experiments on various travel booking domain that allows users to receive rewards while sharing their profile data with other travel industries based on their privacy preferences mentioned in smart contracts.

Data sharing propels the active development of data-driven services and progresses society proficiency. However, data owners may refuse to share their information with other organizations because the data holders are apprehensive about increasing competitors’ competitiveness. By processing the shared data, competitors can improve the quality of their services; hence, the data holders’ business is reduced due to the loss of data. During data sharing, data is exposed without maintaining the privacy of the individuals, hence leading to enormous privacy security risks. As a result, the increased privacy-related risks will impede data sharing. Therefore, we are in need of privacy-preserving techniques to strengthen the data sharing models. To motivate data sharing for data holders, the work in [57] proposed a competitiveness-driven and secure incentive mechanism. The proposed research is based on a data competitiveness model, where the data holders share data with demanders and earn data competitiveness from data demanders by eliminating the competitiveness worry, inducing win-win results for data holders and the demander. The experimental results show privacy is protected using differential privacy, a theoretical contract procedure to formulate the incentive mechanism. Designing an optimal contract helps the data demanders to make the finest decisions and data holders to enhance their utilities. In [58], the authors proposed an incentive mechanism using a two-level Stackelberg game for data sharing. The experiment carried out shows the proposed techniques consist of several leaders and one or more followers. Based on the behaviors of the participants, the proposed Stackelberg game was split into two levels: a data demand network-level game and a data-sharing network level game.

The study in [59] proposed a sustainable incentive scheme for an FL based framework. It is known that in FL, a collective ML model is trained by a federation by implementing privacy preservation technologies. But the participating FL members may have to incur some costs for their contribution in the FL model. Due to the time required in the training and commercialization of the model, the federation experiences delay in paying back to the participants which generates gap between the contributions and the unaccounted rewards in the pay-off sharing schemes. The FL incentivize (FLI) plays a significant role in eliminating such challenges. The budget is dynamically divided, following the context aware technique between the owners of data in a federation. The collective utility is maximized jointly and on the contrary the inequality is minimized while receiving the payoff and its required waiting time. It is further compared with five latest payoff sharing schemes and the results conclude the ability of FLI in attracting high-quality data owners thereby achieving the highest revenue for the federation.

The study in [60] proposed the development of a dynamic digital twin in association with FL along with its incentives for air-ground networks. The air-ground network in a traditional framework enables users to get a continuous connection and real-time services. But it has associated challenges relevant to resource utilization. Hence the FL-based air-ground networks is used in this work. The FL model helps the clients to train models without getting shared, ensuring privacy and security. Fig. 3 depicts the importance of FL for privacy preservation for incentive mechanisms in IoT. Digital twin provides a virtual depiction of the air-ground networks reflecting its status at different time variations. This combines with the FL approach ensuring privacy protection and training of data in the air-ground networks. In the digital twin and FL-based air-ground network, a drone is used as the aggregator, and the clients on the ground help in training the model using network dynamics caught by the digital twins. As an example, in the Stackelberg game, the digital twin in the drone sets preferences for the clients and the clients act as followers that enable choosing of the global training rounds. A dynamic incentive scheme is also designed that adjusts the optimal client selection process and the relevant participant levels. The results reveal and justify the accuracy and efficiency of the proposed incentive scheme.

The study in [50] uses a joint optimization technique for combining reputation and contract theory wherein reputation is used as a metric for measuring the reliability of mobile devices. The majority of the existing works have contributed towards designing various learning algorithms to enhance learning performance. The issues relevant to incentive mechanisms in the process of training and worker selection are yet to be confronted, which have hampered the widespread usage of FL. Thus the reputation metric is introduced as part of a reputation-based worker selection framework wherein a multi-weight subjective model is implemented. Blockchain is also included to ensure reputation management. Experimental findings show an incentive mechanism is also implemented, which combines the reputation metrics with contract theory. This enables the high-reputation mobile devices and their data to participate in the learning process of the model. The results highlight the efficiency and accuracy of the proposed model.

In FL systems, the data owners retain their raw data and share only the results generated by local computations for the training of the global model and its owner. The data owners, in such cases, experience privacy issues. To eliminate such issues, the study in [61] proposes an incentive scheme developing a differentially private federated learning network (DPFL). This framework prevents privacy leakage issues and also models the computation, communication, and privacy costs of the data owners, which are considered as private information. This information remains unknown to the model owner, and the 3D contract approach helps significantly in designing the incentive scheme. The simulation results justify the superiority of the proposed approach in terms of its efficiency when compared with other basic approaches. The predominant usage of e-healthcare systems leads to the generation of the huge amount of healthcare data by IoT devices. These health data have great importance when aggregated with the various distributed devices. But such aggregations have associated security, privacy and confidentiality issues. These issues crop up from differential attacks and patient denial to contribute to healthcare data aggregation. The study in [62] proposes a health data aggregation scheme that enables the secure collection of health data from varied resources and also ensures fair incentives for the contributing patients. Signature techniques are employed to disseminate fair incentives for the patients. Noises are added to the data to achieve differential privacy. Also, the combination of Boneh–Goh–Nissim cryptosystem and Shamir's secret sharing scheme is implemented to achieve the optimum level of fault tolerance and security. The system successfully achieves security, privacy, fault tolerance and also retains fair incentives for the patients ensuring cost efficiency in computation, communication and storage overhead. The study in [63] proposed an incentive-based framework for scheduling transmissions in electronic health (e-health) network systems wherein the delay-sensitive packets are emphasized. The primary emphasis is given on the beyond wireless body area network (WBAN) communications wherein the medical packets arrive at a random fashion to the gateway and the transmission requests are sent to the network regulator located at the base station, which have delay sensitivities reflecting the severity of the medical signals. The base stations

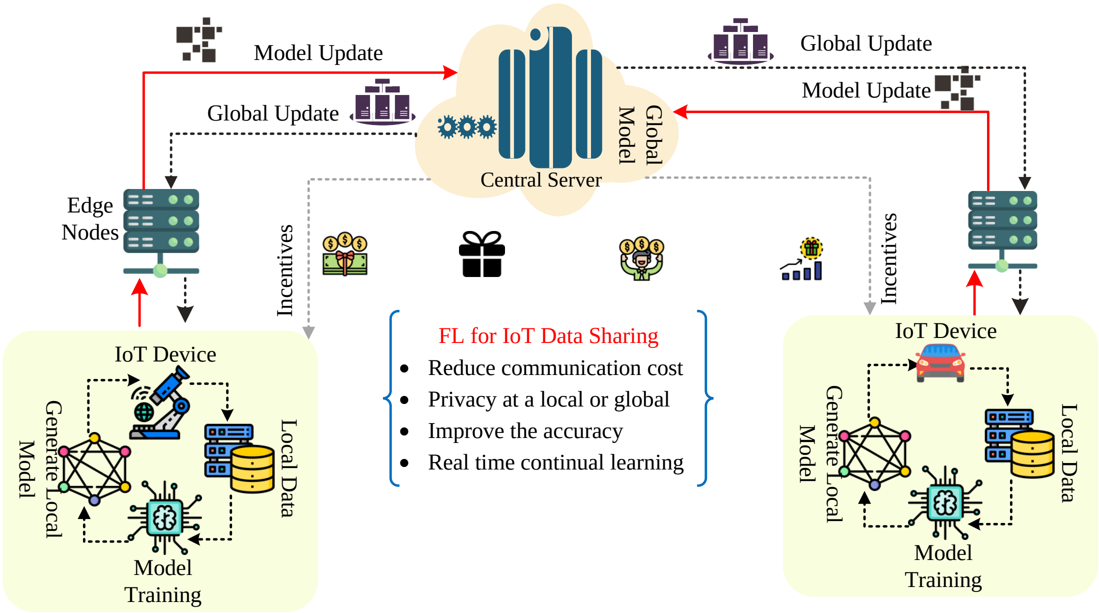

Fig. 3. Federated learning for privacy preservation for incentive mechanism in IoT.

thereby decide on the order of transmission, creating a priority queue. The packet utilities and the profit function points of the base stations are computed. An incentive-based system is thus developed considering the features of the service station such that all the gateways report the actual information pertinent to delay sensitivities of their packets. The proposed system helps in maximizing the profit of the base station, minimizes waiting cost ensuring optimal service prioritization for the emerging medical packets. The results highlight the economic benefit of the proposed incentive-based system.

B. *Incentives for IoT Data Offloading and Caching*

The IoT enables connecting a wide range of intelligent devices over the Internet to transmit and exchange data. Over time, the everyday technology innovations we experience will make these devices increasingly important for how we consume the Internet. IoT devices generate an incredible amount of data, which is then transmitted to the cloud for processing [64], [65]. The most significant challenge in IoT is moving large quantities of data over time to a remote location. As the demand for the data increases, the users who utilize less data should benefit. In this section, recent works on incentives for offloading and caching are discussed.

Data offloading is a technique for sending data from primary links to a terminal-to-terminal (T2T) network that relies on direct communication between mobile users without the need for additional infrastructure. However, to avoid congestion and overload, network operators must increase the capacity of cellular networks, which will result in a significant loss for mobile service providers. With the help of the Vickrey-Clarke-Groves (VCG) mechanism and Rubinstein bargaining game model, an incentive scheme is presented in [66] to control the traffic. According to the results of the experiment, the incentive technique assisted in reducing congestion and improving the QoS in mobile network systems. Additionally, it had a beneficial effect on the revenue of mobile network operators (MNOs), access point owners (APOs), and Internet of Things modules (IoTMs). If the dynamics of time-varying topology and node mobility are not taken into account, this approach may result in data loss and delay.

Due to the rapid increase in mobile traffic, IoT necessitates a large number of access points (APs) to provide data offloading capabilities. As they are self-centered, most APs refuse to participate. To address this issue, the work in [67] considered a behavioral economics-based incentive mechanism motivated by a life phenomenon known as the anchoring effect and loss aversion on offloading (AELAO). The authors added the anchoring effect and loss aversion from behavioral economics into the incentive mechanism and established the reference factor, price-break discounts factor, and regret value to incentivize the APs to participate in repeated data offloading within the time constraint. The findings revealed that because of the incentive mechanism, APs participated more actively. AELAO increases the utility of APs by incorporating the additional reward, but it increases the cost of data offloading requester.

Edge computing has proven to be a successful method for offloading IoT data. IoT devices send massive amounts of data to the network's edge, causing a single edge device to become overburdened. The authors in [68] used multiple edge device resources to reduce straggler effects and improve performance. However, these devices may not have enough bandwidth to transmit data from IoT devices. To address this issue, a deep-learning-based auction mechanism to buy and use bandwidth from service providers for edge devices is proposed in this work. In another work [69], RL is used for privacy in incentive mechanisms, where the results proved that the proposed method maximizes the profit for service providers while satisfying both individual rationality and incentive compatibility properties.

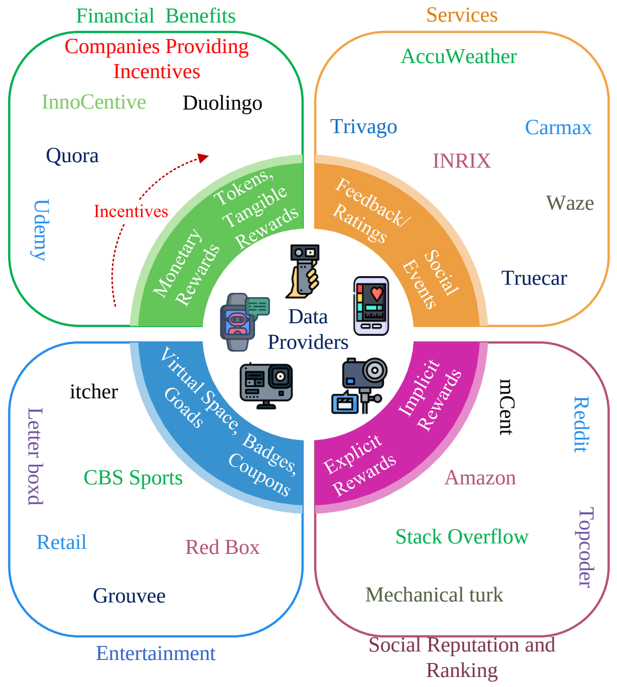

Fig. 4. Different categories of incentive mechanisms in MCS.

C. Incentives for IoT Mobile Crowdsensing

The advancements in communication technologies (4G/5G) and mobile phones in recent years have enabled the emergence of high capacity and efficient networks that allow billions of smartphones connecting with each other. The sensing capabilities of mobile phones are enhanced by integrating them with several IoT sensing devices such as a microphone, gyroscope, camera, accelerometer, GPS, etc., along with their storage and processing capabilities. This evolution of mobile phones has led to the emergence of MCS. MCS is based on the sensors of the mobile devices through which the geospatial data and knowledge can be acquired, which can be shared with other users in the community. Due to smart cities and rapid urbanization, several innovative applications and research areas are being opened up by MCS that can offer the best environment to the citizens that may lead to the growth in the economy. The local data acquired through the sensors of the mobile phones enable sharing of the knowledge regarding traffic conditions, local information, noise level, road conditions, etc. Useful insights can be uncovered by the application of big data analytics, ML algorithms can be applied on the shared acquired data which can be used for smart urban space monitoring that can have a huge impact on the society [70], [71]. MCS helps the organizations to acquire large quantities of data without the need for them to spend huge capital on infrastructure and other resources. Fig. 4 depicts the different categories of incentive mechanisms in MCS.

To acquire a large quantity of data, MCS applications need participation from humans voluntarily. However crowd sensing consumes the resources such as computing power, battery, cost the users their mobile tariffs, etc. Moreover, private information like the location of the volunteers has to be shared that can expose the volunteers to different kinds of security threats [72]. So, unless the volunteers are incentivised, they may not be interested to participate in the MCS as they have to risk the privacy breaches and consumption of several resources of their mobile phones [5]. Different kinds of strategies can be followed to incentivise and attract volunteers to participate in MCS. Some of these strategies are financial rewards, social recognition, ranking and recognition, entertainment-based incentives, etc. [73]–[75]. The work in [76] proposed an approach in which socially connected and popular users among peers are recruited as participants in the MCS. It is assumed that the mobile users who are more active and connected in social media can attract/motivate their connections to participate in the applications [77], [78]. For example, when an active social networking user shares the data of their fitness achievements collected through wearable devices in social media, it can motivate their followers/fiends to use the same application, thus maximizing the profits of the organizations who developed such applications.

