Journal of Parallel and Distributed Computing 199 (2025) 105040

Contents lists available at ScienceDirect

Journal of Parallel and Distributed Computing

journal homepage: www.elsevier.com/locate/jpdc

Skyward secure: Advancing drone data-sharing in 6G with decentralized dataspace and supported technologies

Saeed Hamood Alsamhi [a,b,c,*], Sumit Srivastava [d], Mamoon Rashid [c], Amnnah Alhabeeb [e], Santosh Kumar [f], Navin Singh Rajput [g], Ammar Hawbani [h], Liang Zhao [h], Mohammed A.A. Al-qaness [i,j], Edward Curry [a]

[a] *Insight Centre for Data Analytics, University of Galway, Ireland*
[b] *Department of Computer Science and Engineering, College of Informatics, Korea University, 145 Anam-ro, Seongbuk-gu, Seoul 02841, Republic of Korea*
[c] *School of Information Communication and Technology, Bahrain Polytechnic, PO Box 33349, Isa Town, Kingdom of Bahrain*
[d] *Department of Electronics and Communication Engineering, FET, MJP Rohilkhand University, Bareilly, Uttar Pradesh 243006, India*
[e] *Computer Department, Faculty of Science-Sabratha, Sabratha University, Libya*
[f] *Department of CSE, IIIT Naya Raipur, Chhattisgarh, India*
[g] *Department of Electronics Engineering, IIT (BHU), Varanasi, India*
[h] *School of Computer Science, Shenyang Aerospace University Shenyang, 110136, China*
[i] *College of Physics and Electronic Information Engineering, Zhejiang Normal University, Jinhua 321004, China*
[j] *College of Engineering and Information Technology, Emirates International University, Sana'a, Yemen*

A R T I C L E I N F O

Keywords:
Dataspace
Data sharing
Decentralized data sharing
Drones
B5G
Federated learning
Blockchain
Industry 4.0
Industry 5.0
Dataspace 4.0

A B S T R A C T

The capacity of Dataspace enables the distribution of heterogeneous data from several sources and domains and has attracted attention for resolving data integration challenges. Drone data sharing faces challenges such as protecting privacy and security, building trust and dependability, controlling latency and scalability, facilitating real-time data processing, and preserving the caliber of shared models. Therefore, sixth-generation (6G) networks provide high throughput and low latency to improve drone operations; security issues are exacerbated by the sensitive nature of shared data and the lack of centralized monitoring. To address the challenges, this paper presents a conceptual framework for a Dataspace in the Sky to enable secure and efficient drone data-sharing within 6G networks in the transition from Industry 4.0 to Industry 5.0. The Dataspace in the Sky integrates Federated Learning (FL), a decentralized Machine Learning (ML) approach that enhances security and privacy by sharing models instead of raw data, facilitating effective drone collaboration. However, the quality of shared local models often suffers due to inconsistent data contributions and unreliable recording mechanisms, which can undermine the performance of FL. To tackle the challenges, the framework employs blockchain (BC) to decentralize and secure the Dataspace, ensuring the integrity of contribution records and improving the reliability of shared models. Dataspace in the Sky empowered decentralized data sharing which addresses latency issues by decentralizing decision-making and enhances trust and reliability by leveraging immutable and transparent BC mechanisms. The robustness of Dataspace in the Sky solution is not only secures drone-sharing operations in 6G environments but enables the development of citizen-friendly mobility services, expanding opportunities across smart environments.

1. Introduction

Smart environments face various practical challenges in data management as they transition from a research vision to tangible manifestations in the real world made possible by the Internet of Things (IoT). The challenges include the flexibility required to combine real-time and contextual data, the interface between existing information systems and new digital infrastructures, and easy data-sharing between stakeholders

* Corresponding author.
E-mail addresses: s.alsamhi.rs.ece@iitbhu.ac.in (S.H. Alsamhi), sumitsrivastava@mjpru.ac.in (S. Srivastava), mamoon873@gmail.com (M. Rashid), amna.shushan@sabu.edu.ly (A. Alhabeeb), santosh.rs.cse12@iitbhu.ac.in (S. Kumar), anmande@ustc.edu.cn (A. Hawbani), lzhao@sau.edu.cn (L. Zhao), alqaness@zjnu.edu.cn (M.A.A. Al-qaness), edward.curry@insight-centre.org (E. Curry).

https://doi.org/10.1016/j.jpdc.2025.105040
Received 8 September 2024; Received in revised form 11 December 2024; Accepted 18 January 2025
Available online 21 January 2025

in the smart environment. In addition, since costs must be kept to a minimum, data management strategies for smart environments must allow for flexibility, dynamicity, and gradual change. Users at any event often stream and share pictures and videos, thereby consuming resources on the uplink channel and reducing the network's performance to ensure Quality of Service (QoS) [1]. QoS, energy consumption, and fast data delivery are challenging in drone networks. Sixth Generation (6G) is designed to offer a high data rate and improve QoS. Therefore, 6G presents a key solution to support drones' communication with each other and smart devices in smart environments. The QoS requirements (i.e., handoff, call admission control, channel reservation, etc.) were discussed to improve wireless communication via space technology [2–5,14,15]. While the authors in [16] introduced drone collaboration and HetNet for better QoS. In [17], the authors discussed an intelligent method for supporting QoS and connectivity in 6G networks.

Federated Learning (FL) is a machine learning (ML) technique that enables collaborative model training without sharing raw data, preserving data security and privacy. Moreover, with the massive amount of data gathered by drones, FL plays a vital role in improving the privacy and security of the learning model. Furthermore, Blockchain (BC) is a distributed ledger that ensures transparency, data integrity, and decentralization. In contrast, the FL, BC, and 6G combination in the drone's network leads to high-level security, decentralized learning, and satisfying QoS requirements [18]. While sensing methods have many similarities, the mix of different spatiotemporal resolutions, operational procedures, and the wide range of heterogeneous data collected with a drone has created a unique set of data management challenges. Furthermore, several international initiatives and technical developments in data management are creating particular chances for maximizing the potential of drones as environmental sensing technology. In this process, the drone serves as an IoT data collector, which is needed for privacy-preserving and efficient secure data [13]. As a result, various IoT application scenarios, including smart farming, smart homes, and water-quality monitoring, can benefit from drone-enabled data collection, as shown in Fig. 1.

6G networks pose several significant research challenges for developing a secure framework for drone data sharing, including security and privacy, trust and reliability, scalability and network management, latency, real-time data processing, and the quality of shared models. Drones frequently gather private data that has to be kept safe from unwanted access. Additionally, decentralized drone networks make them more susceptible to cyber threats, including data interception and man-in-the-middle attacks. Implementing end-to-end encryption and using FL to share models rather than raw data can significantly improve data security to overcome these problems [19]. BC technology may be used to build an immutable ledger of all transactions, which is necessary to provide trust in decentralized systems without a central authority [20]. Managing communications and resources effectively becomes more complex as drones rise. To reduce central server loads, edge computing and a decentralized architecture are required to analyze data closer to the source [21]. Low latency is required for real-time applications, and this may be accomplished via local data processing and efficient routing protocols that reduce waiting times [22]. Distributed data processing methods and FL may efficiently handle high data volumes, which allows real-time analysis and decision-making without centralizing data. Using BC to validate each drone's contribution and creating FL improvements to evaluate and upgrade local models before integration are two ways to ensure the correctness of shared models [23]. Moreover, Dataspace plays a crucial role in Decentralized Data- Sharing (DDS) by offering a flexible and adaptive approach to managing data. Dataspace provides flexible and adaptive data management by facilitating the progressive integration of various data sources without an upfront unifying schema [24]. The proposed framework intends to improve the security, effectiveness, and dependability of data sharing among drones in 6G networks [12,7,10], by fusing advanced technologies and architectural solutions, encouraging the creation of cutting-edge drone applications. Table 1 summarizes challenges for data-sharing among drones in 6G networks, justification, solutions, and roles of technologies and requirements for DDS.

Recently, drone networks have developed with the quick advancements in 6G communication technologies, which improve drone applications and introduce cutting-edge ones that call for reliable and low-latency communications [25]. Drones from various owners share collected data in 6G networks to get over the limitations of visual coverage and geographic region, expand the diversity of sensing data, and boost data dependability [26]. Although drones in 6G networks significantly benefit from data sharing, there is growing public concern regarding data-sharing security because a significant amount of sensitive data is included in the acquired data [27]. On the one hand, a lack of control over the data and scant monitoring operations may make drones hesitant to store and share data through ground cloud computing/edge computing infrastructures under centralized data management. Moreover, a DDS and management framework still has problems with illegal data access and security protection, even though the challenges of the centralized data-sharing and management framework can be resolved through data-sharing in a Peer-to-Peer (P2P) network. These difficulties impede the transfer of acquired data, acting as a bottleneck in the eventual spread of drones in 6G networks [28].

Drones have been widely used for mapping, remote sensing, farming, disaster management, search and rescue, boundary delineation, surveillance, and infotainment. In most applications, drones' swarms work together under a swarm controller's control at the ground station. The authors in [29] focused on evaluating the deployed drone's signal strength over smart cities to gather data from smart devices. Furthermore, multi-drone deployment represents the critical solution for collaborating with search and rescue teams in disaster areas [30–32]. Drones communicate and share data to complete time-sensitive and computationally expensive tasks, necessitating intelligence in the communication channel. Depending on the generated data and the application type, Intelligent approaches such as ML and Deep Learning (DL) models are used to train the shared data between drones. However, privacy and security issues are brought up by the centralized sharing of data drones. An intelligent attack by a malicious adversary on the central server could disrupt communication and have disastrous results.

A workable solution to security and privacy problems is the integration of FL in a swarm of drone collaboration. Privacy is maintained since FL only shares the model parameters and not the training data. However, an enemy might contaminate the global model with its local data and get access to confidential information. Furthermore, once the fictitious parameters are distributed iteratively, they could contaminate the global model's training. The intrinsic restrictions in FL attack types are the adversarial poisoning assault on the model and data and the underlying requirement on the nodes to establish collaborative learning membership. Therefore, it is necessary to include a notion of reliability in the FL learning process that mitigates the privacy leakage or the constructive failure of global models of drones to secure these threats. Drones are an entry point for significant industrial verticals and coordinate edge services in a Mobile Edge Computing (MEC) network [33]. Model aggregation outcomes under MEC server attacks in FL lead to a single-point failure that significantly impairs swarm maintenance and operations. Furthermore, the management of updated data gathered from millions of smart IoT devices-enabled drone gadgets is the extent of the scalability of contemporary edge computing systems.

BC is a potential method to overcome the restrictions and foster trust in FL communication. BC ensures traceability, scalability, decentralization, non-reusability, immutability, increased privacy, and security in FL-assisted drone communication. Due to topology changes brought on by various drone mobility models and network restrictions, the holistic integration of BC-leveraged FL-assisted drones offers the highest level of trust and privacy, data sharing, and traceable access under constant local updates [34]. BC technologies have drawn more attention as researchers explore their potential to guarantee secure data-sharing across

Table 1
Challenges for data-sharing among drones in 6G networks.

Challenge	Reasons	Solutions	Role of Technology	Required for DDS
Security and privacy	Sensitive data handling Multiple attacks	End-to-End (E2E) encryption FL Dataspace	Encryption secures data during transmission and storage FL shares models instead of raw data Dataspace manage and organize heterogeneous data securely	Robust encryption Secure model sharing mechanisms Incremental data integration
Trust and reliability	Ensuring trust without a central authority Need for tamper-proof records	BC Dataspace	BC creates a tamper-proof ledger of transactions Dataspace provides a unified view of data	Decentralized trust mechanisms Immutable and transparent Unified data views
Scalability	Managing several drones Dynamic topology due to drone mobility	Decentralized Edge computing Dataspace	Decentralized allows scalable management Edge computing processes data closer to the source Dataspace facilitate incremental integration and scalability	Flexible and adaptive network protocols Localized processing Incremental data integration mechanisms
Latency	Real-time applications High network delays	Edge computing Optimized routing Dataspace	Edge computing reduces latency Optimized routing ensures efficient data transmission Dataspace optimize data access	Low-latency communication infrastructure Efficient routing protocols Optimized data access
Real-Time Data Processing	Decision-making requirements High data volume from drones	Distributed data processing FL Dataspace	Distributed processing handles large data volumes FL enables collaborative data analysis Dataspace provide real-time access and integration of data	High-performance processing Distributed data analysis Real-time data integration and processing
Quality of Shared Models	Maintaining accuracy of models Verifying contributions of each drone	BC verification FL enhancements Dataspace	BC Verification records and verifies contributions FL enhancements assess and improve local models Dataspace ensure data quality and integrity	Accurate and transparent contribution tracking High-quality local model Consistent and reliable data

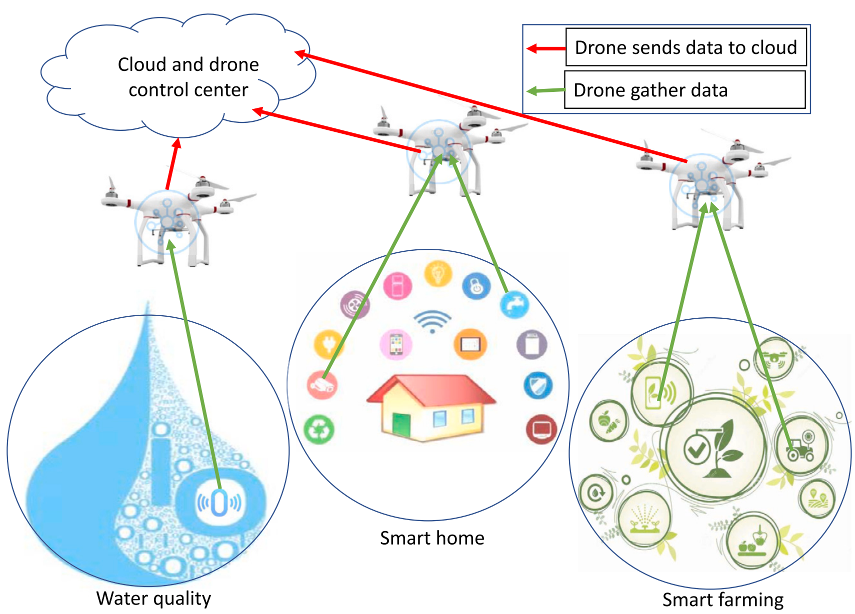

Fig. 1. Drone-enabled data acquisition.

a tamper-proof and decentralized ledger [28]. The authors of [35] used BC to create a network for securely exchanging traffic data between drones. A BC-based drone system was discussed for upcoming IoT applications to achieve secure data management and guarantee drone data integrity [36]. FL implementation via BC is made simpler because single-point failures in the system are avoided, and the need for a central server is removed. BC enables traceability between network entities and continuously observes channel activities transparent to all peer drones. With BC-assisted FL, the model parameters for easily traced using the logs recorded as ledger entries with the efficient process in [11]. The miners check the transactions in the block header, create blocks, add the FL, and model the chain's data.

Dataspace is a new paradigm of managing data from different resources and sharing data that has successfully managed scientific and personal data. However, Dataspace applications in intelligent systems and real-time data are still largely untapped. A real-time linked Dataspace platform was introduced to facilitate data management in intelligent environments [37] such as water environments and smart energy, along with supporting services, tiers of support, and a guiding philosophy for "Pay-As-You-Go" data management. Multi-resource in drone Dataspace refers to the ability of a drone to collect and share multiple types of data simultaneously. Drones can be equipped with various sensors and cameras to collect data on everything from temperature and humidity to air quality and soil moisture. By combining these different data types, drones can provide a more comprehensive view of the environment, which can be helpful in a wide range of applications. To support multi-resource data collection and sharing, drone Dataspace platforms must be designed to handle large volumes of data from various sources. This paper provides a novel framework for drone Dataspace based on securing data-sharing in 6G for Industry 4.0 and Industry 5.0. According to the authors' best knowledge, this paper is the first to highlight how drones can play a vital role in improving real-time linked Dataspace platforms. In addition, we discuss advanced technologies for securing data-sharing among drones.

