Article

DataSpace in the Sky: A Novel Decentralized Framework to Secure Drones Data Sharing in B5G for Industry 4.0 toward Industry 5.0

Saeed Haomood Alsamhi * , Edward Curry , Ammar Hawbani , Santosh Kumar , Umair Ul Hassan , Navin Singh Rajput

Posted Date: 8 May 2023

doi: 10.20944/preprints202305.0529.v1

Keywords: Dataspace; data sharing; drones; B5G; security; IoT; Federated learning; Blockchain; Industry 4.0; Industry 5.0

Article

Dataspace in the Sky: A Novel Decentralized Framework to Secure Drones Data Sharing in B5G for Dataspcae 4.0

Saeed Hamood Alsamhi [1,2,*], Edward Curry [1], Ammar Hawbani [3], Santosh Kumar [4], Umair ul Hassan[1] and Navin Singh Rajput [5]

[1] Insight Center for Data Analytics, University of Galway, Galway, Ireland
[2] Facultuy of Engineering, IBB University, 70270, Ibb, Yemen
[3] School of Computer and Technology, University of Science and Technology of China, Hefei, China
[4] Department of CSE, IIIT Naya Raipur, Chhattisgarh, India
[4] Department of Electronics Engineering, IIT (BHU), Varanasi, India
[*] Correspondence: saeed.alsamhi@insight-centre.org

Abstract: Recently, dataspace has gained popularity due to its design for managing and sharing heterogeneous data from various sources and domains; and its capability to solve data integration issues incrementally. Leveraging dataspace and advanced technologies plays a vital role in solving many real-world applications effectively and efficiently in real-time. Drone technology deploys to gather data from different resources in harsh or smart environments. Beyond fifth-Generation (B5G) communication networks significantly contribute to drones' development and widespread use by providing low latency and high throughput. Therefore, data sharing among drones in B5G networks offers significant potential to enhance commercial and civilian applications. However, several security issues for collaboration and data sharing, such as data privacy leakage, because of sensitive data and the lack of trustworthy centralized monitoring. Furthermore, sharing data is one of the essential requirements for drone collaboration to achieve their tasks effectively and efficiently in real-time. This conceptual framework presents a novel dataspace in the sky, focusing on securing drone data sharing in B5G for Industry 4.0 toward Industry 5.0. Furthermore, we present how Federated Learning (FL) assists drones in collaboration effectively and efficiently, sharing models instead of raw data for efficient security and privacy. However, because of the fragility of the central curator, the reliability of contribution recording, and the poor quality of shared local models, there are still significant security and privacy issues for drone-assisted smart environments in B5G. Therefore, we present the conceptual framework for leveraging blockchain and FL to secure and manage data sharing of collaborative drones' dataspace in a decentralized fashion. The decentralization of dataspace would significantly expand the drive and market to develop citizen-friendly mobility services.

Keywords: dataspace; data sharing; decentralized data sharing; drones; B5G; Federated Learning; blockchain; Industry 4.0; Industry 5.0; Dataspace 4.0

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 bring together real-time and contextual data, the interface between existing information systems and new digital infrastructures, and easy data sharing between stakeholders 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 performance of the network in order to ensure Quality of Service (QoS) [1]. QoS , energy consumption, and fast data delivery are challenging in drone networks. Beyond fifth Generation (B5G) is designed to offer a high data rate and improve QoS. Therefore, B5G 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 [2–7]. While the authors of [8] introduced drone collaboration and HetNet for better QoS. In [9] discussed an intelligent method for supporting QoS and connectivity in B5G networks. Moreover, with the massive amount of data gathered by drones, Federated Learning (FL) plays a vital role in improving the privacy and security of the learning model. In contrast, the FL, blockchain, and B5G combination in the drone's network leads to high-level security, decentralized learning, and satisfying QoS requirements [10].

While sensing methods have many similarities, the mix of different spatiotemporal resolutions, operational procedures, and the wide range of heterogeneous data being 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. 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 Figure 1.

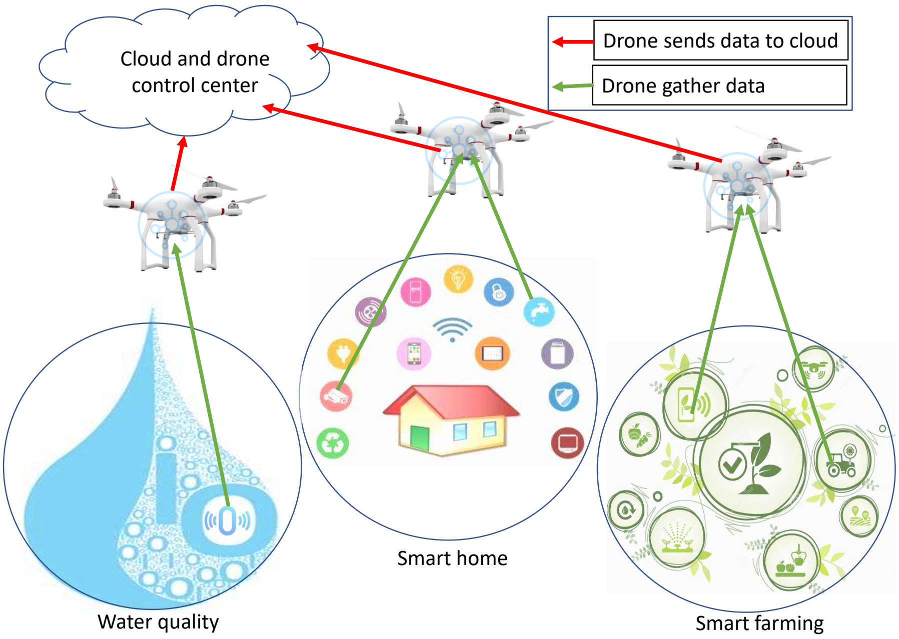

Figure 1. Drone-enabled data acquisition.

Recently, drone networks have developed in tandem with the quick advancements in B5G communication technologies, which improve drone applications and introduce cutting-edge ones that call for reliable and low-latency communications [11]. Drones from various owners share collected data in B5G networks to get over the limitations of visual coverage and geographic region, expand the diversity of sensing data, and boost data dependability [12]. Although drones in B5G 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 [13]. 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 decentralized data sharing and management framework still have 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 B5G networks [14].

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 [15] 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 [16,19]. To complete time-sensitive and computationally expensive tasks, drones communicate and share data with one another, necessitating intelligence in the communication channel. Depending on the generated data and the application type, Intelligent approach such as Machine Learning (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. Since FL only shares the model parameters and not the training data, privacy is maintained. 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 [20]. 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.

Blockchain is a potential method to overcome the aforementioned restrictions and foster trust in FL communication. Blockchain ensures traceability, scalability, decentralization, nonreusability, 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 blockchain-leveraged FL-assisted drones offers the highest level of trust and privacy, of data sharing, and traceable access under constant local updates [21]. Blockchain technologies have drawn more attention as researchers explore their potential to guarantee secure data sharing across a tamper-proof and decentralized ledger [14]. The authors of [22] used blockchain to create a network for securely exchanging traffic data between drones. For upcoming IoT applications, a blockchain-based drone system was discussed to achieve secure data management and guarantee drone data integrity [23]. FL implementation via blockchain is made simpler because single-point failures in the system are avoided, and the need for a central server is removed. Blockchain enables traceability between network entities and continuously observes channel activities transparent to all peer drones. With blockchain-assisted FL, model parameter may be easily traced using the logs recorded as ledger entries. The miners check the transactions in the block header, create blocks, add the FL, and model the chain's data.

A dataspace is a new paradigm of managing data from different resources as well as sharing data that has successfully managed scientific and personal data. However, dataspace application in intelligent systems and real-time data is still largely untapped. A real-time linked dataspace platform was introduced to facilitate data management in intelligent environments [24] such as water environments and smart energy, along with supporting services, tiers of support, and 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 B5G 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*

Accessing the cloud for applications and storage in highly populated locations 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 close to the end user, resulting in greater accessibility and reduced latency.

Decentralized data sharing 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. By sharing data from multiple sources, organizations can work together to identify and address common challenges, avoid duplication of effort, and focus resources on the most needed areas. Additionally, decentralized data sharing can provide decision-makers with a more complete and accurate understanding of a given situation, ultimately leading to more effective and efficient outcomes in applications such as agriculture, environmental monitoring, disaster response, and more.

In this conceptual framework, we propose the dataspace platform of collaborative drones with smart edge intelligent computing capabilities, which can adapt to highly populated locations to cut traffic, especially on the uplink. The proposed framework will reduce the burden of providing ground Base Stations (BSs) and increase network resource availability, thus raising QoS. A decision-making server carries out all problematic tasks to improve drone tasks. 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 behaviour predictions. Furthermore, a blockchain is implemented amongst the various parts of the proposed platform to store information and foster trust between individuals. The contributions of the conceptual framework summary are as follows:

1. We define the requirements for dataspace in the sky by describing the high-level platform design of a real-time linked drone dataspace for enabling smart and harsh environments.
2. Based on identifying the requirements for dataspace in the sky, we present a novel dataspace that focuses on securing drone data sharing in B5G for Industry 4.0 toward Industry 5.0. The framework proposes a decentralized approach to managing and sharing data among drones to overcome the limitations of centralized data management systems vulnerable to security breaches and privacy violations.
3. To effectively limit the sensitivity of shared data leaks and accomplish safe data sharing during collaborative modelling, the proposed framework leverages advanced technologies such as FL for efficient drone collaboration. FL allows drones to share models instead of raw data, reducing the risk of privacy leakage and enhancing data-sharing efficiency. Furthermore, the proposed framework integrates blockchain to ensure the security and privacy of collaborative drones' dataspace in a decentralized fashion. Blockchain provides a tamper-proof ledger for recording contributions and ensuring the quality of shared local models. Leveraging advanced technologies and drone dataspace plays a vital role in decentralized data sharing to enhance the industry, academia, commercial and civilian applications.

1.2. Paper structure

The rest of the paper is organized as follows. Section 2 presents the related work, while Section 3 describes the overview of core technologies. Section 4 represents the conceptual framework of dataspace in the sky, while the validation of the proposed framework is given in Section 5. Section 6 discusses the challenges and future directions. Finally, the conclusion of the work is given in Section 7.

2. Related work

With the benefits of transaction privacy, credibility, tamper resistance, and high dispersion, blockchain, 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 [25] introduced a blockchain-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 blockchain technology's developments to satisfy the network requirements between vehicles and users. Furthermore, a blockchain-based system for medical picture retrieval with privacy protection was proposed [26]. The blockchain-based system's architecture was demonstrated and described for each layer. However, the Shapley value approach may distribute each participant's benefits in this system. 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 were implemented for outsourced data [27]. Additionally, blockchain technologies are used to improve visibility and traceability. Even while blockchain substantially simplifies open and secure data sharing scenarios, it is costly to construct a permissionless blockchain in resource-constrained drones or ground communication infrastructures [28]. Therefore, it is suggested that secure vehicular data sharing systems [14] and spectrum trading [29] be developed using permissioned blockchains, which quickly complete consensus mechanisms on pre-defined miners with low overhead. These systems are effective and especially useful for drones in B5G networks [29].