Several researchers have proposed interesting approaches to incentivize the participants in the MCS, as discussed below:

- **Incentive Mechanisms for Social Reputation and Ranking:** In this mechanism, the volunteers in a community will be awarded points every time they share the data collected through their smart phones like images of points of interest, pot holes, road conditions, food/catalogues in restaurants, etc. Periodically, the volunteers with the highest points will be declared as the winner and their details will be shared in the community. The winners can be rewarded with souvenirs [79].
- **Incentive Mechanisms based on Services:** A participant in some MCS can act both as a consumer and contributor i.e., a participant gets services and also provides services. For instance, if a participant rates a hotel, he receives a rating for another item, or if a participant sends data related to traffic, he might receive information regarding traffic on alternate routes [71].
- **Incentive Mechanisms based on Financial Benefits:** In this strategy, the participants in MCS can be rewarded by providing them with monetary benefits. This strategy is one of the effective means to get quality data from the participants [80].
- **Incentive Mechanisms based on Entertainment:** In this strategy, the participants can be incentivized by providing some entertainment as a reward for participating in MCS. For example, the participants can be given access to play a game, or they can be given movie tickets, etc [81].

To collect high-quality of sensing data within the specified budget, it is essential to choose optimal users/volunteers for MCS. The accuracy of the sensing data depends on the coverage of mobile users in the target area and also on the previous reputation of the mobile users [82], [83]. The work in [84] considered these factors for incentivizing the participants using Stackelberg game theory. In this work, the authors proposed to use a two-stage Stackelberg gaming approach to determine the levels of sensing of mobile users, who are chosen based on their previous reputation and coverage areas. Expectation-maximization algorithm is used in this work to determine the reward/incentive to the mobile users participating in the MCS. Once the sensing data is uploaded by the MUs, the expectation-maximization algorithm evaluates the quality of the data, the reputation of the mobile users is evaluated by the server center based on the quality of the data updated by the mobile users and then the historical reputation of each mobile user is updated. Based on the tasks completed as per the optimal strategy selected, the mobile users will be rewarded. The results obtained proved that the mean square deviation of bandwidth payoff and energy payoff increase with the total reward. Also, the total utility obtained by MUs increases with increase in rewards of the task. The average bandwidth chosen by MUs is less than 2.5 when the total reward is lesser than 1000, whereas the total rewards is greater than 3000 when the average bandwidth selected by the MUs is greater than 4. Similarly, the study in [85] formulated the interactions between MUs and SPs as a multi-stage Stackelberg game in which SP is considered as a lead player and MUs are considered as followers. Based on the unit prices that are announced by the MUs, the SP will be calculating the amount of sensing time for purchasing from every MU through convex problem-solving. Later, every follower observes the records of trading and adjusts the pricing strategy iteratively based on a trail and error method that is based on a multi-agent DRL algorithm. The results obtained show that, in the absence of prior knowledge regarding the quality of data from the MUs, a near-optimal performance is achieved by the proposed model. Also, a sellers market is resulted in intensive competitive environment among the buyers when the average time budget of MUs is less.

The work in [11] proposed an incentive-aware recruitment scheme for vehicles based on edge-assisted MCS. In this work, the authors have designed an incentive mechanism to enable cooperation between the intelligent vehicles and the edge server. The pricing process between the participating candidate and the edge server is modeled as a 2-users cooperative game. Later Nash bargaining theory is applied to reach decision on the best possible incentives to be paid by the edge server to the participant through based on cooperation between edge and the vehicles. To find the level of contribution from the vehicles, a scheme based on the priority of regions of vehicles, the vehicular reputation, and the spatio-temporal availability of the vehicles, is designed, which is NP-hard. To address the NP-hardness of the recruitment problem, a heuristic algorithm is proposed by the authors. The results obtained prove that minimum cost vehicles are selected by the proposed scheme and also many vehicles are selected within the allocated budget for compensating the total value of the users with the increase in candidate vehicles. The proposed scheme outperforms other schemes, proving that it is very important to consider the reputation and spatiotemporal availability of the vehicles along with the budget of the edge server in selecting the participants.

Another interesting work in [86] proposed a non-cooperative vehicular crowdsensing scheme in which the incentives are issued to the vehicles based on the social network effect and the tasks that are priced dynamically. The authors also have proposed an incentive mechanism that is socially aware through DRL that maximizes the overall utility of the drivers of vehicles and also for deriving long term strategy of sensing for the vehicles. The proposed scheme achieved an average utility of vehicles as 0.91 that is 0.43, 0.69, 0.86 higher than that of Q-learning algorithm, greedy algorithm and random algorithm when number of vehicles is 10. Also the average utility of all vehicles for the proposed scheme is 90% higher than that of Q-learning algorithm. when task payoff is 23.

An incentive approach is proposed in [87] for MCS by considering the resource demand of the MUs as the economical model. Based on the idea that different MUs will be participating in the MCS at different levels as they have different behaviors, the authors have formulated an incentive approach by using a popular game theory, Stackelberg. They have also investigated an incentive mechanism which is dynamic by using DRL that preserves the privacy of the MUs. Through this approach, the SP can learn about the strategy for optimal pricing from the game experience directly. In this work, the Stackelberg game is formulated into two stages based on the interaction between the MUs and SP. In the first stage, the pricing policy of the SP, which is the leader of the game, is determined and broadcasted. In the next stage, the sensing efforts of MUs, which are followers, are computed based on the SP's price offer on the MUs' constraints on resources and uncertainties of the demands. To compute the Stackelberg Equilibrium of the MCS game, the private data of the MUs has to be known by the SP, that is impractical in several situations. To preserve the privacy of the MUs, a DRL algorithm is employed in this work, through which the optimal pricing strategy is learnt by the sensing platform through the past records from the game. The proposed scheme has achieved a maximal standard deviation of 0.005, which proves that the proposed scheme is very stable and offers fair price to the MUs.

Most of the researchers focus only on one optimization goal when recruiting and incentivizing the participants in the MCS. However, there are some tasks for which there might be multiple optimization goals. For instance, consider the scenario where photographs have to be taken for a landmark. In this case, the requester of the task might have two optimization goals; one goal is the correctness of the collected photographs of the landmark and the other one is diverse views of the landmark. To address the aforementioned issue of two optimization goals,the study in [88] proposed a novel incentive framework, namely, BiCrowd. The proposed model is proved to possess the properties that are desired such as individual rationality, constant competitiveness, budget feasibility, truthfulness, and computational efficiency. Bicrowd considers selecting workers for the MCS by optimizing spatial diversity and also the reliability of the sensing tasks. In the proposed system, if a worker is selected for a task, the payment for the worker has to be determined by the platform. The service requester will rate the task performed by the worker based on the quality of the data provided by the worker. The worker's reliability is then updated by the platform based on the rating given by the requester. In this work, the authors assume that the workers are game-theoretic. Hence, to maximize the payments received, the bidding prices may be manipulated. The performance evaluation revealed that the proposed method has outperformed other considered schemes with respect to the average completion reliability budget

D. Incentives for IoT Privacy and Security

With the recent development of communication, the data collected from distributed IoT devices is growing in an explosive way. Guaranteeing fair rewards for IoT users is a critical task. For instance, the IoT users may share/contribute their data for benefits, however, the dishonest one can "re-contribute" the same data for more rewards. At the same time, the IoT users' may expose themselves to privacy threats as their data contain personal information (e.g., identity, location) [89], and hence it should be well protected [90]. In such context, data aggregation and incentive mechanisms have attracted numerous researchers' attention from both industry and academia [91]. However, IoT users' data aggregation can leak user information like location, activity, etc. due to system malfunctioning. For example, if users' locations are leaked, it will make them vulnerable especially if their locations are frequent. Although data aggregation and incentive mechanisms are accompanied by security threats and privacy concerns, the majority of incentive mechanisms consider the truthfulness of the mechanisms. Hence privacy and security issues are mostly ignored in incentive mechanisms that can reduce the enthusiasm of IoT users [92], [93]. That is why privacy and security have become hot issues in data aggregation. It has been used in several fields such as healthcare [62], [94], smart grid [95], crowdsourcing [96]. Data security and privacy approaches aim to securely transfer and store the IoT users' data and make them unlearn from unauthorized entities. In this section, we present the different proposed mechanisms based on security and privacy protection using blockchain, AI, and game theory in IoT systems.

Blockchain technology has been integrated these days to eliminate security threats and ensure user's privacy in IoT applications [35], [97]. With blockchain, there is no central authority nor storage server, hence trust of each node is built by reputation. Also, its anonymous features allow the workers to do tasks without disclosing their real identity [98]. Even though blockchain-based IoT systems have myriad features such as attack resistance and avoiding third-party risks, they are face certain challenges in maintaining data privacy and security without risking its leakage. To address these challenges, several researchers are focusing on integrating several privacy-preservation approaches with blockchain. These approaches are *anonymization*, *encryption*, *differential privacy*, and *smart contract* as shown in Fig. 5.

1) Anonymity-based Privacy Preservation: Given the several security and privacy concerns, an absence of anonymity technique makes the IoT users hesitate to participate [99] in incentive mechanisms. Anonymity-based privacy preservation avoids information leaking by removing the personal identifiable information and the k-anonymity technique is one of the most widely used anonymity mechanisms.

According to [100], k-anonymity is defined as *a privacy-preserving participatory sensing scheme that satisfies k-anonymity against the service provider if, for any sensing record reported to the service provider, the service provider cannot distinguish the generator of the record from a group of at least k participants.* In this context, The work in [92] proposed a privacy-preserving incentive mechanism based on the blockchain to ensure privacy provisioning in crowdsensing. Specifically, the sensing data qualities are evaluated via the expectation-maximization algorithm. Then, the k-anonymity approach is used to protect user privacy where the users' sensing data are integrated into a group data, then the server pays the group, and the group distributes the payment for every group member. The study presents a theoretical analysis and simulation results demonstrating the efficacy of the system to deal with the impersonation attacks in the open and transparent blockchain.

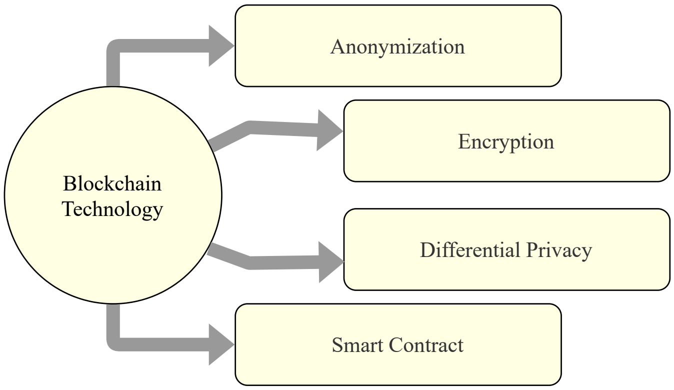

Fig. 5. Privacy-preservation in blockchain-based IoT systems.

A novel privacy-preserving incentive announcement network based on blockchain and anonymity is proposed in [101] for communications for the Internet of vehicles, called *CreditCoin*. It achieves anonymity and reliability simultaneously without leaking private information by using ring signatures anonymized announcements. Also, CreditCoin motivates users/vehicles with incentives to share traffic information by gaining reputation points. The obtained results show that the total time of announcements for a user only is 174ms in assumptions, which is much more efficient than other protocols. However, the anonymization process usually happens on the servers of the companies that collect the IoT users' data, thereby the IoT users have to trust them, which means that it is not enough to protect the privacy.

2) Encryption-based Privacy Preservation: To improve data security, encryption-based privacy preservation has been used in blockchain-based systems. It is one of the widely used mechanisms for secure data transmission. Each blockchain user receives two types of keys, which are public and private.

To ensure secure service provisioning in IoT,the work in [35] proposed a consortium blockchain-based secure provisioning scheme for LCs. In the proposed scheme, the LCs send requests to the SPs through blockchain. To do so, consortium blockchain with the Proof of Authority (PoA) consensus mechanism is used. Also, the Advanced Encryption Standard (AES) 128 encryption technique is used to encrypt the service codes before sending them to LCs. The AES128 is used because it has less execution time as compared to other encryption techniques like SHA256 and RIPEMD160. The blockchain is used here as an underlying security fabric in the service provisioning systems. Finally, the authors have evaluated the efficiency of the proposed scheme by comparing four encryption algorithms in terms of execution time. The evaluation results show that using PoA, the total gas consumption is reduced 17% as compared to Proof of Work as well as the reputation of the SP increases, its participation rate also increases.

Similarly,the study in [102] proposed a blockchain-based secure data sharing for vehicular networks. To motivate the nodes for contribution and ensure their privacy, an incentive model has been proposed and all the communications were done in an encrypted manner using the AES128 technique. Using AES128 made the retrieval of the original data from the ciphertext quite impossible for the intrusion node. In addition, to reduce the gas consumption of the proposed system, the authors used a consensus mechanism based on Proof-of-Authority (PoA). The results of AES128 is better than AES256 in terms of average execution time.

Although encryption-based techniques ensure data confidentiality, it is computationally expensive, where the users should save the set of encryption keys.

3) Differential-based Privacy Preservation: Differential-based privacy techniques can solve the above issues and efficiently protect data privacy [103]. Differential-based privacy techniques (DP) based on data distortion was proposed by Dwork [104] in 2006. The privacy parameter ϵ quantifies the difference, and lower ϵ is more private.

