Edge Computing and Sensor-Cloud: Overview, Solutions, and Directions

TIAN WANG, Beijing Normal University and Beijing Normal University-Hong Kong Baptist University United International College, China (Corresponding author)
YUZHU LIANG, Beijing Normal University, China
XUEWEI SHEN, Huaqiao University, China
XI ZHENG, Macquarie University, Australia
ADNAN MAHMOOD, Macquarie University, Australia
QUAN Z. SHENG, Macquarie University, Australia

Sensor-cloud originates from extensive recent applications of wireless sensor networks and cloud computing. To draw a roadmap of the current research activities of the sensor-cloud community, we first investigate the state-of-the-art sensor-cloud literature reviews published in the recent five years, and discover that these surveys have primarily studied the sensor-cloud in specific aspects, namely, security-enabled solutions, efficient management mechanisms, and architectural challenges. Whilst the existing surveys have reviewed the sensor-cloud from various perspectives, they are inadequate for the three key issues that require urgent attention in the sensor-cloud: *reliability*, *energy*, and *heterogeneity*. To fill this gap, we perform a thorough survey by examining the origins of the sensor-cloud and providing an in-depth and comprehensive discussion of these three key challenges. We summarize initial designs of the new edge-based schemes to address these challenges and identify several open issues and promising future research directions.

CCS Concepts: • **Computer systems organization → Embedded systems**; *Redundancy*; Robotics; • **Networks** → Network reliability.

Additional Key Words and Phrases: Sensor-cloud, WSNs, cloud computing, edge computing.

ACM Reference Format:
Tian Wang, Yuzhu Liang, Xuewei Shen, Xi Zheng, Adnan Mahmood, and Quan Z. Sheng. 2023. Edge Computing and Sensor-Cloud: Overview, Solutions, and Directions. *ACM Comput. Surv.* XX, XX, Article 39 (January 2023), 37 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

Wireless sensor networks (WSNs) are able to gather and integrate information into the physical world [1]. Meanwhile, sensor data and services have become more and more dependent on the cloud [2]. Therefore, in recent years, sensor-cloud infrastructure is becoming popular as it can provide an open, flexible, and reconfigurable platform for multiple applications [3, 4]. Such applications are

Authors' addresses: Tian Wang, Beijing Normal University and Beijing Normal University-Hong Kong Baptist University United International College, Zhuhai, Guangdong, China (Corresponding author), cs_tianwang@163.com; Yuzhu Liang, Beijing Normal University, Beijing, China, cs_yuzhuliang@163.com; Xuewei Shen, Huaqiao University, Xiamen, Fujian, China, shenxw_666@163.com; Xi Zheng, Macquarie University, Sydney, NSW 2109, Australia, james.zheng@mq.edu.au; Adnan Mahmood, Macquarie University, Sydney, NSW 2109, Australia, adnan.mahmood@hdr.mq.edu.au; Quan Z. Sheng, Macquarie University, Sydney, NSW 2109, Australia, michael.sheng@mq.edu.au.

0360-0300/2023/01-ART39 $15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

closely related to every aspect of our daily life, including but not limited to, intelligent transportation, smart agriculture, and smart cities [5, 6].

There are a few state-of-the-art published surveys covering specific aspects of the sensor-cloud systems in the recent five years. To identify the position of our survey, we summarize the publication years, gap analysis, and other metadata of these surveys in Table 1. Specifically, for the column, "Involve one of the three key issues", *few* implies that less than 30% of the reviewed works involve one of the three key challenges, *a few* means that more than 30% but less than 60% of the reviewed works involve one of the three key challenges, *many* suggests that more than 60% of the reviewed works involve one of the three key challenges, and *all* manifests that all of the reviewed works involve one of the three key challenges. In addition, these surveys can be classified into four groups. In Group 1, sensor-cloud security issues are the primary focus. In Group 2, efficient management methods are reviewed. Group 3 includes the works pertinent to the sensor-cloud architecture, whereas, an overview of the sensor-cloud is summarized in Group 4.

For sensor-cloud security, Dwivedi et al. presented a survey that focused on some of the major security attacks [7]. Geetha et al. analyzed the integrated security issues of the existing technologies [8]. Almolhis et al. introduced some new classes of the security and privacy issues, and presented security issues in the integrated IoT-cloud systems [9]. These studies mainly investigate security issues in the sensor-cloud from a single perspective, e.g., security attacks or integrated security issues, and do not provide a comprehensive review of various aspects of security issues, e.g., from a hardware layer, network layer, and transport layer perspective. In addition, the above surveys did not deliberate on edge computing as a promising solution for the sensor-cloud security with better performance, higher efficiency, and more robustness [20, 21]. It is, therefore, indispensable to summarize the latest literature to review the field of edge-based solutions.

For efficient management in the sensor-cloud, Khan et al. presented a survey on energy-efficient data transmission in the sensor-cloud that discussed and compared the state-of-the-art techniques [10]. Dizdarević et al. surveyed communication protocols that fulfill the IoT communication requirements, and their potential for implementation in edge-based and cloud-based IoT systems [11]. Dwivedi et al. focused on how to minimize the energy consumption and communication overhead in the sensor-cloud [12]. Existing surveys mostly focus on energy-efficient communication protocols. However, each layer within the sensor-cloud may lead to non-effective management, e.g., in aspects of energy replenishing level, cloud level, interaction level, and WSNs level, and the said surveys ignore these layers. Moreover, similar to the security domain, there are several studies that address edge-based efficient management mechanisms, nevertheless, there is a lack of surveys in this area.

For sensor-cloud architecture, Dwivedi et al. emphasized on the significance of virtualization in the sensor-cloud, i.e., in terms of saving time [13]. Ren et al. presented a comprehensive survey of emerging computing paradigms, e.g., fog computing and mobile edge computing, from the perspective of end-edge-cloud orchestration [14]. Nazari et al. analyzed the combination of IoT and cloud and detected the challenges of such integration [15]. Wu et al. introduced Cloud-Edge-IoT computing architecture from the perspective of IoT applications [16]. Misra et al. [17] emphasized on theoretical modeling of sensor-cloud and further suggested a paradigm shift of technology from traditional WSNs to sensor-cloud architecture. Even if some surveys introduced edge computing into the sensor-cloud architecture, they lack specific edge-assisted solutions based on those architectures. Furthermore, research on sensor-cloud architectures lack an overview of the heterogeneity issue and which is, in fact, one of the crucial issues due to the characteristics of the sensor-cloud [22–26].

For a general overview, Ahmad et al. presented a comprehensive survey of the enabling cloud-based IoT architectures, services, configurations, and security models [18]. Chen et al. reviewed the most recent research efforts on existing, real, already deployed consumer-oriented IoT cloud applications [19]. Rana et al. proposed a comprehensive study that covered various sensor-cloud

Table 1. Summary of the state-of-the-art published surveys

Group	Ref.	Year	Edge assisted	Involve one of the three key issues	Gap analysis
Group 1	[7]	2019	×	a few	Ignore security issues in hardware layer.
	[8]	2020	×	a few	Ignore security issues in transport layer.
	[9]	2020	×	a few	Lack of investigating the edge-based solutions.
Group 2	[10]	2019	×	few	Ignore non-effective management in interaction level.
	[11]	2019	√	a few	Ignore non-effective management in cloud level.
	[12]	2020	×	few	Lack of investigating the edge-based solutions.
Group 3	[13]	2018	×	few	Lack of investigating the edge-based solutions.
	[14]	2019	√	a few	Ignore the heterogeneous issues.
	[15]	2020	×	few	Lack of investigating the edge-based solutions.
	[16]	2020	√	few	Ignore the heterogeneous issues.
	[17]	2017	×	few	Lack of investigating the edge-based solutions.
Group 4	[3]	2021	×	many	Ignore the edge-based solutions.
	[18]	2021	×	a few	Ignore one of the three key issues and edge-based solutions.
	[19]	2021	×	a few	Ignore one of the three key issues and edge-based solutions.
	Ours	2022	√	all	-

aspects in terms of the architecture, network dynamics, heterogeneity, communication patterns, data management, and security [3]. Whilst the above surveys have reviewed the sensor-cloud from varying perspectives, they are inadequate for the three key issues that require urgent attention in the sensor-cloud: *reliability*, *energy*, and *heterogeneity*. These issues arise from the combination of WSNs and cloud computing, and solving these issues can improve the performance of the sensor-cloud. Also, a lot of research literature has focused on these key issues [22–34], however, most of these works have not been mentioned in the existing surveys, and these studies also verify the need for an in-depth survey to overview them. In addition, existing surveys have also paid less attention to the edge-based solutions.

From the analysis of the existing sensor-cloud surveys, as depicted in Table 1, we have found that a comprehensive survey is missing which can i) improve the performance of the sensor-cloud, and ii) help better understand the sensor-cloud. To fill this gap, we first propose a thorough walk-through of the sensor-cloud with a four-layer architecture and its main components. Subsequently, an in-depth and comprehensive analysis of the three key challenges is presented. Specifically, the first challenge is logically segregated into hardware reliability, network reliability, and transmission reliability. The second challenge is categorized into two types, namely, energy saving methods (i.e., at the WSNs level, interaction level, and cloud level) and energy replenishing methods. The third challenge is divided into device level, network level, and service level. In this way, this work can evaluate all layers of the sensor-cloud in a fine-grained manner and can also include most of the existing solutions related to the three key issues. Unlike existing surveys, we introduce an edge-based architecture in detail and summarize several edge-based solutions to solve the three key issues. We then discuss several promising research directions for the edge-based sensor-cloud.

In summary, we provide a more comprehensive survey of the sensor-cloud. Particularly, we include the latest high-quality research outputs that have not been included in other existing survey articles. We believe this survey can shed new light on the further development of the sensor-cloud. In a nutshell, the main contributions of this survey are summarized as follows:

- A brief classification of the existing sensor-cloud surveys is conducted in a bid to highlight the motivation of our literature review delineated in this survey.
- A thorough walk-through of the sensor-cloud with a four-layer architecture and its main components is provided. Based on the architecture, an in-depth and comprehensive discussion of the key challenges and the state-of-the-art solutions are presented.
- An introduction of edge-based architecture is provided in detail and several edge-based solutions to solve the three key issues are summarized.
- The future promising research directions of the edge-based sensor-cloud are identified and discussed.

The taxonomy of the paper (as depicted in Figure 1) is presented as follows. Section 2 discusses the background of the sensor-cloud. Section 3 describes the overall architecture of the current sensor-cloud and its elements. In Section 4, the paper further analyzes the application of sensor-cloud based on existing relevant research. Section 5 gives edge-based recent studies and its future directions. The last section provides some concluding remarks.

2 SENSOR-CLOUD BACKGROUND

The preliminaries about sensor-cloud systems are introduced, and the reason they have become an important research area is discussed in this section. To begin with, the definition and characteristics of sensor-cloud are described.

A model combining WSNs with the cloud computing paradigm was proposed in [17, 35, 36]. Distefano et al. proposed a to connect Clouds with the Internet of Things (COT) [37]. Introducing

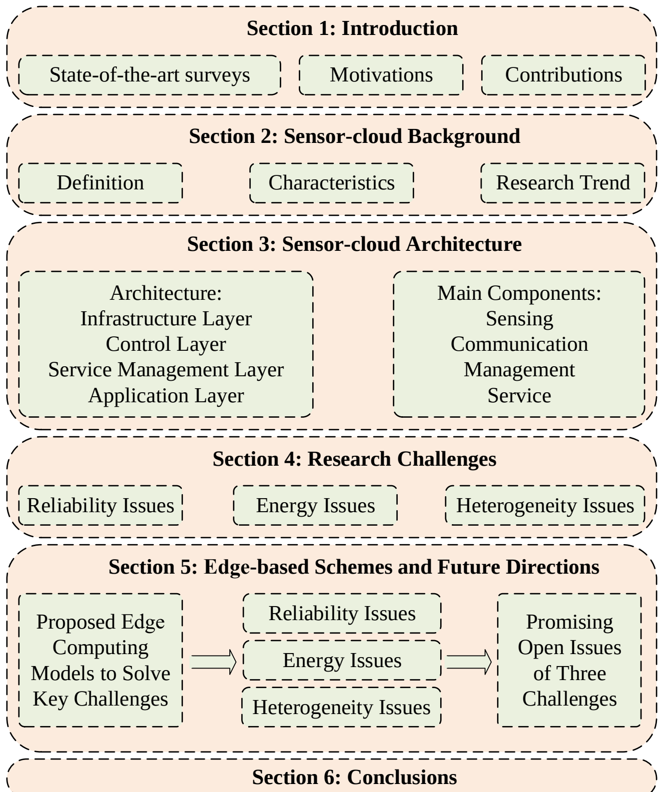


Fig. 1. The taxonomy of the discussed topics.

the benefits of Mobile Cloud Computing (MCC) and WSNs, Zhu et al. also described combining WSNs with mobile cloud computing in [38]. Fortino et al. proposed a framework of Body Cloud, which allowed data collected by sensors to be uploaded to the cloud data center in which the data was processed and analyzed [39]. Yuriyama et al. designed an infrastructure application to realize physical nodes virtualization on the cloud [40]. Al-Ghazi et al. put forward an innovative vision that worked in vehicular networks and integrated vehicle models through mobile devices and cloud computing schemes in [41]. Table 2 shows these examples of integration of networks with the cloud. Some traditional methods of addressing network problems are introduced to design optimized algorithms, and protocols [42, 43].

Since cloud computing has robust capabilities in data processing and storage [44], it can be used to provide a platform for WSNs to manage remote data. Heterogeneous or wrong data can also be processed on this platform. Sensor-cloud is a new paradigm combining cloud computing with WSNs [45–47]. It only requires users to send applications to sensor-cloud, which automatically distributes some sensor networks to provide services in real-time. Table 2 presents some examples of the integration of these networks with the cloud. Users only need to send application requirements to sensor-cloud, which automatically distributes and dispatches some sensor networks to provide services in real-time.

Table 2. Examples of networks integrated with cloud

Sensor Networks	Integration Technology	Purpose	Main Feature
Wireless sensor network	Sensor-cloud CC-WSN (Cloud Computing integrated with WSN) [12, 48] Cloud of sensors [49]	Everything-as-a-Service (XaaS)	With the help of visualization technologies, users can request nodes that combine partial or multiple WSNs to provide services.
Internet of Things (IoT)	CoT (Cloud of things) [50, 51] CloudIoT [52] IoT cloud [53]	IoT-as-a-Service (IoTaaS)	Reduces the time for WSNs to store and process data.
Wireless sensor & actor network	Sensor-cloud [54, 55]	Software-as-a-Service (SaaS)	Monitors each physical node and optimizes its energy distribution [48].
Wireless Body Area Network (WBAN)	Body-cloud [56] WBAN-cloud [57] Cloud-enabled [58]	Mobile sensing	Forms a comprehensive view on data by connecting underlying physical sensors and pass it to the user.
Vehicular Ad-Hoc Network (VANET)	VANET-cloud [59]	Multi-method delivery	Provides private and trust-compatible remote services [60].