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 [30] introduced FL for privacy policy makes it stand out. Several contributors can obtain superior training results when training a DL model than their local models without submitting their raw data to a centralized server. To address the statistical heterogeneity problem of data in FL was used as an optimization approach [31]. The authors of [32] 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 federal learning approaches still have privacy leakage issues. In [33] showed that member inferring attacks could be used to discover private membership information. In both standalone and federated environments, concerning passive and active inference attackers and assuming 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 [34], the difference between the virtual and real gradients was reduced by 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 [35] 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 [36] presented an accountable and effective data sharing system called ADS that may penalize participants with data leaking issues. However, a blockchain-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 blockchain, a decentralized, unhackable, and traceable distributed ledger technology, uses consensus protocols to ensure data privacy and data exchange security effectively [37]. The authors of [38] introduced a blockchain-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 [39] made the secure application and decentralized administration of massive data in the IoT possible using blockchain technology. On the other hand, A consensus mechanism that ensures the consistency of all participating nodes is essential as a crucial technology.

By simultaneously optimizing the location of the drone, the trajectory of the unmanned underwater vehicle, and their interconnection, the authors of [40] 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 [41] introduced RescueChain, a safe and effective information exchange system. Simple blockchain-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 [42]. 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 [43] introduced and discussed how blockchain technology fits with IDS, focusing mainly on the fundamental principles underlying blockchain technology, the various design considerations for creating blockchain implementations, the meaning of smart contracts, and the overall potential of blockchain. Before presenting additions to data integration workflows for dataspace support that goes beyond comparable efforts in data warehouses and data lakes, the authors of [44] 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 blockchain and FL for securing dataspace sharing among drones. Table 1 summarises the most recent and related work to the proposed framework; it highlights technology requirements addressed by the framework.

Table 1. Summaries of the most related works.

Ref.	A	B	C	D	E	F	G
[35]	Securing sensitive data sharing using proxy re-encryption approach	Yes	No	No	No	No	No
[36]	Highlighting an accountable and data sharing approach for Industrial Internet of Things (IIoT)	Yes	Yes	No	No	No	No
[38]	Blockchain for trusting data management	No	Yes	No	No	No	No
[43]	Designing dataspace advantages and ecosystem approaches	Yes	Yes	No	No	Yes	No
[85]	Establishing theoretical principles and foundations of real-time linked dataspaces	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 blockchain for drone data sharing	Yes	Yes	Yes	Yes	Yes	Yes

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

3. Overview of Technologies

3.1. Drones

The most famous drone services include publishing videos and images and broadcasting live videos. These forms of traffic are very resource-intensive on the uplink and have an impact on the functionality of the entire network. The drone divides the data it receives into three categories: delay-tolerant traffic, data that should be transferred to higher levels for processing, and data that will be copied at the drone level. When feasible, the drone saves the delay-tolerant traffic and sends it to the destination after the operation. Delay-tolerant traffic involves a specific spectrum of applications that drones can identify. Drones deployment with transceivers is viable for providing cellular infrastructure flexible assistance [45]. Drone-BSs can be placed where needed to increase ground users' signal quality and expand cellular coverage [46,47]. 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 [48] presented a platform to expand a B5G network slice for video surveillance utilizing a swarm of drones.

In [49], 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 authors introduced the framework and communication protocol to be used with the drone's airborne WSN [50–54]. 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 [49] employed cluster-based aerial data collecting. The network, made up of the sensor nodes placed in the environment under observation, was separated into several cluster zones. The aerial vehicle only needs to interact with the head cluster in the data collection zone when it is close to the cluster region to collect data there. The other member nodes must communicate through at least one relay node to upload the data to the aerial vehicle.

3.2. Blockchain technology

Blockchain, a distributed ledger amongst many users, enables efficient and permanent transaction recording with the utmost security and anonymity. Transaction verification is resistant to cryptography can add to the ledger by all participants in a blockchain without the requirement for a third party to validate and approve [55]. Public, private, and hybrid blockchains are the three subcategories of blockchains. In contrast to private blockchains, which only let particular users with permission, public blockchains (such as Ethereum and Bitcoin) enable everyone to join the network and participate. Since one of the participating entities influences the others, the private category of blockchain is more centralized than the public blockchain. A consortium blockchain is used in which a single business or a group of companies controls the network (e.g., Hyperledger). The benefits of public and private blockchains are combined in the hybrid category, which comprises hybrid blockchains. It offers members in the group privacy and openness.

Much work has been put towards improving data security in drone networks using the potential blockchain. To offload computationally demanding blockchain tasks, the authors of [56] developed a Blockchain-as-a-Service (BaaS) platform linked with MEC for IoT devices. A safe data collection system for MEC-enabled IoT networks is investigated [57], 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. [58] presented a blockchain-based decentralized fashion for data sharing where a Cournot model is developed to maximize advantages for air and ground sensors.

3.3. Federated Learning

FL is an ML technique that enables multiple parties to train ML models collaboratively without sharing their local data. Instead of centralizing the training data in a single location, FL distributes the model training across multiple devices or servers, allowing each device or server to train the model on its 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 (see Figure 2). 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. Technologies pertinent to FL include distributed databases, where data is kept in various physical locations. Distributed ledgers have digital systems for synchronizing transactions. For example, a blockchain is a distributed ledger where numerous independent computers validate transactions. Therefore, to build a safe ecosystem that can stop privacy leakage from every connection from data collection to final prediction, including local gradients, aggregators, etc., it is imperative to construct a non-interactive and privacy-preserving FL scheme.

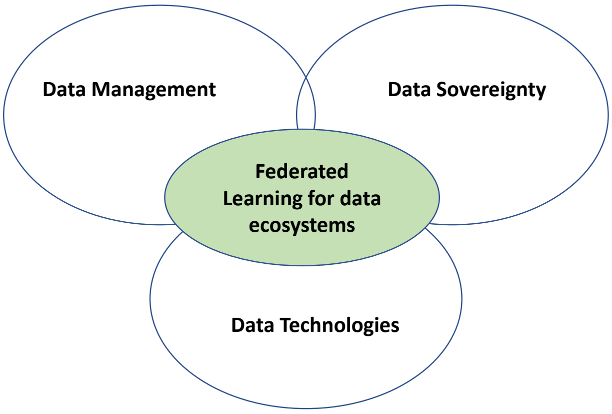

Figure 2. FL and data ecosystems.

Summary: FL can be particularly useful in decentralized environments, where data is stored across multiple nodes. Using FL, each node can train an ML model on its local data without sharing it with other nodes. The resulting models can then be aggregated to create a global model that all nodes in the network can use. In addition, FL provides a way to secure data sharing in other decentralized environments, such as IoT networks or edge computing systems. By training ML models locally, systems can avoid transmitting sensitive data over the network, reducing the risk of data breaches and privacy violations. FL offers a way to train ML models on sensitive data without disclosing that data to others, making it a potent tool for securing data sharing in decentralized environments.

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 [61]. Data-sharing strategies must balance user privacy and a positive user experience while boosting business profits [62]. Blockchain clarifies the quandaries surrounding when, what, and with whom to share data

[62]. Additionally, blockchain facilitates how the data owner should be compensated as a perk for giving their information. Users' data is gathered for business purposes via social media platforms by various firms, who utilize it to improve their business models and better serve their clientele. 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 [63]. According to the dominant paradigm of data ownership, which is frequently represented in service license agreements, data ownership is assumed to be transferred to the organization that collects it and has access to share it with its corporate network. Liu et al. [64] developed a collaborative architecture that integrates the Ethereum blockchain and deep reinforcement learning for effective data collection and safe data sharing to suit the needs of the mobile crowdsensing-based Industrial IoT. The authors of [65] introduced a blockchain-authorized safe 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 into the approved blockchain.

3.5. Dataspace 4.0 empowered Industry 4.0/5.0

The Industry 4.0 paradigm's technocratic emphasis on new technology and digitalization. As a result, the discussion concerning the function of 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 [66] analysed 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, reduce mental workload, and improve data-sharing cognitive ergonomics [67].

Less data sharing is required for privacy-preservation strategies, which would prevent ML models from adequately customizing themselves because clear information fields would be obscured. Furthermore, the anomalous behaviour of smart devices is not taken into account. Therefore, privacy and security-based solutions are insufficient. In Industry 5.0, where diverse and autonomous networks cooperate, data exchange and control trust are essential. Blockchain is a promising solution that can create transparent ledgers with easy control and management of industrial process data. A shared, distributed, and immutable ledger called blockchain 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 [68]. Consensus procedures play a significant part in the efficient management of the blockchain network and regulate the blockchain 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 blockchain is an ideal method for managing and orchestrating real-time data [69].

Through networking protocol stacks, the data is shared across wireless channels over smart environments. Another example of an industry use case is logistics, where products are sent and ML algorithms are employed to guarantee the accuracy of the shipped goods. Food products must be kept fresh throughout the entire production process and until they are sold on the market. There are numerous intermediate sites in the supply chain, and each one is watched to ensure that the product is still fresh [70]. Supply-chain-based greedy algorithm used by drones overloads the computational capacity of sensor nodes in smart factories. Data is collected by drones and given to edge nodes, which then distribute it to other peer nodes for quicker processing [71]. Inventory transactions are maintained on edge devices that install FL models to identify swarm drone mobility irregularity and record the data on blockchain ledgers to support drone operations [72].

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 industries. 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 [133]. 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 blockchain, dataspace 4.0 can provide a secure and efficient platform for sharing data among stakeholders, including companies, individuals, and governments. 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 centres and minimizing the risk of data breaches or other security incidents.

3.6. Dataspace

Dataspace is a new paradigm for serving the data integration and usage requirements of smart environments, including sharing of events and historical data. This approach is considerably different from existing approaches of data management. The dataspace approach acknowledges that it is challenging and expensive to produce an upfront unifying schema across all data sources in large-scale integration situations, which comprise of thousands of data sources [73]. Dataspaces move the focus to support the co-existence of diverse data without requiring a significant initial investment into generating a unifying schema. Dataspaces use 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. Dataspaces have been developed to manage personal information [74], astronomical data [75], and biomedical data [76]. The utility of dataspaces has also been investigated in various settings such as data curation [77], context-based search [78], data modelling [79], data gathering [80], and customer feedback [81].

Dataspaces can offer a method for enabling information management in highly dynamic environments, assisting in addressing the conceptual and technical obstacles to information interoperability. However, research on implementing the dataspace concept in intelligent environments and examining the pertinent support services required for real-time data sources has been limited. Nevertheless, the creation of dataspaces has been attempted in the past in several contexts, including the system of systems [82], energy data management [83], and building data management [84]. Figure 3 shows the example design of a dataspace for real-time and linked data sources.

Summary: 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 is often used to emphasize that data is a valuable resource that should be managed and treated as a collective information space rather than as 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.