To securely aggregate data and guarantee rewards for patients for lightweight e-Healthcare IoT devices,the work in [62] proposed a privacy protection strategy using a DP mechanism and provide rewards to the data owners (i.e., patients). The authors applied DP to support data confidentiality during data transmission and guarantee data privacy (e.g., identities, location). In more detail, the patients sign their private data with a secret key, then the healthcare centers add noises to the collected patients' data and encrypt the perturbed data. Then, the ciphertext is transmitted to the cloud to aggregate the ciphertext, decrypts the aggregated ciphertext, and sends back the result to the data user requests. The results demonstrate that the proposed system ensures patients' data privacy, low communication overhead, and storage requirement.

Another work in [105] proposed an incentive privacy-enhanced mechanism by combining FL, DP, and blockchain in IoT environments. Unlike the other work in [106], that was executed in the clients/devices side, the authors have used DP noise on the extracted features with CNN local model instead of the original data. Then, these features are used as input for fully connected layers for classification tasks in the MEC server. The experiment results demonstrate that the proposed mechanism achieves high accuracy and protects both the model and the clients' data. Moreover, the results show that integrating FL into the consensus process of blockchain, not only improves the utilization of computing resources but also increases the efficiency of the data-sharing scheme. Although this technique has been successfully used to protect user privacy, it can lead to losing performance [107]. Due to the privacy and accuracy trade-off in IoT systems, utilizing differential privacy is a challenging task. The value of the noise addition parameter "ϵ" represents the level of data protection and by varying this parameter, the users can control the level of privacy depending on their needs.

4) Smart Contract-based Privacy Preservation: Smart contracts (SC) are programmable code stored inside of a blockchain that will be executed when certain conditions are met [108]. SC plays the role of an intermediary between contract members and hence replaces the trusted third parties. This helps to reduce the cost and risk as well as making the execution of the statement automatically whenever the SC condition is satisfied. As a result, several researchers have combined SC and blockchain to incentivize the workers who participate in order to improve the security and effectiveness of IoT systems. A contract theory-based incentive mechanism is proposed in [50] to avoid the information asymmetry issues in the FL system. In the proposed approach, each worker has direct reputation opinions generated from past interactions with the FL server and indirect reputation opinions from other FL servers (i.e., task publishers). Before the training task, the workers choose a contract that corresponds to its computation resource and data quality. Then, the FL server selects the workers that have reputations larger than a threshold which is securely stored in blockchain. The results reveal that with the help of SC, the system attracts the workers with high-quality private data and the malicious workers can not participate in the FL task because they will not choose to sign the contract. Also, it maximizes the utilities of both the task publishers and the workers.

Another interesting work in [109] used the SC to perform secure and self-driven data (traffic load and weather condition) sharing for a blockchain on the Internet of Vehicles environment. The experimental results demonstrate that the proposed system maximizes social welfare, ensures security and scalability, as well as the computing cost of SC, which is suitable for low-power devices.

E. Summary and Discussion

Incentive techniques based on AI, blockchain, and game theory play a significant role in motivating the IoT devices to actively participate in several IoT services such as data sharing, data offloading and caching, mobile crowdsensing, and privacy and security. However, several challenges like dynamic calculation of incentives based on the complexity of the tasks, extracting high quality of data from IoT devices without compromising on the privacy of the users, etc. have to be addressed to realize the full potential of incentive mechanisms for high-quality data collection from IoT devices. The applications of incentive techniques for IoT services are summarized in Tables II and III.

IV. Applications of Incentive Techniques in Vertical IoT Domains

In this section, the applications of incentive techniques in several IoT domains such as smart healthcare, smart transportation, smart city, and smart grid are discussed along with recent state of the art.

TABLE II
SUMMARY OF APPLICATIONS OF INCENTIVE TECHNIQUES FOR IOT SERVICES.

IoT Service	Ref.	Incentive Mechanism	Contributions	Limitations and Challenges
IoT Data Sharing	[55]	Shapley value	Increase the number of collaborations that provide useful data and enhance data validity. Shapley value is used to provide a dynamic and fair incentive system for data sharing.	The dynamic incentive distribution based on Shapley value did not offer sufficient evaluation and investigation.
	[56]	Evolutionary game theory	The primary goal of evolutionary game theory with an incentive model is to constantly modify the incentive price in order to increase user involvement in sharing data.	The proposed study does not account for the large number of users who participate in data sharing, large data sizes.
	[59]	FL Incentivization	Proposed a sustainable incentive scheme for an FL based framework. The budget is dynamically divided, following the context aware technique between the owners of data in a federation.	The authors were unable to focus on the issue of estimating the costs incurred by data owners.
	[60]	Stackelberg game	Proposed the development of a Dynamic Digital Twin in association with FL along with its incentives for air-ground networks.	The authors failed to show the global and local updates in which customers chose to participate in the static and dynamic cases.
	[50]	Contract theory	Uses a joint optimization technique for combining reputation and contract theory wherein reputation is used as a metric for measuring the reliability of mobile devices.	The authors were unable to demonstrate optimised reputation calculation accuracy because they used fewer weight parameters, which degraded the reputation analysis.
	[61]	3-D contract-based approach	Proposed an incentive scheme developing a differential private DPFL to prevent privacy leakage issues and also models the computation, communication and privacy costs of the data owners which are considered as private information.	It is difficult for the model owners to extract data owner specific data and construct the proper contract.
Mobile Crowdsensing	[84]	Stackelberg game	A two-stage Stackelberg gaming approach is proposed to determine the incentive mechanism based on levels of sensing of mobile users, who are chosen based on their previous reputation and coverage areas.	The proposed work work does not consider the selection of users when multiple tasks are released.
	[85]	Multi-stage Stackelberg game	Interactions between MUs and SPs are formulated as a multi-stage Stackelberg game in which SP is considered as a lead player and MUs are considered as followers. Multi-agent DRL algorithm is used for designing incentive mechanism.	Single point of failure of the SP will affect the entire crowdsensing process.
	[11]	2-users cooperative game	An incentive mechanism is designed to enable cooperation between the intelligent vehicles, and the edge server. The pricing process between the participating candidate and the edge server is modeled as a 2-users cooperative game.	The proposed work is validated using simulations, but not on a testbed.
	[86]	DRL	Incentives are issued to the vehicles based on the social network effect and the tasks that are priced dynamically.	Hyperparameter tuning is not done for the DRL model.
	[87]	Stackelberg game	An incentive approach for MCS is formulated by using Stackelberg game and by considering the resource demand of the MUs as the economical model. Through this approach the SP can learn about the strategy for optimal pricing from the game experience directly.	The proposed approach requires large number of interactions between Mus and SP that may increase the time complexity to find the optimal price.
	[88]	Game theory	The service requester rates the task performed by the worker based on the quality of the data provided by the worker. The worker's reliability is then updated by the platform based on the rating given by the requester.	The proposed work is validated using simulations, but not on a testbed.

A. Smart Healthcare

In the Internet of medical things (IoMT) systems, mobile devices are usually connected with fog and cloud servers to upload and store electronic health records and other medical information for diagnosis and treatments, and they lack an effective incentive mechanism to collect and share sensitive health and medical data between authorized parties in a secure and private manner [110]–[113]. Indeed, activating collaborative health data sharing between hospitals over different data storage infrastructures can enable third parties to take advantage of big data and AI to provide precise medical and healthcare diagnoses. In [114], an effective data sharing model was proposed for cloud-based healthcare systems, in which the blockchain technology with a smart contract was embedded to ensure high privacy and security during data transmission and storage. Remarkably, a dynamic incentive mechanism was developed to encourage the participants to share authentic and reliable data over multiple cloud platforms, in which the revenue distribution fairness is examined and scored using the Shapley metric [115]. Regarding the use case scenario of health data sharing, a patient collects the examination data from the hospital and sends it to the diagnosis center. Subsequently, the patient will receive the correct diagnosis report if and only if the fee paid by the patient is fairly divided to the diagnosis center and the hospital as their revenues.

TABLE III
SUMMARY OF APPLICATIONS OF INCENTIVE TECHNIQUES FOR IOT SERVICES (CONTINUED).

IoT Service	Ref.	Incentive Mechanism	Contributions	Limitations and Challenges
Privacy and Security	[92]	Blockchain-based anonymous	A privacy-preserving incentive mechanism based on the blockchain is proposed for crowdsensing applications. In this work, the authors have proposed to use a cryptocurrency based on blockchain for secure incentive payment mechanism.	High latency.
	[101]	Blockchain	Blockchain based incentive mechanism is proposed to motivate the users in vehicular announcement networks by preserving the privacy of the users through an anonymous vehicular announcement aggregation protocol.	Suffers from limited scalability.
	[35]	Blockchain-based encryption	A consortium blockchain-based AES128 encryption technique for LCs is proposed. A reputation based incentive mechanism is proposed to provide fair incentives for LCs.	An incentive mechanism is provided based only on the reputation values.
	[102]	Blockchain	Blockchain based incentive mechanism is proposed to encourage the edge nodes in vehicular networks for efficient provisioning of services in a secured manner.	When the data size increase, vehicles authentication, and data storing costs increase.
	[62]	Differential Privacy	Signature techniques are used to incentivize and encourage the patients to contribute their healthcare data. Samir's secret sharing and Boneh–Goh–Nissim cryptosystem are used to secure and preserve the privacy of the patients data.	Low security since it assumes that the transmission channel is secure.
	[105]	Blockchain-based differential privacy	Blockchain based differential privacy mechanism is proposed for privacy preservation of the customers who provide sensitive data of their home appliances for training the FL model to obtain the customers feedback on the home appliances. Reputation based incentive mechanism is to incentivize reliable customers.	Optimal balance between local and global epochs is not performed for achieving high accuracy.
	[50]	Blockchain-based smart contract	A blockchain based secured reputation management approach is proposed to preserve the privacy of the highly reputed devices to participate in the training phase of federated learning to extract high quality data.	Very few parameters were considered for calculation of reputation of the participating devices.
	[109]	Blockchain-based smart contract	Quality-driven auction model is used to incentivize the high quality data providers in Internet of vehicles. Consortium blockchain is used in this work to guarantee trust in off-chain as well as on-chain data.	The system depends on the network infrastructure.
IoT Data Offloading and Caching	[66]	VCG mechanism and Rubinstein bargaining model	This game theory-based incentive mechanism contributes significantly to congestion reduction and quality-of-service (QoS) enhancement in mobile network systems.	In the proposed work if the dynamics of time-varying topology and node mobility are not taken into account, this strategy may result in data loss and delay.
	[67]	Behavioral economics-based incentive mechanism	This incentive mechanism promotes the active participation of access points.	its impact on the cost to service provider due to unpredictable behavior of the user.
	[68]	Deep-learning based incentive mechanism	This incentive mechanism helps in effective utilization of the bandwidth and efficient use of edge devices.	Uncertainty in user engagement was not addressed in the proposed work.

In order to motivate participants to share their own medical data instead of acquiring the available data on free access platforms, an information entropy-based incentive mechanism was recommended in [116], in which the rewards for participants are validated by a smart contract in the blockchain. Unlike the other incentive mechanisms that pay the rewards over the data size for contribution, the proposed mechanism rewards the contributors based on the information entropy of medical data. Interestingly, the value of medical data, measured based on the information entropy, can be converted into transaction points for trading between different single parties in a group and inter-groups via smart contract. After the participants record and upload patients medical data, the consensus node broadcasts the data to an authorized network. With over 50% of node verification in the network using proof of work (PoW), the new data is written into the blockchain, and the block information is returned to the data provider. It is worth noting that the provider is responsible for generating a smart contract (including the complete data, signatures, transaction points, and other information) and sending it to the consumer to confirm the payment points. The proposed incentive mechanism promoted more hospitals and medical institutions to contribute high-quality medical data and encouraged sharing activities.

As an effort to reduce the gap of economic discrepancy while curtailing the virus spread in the period of Coronavirus disease (COVID-19) pandemic, a unique incentive mechanism was developed for national medical systems [117], where government and people can receive some benefits with a win-win situation. In order to prevent the information tempering from unauthorized parties, blockchain is applied to ensure the privacy and security of medical data, including COVID test results and other health records. In the proposed mechanism, an incentive token is issued to the individual for a voluntary COVID test or self-quarantine agreement. This allows the government to keep tracking of the person who willingly joints at the beginning stage or suddenly breaks the pre-signed commitment. The incentive token can be used as a direct monetary benefit or can be exchanged for other living supplies from the government, such as a free supply of daily necessities, a reduction of tax and utility fees (electricity and water), and a reduction of housing rent. The information immutability and accessibility can be attained comprehensively using blockchain, which in turn actuates the revival of the national economy as soon as possible.

In many medical and healthcare systems, the affordability and accessibility of patients for approaching medicine prescription are usually unfair to underserved communities. Consequently, abandoned patients who do not have enough budget for expensive prescriptions cannot access high-quality medical services. To address this challenging issue, a prescription management framework, namely BlockPres, was introduced with an innovative incentive mechanism to encourage patients who are willing to join and engage the services to earn rewards [118]. In the BlockPres framework, blockchain is embedded to possibly provide authorization and authentication to healthcare providers and patients for regular and fair participation. Remarkably, an incentive token as a reward is issued for each time of successful prescription payment, and the token can be redeemed for additional health services and other products in the future. When a patient signs in the service via an authority tool, an account associated with a unique address of a crypto wallet is created for authentication and verification. The tokens as rewards are transferred and stored in the crypto wallet (which links to the management systems of different healthcare centers) to next appointment bookings and prescription payments.

B. Smart Transportation

In intelligent transportation systems (ITS), the overflow of non-cooperative vehicle nodes (individual users) can degrade the performance of vehicular ad hoc networks (VANETs) seriously. To overcome this challenge, two advanced game theory models, namely dynamic member public goods game (DMPGG) and dynamic grouping public goods game (DGPGG) [119] were proposed for being suitable with dynamic VANETs conditions. In DMPGG, vehicle nodes as members of a game can be dynamically varied for being adaptive with the real-world scenario of VANETs, while DGPGG is with a greedy neighbor selection scheme to cooperate vehicle nodes more effectively than the conventional random selection scheme. An incentive mechanism was developed to encourage the vehicle nodes to join the game and propagate their own real-time traffic data. Depending on the incentive degree measured as the number of cooperative neighbors in the game, the revenue was paid by the meaningful data circulated in a group. Two models improved the performance of cooperative nodes proportions under high-vehicle density conditions with static and dynamic networks.