Sensor-cloud provides services through virtualization of physical sensors. The virtualization brings benefits to expand the scope of services and facilitate the operation of systems [61]. Vendors of various WSNs can upload their data to offer more services. The characteristics of sensor-cloud are described as follows:

- **Transparency**. Sensor-cloud systems are transparent regarding the types of sensors used. Users can obtain sensor services from different vendors without constraints of their physical locations and access rules [48, 62].
- **Heterogeneity**. This characteristic can help the sensor-cloud system to process real-time heterogeneous data to make critical decisions [63]. The sensor-cloud provides multiple data services, such as analysis, monitoring, storage, and computing.
- **Management**. The sensor-cloud focuses on managing sensors via clouds [64].
- **Sharing**. Multi-user data sharing can reduce costs of transmission and communication, and increase working efficiency [65].

There are many similarities between WSNs and sensor-cloud, and the former one provides essential support for the latter. WSNs support many application scenarios for more convenient services of sensor-cloud systems. Fig. 2 describes the relations between WSNs and sensor-cloud systems. On the right side, a sensor-cloud can serve multiple applications. One of the leading technologies involved is virtualization, which can abstract the underlying physical sensor nodes. Based on this topology, sensor-cloud systems can meet various needs of users and solve some defects resulted from single data applications. With node level virtualization, it seems to be possible to serve multiple applications without cloud (e.g., Advanticsys, Virtenio), however, it is different from the sensor-cloud [66].

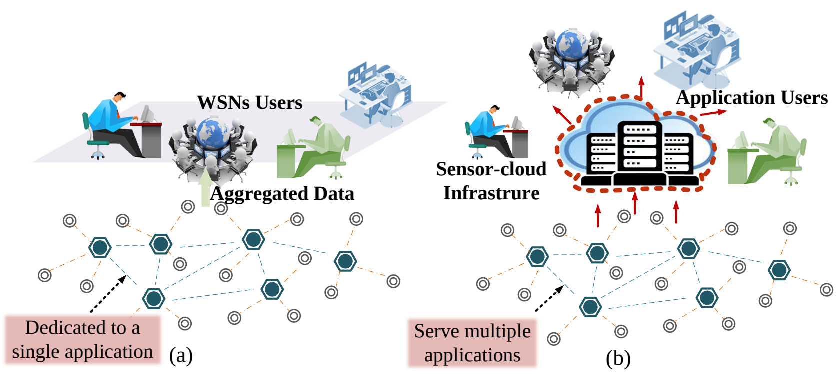
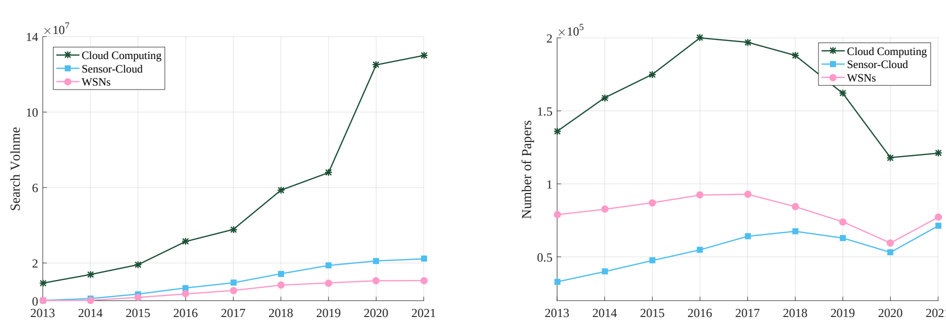


Fig. 2. Comparison of system topologies: (a) WSNs and (b) Sensor-cloud.

The differences between WSNs and sensor-cloud can be summarized in the following aspects: i) type of service. WSNs are data-centric systems, which provide similar data-related services to different users. However, sensor-cloud is a cloud computing-centric architecture, which can provide various types of data-related services to different users; ii) difference between the operational concepts. Sensor-cloud provides virtualization services for the underlying physical nodes and users, while WSNs do not have; iii) the energy, computing, and storage capacity of WSNs are based on sensor nodes, while the sensor-cloud has high expansion and management ability in cloud servers because the data collected by physics nodes can upload to cloud directly.

Currently, the sensor-cloud has received extensive attention from both academia and industry. Sudip et al. analyzed that a sensor-cloud structure has more advantages than the traditional network system, which has created immeasurable value for businesses and consumers [17]. It has been reported that there is an increasing number of manufacturers using the sensor-cloud [67]. Customers can fully take advantage of sensor-cloud to send hardware data and sensor data directly through the network without writing lines of code and programming for numerous servers [68–70].



(a) Search volume by Google. (b) Related work.

Fig. 3. Trends of sensor-cloud research.

The research of sensor-cloud can expand to many potential fields to realize integration services by extending the capabilities of underlying nodes [71]. A new report from Allied Market Research (AMR) indicates that the global sensor network market is predicted to have a growth rate of 11.3% until 2022 when the value of the market will surge to around $241 billion [72]. In the era of IoT, sensors are the key to the IoT perception layer. An authoritative data analysis shows that by 2020 IoT companies can earn an average annual profit of more than $470 billion by selling related comprehensive solutions [73].

Considerable research has been conducted on cloud, WSNs, and sensor-cloud in recent years. Fig. 3a shows the search volume results with the keywords of "cloud computing", "WSNs", and "sensor-cloud" in Google over a nine-year period of 2013–2021 [74]. This volume reveals that cloud computing remains to be a hot topic. What's more, there has been a great deal of research on WSNs, and sensor-cloud is gaining popularity over the years. Fig. 3b shows the number of related papers in Google Scholar, which is clear that studies on cloud and WSNs are decreasing while research on sensor-cloud remains relatively stable. Sensor-cloud combines the advantages of cloud computing and WSNs, which has considerable prospects.

3 SENSOR-CLOUD ARCHITECTURE

Unlike WSNs, sensor-cloud provides more access to underlying sensor nodes and offers maintenance and management services to a broader range of users [75]. Users are allowed to define their services, which can be provided directly by the sensor-cloud platform [76]. This section thoroughly reveals the foundation and components of sensor-cloud.

3.1 Sensor-Cloud Architecture

There is an increasing number of sensor objects interlinked through WSNs in sensor-cloud. Therefore, it is necessary for sensor-cloud models to have flexible and layered architectures [77]. As depicted in Fig. 4, the data switching in sensor-cloud models are designed as three parts, physical world, virtualized world, and utility application. It aims to consider the orchestration for WSNs and cloud computing. Furthermore, it reveals the form of data dissemination and specific functions which determine the connection among sensors or end-users [78, 79].

In terms of data quality, cloud computing facilities the processing, analysis, and extraction of WSN data, which can manage and control the physical world accurately and intelligently [7]. WSNs have a large amount of sensor data but limited processing capacity [80, 81]. The combination with cloud computing brings vitality through i) the integration of various vendor platforms, ii) the improved scalability of data storage, iii) storage-based data access, iv) resource sharing to data, and v) the introduction of new pricing concepts for selecting Cloud Service Providers (CSPs) as criteria.

As for how to use the cloud computing facilities in a sensor-cloud system, the *single-center & multi-terminal pattern* is the most typical and important one. Such a pattern organizes all types of sensor devices with small distribution ranges, and requests for the servers of the cloud center or part of the data center as a processing center. The user terminals are responsible for obtaining information from and delivering it to the data center [82]. The cloud center will set up a unified platform for users to operate. Together with the cloud center, sensor providers provide optimization services such as hierarchical management and data storage with more private clouds. Fig. 5 shows a general sensor-cloud system architecture with the following layers:

3.1.1 ***Infrastructure Layer.*** The first layer is also known as the data plane, which has sensors and actuators. These physical nodes in the sensor-cloud will collect and process the data [83, 84]. A large number of heterogeneous sensors can be added to infrastructures, which can also be added or removed on the fly. The virtualization technology in this layer is the foundation for the sharing

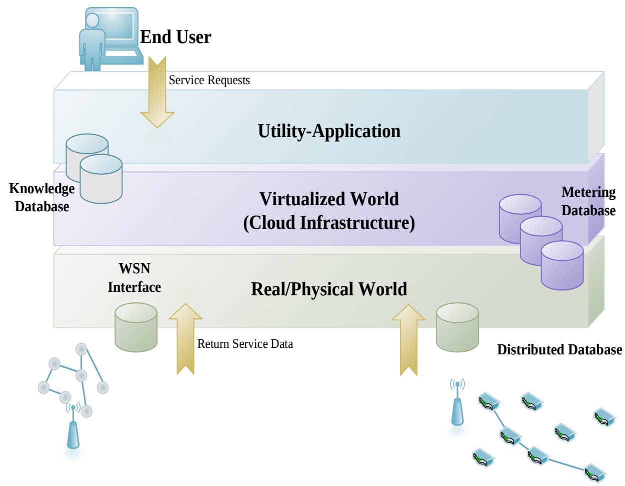


Fig. 4. The hierarchy of data dissemination in sensor-cloud systems.

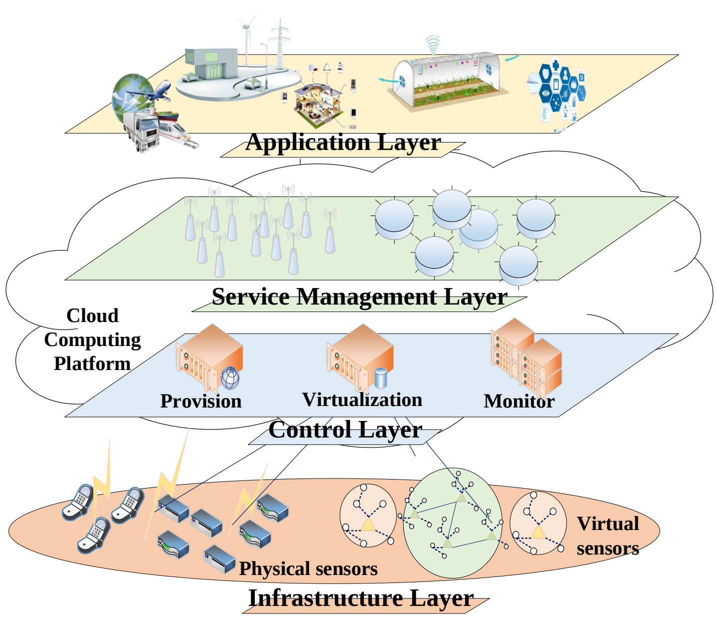


Fig. 5. Senor-cloud system architecture.

of physical sensors, as well as virtual sensors and virtual sensor groups. Whenever a user sends requests to a visualized node or group, the sensor-cloud system will provide data preprocessing, uploading, and analyzing services.

3.1.2 ***Control Layer***. This layer is primarily responsible for dividing tasks, uploading data generated by the infrastructure layer through a secure channel [85]. Before data are transmitted,

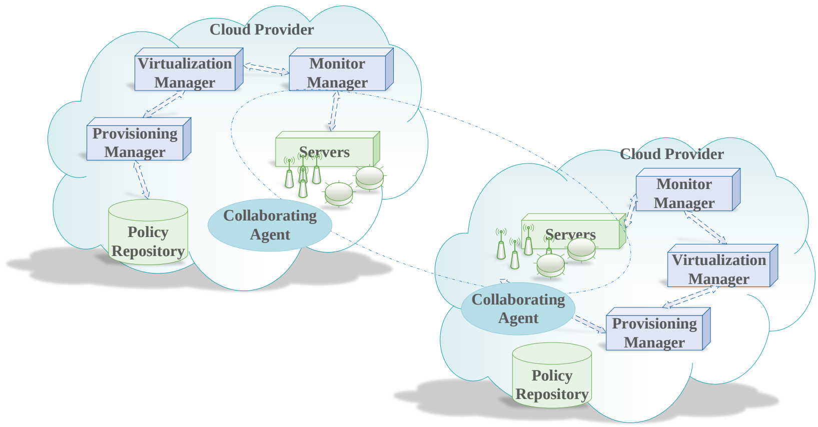


Fig. 6. The multi-center structures of cloud platform in sensor-cloud architecture.

its provisioning, visualization, and monitoring are also completed in this layer. In this context, provisioning managers provide automatic provisioning of virtual sensor groups [86], which plays an important role in the predefined workflow. The virtualization manager is set to virtualize sensor groups automatically [87]. Moreover, the control layer also provides monitoring and management for related data, which are received and monitored from the proxy of virtual servers [88, 89].

3.1.3 ***Service Management Layer***. The task of the service management layer or middleware layer is to match services to the requester by addresses and names. Builders can ignore the heterogeneity issues among hardware platforms for follow-up operations because of the characteristics of this layer. In addition, the layer processes data and provides services based on network protocols [90, 91].

3.1.4 ***Application Layer***. The application layer meets the customer's requests for service. It is mainly focused on business applications and applies the sensor-cloud to enable network services for end-users (e.g., communication and operation) [14]. This layer is important to sensor-cloud because it meets customers' requests by providing high-quality intelligent services [92].

For many enterprises and companies with a large regional span, it is more suitable to use the *multi-center & multi-terminal pattern*. For example, an enterprise operates across many regions or countries. It is necessary to monitor all of its branches and ensure the quality of related services for the headquarter. In the same way, data or information needs to be quickly shared with the terminals. The premise of applying this model is to include public and private clouds, and there is no obstacle to the inter-connection among cloud service users. As a result, some confidential information, such as commercial secrets, can be kept unrevealed. The operations of this system do not affect the transmission and dissemination of information.

One major task that can be completed through this model is to adopt a faster and more efficient method to reach coordination at the highest level. Therefore, the architecture of this model can be regarded as the same as one-to-many in Section 4. Fig. 6 shows the working mechanism of this system. In Fig. 6, monitoring managers and optimization processes can provide valuable information to the design-time environment and help fill the gap between design-time and run-time [93]. In this process, the heterogeneity of sensor-cloud services should be taken into consideration. However, it should cover the requirements of all types of service consumers as much as possible [94].