1.1. Motivation and contributions

This paper addresses safe and effective drone data-sharing in 6G networks, including protecting data, building trust in a decentralized system, handling communications among drones, lowering latency for real-time applications, processing massive data, and preserving the quality of shared models. This conceptual framework refers to Dataspace in the Sky, a novel decentralized platform designed for secure and efficient drone data-sharing in 6G networks. Dataspace in the Sky integrates advanced technologies such as Dataspace, BC, and FL to address scalability, data security, privacy, and real-time processing in diverse environments, including smart and harsh environments. The proposed framework reduces the burden of providing ground Base Stations (BSs) and increases network resource availability, thus raising QoS. A decision-making server carries out all problematic tasks to improve drone tasks such as data processing, load balancing, and resource allocation to optimize drone operations. As the requested services are near the users and dispersed among the drones based on their positions and loads, the strategy is based on user behavior predictions. Furthermore, a BC is implemented among the various parts of the proposed platform to store information and foster trust between individuals. The innovation of combining FL, BC, and Dataspace provides a safe, effective, and scalable drone data-sharing solution in 6G networks.

Accessing the cloud for applications and storage in network-congested areas presents various challenges, including network or server outages caused by the volume of users submitting requests simultaneously and sharing a finite amount of resources. Fast and effective service and data accessibility is made possible by having the data available and close to the users. The most frequently requested data can be kept on several devices near the end user, resulting in greater accessibility and reduced latency. DDS for drone Dataspace-based applications is motivated by several factors, including improved data access and quality, enhanced collaboration, increased efficiency, improved transparency and accountability, and better decision-making. Additionally, DDS provides decision-makers with a complete and accurate understanding of a given situation, leading to effective and efficient applications in agriculture, environmental monitoring, disaster response, and smart environment. The contributions of the conceptual framework summary are as follows:

1. The paper introduces a novel decentralized framework for securing drone data-sharing in 6G networks, combining BC, FL and Dataspace to enhances privacy, data-sharing efficiency, and trustworthiness while addressing the limitations of centralized data management systems.
2. We identify the requirements for Dataspace in the Sky through the design of a high-level platform for a real-time linked Dataspace. The proposed Dataspace in the Sky platform is designed to support efficient and secure data-sharing in both smart environments (e.g., urban areas, smart environments, and smart cities) and harsh environments (e.g., disaster zones, rural areas, and remote areas).
3. The proposed Dataspace in the Sky presents decentralized and secured drone data-sharing and management, leveraging Dataspace, BC, and FL in 6G. The framework proposes shows the vulnerabilities of centralized data management systems, ensuring security and privacy for Industry 4.0 and Industry 5.0 applications.

1.2. Paper structure

The rest of the paper is organized as follows: Section 2 presents the related work, while Section 3 describes an overview of core technologies. Section 4 represents the conceptual framework of the Dataspace in the Sky, while Section 5 validates the proposed framework. Section 6 discusses the challenges and future directions. Finally, Section 7 concludes the work.

2. Related work

With the benefits of transaction privacy, credibility, tamper resistance, and high dispersion, BC, a developing and promising approach in digital currency systems, may communicate data even without a reliable central server. For vehicle-to-grid networks, the authors of [38] introduced a BC-based privacy-preserving payment method that guarantees user payment data anonymity, which empowers data-sharing and secures sensitive data. However, transaction efficiency can be improved with BC technology's developments to satisfy the network requirements between vehicles and users. Furthermore, a BC-based system for medical picture retrieval with privacy protection was proposed [39]. The BC-based system's architecture was demonstrated and described for each layer. Furthermore, adding new applications to extend the proposed system can be considered to improve the system's efficiency. A safe, fine-grained access control system for data read and write operations was implemented for outsourced data [40]. Additionally, BC technologies are used to improve visibility and traceability. Even while BC substantially simplifies open and secure data-sharing scenarios, it is costly to construct a permissionless BC in resource-constrained drones or ground communication infrastructures [41]. Therefore, it is suggested that secure vehicular data-sharing systems [28] and spectrum trading [42] be developed using permissioned BCs, which quickly complete consensus mechanisms on pre-defined miners with low overhead. These systems are effective and especially useful for drones in 6G networks [42].

Compared to conventional data privacy protection tactics, a DL-based data privacy protection algorithm may further increase data availability and reduce the danger of data leakage. As a result, several great approaches for protecting DL privacy have been put forth. The authors of [43] introduced FL for privacy policy, which makes it stand out. Several contributors can obtain superior training results when training a DL model compared to their local models without submitting their raw data to a centralized server. To address the statistical heterogeneity problem of data in FL, it was used as an optimization approach [44]. The authors of [45] proposed personalizing FL could be accomplished more effectively by employing a local data structure to localize the global model. Nevertheless, because there are curious parameter servers and dishonest players, classic FL approaches still have privacy leakage issues. In [46], the authors showed that member inferring attacks could be used to discover private membership information. Passive and active inference attackers are assumed to be in both standalone and federated environments and various adversaries' prior information. However, the investigation's theoretical limits on the privacy invasion caused by DL in a white-box environment were not explicit. In [47], the difference between the virtual and real gradients was reduced using the depth gradient leaking procedure to access private data.

Securing privacy when gathering data is crucial since energy storage devices are decentralized, and the generated data is proprietary. The problem of multiparty data-sharing has recently attracted much attention. The authors of [48] offered a plan to securely exchange sensitive data on big data platforms for dispersed data streams. A secure process protection approach based on a virtual machine monitor and a proxy re-encryption algorithm based on heterogeneous ciphertext transformation was used to facilitate the implementation of system functions. However, optimizing the heterogeneous proxy re-encryption technique can enhance encryption efficiency. Furthermore, reducing communication overhead between parties involved can improve the functionality of the implemented system. For industrial IoT, the authors of [49] presented an accountable and effective data-sharing system called ADS that may penalize participants with data leaking issues. However, a BC-based responsible data-sharing system does not rely on off-chain protocols and has less computational and communication overhead. It is important to note that BC, a decentralized, unhackable, and traceable distributed ledger technology, uses consensus protocols to ensure data privacy and data exchange security effectively [50]. The authors of [51] introduced a BC-based edge computing trustworthy data management system called BlockTDM in response to data security and trust challenges in the edge computing environment. However, scalability and data storage off-chain can improve efficiency and processing time. In [52], the authors made the secure application and decentralized administration of massive data in the IoT possible using BC technology. On the other hand, a consensus mechanism that ensures the consistency of all participating nodes is essential and crucial technology.

By simultaneously optimizing the location of the drone, the trajectory of the unmanned underwater vehicle, and their interconnection, the authors of [53] introduced an energy-oriented target-hunting model. The proposed target-hunting issue is solved using deep Q-learning algorithms. The results demonstrated a trade-off between the system's interconnectivity and energy use. For drone-assisted disaster rescue, the authors in [54] introduced RescueChain, a safe and effective information exchange system. The simple BC-based architecture was constructed to protect data-sharing during catastrophes and immutably track bad actors. Designing Dataspace's benefits and approaches for solving challenges discussed [55]. While data providers retain their sovereignty, sharing data will result in services becoming assets. International Dataspace (IDS) offers a technological tool for developing data economies to exchange knowledge and data, following usage guidelines. The authors of [56] introduced and discussed how BC technology fits with IDS, focusing mainly on the fundamental principles underlying BC technology, the various design considerations for creating BC implementations, the meaning of smart contracts, and the overall potential of BC. Before presenting additions to data integration workflows for Dataspace support that goes beyond comparable efforts in data warehouses and data lakes, the authors of [57] outlined the benefits of FL for addressing the challenges of federated data integration in a case study scenario of mobility engineering.

According to the authors' best knowledge, no study addresses Dataspace in drones with supporting advanced technologies such as BC and FL for securing Dataspace sharing among drones. The proposed framework addresses the gaps and limitations by introducing a novel decentralized approach leveraging BC technology and FL. The framework enhances data security, trust, and accountability by leveraging BC. FL enables efficient data-sharing by allowing drones to exchange models instead of raw data, thus mitigating privacy risks. This combination provides a unique solution for secure and efficient drone data-sharing in 6G networks, addressing existing approaches' identified weaknesses and limitations. The proposed framework contributes to the research community by addressing privacy, decentralization, trust, and efficient data-sharing challenges, making it a novel and promising approach for secure drone data-sharing in 6G networks. Table 2 summarizes the most recent and related work to the proposed framework; it highlights technology requirements addressed by the framework.

3. Overview

3.1. Drones technology

The most famous drone services include publishing videos and images and broadcasting live videos. The forms of traffic are very resource-intensive on the uplink and impact the functionality of the entire network. Drone deployment with transceivers is viable for assisting with cellular infrastructure. Drone-BSs can be placed where needed to increase ground users' signal quality and expand cellular coverage [58,59]. However, because the drones will still receive the traffic and be routed to the closest BS, increasing coverage and connection quality will not lessen the strain on the BSs. Data filtering is one method that may be used to lighten the burden on cellular infrastructure. In this situation, the authors of [60] presented a platform to expand a 6G network slice for video surveillance utilizing a swarm of drones.

In [61], the authors formed a partnership between the drone and the Wireless Sensor Networks (WSN), utilized the drone to gather WSN data, and adjusted the drone's flight route in response to WSN feedback data to increase the WSN's data collection efficiency. Furthermore, the framework and communication protocol for the drone's airborne WSN introduced [62–66]. In addition to gathering data in a large-scale WSN, drone-based aerial data collection also addresses the issue of ground data collection limitations when ground transportation is problematic. The author of [61] employed cluster-based aerial data collecting. The network, comprised of the sensor nodes placed in the environment under observation, was separated into several cluster zones.

3.2. BC technology

BC, a distributed ledger among many users, enables efficient and permanent transaction recording with the utmost security and anonymity. Transaction verification is resistant to cryptography and can be added to the ledger by all participants in a BC without the requirement for a third party to validate and approve [67]. Public, private, and hybrid BC s are the three suBC ategories of BC s. In contrast to private BC s, which only let particular users have permission, public BCs (such as Ethereum and Bitcoin) enable everyone to join the network and participate. The benefits of public and private BCs are combined in the hybrid category, which comprises hybrid BCs. It offers members in the group privacy and openness. To offload computationally demanding BC tasks, the authors of [68] developed a BC -as-a-Service (BaaS) platform linked with MEC for IoT devices. A safe data collection system for MEC-enabled IoT networks is investigated [69], in which flying drones act as relay nodes for identity identification before transmitting data to MEC servers. In an air-to-ground IoT network, Zhu et al. [70] presented a BC-based decentralized fashion for data-sharing where a Cournot model is developed to maximize advantages for air and ground sensors. Smart contracts are self-executing contracts with the terms of the agreement directly written into code on the BC. Smart contracts automatically execute predefined actions when specific conditions are met, eliminating the need for intermediaries and enhancing efficiency and trust in transactions. Smart contracts are typically built using programming languages specific to the BC platform, such as Solidity for Ethereum.

3.3. Federated learning

FL is an ML technique that enables multiple parties to train ML models collaboratively without sharing their local data. FL influences data management, how other data science technologies interact with it, and increasingly, data sovereignty concerns, is a crucial technology for developing future data ecosystems. Data management is a significant challenge because of the following factors: (1) Organizations collect increasing amounts of heterogeneous data (such as business, economic, social media, and alternative data); (2) Data are stored in isolated data sets; (3) Organizations collaborate with partner organizations on analytics; (4) Organizations must secure the data; and (5) Organizations commercialize their data for their business, potentially as a new revenue source. Data technologies, including common digital IDs, data standards, data analytics, and data record technologies, are involved in information management with FL. The utilization of ML techniques for data-sharing in various environments is well established. However, FL brings a unique and novel approach to data-sharing among drones in the context of 6G networks.

Table 2
Summaries of the most related works.

Ref.	A	B	C	D	E	F	G
[48]	Securing sensitive data-sharing using proxy re-encryption approach	Yes	No	No	No	No	No
[49]	Highlighting an accountable and data-sharing approach for Industrial Internet of Things (IIoT)	Yes	Yes	No	No	No	No
[51]	BC for trusting data management	No	Yes	No	No	No	No
[56]	Designing Dataspace advantages and ecosystem approaches	Yes	Yes	No	No	Yes	No
[93]	Establishing theoretical principles and foundations of real-time linked Dataspace	Yes	No	No	No	Yes	No
This work	The requirements for Dataspace in the sky Highlighting the cutting-edge technologies needed to secure data transmitted through the Dataspace in the sky Providing a conceptual framework integration of FL and BC for drone data-sharing	Yes	Yes	Yes	Yes	Yes	Yes

A = Highlight, B = Data sharing, C = BC, D = FL, E = FL and BC, F = Dataspace, G = Dataspace in the Sky

3.4. Securing data-sharing

Transparency and openness policies encourage data-sharing by various organizations, including businesses and academic institutions. Technical advancement and related research on cooperative methods for sharing user data among organizations have intensified recently [71]. Data-sharing strategies must balance user privacy and a positive user experience while boosting business profits [72]. BC clarifies the quandaries surrounding when, what, and with whom to share data [72]. Additionally, BC facilitates how the data owner should be compensated as a perk for giving their information. However, collecting user data sparks serious privacy concerns, which either the organization addresses in the data privacy policy or by following the user activity tracked by internal audit [73]. Liu et al. [74] developed a collaborative architecture that integrates the Ethereum BC and deep reinforcement learning for effective data collection and safe data-sharing to suit the mobile crowdsensing-based Industrial IoT needs. The authors of [75] introduced a BC -authorized secure data-sharing architecture for dispersed parties in Industrial IoT applications. This technique strengthens the security of the sharing process without requiring centralized trust and includes cooperative learning in the approved BC.

3.5. Dataspace

Dataspace is a new paradigm for serving the data integration and usage requirements of smart nvironments, including the sharing of events and historical data. Dataspace approach acknowledges that producing an upfront unifying schema across all data sources in large-scale integration situations is challenging and expensive, which comprise thousands of data sources [81]. Dataspace focuses on supporting the co-existence of diverse data without requiring a significant initial investment to generate a unifying schema. Dataspace uses incremental strategies for semantic matching and mapping of source schemas. When tighter semantic integration is needed, it can be accomplished in a “Pay-As-You-Go” manner by more tightly integrating the relevant data sources. Dataspace has been developed to manage personal information [82], astronomical data [83], and biomedical data [84]. The utility of Dataspace has also been investigated in various settings such as data curation [85], context-based search [86], data modeling [87], data gathering [88], and customer feedback [89].

Dataspace can enable information management in highly dynamic environments, addressing the conceptual and technical obstacles to information interoperability. However, research has been limited to implementing the Dataspace concept in intelligent environments and examining the pertinent support services required for real-time data sources. Nevertheless, the creation of Dataspace has been attempted in the past in several contexts, including the system of systems [90], energy data management [91], and building data management [92]. Fig. 2 shows the example design of a Dataspace for real-time and linked data sources. Briefly, a Dataspace is a collection of data sources, typically organized and stored in a heterogeneous manner, to allow for efficient management, retrieval, and analysis. The term often emphasizes that data is a valuable resource that should be managed and treated as a collective information space rather than individual data points. It can help organizations and individuals better understand and utilize their data, making it easier to extract insights, make decisions, and drive innovation.