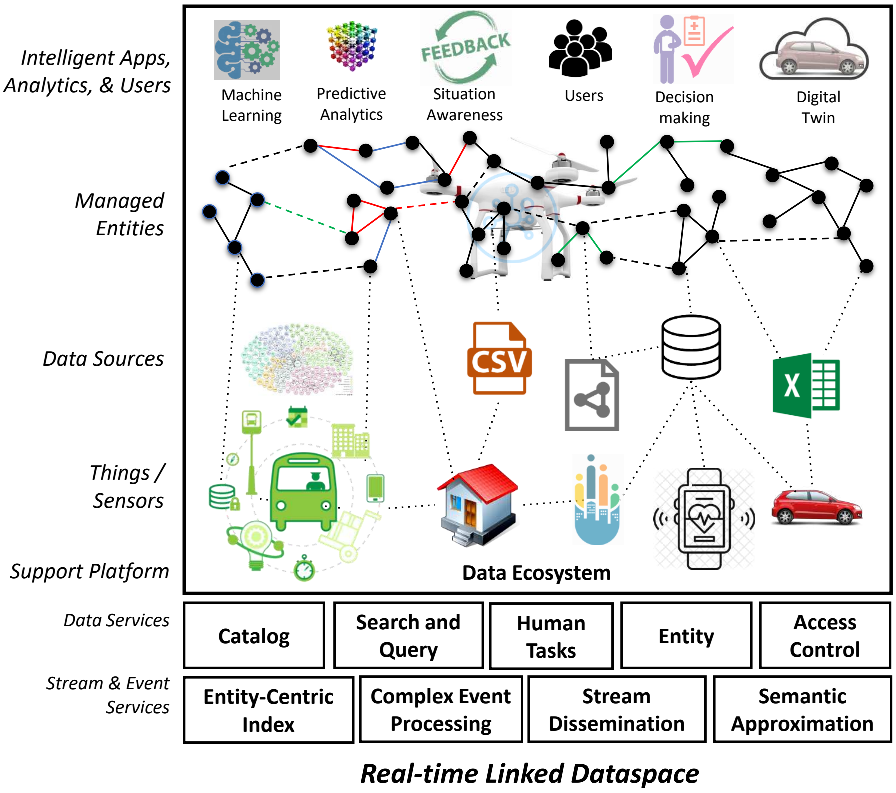

Figure 3. Real-time linked drone dataspace (Adapted from [85]).

3.7. Mobility dataspace through drones

The community for data sharing where everyone tries to create and make available data for the mobility of the future 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 the circumstances of 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. Figure 4 shows an overview of drone dataspace for supporting various mobility events in which drones' function is to gather mobility data from different environments.

The applications of the mobility drone dataspace can offer valuable insight into people's movement patterns that address public concerns, including public health, urban planning, transportation, poverty, migration, and disaster response. The role mobility of drone dataspace plays in assisting researchers in addressing social issues is vast in scope, but it may be divided into i) prescriptive, (ii) predictive, and (iii) descriptive.

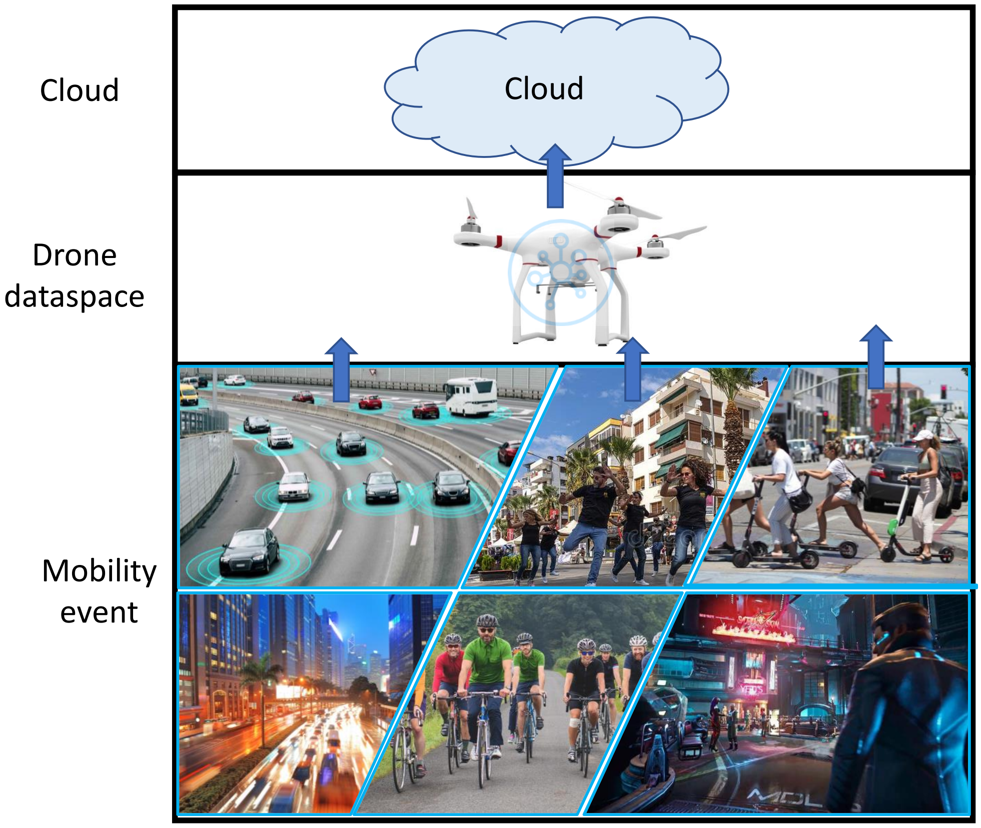

Figure 4. Drone dataspace supporting mobility events.

Summary: The mobility aspect of drone dataspace refers to the ease with which drone data can be transferred, shared, and accessed across different devices, platforms, and locations. A mobile drone dataspace makes it possible to quickly and easily share drone data with relevant stakeholders, whether in the same location or somewhere else. This can support more effective collaboration and decision-making and help organizations respond quickly to changing needs and opportunities. For example, in a disaster response scenario, a mobile drone dataspace can allow for the real-time sharing of aerial images and video, helping to direct response efforts and allocate resources more effectively. In agriculture, a mobile drone dataspace can help farmers make informed decisions by providing real-time crop health and yield data. The mobility of a drone dataspace is vital for unlocking the full potential of drone technology and ensuring that organizations can use drone data flexibly and effectively.

3.8. Smart environments

The construction and operation of smart environments are driven by two factors: capturing environmental data and enabling meaningful use of that data by people. 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 [86]. Furthermore, the authors of [87] 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 [88] and smart transportation [89,90], etc. The authors of [91] highlighted the collaboration of drones and IoT for public safety in smart cities with improving network performance and QoS. While the collaboration of multi-drone and

Search and rescue teams is used for disaster management [16–18]. Moreover, blockchain technology is used to manage and decentralize multi-drone collaboration [92], empowering the security of drone swarm in a smart environment [93]. Moreover, the combination of FL and blockchain helps to improve drone edge intelligence performance in smart environments [94].

For real-time dataspace important to improve smart cities applications, the authors of [95] explored how catalogues in dataspaces help satisfy this requirement; they then detailed how entity management services may be used to manage entity data more efficiently within a dataspace. In [96], 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 the digitalization of the environment using IoT and big data, and the second is on 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 of [97] 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" are driven by acquiring environmental data and enabling people to use that data meaningfully, sometimes changing behaviour. The IoT and big data, which enable the digitalization of physical infrastructures with sensors, networks, and social capabilities, are two fundamental technologies driving smart environments' development. 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 with the purpose of collecting public data about things like traffic and human mobility. Data-driven learning is a sophisticated ML technique focused heavily on data collecting, pattern recognition, and data prediction. The authors of [99] examined how DL approaches have recently advanced in relation to 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.

Harsh environments are challenging for drones to operate in due to various factors such as extreme weather conditions, rough terrain, and limited accessibility. These environments can pose risks to the safety of drones and their operators and affect the quality and reliability of data gathered by drones. Examples of harsh environments include disaster zones, construction sites, and remote areas with limited infrastructure. By enabling secure and efficient data sharing among drones in these environments, the proposed framework can enhance the capabilities of drones and improve their effectiveness in performing various tasks. Drones computing is used to manage rescue teams in harsh environments [19].

4. Framework of dataspace in sky

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. We assume that multiple drone collaborators will be involved in collaborative information modelling and sharing. Multiple drone collaborators work together to jointly model the specified job 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 blockchain as the network architecture for the decentralized collaboration system to store, retrieve, and audit the collaborative modelling process to ensure data provenance and security. In this novel framework, we detail the FL and blockchain

doi:10.20944/preprints202305.0529.v1

combination, to achieve data sharing between drones dataspace in a decentralized fashion. The high-level concept framework with architecture layers is shown in Figure 5.

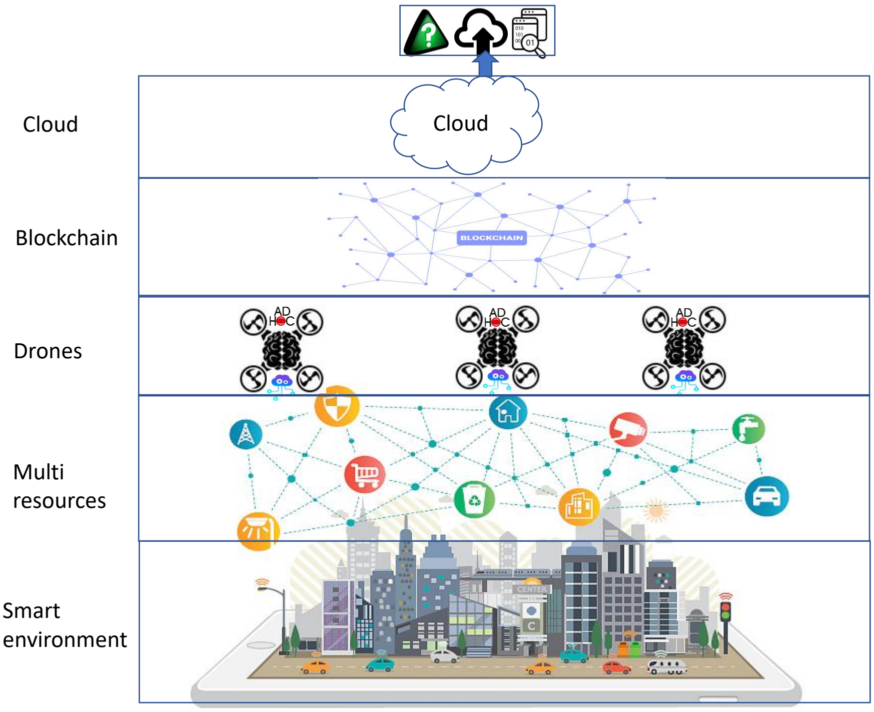

Figure 5. Dataspace in the sky.