Table 3. The characteristics of sensor-cloud architecture

Models	Sensing	Communication	Management	Services
OpenIoT [95]	Self-organized	Web 2.0/Web 3.0	Optimal distributed control	Mobile sensing applications
Pub/Sub [76]	–	Web 2.0	Event/Stream Monitoring and Processing Component (SMPC)	SaaS (Software-as-a-Service)
MMDD [96]	–	Device-to-Device	Data traffic monitoring	Multi-method Data Delivery
RWSN [97]	IEEE 802.15.4	6LoWPAN	Low-Rate Wireless Personal Area Networks (LR-WPANs)	Message Queue Telemetry Transport (MQTT)
Automation-cloud [67]	–	Service Oriented Architecture (SOA)	PLCs	XaaS (Everything-as-a-Service)
IoT cloud [69]	–	Cross-cloud Federation	Hypervisor Virtualization (HVV)	IoTaaS (IoT-as-a-Service)
CEB (Cloud-Edge-Beneath) [98]	XML-encoded Device Description Language (DDL)	Open Services Gateway initiative (OSGi)	Atlas Cloud Middleware (ACM)	Utility Service Mart (USM)

User's requirements may vary depending on different scenarios, data sizes, and degrees of implementation. Therefore, it is necessary to divide the requirements in sensor-cloud systems into temporary scenarios and persistent ones [70]. In a persistent scenario, cloud providers need to provide more stable collaboration and such a requirement may exist throughout the operation. After receiving the user's requests, the Service Management Layer will make the overall plan and decide resources and cloud providers. Once collaborative automation begins, the control layer can guide management, scheduling, and other related decisions. In addition, the control layer needs to make an initial decision as required and guides the collaborative agents to obtain external resources to complete scheduling with other modules [99].

3.2 The Main Components

Some main elements are described in this section, which are necessary to deliver the functionality of the sensor-cloud and to help readers understand the composition and characteristics of the sensor-cloud. The summary of existing functions is shown in Table 3.

3.2.1 ***Sensing***. The sensing device collects data from objects under the network coverage within a certain period, and then connects them with the database and cloud [100]. Table 3 shows that the devices are directly connected to the management portals, which are centrally located at the management level to ensure that data required for customers can be obtained by a series of sensor devices with specific specifications [101, 102].

3.2.2 ***Communication***. Generally, sensor nodes adopt a low-power mode in communication channels with loss and noise. Examples of communication protocols used are Web 2.0/3.0, OSGi, and IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN) [103]. These specify the media access control for reliable and scalable communications and illustrate a low-power state in the physical layer.

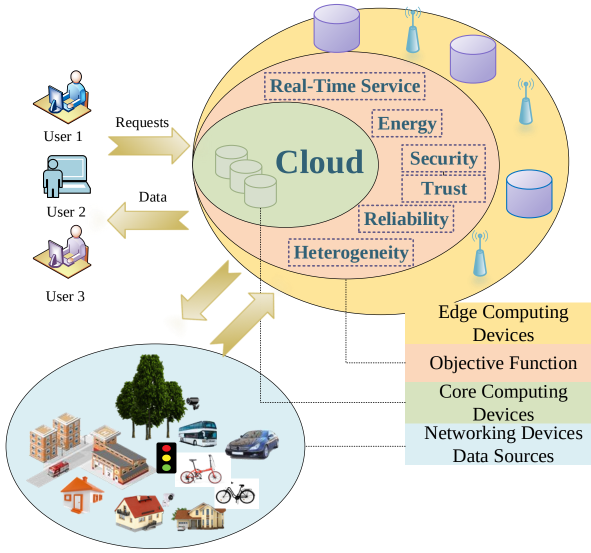


Fig. 7. An example of the sensor-cloud.

3.2.3 ***Management.*** As the name implies, sensor-cloud administrators provide management services. Management plays an important role in the operation of sensor-cloud systems [104], which can maintain all types of sensor groups through location calibration for the application layer and enhance virtualization of resources for the control layer.

3.2.4 ***Service.*** Overall, most of the existing application categories are very complex, with identity authentication, information filtering, querying, and collaborative-awareness services as the core contents [6]. The heterogeneity of sensor-cloud requires a thorough solution to realize ubiquitous services.

4 RESEARCH CHALLENGES

In this section, some challenges that exist in the current sensor-based cloud applications will be discussed together with the state-of-the-art developments and trends pertinent to the services delivered by a sensor-cloud. As illustrated in this section, numerous factors influence the design of a sensor-cloud system, including but not limited to, reliability, energy efficiency, and heterogeneity.

4.1 General Sensor-cloud Issues

Sensor-cloud systems encompass spatially distributed sensors or autonomous devices that are capable of sensing and monitoring physical environmental conditions in an intelligent and cooperative manner [105]. WSNs can provide all types of valuable data and the same could be applied for several domains [106]. Fig. 7 depicts general sensor-cloud issues, including security issues, trust issues, real-time services, reliability issues, energy issues, and heterogeneity issues.

With the development of the sensor-cloud systems, data security issues have become highly prominent. Hu et al. designed a facial recognition technique based on the edge pattern which had a positive effect on improving the performance in terms of confidentiality, integrity, and availability [107]. Henze et al. proposed a control mechanism for users to manage data stored in the cloud [108]. A new entity serves as a trusted node and acts as a bridge between the WSNs and the cloud server to connect them to the gateway. At the same time, the security of communication between the WSNs and the cloud is realized and the encryption mechanism is managed by an authorization service. To better address this problem, the authors continued the research and proposed a transparent access mechanism for the cloud service developers to use data [109].

Trust management plays a significantly important role in guaranteeing the privacy and security of a sensor-cloud and helps people overcome uncertainty and risky perceptions. Nevertheless, the problem of trust management in a sensor-cloud is rarely solved and defects in this aspect could affect a user's choice of the cloud service. Yang et al. proposed a trust evaluation mechanism to deliver content with low-latency based on the Fog Radio Access Networks (Fog-RAN) and presented a Riemannian trust-region method to solve the challenges of Low-Rank Matrix Completion (LRMC) [110]. In [111], a Trust-Assisted Sensor-Cloud (TASC) was envisaged to improve the quality of service (QoS) of a sensor-cloud to facilitate users so as to obtain sensory data from the cloud. Zhu et al. discussed how the edge-based trust evaluation mechanisms could be used to maintain the system security [112].

Centralized analysis and processing of data is an indispensable part of the multitudinous applications of instantaneity. Li et al. envisaged a novel real-time notification protocol that comprised of two different types of controls, namely (a) urgent actuator-oriented control and (b) uplink access and scheduling control [113]. During wireless control in the edge computing, this scheme can transmit real-time notification without interrupting any sort of ongoing transmissions. To avoid frequent transmission of the similar data and multi-user data requests at the same time to a sensor-cloud, Zhu et al. proposed a data transfer interaction scheme for multi-users that could better guarantee the sensor-cloud users' requirements regarding the delivery cost or delivery time [114].

The above studies mainly pay attention to security issues, trust issues, and real-time services and provide feasible solutions to those issues. However, the issues on reliability, energy, and heterogeneity are also indispensable to be addressed in a sensor-cloud system as they can effectively promote the development of a sensor-cloud. Hence, we particularly focus on these issues in this section.

4.2 Reliability Issues

The reliability issues within the sensor-cloud systems cannot be fully ignored primarily owing to the following facts. First, wireless reliable communication is vulnerable to path loss, shadowing, multi-path fading, and similar other key problems [115, 116]. Second, both node faults and link faults may result in reliability issues and bring negative impacts for the environment and this itself explains why the topology of a wireless sensor network changes dynamically [117]. Third, poor computing power and limited storage capacity of these nodes result in a large number of packet loss. Finally, a number of applications run in larger networks which reduce the overall reliability of wireless communication due to long-distance transmission and multi-hop errors [118]. In the next section, the reliability problem is divided into *hardware reliability*, *network reliability*, and *transmission reliability* in a logical manner.

4.2.1 ***Hardware Level***. A substantial number of the existing methods focus on capturing the state of sensor devices and monitoring the performance of nodes. Furthermore, the problem of coordination and reconfiguration between the nodes is always addressed by ensuring a solution for the reliability of nodes. Farshid et al. proposed a multi-directional adaptive sensing algorithm which took into consideration the condition of belief in the propagation protocol [27]. In Fig. 8, the server can coordinate nodes to achieve efficient data processing and reduce overhead, whereas, the data center has the mandate of fusing and storing the data along with predicting the number of lost packets. In [119], Sensor SelComp was proposed as a smart component and was implemented on

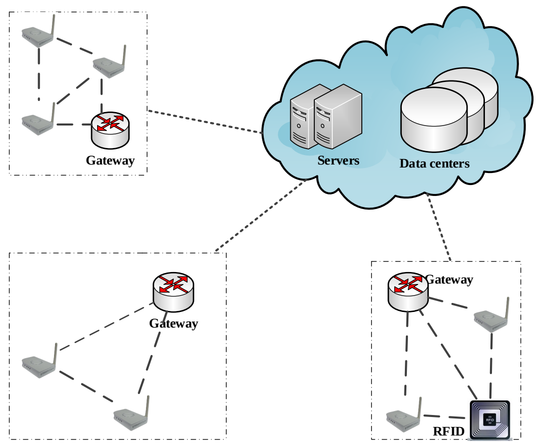


Fig. 8. The multi-directional adaptive sensing network architecture.

the factories' shop-floors. It could create the digital twin of a machine via sensors so as to ascertain the condition and behavior of equipment and subsequently expose its functionalities as services. A novel and extensible urban cloud network was proposed in [28]. The system components of this model were inspired by the theory of modularization and service composition which can maintain the stability and availability of the processing module. Nevertheless, the said schemes still need to be extended in order to achieve the optimal results and actual deployment. A fully distributed multi-link scenario is required for the follow-up discussion.

4.2.2 ***Network Level.*** The key of reliability on the network level lies in two aspects: i) the trade-off between reliability and collaboration and ii) the trade-off between reliability and sharing. Zhou et al. developed an analytical framework of reliability-oriented cooperative computation optimization and solved an execution time minimization model to obtain the success probability of application completion with the constrained computational capacity and application requirements [120]. By combining these models, the reliability of communication and computation by optimizing the data partitions among different cooperators can be achieved. A device/cloud framework had been presented in [121] to enable a trade-off between reliability and collaboration between smart devices and clouds [29].

Kuljeet et al. presented an edge-cloud interplay based on the promising paradigm of software-defined networks (SDN) [122]. The flow management using SDN is depicted in Fig. 9. Both the edge devices and the data centers have three states: Waiting, Active, and Suspended. According to the data center's network topology, the number of shortest paths between the edge devices is calculated and the traffic monitoring is turned on. The SDN controller detects whether the link traffic reaches the threshold value of the link bandwidth and dynamically adjusts the state value of an edge device. The SDN switches are responsible for judging the status value of the device and cloud and whether the data can be exchanged. Through the above scheme, the load flow in the data center network can be effectively balanced and the link congestion in the data center network can be alleviated. The underlying nodes are deployed in a complex environment, and therefore, more research should focus on the reliability of a sensor-cloud in various environments to keep the trade-off between reliability and collaboration and the trade-off between reliability and sharing.

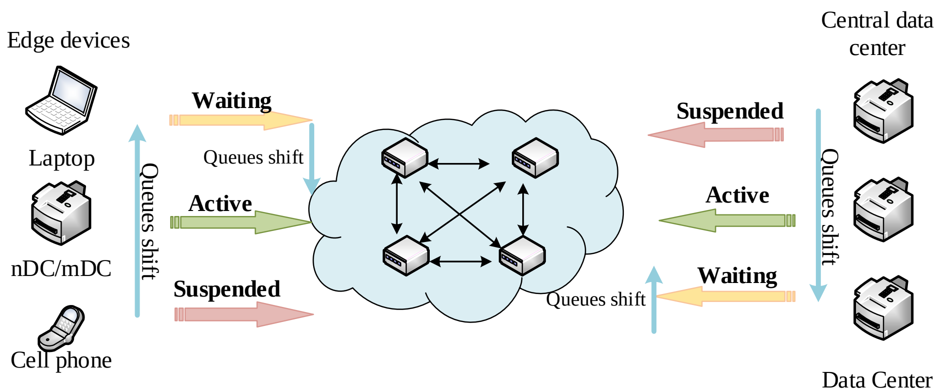


Fig. 9. Flow management using SDN.

4.2.3 ***Transmission Level.*** A reliable energy efficient platform that reduces the energy consumption and maintains privacy in transmission process was introduced [123]. The security approach of the platform utilizes a modified version of the sharing-based scheme and a precision enhanced and encryption mixed privacy preserving data aggregation scheme. A sensor-cloud collects and processes information from several sensor networks, enables information sharing on a big scale, and collaborates amongst the users via applications on the cloud [30]. In the current research, the performance of network architectures mainly focuses on setting different priorities, cultivating competition awareness, and integrating documents to address different information sources from where numerous sensor sets are virtualized. In the near future, more attention would perhaps be paid to design an object-oriented storage system and its performance of data service can be improved via exploring bandwidth and reliability or latency and reliability.

4.3 Energy Issues

Similar to the WSNs, the energy issues also act as a bottleneck in restricting the performance of a sensor-cloud. Adequate and stable energy supply forms an indispensable basis of data collection in any system [124, 125]. In this section, energy issues are categorized into two types, namely, energy saving methods and energy replenishing methods. The former emphasizes the reduction of energy consumption in the sensor-cloud systems via a particular architecture or scheme, whereas, the latter outlines the methods for stable and reliable energy supply for the sensor-cloud systems, especially for WSNs.

4.3.1 ***WSNs Level.*** All of the highlighted methods envisaged algorithms on sensors or sensor gates with relatively low computational capacity in contrast to the cloud. Therefore, the complexity of algorithms is minimal. However, many studies chose sensor gateways to apply their algorithms primarily owing to the differentiation advantages. The authors in [126] proposed an optimal bridge node selection strategy in order to minimize the energy consumption during the process of data transmission from a sensor network to a sensor-cloud. The study in [127] introduced an energy-efficient middleware mechanism for a sensor-cloud. It aimed to minimize the data transmission between the sensor gateways and the cloud gateways. Wu et al. [128] proposed a method taking into consideration the sampling frequency, residual energy, and the importance of sensors for an optimal relay sensor selection in order to balance the energy consumption in WSNs. Similarly, to reduce the energy consumption of the sensor-cloud systems, the authors in [129] proposed an event-driven data gathering scheme with fuzzy logic. Similar to WSNs, the architectural designs and services' deployment are more complex in case of the distributed services. With an increase in the system throughput, the response time becomes longer and longer, resulting in defects in other aspects [31, 130]. At the same time, running and maintenance of the system will meet greater challenges along with greater difficulties in testing and error detection.