3.6. Dataspace 4.0 empowered industry 4.0/5.0

The Industry 4.0 paradigm’s technocratic emphasis on new technology and digitalization [6]. As a result, the discussion concerning the function and justifications for using the new paradigm was immediately sparked when the new industrial paradigm, Industry 5.0, appeared. Industry 5.0 is a supplement to the current Industry 4.0 paradigm that emphasizes the importance of the worker in the industrial process, as was highlighted during the COVID-19 pandemic. The authors of [76] analyzed the shifting Industry 4.0 toward Industry 5.0 with the assistance of virtual reality and augmented reality technologies, Industry 4.0 technologies enhance perception and prompt interactions, improve cybersecurity resilience [8], reduce mental workload, and improve data-sharing cognitive ergonomics [77]. In Industry 5.0, where diverse and autonomous networks cooperate, data exchange and control trust are essential. BC is a promising solution for creating transparent ledgers with easy control and managing industrial process data. A shared, distributed, and immutable ledger called BC makes it easier to track assets and record transactions in P2P networks. In addition, it creates dependable review tools that aid in compliance and auditing [78]. Consensus procedures play a significant part in the efficient management of the BC network and regulate the BC network’s scalability, node throughput, and mining delay. However, the resource-intensive PoW and PoS consensus models are inappropriate for responsive data-sharing in industrial operations. Therefore, in Industry 5.0 environments, low-powered consensus techniques like Reliable-Replicated-Redundant And Fault-Tolerant (RAFT), Tangle, and Directed Acyclic Graph (DAG) are primarily used; a permission BC is an ideal method for managing and orchestrating real-time data [79].

Industry 4.0/5.0 and Dataspace 4.0 are closely related concepts focused on creating a connected and intelligent system for managing data and optimizing operations in various sectors. Industry 4.0/5.0 aims to create a connected and intelligent system enabling real-time decision-making and optimization, increasing efficiency, productivity, and profitability. Dataspace 4.0 is a concept that builds on the principles of Industry 4.0/5.0, focusing on managing and sharing data [131,9]. Dataspace 4.0 is a connected and intelligent system for managing data, enabling secure and efficient data-sharing across various industries and stakeholders. The relationship between Industry 4.0/5.0 and Dataspace 4.0 is that they both aim to create a connected and intelligent system for managing data and optimizing operations. By leveraging advanced technologies such as the IoT, big data analytics, drones, FL, and BC, Dataspace 4.0 can provide a secure and efficient platform for sharing data among stakeholders, including companies, individuals, and gov-

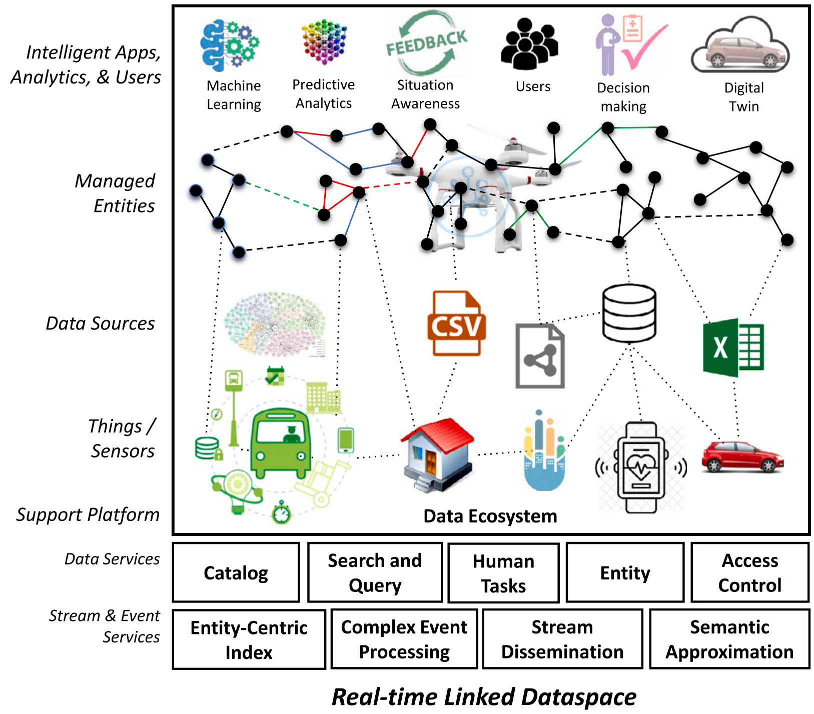

Fig. 2. Real-time linked drone Dataspace (Adapted from [93]).

ernments. Furthermore, Industry 4.0/5.0 and Dataspace 4.0 focus on creating a decentralized and distributed system where data is stored and processed locally, reducing the need for centralized data centers and minimizing the risk of data breaches or other security incidents.

3.7. Mobility dataspace through drones

The community for data-sharing where everyone tries to create and make available data for future mobility is considered the mobility dataspace. Such a Dataspace encourages competition around cutting-edge, ecologically responsible, and user-centric transportation solutions by providing all users equitable and transparent access to pertinent data. All users have exclusive chances within the mobility Dataspace to profit from the potential additional value of their data. The mobility Dataspace provides a framework where data suppliers may describe and regulate how and where others may utilize their data. Data users can be confident about the source and quality of their data thanks to this strategy, which also fosters data sovereignty and trust. The mobility Dataspace transforms into a digital distribution channel for data-driven business models by combining data from the public and commercial sectors via regional and national platforms, offering completely new choices for data collection, connection, and exploitation. With the creation of mobility dataspace, current data platforms will be connected, and access to sensitive mobility data and real-time traffic data will be available. Thus, it can offer specific mobility data at various levels in the future. Fig. 3 shows an overview of drone Dataspace for supporting various mobility events where drones gather data from different environments.

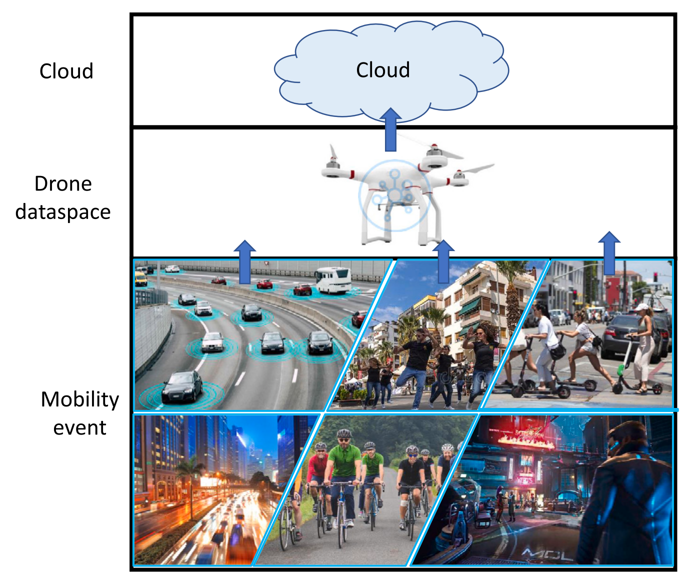

Fig. 3. Drone Dataspace supporting mobility events.

3.8. Smart environments

The construction and operation of smart environments are driven by capturing environmental data and enabling people to make meaningful use of that data. In the context of ongoing research in artificial intelligence and human-computer interaction, smart environments provide a viable source of innovation. Systems developed in this discipline are located, and their utility is derived from contextual awareness gleaned from the interpretation of sensor data. Therefore, IoT is the enabled technology for smart environments [94]. Furthermore, the authors of [95] introduced ML and IoT for smart environments focusing on challenges, applications, technologies and opportunities.

Drone plays a vital role in improving the smartness of smart cities [96] and smart transportation [97,98], etc. While the collaboration of multi-drone and Search and rescue teams is used for disaster management [30–32]. Moreover, BC technology is used to manage and decentralize multi-drone collaboration [99], empowering the security of drone swarm in a smart environment [100]. Moreover, the FL and BC combination helps improve drone edge intelligence performance in smart environments [101].

For real-time Dataspace important to improve smart cities applications, the authors of [102] explored how catalogs in Dataspace help satisfy this requirement; they then detailed how entity management services may be used to manage entity data more efficiently within a

Table 3
Role of technologies in the proposed framework.

Tech.	Role	Description	Benefits
FL	Preserve data privacy. Enables collaborative learning. Supports dynamic and decentralized environments.	Local model training without data-sharing. Aggregates global model from local updates. Updates models dynamically across nodes.	Privacy preservation. Efficiency in resource-constrained environments. Adaptability to network dynamics.
BC	Provides a decentralized and tamper-proof ledger. Ensures data integrity and transparency. Facilitates automated and secure transactions.	Records transactions securely and transparently. Cryptographically secures data transactions. Executes predefined rules.	Decentralized and trustless environment. Immutability and transparency of data. Automation of rules.
Data-space	Integrates and manages heterogeneous data sources. Supports incremental and flexible data integration. Enables context-aware data processing and decision-making.	Provides a unified view of disparate data sources. Integrates new data sources as they become available. Utilizes contextual information for data analysis and decisions.	Heterogeneous data integration. Flexibility and scalability in data integration. Contextual awareness for enhanced decision-making.

Dataspace. In [103], the authors presented a user experience paradigm for smart settings that the IoT enhances. The model was divided into two sections: the first focuses on digitalizing the environment using IoT and big data, and the second is human-computer interaction, focusing on the users' journeys using behavioral models and user experience design. The objective has been to involve users in IoT-enabled smart environments to raise awareness of, manage, and practice water and energy conservation. The authors in [104] discussed the function of a real-time linked Dataspace in facilitating the development of digital twins and assessing intelligent applications.

Smart environments include smart manufacturing, smart transportation, smart healthcare, smart cities, smart farming, and smart housing. As an illustration, a smart environment may receive information about water and energy consumption from sensors, transmit it to smart devices, and then allow users to adjust their water and energy use accordingly. Building and operating "smart cities" is driven by acquiring environmental data and enabling people to use that data meaningfully, sometimes changing behavior. IoT and big data, which enable the digitalization of physical infrastructures with sensors, networks, and social capabilities, are two fundamental technologies driving the development of smart environments. In addition, IoT-enabled smart environments can assist in creating resource management apps (for instance, for managing water and energy resources) for the environment. IoT sensors have been put in a few locations in smart cities to collect public data about traffic and human mobility. Data-driven learning is a sophisticated ML technique focused on data collecting, pattern recognition, and prediction. The authors of [105] examined how DL approaches have recently advanced in the construction of smart cities. Smart cities enrich human existence by offering various intelligent services to assist in managing many sectors, including traffic, transportation, healthcare and communication, increasing users' overall quality of life.

4. Dataspace in the sky framework

In this section, we discuss the conceptual framework of drone Dataspace with supporting technologies to facilitate secure data-sharing among drones to deliver services to multiple organizations and users. The role of technologies in the proposed framework is described with benefits in Table 3. Dataspace is a conceptual framework in data management that facilitates the integration of diverse data sources without needing a predefined schema, allowing flexible integration of heterogeneous data formats dynamically. However, Dataspace in the Sky extends this concept to drone networks and 6G networks, focusing on using drones equipped with smart sensors and communication capabilities to collect, process, and share data in real-time while securing data management in dynamic environments. The fundamental infrastructure for combining heterogeneous data from multiple drones and disciplines is provided by Dataspace. It maintains scalability and interoperability while enabling smooth and effective data transfer. Dataspace facilitates improved decision-making, more cooperation, and support for intricate, dynamic applications such as environmental monitoring, disaster response, and precision agriculture by decentralizing the organization and structure of data.

The proposed framework addresses the challenges (shown in Table 1) by leveraging a decentralized approach that combines BC and FL. BC provides a secure and transparent platform for DDS, ensuring data integrity, authentication, and access control. FL enables collaborative learning without sharing raw data, preserving privacy while allowing the generation of global models. We assume multiple drone collaborators will be involved in collaborative information modeling and sharing. Multiple drone collaborators work together to model the specified job jointly since each drone has data collection capabilities that can help train local models with the help of FL techniques. FL's model update procedure is decentralized at each drone, making it resistant to the failure of conventional aggregators. We employ the BC as the network architecture for the decentralized collaboration system to store, retrieve, and audit the collaborative modeling process to ensure data provenance and security. In this novel framework, we discuss the FL and BC combination to achieve data-sharing between drones Dataspace in a decentralized fashion. The high-level concept framework with architecture layers is shown in Fig. 4.

Smart environment layer: A smart environment consists of many smart devices that gather data from their surroundings and other sensing devices of numerous characteristics [106]. Smart devices collect perception data, which is then sent to drones for further analysis and sharing. In Fig. 4, the smart environment is a smart city composed of smart streets, smart traffic, self-driving cars, smart lights, etc. These devices gather data and send it to drones as they move closer to them. Drones equipped with their own smart devices can also gather data about the environment automatically. Therefore, drones have two functions here, either gathering data from smart devices deployed in smart environments or gathering data directly from smart environments.

Multi-resource layer: The smart environment has different smart devices that gather data for various purposes and in heterogeneous formats. Each data source should manage just one data source, a local database, a network source, or a file. Data sources may provide links for their potential applications and the core systems for executing basic data operations. Therefore, management of gathered data in drone technology is required to save energy [107], reduce latency and enhance the quality of service [108]. Multiple end-to-end applications competing for shared resources in a system with heterogeneous nodes, linkages, shared and constrained resources, and deployment in dynamic situations make delivering quality service challenging. The authors of [109] provide an initial solution to such a challenge in a multi-drone surveillance and target tracking program and support for system-wide end-to-end quality of service management.

A Dataspace in the multi-resource layer is a dynamic approach for organizing and managing multiple data sources. This involves creating a semi-structured and hierarchical organization scheme for data, with each source representing a different form and frequency of data. This al-

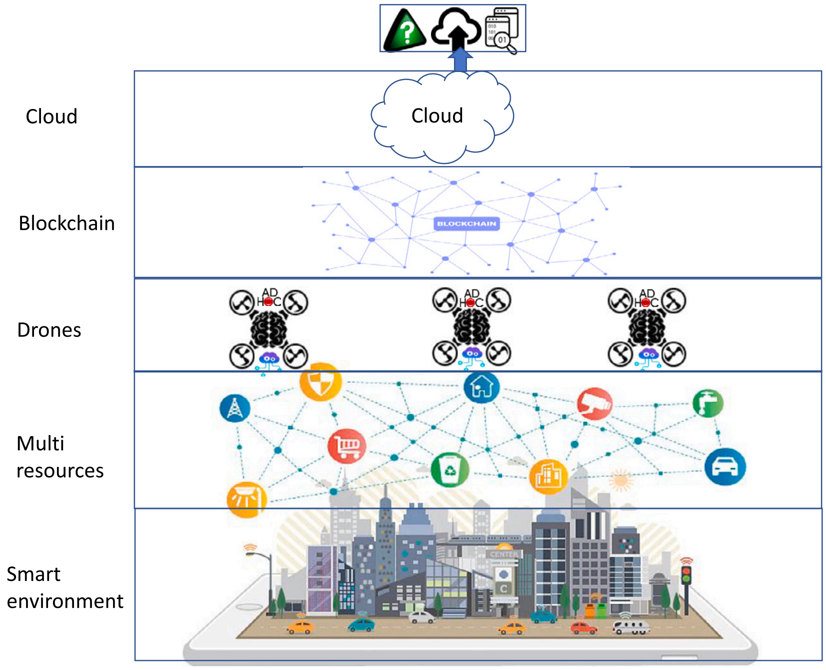

Fig. 4. Dataspace in the sky.

lows for more flexible and effective data management as needed by mobile drones and more accessible data access and analysis. For example, in a smart city environment, a Dataspace multi-resource layer could include data from multiple sources, such as traffic, weather, energy usage, and social media. Each layer would represent a different data source, making it easier to organize and manage the data and access and analyze specific data sets as needed. This elastic structure provides several benefits, including improved data management, greater data security, and more accessible data analysis. It also makes it easier to integrate new data sources into the Dataspace as they become available, helping to ensure that the Dataspace remains relevant and up-to-date. Briefly, a Dataspace approach to the multi-resource layer provides an organized and efficient yet pliable way to manage and analyze data, helping unlock the full potential of data and driving better decision-making and outcomes.