Smart environment layer: A smart environment consists of a massive number of smart devices that gather data from their surroundings and other sensing devices of numerous characteristics [100]. Smart devices collect perception data, which is then sent to drones for further analysis and sharing. In Figure 5, the smart environment equates to a smart city that is 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 themselves can also gather data automatically about the environment. Therefore, drones have two functions here, either gathering data from smart devices deployed in smart environments or gathering data directly from smart environments.

Summary: A dataspace in a smart environment refers to the distributed repositories where this data is stored and analyzed. The dataspace provides a set of services for managing the data generated by the smart environment, making it easier to extract insights, identify patterns, and make decisions that can improve the performance and efficiency of the environment. For example, in a smart building, a dataspace could be used to store and analyze data from sensors that monitor temperature, light levels, and energy usage, helping optimize energy consumption and create a more comfortable environment for the occupants. Likewise, in a smart city, a dataspace could be used to store and analyze traffic sensors' data, helping optimize traffic flow and reduce congestion. Briefly, the dataspace in a smart environment plays a critical role in the management and optimization of the environment, making it an essential component of the overall smart environment ecosystem.

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 the execution of basic data operations. Therefore, management of gathered data in drone technology is required to save energy [101], reduce latency and enhance the quality of service [102]. 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 [103] 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 allows for more flexible and effective data management as needed by mobile drones and easier 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 data. Each layer would represent a different source of data, 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 blockchain and cloud layers for data sharing. Drones must share information among themselves to avoid collisions and manage the drone coverage area. In [104], drone computing is highlighted by discussing requirements, challenges and future directions. 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, drone data sharing plays a vital role in improving drones' performance and operation during task performance. In this layer, several technologies (i.e., blockchain, 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 show significant benefits in 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 [105]. Furthermore, in [106], creating clusters 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. For improving security, drones depend on BSs, which can be easily attacked. Therefore, blockchain 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 [107] 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 [107] conducted a security analysis to determine the security objectives and examined several fake attack strategies on data dissemination. In drones, architecture is designed using blockchain, which uses a proof-of-stake consensus protocol for the block validation and uses game theory to identify the forger node [108]. Therefore, the authors of [109] presented increases 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 support 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 dataspaces, 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.

In summary An Ad-hoc network can be an effective solution for supporting a drone dataspace, enabling real-time data transfer and communication between drones and other devices, and providing benefits such as increased flexibility, scalability, reliability, and availability.

Table comparing the advantages and drawbacks of different communication technologies in the context of the proposed framework:

Table 2. Advantages and drawbacks of communication technologies for supporting proposed framework.

Technology	Advantages	Drawbacks	Potential Impact on Time-based Blockchain 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 blockchain
5G	High data rates, Low latency,Massive connectivity	Requires infrastructure, Coverage limitations in remote areas	Reduced chances of data inconsistencies or delays in the blockchain
B5G	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 blockchain performance, but subject to future development and implementation

2. **FL :** FL is certainly 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 [110]. 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 [110]. However, there are still additional FL-related problems; malicious actors may try to access the client's dataset or compromise the global model. Additionally, the client's lack of desire or incentive to work with the FL system can become an issue. Adopting and utilizing blockchain technologies for FL applications might solve this problem.

   In a drone dataspace, FL can also be used to 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.

In summary, FL in drone dataspaces can improve drone performance while providing benefits such as improved data privacy, model accuracy, and more efficient model training.

Table 3. Proposed framework solutions and benefits.

Proposed solution	**Benefits**	**Decentralized Data Sharing**	**Security**
Drones dataspace	Flexible and mobility, High-quality data, Provide services close to user, Efficient data management	NA	Traditional methods, Vulnerable to attacks
Blockchain	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 blockchain	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-level 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 dataspace sharing	Efficient and high-level security and privacy

Summary: Drone dataspace is a system for collecting, storing, and organizing drone-generated data. Drone dataspaces can include flight paths, video and imaging data, flight performance metrics, and telemetry data. This data can be used for various purposes, such as analyzing flight performance, improving drone design, and creating maps and models for various industries, including agriculture, construction, and environmental monitoring. The data can also be used to support decision-making processes, such as identifying areas for infrastructure improvement, monitoring environmental changes, and supporting disaster response efforts. A drone dataspace is a crucial tool for managing, analyzing, and leveraging the vast amounts of data generated by drone operations.

Blockchain layer: The drones use blockchain to record the parameters of each local model as they train their local models using their local data sets. Then, the aggregation approach employed by FL and blockchain produce the Global Model (GM). The joint modelling model GM is finally added to the blockchain, and the task requester uses the blockchain to access the result Req GM from the joint modelling model. We categorized the transactions in the blockchain 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, when they contribute professional data, they will set the data privacy level to public data in the community.

A drone receives a unique identification when it registers a blockchain account. There are two ways to encrypt data acquired by the 6G drone before it is transferred to the cloud. One method involves the drone encrypting the data with an allocated symmetric key and sending the ciphertext to the node management. The key is then encrypted by the node management 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 key production. A user is a person capable of decrypting and reading gathered data and instructions.

The following describes the secure data sharing procedure for B5G drones based on the blockchain as shown in Figure 6. First, the drone encrypts the symmetric encryption key and the data it has acquired using symmetric encryption. The drone then requests data upload from the blockchain. Following receipt, the blockchain verifies the request using a pre-negotiated smart contract. The blockchain provides the drone with a credential if the request is legitimate. The drone uploads the ciphertext and the credential to the cloud as soon as it receives them. When the ciphertext is determined to be legitimate, the cloud saves it and notifies the blockchain of the storage confirmation. The distributed ledger of the blockchain stores the shared ciphertext data as transactions. The blockchain 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 mechanism for distributing communication keys among drones is similar.

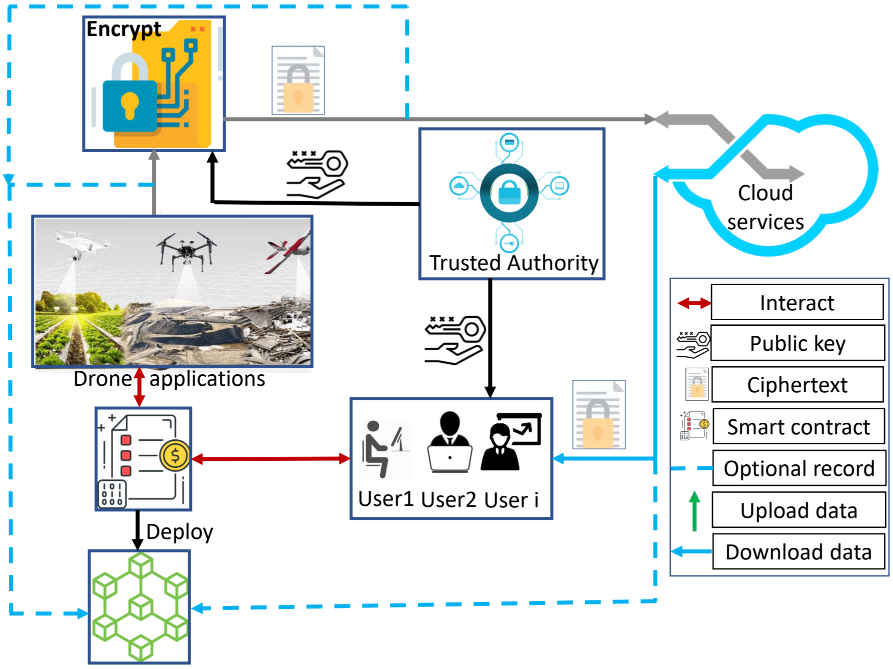

Figure 6. Blockchain enabling securing dataspace sharing in the sky.

The conceptual framework of drone dataspace includes the network, FL, task, mobility, communication, and threat models. The blockchain-empowered FL for dataspace in the drone-assisted MCS scenario is depicted in Figure 7 and comprises several drones, task publishers, MEC nodes, BSs, and a consortium blockchain. Therefore, data owners and requestors can share data quickly and reliably while storing the sharing records on the blockchain for tracking.

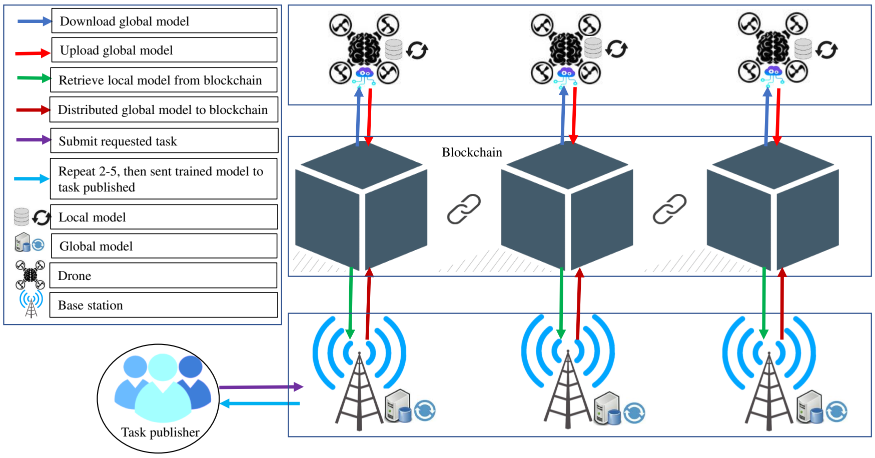
Download global model
Upload global model
Retrieve local model from blockchain
Distributed global model to blockchain
Submit requested task
Repeat 2-5, then sent trained model to task published
Local model
Global model
Drone
Base station
Blockchain
Task publisher

Figure 7. Combination of FL and blockchain for data sharing and processing.

Cloud: The cloud processing layer handles the data storage and heavy lifting involved in drones 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 [111]. 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, which aggregates all of the local FL models and keeps the global FL model in the cloud [112]. Table 3 describes the proposed framework solutions and their benefits for drones decentralized dataspace sharing. Table 4 illustrates the comparison of the proposed framework with well-known competitors, advantages, and drawbacks.

Table 4. Comparison of the proposed framework technologies with well-known competitors.

Competitor	Advantages	Drawbacks
Blockchain	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 machine learning 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-Subscribe 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

Combination of technologies and applications: The combination of technologies (i.e., FL and blockchain and drones) creates a decentralized drone dataspace sharing solution that increases security and privacy for the data being shared. In the proposed framework, each drone would contribute 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 blockchain, creating an immutable and secure ledger of the model's evolution. Additionally, this setup provides increased transparency and trust, as all network participants can see the model updates and verify their authenticity. Therefore, combining technologies will achieve a decentralized drone dataspace sharing solution that can provide improved data privacy and security. The combination of FL and blockchain technology for drone dataspace sharing provides several benefits, as shown in Table 5:

Table 5. Combining FL and blockchain 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, while the updates to the model are recorded on the blockchain, providing a secure and transparent record of the model's evolution.
Increased transparency and trust	Blockchain 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 blockchain improves the drone dataspace to many participants in 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 blockchain, it is secure and efficient to share data between participants, even in large and complex networks.