4.3.2 ***Interaction Level***. The methods in this sub-section are characterized in accordance with the information provided by the WSNs, i.e., the cloud can optimize some parameters, such as the time interval, and send them back to the WSNs [32]. Owing to the strong computational power of the clouds, complex algorithms can be deployed to achieve optimal results. Javed et al. [93] proposed a decentralized smart controller combining the cloud with a random neural network in order to control the heating, ventilation, and air conditioning of the buildings. The authors in [131] segregated sensing missions into three different types and separated each type into many fine-grained operations. Dinh and Kim [132] proposed a decoupling model for both the information producers (IPDs) (i.e., physical sensors) and the information providers (IPVs). Yan et al. considered the optimal time interval selection strategy of the WSNs [133]. Several energy-saving methods reduce energy consumption by minimizing the communication between the WSNs and the cloud, i.e., either by reducing the data size of a single transmission via data compression and decoupling or by reducing the transmission frequency in the data prediction, aggregation, and time interval optimization [134]. Nevertheless, those schemes require high costs (i.e., for equipment and server) and are often attributed to slower implementation speed [135, 136]. Furthermore, the difficulty in balancing back-up and regeneration complicates the data migration process.

4.3.3 ***Cloud Level***. This sub-section emphasizes some of the operations of the cloud, i.e., applying machine learning algorithms for the data prediction and optimal sensor distribution for different user applications. To predict Bitcoin price at different frequencies using machine learning techniques, Chen et al. first classified Bitcoin price by the daily price and the high frequency price [137]. A set of high-dimensional features including property and network, trading and market, and attention and gold spot price are used for Bitcoin daily price prediction, whereas, the basic trading features acquired from a cryptocurrency exchange are used for 5-minute interval price prediction [138, 139]. Elodie et al. used a genetic algorithm to determine the optimal sensor distribution to estimate the horizontal stress due to strain observations [140]. Liu et al. proposed a new Bi-Population QUasi-Affine TRansformation Evolution (BP-QUATRE) algorithm for global optimization and applied the proposed algorithm to dynamic deployment in wireless sensor networks to make a good balance between exploration and exploitation capability [33]. WSNs could upload complex tasks to the cloud to reduce the local energy consumption [34, 141]. However, energy consumption for the transmission increases as the distance between the cloud and WSNs is relatively large.

4.3.4 ***Replenishing Level***. Owing to the fact that a cloud-based infrastructure results in increasing the response time and the bandwidth consumption, energy replenishing is also one of the research directions. This sub-section emphasizes wireless power transferring techniques in the sensor-cloud systems, a paradigm which has been attracting attention in recent years. In [142], the authors proposed a novel framework combining mobile cloud computing with the Microwave Power Transfer (MPT). The framework develops optimal policies so as to realize the optimization and selection of mobile mode in static and dynamic channels for replenishing energy to the mobile devices. A wireless charging platform based on quadcopters was proposed by Chen et al. [143] to address the charging problems in harsh environments. However, future research hot spots may focus on minimizing energy consumption for data processing, better task selection, and scheduling at the edge of the network and decentralized computing [144].

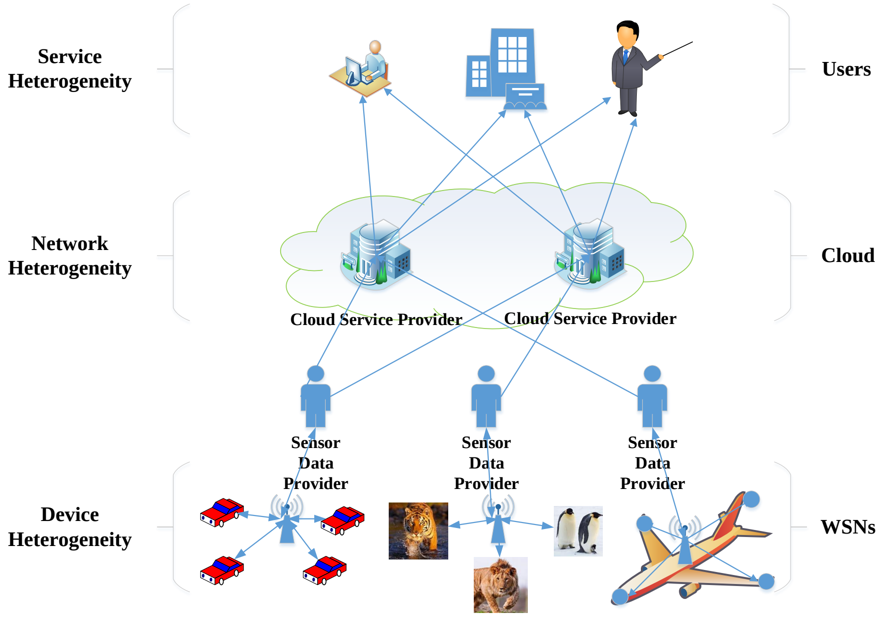


Fig. 10. Heterogeneity issues in different sensor-cloud layers.

4.4 Heterogeneity Issues

The heterogeneity issues are segregated into three layers in a sensor-cloud multi-tier architecture, as portrayed in Fig. 10. With an increase in the popularity of sensor-cloud, more and more heterogeneous sensor networks and cloud applications are embedded into sensor-cloud systems and the relationships between the service providers and users are becoming increasingly interconnected [25, 26]. Furthermore, a momentous amount of heterogeneous sensor data is produced, transmitted, and processed in the sensor-cloud systems on a continual basis [24]. Therefore, the heterogeneity issue becomes extremely important and indispensable. A simple example of the heterogeneity issue resembles a typical transmission application in our daily lives [145]. Imagine that one person plans to move from one place to another and she aims to find different travel information to meet her unique requirements. In this scenario, there are three important types of providers from the bottom to the top in a sensor-cloud, i.e., the sensor data providers (SDPs), CSPs, and transportation service providers (TSPs) [146]. Every sensor provider owns a subset of data such as information about bus, car, airplane and ship, and one or more of them send all or part of the sensor data to the sensor-cloud providers. We especially focus on heterogeneity at device level, network level, and service level in this section.

4.4.1 ***Device Level.*** There are two types of heterogeneity issues at the device level. The first one pertains to heterogeneous machines or sensors in the same sensor network. For the second one, heterogeneous machines or sensors lie in different sensor networks, which is derived from the resource sharing of sensor-cloud that virtualizes physical sensor nodes into clouds [48]. Hwang et al. [22] presented two scenarios: i) nodes were physically located in the same region and possess similar properties and ii) heterogeneous sensor nodes spread across different geographic regions and were used in the same VSs (Virtual Sensors). Fazio and Puliafito [147] also put forward two different models: a data-centric model and a device-centric model. For the device-centric model, a virtual sensing infrastructure could be used to satisfy the specific needs of the users. In regard to the device level, the most indispensable heterogeneity issue in the device level is the communication between sensor nodes within the same network and cooperation amongst sensor nodes from different networks to service one application. Nevertheless, all of such devices have basic features of servicing one-to-one application which makes the system less reliable than expected.

4.4.2 ***Network Level.*** This type of heterogeneity issues is a concern for CSPs which obtain sensor data from several SDPs. In a sensor-cloud, a number of sensor networks belong to different SDPs and provide different sensor data services. The heterogeneous sensor networks also exploit numerous communication technologies, including but not limited to, Wi-Fi, ZigBee, UMTS, and Ethernet. Neiat et al. [148] proposed a bridge node method that could be used to solve the transmission challenges from an underlying network to the cloud [23]. In the healthcare sector, patients are usually migrated from one heterogeneous monitoring area to another. However, how to ensure the interconnection between heterogeneous WSNs remains a major problem [149]. As for the network level, the integration of the sensor data which stems from the heterogeneous sensor networks becomes even more challenging when there is an influx of sensor data required to be processed in real-time [150]. In addition, researchers also have other concerns, such as delay, format translation, and storage mode [119].

4.4.3 ***Service Level.*** There are several application services in the sensor-cloud systems, nevertheless, each of them possesses different standards and data formats. Under these circumstances, users need to intelligently compare a number of these application services before they are able to choose the specific one in order to satisfy their unique requirements [154]. As for the users' mobility, resource provisioning becomes quite uncertain under different network environments as each task is implemented individually when complicated multitask applications are offloaded. Qi et al. [155] proposed a software-defined infrastructure system to decouple the resource control of the mobile clouds from the user plane. At the service level, a number of applications are emerging and users may select diverse heterogeneous services to satisfy their requirements. In this case, the focus of the service level should shift to provide users with uniform data interfaces from different service providers.

Summary. Table 4 summarizes the state-of-the-art sensor-cloud research. As for the architecture, some new sensor-cloud architectures are proposed to solve different problems but the physical layer or the cloud layer is often idealized to achieve better performance [93, 131]. edge computing has the characteristics of local deployment, i.e., closer to the users, offering a low delay, and so on. With the support of the edge computing, the edge computing layer acts as the intermediate tier between the upper and the lower layers of the cloud and the sensors which can achieve the ideal conditions mentioned in the above literature. Besides, running the proposed algorithm in the edge layer can further improve system performance. As for reliability, the existing methods mainly use complex encryption algorithms or trusted technology to ensure reliability but these methods often have a higher time complexity and a large delay [22, 151]. The edge layer is closer to users and safer and thus the important data can be only uploaded to the edge layer which can further improve the reliability of the system. As for mobility, fixed physical nodes are often used to collect data [67, 117]. Even mobile nodes are mainly used for mobile data collection. These mobile nodes naturally have the advantage of becoming the edge nodes. If these nodes constitute the edge layer, not only the mobility of the system can be improved but also the delay of the system can be further improved.

Table 4. Current sensor-cloud research

Sensor-cloud key tech.	Features	Requirements	Cyber approach description	Details of provided APIs	Handoff	Traffic	Client modification	References
Architecture	Model checking	Data sharing and protection	Collecting, storing, and sharing data from heterogeneous sensors.	√	Seamless	Down or uplink	×	[32], [80], [131], [93], [133].
Reliability	Symbolic execution	Updating and patching	Monitoring, maintenance, and data processing in some high-risk situations.	√	Time delay	Uplink	√	[151], [102], [101], [22].
Mobility	Theorem proving	Authentication, identification, and access control	A decentralized virtualization environment.	×	Seamless	Uplink	√	[116], [120], [67], [121], [30], [123], [90], [46].
Performance	Model checking	System, application, and solution lifecycle	Preform both online and offline data streams analysis through sensors.	√	Seamless	Down or uplink	×	[17], [87], [62], [93], [85], [88].
Load balancing	Model checking	Proportional and optimization	Maintain the weighting ratio of maximize throughput and fair bandwidth allocation.	×	Time delay	Uplink	×	[13], [152], [42], [77], [82], [153].
Energy efficiency	Symbolic execution	Available bandwidth	Reducing packet switching delays while cutting down energy consumption.	×	Time delay	Downlink	√	[102], [6], [103], [104].
Overall performance	Theorem proving	Number of clients	Including transmission, re-association cost, and inter-packet delay, etc.	√	Time delay	Down or uplink	√	[26], [24], [25].
Management	Symbolic execution	Monitoring, analysis, and response	A resource abstraction at the sensor level and provide uninterrupted services.	√	Seamless	Downlink	√	[27], [28], [30], [119].

As for load balancing, it avoids a situation, wherein some edge data centers are heavily loaded while others are in an idle state or doing little data processing [13, 153]. Because of the mobility of the edge nodes, the system architecture can be dynamically adjusted to achieve load balancing. As for energy efficiency, it is a significant issue in the edge computing paradigm to reduce the service cost and protect the environment [6, 102]. A plethora of research has been conducted to reduce energy consumption in the edge computing primarily focusing on the scheduling of incoming jobs to improve energy efficiency. As for management, the research focuses on a resource abstraction at the sensor level and uninterrupted services are provided [24, 25]. edge computing is introduced to provide computation, storage, and networking services between the end users and traditional cloud computing data centers. With the help of the edge computing, the current edge computing platform can be expanded so as to support secure collaboration and interoperability between different users' requested resources. As for overall performance, the papers focus on transmission, re-association cost, and inter-packet delay, etc. The performance of the system can be improved in respect of nodes management, collection control, data process, and data storage in edge computing.

In conclusion, most of the existing solutions propose a somewhat similar sensor-cloud architecture and none of these studies have provided a holistic integrated view of the factors which drives the design of a sensor-cloud system. These factors are extremely critical primarily owing to the fact that they serve as a useful guideline in the design of a protocol (or an algorithm) for the sensor-cloud systems [156]. It is also interesting to note that the edge layer is only used in certain specialized scenarios, e.g., in the domain of healthcare. Future studies should consider more general scenarios. We, thus, need to enhance the study on the capability of the edge layer to design a more secure and sophisticated system that could advance the development of the sensor-clouds.

5 LEVERAGING THE EDGE COMPUTING FOR A SENSOR-CLOUD AND ITS FUTURE DIRECTIONS

edge computing could be applied across several industries primarily owing to its strong computational and storage capabilities. In this section, several research aspects will be examined which mainly focus on how to improve the reliability and energy efficiency of a sensor-cloud and how to design an efficient scheme to solve the heterogeneity issues in a sensor-cloud system. Such models facilitate in eliminating problems, including but not limited to, limitations in storage resources, constraints in computing power, and high communication costs for the users. This section also discusses some potential enhancements to the sensor-cloud systems enabled by the edge computing and highlights further improvements as future research directions.

5.1 Proposed edge computing Model

To achieve efficacious system performance, the edge computing model is introduced as a supplement to the cloud computing as depicted in Fig. 11. This model is another contribution of this paper. In the three-layered abstract mechanism of the sensor-cloud systems, the top-most layer is a cloud service data center with strong computational and storage capabilities [56, 57]. The bottom layer is a sensor network layer encompassing ordinary sensor nodes [157]. In the middle layer, the edge server is composed up of nodes possessing strong capability within the WSNs. Some localized and real-time computational tasks would be processed in the edge nodes [89].

The introduction of the edge computing breaks the conventional settings and extends computing to the edge of the network by employing the promising paradigm of distributed computing [158, 159]. Fig. 11 delineates the architectural design of the edge computing. Sensor-cloud systems contain several advantages, including but not limited to, speeding up data processing, improving efficiency, saving the network bandwidth, and improving security and elasticity. However, many important IoT use cases are difficult or impossible to implement in a completely cloud-based or a thing-based architecture owing to some objective requirements [160]. With the introduction of the edge layer, the system can be improved in respect of the node management, collection control, data process, and data storage. Besides, the edge layer can enhance the traditional WSNs as it can make up for the defects in the underlying network, i.e., in terms of energy shortage and insufficient compute and storage. Once the key requirements and architecture of the edge are clear, it is then possible to further segregate the system into edge elements. Subsequently, we can make full use of these elements to generate effective structures and the high-level designs. The proposed edge computing model can improve numerous aspects of a sensor-cloud which would be elaborated below, thereby implying that edge is conducive to solving various problems [161, 162].