Drones layer: The drones offer mobile computing capabilities while flying closer to the smart environment, and they are responsible for gathering data. Drones' computing provides task scheduling, resource allocation, service allocation, and data collaboration related to BC and cloud layers for data-sharing. Drones must share information to avoid collisions and manage the drone coverage area. For instance, the Flying Ad-hoc NETwork (FANET) supports data gathering from smart environments in a data collection scenario, as drones may readily approach smart devices with low transmitting power. Therefore, data-sharing is vital in improving drones' performance and operation during task performance. In this layer, several technologies (i.e., BC, ad-hoc network, FL) are included for secure data-sharing among drones, clients, and the cloud.

1. **Ad-hoc networks:** Drones are considered one of the best ways to collect data in the Industrial IoT domain. Furthermore, Ad-hoc networks with flying drones significantly benefit from gathering data effectively, efficiently and collaboratively from large areas. Massive numbers of drones, also known as FANET, can be deployed to work together to complete complicated missions that are frequently impossible for a single drone to complete [110]. Furthermore, in [111], the authors created clusters that can enable cooperation that improves resource use efficiency and reduces the loss of secrecy compared to the individual drone. FANET use, nevertheless, also raises concerns about drone communication security. Drones depend on BSs to improve security, which can be easily attacked. Therefore, BC technology is the critical solution for decentralized, massive, and heterogeneous drones.

By improving network connectivity, drones assist the ground vehicle in sending data from one node to another. The authors of [112] presented a new architecture model for vehicle ad hoc networks to convey data and investigated various online and deceptive attacks on data distribution. In addition, in [112], the authors conducted a security analysis to determine the security objectives and examined several fake attack strategies on data dissemination. In drones, the architecture uses BC, which uses a proof-of-stake consensus protocol for block validation and uses game theory to identify the forger node [113]. Therefore, the authors of [114] presented increases in the drone swarm's transmission efficiency and coverage capacity while also analyzing the interference brought by drone communication.

In a drone Dataspace, an ad hoc network supports data transfer and communication between drones, enabling real-time data-sharing and collaboration. For example, in a disaster response scenario, a drone could use an ad hoc network to share images and video in real-time with other drones and response teams on the ground, helping to direct response efforts and allocate resources more effectively. Ad-hoc networks provide several benefits in supporting drone Dataspace, including increased flexibility and scalability, as the network can be easily reconfigured and expanded to support changing needs and requirements. They also provide improved reliability and availability, as communication can be maintained even in the event of a failure in the central infrastructure.Table 4 comparing the advantages and drawbacks of different communication technologies. 6G networks are vital for real-time drone operations and data-sharing because of high throughput, ultra-low latency, and improved dependability. Drone networks have demanding applications that have 6G's capabilities, including high-speed data transfer, enormous IoT integration, and real-time decision-making. 6G offers the infrastructure required to manage drone networks' scalability and dynamic nature, especially in intricate settings like smart cities or disaster areas.

Table 4
Advantages and drawbacks of communication technologies for supporting proposed framework.

Technology	Advantages	Drawbacks	Potential Impact on Time-based BC Errors
P2P Networks	Decentralized, Self-organizing, operating without infrastructure	Scalability challenges, Security concerns, Resource management issues	Potential delays in block propagation or increased chances of forks in the BC
5G	High data rates, Low latency, Massive connectivity	Requires infrastructure, Coverage limitations in remote areas	Reduced chances of data inconsistencies or delays in the BC
6G	Hyper-connectivity, Extremely low latency, High energy efficiency, High reliability and availability	Currently in the developmental stage, May require new infrastructure and technologies, Regulatory challenges	Potential improvements in overall BC performance, but subject to future development and implementation

2. **FL:** FL is undoubtedly helpful for data privacy in ML and analytics over drones. First, FL requires less communication since it just sends updates, whereas sending local data to a central server increases network traffic and storage expenses. Second, there is less data leakage since the local client's dataset is never transferred to the server. The benefit is that model training is no longer directly dependent on having access to raw training data [115]. By reducing the attack surface to only the device rather than the device plus the cloud, FL can considerably lower privacy and security risks for applications where the model training aim can be determined based on data accessible to each client [115]. However, there are still additional FL-related problems; malicious actors may try to access the client's dataset or compromise the global model. The client's lack of desire or incentive to work with the FL system can also become an issue. Adopting and utilizing BC technologies for FL applications might solve this problem.
   By enabling drones to work together to build models without sharing raw data, FL addresses security and privacy challenges and makes decentralized possible. This is vital to protecting private information while using drones by sending model updates instead of big datasets.FL uses less bandwidth, which is crucial for drone networks to process data in real-time and with low latency. In a drone Dataspace, FL can improve the performance of drone algorithms, such as autonomous flight and object recognition. For example, each drone could collect data about its environment and share its model parameters with a central server, where a shared model is built and updated. All drones can then use this model in the network to make decisions and improve performance.

BC layer: We categorize the transactions in the BC database according to the level of privacy to offer fine-grained data-sharing services. Public data, community public data, and encrypted data are included in the privacy levels in decreasing order. Public data in this context refers to data visible to all nodes, community public data to data visible to all nodes within the same community, and encrypted data to data that is primarily private or that users desire to buy or sell. For more users who need the data to see them, they will set the data privacy level to public data in the community when they contribute professional data. BC guarantees the data-sharing process's integrity, transparency, and reliability. For verify the contributions and validity of shared data and model revisions, it offers a safe and unchangeable digital ledger. BC is vital for avoiding tampering, fostering stakeholder confidence, and facilitating dependable data management in a decentralized system like Dataspace in the Sky.

When it registers a BC account, a drone receives a unique identification. Data acquired by the 6G drone before it is transferred to the cloud can be encrypted in two ways. One method involves the drone encrypting the data with an allocated symmetric key and sending the ciphertext to the node management. The node management then encrypts the key using attribute-based encryption. The second method involves the drone randomly generating a key, encrypting the data with it, and then using attribute-based encryption to encrypt the key. The system's public and master secret keys can be generated by the trusted authority acting as the system's central hub for tasks like initialization and secret critical production. A user is capable of decrypting and reading gathered data and instructions.

The following describes the secure data-sharing procedure for 6G drones based on the BC, as shown in Fig. 5. First, the drone encrypts the symmetric encryption key and the data it has acquired using symmetric encryption. The drone then requests data to be uploaded from the BC. Following receipt, the BC verifies the request using a pre-negotiated smart contract. The BC provides the drone with a credential if the request is legitimate. The drone uploads the ciphertext and the credentials to the cloud as soon as it receives them. When the ciphertext is determined to be legitimate, the cloud saves it and notifies the BC of the storage confirmation. The distributed ledger of the BC stores the shared ciphertext data as transactions. The BC will employ smart contracts to confirm a data consumer's identity and determine whether his or her attributes comply with the ciphertext's access policy if the data consumer (a drone or user) requests access to the ciphertext. An access credential is returned to the customer if their identity is real and their qualities comply with the policy. The user can then use the credential to access the ciphertext in the cloud. The 6G drones' BC-based data-sharing protocol ensures secure access to encrypted cloud data. The BC system checks the identity and characteristics of a drone or user requesting access to ciphertext against pre-established regulations. An access certificate that grants access to the ciphertext is granted if the identity is authentic and the attributes meet policy requirements. The access credential is blocked, preventing unwanted access to the encrypted data if the identity is false or does not comply with policy standards. Within 6G drone networks, data integrity and privacy are protected by this stringent verification procedure.

The conceptual framework of drone Dataspace includes the network, FL, task, mobility, communication, and threat models. The BC-empowered FL for Dataspace in the drone-assisted MCS scenario is depicted in Fig. 6 and comprises several drones, task publishers, MEC nodes, BSs, and a consortium BC. Therefore, data owners and requestors can share data quickly and reliably while storing the sharing records on the BC for tracking.

Cloud: The cloud processing layer handles the data storage and heavy lifting involved in drone computing. For global model aggregation, the cloud gathers the local model parameters from each drone and delivers the updated global model parameters. Monitoring the resource availability of incoming smart devices at various network tiers is necessary for resource management [116]. Adding a layer of drones between the cloud and consumer devices can help with this monitoring. In wireless networks, FL training models have been researched when the local FL models are relayed to the cloud, aggregating all of the local FL models and keeping the global FL model in the cloud [117]. Table 5 describes the proposed framework solutions and their benefits for drone DSS. Table 6 illustrates the comparison of the proposed framework with well-known competitors, advantages, and drawbacks.

Combination of technologies and applications: The combination of technologies (i.e., FL and BC and drones) creates a decentralized drone Data-sharing solution that increases security and privacy for shared data. In the proposed framework, each drone would contribute

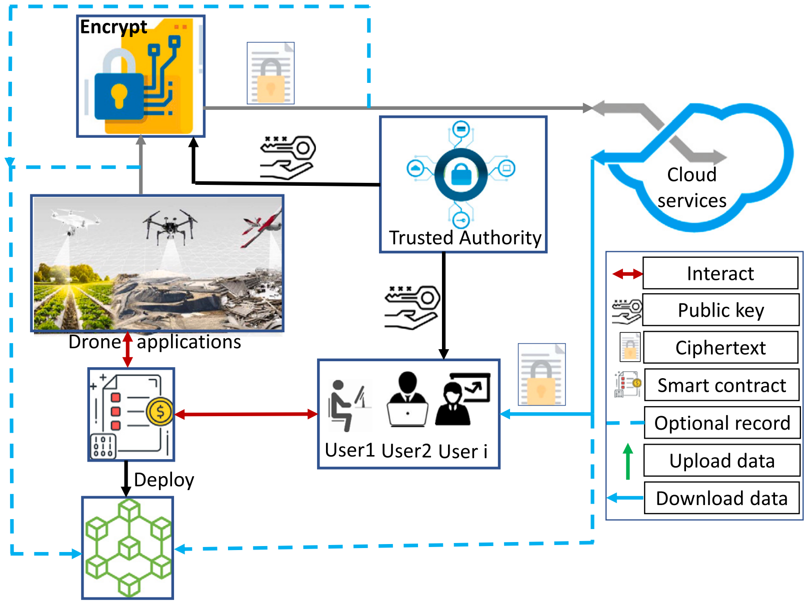

Fig. 5. BC enabling securing Dataspace sharing in the sky. .

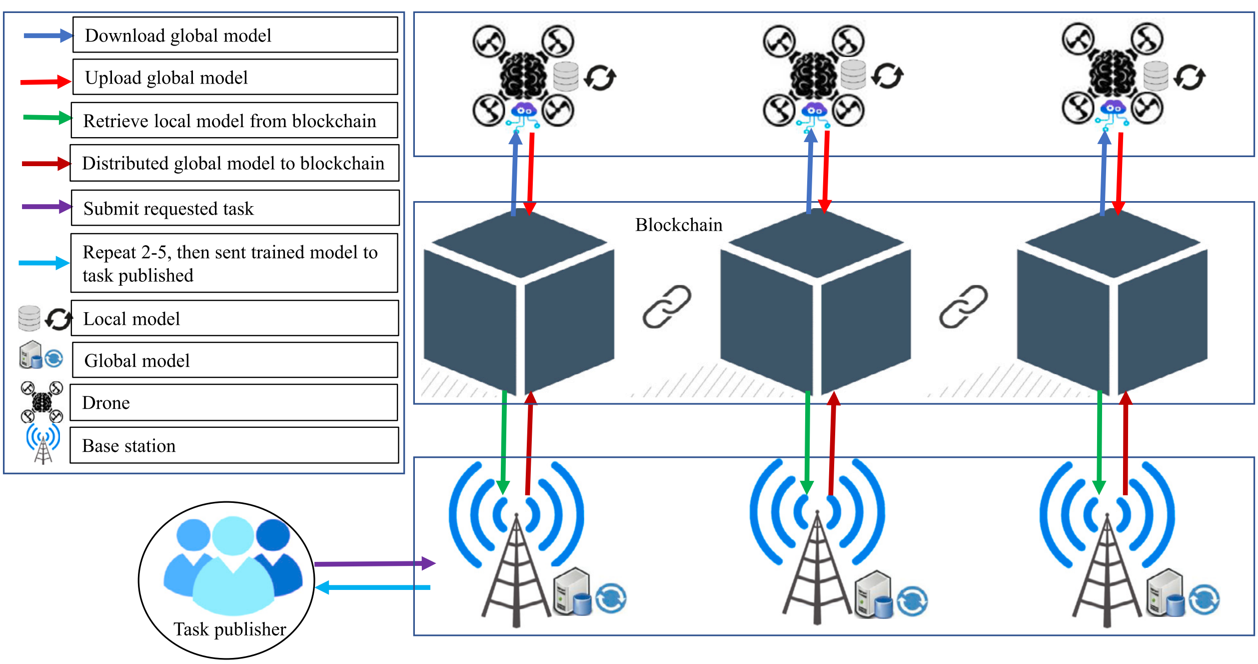

Fig. 6. Combination of FL and BC for data-sharing and processing.

to a shared model through FL, which is updated and refined as more data is collected. The updates to the model would be recorded on a BC, creating an immutable and secure ledger of the model's evolution. Additionally, this setup increases transparency and trust, as all network participants can see the model updates and verify their authenticity.

5. Evaluation of proposed framework

In this section, we evaluate the proposed Dataspace in the Sky to secure data-sharing decentralized using multi-drone to support Dataspace 4.0 in Industry 4.0 and Industry 5.0 applications. The main objective of combining BC and FL is to facilitate distributed drones' secure collaboration. All miners may independently verify the quality of models uploaded and stored on the BC thanks to the decentralized accountability system. Table 7 summarizes the benefits with descriptions of technologies mapped to the stated framework criteria.

5.1. Evaluation based on existing data-sharing framework

Relevant literature and research that support the validation of the proposed framework include drone-edge-assisted secure data-sharing for 6G and beyond [23], research on a BC-based framework for safe and efficient data-sharing in the Internet of Vehicles [132], and a decentralized framework for secure data-sharing and privacy preservation in smart communities [133,134]. The proposed framework is based on a decentralized architecture leveraging BC. The decentralized approach eliminates the need for a central entity and enhances data security, integrity, and immutability. In contrast, traditional centralized approaches to drone data-sharing may have limitations regarding data

Table 5
Proposed framework solutions and benefits.

Proposed solution	Benefits	DDS	Security
Drones Dataspace	Flexible and mobility, High-quality data, Provide services close to the user, Efficient data management	NA	Traditional methods, Vulnerable to attacks
BC	Trust among drones	Decentralization to improve drones collaborations	High
FL	Training model's of collected data	Support decentralized	High
Ad-hoc networks	Support P2P network	Yes	Little protection and encryption required for providing security
FL and BC	Federated, No single point of failure, Creating trust among drones and servers, Improving the scalability of drones intelligent computing networks	Support decentralized and P2P collaboration	High security
Combination of technologies	Improved data privacy and security, Increased transparency and trust, Increased scalability and decentralization, Improved accuracy and performance, Efficient data-sharing	Support decentralized drone data-sharing	Efficient and high security and privacy

Table 6
Comparison of the proposed framework technologies with well-known competitors.