In summary: The amalgamation of FL, blockchain, and B5G for drones dataspace sharing plays a vital role in improving many applications. The security of sensitive data is of vital importance in many applications such as smart manufacturing, healthcare, etc. Thus, the primary motivation for FL is that the model is trained locally without sharing the data from nearby smart environments with the help of drone technology. Therefore, FL guarantees the privacy and security of shared data between drone networks or swarms. Contrarily, blockchain technology ensures drone trust in distributed, open, and autonomous smart environments through cryptography techniques and consensus procedures. As a result, blockchain-enabled FL-driven drones communicate the learning outcomes via transactional ledgers to prevent changes to model gradients, weights, and other parameters. Additionally, the global server can save the global model meta-data on the blockchain, which the local drone can then download. Drone networks produce enormous amounts of data in real-time environments. As a result, there is a need for extremely low latency, near-real-time communication. Thus, the latency and bandwidth requirements of huge drone communication can be orchestrated by B5G networks. Additionally, it supports mobile operations, tight end-latency specifications, and dense drone connectivity. With tailored connectivity to meet specific needs, the B5G network design is expected to facilitate deep sea-air-ground communication and enormous information-centric IoT networks.

5. Validation of proposed framework

In this section, we validate the proposed dataspace in the sky framework. We aim to secure data sharing decentralised using multi-drone to support dataspace 4.0 in Industry 4.0 and Industry 5.0 applications. For this purpose, we considered the combination of blockchain and FL to satisfy the aforementioned high-level requirements. The main purpose of combining blockchain and FL is to facilitate distributed drones' secure collaboration. All miners may independently verify the quality of models uploaded and stored on the blockchain thanks to the decentralized accountability system. Table 7 summarises how the benefits of technologies and techniques are mapped to the stated framework criteria.

5.1. Validation 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 B5G and beyond [134], research on a blockchain-based framework for secure and efficient data sharing in the Internet of Vehicles [135], and a decentralized framework for secure data sharing and privacy preservation in smart communities [136,137]. The proposed framework presents several novel aspects that differentiate from existing frameworks and technologies:

Decentralized Framework: The proposed framework is based on a decentralized architecture leveraging blockchain. 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 privacy and single point of failure risks. Table 6 gives the comparison of the proposed framework and traditional centralized data sharing.

Table 6. Comparison of the proposed framework and traditional centralized data sharing.

Aspect	Proposed framwork	Traditional Centralized Data Sharing
Architecture	Decentralized using blockchain	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 B5G and Dataspcae 4.0 Environments	Tailored for B5G and Dataspcae 4.0 environments	May not be optimized for specific requirements

Smart Contract-based Governance: 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.

B5G and Dataspcae 4.0 Focus: The proposed framework addresses the challenges of secure drone data sharing in B5G 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 blockchain, and smart contract-based governance provide innovative solutions to these challenges.

Enhanced Security: The proposed framework ensures data security through blockchain, which provides tamper-proof and transparent data storage. Additionally, 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.

Enhanced Resilience: The decentralized architecture and use of blockchain in the proposed framework provide enhanced 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 7. Proposed framework validation.

Requirement	Enabled by
Data collection	Smart devices in smart environments
Data processing locally	FL techniques
Local model	Drones
Global model	DataSpace
Authentication	Blockchain technology
Data Sharing	Blockchain and Fl
Decentralized	FL, blockchain and ad hoc networks
Collaboration	Blockchain and consensus algorithms

Decentralized dataspace sharing in drones : Drones need to collaborate and share tasks to share data and take appropriate action. To (1) maintain trust among P2P networks [116], (2) enable traceability across drone networks [117], (3) provide insightful consensus-based decision-making processes [118], and (4) deliver efficient solutions by utilizing the decentralization feature of blockchain technology [119], it is advantageous for dataspace sharing among drones to use blockchain technology. The shared data is divided among the multiple drones covering an event in the dataspace in the sky framework solution. To give the highest service performance, many drones are often employed to cover different areas in an active region because drones can connect and work together by sharing resources. In [120] presented a model-based blockchain 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 safe data sharing involves four stages: initialization, identity authentication, signature and verification, and then data sharing. Drones 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 B5G to satisfy Industry 4.0 and Industry 5.0 expectations. Drones data sharing can be made possible by combining blockchain 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 blockchain 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 blockchain offers data sharing among multiple drones during activities in smart environments to satisfy Industry 4.0 and Industry 5.0 needs.

The data is data near the user and then split into groups of service blocks and distributed across the drones by the cloud. The cloud can determine the location of the grouped messages based on sensor sources. Then, the data is duplicated and sent to the drones patrolling the area to efficiently distribute the information and give interested users quick access to the service. Data management is then divided across the drones by data management according to their position and available storage. Blockchain 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 performance of the entire network. 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. (Figure 8). When feasible, the drone saves delay-tolerant traffic and sends it final destination after the operation. 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 of time before recharging. When this happens, the drone travels to the closest charging station, distributes the stored delay-tolerant traffic from there, 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 area [15]) 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.

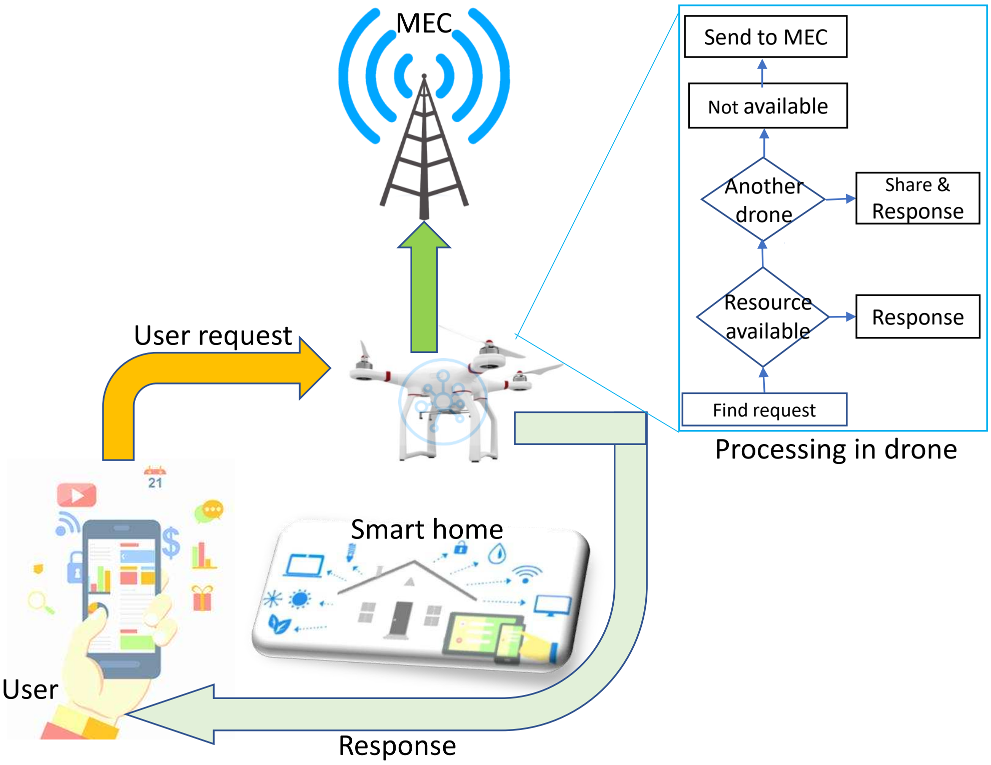

Figure 8. Data sharing and processing in drone.

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 that are 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 reduces 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 B5G networks, FL, and blockchain, 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 modelling 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 blockchain technologies, which have the potential to address the security and privacy concerns in drone 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.

The evaluation of the proposed framework is based on the following metrics given in Table 8.

Table 8. Evaluation metrics for framework validation.

Metrics	Description
Data privacy and security	The level of privacy and security provides to protect sensitive data from unauthorized access or modification
Model accuracy	The accuracy of the models 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 modelling process

5.2. Validation based on testing 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 blockchain for decentralized drone dataspace involves creating a platform for drones to share data while preserving the privacy and security of the data. The platform utilizes FL, allowing multiple drones to train an ML model collaboratively without sharing their raw 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. This approach allows drones to learn from each other without sharing sensitive data, preserving the privacy of the data and the drones themselves. The platform also utilizes blockchain technology, which provides a secure and transparent digital ledger for storing and sharing data. Blockchain 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. There are numerous applications for combining FL and blockchain for decentralized drone dataspace data sharing. Some of the key applications include:

1. **Precision agriculture:** It uses technology to optimize agricultural production while reducing waste and environmental impact. Drones are an essential technology for precision agriculture, as they can collect high-resolution data on crop health and growth that is difficult or impossible to obtain from the ground. By combining FL and blockchain for drones' 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 optimising 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 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 blockchain for drone dataspace 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 that are particularly hard-hit by the disaster 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 blockchain for drone dataspace sharing optimize disaster response efforts by allowing drones to share data and train ML models that can help identify areas of need and optimize the delivery of aid. 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 blockchain for drone dataspace 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 be used to 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 efforts' effectiveness and help protect human health and the environment. This can lead to better environmental outcomes and a healthier planet overall. In summary, combining FL and blockchain for drone dataspace sharing improve environmental monitoring efforts by allowing drones to share data and train ML models that can help identify patterns and trends in the data. This can lead to better-targeted interventions to address environmental issues and protect human health and the environment. Table 9 describes how technologies are used in the proposed framework in the use cases, i.e., Precision Agriculture, Environmental Monitoring, and Disaster Response. Furthermore, Table.10 illustrates the validation criteria of the use cases.

Table 9. Description of the 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.
Blockchain	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 drones dataspace, preserving data privacy and security and enabling improved decision-making for precision agriculture management, environmental management, and disaster response and recovery.
B5G	Enabling 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 decentralized data sharing for precision agriculture, including drone data, sensor data, and situational awareness information.

Table 10. Use case and validation criteria.

Use case	Validation Criteria
Precision agriculture	Ability to secure the sharing of drone data among different stakeholders. Effectiveness in protecting the privacy of sensitive agricultural data.
Monitor environment	Ability to secure the sharing of environmental data among different stakeholders. Effectiveness in ensuring data integrity. Ability to prevent unauthorized access to sensitive environmental data.
Disaster response	Ability to facilitate the secure sharing of disaster response data among stakeholders. Effectiveness in ensuring the timely and efficient sharing of critical disaster response data.

6. Challenges and future directions

1. **Deployment optimization for ground BSs:** In blockchain-based drones in B5G networks, the ground BSs serve as miners, which is a significant role. When few ground BSs are available or a heterogeneous B5G network, it can be difficult to develop the best ground BSs deployment schemes to increase communication reliability further and decrease communication time between moving drones and miners.
2. **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. The failure is an unwelcome occurrence that can make a drone 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 a significant quantity of 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.
3. **ML for efficient miner selection:** Using machine learning-based approaches, such as DRL [125], to design efficient and secure miner selection schemes is a promising direction. This is because

ML has the great potential to solve complex decision-making problems of wireless networks. We can also investigate effective and simple DRL deployment strategies for ground BSs in massive drones in B5G networks using swiftly moving drones.