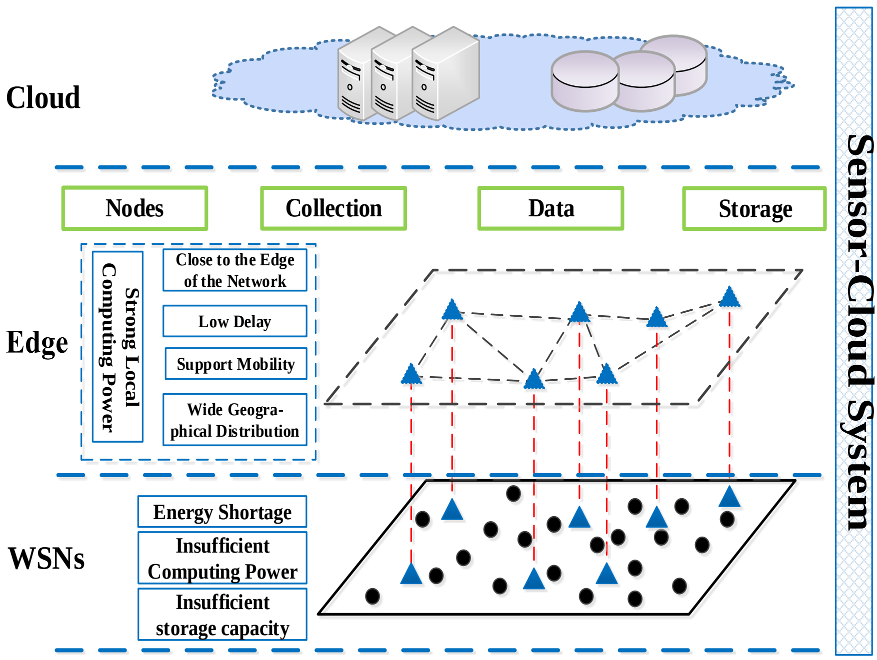


Fig. 11. An edge-based model in the sensor-cloud systems.

5.2 Leveraging edge computing for Sensor-cloud and Its Future Directions

5.2.1 ***Reliability Issues.*** With an expedited proliferation in the generation of numerous forms of data, the emergence of the cloud storage has attracted considerable attention. For the public cloud applications, the cloud service providers maintain and orchestrate infrastructure [163]. This implies that a user's data cannot be controlled by herself and the reliability of data is at great risk. The data of the users is likely to be delivered to the parties who are thus not reliable. To protect users' privacy, an edge-based three-layer storage (TLS) scheme is proposed which enables users to manage the data and enhances data security to a certain extent. As illustrated in Fig. 12, the framework mainly makes use of the data storage and the processing capability of the edge server. In the three-layered structure, Hash-Solomon code is applied to ascertain the minimum volume of data that can be stored locally (e.g., 1%). The remaining data is properly segregated and thus uploaded to the edge server (e.g., 4%), and the cloud server can protect privacy and ensure the reliability and security of the users' data (e.g., 95%). Such a design effectively protects data from being restored to its entirety even if any layer of data is maliciously leaked or stolen.

A reputation evaluating mechanism was also designed for Cloud Server Provider (CSP) in edge layer [164] . Each bad behavior caused by CSP will have a negative influence on itself. The reputation evaluation is composed of user's grade, and the basic value of the CSP. The user's grade is subjective. Hence the authors add an objective perspective as the basic value of the CSP, which consists of industry metrics, such as storage technology, price storage performance, and so on. The percentage of this part in the whole value is 70%-80% and will be renewed once a year.

The proposed design has been validated via an experiment. Fig. 13a reflects the difference between TLS and scheme without credit [165] (i.e., no-credit scheme). It is clear that the number of failures of

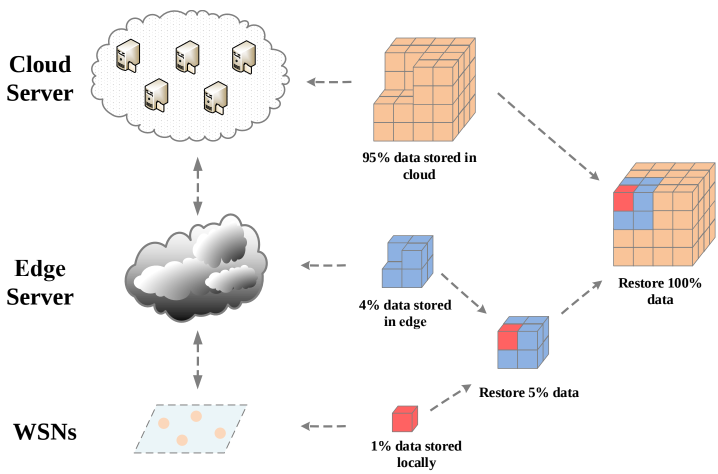
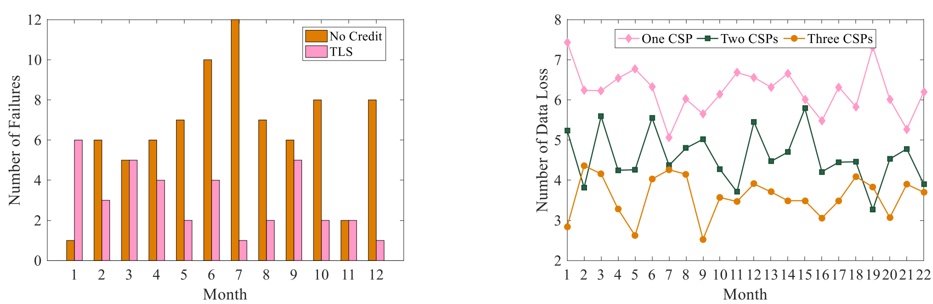


Fig. 12. Applying the three-layer storage scheme.



(a) The proposed scheme vs. no-credit mechanism.

(b) One CSP vs. Multi-CSPs.

Fig. 13. Performance of the proposed edge-based storage scheme.

CSPs in TLS is less than the number of failures in the no-credit scheme. This is because of the CSPs' self-adjusting according to the feedback from the reputation evaluation. Fig. 13b highlights that the number of data loss declines when the number of CSPs increases. Less data loss means more reliability of the user's data, which proves that more CSPs can ensure the reliability of the users' data. However, choosing more CSPs means higher economic cost, so how to balance economic cost and data reliability is an interesting research direction.

Nevertheless, many reliability challenges need to be addressed shortly. The first challenge is transient storage, i.e., the local storage embedded to simplify the data management operations may result in new challenges in the context of security and privacy [166]. Therefore, studies on the security of the sensor-cloud take into consideration sensitive data identification and protection and secure data sharing [167, 168]. Against the backdrop of big data, it is possible to combine the characteristics of edge computing with the paradigm of deep learning. The hierarchical processing mode is a good attempt to amalgamate these two technologies. From the extraction and analysis of the features of data, the system can handle data persistence to solve the storage and sharing problems of big data so as to ensure the security and convenience of the entire system. The second challenge is the attack surface, i.e., by decoupling the control plane from the data plane, the attack surface for sensor-cloud is enlarged when compared with the conventional networks [169]. Edge computing offers technical support to avoid this problem. The mobile edge nodes send commands and read data through communication processes, whereas, the cloud is only the center for data convergence. The control and trust of data are addressed as well. To solve the above challenges, federated learning (FL) [170] has emerged as another promising privacy preserving approach that is integrated with the edge computing architecture. A multi-layer federated learning protocol needs to be designed for the edge-based sensor-cloud system which adopts two levels (i.e., the edge level and the cloud level) of model aggregation enacting different aggregation strategies to improve the reliability of the system.

5.2.2 ***Energy Issues****.* The data acquisition process in a sensor-cloud is primarily constrained by the weak communication capabilities of the WSNs [118, 171]. As sensors possess low bandwidth and limited energy sources, the ordinary nodes are unable to meet the requirements of limited energy in a sensor-cloud system [172, 173]. The proposed model is composed of multiple high-performance mobile nodes which can compensate for the technical deficiencies between the WSNs and the cloud [174]. In the architecture portrayed in Fig. 14, the three layers cooperate to maximize the throughput and reduce transmission delay to reduce energy consumption. The principle of Voronoi from the graph theory is adopted to divide the plane into regions and achieve the initial setting of the said architecture. Based on the architecture, a Distributed Coordination Function (DCF) was designed to obtain the minimum cost schedule between Voronoi areas (VA), to maximize throughput and minimize the latency from WSNs to the Cloud. Specifically, they design an energy-efficient routing algorithm for sensors in edge layer, which considers energy consumption and hops.

To evaluate the proposed algorithm, the authors also compare DCF with Ad hoc On-demand Distance Vector Routing (AODV) [175] and Random Rebroadcast Delay (RRD) [176]. AODV is an on-demand routing method in which the network generates routes at the beginning of communication and RRD is a simple random rebroadcast routing protocol based on the process of flooding-based route discovery. Experiments portray the performance comparison vis-á-vis the other state-of-the-art schemes. Fig. 15a shows the total energy consumption results in which DCF spends less energy than RRD and AODV because RRD spends more energy in route finding and AODV needs to repair unreachable paths. Fig. 15b indicates that the number of exhausted sensors as a function of data volume increases. Because there is a path selection in DCF, the rate of exhausted sensors is approximately 45% less than that of RRD and approximately 20% less than that of AODV. In a word, DCF has the merit of low energy consumption than RRD and AODV which proves the proposed scheme in [174] can efficiently reduce energy consumption.

The energy issues from the combination of the sensor-cloud systems and the edge computing are far from perfect. In the above scheme, the Voronoi area is formed by the location of the mobile station. In the future, we can try to consider the clustering method for partition, and design the mobile collection path of the station. In addition, combining the traditional methods with the edge computing model is a promising way to solve energy issues in the sensor-cloud systems. The traditional energy-saving methods reduce energy consumption by minimizing the communication between the WSNs and the cloud [177], i.e., either in the form of a reduction in the data size of a single transmission namely data compression or decoupling or with a cut back in the transmission frequency such as specific data prediction and optimization of the data screening and the time interval [178]. In the future, as for the data prediction methods, through the historical data collected by the edge layer, the data prediction model is established which can greatly reduce energy consumption during the process of data transmission [179]. To be more specific, the

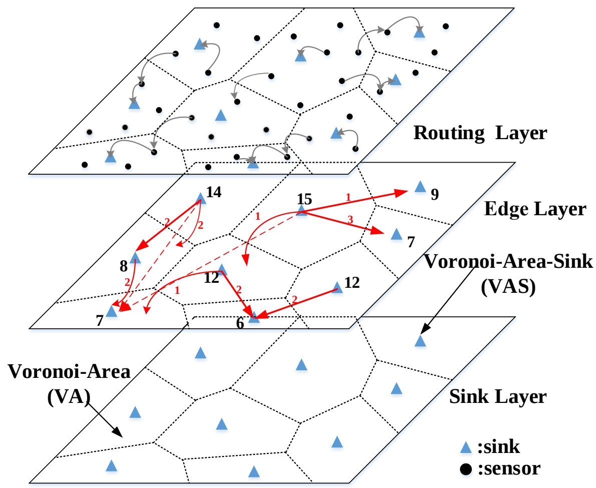
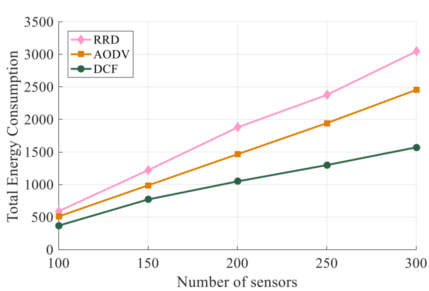
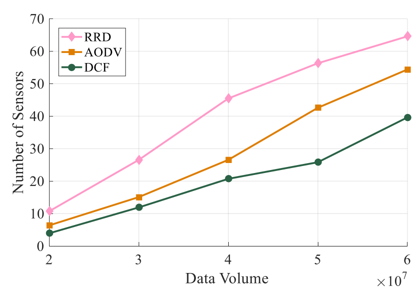


Fig. 14. Illustration of the envisaged real-time data collection scheme based on edge.



(a) Total energy consumption of three scheduling schemes.



(b) Number of exhausted sensors with different data volume.

Fig. 15. The algorithm performance of the three layers cooperative data collection.

same prediction algorithm could be deployed between the cloud-edge and the edge-end. There is no need to transmit data if the data prediction accuracy is acceptable between the cloud-edge and the edge-end, which saves lots of energy consumption. For instance, as for data screening methods, a data filtering scheme based on the edge computing needs to be designed which aims to maintain a spatial data set through the edge servers (i.e., data may either be a single value or a vector data value) and distinguishes between the spatial positions via projections on three planes [180]. The data values could be displayed intuitively through this mechanism and abnormal values would be highlighted directly in the spatial coordinates via the characteristics of color and volume followed by their screening and elimination within the subsequent operation. In this way, energy consumption can be significantly reduced.

Similar to the reliability issues, the federated edge learning [181] method is another promising way to improve the energy efficiency in which an edge server coordinates a set of edge devices in order to train a shared machine learning model based on their locally distributed data samples. Specifically, during the distributed training, the joint communication and computation design

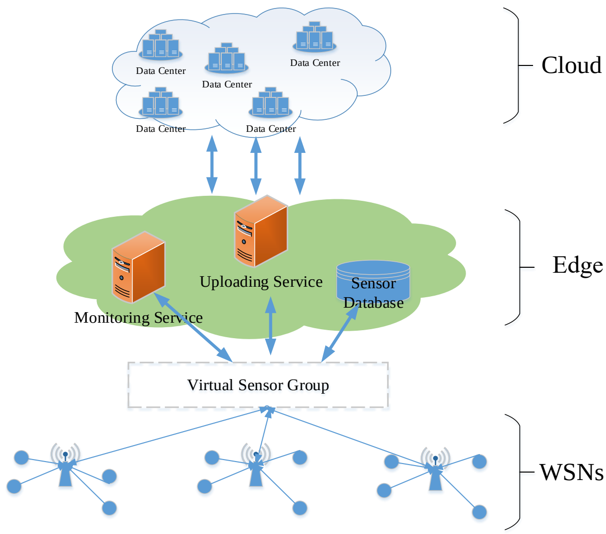


Fig. 16. Three levels of the hierarchical trust mechanism.

can be exploited for improving the system's energy efficiency, wherein both the communication resource allocation for aggregating global ML parameters and the computation resource allocation for locally updating ML parameters can be jointly optimized.