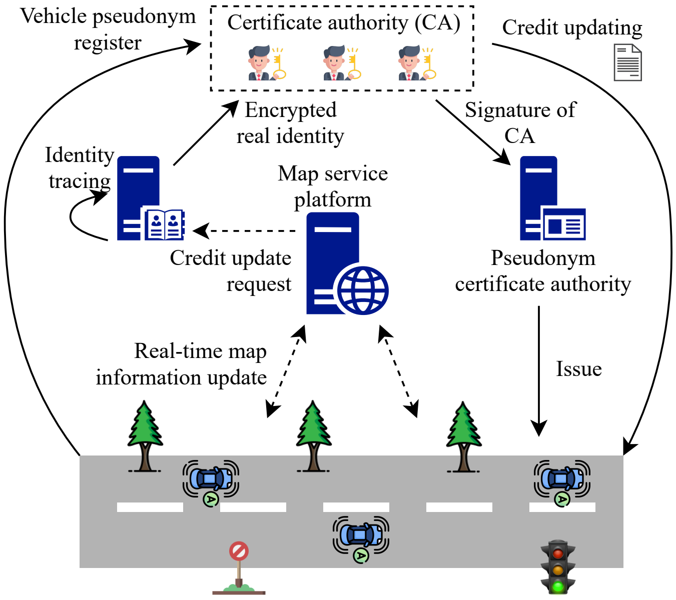
Vehicle pseudonym register
Certificate authority (CA)
Credit updating
Encrypted real identity
Signature of CA
Identity tracing
Map service platform
Credit update request
Pseudonym certificate authority
Real-time map information update
Issue

Fig. 6. System model with the SPIR scheme [121].

Game theory has been leveraged to improve traffic efficiency and reduce accidents in ITS. In [120], the Stackelberg equilibrium game model was combined with a model predictive control in a multivehicle coordinated lane change (MCLC) algorithm to learn the interactive patterns between the lane-changing vehicle and its neighbors in IoV networks. The high-level information about driving styles (i.e., how fast and how long the driver speeds up and slow down) is encouraged to share among vehicle nodes via a fair incentive scheme. As being the rewards, the information received from neighbors can be cooperatively processed by the MCLC algorithm to improve the accuracy of lane-changing detection and estimation. The proposed game theory-based path planning algorithm with the incentive-based extra information not only improved the performance of traffic scheduling in a heavy traffic condition but also encouragingly reduced urban traffic collision.

In VANETs, the resource-constrained vehicles may not be exciting to cooperate for saving energy, memory, and buffer. In this context, an incentive and punishment scheme (IPS) [122] was proposed to motivate the cooperation between vehicle nodes in a network. The VCG game-theoretic model [123] was applied to elect cluster head, auxiliary head, and incentive head for each cluster involving participating vehicle nodes and to examine the weight (as the number of resources possessed by a node) of these heads. Vehicle nodes participating in the election game can increase their incentive (i.e., impression/reputation) via active activities like forwarding data, whereas the nodes exposing selfish behaviors or showing lazy activities will be penalized. Besides, the proposed IPS suggested a positive payment in the form of a reputation for generous nodes and a negative payment in the form of punishment for selfish nodes. Relying on the simulations using VDTNSim, an extension of the opportunistic environment simulator, the proposed IPS achieved high performance in terms of packet delivery ratio, average cost, average delay, and overhead.

Parking availability information management plays an important role in ITS. However, it suffers two critical issues: untrustworthy data and sluggish participation of a few vehicle nodes. In this context, a novel incentive platform, namely TruCentive [124], was designed to utilize the parking data acquired from mobile users in high-density traffic areas. In particular, the TruCentive platform offers hierarchical incentives to encourage mobile users to provide parking information (e.g., time, location, and current status), and the customers are drivers who use that information for seeking a parking slot. The incentive is paid regarding the utility level of contributed data, where the data validation and data utilization confirmation are performed via a game-theoretically formulated protocol. The TruCentive platform has addressed the drawback of existing static and bidding-based dynamic incentive mechanisms while ensuring high practicability and stability.

In the context of how to satisfy the demand for low-latency and high-rate services and applications in 5G-enabled VANETs, edge caching reveals to be a promising solution to optimize resource utilization and offload backhaul. As an effort to encourage vehicle nodes to improve caching efficiency, a game-based incentive mechanism was designed for VANETs [125], in which a small base station (SBS) activates mobile vehicles as participants to store popular contents on their embarked caches and share it to others via vehicle-to-vehicle (V2V) communication. To record the contributions of participating vehicles, SBS can offer rewards regarding caching activities. The content popularity is validated at the centralized global software-defined network (SDN) controller to make caching decisions. For modeling the interaction between the SBS and cache-ready vehicles, a Stackelberg game-theoretic algorithm is applied, in which a non-cooperative sub-game strategy is exploited to address the conflict between cache-ready vehicles. The interaction flow can be described as follows: the SBS at first notifies the amount of data that requests to cache, the cache-ready vehicles then respond to the amount of data that accepts to cache, and finally the caching incentive is estimated correspondingly. With the proposed incentive caching mechanism, the network backhaul traffic was reduced significantly in VANETs.

As a key feature in autonomous vehicles navigation, the real-time high-precision map updates with MCS combining different sensing technologies to reflect dynamic maps effectively and accurately, however, resource-constrained vehicle nodes may not be willing to collect and share their sensing data for updating and maintaining maps without benefit. Moreover, critical concerns about security and privacy should be taken into account in data transmission and storage in vehicles and a data center. In consideration of these problems, a secure and private incentive scheme, namely SPIR [121], was proposed for a reliable real-time map update system as shown in Fig. 6. In general, based on the type of data that the map service platform (MSP) requires, the participating vehicle nodes can collect data properly and bid for it via an auction. The MSP is responsible for deciding the winner according to its budget and user's quotation. Then, the winner has a responsibility to provide data to the MSP. Finally, after the data examination (of quantity and quality) and acceptance of MSP, the revenue will be paid over a secure blockchain-based payment system. Concerning the incentive process, a pseudonym management mechanism is deployed to achieve secrecy and conditional privacy of participating vehicle nodes, which consists of three processing steps: pseudonym registration of vehicle nodes, certificate issuance, and identity tracing with credit updating. The proposed SPIR scheme enhanced the performance of real-time map updating services with high-reliable data while providing a good agreement between MSP and vehicle nodes.

C. *Smart City*

Smart city aims to improve the quality of life of urban citizens by integrating the ICT infrastructure with social and physical infrastructure in cities to provide smart services to the citizens of smart cities such as utilities, transportation, public safety, healthcare, education, administration, etc [126]–[128]. In order to provide these services, citizens, vehicles, IoT devices, etc. can be employed to sense the quality data and provide the same to the administration so that they can take appropriate and timely decisions to improve the quality of life of the urban citizens. To motivate the providers of data to participate in sensing, effective incentives have to be offered to them [129]. Some of the applications where incentive mechanisms can effectively improve the administration of smart cities are, incentivizing citizens, vehicles, hospitals, who provide data related to the condition of the roads, bridges, traffic sharing, potholes, sharing of resources with their peers, and so on, as depicted in Fig. 7. Several state-of-the-art studies on incentivizing the participants in smart city environments are discussed in the rest of the sub-section.

A blockchain-based edge computing system with three layers for incentivizing the nodes participating in the mining process using game theory is proposed in [130]. In the proposed work, computing resources can be purchased by the miners from the edge service providers. The limitations of wireless sensor networks in the smart city due to limited storage and computing resources of sensors can be overcome by the proposed system. To encourage the edge service providers to provide the computational resources and the nodes to participate in mining, the authors proposed an optimal incentive mechanism using a Stackelberg game by exploring the interactions and relations between them. The edge service provider is the leader and the miners are considered as followers in this work. The results obtained proved that the proposed approach has achieved better performance with respect to rewarding the miners compared to state of the art.

One of the essential smart city services is to provide dynamic travel routes and modalities to travelers as part of ITS. ITS can incentivize the travelers to make cognizant choices regarding transport modality and make their trip choices

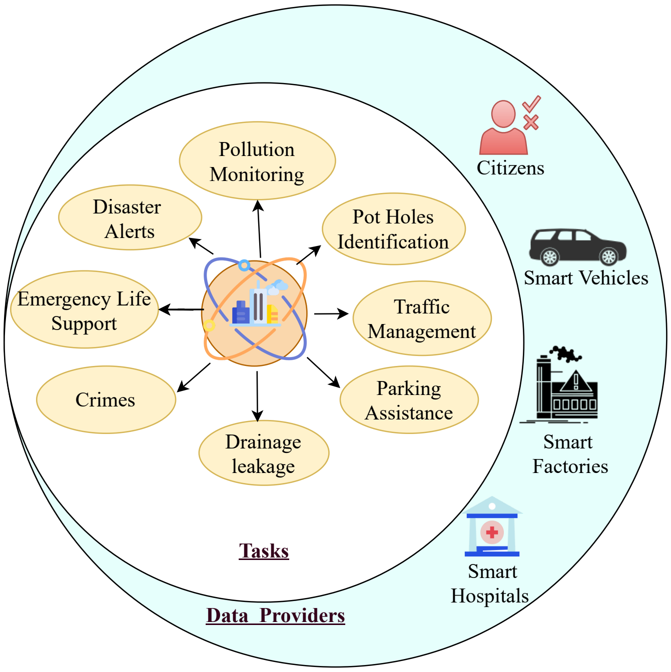

Fig. 7. Incentive mechanisms for smart city applications.

during their daily travel that will help them in achieving sustainable transport goals. Incentive generation in ITS, which supports multidimensional travel goals and is personalized and context-driven, is a challenging task as the travelers will have their own constraints and preferences for modality and route due to dynamic travelling conditions. The generation of personalized incentives should meet multiple travel goals from several travelers that change dynamically. To address this issue, the work in [131] has proposed a rule-based incentive mechanism that uses evolutionary game theory and decision tree for processing the traveling information and generating the personalized incentives intelligently for the travelers. Personal evolution is used in this work for addressing the personal incentives problem. The simulation results proved that the personal evolution approach improved the average utility of the incentive member population.

Crowdsourcing based on vehicles is a powerful mechanism in smart cities through which important tasks can be outsourced to the vehicles by using their resources. A delay-aware incentive mechanism is designed in [132] based on reverse auction to motivate the vehicles to join the crowdsourcing system in a timely manner. The proposed system does not acquire the sensitive trajectory information of the vehicles. The proposed method allows the vehicles to estimate and report their estimated time of completion for the tasks they bid for. Based on costs and the estimated time of completion of sensing tasks by the vehicles participating in the bidding, the crowdsourcing platform identifies the winning bids and payments. The simulation results prove the effectiveness of the proposed incentive mechanism.

Due to the rapid growth of mobile crowdsensing, the sensing tasks in smart city applications are recently outsourced to vehicles or mobile devices. Even though mobile crowdsensing can be used for diverse smart city applications, due to the lack of an efficient incentive methodology, the development of some of the applications of smart cities and IoT, such as IoV, is restricted. As the vehicles are usually reluctant to participate in sensing tasks. In IoV environment, some of the sensing tasks may be arriving suddenly, but due to the lack of resources in a vehicle for sensing tasks, it is required that the multiple vehicles collaborate in sensing tasks. In such cases, task scheduling and incentive mechanisms for collective collaboration of the vehicles are required. To address these issues, the study in [133] proposed a novel model for the collaboration of two vehicles that considers the sudden arrival of sensing tasks. The authors have proposed a bidding mechanism for general sensing tasks to encourage the vehicles to give their resources, and accordingly the scheduling of tasks will be done for those vehicles. The authors have proposed a novel method based on time-window for sudden sensing tasks for incentivizing and managing the tasks among the vehicles. A blockchain-based framework is developed for the proposed models in IoV to secure the exchange of information with the help of smart contracts. The results obtained proved the superiority of the proposed approach where emergent tasks are given better incentives when compared to general tasks.

D. Smart Grid

Smart grids play a significant role in providing electricity in a smart manner to households and industry through electricity grids. Through smart grid, automatic fault detection in the electric lanes, load optimization, detection of electricity thefts, etc., will be easier. IoT is a key enabler in smart grids [134]. Incentive mechanisms can play a vital role in several operations of smart grid-like voluntary shedding of loads by the consumers, excess energy sharing, energy trading, encouraging the electricity providers to use renewable energy, etc., as depicted in Fig. 8.