4. **Data security:** Since each drone only stores duplicated data after verifying its source, the usage of blockchain 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 blockchain, 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 supports drones to develop portable defensive systems with assured data integrity [126]. Ensuring the security and privacy of the data shared among drones in a decentralized fashion is challenging. While blockchain provides security and transparency, potential vulnerabilities and attacks could still compromise the system. To address this challenge, exploring advanced encryption and authentication mechanisms require to protect the data and ensure secure communication between drones.
5. **Assessment criteria for miner:** In conventional blockchain 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 [127]. 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.
6. **Miner selection:** The current permissioned blockchains choose miners in a decentralized manner using insecurely random selection techniques, in contrast to permissionless blockchains that do so using proof-based algorithms and suffer from single-point-of-failure issues [128]. As a result, the miner selection algorithms are arbitrary and cannot counteract malicious nodes' influence.
7. **Drone energy:** Due to drone LoS links, drones that fly above events can give ground users favourable coverage. In addition, as edge devices, drones can enhance existing infrastructure 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: travelling 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 [129**?**]. 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.
8. **Monitoring selected miners:** Because permissioned blockchains are decentralized, monitoring certain miners in real-time is complicated and inefficient. Due to a lack of timely and flexible surveillance techniques, removing a chosen miner from the system is impossible if it is compromised and misbehaves. Even worse, compromised miners can be chosen to resume mining without time-accumulated measurements to update the performance and behaviour of the miner candidates.
9. **Drone service provider:** The QoS provided has always benefited from competition amongst 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.

10. **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 [130]. Furthermore, the combination of blockchain and DT are used for solving real-time applications such as transportation [131] and delivery during a pandemic [132].
11. **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.
12. **Interoperability:** Ensuring the interoperability of the different technologies used in the framework is challenging, including FL, blockchain, and B5G networks. 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.

7. Conclusion

In this conceptual framework, we have introduced a novel framework for drone dataspace in B5G for dataspace 4.0. When several users share the same network resources, the network infrastructure becomes saturated by the large number of simultaneous requests, which lowers performance. The data is transmitted by drones that follow their position and are filled to their maximum capacity. For securing data sharing, we have presented the combination of blockchain and FL for high-level data sharing security among drone dataspace networks. The combination can drive different drone dataspace applications in Industry 4.0/ Industry 5.0. Moreover, we outlined the challenges and future directions of combining FL and blockchain for drone dataspace in B5G. Finally, it is concluded that drones dataspace can support effectively and efficiently dataspace technology and lead to a new revolution in the next generation of dataspace. Furthermore, the combination of FL and blockchain would serve as a high level of trust and secure solutions for drones' dataspace networks over smart environments.

Funding: This publication has emanated from research supported in part by a grant from Science Foundation Ireland under Grant number SFI/12/RC/2289 P2. For the purpose of Open Access, the author has applied a CC BY public copyright licence to any Author Accepted Manuscript version arising from this submission.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. O. Bouachir, M. Aloqaily, F. Garcia, N. Larrieu, and 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. Alsamhi, S. H., Rajput, N. S., & Mishra, V. N. Guarantee QoS in Coexistencee of High Altitude Platform System and WiMAX TerrestrialSystem.
3. Alsamhi, S. H., & Rajput, N. S. (2015). An intelligent HAP for broadband wireless communications: developments, QoS and applications. International Journal of Electronics and Electrical Engineering, 3(2), 134-143.
4. Alsamhi, S. H., & Rajput, N. S. (2015). An intelligent hand-off algorithm to enhance quality of service in high altitude platforms using neural network. Wireless Personal Communications, 82(4), 2059-2073.
5. Alsamhi, S. H., & Rajput, N. S. (2016). Implementation of call admission control technique in HAP for enhanced QoS in wireless network deployment. Telecommunication Systems, 63(2), 141-151.
6. Alsamhi, S. H., & Rajput, N. S. (2016). An efficient channel reservation technique for improved QoS for mobile communication deployment using high altitude platform. Wireless Personal Communications, 91(3), 1095-1108.
7. Alsamhi, S. H., & Rajput, N. S. (2014, 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 (pp. 1-6). IEEE.
8. Gupta, A., Sundhan, S., Gupta, S. K., Alsamhi, S. H., & Rashid, M. (2020). Collaboration of UAV and HetNet for better QoS: a comparative study. International Journal of Vehicle Information and Communication Systems, 5(3), 309-333.
9. Alsamhi, S. H., Almalki, F. A., Al-Dois, H., Othman, S. B., Hassan, J., Hawbani, A., ... & Saleh, H. (2021). Machine learning for smart environments in B5G networks: connectivity and QoS. Computational Intelligence and Neuroscience, 2021.
10. Saraswat, D., Verma, A., Bhattacharya, P., Tanwar, S., Sharma, G., Bokoro, P. N., & Sharma, R. (2022). Blockchain-Based Federated Learning in UAVs Beyond 5G Networks: A Solution Taxonomy and Future Directions. IEEE Access, 10, 33154-33182.
11. S. Garg, A. Singh, S. Batra, N. Kumar, and L. T. Yang, "UAV-empowered edge computing environment for cyber-threat detection in smart vehicles," IEEE network, vol. 32, no. 3, pp. 42-51, 2018.
12. P. Mehta, R. Gupta, and S. Tanwar, "Blockchain envisioned UAV networks: Challenges, solutions, and comparisons," Computer Communications, vol. 151, pp. 518-538, 2020.
13. T. Dasu, Y. Kanza, and 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.
14. J. Kang, Z. Xiong, D. Niyato, D. Ye, D. I. Kim, and J. Zhao, "Toward secure blockchain-enabled internet of vehicles: Optimizing consensus management using reputation and contract theory," IEEE Transactions on Vehicular Technology, vol. 68, no. 3, pp. 2906-2920, 2019.
15. Alsamhi, S. H., Almalki, F., Ma, O., Ansari, M. S., & Lee, B. (2021). Predictive estimation of optimal signal strength from drones over IoT frameworks in smart cities. IEEE Transactions on Mobile Computing.
16. Alsamhi, S. H., Almalki, F. A., AL-Dois, H., Shvetsov, A. V., Ansari, M. S., Hawbani, A., ... & Lee, B. (2021). Multi-drone edge intelligence and SAR smart wearable devices for emergency communication. Wireless Communications and Mobile Computing, 2021.
17. Saif, A., Dimyati, K., Noordin, K. A., Alsamhi, S. H., & Hawbani, A. (2021). Multi-UAV and SAR collaboration model for disaster management in B5G networks. Internet Technology Letters, e310.
18. Alsamhi, S. H., Ansari, M. S., & Rajput, N. S. (2018). Disaster coverage predication for the emerging tethered balloon technology: capability for preparedness, detection, mitigation, and response. Disaster medicine and public health preparedness, 12(2), 222-231.
19. Alsamhi, S. H., Shvetsov, A. V., Kumar, S., Shvetsova, S. V., Alhartomi, M. A., Hawbani, A., ... & Nyangaresi, V. O. (2022). UAV computing-assisted search and rescue mission framework for disaster and harsh environment mitigation. Drones, 6(7), 154.
20. S. Aggarwal, N. Kumar, and S. Tanwar, "Blockchain-envisioned UAV communication using 6G networks: Open issues, use cases, and future directions," IEEE Internet of Things Journal, vol. 8, no. 7, pp. 5416-5441, 2020.
21. M. Aloqaily, I. Al Ridhawi, and M. Guizani, "Energy-aware blockchain and federated learning-supported vehicular networks," IEEE Transactions on Intelligent Transportation Systems, 2021.

22. H. Chao, A. Maheshwari, V. Sudarsanan, S. Tamaskar, and D. A. DeLaurentis, "UAV traffic information exchange network," in 2018 Aviation Technology, Integration, and Operations Conference, 2018, p. 3347.
23. X. Liang, J. Zhao, S. Shetty, and D. Li, "Towards data assurance and resilience in IoT using blockchain," in MILCOM 2017-2017 IEEE Military Communications Conference (MILCOM), 2017: IEEE, pp. 261-266.
24. Curry, E., Derguech, W., Hasan, S., Kouroupetroglou, C., & ul Hassan, U. (2019). A real-time linked dataspace for the internet of things: enabling “pay-as-you-go” data management in smart environments. Future Generation Computer Systems, 90, 405-422.
25. F. Gao, L. Zhu, M. Shen, K. Sharif, Z. Wan, and K. Ren, "A blockchain-based privacy-preserving payment mechanism for vehicle-to-grid networks," IEEE network, vol. 32, no. 6, pp. 184-192, 2018.
26. M. Shen, Y. Deng, L. Zhu, X. Du, and N. Guizani, "Privacy-preserving image retrieval for medical IoT systems: A blockchain-based approach," IEEE Network, vol. 33, no. 5, pp. 27-33, 2019.
27. Q. Xia et al., "Secured fine-grained selective access to outsourced cloud data in IoT environments," IEEE Internet of Things Journal, vol. 6, no. 6, pp. 10749-10762, 2019.
28. T. Alladi, V. Chamola, N. Sahu, and M. Guizani, "Applications of blockchain in unmanned aerial vehicles: A review," Vehicular Communications, vol. 23, p. 100249, 2020.
29. J. Qiu, D. Grace, G. Ding, J. Yao, and Q. Wu, "Blockchain-based secure spectrum trading for unmanned-aerial-vehicle-assisted cellular networks: An operator’s perspective," IEEE Internet of Things Journal, vol. 7, no. 1, pp. 451-466, 2019.
30. K. Bonawitz et al., "Towards federated learning at scale: System design," Proceedings of Machine Learning and Systems, vol. 1, pp. 374-388, 2019.
31. J. Konečný, H. B. McMahan, D. Ramage, and P. Richtárik, "Federated optimization: Distributed machine learning for on-device intelligence," arXiv preprint arXiv:1610.02527, 2016.
32. A. Fallah, A. Mokhtari, and A. Ozdaglar, "Personalized federated learning: A meta-learning approach," arXiv preprint arXiv:2002.07948, 2020.
33. M. Nasr, R. Shokri, and 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), 2019: IEEE, pp. 739-753.
34. L. Zhu, Z. Liu, and S. Han, "Deep leakage from gradients," Advances in neural information processing systems, vol. 32, 2019.
35. X. Dong, R. Li, H. He, W. Zhou, Z. Xue, and H. Wu, "Secure sensitive data sharing on a big data platform," Tsinghua science and technology, vol. 20, no. 1, pp. 72-80, 2015.
36. C. Huang, D. Liu, J. Ni, R. Lu, and X. Shen, "Achieving accountable and efficient data sharing in industrial internet of things," IEEE Transactions on Industrial Informatics, vol. 17, no. 2, pp. 1416-1427, 2020.
37. S. Huh, S. Cho, and S. Kim, "Managing IoT devices using blockchain platform," in 2017 19th international conference on advanced communication technology (ICACT), 2017: IEEE, pp. 464-467.
38. M. Zhaofeng, W. Xiaochang, D. K. Jain, H. Khan, G. Hongmin, and W. Zhen, "A blockchain-based trusted data management scheme in edge computing," IEEE Transactions on Industrial Informatics, vol. 16, no. 3, pp. 2013-2021, 2019.
39. M. Zhaofeng, W. Lingyun, W. Xiaochang, W. Zhen, and Z. Weizhe, "Blockchain-enabled decentralized trust management and secure usage control of IoT big data," IEEE Internet of Things Journal, vol. 7, no. 5, pp. 4000-4015, 2019.
40. Wei, W., Wang, J., Fang, Z., Chen, J., Ren, Y., & Dong, Y. (2022). 3U: Joint Design of UAV-USV-UUV Networks for Cooperative Target Hunting. IEEE Transactions on Vehicular Technology.
41. Wang, Y., Su, Z., Xu, Q., Li, R., & Luan, T. H. (2021, May). 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 (pp. 1-10). IEEE.
42. Otto, B., ten Hompel, M., & Wrobel, S. (2022). Designing Data Spaces: The Ecosystem Approach to Competitive Advantage.
43. Prinz, W., Rose, T., & Urbach, N. (2022). Blockchain technology and international data spaces. Designing Data Spaces: The Ecosystem Approach to Competitive Advantage, 165-180.
44. Jarke, M., & Quix, C. (2022). Federated Data Integration in Data Spaces. Designing Data Spaces, 181.
45. Amponis, G., Lagkas, T., Zevgara, M., Katsikas, G., Xirofotos, T., Moscholios, I., & Sarigiannidis, P. (2022). Drones in B5G/6G Networks as Flying Base Stations. Drones, 6(2), 39.