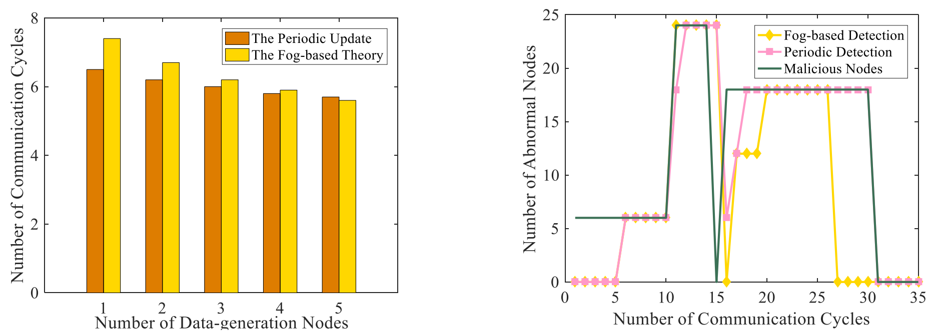
5.2.3 ***Heterogeneity Issues.*** As we mentioned, the heterogeneity issues become extremely important and indispensable. However, current methods cannot solve the problem well because it is hard to manage the various heterogeneous devices [156, 182]. Furthermore, several heterogeneous devices are non-trusted which may produce false sensory data to mislead users to make incorrect decisions.

To address the heterogeneity issues and to overcome the limitations of trust evaluation in the underlying networks, an edge-based trust evaluation scheme is proposed [183]. As shown in Fig. 16, this hierarchical trust mechanism comprises the following three levels:

- The direct trust calculation at the first level is ascertained via Eq. (1). T_{packet} means the ratio that the number of data packets lost. $Delay_{forward}$ means the time interval from receiving data to forwarding data. $T_{history}$ means the history direct trust value to reduce the influence of nodes' value fluctuates with the change of network load and environment. The value of $Delay_{forward}$ is calculated by T_{packet} and $T_{history}$ based on the weighted method. For weighted values, $w_1 + w_2 = 1$. To decrease energy consumption in the data transmission, the trust detection period among nodes is maximized in a reasonable range, but the trust value might become too old to reflect the current trust state of the node. So the weight of $T_{history}$ was cut down in the experiment.

$$T_{direct} = \left(w_1 T_{packet} + w_2 T_{history}\right) \times Delay_{forward} \tag{1}$$

- The recommendation trust value at the second level is computed via Eq. (2). The $set(neighbor)$ refers to a trusted node set of the source node. The $Trest_{(j,k)}$ refers to the trust value of node j to node k. The $w_i(i, j)$ refers to the weighted value of every adjacent node by an arithmetic progression, as Eq. (3). Where parameter i refers to the location value of nodes and parameter n refers to the node number in $set(neighbor)$. Moreover, synthesis trust is computed via



(a) Detection speed of malicious nodes.

(b) Misjudgment node recovery.

Fig. 17. Performance of the proposed edge-based evaluation mechanism.

Eq. (4) in edge layer, which is based on T_{direct} and $T_{recommendation}$. The weighted value of $T_{recommendation}$ is smaller than T_{direct}, and $w_3 + w_4 = 1$.

$$T_{recommendation} = \sum_{i \in set(neighbor)} w_{i(i,j)} \times T_{(j,k)} \tag{2}$$

$$w_i(i,j) = \frac{i}{\sum_1^n i} = 2 \times \frac{i}{n(n+1)} \tag{3}$$

$$T_{synthesis} = w_3 \times T_{direct} + w_4 \times T_{recommendation} \tag{4}$$

- At the third level, an important part is the analysis of the heterogeneous devices. Some heterogeneous devices provide wrong sensor data to lead users to make wrong decisions. The edge layer can process sensor data from several nodes at the same time and recognize whether there are malicious nodes by some data correlation phenomenon indicators, such as similar trajectory, variation trend, fault-tolerant interval, etc.

Wang et al. provide a comparison of the periodic update [184] and the edge-based approach [183]. For the periodic update, nodes update trust values of their neighbor nodes when the period is over. In Fig. 17a, the authors randomly add heterogeneous devices in three levels. The proposed scheme indicates a more intuitive downward trend in communication cycles which means the scheme can evaluate heterogeneity issues well. In Fig. 17b, the authors add one type of condition every five communication cycles. After six communication cycles, the edge-based design and periodic update method recognize malicious nodes simultaneously. The cleanup method of malicious nodes is implemented at 15 communication cycles and the environment is changed at 16 communication cycles. Some nodes that are sensitive to environment display anomalous behaviors which might be misjudged as malicious nodes. For those nodes, the edge layer analyzes whether those nodes are real malicious or not by the direct trust tables, recommendation trust tables, long-term sensor data, and network topology. After a reasonable delay, the proposed scheme recovers misjudgment nodes before the cleanup method at 31 communication cycles. The results indicate that the scheme can execute the recovery of misjudged nodes and guarantee the permanent stability of the network performance.

Table 5. Comparison of edge-based schemes

Key issues	Main Feature	Handoff	Edge assisted	Provided APIs	Client modification	References
Reliability	Integrating linear error correcting codes and linear homomorphic authentication schemes.	Data loss	×	√	√	[163] [165][166]
	Allowing only authorized servers to jointly test whether a search token matches a stored ciphertext.	Number of failures	√	×	√	[167] [168][169]
	Including erasure code, malicious modification detection and reputation evaluating.	Data loss and number of failures	√	√	√	[164] (Proposed)
Energy	Random rebroadcast routing algorithm based on flooding-based route discovery.	Energy consumption	√	×	√	[175] [118] [171]
	Generating on-demand routes at the beginning of communication.	Delay	×	√	×	[176] [177] [178]
	Obtaining the minimum cost schedule between Voronoi areas.	Energy consumption and delay	√	√	√	[174] (Proposed)
Heterogeneity	Providing protection against rank and sybil attacks.	Communication cycles	√	√	×	[184] [185][186]
	Solving uncertainty and fuzziness of trust based on cloud theory.	Number of abnormal nodes	×	√	√	[182][156] [187]
	Monitoring the whole network trust state, detecting data attacks and recovering misjudgment nodes.	Communication cycles and number of abnormal nodes	√	√	√	[183] (Proposed)

Similar to the reliability issues and the energy issues, there are several edge-based solutions for enhancing improvements in the near future. One of the future research directions is to build a trust recovery mechanism in edge layer. The combination of data analysis and verification scheme can be used to verify whether the "malicious member" is malicious through the known information. Edge-based trust assessment is another promising way to solve heterogeneity issues. Edge nodes can be envisaged by utilizing their capability of communication which gives full play to the mobility of the edge nodes. Edge nodes can move to any heterogeneous devices, thereby constructing a trust transmission chain in a bid to collect the data of heterogeneous devices. The chain formation needs to be realized in such a way that the total length should be as short as possible whilst avoiding the selection of the untrusted nodes. This ensures the accuracy of trust evaluation to improve data quality. Based on the trust assessment, mobile data from trusted nodes could be gathered and any untrusted sensor nodes could be bypassed to avoid unnecessary movement delay [185, 186]. Furthermore, one research domain that needs to be researched is the ascertaining of trust evaluation of mobile nodes concerning the scope of their activities. Thus, a path planning strategy, with no reliance on the previous point-to-point evaluation mechanism, may be designed and subsequently employed to transform the activity range of mobile nodes into their corresponding parameters for overall trust evaluation [187–189].

Table 5 summarizes the state-of-the-art schemes to solve the three key issues. As for the reliability issue, the current research mainly adopts the solution based on cloud technology and does not consider the tradeoff between reliability and efficiency. Even if some schemes introduce edge computing, they do not fully consider the cooperation between cloud and edge in computing, storage, and network resources. This causes serious packet loss and high data transmission errors. Wang et al. [164] propose TLS scheme to overcome the shortcomings which makes a good tradeoff between reliability and efficiency.

As for the energy issues, the schemes mainly depend on the underlying devices to collect data, which results in large delays and high energy consumption due to the limited energy and storage capacity of the underlying devices. Wang et al. [174] propose the DCF scheme, which makes full use of the computing capacity of the edge layer and reduces energy consumption. As for the heterogeneity issues, the main idea of the current scheme is to use centralized cloud servers or only local devices to evaluate the underlying nodes, and rarely consider the advantages of edge computing, thus resulting in high communication cost and abnormal node access. Wang et al. [183] propose a scheme which makes full use of the high reliability of the edge layer and can reasonably evaluate the nodes.

In short, the present research is trying to combine sensor-cloud with edge computing. However, on the one hand, the current schemes mainly use centralized cloud technology, which does not give full play to the advantages of "nearby computing" of edge computing. Sensor-cloud and edge computing collaboration is still in the preliminary stage. On the other hand, the algorithms are scattered, personalized, and only solve specific problems. One of the future research directions is the in-depth collaboration of sensor-cloud and edge computing.

6 CONCLUSION

Sensor-cloud facilitates the construction of pervasive data networks by extensively leveraging the paradigms of wireless sensor networks and the powerful cloud computing. It has been established as a promising notion for the efficiency and reliability in critical services. In this paper, we offer a more thorough walk-through of sensor-cloud with four-layer architecture and the main components.

We present a comprehensive survey on over 180 academic and industrial works related to edge-based sensor-cloud, which focus on the various research problems. We contribute to classify those emerging problems into three different categories, namely reliability, energy, and heterogeneity, and further explore the complexities involved in the state-of-the-art edge-based schemes. We then propose a generic edge-based framework that aims to overcome the various challenges. We particularly consider those challenges of leveraging edge computing for a sensor-cloud and develop several edge-based research prototypes targeting the three key challenges, which have great potential to be applied in real-world scenarios. As another important contribution of this paper, we highlight the salient open issues and future directions. These issues are currently the focus of extensive research and would continue to receive considerable attention in the near future.

ACKNOWLEDGMENTS

The above work was supported in part by grants from the National Key R&D Program of China (2022YFE0201400), the National Natural Science Foundation of China (NSFC) under Grant No. 62172046, the Natural Science Foundation of Fujian Province of China (No. 2020J06023), the Special Project of Guangdong Provincial Department of Education in Key Fields of Colleges and Universities (2021ZDZX1063), the Jiont Project of Production, Teaching and Research of Zhuhai (ZH22017001210133PWC), Guangdong Key Lab of AI and Multi-modal Data Processing, BNU-HKBU United International College (UIC), Zhuhai, No. 2020KSYS007, UIC Start-up Research Fund under Grant No. R72021202.2, UIC General project under Grant No. R0200005-22, the Australian Research Council Linkage Project under Grant LP190100676, the Australian Research Council (ARC) Future Fellowship Grant FT140101247, and the Interdisciplinary Fund Project for Academic Year 2021-2022 of Beijing Normal University at Zhuhai (BNUZHXKJC-14).

REFERENCES

[1] Ding Wang, Ping Wang, and Chenyu Wang. Efficient multi-factor user authentication protocol with forward secrecy for real-time data access in wsns. *ACM Transactions on Cyber-Physical Systems*, 4(3):1–26, May 2020.

[2] Tian Wang, Yuzhu Liang, Yi Yang, Guangquan Xu, Hao Peng, Anfeng Liu, and Weijia Jia. An intelligent edge-computing-based method to counter coupling problems in cyber-physical systems. *IEEE Network*, 34(3):16–22, 2020.

[3] Rana M Abdul Haseeb-Ur-Rehman, Misbah Liaqat, Azana Hafizah Mohd Aman, Siti Hafizah Ab Hamid, Rana Liaqat Ali, Junaid Shuja, and Muhammad Khurram Khan. Sensor cloud frameworks: State-of-the-art, taxonomy, and research issues. *IEEE Sensors Journal*, 21(20):22347–22370, 2021.

[4] Sunanda Bose, Sumit Kumar Paul, and Nandini Mukherjee. Predicting spatio-temporal phenomena of mobile resources in sensor cloud infrastructure. *ACM Transactions on Spatial Algorithms and Systems*, 7(3):1–38, 2021.

[5] Tian Wang, Yuzhu Liang, Weijia Jia, Muhammad Arif, Anfeng Liu, and Mande Xie. Coupling resource management based on fog computing in smart city systems. *Journal of Network and Computer Applications*, 135:11–19, 2019.

[6] Guangjie Han, Xu Miao, Hao Wang, Mohsen Guizani, and Wenbo Zhang. Cpslp: a cloud-based scheme for protecting source location privacy in wireless sensor networks using multi-sinks. *IEEE Transactions on Vehicular Technology*, 68(3):2739–2750, March 2019.

[7] Rajendra Kumar Dwivedi, Munish Saran, and Rakesh Kumar. A survey on security over sensor-cloud. In *Proceedings of the 2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence'19)*, pages 31–37. IEEE, 2019.

[8] R Geetha, AK Suntheya, and G Umarani Srikanth. Cloud integrated iot enabled sensor network security: research issues and solutions. *Wireless Personal Communications*, 113(2):747–771, 2020.

[9] Nawaf Almolhis, Abdullah Mujawib Alashjaee, Salahaldeen Duraibi, Fahad Alqahtani, and Ahmed Nour Moussa. The security issues in iot-cloud: a review. In *2020 16th IEEE International Colloquium on Signal Processing & Its Applications (CSPA)*, pages 191–196. IEEE, 2020.

[10] Mohammad Farhan Khan, Rajendra Kumar Dwivedi, and Rakesh Kumar. Towards power aware data transmission in sensor cloud: a survey. In *Proceedings of the International Conference on Computer Networks and Inventive Communication Technologies (ICCNCT'19)*, pages 317–325. Springer, 2019.

[11] Jasenka Dizdarević, Francisco Carpio, Admela Jukan, and Xavi Masip-Bruin. A survey of communication protocols for internet of things and related challenges of fog and cloud computing integration. *ACM Computing Surveys (CSUR)*, 51(6):1–29, 2019.

[12] Rajendra Kumar Dwivedi, Nikita Kumari, and Rakesh Kumar. Integration of wireless sensor networks with cloud towards efficient management in iot: a review. In *Proceedings of the Advances in Data and Information Sciences*, pages

97–107. Springer, 2020.

[13] Rajendra Kumar Dwivedi and Rakesh Kumar. Sensor cloud: integrating wireless sensor networks with cloud computing. In *Proceedings of the 2018 5th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON'18)*, pages 1–6. IEEE, November 2018.

[14] Ju Ren, Deyu Zhang, Shiwen He, Yaoxue Zhang, and Tao Li. A survey on end-edge-cloud orchestrated network computing paradigms: transparent computing, mobile edge computing, fog computing, and cloudlet. *ACM Computing Surveys (CSUR)*, 52(6):1–36, 2019.

[15] Motahareh Nazari Jahantigh, Amir Masoud Rahmani, Nima Jafari Navimirour, and Ali Rezaee. Integration of internet of things and cloud computing: a systematic survey. *IET Communications*, 14(2):165–176, 2020.

[16] Yulei Wu. Cloud-edge orchestration for the internet-of-things: Architecture and ai-powered data processing. *IEEE Internet of Things Journal*, 2020:1–14, 2020.

[17] Sudip Misra, Subarna Chatterjee, and Mohammad Obaidat. On theoretical modeling of sensor cloud: A paradigm shift from wireless sensor network. *IEEE Systems Journal*, 11(2):1084–1093, June 2017.