Competitor	Advantages	Drawbacks
BC	Decentralized and transparent data sharing, Immutable and tamper-proof records, Consensus-based decision making	High computational overhead, Scalability challenges, Potential for forking and double-spending attacks
PKI	Centralized and well-established approach, Efficient management of digital certificates and keys, Widely used in various applications	- Single point of failure, Vulnerability to certificate revocation and key compromise, Lack of transparency and accountability
FL	Decentralized and privacy-preserving approach, Collaboration among multiple parties, Retains data ownership	Communication and synchronization overhead, Heterogeneity of data and models, Complexity in coordination
Cognitive Networks	Utilizes ML and AI techniques for optimized resource allocation, Dynamic adaptation to changing network conditions, Enhanced decision-making capabilities	Complexity in implementation and management, Privacy and security concerns, Limited scalability
Datastore vs DNS/mDNS	Efficient data retrieval and storage, Widely used for data-sharing and discovery, Scalable and robust	Centralized or distributed data storage, Limited support for data integrity and security, Reliance on DNS or mDNS infrastructure
Publish-Subscriber Servers	Scalable and efficient data dissemination, Decoupling of publishers and subscribers, Supports dynamic and flexible data sharing	Reliance on central servers, Potential for a single point of failure, Scalability challenges
Proposed framework	Integration of FL, BC, and Dataspace for secure, efficient, and scalable data sharing, E2E encryption and privacy-preserving model sharing	High complexity in implementation and management, Synchronization and communication overhead, Coordination of heterogeneous data sources

Table 7
Combining FL and BC for drone Dataspace.

Benfit	Description
Improved data privacy and security	By using FL, the data remains on the local devices and is only shared in an encrypted form, the updates to the model are recorded on the BC, providing a secure and transparent record of the model's evolution.
Increased transparency and trust	BC is easier to build and maintain a community of trusted participants who can collaborate on improving the model and the drone Dataspace.
Increased scalability and decentralization	Combination of FL and BC improves the drone Dataspace to many participants in a dcentralized fashion.
Improved accuracy and performance	FL enable the model to be trained on a more extensive and diverse dataset, improving its accuracy and performance and allowing for the continuous improvement of the drone Dataspace.
Efficient data-sharing	By using BC, it is secure and efficient to share data between participants, even in large and complex networks.

Table 8
Comparison of the proposed framework and traditional centralized data-sharing.

Aspect	Proposed framwork	Traditional Centralized Data Sharing
Architecture	Decentralized using BC	Centralized
Access Control	Fine-grained through smart contracts	Coarse-grained
Transparency and Trust	Transparent and auditable through consensus	Trust placed on a single entity
Security	Tamper-proof data storage and smart contracts	Reliance on a single entity, potential risks
Adaptability to 6G and Dataspcae 4.0 Environments	Tailored for 6G and Dataspcae 4.0 environments	May not be optimized for specific requirements

privacy and single point-of-failure risks. Table 8 compares the proposed framework and traditional centralized data-sharing. The proposed framework uses smart contracts to govern drone data-sharing. The smart contracts enforce fine-grained access control mechanisms, ensuring only authorized entities can access and share data, enabling a more robust and governance-enabled solution than P2P approaches that may need more unified governance mechanisms.

6G and Dataspcae 4.0 Focus: The proposed framework addresses the challenges of secure drone data-sharing in 6G and Dataspcae 4.0 environments. The advanced environments pose unique challenges, such as high data volume, high data velocity, low latency, and diverse data sources. The framework's decentralized approach, use of BC, and smart contract-based governance provide innovative solutions to these challenges. The proposed framework ensures data security through BC, which provides tamper-proof and transparent data storage. Addition-

Table 9
Proposed framework evaluation and validation.

Requirement	Enabled by
Data collection	Smart devices in smart environments
Data processing locally	FL techniques
Local model	Drones
Global model	Dataspace
Authentication	BC technology
data-sharing	BC and Fl
Decentralized	FL, BC and ad hoc networks
Collaboration	BC and consensus algorithms

ally, the framework's access control mechanisms, enforced through smart contracts, ensure that only authorized entities can access and share data. Therefore, it enhances the overall security of drone data sharing, protecting against threats such as data breaches, tampering, and unauthorized access. The decentralized architecture and use of BC in the proposed framework enhance resilience against potential threats and attacks, such as data breaches, data tampering, and unauthorized access. The proposed framework improves the overall security and reliability of drone data sharing, ensuring the integrity and confidentiality of shared data. Table 9 describes the proposed framework evaluation and validation.

Decentralized Dataspace sharing in drones : Drones must collaborate and share tasks to share data and take appropriate action. To (1) maintain trust among P2P networks [118], (2) enable traceability across drone networks [80], (3) provide insightful consensus-based decision-making processes [119], and (4) deliver efficient solutions by utilizing the decentralization feature of BC technology [120], it is advantageous for Dataspace sharing among drones to use BC technology. The shared data is divided among the multiple drones covering an event in the Dataspace in the Sky framework solution. Many drones are often employed to cover different areas in an active region to give the highest service performance because drones can connect and work together by sharing resources. In [113], the authors presented a model-based BC distributed network to secure drone communication for data gathering and transfer. Furthermore, an effective and safe data-sharing system was proposed [121]. The system used label data to categorize customers to deliver more granular data-sharing services. Achieving effective and secure data-sharing involves four stages: initialization, identity authentication, signature and verification, and then data sharing.

Drone data-sharing aims to transfer data over a shared environment to serve end users based on drone computing networks. Therefore, it is crucial to offer dependable and scalable drone data-sharing solutions in 6G to satisfy Industry 4.0 and Industry 5.0 expectations. Drones data-sharing can be made possible by combining BC and FL for high-security capabilities. Each drone explicitly serves as an FL client to communicate data collaboratively with an aggregate cloud. Drones can request data-sharing from the cloud for various services, including traffic flow estimates and path selection. To manage the data-sharing requests from drones with a Deep Reinforcement Learning (DRL) method for sharing cost minimization, the cloud converts the data-sharing process into a computing task from linked drones. An immutable BC ledger is installed on the drone network to execute the verification of model parameter updates and store them in blocks in a decentralized way, specifically to ensure the security and dependability of the drone's data-sharing. The combination of FL and BC offers data-sharing among multiple drones during activities in smart environments to satisfy Industry 4.0 and Industry 5.0 needs.

The data management system distributes the data among the drones based on their location and storage capacity. BC and metaheuristic approaches used for drone data optimization and management in fog computing paradigm [122]. Therefore, drones perform data gathering, optimizing, managing, scheduling, preservation and processing in high-level security in the fog computing paradigm. The drones need to share data to satisfy and respond to end-user requirements; the drone itself or a nearby drone may be able to provide the requested information. If not, the drone uses the cellular network to send the request to the proper clouds. As a result, the cloud can provide incoming users' data and service requirements.

The most popular services during packed events are real-time and video streaming of movies and images. However, these forms of traffic are very resource-intensive on the uplink and hurt the entire network's performance. Users and IoT devices produce delay-tolerant traffic, which may be locally stored in a drone and sent to the target after an activity. The drone must divide the data it receives into data that should be processed at the drone level delay-tolerant traffic and data that should be sent to higher levels for processing, i.e., cloud. (Fig. 7). The drone stores delay-tolerant traffic and transmits the final destination afterward. Due to drones' restricted computational and storage capabilities, a specific amount of space is set aside for delay-tolerant traffic. When the drone's capacity is reached, it treats the delay-tolerant traffic like regular data and sends it straight to the network. Due to its battery, each drone can only fly for a certain amount before recharging. When this happens, the drone travels to the closest charging station, distributes the stored delay-tolerant traffic, and is replaced by a new drone. The drones are linked to the cloud through the cellular network. Multi-dorne is dispersed over an event area, and the acquired data is divided according to their positions. Each drone offers coverage to a set of users (different altitude has different coverage areas [29]) and, when practical, responds to their inquiries using information either collected locally or by another drone in the swarm. To ensure continued service, each drone is sent to the charging station before its battery runs out and replaced immediately by a different drone.

Dataspace is dynamically chosen and disseminated across the many drones scouring the congested region in the suggested system. The cloud decides whether to manage depending on its forecast of service requests from future users. The most common user requests processed locally by drones or transmitted to other clouds are reported by drones [123]. The cloud forecasts future service demand (for instance, for a particular database or piece of online content) using a DL-based long-short-term memory [124]. By handling some of the requests locally, deploying drone capabilities between the cloud and the users reduce the strain on the uplink. For example, a drone divides a busy area into several smaller areas, increasing the number of resources available to nearby users. Drones receive all requests; some are handled locally, while others are routed to the serving cloud. As a result, the infrastructure load can be decreased, and uplink resources can be released, enhancing network performance. In addition, the collaboration of multiple drones boosts the drone's storage capacity and speeds up response times.

The proposed framework's potential impact on real-world drone applications includes cost savings and improved efficiency and capabilities. By enabling secure and efficient data-sharing among multiple drones, our framework can reduce the need for redundant data collection and processing, leading to significant cost savings. Additionally, by leveraging advanced technologies such as 6G networks, FL, and BC, our framework can provide more accurate and robust models to enhance drone capabilities and improve mission success rates. Furthermore, the proposed framework can enable more efficient use of resources, including drones, sensors, and computational power, by enabling collaborative modeling and sharing models instead of raw data, leading to more effective resource allocation and utilization and increasing overall efficiency and productivity. The ability to securely share data among multiple drones in a decentralized fashion opens up new possibilities for collaboration and coordination, allowing drones to work together to achieve common goals and solve complex problems. The proposed framework has significant potential to transform how drone applications are designed, deployed, and operated, improving cost-effectiveness, efficiency, and capabilities and enabling new use cases and applications.

The uniqueness of the proposed framework lies in its decentralized methodology and the incorporation of FL and BC technologies, which have the potential to address the security and privacy concerns in drone

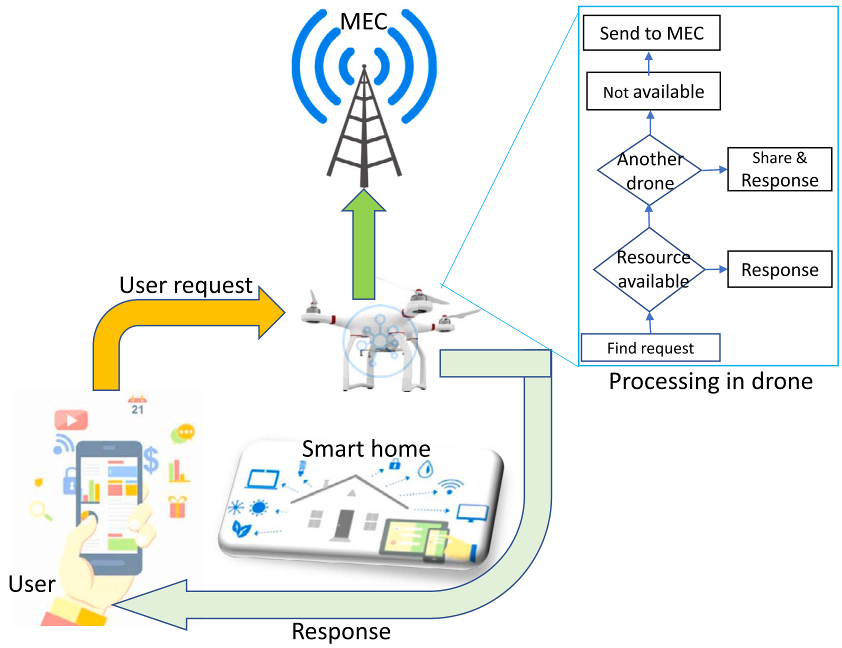

Fig. 7. Data-sharing and processing in drone. .

Table 10
Evaluation metrics for framework validation.

Metrics	Description
Data privacy and security	Privacy and security provide to protect sensitive data from unauthorized access or modification.
Model accuracy	Model accuracy generated evaluate how well the models can perform in real-world scenarios.
Communication overhead	The communication overhead introduced how messages are sent between drones, the amount of data transmitted, and the time taken to transfer data.
Scalability	Scalability measures how well the framework can handle an increasing number of drones and data sources.
Resource utilization	The resource utilization includes the CPU, memory, and storage used by the drones during the collaborative modeling process.

data-sharing and collaboration. In addition, cost savings, increased effectiveness, and new capabilities are potential effects of the framework on real-world drone applications. The evaluation criteria of the proposed framework are security, scalability, privacy, speed, and ease of use, as shown in the Table 10.

6. Validation-based use cases

Validation is based on testing the framework in a variety of scenarios, such as precision agriculture, environmental monitoring, and disaster response. Combining FL and BC for decentralized drone Dataspace involves creating a platform for drones to share data while preserving the privacy and security of the data. The updates to the model are then aggregated on a central server, and a new model is sent back to the participating drones for further training.BC technology ensures that the updates to the ML model are recorded and verified and that the data shared by the participating drones are stored securely and transparently.

1. **Precision agriculture:** It uses technology to optimize agricultural production while reducing waste and environmental impact. Drones collect high-resolution data on crop health and growth that is difficult or impossible to obtain from the ground. By combining FL and BC for drone's Dataspace sharing, drones can share data without compromising the privacy and security of the data or the drones themselves. In addition, drones can use FL to collaboratively train ML models that can analyze the data and identify patterns and trends.
   ML models can then be used to optimize crop management by providing insights into the health and growth of the crops and suggesting improvements to the management practices. For example, the models might identify areas of the field that require additional watering or fertilizer or suggest changes to the timing or type of crop treatments. Farmers can increase crop yields by optimizing crop management while reducing waste and environmental impact. For example, by using data to apply water and fertilizer only where it is needed precisely, farmers can reduce the resources they use while still achieving high crop yields. This can lead to cost savings for farmers and more sustainable agricultural practices overall.
2. **Disaster response:** Drones are becoming increasingly used to support disaster response and recovery efforts, as they collect high-resolution data on disaster-stricken areas quickly and efficiently. The data can include images and videos of the affected areas. By combining FL and BC for drone data-sharing, drones can share this data with other organizations involved in the disaster response effort. data-sharing can enable a more coordinated and effective response, as different groups can work together to identify areas of need and prioritize their response efforts. For example, the ML models might identify areas particularly hit by disasters or areas with large numbers of people needing assistance.
   The analysis can then be used to optimize the delivery of aid and resources to the affected areas. For example, the models might suggest the most efficient routes for delivering supplies or the best locations for setting up temporary shelters or medical clinics. By using drones and ML models to optimize aid delivery, disaster response organizations can improve the effectiveness of their response efforts and help more people in need. This can lead to more efficient and cost-effective disaster response and recovery efforts and better outcomes for the communities affected by the disaster. Combining FL and BC

Table 11
Description of proposed framework and traditional centralized data-sharing.

Technology	Description of the technology-empowered use cases
Drones	Remote sensing and monitoring of crops, soil, and weather conditions for precision agriculture management. Remote sensing and monitoring of environmental parameters, such as air quality, water quality, and wildlife habitats. Disaster reconnaissance, damage assessment, search and rescue operations, and situational awareness in disaster-affected areas.
BC	Provides security, transparency, and accountability in data management, ensuring data integrity, preventing tampering or unauthorized access, and providing a verifiable and auditable record of data transactions, ensuring data integrity, preventing tampering or unauthorized access, and providing a verifiable and auditable record of data transactions.
FL	Collaborative model training on precision agriculture data stored in the drone dataspace, preserving data privacy and security and enabling improved decision-making for precision agriculture management, environmental management, and disaster response and recovery.
6G	Enables advanced communication and networking capabilities, such as URLLC, mMTC, and network slicing, for improved data exchange, communication, and coordination among drones and Dataspace for precision agriculture, environmental monitoring, and disaster response components.
Combination	Combination for DDS for precision agriculture, including drone data, sensor data, and situational awareness information.

for drone Data-sharing optimizes disaster response efforts by allowing drones to share data and train ML models to help identify areas of need and optimize aid delivery. This can lead to more efficient and effective disaster response efforts and better outcomes for the communities affected by the disaster.