Demand response (DR) is a mechanism in which the consumers can play an important role in the operation of a smart grid by shifting or reducing their power consumption during peak hours. The electricity operators and electric system planners are using DR to balance the demand and supply of the electricity, which can help in the reduction of the electricity cost in the wholesale markets, which results in lowering of retail rates [135]. To encourage the customers to participate in the DR by proactively shedding the load of their appliances during peak time, the utilities have to provide incentives to them [136]. Several researchers have proposed interesting works to incentivize the consumers who participate in DR. The authors in [137] proposed an approach for incentivizing the consumers, in which the DR problem is formulated a Stackelberg game. In the proposed approach, the leader in the utility company and the customers are treated as followers of the leader. To maximize the weighted summation of peak-to-average ratio and weighted summation of the revenue, the utility will define a price. The authors formulated the competition between the customers as a non-cooperative sub-game with respect to the rate of power transmission. The simulation results proved that the proposed real-time pricing incentive

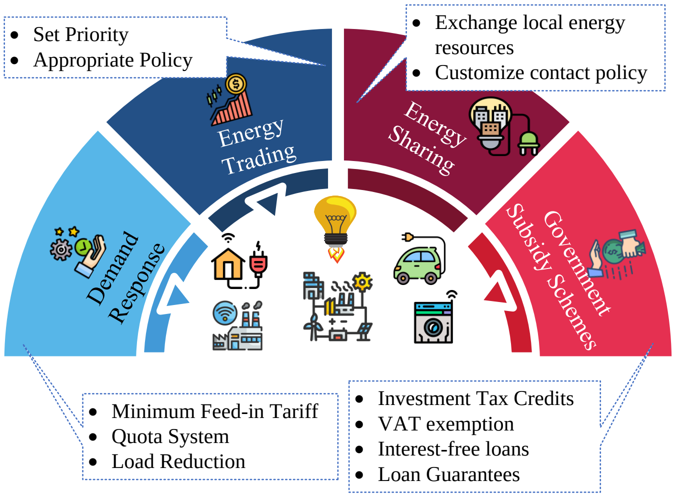

Fig. 8. Incentive mechanisms for smart grid.

scheme can reduce the daily costs by 37%. A similar work in [138] considered a real-time pricing policy for electricity for calculating the incentives with respect to reduced cost and electricity price. The authors have developed a technique based on backtracking to develop a mathematical model for calculating the load consumed and shifted in a particular time slot, through which the price of the electricity is calculated for all categories of users for estimating the incentives based on the profile of load shifting. The load is shifted to other time slots to keep the load under the upper limit that helps in accommodating the consumers in social welfare schemes. A customer will not get any benefit if he is not interested in participating. A genetic algorithm is then used to solve the optimization problem. The results obtained proved that the customers participating in the DR get reasonable incentives without impacting the electricity bills of other customers. Similarly, the work in [139] proposed a Stackelberg game with multiple users and multiple power retailers for maximizing the retailers' revenue and also the users' payoff in the retail power market. The authors also have designed an incentive mechanism to adjust the retailers' price information to ensure the proper operation of a smart grid and also to balance the supply-demand. The results obtained proved that the real-time pricing of the power can be reduced by the proposed scheme.

The authors in [10] proposed a novel real-time incentive-based DR algorithm with deep neural networks and RL for smart grids. The aim of this work is to support the service providers in purchasing the energy from their consumers that balances energy fluctuations, which in turn ensures the reliability of the smart grid. For predicting the energy demands and unknown prices, a deep neural network is used. To get the apt incentive rates for every customer, the RL algorithm is used by the authors, considering the profits of consumers as well as the service providers. The results obtained proved that the proposed incentive based DR algorithm encourages demand side participation, increase the profitabilities of customers as well as service providers, thus improving the reliability of the system by balancing the energy resources. Another work in [140] proposed an approach based on layered stochastic optimization based on incentive mechanism and real-time pricing for residential DR. In this work, homes are incentivized by the residential load aggregator, and the loads are controlled by the home energy management systems to maximize the rewards in real-time. The case studies presented by the authors proved that the proposed incentive based energy management system reduced the energy cost by 28%, reduced the peak demand by 17%. An interesting work in [141] proposed a score-based incentive mechanism to motivate the residential users in participating in the DR. In the proposed approach, firstly, the authors establish the load models of the appliances in residencies taking into account the comfort levels of the consumers. Later, based on the residential users and power grid company, a cost-benefit analysis is performed, based on which a score-based incentive mechanism to promote the DR is formulated by a bi-level optimization model. The case studies proved that after the implementation of the proposed scheme the peak load is reduced by 18.99% and the late peak period is reduced by 20.41%. Also, an increase of 14.06% is observed in the total profit of the power grid company. Similarly, [142] proposed a direct load control planning that provides free energy credits to the consumers for a load of air conditioning, ventilation, and heating appliances during the DR events. The consumers can use the credit obtained during the periods of higher price-free of cost that will enable the consumers to reduce the electricity costs. DR in data centers is a promising approach to mitigate the operational stability issues in smart grids. It has significant potential in the reduction of peak loads that paves the way for distributed generation of power. Incentives from the utilities to the cloud service providers can help reduce the burden of cloud providers to meet the demands on increased electricity costs. The simulation results proved that the proposed energy credits strategy reduced the total cost by approximately 10%.

Peer-to-peer selling of energy through local energy markets is possible in smart grids when renewable energy sources are integrated with smart grids. This approach faces some challenges such as single-point of failure in the management of energy data, lack of trust in the trading of energy, verification and transparency in the distribution of energy, and non-incentivized energy trading. To address the aforementioned problems, the authors in [95] proposed an incentivized and trustworthy framework for energy trading in a smart grid. An iterative VCG approach is used by the authors in this work for incentivizing energy trading. In this approach, by Vikrey auction method, prosumers are issued cash coins, consumers are issued energy tokens, and the results are updated in the blockchain. In this way, the proposed method incentivizes the consumers, addresses the challenges related to transparency, trust issues through blockchain. The vickrey auction [143] approach is designed for ensuring the selling of a product in which the bidder who bids highest will be getting the product in the auction. The winner of the bidding has to pay the bidded amount equal to the next highest bid as an incentive. The authors have modified the basic Vickrey's auction mechanism to map the demands of consumer's energy with the energy generation of prosumers. The ownership of energy tokens is then updated by assigning the tokens to the winner of the auction, after which the winner is removed from the auction process and the energy won is reduced from the available energy. This process of auctioning is carried out recursively for the energy available without changing the bidding value of the bidders until the energy available becomes zero. The government's energy generators can provide the energy to the loser of the auction. The unsold energy from the prosumers can be sold directly to the government. The simulation results proved that the winner percentage is more in the proposed framework when compared to existing works. In a similar work, the authors in [144] proposed an incentive mechanism based on blockchain for the trading of renewable energy power to motivate the improvement in the scale and quality of generation of power from the producers. The remuneration can be paid fairly and automatically according to the incentive algorithm to the producers of renewable energy. The simulation results proved that the purchasing price of the power is reduced along with the reduced load on the grid. In another interesting work, to address the growing privacy and security concerns and to detect malicious activities in a smart grid, the work in [145] proposed a novel data analytics based on blockchain. The data integrity issues in smart grid such as smart meter failure and false data injection attacks, are detected by the proposed approach. A smart contract-based blockchain incentive mechanism is proposed by the authors for the utility providers to handle the malicious activities on their side that offers incentives if malicious activity is detected. The simulation results showed that the proposed approach achieves a trip latency of below 1 milli second and reliability of 99.99% that is better when compared to traditional approaches.

E. Other Applications

The rapid digitization of industrial production is seeing a tremendous amount of data being generated from smart factories through IoT sensors, actuators, etc. Traditional centralized processing in clouds in industrial IoT faces several issues such as high maintenance costs and large infrastructure. Also, the privacy and security of the smart factories and device manufacturers are main concerns due to the interconnection of devices. A blockchain-based framework is proposed in [146] for industrial IoT to address the issues such as trustworthiness, privacy preservation in the construction of the ecosystem of industrial IoT. In this work, smart contracts and other blockchain-based techniques are integrated with IoT. Smart contract acts as a contract of manufacturing resources and consumers to provide manufacturing services on-demand. To encourage the SPs or third parties to provide their resources for smart factories, the authors proposed an incentive mechanism for the SPs, where the SPs will act as miners in the blockchain network that will enable the construction of a trusted blockchain-based data-sharing network. The SPs contributing their resources can participate in the blockchain network management and obtain the incentive.

F. Summary and Discussion

Incentive mechanisms based on AI, blockchain, and game theory have been extensively studied and experimented to motivate the users to share quality data to the requesters in several IoT-based applications such as smart healthcare, smart transportation, smart city, and smart grid. However, to further improve the data collected from the participants, some of the challenges such as fair incentive calculation, transparency in reward calculation for the data providers/IoT devices, sharing of the resources among the incentive providers, providing incentives to the applications that require high bandwidth and low latency in the upcoming 6G era have to be addressed. The applications of incentive techniques in vertical IoT domains are summarized in Table IV.

V. Challenges, Open Issues, and Future Directions

In this section, several open research challenges related to the incentive techniques for IoT and possible solutions are discussed.

A. Issues in IoT Data Offloading and Caching

Although data offloading and caching incentives help, their implementation is still challenging. The data in use is dynamic and depends on user needs. In an environment of constant change, incentives can't be effective. A failure could occur if the network is overloaded because all users are maxing out their allotted bandwidth. To overcome this issue, we suggest a categorical and AI-based incentive mechanism where the data usage demand is predicted based on historical events, and the data is categorized by its importance. Additionally, there is a concern about how IoT devices will impact the networks because some devices tend to frequently offload data. Some sensors are randomly placed throughout the facility, with huge amounts of data transmitted via cellular networks. Due to the sensors' growth, the network's load will continually increase. A strategy to counteract this problem is to use meta-heuristic algorithms to place sensors strategically, which helps with offloading mobile network data efficiently.

B. On-device Intelligent Incentive Platforms

One of the challenges in developing on-device incentive platforms in IoT devices is the limited hardware, storage, and computational capabilities in IoT devices [65]. For example, AI-based incentive platforms require sufficient storage capabilities to store the data for training the algorithms. They also need sufficient hardware and computational resources to run the AI algorithms in calculating the incentives. One of the solutions to address these issues is to use edge devices for offloading the data generated from IoT devices [147]. Edge devices can use edge analytics that can support AI/game theory-based incentive platforms. Also, some effective pre-processing mechanisms can be applied to filter out the unrelated/noisy data that can reduce the dimensionality of the data [148] [149]. In addition, using lightweight ML/DL models is helpful to get faster prediction as well as to achieve the trade-off between the energy consumption of certain IoT devices and the final model performance.

TABLE IV
SUMMARY OF APPLICATIONS OF INCENTIVE TECHNIQUES IN VERTICAL IOT DOMAINS.

IoT Applications	Ref.	Incentive Mechanism	Contributions	Limitations and Challenges
Smart Healthcare	[114]	Blockchain	A dynamic incentive mechanism aims to promote data sharing over cloud-based healthcare systems. Revenue distribution fairness is measured based on the Shapley metric.	The revenues for hospital and diagnosis center is fairly divided regardless their inequitable roles.
	[116]	Blockchain	An information entropy-based incentive mechanism to motivate participants in sharing medical data. Rewards are verified and confirmed via a blockchain network using PoW as the consensus algorithm.	The consensus algorithm with 50% node verification can be vulnerable.
	[117]	Blockchain	A blockchain-based incentive mechanism to reduce the gap of economic discrepancy caused by COVID-19. Incentive tokens are issued to an individual for free COVID test and self-quarantine agreement.	The system deployment is expensive besides some critical concerns about authority and security.
	[118]	Blockchain	A prescription management framework with an incentive mechanism to enable low-budget patients to approach high-quality medical services. Transactions are secured for authentication and authorization using cryptographic methods.	Lack of incentive verification and distribution schemes.
Smart Transportation	[119]	Public good game	A game theory-based incentive technique to encourage vehicle nodes in VANETs to share real-time traffic data. Revenue is paid based on the valuable data circulated in a group of vehicles joining a game.	More rounds of the game may be required to calculate revenue for non-cooperative conditions.
	[120]	Stackelberg game	Rewards paid by an incentive scheme are meaningful information to improve accuracy of lane changing detection and estimation.	The diversity of sharing information is limited. Lack of a mechanism to validate the trustworthiness of data.
	[122]	VCG game	A game-based incentive and punishment scheme is to motivate the cooperation between vehicles nodes. Nodes joining a game can earn incentive via active activities, whereas nodes with lazy activities can be penalized.	It is so hard to identity active/lazy nodes in calculating incentive.
	[124]	Game theory	A hierarchical incentive mechanism is to encourage mobile users to share trustworthy parking data. The incentive is paid based on the utility level of data validated and confirmed by a game theory-based protocol.	The proposed mechanism is quite simple and therefore cannot reflect complicated real-world behaviors.
	[125]	Stackelberg game	A game based incentive mechanism allows mobile vehicles to store and share popular contents via V2V communication. Rewards are calculated as a content popularity metric by the centralized global SDN controller.	As an assumption, all SBSs should be homogeneous to calculate cost and reward of moving controller vehicles.
	[121]	Blockchain	A secure and private incentive scheme to encourage vehicles nodes to collect and share sensing data for a real-time map update system. Via an auction, the winner will collect data on demand of MSP and the revenue will be calculated and paid over a blockchain-based payment system with a smart contract.	The incentive method can be crashed due to the failure of auction and the withdrawal of winner.
Smart City	[130]	Stackelberg game	To encourage the edge service providers to provide the computational resources and the nodes to participate in mining in smart city applications, an optimal incentive mechanism using a Stackelberg game is proposed by exploring the interactions and relations between them.	The proposed work does not consider the co-existence of multiple edge service providers in the system.
	[131]	Game theory	A rule-based incentive mechanism that uses evolutionary game theory and decision tree for processing the travelling information and generating the personalized incentives intelligently for the travellers in smart city is proposed.	The proposed work is not validated on a testbed. The proposed approach will give better results when the sample dataset is large.
	[133]	Blockchain	A bidding mechanism for general sensing tasks to encourage the vehicles to give their resources is proposed that can schedule the tasks for those vehicles.	The proposed work is not validated on a testbed, and large resources are required for blockchain.
Smart Grid	[137]	Stackelberg game	An approach for incentiving the consumers is proposed, in which the DR problem is formulated a Stackelberg game, where the leader is the utility company and the customers are treated as followers of the leader.	The simulation is performed on existing data. The performance of the proposed approach is unknown in real-time.
	[10]	Deep neural networks and RL	A novel real-time incentive-based DR algorithm is proposed with deep neural networks and RL for smart grids.	The proposed work is validated using simulations, but not implemented on a testbed or in real time. The proposed work considered only single SP.
	[141]	Score-based method	Based on the residential users and power grid company, a cost-benefit analysis is performed and a score based incentive mechanism to promote the DR is formulated by a bi-level optimization model.	The penalty incurred may be greater than the benefits due to incentives, thus the market may not be balanced.
	[95]	VCG approach and blockchain	An incentivized and trustworthy framework for energy trading is proposed for the smart grid. An iterative VCG approach is used for incentivizing the energy trading.	Scalability of the proposed framework has to be improved.
	[145]	Blockchain	A smart contract based blockchain incentive mechanism is proposed for the utility providers to handle the malicious activities on their side that offers incentives if a malicious activity is detected.	The proposed work is validated using simulations, but not implemented on a testbed or in real time. The proposed work considered only single SP.