[18] Waqas Ahmad, Aamir Rasool, Abdul Rehman Javed, Thar Baker, and Zunera Jalil. Cyber security in iot-based cloud computing: A comprehensive survey. *Electronics*, 11(1):1–34, 2021.

[19] Fei Chen, Duming Luo, Tao Xiang, Ping Chen, Junfeng Fan, and Hong-Linh Truong. Iot cloud security review: A case study approach using emerging consumer-oriented applications. *ACM Computing Surveys (CSUR)*, 54(4):1–36, 2021.

[20] Xiting Peng, Kaoru Ota, and Mianxiong Dong. Multi-attribute based double auction towards resource allocation in vehicular fog computing. *IEEE Internet of Things Journal*, 7(4):3094–3103, 2020.

[21] Chuan Lin, Guangjie Han, Xingyue Qi, Mohsen Guizani, and Lei Shu. A distributed mobile fog computing scheme for mobile delay-sensitive applications in sdn-enabled vehicular networks. *IEEE Transactions on Vehicular Technology*, 69(5):5481–5493, 2020.

[22] Renhung Hwang, Yuling Hsueh, and Haowei Chung. A novel time-obfuscated algorithm for trajectory privacy protection. *IEEE Transactions on Services Computing*, 7(2):126–139, June 2014.

[23] Lianyong Qi, Shunmei Meng, Xuyun Zhang, Ruili Wang, Xiaolong Xu, Zhili Zhou, and Wanchun Dou. An exception handling approach for privacy-preserving service recommendation failure in a cloud environment. *Sensors*, 18(7):1–11, June 2018.

[24] Fabio Antonelli, Vittorio Cortellessa, Marco Gribaudo, Riccardo Pinciroli, Kishor S. Trivedi, and Catia Trubiani. Analytical modeling of performance indices under epistemic uncertainty applied to cloud computing systems. *Future Generation Computer Systems*, 102:746–761, 2020.

[25] Azadeh Neiat, Athman Bouguettaya, Timos Sellis, and Sajib Mistry. Crowdsourced coverage as a service: two-level composition of sensor cloud services. *IEEE Transactions on Knowledge and Data Engineering*, 29:1384–1397, July 2017.

[26] Chunlin Li A B, Jingpan Bai A, Ge B Yuan, and Youlong Luo A. Heterogeneity-aware elastic provisioning in cloud-assisted edge computing systems. *Future Generation Computer Systems*, 112:1106–1121, 2020.

[27] Farshid Bijarbooneh, Wei Du, Edith Ngai, Xiaoming Fu, and Jiangchuan Liu. Cloud-assisted data fusion and sensor selection for internet of things. *IEEE Internet of Things Journal*, 3(3):257–268, June 2016.

[28] Hao, Yufu Suling, and Jia Jinxing. A scalable cloud for internet of things in smart cities. *Journal of Computers*, 26(3):1–13, 2015.

[29] Hanbo Yang, Zheng Sun, Gedong Jiang, Fei Zhao, Xufeng Lu, and Xuesong Mei. Cloud manufacturing-based condition monitoring platform with 5g and standard information model. *IEEE Internet of Things Journal*, 8(8):6949–6948, 2020.

[30] S Subashini and P Mathiyalagan. A cross layer design and flower pollination optimization algorithm for secured energy efficient framework in wireless sensor network. *Wireless Personal Communications*, 112:1601–1628, 2020.

[31] M Amin Yazdi and Marius Politze. Reverse engineering: the university distributed services. In *Proceedings of the Future Technologies Conference (FTC'20)*, pages 223–238. Springer, 2020.

[32] Aishwariya Chakraborty, Sudip Misra, and Ayan Mondal. Qos-aware dynamic cost management scheme for sensors-as-a-service. *IEEE Transactions on Services Computing*, 2020:1–12, 2020.

[33] Nengxian Liu, Jeng-Shyang Pan, et al. A bi-population quasi-affine transformation evolution algorithm for global optimization and its application to dynamic deployment in wireless sensor networks. *EURASIP Journal on Wireless Communications and Networking*, 2019(1):175, 2019.

[34] Fatemeh Heravan, Mohammad Moghaddam, and Seyed Seno. Sdn-based scheduling strategy on load balancing of virtual sensor resources in sensor-cloud. In *Proceedings of the 8th International Symposium on Telecommunications (IST'16)*, pages 666–671, September 2016.

[35] Dwivedi R K, Singh S, and Kumar R. Integration of wireless sensor networks with cloud: a review. In *Proceedings of the 2019 9th International Conference on Cloud Computing, Data Science and Engineering (Confluence'19)*, pages 114–119. IEEE, 2019.

[36] Tian Wang, Yuzhu Liang, Yujie Tian, Md Zakirul Alam Bhuiyan, Anfeng Liu, and A Taufiq Asyhari. Solving coupling security problem for sustainable sensor-cloud systems based on fog computing. *IEEE Transactions on Sustainable*

Computing, 6(1):43–53, 2021.
[37] Salvatore Distefano, Giovanni Merlino, and Antonio Puliafito. Enabling the cloud of things. In *Proceedings of the IEEE International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS'12)*, pages 858–863. IEEE, July 2012.
[38] Chunsheng Zhu, Victor Leung, Laurence Yang, and Lei Shu. Collaborative location-based sleep scheduling to integrate wireless sensor networks with mobile cloud computing. In *Proceedings of the IEEE International Workshop on Globecom Workshops (GC Wkshps'13)*, pages 452–457. IEEE, December 2013.
[39] Giancarlo Fortino, Mukaddim Pathan, and Giuseppe Fatta. Bodycloud: integration of cloud computing and body sensor networks. In *Proceedings of the IEEE International Conference on Cloud Computing Technology and Science (CloudCom'12)*, pages 851–856. IEEE, December 2012.
[40] Madoka Yuriyama and Takayuki Kushida. Sensor-cloud infrastructure-physical sensor management with virtualized sensors on cloud computing. In *Proceedings of the IEEE International Conference on 13th Network-Based Information Systems (NBiS'10)*, pages 1–8. IEEE, September 2010.
[41] Mahmoud Abuelela and Stephan Olariu. Taking vanet to the clouds. In *Proceedings of the 8th International Conference on Advances in Mobile Computing and Multimedia (MoMM '10)*, pages 6–13. ACM, November 2010.
[42] Ihsan Ali, Abdullah Gani, Ismail Ahmedy, Ibrar Yaqoob, Suleman Khan, and Mohammad Anisi. Data collection in smart communities using sensor cloud: recent advances and taxonomy and future research directions. *IEEE Communications Magazine*, 56(7):192–197, July 2018.
[43] Loyao Yeh, Peiyuu Chiang, Yilang Tsai, and Jiunlong Huang. Cloud-based fine-grained health information access control framework for lightweight iot devices with dynamic auditing and attribute revocation. *IEEE Transactions on Cloud Computing*, 6(2):532–544, April 2018.
[44] Subarna Chatterjee, Sudip Misra, and Samee U. Khan. Optimal data center scheduling for quality of service management in sensor-cloud. *IEEE Transactions on Cloud Computing*, 7(1):89–101, March 2019.
[45] Tamoghna Ojha, Sudip Misra, Narendra Singh Raghuwanshi, and Hitesh Poddar. Dvsp: dynamic virtual sensor provisioning in sensor–cloud-based internet of things. *IEEE Internet of Things Journal*, 6(3):5265–5272, 2019.
[46] Tian Wang, Yang Li, Weiwei Fang, Wenzheng Xu, Junbin Liang, Yewang Chen, and Xuxun Liu. A comprehensive trustworthy data collection approach in sensor-cloud system. *IEEE Transactions on Big Data*, 2018:1–12, March 2018.
[47] P Sangulagi and A Sutagundar. Agent based load balancing in sensor cloud. In *Proceedings of the 2020 International Conference on Inventive Computation Technologies (ICICT'20)*, pages 342–347. IEEE, 2020.
[48] Chunsheng Zhu, Xiuhua Li, Victor Leung, Xiping Hu, and Laurence Yang. Job scheduling for cloud computing integrated with wireless sensor network. In *Proceedings of the IEEE International Conference on Cloud Computing Technology and Science (CloudCom'14)*, pages 62–69. IEEE, December 2014.
[49] Zomaya Albert, Delicato Flavia, Santos Igor, Khan Samee, and Pirmez Luci. Olympus: the cloud of sensors. *IEEE Cloud Computing*, 2(2):48–56, April 2015.
[50] Mohammad Aazam and Euinam Huh. Fog computing and smart gateway based communication for cloud of things. In *Proceedings of the IEEE International Conference on Future Internet of Things and Cloud (FiCloud'14)*, pages 464–470. IEEE, August 2014.
[51] Adam A Alli and Muhammad Mahbub Alam. The fog cloud of things: A survey on concepts, architecture, standards, tools, and applications. *Internet of Things*, 9:1–20, 2020.
[52] Priyanka Rawat, authorKamal Deep Singh, Hakima Chaouchi, and Jean Marie Bonnin. Wireless sensor networks: A survey on recent developments and potential synergies. *Journal of Supercomputing*, 68(1):1–48, April 2014.
[53] T Vigneswari et al. Smart iot cloud based livestock monitoring system: A survey. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, 12(10):3308–3315, 2021.
[54] Proshikshya Mukherjee, Tanmaya Swain, and Amlan Datta. Issues of some task scheduling strategies on sensor cloud environment. In *Smart Intelligent Computing and Applications*, volume 160, pages 651–663. Springer, 2020.
[55] Kanegonda Ravi Chythanya, KomuravellySudheer Kumar, Mothe Rajesh, and S Tharun Reddy. Sensor cloud: A breakdown information on the utilization of wireless sensor network by means of cloud computing. *Test Eng Manage*, 82:13945–13954, 2020.
[56] Giancarlo Fortino, Daniele Parisi, Vincenzo Pirrone, and Giuseppe Fatta. Bodycloud: A saas approach for community body sensor networks. *Future Generation Computer Systems*, 35:62–79, June 2014.
[57] Kalyani Divi and Hong Liu. Modeling of wban and cloud integration for secure and reliable healthcare. In *Proceedings of the 8th International Conference on Body Area Networks (BodyNets '13)*, pages 128–131. ICST, October 2013.
[58] Jiafu Wan, Caifeng Zou, Sana Ullah, Chinfeng Lai, Ming Zhou, and Xiaofei Wang. Cloud-enabled wireless body area networks for pervasive healthcare. *IEEE Network*, 27(5):56–61, September 2013.
[59] Salim Bitam, Abdelhamid Mellouk, and Sherali Zeadally. Vanet-cloud: a generic cloud computing model for vehicular ad hoc networks. *IEEE Wireless Communications*, 22(1):96–102, February 2015.

[60] Arif Muhammad, Wang Guojun, and Balas Valentina Emilia. Secure vanets: trusted communication scheme between vehicles and infrastructure based on fog computing. *Studies in Informatics and Control*, 27(2):235–246, 2018.

[61] Madria S. Sensor cloud: sensing-as-a-service paradigm. In *Proceedings of the 2018 19th IEEE International Conference on Mobile Data Management (MDM'18)*, pages 13–6. IEEE, 2018.

[62] Peng Xu, Shuanghong He, Wei Wang, Willy Susilo, and Hai Jin. Lightweight searchable public-key encryption for cloud-assisted wireless sensor networks. *IEEE Transactions on Industrial Informatics*, 14(8):3712–3723, August 2018.

[63] R Pereira, C Barros, S Pereira, PM Mendes, and CA Silva. A middleware for managing the heterogeneity of data provining from iot devices in ambient assisted living environments. In *Proceedings of the 2020 IEEE ANDESCON (ANDESCON'20)*, pages 1–6. IEEE, 2020.

[64] Eun Lee, Hariharasudhan Viswanathan, and Dario Pompili. Model-based thermal anomaly detection in cloud datacenters using thermal imaging. *IEEE Transactions on Cloud Computing*, 6(2):330–343, April 2018.

[65] R Bruce Wallace, Frank Horsfall, Rafik Goubran, Ali El-Haraki, and Frank Knoefel. The challenges of connecting smart home health sensors to cloud analytics. In *Proceedings of the 2019 IEEE Sensors Applications Symposium (SAS'19)*, pages 1–5. IEEE, May 2019.

[66] Mohammad Nazmul Alam and Roch H Glitho. An infrastructure as a service for the internet of things. In *Proceedings of the IEEE 7th International Conference on Cloud Networking (CloudNet'18)*, pages 1–7. IEEE, 2018.

[67] Jinfang Jiang, Guangjie Han, Lei Shu, Sammy Chan, and Kun Wang. A trust cloud model for underwater wireless sensor networks. *IEEE Communications Magazine*, 55(3):110–116, March 2017.

[68] Chunsheng Zhu, Xiuhua Li, Victor Leung, Laurence Yang, Edith Ngai, and Lei Shu. Towards pricing for sensor-cloud. *IEEE Transactions on Cloud Computing*, 8(4):1018–1029, 2020.

[69] Sherif Abdelwahab, Bechir Hamdaoui, Mohsen Guizani, and Taieb Znati. Cloud of things for sensing as a service: sensing resource discovery and virtualization. In *Proceedings of the IEEE International Conference on Global Communications (GLOCOM'15)*, pages 1–7. IEEE, December 2015.

[70] Huajun Hong, Chingling Fan, Yenchen Lin, and Chenghsin Hsu. Optimizing cloud-based video crowdsensing. *IEEE Internet of Things Journal*, 3(3):299–313, June 2016.

[71] Jianhua Liu, Jiadi Yu, and Shigen Shen. Energy-efficient two-layer cooperative defense scheme to secure sensor-clouds. *IEEE Transactions on Information Forensics and Security*, 13(2):408–420, February 2018.

[72] Prasenjit Maiti, Jaya Shukla, Bibhudatta Sahoo, and Ashok Turuk. Qos-aware fog nodes placement. In *Proceedings of the IEEE International Conference on Recent Advances in Information Technology (RAIT'18)*, pages 1–6. IEEE, March 2018.

[73] Xu Xiaolong, Zhang Xuyun, gao Honghao, and Xue Yuan. Become: blockchain-enabled computation offloading for iot in mobile edge computing. *IEEE Transactions on Industrial Informatics*, 16(6):4187–4195, 2019.

[74] Shi Ming Huang, David C Yen, Ting Jyun Yan, and Yi Ting Yang. An intelligent mechanism to automatically discover emerging technology trends: Exploring regulatory technology. *ACM Transactions on Management Information Systems (TMIS)*, 13(2):1–29, 2021.

[75] Z Fan, W Yang, and K Tian. An edge computing service model based on information-centric networking. In *Proceedings of the 2019 IEEE 25th International Conference on Parallel and Distributed Systems (ICPADS'19)*, pages 498–505. IEEE, 2019.