3. **Environmental monitoring:** Drones are becoming an increasingly important tool for environmental monitoring, as they can collect data on environmental conditions quickly and efficiently. For example, drones can collect data on air quality, water quality, and other environmental factors that affect human health and well-being. By combining FL and BC for drone Data-sharing, drones can share this data with other organizations involved in environmental monitoring efforts. This can enable a more coordinated and effective response to environmental issues, as different groups can work together to analyze the data and identify patterns and trends.
The analysis can then develop targeted interventions to address environmental issues. For example, environmental monitoring organizations might use the data to identify areas where air quality is inferior and deploy air purifiers or other mitigation measures. Similarly, water quality organizations might use the data to identify sources of pollution and develop strategies to reduce pollution in those areas. By using drones and ML models to analyze environmental data, environmental monitoring organizations can improve their effectiveness and help protect human health and the environment. This can lead to better environmental outcomes and a healthier planet overall. Table 11 describes how technologies are used in the proposed framework in the use cases.
Drones, FL, BC, and Dataspace all function well together when included in the "Dataspace in the Sky" architecture for environmental monitoring and protection. The drones can gather important information about different species' health indicators, movement patterns, and population counts. FL is used to analyze massive quantities of data and identify patterns in biodiversity, habitat quality, and wildlife behavior across time. FL protects animal whereabouts and activities by combining information from several sources without centralizing sensitive data. Furthermore, BC technology makes observations and study findings more transparent and tamper-proof, which improves the validity and dependability of wildlife monitoring data. This guarantees the accuracy and reliability of the data used in ecological research and policy-making. Additionally, integrating Dataspace makes it easier for various stakeholders, such as government agencies, conservation groups, and wildlife researchers, to share data securely and effectively. Dataspace promotes informed conservation plans and biodiversity management activities by facilitating smooth cooperation and information exchange while maintaining data privacy and integrity.
4. **Smart City:** When applied to smart cities, this framework transforms traffic management by utilizing drones outfitted with high-definition cameras and sensors to collect data in real-time on traffic patterns, incidents, and road conditions. Edge computing is used to process this data locally without depending on centralized servers, reducing latency and facilitating quick decision-making. By training traffic prediction models using dispersed datasets from several drones, FL algorithms improve traffic prediction models while protecting data privacy by sharing models rather than transmitting raw data. This method enhances total urban mobility by rerouting traffic to minimize congestion and optimizing traffic light timings.
The framework improves emergency response and surveillance in the field of public safety. Drones with cameras and sensors track public spaces in real-time, looking for safety concerns like shady activity or big crowds. Video feeds and environmental indicators are among the data that are gathered and safely incorporated into a Dataspace. BC technology creates an unchangeable record of transactions to guarantee the validity and integrity of this data. Drones give first responders crucial situational knowledge during crises, such as natural disasters or security events, allowing them to allocate resources effectively and coordinate response activities. The "Dataspace in the Sky" paradigm shows excellent promise to revolutionize public safety and urban administration by providing scalable solutions that improve resilience, safety, and efficiency in smart city environments.
5. **Healthcare Medical Supply Delivery:** The "Dataspace in the Sky" architecture brings revolutionary possibilities to the healthcare field, especially in remote medical diagnostics and supply distribution. First and foremost, drones are essential for quickly and effectively delivering vital medical supplies to remote or disaster-affected locations. Drones with sophisticated navigational technology can quickly transport emergency supplies, pharmaceuticals, or vaccinations across large geographic distances. With the help of BC technology, medical supply traceability and transparency are guaranteed along the delivery chain, giving authorities and healthcare professionals up-to-date information on the whereabouts and state of the goods. This openness improves the entire logistics of healthcare delivery by reducing the loss, theft, and improper management of vital medicinal materials.
In remote medical diagnostics, drones fitted with imaging and medical sensors can completely transform the availability of healthcare in rural or underdeveloped areas. The UAVs gather health information from people in real-time, including environmental parameters, diagnostic pictures, and vital signs. The gathered data is safely sent to medical institutions or specialist diagnostic laboratories for analysis and interpretation. By combining and evaluating data from many sources, FL algorithms allow for the development of reliable diagnostic models without jeopardizing patient privacy. Even in distant locations with limited access to specialist medical knowledge, healthcare professionals create precise prediction models and therapy suggestions catered to the requirements of specific patients by utilizing FL.
6. **Infrastructure Inspection and Maintenance:** Dataspace in the Sky architecture provides notable advances in infrastructure in-

spection and maintenance in power line and pipeline inspection and construction site monitoring. First, drones with specialized sensors and cameras are essential for performing thorough and frequent inspections of vital infrastructure, such as electricity lines and pipelines. Large sections of pipelines or electricity lines may be independently traversed by these drones, gathering high-resolution data and pictures that are essential for spotting any problems like leaks, corrosion, or structural flaws. By guaranteeing the accuracy and unchangeability of inspection data, BC technology offers an open, unchangeable record of all conclusions. Ensuring the accuracy and dependability of inspection reports is crucial for preserving the safety and dependability of infrastructure networks. Additionally, by combining insights from several inspection data sources without sacrificing sensitive operational information, FL algorithms may be used to enhance predictive maintenance models and defect detection constantly.

Regarding monitoring construction sites, drones with cameras and sensors give stakeholders and project managers access to real-time updates on the project's status, providing insightful information. Drones allow construction teams to monitor site operations, check progress against schedules, and evaluate adherence to financial limitations by taking aerial imagery and data. Dataspace real-time monitoring data may be seamlessly integrated with other project management systems and tools, such as budgeting and scheduling software. The integration improves decision-making skills by providing a thorough and consolidated perspective of project progress, resource allocation, and possible hazards. Moreover, construction managers may make well-informed decisions to streamline processes, reduce delays, and guarantee that project milestones are fulfilled effectively by utilizing historical and real-time data kept within dataspaces.

7. Challenges and future directions

In this section, we highlight the challenges and future direction of the proposed Dataspace in the Sky.

7.1. Challenges

Deployment optimization for ground BSs: In BC-based drones in 6G networks, the ground BSs serve as miners, which plays a significant role. When few ground BSs are available or a heterogeneous 6G network, it can be difficult to develop the best ground BS deployment schemes to increase communication reliability further and decrease communication time between moving drones and miners.

Integration of BC and FL: There are several possible trade-offs and difficulties with integrating FL and BC, such as processing cost, latency, and data privacy issues. The processing expense related to BC and FL is one major obstacle. FL needs a significant amount of computing power for local model training on drones, while BC adds more overhead because of its encryption and consensus procedures. Using edge computing to offload part of the computational activities can resolve this and distribute the processing burden more effectively throughout the network. The higher delay brought on by the requirement for synchronization in both FL and BC presents another difficulty. Delays may be introduced by the consensus process in BC and the periodic aggregation of models in FL. By enabling more flexible and quick data processing and model updates, asynchronous FL approaches and optimized consensus algorithms can assist in reducing these latency problems. The openness of BC technology raises serious concerns regarding data privacy since it may unintentionally reveal model update information. To ensure that sensitive information is secured even when data provenance and integrity are upheld through the BC, this may be handled by including privacy-preserving methods such as differential privacy and secure multi-party computing. Leveraging the full benefits of FL and BC in a Dataspace architecture necessitates a careful balance between security, efficiency, and performance to address these challenges.

Data storage: Computing is one of a drone's most energy-consuming activities. The suggested platform uses data filtering tasks each drone performs to decide whether to process a request locally or send it to the cloud. The design procedure should be straightforward and reliable to prevent problems and failures. Failure is an unwelcome occurrence that can cause a drone to lose motion control and repeat tasks, which uses more energy. So, reducing the complexity of the algorithm increases drone energy efficiency. In addition, drones must store significant data locally since they are edge devices. The storage capacity should be maximized while considering other jobs and the aircraft's limited energy restrictions to ensure QoS performance.

Data security: Since each drone only stores duplicated data after verifying its source, the usage of BC between clouds and drones promotes confidence between the parties. Furthermore, since the duplicated data on the drone reflects the content of the blocks approved and uploaded to the BC, the cloud may transmit data to the drone. In contrast, the participating drones know data management at the drone layer. However, as hostile attackers might alter the shared duplicated data, this solution cannot ensure security and integrity. Furthermore, a drone network is open and has few security features, making it susceptible to many assaults. Further research is needed on the security and cyberattacks on edge computing that support drones to develop portable defensive systems with assured data integrity [125]. Ensuring the security and privacy of the data shared among drones in a decentralized fashion is challenging. While BC provides security and transparency, potential vulnerabilities and attacks could still compromise the system. Exploring advanced encryption and authentication mechanisms is required to address this challenge of protecting data and ensuring secure communication between drones.

Drone energy: Due to drone LoS links, drones that fly above events can give ground users favorable coverage. In addition, drones can enhance existing infrastructure as edge devices by providing various services near the users. However, the drones' low power capacity affects their operating and network lifetimes since each drone carries out three energy-intensive tasks: traveling at a specific altitude, computation, and communication. Consequently, offering energy-efficient solutions to decrease consumption and lengthen the lifespan of drones is crucial when creating a sustainable drone service platform. Drones should be given tasks optimized to prevent undesirable or needless energy-consuming activities, such as travelling large distances to an unknown place or repeatedly transmitting the same message because of network or processing issues. Several proposed techniques reduce the energy consumption of drones [127]. For example, an optimized target location supports the optimum coverage area for users, and an appropriate altitude is a trade-off between the energy used and the coverage region. Task scheduling and energy-conscious communication protocols are different ways to improve system performance and power economy.

Drone service provider: The QoS provided has always benefited from competition among different service providers. The competition is expected to be fair because it is based on stringent rules designed to improve and secure the necessary services for the users. A more modern platform idea is the drone service provider, which uses several drone types to provide various services. Multiple drone service providers working together to do tasks in one location can lead to problems with drone navigation, collisions, resource sharing, privacy, security, and many other things. Therefore, tight regulation in this sector must clarify drone service provider collocation rules.

Reliability and accuracy: Ensuring the reliability and accuracy of the models shared among drones is challenging. The quality of the models depends on the quality and quantity of the data collected by each drone, which can vary depending on the environment and the sensors used. To address this challenge, investigation techniques for improving the quality of the data collected by drones are required, such as using more advanced sensors and data fusion techniques.

Interoperability: Ensuring the interoperability of the different technologies used in the framework, including FL, BC, and 6G networks, is challenging. Integrating technologies requires careful consideration of the protocols, interfaces, and standards, which can be complex and time-consuming. To address this challenge, working closely with industry partners and stakeholders requires developing interoperable solutions and standards that can facilitate the deployment and adoption of the framework.

Computational and Resource Constraints: Both FL and BC have a considerable computational cost. Because drones usually have limited energy, storage, and computing power, executing complicated algorithms and keeping up BC ledgers might take much work. By shifting labor-intensive operations to more potent edge servers, edge computing might help ease these restrictions. In addition, effective data processing methods and lightweight consensus algorithms may be created to reduce the resource burden on individual drones.

Latency and Real-Time: Because of consensus procedures and model aggregation, FL and BC increase the delay. This delay can be disastrous for time-sensitive applications like surveillance or disaster response. Latency can be decreased by enhancing BC consensus methods and implementing asynchronous FL strategies. Moreover, edge computing's local processing capabilities may guarantee that crucial data is processed and used immediately, reducing waiting times.

Scalability and Network Management: Efficient management of communications, data exchange, and resource allocation becomes increasingly challenging as the number of drones in the network rises. Drone networks' changing topology contributes to this complexity. Creating a scalable, decentralized architecture that enables dynamic resource and data management is essential. Scalability and network management may be improved by implementing effective network protocols and utilizing edge computing for localized processing.

Trust and Interoperability: Achieving interoperability across various platforms and maintaining confidence between drones controlled by disparate companies without a central authority can be difficult. By guaranteeing data integrity, BC technology may provide a tamper-proof ledger of every transaction, promoting participant confidence. Standardized protocols and interfaces should be created to promote interoperability across various drone systems and networks.

7.2. Future directions

Digital twins and securing drone Dataspace: Another unresolved research question that must be resolved is Digital Twins (DT) and FL's reliability. Although DT and FL are thought to be more dependable, there is a need for schemes to address DT and FL's dependability in the Internet of drones. For example, the network efficiency may be examined using DT, which offers a virtual representation of the networks. However, efficiency issues may arise when the same DT model is deployed in real-time. This creates a new opportunity for academics to create models that consider the effectiveness of real-time and DT-based networks. Additionally, the Internet of drones does not make use of DT. The applications of combining DT and FL for the Internet of drones were discussed [128]. Furthermore, the combination of BC and DT is used for solving real-time applications such as transportation [129] and delivery during a pandemic [130].

Encryption and privacy-preserving: Both FL and BC improve security and privacy. However, if not properly managed, the decentralized nature of FL and the openness of BC may disclose metadata and result in possible data leakage. Privacy-preserving methods like secure multi-party computing and differential privacy in the FL architecture may safeguard sensitive data. To protect metadata and preserve transparency and integrity, BC can also use cutting-edge encryption techniques.

Trustworthy metrics for miner performance: In conventional BC systems, miners are typically chosen at random using metrics of resource competition, such as proof-of-work based on computing power and proof-of-stake based on stake [126]. However, the energy- and computation-intensive approaches are not appropriate or useful. It is essential to put forward a trustworthy metric to evaluate the performance and conduct of mining applicants fairly.

8. Conclusion

In this conceptual framework, we have introduced a novel Dataspece in the Sky framework for drone data-sharing and management in 6G for Industry 4.0 and Industry 5.0. In the context of Industry 4.0 and Industry 5.0, Dataspace 4.0 is crucial in facilitating the secure, efficient, and flexible data exchange required in dynamic environments like applications supported by drone networks. When several users share the same network resources, the network infrastructure becomes saturated by the large number of simultaneous requests, which lowers performance. Drones adjust dynamically to their positions and fill their maximum capacity and are employed to mitigate these challenges. We combined BC, FL, and Dataspace to secure data-sharing, providing high-level security for data exchange within drone Dataspace networks. Therefore, the combination drives various drone applications in Industry 4.0 and 5.0, requiring high trust and security. We have outlined the challenges and future directions for integrating FL and BC in drone Dataspace within 6G networks. Moreover, the integration has offered a robust, secure solution for drone networks, enabling seamless operations in both innovative and challenging industrial environments.

CRediT authorship contribution statement

Saeed Hamood Alsamhi: Writing – review & editing, Writing – original draft, Visualization, Supervision, Resources, Methodology, Investigation, Conceptualization. **Sumit Srivastava:** Resources, Funding acquisition, Formal analysis. **Mamoon Rashid:** Data curation, Formal analysis, Writing – review & editing. **Amnnah Alhabeeb:** Data curation, Formal analysis, Resources, Software. **Santosh Kumar:** Software, Resources, Investigation, Funding acquisition. **Navin Singh Rajput:** Validation, Supervision, Software. **Ammar Hawbani:** Supervision, Resources, Conceptualization. **Liang Zhao:** Resources, Formal analysis, Data curation. **Mohammed A.A. Al-qaness:** Visualization, Formal analysis, Data curation. **Edward Curry:** Writing – original draft, Supervision.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

This publication has emanated from research conducted with the financial support of Science Foundation Ireland under Grant number SFI/12/RC/2289_P2.

Data availability

No data was used for the research described in the article.

References

[1] O. Bouachir, M. Aloqaily, F. Garcia, N. Larrieu, T. Gayraud, Testbed of qos ad-hoc network designed for cooperative multidrone tasks, in: Proceedings of the 17th ACM International Symposium on Mobility Management and Wireless Access, 2019, pp. 89–95.