C. Privacy for Incentive-IoT Systems

Data providers may be reluctant to provide the data even if the incentives are attractive as they may be wary of their personal and sensitive data being compromised. For example, suppose the location of an IoT device is exposed. In that case, the attackers may use the information to find the patterns of the places being visited by the users and correctly predict a location they may be visiting at a particular time/day to take advantage. Hence, preserving the privacy of the IoT devices is of paramount importance to attract a good number of users to voluntarily provide the data [85]. However, preserving privacy comes with a cost. If the private data of the users is important for the requester, and privacy has to be preserved, it may be a direct conflict with the high-quality data requirement from the requester. For example, consider that the requester wants to analyze the patterns regarding the visits of customers to a restaurant. As the location details are private and sensitive, if the privacy of the users has to be preserved, the location details may not be shared with the service providers. So the data shared with the requester may be missing a very important component, location. The data providers may end up providing higher incentives for fewer quality data provided by the IoT devices due to privacy preservation. Hence, the design of incentive mechanism has to maintain the balance between the privacy preservation and the quality of the data provided by the IoT devices, which is a significant future direction in the design of incentive mechanisms for IoT devices [3]. Moreover, some privacy-preserving mechanisms may be expansive in terms of computation and communication overhead and energy consumption, especially with the lightweight IoT devices having fewer CPU resources and limited battery capacity. Consequently, certain IoT devices can be discouraged from participating in collaborative tasks. Therefore, further security and privacy protection in data aggregation is still an ongoing research topic, and new techniques are required to improve privacy for IoT-based systems.

D. Incentives for Edge-based IoT

As discussed earlier, edge devices play a vital role in real-time analytics on the large volume of data generated from IoT-based applications. The recent rise in fog/edge computing has made it possible to migrate the services of cloud providers to micro-data centers to address the issues faced by the applications based on cloud computing. The edge devices in MEC networks may belong to different organizations; thus, storage, computation, and communication resources may not be efficiently utilized. The establishment of data sharing mechanism among the heterogeneous edge devices for IoT-based applications is a challenge. The development of incentive mechanisms to attract micro-data centers for hosting the services for IoT-based applications is an open issue that needs to be addressed to balance the benefits of edge service providers and IoT users [150]–[152].

E. Incentives for IoT Networks in the 6G era

In the future 6G communications, IoT-based applications may use smart wearables, implanted devices, and nanodevices. The development of suitable incentive mechanisms for these devices in the upcoming 6G era is a challenge. Several mission-critical applications such as remote surgery, smart transportation through autonomous vehicles, smart grids, etc., require ultra-high network reliability with very low latency to ensure the transfer of data with high reliability in a few milliseconds. How to develop incentive mechanisms for such IoT-based mission-critical applications that require huge resources and spectrum from multiple service providers is a challenge [153], [154].

F. Interpretability of AI-based Incentive Mechanisms

AI algorithms can be used effectively to design/develop incentive mechanisms for several IoT-based applications. These algorithms can assist the requesters in calculating the rewards for several participants in incentive mechanisms. However, the black-box nature of AI algorithms makes it very difficult for humans to understand the reasons behind the calculations of incentive that may lead to a lack of trust in these mechanisms. How to design incentive mechanisms for IoT-based applications that can give interpretable decisions regarding the incentive calculation to increase the trust of the participants is a significant challenge. Explainable AI can be used to solve the aforementioned challenges [155], [156].

VI. Conclusion

Incentive mechanisms are important in the manner through which IoT devices are encouraged to participate and contribute to the IoT network. This paper has been conducted to bridge the gap in the existing studies that a comprehensive survey on incentive techniques for IoT has not been carried out. In this paper, we have provided a comprehensive survey on incentive techniques for IoT. First, we have presented the fundamentals of AI and three important incentive techniques, including game theory, blockchain, and AI. Second, we have discussed the use of incentive techniques for IoT applications and services in more detail. Further, from the extensive review, we have highlighted various challenges and future directions that drive further research of IoT incentive studies. It is expected that this paper will stimulate more attention and research efforts toward the use of incentive techniques for IoT services and applications.

References

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," *IEEE communications surveys & tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.

[2] M. S. Mahdavinejad, M. Rezvan, M. Barekatain, P. Adibi, P. Barnaghi, and A. P. Sheth, "Machine learning for internet of things data analysis: A survey," *Digital Communications and Networks*, vol. 4, no. 3, pp. 161–175, 2018.

[3] L. G. Jaimes, I. J. Vergara-Laurens, and A. Raij, "A survey of incentive techniques for mobile crowd sensing," *IEEE Internet of Things Journal*, vol. 2, no. 5, pp. 370–380, 2015.

[4] D. C. Nguyen, M. Ding, P. N. Pathirana, A. Seneviratne, J. Li, D. Niyato, and H. V. Poor, "Federated learning for industrial internet of things in future industries," *arXiv preprint arXiv:2105.14659*, 2021.

[5] X. Zhang, Z. Yang, W. Sun, Y. Liu, S. Tang, K. Xing, and X. Mao, "Incentives for mobile crowd sensing: A survey," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 54–67, 2016.

[6] H. Gao, C. H. Liu, W. Wang, J. Zhao, Z. Song, X. Su, J. Crowcroft, and K. K. Leung, "A survey of incentive mechanisms for participatory sensing," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 2, pp. 918–943, 2015.

[7] A. K. Shrestha, J. Vassileva, and R. Deters, "A blockchain platform for user data sharing ensuring user control and incentives," *Frontiers in Blockchain*, vol. 3, p. 48, 2020.

[8] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Integration of blockchain and cloud of things: Architecture, applications and challenges," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2521–2549, 2020.

[9] Y. Chen, X. Gong, R. Ou, L. Duan, and Q. Zhang, "Crowdcaching: Incentivizing D2D-enabled caching via coalitional game for IoT," *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 5599–5612, 2020.

[10] R. Lu and S. H. Hong, "Incentive-based demand response for smart grid with reinforcement learning and deep neural network," *Applied energy*, vol. 236, pp. 937–949, 2019.

[11] L. Liu, X. Wen, L. Wang, Z. Lu, W. Jing, and Y. Chen, "Incentive-aware recruitment of intelligent vehicles for edge-assisted mobile crowdsensing," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 10, pp. 12 085–12 097, 2020.

[12] J. Nie, J. Luo, Z. Xiong, D. Niyato, P. Wang, and M. Guizani, "An incentive mechanism design for socially aware crowdsensing services with incomplete information," *IEEE Communications Magazine*, vol. 57, no. 4, pp. 74–80, 2019.

[13] Y. Zhang, M. Pan, L. Song, Z. Dawy, and Z. Han, "A survey of contract theory-based incentive mechanism design in wireless networks," *IEEE wireless communications*, vol. 24, no. 3, pp. 80–85, 2017.

[14] C. Yang, J. Xiao, J. Li, X. Shao, A. Anpalagan, Q. Ni, and M. Guizani, "DISCO: Interference-aware distributed cooperation with incentive mechanism for 5G heterogeneous ultra-dense networks," *IEEE Communications Magazine*, vol. 56, no. 7, pp. 198–204, 2018.

[15] J. Moura and D. Hutchison, "Game theory for multi-access edge computing: Survey, use cases, and future trends," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 260–288, 2018.

[16] Z. Liu, N. C. Luong, W. Wang, D. Niyato, P. Wang, Y.-C. Liang, and D. I. Kim, "A survey on blockchain: A game theoretical perspective," *IEEE Access*, vol. 7, pp. 47 615–47 643, 2019.

[17] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, "A survey of distributed consensus protocols for blockchain networks," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1432–1465, 2020.

[18] W. Sun, L. Wang, P. Wang, and Y. Zhang, "Collaborative blockchain for space-air-ground integrated networks," *IEEE Wireless Communications*, vol. 27, no. 6, pp. 82–89, 2020.

[19] Z. Chang, W. Guo, X. Guo, T. Chen, G. Min, K. M. Abualnaja, and S. Mumtaz, "Blockchain-empowered drone networks: Architecture, features, and future," *IEEE Network*, vol. 35, no. 1, pp. 86–93, 2021.

[20] Y. Wang, Z. Su, K. Zhang, and A. Benslimane, "Challenges and solutions in autonomous driving: A blockchain approach," *IEEE Network*, vol. 34, no. 4, pp. 218–226, 2020.

[21] R. Zhang, F. R. Yu, J. Liu, R. Xie, and T. Huang, "Blockchain-incentivized D2D and mobile edge caching: A deep reinforcement learning approach," *IEEE Network*, vol. 34, no. 4, pp. 150–157, 2020.

[22] D. C. Nguyen, P. Cheng, M. Ding, D. Lopez-Perez, P. N. Pathirana, J. Li, A. Seneviratne, Y. Li, and H. V. Poor, "Enabling AI in future wireless networks: a data life cycle perspective," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 1, pp. 553–595, 2020.

[23] Q. Pan, J. Wu, J. Li, W. Yang, and Z. Guan, "Blockchain and AI empowered trust-information-centric network for beyond 5G," *IEEE Network*, vol. 34, no. 6, pp. 38–45, 2020.

[24] D. C. Nguyen, M. Ding, Q.-V. Pham, P. N. Pathirana, L. B. Le, A. Seneviratne, J. Li, D. Niyato, and H. V. Poor, "Federated learning meets blockchain in edge computing: Opportunities and challenges," *IEEE Internet of Things Journal*, vol. 8, no. 16, pp. 12 806–12 825, 2021.

[25] Y. Zhan, J. Zhang, Z. Hong, L. Wu, P. Li, and S. Guo, "A survey of incentive mechanism design for federated learning," *IEEE Transactions on Emerging Topics in Computing*, 2021.

[26] R. Zeng, C. Zeng, X. Wang, B. Li, and X. Chu, "A comprehensive survey of incentive mechanism for federated learning," *arXiv preprint arXiv:2106.15406*, 2021.

[27] S. Nižetić, P. Šolić, D. L.-d.-I. González-de, L. Patrono *et al.*, "Internet of things (IoT): Opportunities, issues and challenges towards a smart and sustainable future," *Journal of Cleaner Production*, vol. 274, p. 122877, 2020.

[28] R. Belchior, A. Vasconcelos, S. Guerreiro, and M. Correia, "A survey on blockchain interoperability: Past, present, and future trends," *ACM Computing Surveys (CSUR)*, vol. 54, no. 8, pp. 1–41, 2021.

[29] N. Upadhyay, "Demystifying blockchain: A critical analysis of challenges, applications and opportunities," *International Journal of Information Management*, vol. 54, p. 102120, 2020.

[30] W. Wang, H. Xu, M. Alazab, T. R. Gadekallu, Z. Han, and C. Su, "Blockchain-based reliable and efficient certificateless signature for IIoT devices," *IEEE Transactions on Industrial Informatics*, 2021.

[31] N. Deepa, Q.-V. Pham, D. C. Nguyen, S. Bhattacharya, B. Prabadevi, T. R. Gadekallu, P. K. R. Maddikunta, F. Fang, and P. N. Pathirana, "A survey on blockchain for big data: Approaches, opportunities, and future directions," *Future Generation Computer Systems*, vol. 131, pp. 209–226, 2022.

[32] T. R. Gadekallu, Q.-V. Pham, D. C. Nguyen, P. K. R. Maddikunta, N. Deepa, B. Prabadevi, P. N. Pathirana, J. Zhao, and W.-J. Hwang, "Blockchain for edge of things: Applications, opportunities, and challenges," *IEEE Internet of Things Journal*, vol. 9, no. 2, pp. 964–988, 2021.

[33] X. Ding, J. Guo, D. Li, and W. Wu, "An incentive mechanism for building a secure blockchain-based internet of things," *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 1, pp. 477–487, 2020.

[34] X. Ding, J. Guo, D. Li, and W. Wu, "An incentive mechanism for building a secure blockchain-based internet of things," *IEEE Transactions on Network Science and Engineering*, pp. 1–1, 2020.

[35] T. A. Alghamdi, I. Ali, N. Javaid, and M. Shafiq, "Secure service provisioning scheme for lightweight IoT devices with a fair payment system and an incentive mechanism based on blockchain," *IEEE Access*, vol. 8, pp. 1048–1061, 2020.

[36] Z. Tian, X. Gao, S. Su, J. Qiu, X. Du, and M. Guizani, "Evaluating reputation management schemes of internet of vehicles based on evolutionary game theory," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 6, pp. 5971–5980, 2019.

[37] J. R. Marden and J. S. Shamma, "Game theory and control," *Annual Review of Control, Robotics, and Autonomous Systems*, vol. 1, pp. 105–134, 2018.

[38] Y. Xu, J. Liu, Y. Shen, J. Liu, X. Jiang, and T. Taleb, "Incentive jamming-based secure routing in decentralized internet of things," *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 3000–3013, 2021.

[39] P. Kamalinejad, C. Mahapatra, Z. Sheng, S. Mirabbasi, V. C. M. Leung, and Y. L. Guan, "Wireless energy harvesting for the internet of things," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 102–108, 2015.

[40] Z. Hou, H. Chen, Y. Li, and B. Vucetic, "Incentive mechanism design for wireless energy harvesting-based internet of things," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2620–2632, 2018.

[41] M. Haenlein and A. Kaplan, "A brief history of artificial intelligence: On the past, present, and future of artificial intelligence," *California management review*, vol. 61, no. 4, pp. 5–14, 2019.

[42] J. Cai, J. Luo, S. Wang, and S. Yang, "Feature selection in machine learning: A new perspective," *Neurocomputing*, vol. 300, pp. 70–79, 2018.

[43] S. Dargan, M. Kumar, M. R. Ayyagari, and G. Kumar, "A survey of deep learning and its applications: a new paradigm to machine learning," *Archives of Computational Methods in Engineering*, vol. 27, no. 4, pp. 1071–1092, 2020.