46. Saif, A., Dimyati, K., Noordin, K. A., Alsamhi, S. H., Mosali, N. A., & Gupta, S. K. (2022). UAV and Relay Cooperation Based on RSS for Extending Smart Environments Coverage Area in B5G.
47. Alsamhi, S. H., & Rajput, N. S. (2014, September). HAP antenna radiation pattern for providing coverage and service characteristics. In 2014 international conference on advances in computing, communications and informatics (ICACCI) (pp. 1434-1439). IEEE.
48. Khan, M. A., Kumar, N., Mohsan, S. A. H., Khan, W. U., Nasralla, M. M., Alsharif, M. H., ... & Ullah, I. (2022). Swarm of UAVs for network management in 6G: A technical review. IEEE Transactions on Network and Service Management.
49. J. R. Martinez-De Dios, K. Lferd, A. De San Bernabe, G. N ´ u´nez, ~ A. Torres-Gonzalez, and A. Ollero, "Cooperation between UAS ´ and wireless sensor networks for efficient data collection in large environments," Journal of Intelligent & Robotic Systems, vol. 70, no. 1–4, pp. 491–508, 2013.
50. 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), pp. 117–129, ACM, Sydney, Australia, November 2007.
51. Ismail, A. S., Wang, X., Hawbani, A., Alsamhi, S., & Abdel Aziz, S. (2022). Routing protocols classification for underwater wireless sensor networks based on localization and mobility. Wireless Networks, 28(2), 797-826.
52. Chaudhri, S. N., Rajput, N. S., Alsamhi, S. H., Shvetsov, A. V., & Almalki, F. A. (2022). Zero-padding and spatial augmentation-based gas sensor node optimization approach in resource-constrained 6G-IoT paradigm. Sensors, 22(8), 3039.
53. Wang, X., Zhou, W., Hawbani, A., Liu, P., Zhao, L., & Alsamhi, S. H. (2023). A Dynamic Opportunistic Routing Protocol for Asynchronous Duty-Cycled WSNs. IEEE Transactions on Sustainable Computing.
54. Al-qaness, M. A., Abbasi, A. A., Fan, H., Ibrahim, R. A., Alsamhi, S. H., & Hawbani, A. (2021). An improved YOLO-based road traffic monitoring system. Computing, 103, 211-230.
55. M. Aloqaily, O. Bouachir, A. Boukerche, and I. Al Ridhawi, "Design guidelines for blockchain-assisted 5G-UAV networks," IEEE network, vol. 35, no. 1, pp. 64-71, 2021.
56. A. Asheralieva and 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 of Things Journal, vol. 7, no. 3, pp. 1974-1993, 2019.
57. A. Islam and S. Y. Shin, "BUAV: A blockchain based secure UAV-assisted data acquisition scheme in Internet of Things," Journal of Communications and Networks, vol. 21, no. 5, pp. 491-502, 2019.
58. Y. Zhu, G. Zheng, and K.-K. Wong, "Blockchain-empowered decentralized storage in air-to-ground industrial networks," IEEE Transactions on Industrial Informatics, vol. 15, no. 6, pp. 3593-3601, 2019.
59. Alghamdi, A., Zhu, J., Yin, G., Shorfuzzaman, M., Alsufyani, N., Alyami, S., & Biswas, S. (2022). Blockchain Empowered Federated Learning Ecosystem for Securing Consumer IoT Features Analysis. Sensors, 22(18), 6786.
60. Bogacka, K., Wasielewska-Michniewska, K., Paprzycki, M., Ganzha, M., Danilenka, A., Tassakos, L., & Garro, E. (2022). Introducing Federated Learning into Internet of Things ecosystems–preliminary considerations. arXiv preprint arXiv:2207.07700.
61. A. K. Shrestha and 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.
62. C. Tenopir, C. L. Palmer, L. Metzer, J. van der Hoeven, and J. Malone, "Sharing data: Practices, barriers, and incentives," Proceedings of the American Society for Information Science and Technology, vol. 48, no. 1, pp. 1-4, 2011.
63. A. Meadows, "To Share or not to Share? That is the (Research Data) Question… | The Scholarly Kitchen," ed, 2014.
64. C.H. Liu, Q. Lin, S. Wen, Blockchain-enabled data collection and sharing for industrial IoT with deep reinforcement learning, IEEE Trans. Industr. Inf. 15 (6) (2019) 3516–3526.
65. Y. Lu, X. Huang, Y. Dai, S. Maharjan, Y. Zhang, Blockchain and federated learning for privacy-preserved data sharing in industrial IoT, IEEE Trans. Industr. Inf. 16 (6) (2020) 4177–4186.
66. M. C. Zizic, M. Mladineo, N. Gjeldum, and L. Celent, "From Industry 4.0 towards Industry 5.0: A Review and Analysis of Paradigm Shift for the People, Organization and Technology," Energies, vol. 15, no. 14, p. 5221, 2022.

67. N. F. S. Jeffri and D. R. A. Rambli, "A review of augmented reality systems and their effects on mental workload and task performance," Heliyon, vol. 7, no. 3, p. e06277, 2021.
68. N. F. S. Jeffri and D. R. A. Rambli, "A review of augmented reality systems and their effects on mental workload and task performance," Heliyon, vol. 7, no. 3, p. e06277, 2021.44] S. R. Singh, H. Mithaiwala, N. Chauhan, P. Shah, C. Trivedi, and U. P. Rao, "Decentralized Blockchain-Based Framework for Securing Review System," Security, Privacy and Data Analytics, pp. 239-255, 2022.
69. P. Bhattacharya et al., "Coalition of 6G and blockchain in AR/VR space: Challenges and future directions," IEEE Access, vol. 9, pp. 168455-168484, 2021.
70. A. M. Almasoud and A. E. Kamal, "Data dissemination in IoT using a cognitive UAV," IEEE Transactions on Cognitive Communications and Networking, vol. 5, no. 4, pp. 849-862, 2019.
71. G. Lee, W. Saad, and M. Bennis, "Online optimization for UAV-assisted distributed fog computing in smart factories of industry 4.0," in 2018 IEEE Global Communications Conference (GLOBECOM), 2018: IEEE, pp. 1-6.
72. T. M. Fernández-Caramés, O. Blanco-Novoa, I. Froiz-Míguez, and 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, vol. 19, no. 10, p. 2394, 2019.
73. Franklin, M., Halevy, A., & Maier, D. (2005). From databases to dataspaces: a new abstraction for information management. ACM Sigmod Record, 34(4), 27-33.
74. Blunschi, L., Dittrich, J. P., Girard, O. R., Karakashian, S. K., & Salles, M. A. V. (2007, January). A dataspace odyssey: The iMeMex personal dataspace management system. In CIDR (pp. 114-119).
75. R. Grossman, E. Creel, M. Mazzucco, and R. Williams, "A dataspace infrastructure for astronomical data," in Data Mining for Scientific and Engineering Applications: Springer, 2001, pp. 115-123.
76. A. Hasnain et al., "Linked biomedical dataspace: lessons learned integrating data for drug discovery," in International Semantic Web Conference, 2014: Springer, pp. 114-130.
77. D. W. Archer, L. M. Delcambre, and 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.
78. Y. Li and 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.
79. A. D. Sarma, X. L. Dong, and A. Y. Halevy, "Data modeling in dataspace support platforms," in Conceptual Modeling: Foundations and Applications: Springer, 2009, pp. 122-138.
80. R. Grossman and M. Mazzucco, "DataSpace: a data Web for the exploratory analysis and mining of data," Computing in Science & Engineering, vol. 4, no. 4, pp. 44-51, 2002.
81. U. ul Hassan, S. O'Riain, and 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.
82. E. Curry, "System of systems information interoperability using a linked dataspace," in 2012 7th International Conference on System of Systems Engineering (SoSE), 2012: IEEE, pp. 101-106.
83. E. Curry, S. Hasan, and S. O'Riain, "Enterprise energy management using a linked dataspace for energy intelligence," in 2012 Sustainable Internet and ICT for Sustainability (SustainIT), 2012: IEEE, pp. 1-6.
84. E. Curry, J. O'Donnell, E. Corry, S. Hasan, M. Keane, and S. O'Riain, "Linking building data in the cloud: Integrating cross-domain building data using linked data," Advanced Engineering Informatics, vol. 27, no. 2, pp. 206-219, 2013.
85. Curry, Edward. Real-time linked dataspaces: Enabling data ecosystems for intelligent systems. Springer Nature, 2020.
86. Gomez, C., Chessa, S., Fleury, A., Roussos, G., & Preuveneers, D. (2019). Internet of Things for enabling smart environments: A technology-centric perspective. Journal of Ambient Intelligence and Smart Environments, 11(1), 23-43.
87. Marques, G., González-Briones, A., & López, J. M. M. Machine Learning for Smart Environments/Cities.
88. Alsamhi, S. H., Ma, O., Ansari, M. S., & Almalki, F. A. (2019). Survey on collaborative smart drones and internet of things for improving smartness of smart cities. Ieee Access, 7, 128125-128152.
89. Shvetsova, S. V., & Shvetsov, A. V. (2021). Ensuring safety and security in employing drones at airports. Journal of Transportation Security, 14(1), 41-53.