[2] S.H. Alsamhi, N.S. Rajput, Mishra, V.N. Guarantee, QoS in Coexistencee of High Altitude Platform System and WiMAX TerrestrialSystem.

[3] S.H. Alsamhi, N.S. Rajput, An intelligent HAP for broadband wireless communications: developments, QoS and applications, Int. J. Adv. Electr. Electron. Eng. 3 (2) (2015) 134–143.

[4] S.H. Alsamhi, N.S. Rajput, An intelligent hand-off algorithm to enhance quality of service in high altitude platforms using neural network, Wirel. Pers. Commun. 82 (4) (2015) 2059–2073.

[5] S.H. Alsamhi, N.S. Rajput, Implementation of call admission control technique in HAP for enhanced QoS in wireless network deployment, Telecommun. Syst. 63 (2) (2016) 141–151.
[6] Alsamhi Saeed Hamood, Ammar Hawbani, Radhya Sahal, Sumit Srivastava, Santosh Kumar, Liang Zhao, Mohammed A.A. Al-qaness, Jahan Hassan, Mohsen Guizani, Edward Curry, Towards sustainable industry 4.0: a survey on greening IoE in 6G networks, Ad Hoc Netw. 165 (2024) 103610.
[7] Muhammad Asghar Khan, Neeraj Kumar, Saeed Hamood Alsamhi, Gordana Barb, Justyna Zywiołek, Insaf Ullah, Fazal Noor, Jawad Ali Shah, Abdullah M. Almuhaideb, Security and privacy issues and solutions for UAVs in B5G networks: a review, IEEE Trans. Netw. Serv. Manag. (2024).
[8] Jia Yu, Alexey V. Shvetsov, Saeed Hamood Alsamhi, Leveraging machine learning for cybersecurity resilience in industry 4.0: challenges and future directions. " IEEE access (2024).alsamhi, saeed hamood, ammar hawbani, santosh Kumar, mohan timilsina, majjed al-qatf, rafiqul haque, farhan nashwan, liang zhao, and edward curry. "Empowering dataspace 4.0: unveiling promise of decentralized data-sharing, IEEE Access (2024).
[9] Alsamhi Saeed Hamood, Ammar Hawbani, Santosh Kumar, Mohan Timilsina, Majjed Al-Qatf, Rafiqul Haque, Farhan Nashwan, Liang Zhao, Edward Curry, Empowering dataspace 4.0: unveiling promise of decentralized data-sharing, IEEE Access (2024).
[10] Abdu Saif, Nor Shahida Mohd Shah, Aiman Alnoamani, Ali Ameen, Edward Curry, Vailet Hikmat Faraj, Al Khattat, Saeed Hamood Alsamhi, Resilient skies: advancing climate-resilient UAVs for energy-efficient B5G communication in challenging environments, in: 2024 4th International Conference on Emerging Smart Technologies and Applications (eSmarTA), IEEE, 2024, pp. 1–7.
[11] Raushan Myrzashova, Saeed Hamood Alsamhi, Ammar Hawbani, Edward Curry, Mohsen Guizani, Xi Wei, Safeguarding patient data-sharing: blockchain-enabled federated learning in medical diagnostics, IEEE Transactions on Sustainable Computing (2024).
[12] Farheen Syed, Saeed Hamood Alsamhi, Sachin Kumar Gupta, Abdu Saif, LSB-XOR technique for securing captured images from disaster by UAVs in B5G networks, Concurr. Comput. Pract. Exp. 36 (12) (2024), e8061.
[13] Su Peng, Neeraj Kumar, Saeed Hamood Alsamhi, Qiang He, Liang Zhao, Securing IoT data: FDUP-RDIC-a fully decentralized approach for privacy-preserving and efficient data integrity, IEEE Internet Things J. (2024).
[14] S.H. Alsamhi, N.S. Rajput, An efficient channel reservation technique for improved QoS for mobile communication deployment using high altitude platform, Wirel. Pers. Commun. 91 (3) (2016) 1095–1108.
[15] S.H. Alsamhi, N.S. Rajput, March. Performance and analysis of propagation models for efficient handoff in high altitude platform system to sustain QoS, in: 2014 IEEE Students' Conference on Electrical, Electronics and Computer Science, IEEE, 2014, pp. 1–6.
[16] A. Gupta, S. Sundhan, S.K. Gupta, S.H. Alsamhi, M. Rashid, Collaboration of UAV and HetNet for better QoS: a comparative study, Int. J. Veh. Inf. Commun. Syst. 5 (3) (2020) 309–333.
[17] S.H. Alsamhi, F.A. Almalki, H. Al-Dois, S.B. Othman, J. Hassan, A. Hawbani, et al., Machine learning for smart environments in B5G networks: connectivity and QoS, Comput. Intell. Neurosci. 2021 (2021).
[18] D. Saraswat, A. Verma, P. Bhattacharya, S. Tanwar, G. Sharma, P.N. Bokoro, R. Sharma, Blockchain-based federated learning in UAVs beyond 5G networks: a solution taxonomy and future directions, IEEE Access 10 (2022) 33154–33182.
[19] Haiao Li, Lina Ge, Lei Tian, Survey: federated learning data security and privacy-preserving in edge-Internet of things, Artif. Intell. Rev. 57 (5) (2024) 130.
[20] Alsamhi Saeed Hamood, Raushan Myrzashova, Ammar Hawbani, Santosh Kumar, Sumit Srivastava, Liang Zhao, Xi Wei, Mohsen Guizan, Edward Curry, Federated learning meets blockchain in decentralized data-sharing: healthcare use case, IEEE Internet Things J. (2024).
[21] Tri Nguyen, Huong Nguyen, Tuan Nguyen Gia, Exploring the integration of edge computing and blockchain IoT: principles, architectures, security, and applications, J. Netw. Comput. Appl. (2024) 103884.
[22] Karam Sana Nasim, Kashif Bilal, Abdul Nasir Khan, Junaid Shuja, Said Jadid Abdulkadir, Energy-efficient routing protocol for reliable low-latency Internet of things in oil and gas pipeline monitoring, PeerJ Comput. Sci. 10 (2024) e1908.
[23] Chaoyang Zhu, Xiao Zhu, Junyu Ren, Tuanfa Qin, Blockchain-enabled federated learning for UAV edge computing network: issues and solutions, IEEE Access 10 (2022) 56591–56610.
[24] Alsamhi, Saeed Haomood, Edward Curry, Ammar Hawbani, Santosh Kumar, Umair Ul Hassan, Navin Singh Rajput, DataSpace in the sky: a novel Decentralized framework to secure drones Data-sharingin B5G for industry 4.0 toward industry 5.0, 2023.
[25] S. Garg, A. Singh, S. Batra, N. Kumar, L.T. Yang, UAV-empowered edge computing environment for cyber-threat detection in smart vehicles, IEEE Netw. 32 (3) (2018) 42–51.
[26] P. Mehta, R. Gupta, S. Tanwar, Blockchain envisioned UAV networks: challenges, solutions, and comparisons, Comput. Commun. 151 (2020) 518–538.
[27] T. Dasu, Y. Kanza, D. Srivastava, Geofences in the sky: herding drones with blockchains and 5G, in: Proceedings of the 26th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems, 2018, pp. 73–76.
[28] J. Kang, Z. Xiong, D. Niyato, D. Ye, D.I. Kim, J. Zhao, Toward secure blockchain-enabled Internet of vehicles: optimizing consensus management using reputation and contract theory, IEEE Trans. Veh. Technol. 68 (3) (2019) 2906–2920.
[29] S.H. Alsamhi, F. Almalki, O. Ma, M.S. Ansari, B. Lee, Predictive estimation of optimal signal strength from drones over IoT frameworks in smart cities, IEEE Trans. Mob. Comput. (2021).
[30] S.H. Alsamhi, F.A. Almalki, H. AL-Dois, A.V. Shvetsov, M.S. Ansari, A. Hawbani, et al., Multi-drone edge intelligence and SAR smart wearable devices for emergency communication, Wirel. Commun. Mob. Comput. 2021 (2021).
[31] A. Saif, K. Dimyati, K.A. Noordin, S.H. Alsamhi, A. Hawbani, Multi-UAV and SAR collaboration model for disaster management in B5G networks, Internet Technology Letters e310 (2021).
[32] S.H. Alsamhi, M.S. Ansari, N.S. Rajput, Disaster coverage predication for the emerging tethered balloon technology: capability for preparedness, detection, mitigation, and response, Disaster Med. Public Health Prep. 12 (2) (2018) 222–231.
[33] S. Aggarwal, N. Kumar, S. Tanwar, Blockchain-envisioned UAV communication using 6G networks: open issues, use cases, and future directions, IEEE Internet Things J. 8 (7) (2020) 5416–5441.
[34] M. Aloqaily, I. Al Ridhawi, M. Guizani, Energy-aware blockchain and federated learning-supported vehicular networks, IEEE Trans. Intell. Transp. Syst. (2021).
[35] H. Chao, A. Maheshwari, V. Sudarsanan, S. Tamaskar, D.A. DeLaurentis, UAV traffic information exchange network, in: 2018 Aviation Technology, Integration, and Operations Conference, 2018, p. 3347.
[36] X. Liang, J. Zhao, S. Shetty, D. Li, Towards data assurance and resilience in IoT using blockchain, in: MILCOM 2017-2017 IEEE Military Communications Conference (MILCOM), 2017, pp. 261–266, IEEE.
[37] E. Curry, W. Derguech, S. Hasan, C. Kouroupetroglou, U. ul Hassan, A real-time linked dataspace for the Internet of things: enabling "pay-as-you-go" data management in smart environments, Future Gener. Comput. Syst. 90 (2019) 405–422.
[38] F. Gao, L. Zhu, M. Shen, K. Sharif, Z. Wan, K. Ren, A blockchain-based privacy-preserving payment mechanism for vehicle-to-grid networks, IEEE Netw. 32 (6) (2018) 184–192.
[39] M. Shen, Y. Deng, L. Zhu, X. Du, N. Guizani, Privacy-preserving image retrieval for medical IoT systems: a blockchain-based approach, IEEE Netw. 33 (5) (2019) 27–33.
[40] Q. Xia, et al., Secured fine-grained selective access to outsourced cloud data in IoT environments, IEEE Internet Things J. 6 (6) (2019) 10749–10762.
[41] T. Alladi, V. Chamola, N. Sahu, M. Guizani, Applications of blockchain in unmanned aerial vehicles: a review, Veh. Commun. 23 (2020) 100249.
[42] J. Qiu, D. Grace, G. Ding, J. Yao, Q. Wu, Blockchain-based secure spectrum trading for unmanned-aerial-vehicle-assisted cellular networks: an operator's perspective, IEEE Internet Things J. 7 (1) (2019) 451–466.
[43] K. Bonawitz, et al., Towards federated learning at scale: system design, in: Proceedings of Machine Learning and Systems, vol. 1, 2019, pp. 374–388.
[44] J. Konečný, H.B. McMahan, D. Ramage, P. Richtárik, Federated optimization: distributed machine learning for on-device intelligence, arXiv preprint, arXiv:1610.02527, 2016.
[45] A. Fallah, A. Mokhtari, A. Ozdaglar, Personalized federated learning: a meta-learning approach, arXiv preprint, arXiv:2002.07948, 2020.
[46] M. Nasr, R. Shokri, A. Houmansadr, Comprehensive privacy analysis of deep learning: passive and active white-box inference attacks against centralized and federated learning, in: 2019 IEEE Symposium on Security and Privacy (SP), IEEE, 2019, pp. 739–753.
[47] L. Zhu, Z. Liu, S. Han, Deep leakage from gradients, Adv. Neural Inf. Process. Syst. 32 (2019).
[48] X. Dong, R. Li, H. He, W. Zhou, Z. Xue, H. Wu, Secure sensitive data-sharingon a big data platform, Tsinghua Sci. Technol. 20 (1) (2015) 72–80.
[49] C. Huang, D. Liu, J. Ni, R. Lu, X. Shen, Achieving accountable and efficient data-sharingin industrial Internet of things, IEEE Trans. Ind. Inform. 17 (2) (2020) 1416–1427.
[50] S. Huh, S. Cho, S. Kim, Managing IoT devices using blockchain platform, in: 2017 19th International Conference on Advanced Communication Technology (ICACT), IEEE, 2017, pp. 464–467.
[51] M. Zhaofeng, W. Xiaochang, D.K. Jain, H. Khan, G. Hongmin, W. Zhen, A blockchain-based trusted data management scheme in edge computing, IEEE Trans. Ind. Inform. 16 (3) (2019) 2013–2021.
[52] M. Zhaofeng, W. Lingyun, W. Xiaochang, W. Zhen, Z. Weizhe, Blockchain-enabled decentralized trust management and secure usage control of IoT big data, IEEE Internet Things J. 7 (5) (2019) 4000–4015.
[53] W. Wei, J. Wang, Z. Fang, J. Chen, Y. Ren, Y. Dong, 3U: joint design of UAV-USV-UUV networks for cooperative target hunting, IEEE Trans. Veh. Technol. (2022).
[54] Y. Wang, Z. Su, Q. Xu, R. Li, T.H. Luan, Lifesaving with RescueChain: energy-efficient and partition-tolerant blockchain based secure information sharing for UAV-aided disaster rescue, in: IEEE INFOCOM 2021-IEEE Conference on Computer Communications, IEEE, May 2021, pp. 1–10.
[55] B. Otto, M. ten Hompel, S. Wrobel, Designing Data Spaces: the Ecosystem Approach to Competitive Advantage, 2022.
[56] W. Prinz, T. Rose, N. Urbach, Blockchain technology and international data spaces, Des. Data Spaces Ecosystems Compet. Advant. (2022) 165–180.
[57] M. Jarke, C. Quix, Federated data integration in data spaces, Des. Data Spaces (2022) 181.