[44] N. Ketkar and E. Santana, *Deep learning with Python*. Springer, 2017, vol. 1.

[45] D. C. Nguyen, M. Ding, P. N. Pathirana, A. Seneviratne, J. Li, and H. V. Poor, "Federated learning for Internet of Things: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 3, pp. 1622–1658, 2021.

[46] D. C. Nguyen, Q.-V. Pham, P. N. Pathirana, M. Ding, A. Seneviratne, Z. Lin, O. A. Dobre, and W.-J. Hwang, "Federated learning for smart healthcare: A survey," *ACM Computing Surveys*, vol. 55, no. 3, pp. 1–37, 2022.

[47] J. Weng, J. Weng, J. Zhang, M. Li, Y. Zhang, and W. Luo, "DeepChain: Auditable and privacy-preserving deep learning with blockchain-based incentive," *IEEE Transactions on Dependable and Secure Computing*, 2019.

[48] S. Agrawal, S. Sarkar, O. Aouedi, G. Yenduri, K. Piamrat, S. Bhattacharya, P. K. R. Maddikunta, and T. R. Gadekallu, "Federated learning for intrusion detection system: Concepts, challenges and future directions," *arXiv preprint arXiv:2106.09527*, 2021.

[49] L. Li, Y. Fan, M. Tse, and K.-Y. Lin, "A review of applications in federated learning," *Computers & Industrial Engineering*, p. 106854, 2020.

[50] J. Kang, Z. Xiong, D. Niyato, S. Xie, and J. Zhang, "Incentive mechanism for reliable federated learning: A joint optimization approach to combining reputation and contract theory," *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 10 700–10 714, 2019.

[51] P. B, N. Deepa, Q.-V. Pham, D. C. Nguyen, P. K. R. M, T. R. G, P. N. Pathirana, and O. Dobre, "Toward blockchain for Edge-of-Things: A new paradigm, opportunities, and future directions," *IEEE Internet of Things Magazine*, vol. 4, no. 2, pp. 102–108, 2021.

[52] S. P. RM, S. Bhattacharya, P. K. R. Maddikunta, S. R. K. Somayaji, K. Lakshmanna, R. Kaluri, A. Hussien, and T. R. Gadekallu, "Load balancing of energy cloud using wind driven and firefly algorithms in internet of everything," *Journal of parallel and distributed computing*, vol. 142, pp. 16–26, 2020.

[53] T. R. Gadekallu, Q.-V. Pham, T. Huynh-The, S. Bhattacharya, P. K. R. Maddikunta, and M. Liyanage, "Federated learning for big data: A survey on opportunities, applications, and future directions," *arXiv e-prints*, pp. arXiv–2110, 2021.

[54] Z. Allam and Z. A. Dhunny, "On big data, artificial intelligence and smart cities," *Cities*, vol. 89, pp. 80–91, 2019.

[55] M. Shen, J. Duan, L. Zhu, J. Zhang, X. Du, and M. Guizani, "Blockchain-based incentives for secure and collaborative data sharing in multiple clouds," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 6, pp. 1229–1241, 2020.

[56] S. Xuan, L. Zheng, I. Chung, W. Wang, D. Man, X. Du, W. Yang, and M. Guizani, "An incentive mechanism for data sharing based on blockchain with smart contracts," *Computers & Electrical Engineering*, vol. 83, p. 106587, 2020.

[57] B. Guo, X. Deng, J. Tian, Q. Guan, and X. Zheng, "A secure incentive mechanism for competitive organization data sharing: A contract theoretic approach," *IEEE Access*, vol. 7, pp. 60 067–60 078, 2019.

[58] B. Guo, X. Deng, Q. Guan, J. Tian, and X. Zheng, "An incentive mechanism for cross-organization data sharing based on data competitiveness," *IEEE Access*, vol. 6, pp. 72 836–72 844, 2018.

[59] H. Yu, Z. Liu, Y. Liu, T. Chen, M. Cong, X. Weng, D. Niyato, and Q. Yang, "A sustainable incentive scheme for federated learning," *IEEE Intelligent Systems*, vol. 35, no. 4, pp. 58–69, 2020.

[60] W. Sun, N. Xu, L. Wang, H. Zhang, and Y. Zhang, "Dynamic digital twin and federated learning with incentives for air-ground networks," *IEEE Transactions on Network Science and Engineering*, 2020.

[61] M. Wu, D. Ye, J. Ding, Y. Guo, R. Yu, and M. Pan, "Incentivizing differentially private federated learning: A multi-dimensional contract approach," *IEEE Internet of Things Journal*, 2021.

[62] W. Tang, J. Ren, K. Deng, and Y. Zhang, "Secure data aggregation of lightweight e-healthcare IoT devices with fair incentives," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8714–8726, 2019.

[63] C. Yi, A. S. Alfa, and J. Cai, "An incentive-compatible mechanism for transmission scheduling of delay-sensitive medical packets in e-health networks," *IEEE Transactions on Mobile Computing*, vol. 15, no. 10, pp. 2424–2436, 2015.

[64] W. Chen, Z. Zhang, Z. Hong, C. Chen, J. Wu, S. Maharjan, Z. Zheng, and Y. Zhang, "Cooperative and distributed computation offloading for blockchain-empowered industrial internet of things," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8433–8446, 2019.

[65] A. Heidari, M. A. Jabraeil Jamali, N. Jafari Navimipour, and S. Akbarpour, "Internet of things offloading: ongoing issues, opportunities, and future challenges," *International Journal of Communication Systems*, vol. 33, no. 14, p. e4474, 2020.

[66] Y. Park and S. Kim, "Game-based data offloading scheme for IoT system traffic congestion problems," *EURASIP Journal on Wireless Communications and Networking*, vol. 2015, no. 1, pp. 1–10, 2015.

[67] J. Liu, W. Gao, D. Li, S. Huang, and H. Liu, "An incentive mechanism combined with anchoring effect and loss aversion to stimulate data offloading in IoT," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4491–4511, 2019.

[68] J. S. Ng, W. Y. B. Lim, Z. Xiong, S. Garg, D. Niyato, and C. Leung, "Deep-learning based auction resource allocation in coded computation offloading for Internet-of-Things," in *2021 IEEE International Conference on Communications Workshops (ICC Workshops)*, 2021, pp. 1–5.

[69] H. Xu, X. Qiu, W. Zhang, K. Liu, S. Liu, and W. Chen, "Privacy-preserving incentive mechanism for multi-leader multi-follower IoT-edge computing market: A reinforcement learning approach," *Journal of Systems Architecture*, vol. 114, p. 101932, 2021.

[70] D. E. Boubiche, M. Imran, A. Maqsood, and M. Shoaib, "Mobile crowd sensing–taxonomy, applications, challenges, and solutions," *Computers in Human Behavior*, vol. 101, pp. 352–370, 2019.

[71] F. Khan, A. U. Rehman, J. Zheng, M. A. Jan, and M. Alam, "Mobile crowdsensing: A survey on privacy-preservation, task management, assignment models, and incentives mechanisms," *Future Generation Computer Systems*, vol. 100, pp. 456–472, 2019.

[72] B. Zhao, S. Tang, X. Liu, and X. Zhang, "PACE: Privacy-preserving and quality-aware incentive mechanism for mobile crowdsensing," *IEEE Transactions on Mobile Computing*, vol. 20, no. 5, pp. 1924–1939, 2020.

[73] R. She, "Survey on incentive strategies for mobile crowdsensing system," in *2020 IEEE 11th International Conference on Software Engineering and Service Science (ICSESS)*. IEEE, 2020, pp. 511–514.

[74] R. I. Ogie, "Adopting incentive mechanisms for large-scale participation in mobile crowdsensing: from literature review to a conceptual framework," *Human-centric computing and information sciences*, vol. 6, no. 1, pp. 1–31, 2016.

[75] J. Liu, H. Shen, H. S. Narman, W. Chung, and Z. Lin, "A survey of mobile crowdsensing techniques: A critical component for the internet of things," *ACM Transactions on Cyber-Physical Systems*, vol. 2, no. 3, pp. 1–26, 2018.

[76] J. Nie, J. Luo, Z. Xiong, D. Niyato, P. Wang, and H. V. Poor, "A multi-leader multi-follower game-based analysis for incentive mechanisms in socially-aware mobile crowdsensing," *IEEE Transactions on Wireless Communications*, vol. 20, no. 3, pp. 1457–1471, 2020.

[77] D. Guo, X. Feng, and H. Zheng, "Incentive mechanism design for mobile crowdsensing considering social networks," in *2020 IEEE 6th International Conference on Computer and Communications (ICCC)*. IEEE, 2020, pp. 2345–2350.

[78] J. Lu, Y. Xin, Z. Zhang, F. Wu, and J. Han, "Online rating protocol using endogenous and incremental learning design for mobile crowdsensing," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 3, pp. 3190–3201, 2020.

[79] M. Pouryazdan, B. Kantarci, T. Soyata, L. Foschini, and H. Song, "Quantifying user reputation scores, data trustworthiness, and user incentives in mobile crowd-sensing," *IEEE Access*, vol. 5, pp. 1382–1397, 2017.

[80] T. Luo, S. S. Kanhere, J. Huang, S. K. Das, and F. Wu, "Sustainable incentives for mobile crowdsensing: Auctions, lotteries, and trust and reputation systems," *IEEE Communications Magazine*, vol. 55, no. 3, pp. 68–74, 2017.

[81] F. Restuccia, S. K. Das, and J. Payton, "Incentive mechanisms for participatory sensing: Survey and research challenges," *ACM Transactions on Sensor Networks (TOSN)*, vol. 12, no. 2, pp. 1–40, 2016.

[82] X. Yang, J. Zhang, J. Peng, and L. Lei, "Incentive mechanism based on stackelberg game under reputation constraint for mobile crowdsensing," *International Journal of Distributed Sensor Networks*, vol. 17, no. 6, p. 15501477211023010, 2021.

[83] X. Dong, Z. You, T. H. Luan, Q. Yao, Y. Shen, and J. Ma, "Optimal mobile crowdsensing incentive under sensing inaccuracy," *IEEE Internet of Things Journal*, vol. 8, no. 10, pp. 8032–8043, 2020.

[84] J. Zhang, X. Yang, X. Feng, H. Yang, and A. Ren, "A joint constraint incentive mechanism algorithm utilizing coverage and reputation for mobile crowdsensing," *Sensors*, vol. 20, no. 16, p. 4478, 2020.

[85] B. Gu, X. Yang, Z. Lin, W. Hu, M. Alazab, and R. Kharel, "Multiagent actor-critic network-based incentive mechanism for mobile crowdsensing in industrial systems," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 9, pp. 6182–6191, 2020.

[86] Y. Zhao and C. H. Liu, "Social-aware incentive mechanism for vehicular crowdsensing by deep reinforcement learning," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 4, pp. 2314–2325, 2020.

[87] Y. Zhan, Y. Xia, J. Zhang, T. Li, and Y. Wang, "An incentive mechanism design for mobile crowdsensing with demand uncertainties," *Information Sciences*, vol. 528, pp. 1–16, 2020.

[88] Y. Zhang, X. Zhang, and F. Li, "BiCrowd: online biobjective incentive mechanism for mobile crowdsensing," *IEEE Internet of Things Journal*, vol. 7, no. 11, pp. 11 078–11 091, 2020.

[89] N. Xia, H. H. Song, Y. Liao, M. Iliofotou, A. Nucci, Z.-L. Zhang, and A. Kuzmanovic, "Mosaic: Quantifying privacy leakage in mobile networks," in *Proceedings of the ACM SIGCOMM 2013 conference on SIGCOMM*, 2013, pp. 279–290.

[90] C. M. Medaglia and A. Serbanati, "An overview of privacy and security issues in the internet of things," *The internet of things*, pp. 389–395, 2010.

[91] E. Fitzgerald, M. Pióro, and A. Tomaszwski, "Energy-optimal data aggregation and dissemination for the internet of things," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 955–969, 2018.

[92] J. Wang, M. Li, Y. He, H. Li, K. Xiao, and C. Wang, "A blockchain based privacy-preserving incentive mechanism in crowdsensing applications," *IEEE Access*, vol. 6, pp. 17 545–17 556, 2018.

[93] J. BURKE, "Participatory sensing," in *Proc. World Sensor Web Workshop, 2006*, 2006, pp. 1–5.

[94] H. Lin, S. Garg, J. Hu, X. Wang, M. J. Piran, and M. S. Hossain, "Privacy-enhanced data fusion for COVID-19 applications in intelligent internet of medical things," *IEEE Internet of Things Journal*, 2020.

[95] A. Muzumdar, C. Modi, G. Madhu, and C. Vyjayanthi, "A trustworthy and incentivized smart grid energy trading framework using distributed ledger and smart contracts," *Journal of Network and Computer Applications*, vol. 183, p. 103074, 2021.

[96] G. Hajian, B. S. Ghahfarokhi, M. A. Vasfi, and B. T. Ladani, "Privacy, trust, and secure rewarding in mobile crowd-sensing based spectrum monitoring," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–21, 2021.

[97] A. Ouaddah, A. Abou Elkalam, and A. A. Ouahman, "Towards a novel privacy-preserving access control model based on blockchain technology in IoT," in *Europe and MENA cooperation advances in information and communication technologies*. Springer, 2017, pp. 523–533.

[98] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, "Applications of blockchains in the internet of things: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1676–1717, 2018.

[99] K. P. Puttaswamy, R. Bhagwan, and V. N. Padmanabhan, "Anonygator: Privacy and integrity preserving data aggregation," in *ACM/IFIP/USENIX International Conference on Distributed Systems Platforms and Open Distributed Processing*. Springer, 2010, pp. 85–106.

[100] F. Qiu, F. Wu, and G. Chen, "Privacy and quality preserving multimedia data aggregation for participatory sensing systems," *IEEE Transactions on Mobile Computing*, vol. 14, no. 6, pp. 1287–1300, 2014.