90. Shvetsova, S., & Shvetsov, A. (2021). Safety when flying unmanned aerial vehicles at transport infrastructure facilities. Transportation research procedia, 54, 397-403.
91. Alsamhi, S. H., Ma, O., Ansari, M. S., & Gupta, S. K. (2019). Collaboration of drone and internet of public safety things in smart cities: An overview of qos and network performance optimization. Drones, 3(1), 13.
92. Alsamhi, S. H., Lee, B., Guizani, M., Kumar, N., Qiao, Y., & Liu, X. (2021). Blockchain for decentralized multi-drone to combat COVID-19 and future pandemics: framework and proposed solutions. Transactions on Emerging Telecommunications Technologies, 32(9), e4255.
93. Alsamhi, S. H., Shvetsov, A. V., Shvetsova, S. V., Hawbani, A., Guizan, M., Alhartomi, M. A., & Ma, O. (2022). Blockchain-Empowered Security and Energy Efficiency of Drone Swarm Consensus for Environment Exploration. IEEE Transactions on Green Communications and Networking.
94. Alsamhi, S. H., Almalki, F. A., Afghah, F., Hawbani, A., Shvetsov, A. V., Lee, B., & Song, H. (2021). Drones' edge intelligence over smart environments in b5g: blockchain and federated learning synergy. IEEE Transactions on Green Communications and Networking, 6(1), 295-312.
95. Ojo, A., & Curry, E. (2020). Catalog and Entity Management Service for Internet of Things-Based Smart Environments. In Real-time Linked Dataspaces (pp. 89-103). Springer, Cham.
96. Curry, E., Fabritius, W., Hasan, S., Kouroupetroglou, C., & Derguech, W. (2020). A model for internet of things enhanced user experience in smart environments. In Real-time Linked Dataspaces (pp. 271-294). Springer, Cham.
97. Curry, E., Derguech, W., Hasan, S., Kouroupetroglou, C., & Fabritius, W. (2020). Building internet of things-enabled digital twins and intelligent applications using a real-time linked dataspace. In Real-time Linked Dataspaces (pp. 255-270). Springer, Cham.
98. Ferro-Escobar, R., Vacca-González, H., & Gómez-Castillo, H. (2022). Smart and Sustainable Cities in Collaboration with: The Singapore Success Case. In Machine Learning for Smart Environments/Cities (pp. 213-243). Springer, Cham.
99. Zanury, N. A., Remli, M. A., Adli, H. K., & Wong, K. N. S. W. (2022). Recent Developments of Deep Learning in Future Smart Cities: A Review. Machine Learning for Smart Environments/Cities, 199-212.
100. Qiu, T., Liu, J., Si, W., Wu, D.O., 2019. Robustness optimization scheme with multi-population co-evolution for scale-free wireless sensor networks. IEEE/ACM Trans. Netw. 27 (3), 1028–1042.
101. Saif, A., Dimyati, K., Noordin, K. A., Shah, N. S. M., Alsamhi, S. H., & Abdullah, Q. (2021, August). Energy-efficient tethered UAV deployment in B5G for smart environments and disaster recovery. In 2021 1st International Conference on Emerging Smart Technologies and Applications (eSmarTA) (pp. 1-5). IEEE.
102. Khaleefa, S. A., Alsamhi, S. H., & Rajput, N. S. (2014, March). Tethered balloon technology for telecommunication, coverage and path loss. In 2014 IEEE Students' Conference on Electrical, Electronics and Computer Science (pp. 1-4). IEEE.
103. Manghwani, P., Loyall, J., Sharma, P., Gillen, M., & Ye, J. (2005, April). End-to-end quality of service management for distributed real-time embedded applications. In 19th IEEE International Parallel and Distributed Processing Symposium (pp. 8-pp). IEEE.
104. Alsamhi, S. H., Shvetsov, A. V., Kumar, S., Hassan, J., Alhartomi, M. A., Shvetsova, S. V., ... & Hawbani, A. (2022). Computing in the sky: A survey on intelligent ubiquitous computing for uav-assisted 6g networks and industry 4.0/5.0. Drones, 6(7), 177.
105. A. Bujari, C. T. Calafate, J.-C. Cano, P. Manzoni, C. E. Palazzi, and D. Ronzani, "Flying ad-hoc network application scenarios and mobility models," International Journal of Distributed Sensor Networks, vol. 13, no. 10, p. 1550147717738192, 2017.
106. S. Han, S. Xu, W. Meng, and C. Li, "Dense-device-enabled cooperative networks for efficient and secure transmission," IEEE Network, vol. 32, no. 2, pp. 100-106, 2018.
107. N. Vanitha and 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), 2018: IEEE, pp. 1-8.
108. S. Aggarwal, M. Shojafar, N. Kumar, and M. Conti, "A new secure data dissemination model in internet of drones," in ICC 2019-2019 IEEE international conference on communications (ICC), 2019: IEEE, pp. 1-6.
109. S. Jacob, V. G. Menon, P. Shynu, S. K. Fathima, B. Mahapatra, and S. Joseph, "Bidirectional multi-tier cognitive swarm drone 5G network," in IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 2020: IEEE, pp. 1219-1224.

110. McMahan, B., Moore, E., Ramage, D., Hampson, S., & y Arcas, B. A. (2017, April). Communication-efficient learning of deep networks from decentralized data. In Artificial intelligence and statistics (pp. 1273-1282). PMLR.
111. Trindade, S., Bittencourt, L. F., & da Fonseca, N. L. (2022). Resource management at the network edge for federated learning. Digital Communications and Networks.
112. Chen, M., Yang, Z., Saad, W., Yin, C., Poor, H. V., & Cui, S. (2020). A joint learning and communications framework for federated learning over wireless networks. IEEE Transactions on Wireless Communications, 20(1), 269-283.
113. Jelasity, M. (2011). Gossip. In Self-organising software (pp. 139-162). Springer, Berlin, Heidelberg.
114. Pokhrel, S. R., & Choi, J. (2020). Federated learning with blockchain for autonomous vehicles: Analysis and design challenges. IEEE Transactions on Communications, 68(8), 4734-4746
115. Lu, Y., Huang, X., Dai, Y., Maharjan, S., & Zhang, Y. (2019). Blockchain and federated learning for privacy-preserved data sharing in industrial IoT. IEEE Transactions on Industrial Informatics, 16(6), 4177-4186.
116. Khacef, K., & Pujolle, G. (2019, March). Secure Peer-to-Peer communication based on Blockchain. In Workshops of the International Conference on Advanced Information Networking and Applications (pp. 662-672). Springer, Cham.
117. Fernández-Caramés, T. M., Blanco-Novoa, O., Froiz-Míguez, I., & Fraga-Lamas, P. (2019). 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), 2394.
118. Ramachandran, R., Babu, V., & Murugesan, V. P. (2022). The role of blockchain technology in the process of decision-making in human resource management: a review and future research agenda. Business Process Management Journal, (ahead-of-print).
119. Zarrin, J., Wen Phang, H., Babu Saheer, L., & Zarrin, B. (2021). Blockchain for decentralization of internet: prospects, trends, and challenges. Cluster Computing, 24(4), 2841-2866.
120. Aggarwal, S., Shojafar, M., Kumar, N., & Conti, M. (2019, May). A new secure data dissemination model in internet of drones. In ICC 2019-2019 IEEE international conference on communications (ICC) (pp. 1-6). IEEE.
121. Chi, J., Li, Y., Huang, J., Liu, J., Jin, Y., Chen, C., & Qiu, T. (2020). A secure and efficient data sharing scheme based on blockchain in industrial Internet of Things. Journal of Network and Computer Applications, 167, 102710.
122. Khan, A. A., Laghari, A. A., Gadekallu, T. R., Shaikh, Z. A., Javed, A. R., Rashid, M., ... & Mikhaylov, A. (2022). A drone-based data management and optimization using metaheuristic algorithms and blockchain smart contracts in a secure fog environment. Computers and Electrical Engineering, 102, 108234.
123. Aloqaily, M., Jararweh, Y., & Bouachir, O. (2021). Trustworthy Cooperative UAV-Based Data Management in Densely Crowded Environments. IEEE Communications Standards Magazine, 5(4), 18-24.
124. Wang, X., Huang, T., Zhu, K., & Zhao, X. (2022). LSTM-Based Broad Learning System for Remaining Useful Life Prediction. Mathematics, 10(12), 2066.
125. Z. Xiong, Y. Zhang, D. Niyato, R. Deng, P. Wang, and L.-C. Wang, "Deep reinforcement learning for mobile 5G and beyond: Fundamentals, applications, and challenges," IEEE Vehicular Technology Magazine, vol. 14, no. 2, pp. 44-52, 2019.
126. Sedjelmaci, Hichem, Aymen Boudguiga, Inès Ben Jemaa, and Sidi Mohammed Senouci. "An efficient cyber defense framework for UAV-Edge computing network." Ad Hoc Networks 94 (2019): 101970.
127. Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. Leung, "Blockchain-based decentralized trust management in vehicular networks," IEEE Internet of Things Journal, vol. 6, no. 2, pp. 1495-1505, 2018.
128. O. Dib, K.-L. Brousmiche, A. Durand, E. Thea, and E. B. Hamida, "Consortium blockchains: Overview, applications and challenges," International Journal On Advances in Telecommunications, vol. 11,no. 1&2, pp. 51-64, 2018.
129. Li, Mushu, Nan Cheng, Jie Gao, Yinlu Wang, Lian Zhao, and Xuemin Shen. "Energy-efficient UAV-assisted mobile edge computing: Resource allocation and trajectory optimization." IEEE Transactions on Vehicular Technology 69, no. 3 (2020): 3424-3438.
130. Jamil, S., & Rahman, M. (2022). A Comprehensive Survey of Digital Twins and Federated Learning for Industrial Internet of Things (IIoT), Internet of Vehicles (IoV) and Internet of Drones (IoD). Applied System Innovation, 5(3), 56.

131. Sahal, R., Alsamhi, S. H., Brown, K. N., O'Shea, D., McCarthy, C., & Guizani, M. (2021). Blockchain-empowered digital twins collaboration: smart transportation use case. Machines, 9(9), 193.
132. Sahal, R., Alsamhi, S. H., Brown, K. N., O'Shea, D., & Alouffi, B. (2022). Blockchain-based digital twins collaboration for smart pandemic alerting: decentralized COVID-19 pandemic alerting use case. Computational Intelligence and Neuroscience, 2022.
133. 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/
134. Zhu, C., Zhu, X., Ren, J., & Qin, T. (2022). Blockchain-enabled federated learning for UAV edge computing network: Issues and solutions. Ieee Access, 10, 56591-56610.
135. Yahiatene, Y., Rachedi, A., Riahla, M. A., Menacer, D. E., & Nait-Abdesselam, F. (2019). A blockchain-based framework to secure vehicular social networks. Transactions on emerging telecommunications technologies, 30(8), e3650.
136. Makhdoom, I., Zhou, I., Abolhasan, M., Lipman, J., & Ni, W. (2020). PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities. Computers & Security, 88, 101653.
137. Patel, V. (2019). A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. Health informatics journal, 25(4), 1398-1411.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.