[58] A. Saif, K. Dimyati, K.A. Noordin, S.H. Alsamhi, N.A. Mosali, S.K. Gupta, UAV and Relay Cooperation Based on RSS for Extending Smart Environments Coverage Area in B5G, 2022.
[59] S.H. Alsamhi, N.S. Rajput, September. HAP antenna radiation pattern for providing coverage and service characteristics, in: 2014 International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2014, pp. 1434–1439, IEEE.
[60] M.A. Khan, N. Kumar, S.A.H. Mohsan, W.U. Khan, M.M. Nasralla, M.H. Alsharif, et al., Swarm of UAVs for network management in 6G: a technical review, IEEE Trans. Netw. Serv. Manag. (2022).
[61] J.R. Martinez-De Dios, K. Lferd, A. De San Bernabe, G.N. ´ uńez, A. Torres-Gonzalez, A. Ollero, Cooperation between UAS ´ and wireless sensor networks for efficient data collection in large environments, J. Intell. Robot. Syst. 70 (1–4) (2013) 491–508.
[62] J. Allred, A.B. Hasan, S. Panichsakul, et al., SensorFlock: an airborne wireless sensor network of micro-air vehicles, in: Proceedings of the 5th ACM International Conference on Embedded Networked Sensor Systems, (SenSys'07), ACM, Sydney, Australia, November 2007, pp. 117–129.
[63] A.S. Ismail, X. Wang, A. Hawbani, S. Alsamhi, S. Abdel Aziz, Routing protocols classification for underwater wireless sensor networks based on localization and mobility, Wirel. Netw. 28 (2) (2022) 797–826.
[64] S.N. Chaudhri, N.S. Rajput, S.H. Alsamhi, A.V. Shvetsov, F.A. Almalki, Zero-padding and spatial augmentation-based gas sensor node optimization approach in resource-constrained 6G-IoT paradigm, Sensors 22 (8) (2022) 3039.
[65] X. Wang, W. Zhou, A. Hawbani, P. Liu, L. Zhao, S.H. Alsamhi, A dynamic opportunistic routing protocol for asynchronous duty-cycled WSNs, IEEE Transactions on Sustainable Computing. (2023).
[66] M.A. Al-qaness, A.A. Abbasi, H. Fan, R.A. Ibrahim, S.H. Alsamhi, A. Hawbani, An improved YOLO-based road traffic monitoring system, Computing 103 (2021) 211–230.
[67] M. Aloqaily, O. Bouachir, A. Boukerche, I. Al Ridhawi, Design guidelines for blockchain-assisted 5G-UAV networks, IEEE Netw. 35 (1) (2021) 64–71.
[68] A. Asheralieva, D. Niyato, Distributed dynamic resource management and pricing in the IoT systems with blockchain-as-a-service and UAV-enabled mobile edge computing, IEEE Internet Things J. 7 (3) (2019) 1974–1993.
[69] A. Islam, S.Y. Shin, BUAV: a blockchain based secure UAV-assisted data acquisition scheme in Internet of things, J. Commun. Netw. 21 (5) (2019) 491–502.
[70] Y. Zhu, G. Zheng, K.-K. Wong, Blockchain-empowered decentralized storage in air-to-ground industrial networks, IEEE Trans. Ind. Inform. 15 (6) (2019) 3593–3601.
[71] A.K. Shrestha, J. Vassileva, Towards decentralized data storage in general cloud platform for meta-products, in: Proceedings of the International Conference on Big Data and Advanced Wireless Technologies, 2016, pp. 1–7.
[72] C. Tenopir, C.L. Palmer, L. Metzer, J. van der Hoeven, J. Malone, Sharing data: practices, barriers, and incentives, Proc. Am. Soc. Inf. Sci. Technol. 48 (1) (2011) 1–4.
[73] A. Meadows, To Share or not to Share? That is the (Research Data) Question…| The Scholarly Kitchen 2014.
[74] C.H. Liu, Q. Lin, S. Wen, Blockchain-enabled data collection and sharing for industrial IoT with deep reinforcement learning, IEEE Trans. Ind. Inform. 15 (6) (2019) 3516–3526.
[75] Y. Lu, X. Huang, Y. Dai, S. Maharjan, Y. Zhang, Blockchain and federated learning for privacy-preserved data-sharingin industrial IoT, IEEE Trans. Ind. Inform. 16 (6) (2020) 4177–4186.
[76] M.C. Zizic, M. Mladineo, N. Gjeldum, L. Celent, From industry 4.0 towards industry 5.0: a review and analysis of paradigm shift for the people, organization and technology, Energies 15 (14) (2022) 5221.
[77] N.F.S. Jeffri, D.R.A. Rambli, A review of augmented reality systems and their effects on mental workload and task performance, Heliyon 7 (3) (2021) e06277.
[78] N.F.S. Jeffri, D.R.A. Rambli, A review of augmented reality systems and their effects on mental workload and task performance, Heliyon 7 (3) (2021) e06277, 44; S.R. Singh, H. Mithaiwala, N. Chauhan, P. Shah, C. Trivedi, U.P. Rao, Decentralized blockchain-based framework for securing review system, Secur. Priv. Data Anal. (2022) 239–255.
[79] P. Bhattacharya, et al., Coalition of 6G and blockchain in AR/VR space: challenges and future directions, IEEE Access 9 (2021) 168455–168484.
[80] T.M. Fernández-Caramés, O. Blanco-Novoa, I. Froiz-Míguez, P. Fraga-Lamas, Towards an autonomous industry 4.0 warehouse: a UAV and blockchain-based system for inventory and traceability applications in big data-driven supply chain management, Sensors 19 (10) (2019) 2394.
[81] M. Franklin, A. Halevy, D. Maier, From databases to dataspaces: a new abstraction for information management, ACM SIGMOD Rec. 34 (4) (2005) 27–33.
[82] L. Blunschi, J.P. Dittrich, O.R. Girard, S.K. Karakashian, M.A.V. Salles, A dataspace odyssey: The iMeMex personal dataspace management system, in: CIDR, January 2007, pp. 114–119.
[83] R. Grossman, E. Creel, M. Mazzucco, R. Williams, A dataspace infrastructure for astronomical data, in: In Data Mining for Scientific and Engineering Applications, Springer, 2001, pp. 115–123.
[84] A. Hasnain, et al., Linked biomedical dataspace: lessons learned integrating data for drug discovery, in: International Semantic Web Conference, 2014, pp. 114–130, Springer.
[85] D.W. Archer, L.M. Delcambre, D. Maier, A framework for fine-grained data integration and curation, with provenance, in a dataspace, in: Workshop on the Theory and Practice of Provenance, 2009.
[86] Y. Li, X. Meng, Supporting context-based query in personal DataSpace, in: Proceedings of the 18th ACM Conference on Information and Knowledge Management, 2009, pp. 1437–1440.
[87] A.D. Sarma, X.L. Dong, A.Y. Halevy, Data modeling in dataspace support platforms, in: Conceptual Modeling: Foundations and Applications, Springer, 2009, pp. 122–138.
[88] R. Grossman, M. Mazzucco, DataSpace: a data web for the exploratory analysis and mining of data, Comput. Sci. Eng. 4 (4) (2002) 44–51.
[89] U. ul Hassan, S. O'Riain, E. Curry, Leveraging matching dependencies for guided user feedback in linked data applications, in: Proceedings of the Ninth International Workshop on Information Integration on the Web, 2012, pp. 1–6.
[90] E. Curry, System of systems information interoperability using a linked dataspace, in: 2012 7th International Conference on System of Systems Engineering (SoSE), IEEE, 2012, pp. 101–106.
[91] E. Curry, S. Hasan, S. O'Riain, Enterprise energy management using a linked dataspace for energy intelligence, in: 2012 Sustainable Internet and ICT for Sustainability (SustainIT), 2012, pp. 1–6, IEEE.
[92] E. Curry, J. O'Donnell, E. Corry, S. Hasan, M. Keane, S. O'Riain, Linking building data in the cloud: integrating cross-domain building data using linked data, Adv. Eng. Inform. 27 (2) (2013) 206–219.
[93] Edward Curry, Real-Time Linked Dataspaces: Enabling Data Ecosystems for Intelligent Systems, Springer Nature, 2020.
[94] C. Gomez, S. Chessa, A. Fleury, G. Roussos, D. Preuveneers, Internet of things for enabling smart environments: a technology-centric perspective, J. Ambient Intell. Smart Environ. 11 (1) (2019) 23–43.
[95] G. Marques, A. González-Briones, J.M.M. López, Machine Learning for Smart Environments/Cities.
[96] S.H. Alsamhi, O. Ma, M.S. Ansari, F.A. Almalki, Survey on collaborative smart drones and Internet of things for improving smartness of smart cities, IEEE Access 7 (2019) 128125–128152.
[97] S.V. Shvetsova, A.V. Shvetsov, Ensuring safety and security in employing drones at airports, Journal of Transportation Security 14 (1) (2021) 41–53.
[98] S. Shvetsova, A. Shvetsov, Safety when flying unmanned aerial vehicles at transport infrastructure facilities, Transp. Res. Proc. 54 (2021) 397–403.
[99] S.H. Alsamhi, B. Lee, M. Guizani, N. Kumar, Y. Qiao, X. Liu, Blockchain for decentralized multi-drone to combat COVID-19 and future pandemics: framework and proposed solutions, Trans. Emerg. Telecommun. Technol. 32 (9) (2021) e4255.
[100] S.H. Alsamhi, A.V. Shvetsov, S.V. Shvetsova, A. Hawbani, M. Guizan, M.A. Alhartomi, O. Ma, Blockchain-empowered security and energy efficiency of drone swarm consensus for environment exploration, IEEE Trans. Green Commun. Netw. (2022).
[101] S.H. Alsamhi, F.A. Almalki, F. Afghah, A. Hawbani, A.V. Shvetsov, B. Lee, H. Song, Drones' edge intelligence over smart environments in b5g: blockchain and federated learning synergy, IEEE Trans. Green Commun. Netw. 6 (1) (2021) 295–312.
[102] A. Ojo, E. Curry, Catalog and entity management service for Internet of things-based smart environments, in: Real-Time Linked Dataspace, Springer, Cham, 2020, pp. 89–103.
[103] E. Curry, W. Fabritius, S. Hasan, C. Kouroupetroglou, W. Derguech, A model for Internet of things enhanced user experience in smart environments, in: Real-Time Linked Dataspace, Springer, Cham, 2020, pp. 271–294.
[104] E. Curry, W. Derguech, S. Hasan, C. Kouroupetroglou, W. Fabritius, Building Internet of things-enabled digital twins and intelligent applications using a real-time linked dataspace, in: Real-Time Linked Dataspace, Springer, Cham, 2020, pp. 255–270.
[105] N.A. Zanury, M.A. Remli, H.K. Adli, K.N.S.W. Wong, Recent developments of deep learning in future smart cities: a review, Mach. Learn. Smart Environ./Cities (2022) 199–212.
[106] T. Qiu, J. Liu, W. Si, D.O. Wu, Robustness optimization scheme with multi-population co-evolution for scale-free wireless sensor networks, IEEE/ACM Trans. Netw. 27 (3) (2019) 1028–1042.
[107] A. Saif, K. Dimyati, K.A. Noordin, N.S.M. Shah, S.H. Alsamhi, Q. Abdullah, Energy-efficient tethered UAV deployment in B5G for smart environments and disaster recovery, in: 2021 1st International Conference on Emerging Smart Technologies and Applications, IEEE, August 2021, pp. 1–5, (eSmarTA).
[108] S.A. Khaleefa, S.H. Alsamhi, N.S. Rajput, March. Tethered balloon technology for telecommunication, coverage and path loss, in: 2014 IEEE Students' Conference on Electrical, Electronics and Computer Science, IEEE, 2014, pp. 1–4.
[109] P. Manghwani, J. Loyall, P. Sharma, M. Gillen, J. Ye, April. End-to-end quality of service management for distributed real-time embedded applications, in: 19th IEEE International Parallel and Distributed Processing Symposium, IEEE, 2005, p. 8.
[110] A. Bujari, C.T. Calafate, J.-C. Cano, P. Manzoni, C.E. Palazzi, D. Ronzani, Flying ad-hoc network application scenarios and mobility models, Int. J. Distrib. Sens. Netw. 13 (10) (2017) 1550147717738192.
[111] S. Han, S. Xu, W. Meng, C. Li, Dense-device-enabled cooperative networks for efficient and secure transmission, IEEE Netw. 32 (2) (2018) 100–106.
[112] N. Vanitha, G. Padmavathi, A comparative study on communication architecture of unmanned aerial vehicles and security analysis of false data dissemination attacks, in: 2018 International Conference on Current Trends Towards Converging Technologies (ICCTCT), IEEE, 2018, pp. 1–8.

[113] S. Aggarwal, M. Shojafar, N. Kumar, M. Conti, A new secure data dissemination model in Internet of drones, in: ICC 2019-2019 IEEE International Conference on Communications (ICC), IEEE, 2019, pp. 1–6.
[114] S. Jacob, V.G. Menon, P. Shynu, S.K. Fathima, B. Mahapatra, S. Joseph, Bidirectional multi-tier cognitive swarm drone 5G network, in: IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), IEEE, 2020, pp. 1219–1224.
[115] B. McMahan, E. Moore, D. Ramage, S. Hampson, B.A. y Arcas, April. Communication-efficient learning of deep networks from decentralized data, in: Artificial Intelligence and Statistics, PMLR, 2017, pp. 1273–1282.
[116] S. Trindade, L.F. Bittencourt, N.L. da Fonseca, Dig. Commun. Netw. (2022), Resource management at the network edge for federated learning.
[117] M. Chen, Z. Yang, W. Saad, C. Yin, H.V. Poor, S. Cui, A joint learning and communications framework for federated learning over wireless networks, IEEE Trans. Wirel. Commun. 20 (1) (2020) 269–283.
[118] K. Khacef, G. Pujolle, March. Secure peer-to-peer communication based on blockchain, in: Workshops of the International Conference on Advanced Information Networking and Applications, Springer, Cham, 2019, pp. 662–672.
[119] R. Ramachandran, V. Babu, V.P. Murugesan, The role of blockchain technology in the process of decision-making in human resource management: a review and future research agenda, Bus. Process Manag. J. (2022), (ahead-of-print).
[120] J. Zarrin, H. Wen Phang, L. Babu Saheer, B. Zarrin, Blockchain for decentralization of Internet: prospects, trends, and challenges, Clust. Comput. 24 (4) (2021) 2841–2866.
[121] J. Chi, Y. Li, J. Huang, J. Liu, Y. Jin, C. Chen, T. Qiu, A secure and efficient data-sharingscheme based on blockchain in industrial Internet of things, J. Netw. Comput. Appl. 167 (2020) 102710.
[122] A.A. Khan, A.A. Laghari, T.R. Gadekallu, Z.A. Shaikh, A.R. Javed, M. Rashid, et al., A drone-based data management and optimization using metaheuristic algorithms and blockchain smart contracts in a secure fog environment, Comput. Electr. Eng. 102 (2022) 108234.
[123] M. Aloqaily, Y. Jararweh, O. Bouachir, Trustworthy cooperative UAV-based data management in densely crowded environments, Comm. Stand. Mag. 5 (4) (2021) 18–24.
[124] X. Wang, T. Huang, K. Zhu, X. Zhao, LSTM-based broad learning system for remaining useful life prediction, Mathematics 10 (12) (2022), 2066.
[125] Hichem Sedjelmaci, Aymen Boudguiga, Inès Ben Jemaa, Sidi Mohammed Senouci, An efficient cyber defense framework for UAV-edge computing network, Ad Hoc Netw. 94 (2019) 101970.
[126] Z. Yang, K. Yang, L. Lei, K. Zheng, V.C. Leung, Blockchain-based decentralized trust management in vehicular networks, IEEE Internet Things J. 6 (2) (2018) 1495–1505.
[127] Mushu Li, Nan Cheng, Jie Gao, Yinlu Wang, Lian Zhao, Xuemin Shen, Energy-efficient UAV-assisted mobile edge computing: resource allocation and trajectory optimization, IEEE Trans. Veh. Technol. 69 (3) (2020) 3424–3438.
[128] S. Jamil, M. Rahman, A comprehensive survey of digital twins and federated learning for industrial Internet of things (IIoT)Internet of Vehicles (IoV) and Internet of Drones (IoD)., Appl. Syst. Innov. 5 (3) (2022) 56.
[129] R. Sahal, S.H. Alsamhi, K.N. Brown, D. O'Shea, C. McCarthy, M. Guizani, Blockchain-empowered digital twins collaboration: smart transportation use case, Machines 9 (9) (2021) 193.
[130] R. Sahal, S.H. Alsamhi, K.N. Brown, D. O'Shea, B. Alouffi, Blockchain-based digital twins collaboration for smart pandemic alerting: decentralized COVID-19 pandemic alerting use case, Comput. Intell. Neurosci. 2022 (2022).
[131] A common data space 4.0 for European manufacturing, Available in, https://digitalfactoryalliance.eu/moving-towards-a-common-data-space-4-0-for-european-manufacturing/.
[132] Y. Yahiatene, A. Rachedi, M.A. Riahla, D.E. Menacer, F. Nait-Abdesselam, A blockchain-based framework to secure vehicular social networks, Trans. Emerg. Telecommun. Technol. 30 (8) (2019) e3650.
[133] I. Makhdoom, I. Zhou, M. Abolhasan, J. Lipman, W. Ni, PrivySharing: a blockchain-based framework for privacy-preserving and secure data-sharingin smart cities, Comput. Secur. 88 (2020) 101653.
[134] V. Patel, A framework for secure and decentralized sharing of medical imaging data via blockchain consensus, Health Inform. J. 25 (4) (2019) 1398–1411.