[101] L. Li, J. Liu, L. Cheng, S. Qiu, W. Wang, X. Zhang, and Z. Zhang, "Creditcoin: A privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 7, pp. 2204–2220, 2018.

[102] M. U. Javed, M. Rehman, N. Javaid, A. Aldegheishem, N. Alrajeh, and M. Tahir, "Blockchain-based secure data storage for distributed vehicular networks," *Applied Sciences*, vol. 10, no. 6, p. 2011, 2020.

[103] M. U. Hassan, M. H. Rehmani, and J. Chen, "Differential privacy techniques for cyber physical systems: a survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 746–789, 2019.

[104] C. Dwork, "Differential privacy: A survey of results," in *International conference on theory and applications of models of computation*. Springer, 2008, pp. 1–19.

[105] Y. Zhao, J. Zhao, L. Jiang, R. Tan, D. Niyato, Z. Li, L. Lyu, and Y. Liu, "Privacy-preserving blockchain-based federated learning for IoT devices," *IEEE Internet of Things Journal*, vol. 8, no. 3, pp. 1817–1829, 2020.

[106] Y. Lu, X. Huang, Y. Dai, S. Maharjan, and Y. Zhang, "Blockchain and federated learning for privacy-preserved data sharing in industrial IoT," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4177–4186, 2019.

[107] U. Gupta, D. Stripelis, P. K. Lam, P. M. Thompson, J. L. Ambite, and G. V. Steeg, "Membership inference attacks on deep regression models for neuroimaging," *arXiv preprint arXiv:2105.02866*, 2021.

[108] D. Macrinici, C. Cartofeanu, and S. Gao, "Smart contract applications within blockchain technology: A systematic mapping study," *Telematics and Informatics*, vol. 35, no. 8, pp. 2337–2354, 2018.

[109] W. Chen, Y. Chen, X. Chen, and Z. Zheng, "Toward secure data sharing for the IoV: a quality-driven incentive mechanism with on-chain and off-chain guarantees," *IEEE Internet of Things Journal*, vol. 7, no. 3, pp. 1625–1640, 2019.

[110] M. W. Condry and C. B. Nelson, "Using smart edge IoT devices for safer, rapid response with industry IoT control operations," *Proceedings of the IEEE*, vol. 104, no. 5, pp. 938–946, 2016.

[111] T. Huynh-The, C.-H. Hua, and D.-S. Kim, "Visualizing inertial data for wearable sensor based daily life activity recognition using convolutional neural network," in *Proc. 2019 41st Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*, 2019, pp. 2478–2481.

[112] C.-H. Hua, T. Huynh-The, K. Kim, S.-Y. Yu, T. Le-Tien, G. H. Park, J. Bang, W. A. Khan, S.-H. Bae, and S. Lee, "Bimodal learning via trilogy of skip-connection deep networks for diabetic retinopathy risk progression identification," *International Journal of Medical Informatics*, vol. 132, p. 103926, 2019.

[113] H. Xiong, C. Jin, M. Alazab, K.-H. Yeh, H. Wang, T. R. R. Gadekallu, W. Wang, and C. Su, "On the design of blockchain-based ecdsa with fault-tolerant batch verication protocol for blockchain-enabled IoMT," *IEEE Journal of Biomedical and Health Informatics*, 2021.

[114] M. Shen, J. Duan, L. Zhu, J. Zhang, X. Du, and M. Guizani, "Blockchain-based incentives for secure and collaborative data sharing in multiple clouds," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 6, pp. 1229–1241, 2020.

[115] W. Hu, Y. Hou, L. Tian, and Y. Li, "A novel profit-allocation strategy for SDN enterprises," *Enterprise Information Systems*, vol. 11, no. 1, pp. 4–16, 2017.

[116] X. Liang, W. Chen, J. Li, Y. Mu, and Z. Tian, "Incentive mechanism of medical data sharing based on information entropy in blockchain environment," *Journal of Physics: Conference Series*, vol. 1302, p. 022056, aug 2019.

[117] M. Manoj, G. Srivastava, S. R. K. Somayaji, T. R. Gadekallu, P. K. R. Maddikunta, and S. Bhattacharya, "An incentive based approach for COVID-19 planning using blockchain technology," in *Proc. 2020 IEEE Globecom Workshops*, 2020, pp. 1–6.

[118] A. Litchfield and A. Khan, "BlockPres: A novel blockchain-based incentive mechanism to mitigate inequalities for prescription management system," *Sensors*, vol. 21, no. 15, 2021.

[119] Q. Ding, X. Zeng, X. Zhang, and D. K. Sung, "A public goods game theory-based approach to cooperation in VANETs under a high vehicle density condition," *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 11, pp. 3995–4005, 2019.

[120] N. Ding, X. Meng, W. Xia, D. Wu, L. Xu, and B. Chen, "Multivehicle coordinated lane change strategy in the roundabout under internet of vehicles based on game theory and cognitive computing," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 8, pp. 5435–5443, 2020.

[121] C. Lai, M. Zhang, J. Cao, and D. Zheng, "SPIR: A secure and privacy-preserving incentive scheme for reliable real-time map updates," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 416–428, 2020.

[122] G.-U. Rehman, A. Ghani, M. Zubair, S. H. A. Naqvi, D. Singh, and S. Muhammad, "IPS: Incentive and punishment scheme for omitting selfishness in the internet of vehicles (IoV)," *IEEE Access*, vol. 7, pp. 109 026–109 037, 2019.

[123] N. Mohammed, H. Otrok, L. Wang, M. Debbabi, and P. Bhattacharya, "Mechanism design-based secure leader election model for intrusion detection in MANET," *IEEE Transactions on Dependable and Secure Computing*, vol. 8, no. 1, pp. 89–103, 2011.

[124] B. Hoh, T. Yan, D. Ganesan, K. Tracton, T. Iwuchukwu, and J.-S. Lee, "TruCentive: A game-theoretic incentive platform for trustworthy mobile crowdsourcing parking services," in *Proc. 2012 15th International IEEE Conference on Intelligent Transportation Systems*, 2012, pp. 160–166.

[125] A. Alioua, S. Simoud, S. Bourema, M. Khelifi, and S.-M. Senouci, "A stackelberg game approach for incentive V2V caching in software-defined 5G-enabled VANET," in *Proc. 2020 IEEE Symposium on Computers and Communications (ISCC)*, 2020, pp. 1–6.

[126] S. Bhattacharya, S. R. K. Somayaji, T. R. Gadekallu, M. Alazab, and P. K. R. Maddikunta, "A review on deep learning for future smart cities," *Internet Technology Letters*, p. e187, 2020.

[127] A. Camero and E. Alba, "Smart city and information technology: A review," *cities*, vol. 93, pp. 84–94, 2019.

[128] F. Zhao, O. I. Fashola, T. I. Olarewaju, and I. Onwumere, "Smart city research: A holistic and state-of-the-art literature review," *Cities*, vol. 119, p. 103406, 2021.

[129] M. Pouryazdan and B. Kantarci, "The smart citizen factor in trustworthy smart city crowdsensing," *IT Professional*, vol. 18, no. 4, pp. 26–33, 2016.

[130] Z. Chang, W. Guo, X. Guo, Z. Zhou, and T. Ristaniemi, "Incentive mechanism for edge-computing-based blockchain," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 11, pp. 7105–7114, 2020.

[131] H. Mei, S. Poslad, and S. Du, "A game-theory based incentive framework for an intelligent traffic system as part of a smart city initiative," *Sensors*, vol. 17, no. 12, p. 2874, 2017.

[132] X. Chen, L. Zhang, B. Lin, and Y. Fang, "Delay-aware incentive mechanism for crowdsourcing with vehicles in smart cities," in *2019 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2019, pp. 1–6.

[133] B. Yin, Y. Wu, T. Hu, J. Dong, and Z. Jiang, "An efficient collaboration and incentive mechanism for internet of vehicles (IoV) with secured information exchange based on blockchains," *IEEE Internet of Things Journal*, vol. 7, no. 3, pp. 1582–1593, 2019.

[134] M. Faheem, S. B. H. Shah, R. A. Butt, B. Raza, M. Anwar, M. W. Ashraf, M. A. Ngadi, and V. C. Gungor, "Smart grid communication and information technologies in the perspective of Industry 4.0: opportunities and challenges," *Computer Science Review*, vol. 30, pp. 1–30, 2018.

[135] X. Jiang and L. Wu, "Residential power scheduling based on cost efficiency for demand response in smart grid," *IEEE Access*, vol. 8, pp. 197 324–197 336, 2020.

[136] S. M. Ali, Z. Ullah, G. Mokryani, B. Khan, I. Hussain, C. A. Mehmood, U. Farid, and M. Jawad, "Smart grid and energy district mutual interactions with demand response programs," *IET Energy Systems Integration*, vol. 2, no. 1, pp. 1–8, 2020.

[137] Y. Zhou, S. Ci, H. Li, and Y. Yang, "Designing pricing incentive mechanism for proactive demand response in smart grid," in *2018 IEEE International Conference on Communications (ICC)*. IEEE, 2018, pp. 1–6.

[138] T. Alquthami, A. H. Milyani, M. Awais, and M. B. Rasheed, "An incentive based dynamic pricing in smart grid: A customer's perspective," *Sustainability*, vol. 13, no. 11, p. 6066, 2021.

[139] Y. Dai, Y. Gao, H. Gao, and H. Zhu, "A demand response approach considering retailer incentive mechanism based on stackelberg game in smart grid with multi retailers," *International Transactions on Electrical Energy Systems*, vol. 28, no. 9, p. e2590, 2018.

[140] Z. Wang, R. Paranjape, Z. Chen, and K. Zeng, "Layered stochastic approach for residential demand response based on real-time pricing and incentive mechanism," *IET Generation, Transmission & Distribution*, vol. 14, no. 3, pp. 423–431, 2019.

[141] X. Liu, Z. Zhang, J. Hou, Z. Lin, L. Yang, F. Wen, and Y. Xue, "Optimal design of a score-based incentive mechanism for promoting demand response participations of residential users," in *2020 International Conference on Smart Grids and Energy Systems (SGES)*. IEEE, 2020, pp. 982–987.

[142] O. Erdinc, A. Taşcikaraoğlu, N. G. Paterakis, and J. P. Catalao, "Novel incentive mechanism for end-users enrolled in DLC-based demand response programs within stochastic planning context," *IEEE Transactions on Industrial Electronics*, vol. 66, no. 2, pp. 1476–1487, 2018.

[143] X. Zhang, K. An, B. Zhang, Z. Chen, Y. Yan, and D. Guo, "Vickrey auction-based secondary relay selection in cognitive hybrid satellite-terrestrial overlay networks with non-orthogonal multiple access," *IEEE Wireless Communications Letters*, vol. 9, no. 5, pp. 628–632, 2020.

[144] Z. Liu, D. Wang, J. Wang, X. Wang, and H. Li, "A blockchain-enabled secure power trading mechanism for smart grid employing wireless networks," *IEEE Access*, vol. 8, pp. 177 745–177 756, 2020.

[145] A. Kumari, M. M. Patel, A. Shukla, S. Tanwar, N. Kumar, and J. J. Rodrigues, "ArMor: a data analytics scheme to identify malicious behaviors on blockchain-based smart grid system," in *GLOBECOM 2020-2020 IEEE Global Communications Conference*. IEEE, 2020, pp. 1–6.

[146] L. Bai, M. Hu, M. Liu, and J. Wang, "BPIIoT: a light-weighted blockchain-based platform for industrial iot," *IEEE Access*, vol. 7, pp. 58 381–58 393, 2019.

[147] W. Rafique, L. Qi, I. Yaqoob, M. Imran, R. U. Rasool, and W. Dou, "Complementing IoT services through software defined networking and edge computing: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1761–1804, 2020.

[148] O. Aouedi, K. Piamrat, and B. Parrein, "Performance evaluation of feature selection and tree-based algorithms for traffic classification," 2021.

[149] G. T. Reddy, M. P. K. Reddy, K. Lakshmanna, R. Kaluri, D. S. Rajput, G. Srivastava, and T. Baker, "Analysis of dimensionality reduction techniques on big data," *IEEE Access*, vol. 8, pp. 54 776–54 788, 2020.

[150] I. Petri, O. F. Rana, J. Bignell, S. Nepal, and N. Auluck, "Incentivising resource sharing in edge computing applications," in *International Conference on the Economics of Grids, Clouds, Systems, and Services*. Springer, 2017, pp. 204–215.

[151] X. Zhang, X. Zhu, M. Chikuvanyanga, and M. Chen, "Resource sharing of mobile edge computing networks based on auction game and blockchain," *EURASIP Journal on Advances in Signal Processing*, vol. 2021, no. 1, pp. 1–23, 2021.

[152] Z. Li, Z. Yang, and S. Xie, "Computing resource trading for edge-cloud-assisted internet of things," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3661–3669, 2019.

[153] H. Alhosani, M. H. ur Rehman, K. Salah, C. Lima, and D. Svetinovic, "Blockchain-based solution for multiple operator spectrum sharing (MOSS) in 5G networks," in *2020 IEEE Globecom Workshops (GC Wkshps*. IEEE, 2020, pp. 1–6.

[154] P. Gorla, D. Paithankar, V. Chamola, S. Bitragunta, and M. Guizani, "Optimal spectral resource allocation and pricing for 5G and beyond: A game theoretic approach," *IEEE Networking Letters*, 2021.

[155] A. B. Arrieta, N. Díaz-Rodríguez, J. Del Ser, A. Bennetot, S. Tabik, A. Barbado, S. García, S. Gil-López, D. Molina, R. Benjamins *et al.*, "Explainable artificial intelligence (XAI): concepts, taxonomies, opportunities and challenges toward responsible AI," *Information Fusion*, vol. 58, pp. 82–115, 2020.

[156] A. Adadi and M. Berrada, "Peeking inside the black-box: A survey on explainable artificial intelligence (XAI)," *IEEE access*, vol. 6, pp. 52 138–52 160, 2018.