[76] Mohammad Hassan, Biao Song, and Euinam Huh. A framework of sensor-cloud integration opportunities and challenges. In *Proceedings of the 3rd international conference on Ubiquitous information management and communication (ICUIMC '09)*, pages 618–626. ACM, January 2009.

[77] Carlo Puliafito, Enzo Mingozzi, Francesco Longo, Antonio Puliafito, and Omer F. Rana. Fog computing for the internet of things: a survey. *ACM Transactions on Internet Technology*, 19(2):1–41, 2019.

[78] Riccardo Venanzi, Burak Kantarci, Luca Foschini, and Paolo Bellavista. Mqtt-driven sustainable node discovery for internet of things-fog environments. In *Proceedings of the IEEE International Conference on Communications (ICC'18)*, pages 1–6. IEEE, May 2018.

[79] Salma Abdalla Hamad, Quan Z Sheng, Wei Emma Zhang, and Surya Nepal. Realizing an internet of secure things: A survey on issues and enabling technologies. *IEEE Communications Surveys & Tutorials*, 22(2):1372–1391, 2020.

[80] Mithun Mukherjee, Lei Shu, and Di Wang. Survey of fog computing: fundamental and network applications and research challenges. *IEEE Communications Surveys & Tutorials*, 20(3):1826–1857, March 2018.

[81] Yazdan Ahmad Qadri, Ali Nauman, Yousaf Bin Zikria, Athanasios V. Vasilakos, and Sung Won Kim. The future of healthcare internet of things: a survey of emerging technologies. *IEEE Communications Surveys and Tutorials*, 22(2):1121–1167, 2020.

[82] C Liu, J Hua, and C Julien. Scents: collaborative sensing in proximity iot networks. In *Proceedings of the 2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops'19)*, pages 189–195. IEEE, 2019.

[83] Mung Chiang and Tao Zhang. Fog and iot: an overview of research opportunities. *IEEE Internet of Things Journal*, 3(6):854–864, December 2016.
[84] Min Chen, Yongfeng Qian, Yixue Hao, Yong Li, and Jeungeun Song. Data-driven computing and caching in 5g networks: architecture and delay analysis. *IEEE Wireless Communications*, 25(1):70–75, 2018.
[85] Amitav Mukherjee. Fog-aided data reception in next-generation mimo radio access networks with edge sensing. In *Proceedings of the IEEE International Conference on Communications (ICC'18)*, pages 1–6. IEEE, May 2018.
[86] Jinkyu Kang, Osvaldo Simeone, Joonhyuk Kang, and Shlomo Shitz. Control-data separation with decemberentralized edge control in fog-assisted uplink communications. *IEEE Transactions on Wireless Communications*, 17(6):3686–3696, June 2018.
[87] A L É Battisti, D C Muchaluat-Saade, and F C Delicato. V-prism: an edge-based iot architecture to virtualize multimedia sensors. In *Proceedings of the 2020 IEEE 6th World Forum on Internet of Things (WF-IoT'20)*, pages 1–6. IEEE, 2020.
[88] Saurav Sthapit, John Thompson, Neil M Robertson, and James R Hopgood. Computational load balancing on the edge in absence of cloud and fog. *IEEE Transactions on Mobile Computing*, 18(7):1499–1512, 2018.
[89] Abebe Diro and Naveen Chilamkurti. Leveraging lstm networks for attack detection in fog-to-things communications. *IEEE Communications Magazine*, 56(9):124–130, September 2018.
[90] Peng Yang, Ning Zhang, Shan Zhang, Kan Yang, Li Yu, and Xuemin Shen. Identifying the most valuable workers in fog-assisted spatial crowdsourcing. *IEEE Internet of Things Journal*, 4(5):1193–1203, October 2017.
[91] Cheol-Ho Hong and Blesson Varghese. Resource management in fog/edge computing: a survey on architectures, infrastructure, and algorithms. *ACM Computing Surveys (CSUR)*, 52(5):1–37, 2019.
[92] Tie Qiu, Jiancheng Chi, Xiaobo Zhou, Zhaolong Ning, and Dapeng Oliver Wu. Edge computing in industrial internet of things: architecture, advances and challenges. *IEEE Communications Surveys and Tutorials*, 22(4):2462–2488, 2020.
[93] Abbas Javed, Hadi Larijani, Ali Ahmadinia, Rohinton Emmanuel, Mike Mannion, and Des Gibson. Design and implementation of a cloud enabled random neural network-based decentralized smart controller with intelligent sensor nodes for hvac. *IEEE Internet of Things*, 4(2):393–403, April 2017.
[94] Stephanie Challita, Fawaz Paraiso, and Philippe Merle. Towards formal-based semantic interoperability in multi-clouds: the fclouds framework. In *Proceedings of the IEEE International Conference on Cloud Computing (CLOUD'17)*, pages 710–713. IEEE, June 2017.
[95] Anh LeTun, Hoan N. Mau Quoc, Martin Serrano, Manfred Hauswirth, John Soldatos, Thanasis Papaioannou, and Karl Aberer. Global sensor modeling and constrained application methods enabling cloud-based open space smart services. In *Proceedings of the IEEE Ubiquitous Intelligence and Computing and 9th International Conference on Autonomic and Trusted Computing (UIC/ATC'12)*, pages 196–203. IEEE, September 2012.
[96] Chunsheng Zhu, Victor Leung, Kun Wang, Laurence Yang, and Yan Zhang. Multi-method data delivery for green sensor-cloud. *IEEE Communications Magazine*, 55(5):176–182, May 2017.
[97] Sevil Ahmed, Andon Topalov, and Nikola Shakev. A robotized wireless sensor network based on mqtt cloud computing. In *Proceedings of the IEEE International Workshop on Electronics and Control and Measurement and Signals and their Application to Mechatronics (ECMSM'17)*, pages 1–6. IEEE, May 2017.
[98] Yi Xu and Abdelsalam Helal. Scalable cloud–sensor architecture for the internet of things. *IEEE Internet of Things Journal*, 3(3):285–298, 2015.
[99] Jiantao Zhou, Yong Xiang, Leoyu Zhang, Fei Chen, Shaoning Pang, and Xiaofeng Liao. Computation outsourcing meets lossy channel: secure sparse robustness decoding service in multi-clouds. *IEEE Transactions on Big Data*, 4:1–10, June 2017.
[100] Antonio Celesti, Maria Fazio, Maurizio Giacobbe, Antonio Puliafito, and Massimo Villari. Characterizing cloud federation in iot. In *Proceedings of the IEEE International Workshops on Advanced Information Networking and Applications Workshops (WAINA'16)*, pages 93–98. IEEE, March 2016.
[101] Massimo Ficco, Christian Esposito, Yang Xiang, and Francesco Palmieri. Pseudo-dynamic testing of realistic edge-fog cloud ecosystems. *IEEE Communications Magazine*, 55(11):98–104, November 2017.
[102] Zhi Li, Xianwei Zhou, Yanzhu Liu, Haitao Xu, and Li Miao. A non-cooperative differential game-based security model in fog computing. *China Communications*, 14(1):180–189, January 2017.
[103] Daewoo Kim, Hyojung Lee, Hyungseok Song, Nakjung Choi, and Yung Yi. On the economics of fog computing: inter-play among infrastructure and service providers and users and edge resource owners. In *Proceedings of the IEEE International Conference on Communications (ICC'18)*, pages 1–6. IEEE, May 2018.
[104] Chi Yang, Deepak Puthal, Saraju Mohanty, and Elias Kougianos. Big-sensing-data curation for the cloud is coming: a promise of scalable cloud-data-center mitigation for next-generation iot and wireless sensor networks. *IEEE Consumer Electronics Magazine*, 6(4):48–56, October 2017.
[105] Arijit Roy, Sudip Misra, and Soumi Nag. Prime: an optimal pricing scheme for mobile sensors-as-a-service. *IEEE Transactions on Mobile Computing*, 2020:1–12, 2020.

[106] Heng Wang, Liuqing Chen, Min Li, and Pengfei Gong. Consensus-based clock synchronization in wireless sensor networks with truncated exponential delays. *IEEE Transactions on Signal Processing*, 68:1425–1438, 2020.

[107] Pengfei Hu, Huansheng Ning, Tie Qiu, Houbing Song, Yanna Wang, and Xuanxia Yao. Security and privacy preservation scheme of face identification and resolution framework using fog computing in internet of things. *IEEE Internet of Things Journal*, 4(5):1143–1155, Oct 2017.

[108] Martin Henze, René Hummen, Roman Matzutt, Daniel Catrein, and Klaus Wehrle. Maintaining user control while storing and processing sensor data in the cloud. *International Journal of Grid and High Performance Computing (IJGHPC)*, 5(4):97–112, Dec 2013.

[109] Martin Henze. The quest for secure and privacy-preserving cloud-based industrial cooperation. In *Proceedings of IEEE Conference on Communications and Network Security (CNS'20)*, pages 1–5. IEEE, 2020.

[110] Kai Yang, Yuanming Shi, and Zhi Ding. Low-rank matrix completion for mobile edge caching in fog-ran via riemannian optimization. In *Proceedings of the IEEE Global Communications Conference (GLOBECOM'17)*, pages 1–6. IEEE, Feb 2017.

[111] Chunsheng Zhu, Victor Leung, Laurence Yang, Lei Shu, Joel Rodrigues, and Xiuhua Li. Trust assistance in sensor-cloud. In *Proceedings of the IEEE International Conference on Computer Communications Workshops (INFOCOM WKSHPS'15)*, pages 342–347. IEEE, Aug 2015.

[112] Liehuang Zhu, Chuan Zhang, Chang Xu, and Kashif Sharif. Rtsense: Providing reliable trust-based crowdsensing services in cvcc. *IEEE Network*, 32(3):20–26, June 2018.

[113] Li Feng, Jie Yang, and Huan Zhang. Rt-notification: A novel real-time notification protocol for wireless control in fog computing. *China Communication*, 14(11):17–28, Dec 2017.

[114] Chiamu Yu, Chiyuan Chen, and Hanchieh Chao. Verifiable and privacy-assured and and accurate signal collection for cloud-assisted wireless sensor networks. *IEEE Communications Magazine*, 53(8):48–53, Aug 2015.

[115] Sajeeb Saha, Md. Ahsan Habib, Tamal Adhikary, Md. Abdur Razzaque, and Md. Mustafizur Rahman. Tradeoff between execution speedup and reliability for compute-intensive code offloading in mobile device cloud. *Multimedia Systems*, 25(5):577–589, 2019.

[116] Stephan Olariu. A survey of vehicular cloud research: trends, applications and challenges. *IEEE Transactions on Intelligent Transportation Systems*, 21(6):2648–2663, 2020.

[117] Xavi Bruin, Eva Tordera, and Ghazal Tashakor. Foggy clouds and cloudy fogs: a real need for coordinated management of fog-to-cloud computing systems. *IEEE Wireless Communications*, 23(5):120–128, October 2016.

[118] Xiaoyu Chen, Lening Wang, and Canran Wang. Predictive offloading in mobile-fog-cloud enabled cyber-manufacturing systems. In *Proceedings of the 2018 IEEE Industrial Cyber-Physical Systems (ICPS'18)*, pages 167–172. IEEE, May 2018.

[119] Luis Neto, Joao Reis, Ricardo Silva, and Gil Goncalves. Sensor selcomp and a smart component for the industrial sensor cloud of the future. In *Proceedings of the IEEE International Conference on Industrial Technology (ICIT'17)*, pages 1256–1261. IEEE, May 2017.

[120] Jianshan Zhou, Daxin Tian, Yunpeng Wang, Zhengguo Sheng, Xuting Duan, and Victor CM Leung. Reliability-optimal cooperative communication and computing in connected vehicle systems. *IEEE Transactions on Mobile Computing*, 19(5):1216–1232, 2019.

[121] Ahmed Salim Alrawahi, Kevin Lee, and Ahmad Lotfi. A multiobjective qos model for trading cloud of things resources. *IEEE Internet of Things Journal*, 6(6):9447–9463, 2019.

[122] Kuljeet Kaur, Sahil Garg, Georges Kaddoum, Syed Hassan Ahmed, Francois Gagnon, and Mohammed Atiquzzaman. Demand-response management using a fleet of electric vehicles: An opportunistic-sdn-based edge-cloud framework for smart grids. *IEEE Network*, 33(5):46–53, 2019.

[123] Mohammad Al-Shayeji, Fahad Ebrahim, et al. A secure and energy-efficient platform for the integration of wireless sensor networks and mobile cloud computing. *Computer Networks*, 165(24):1–13, 2019.

[124] Guangjie Han, Jiaxin Du, Chuan Lin, Hongyi Wu, and Mohsen Guizani. An energy-balanced trust cloud migration scheme for underwater acoustic sensor networks. *IEEE Transactions on Wireless Communications*, 19(3):1636–1649, 2020.

[125] Sherali Zeadally, Faisal Karim Shaikh, Anum Talpur, and Quan Z Sheng. Design architectures for energy harvesting in the internet of things. *Renewable and Sustainable Energy Reviews*, 128:1–22, 2020.

[126] Subarna Chatterjee, Subhadeep Sarkar, and Sudip Misra. Energy-efficient data transmission in sensor-cloud. In *Proceedings of the IEEE International Conference on Applications and Innovations in Mobile Computing (AIMoC'15)*, pages 68–73. IEEE, February 2015.

[127] Shakena Grace and Sumalatha. Sca-an energy efficient transmission in sensor cloud. In *Proceedings of the IEEE International Conference on Recent Trends in Information Technology (ICRTIT'14)*, pages 1–5. IEEE, April 2014.

[128] Dapeng Wu, Boran Yang, Honggang Wang, Dalei Wu, and Ruyan Wang. An energy-efficient data forwarding strategy for heterogeneous wbans. *IEEE Access*, 4:7251–7261, September 2016.

[129] Suman Bhunia, Jayita Pal, and Nandini Mukherjee. Fuzzy assisted event driven data collection from sensor nodes in sensor-cloud infrastructure. In *In Proceedings of the 14th IEEE/ACM International Symposium on Cluster and Cloud and Grid Computing (CCGrid'14)*, pages 635–640. IEEE/ACM, May 2014.
[130] Tian Wang, Yuzhu Liang, Yilin Zhang, Xi Zheng, Muhammad Arif, Jin Wang, and Qun Jin. An intelligent dynamic offloading from cloud to edge for smart iot systems with big data. *IEEE Transactions on Network Science and Engineering*, 7(4):2598–2607, 2020.
[131] Rashmi Dalvi and Sanjay Madria. Energy efficient scheduling of fine-granularity tasks in a sensor cloud. In *Proceedings of the IEEE International Conference on Database Systems for Advanced Applications (DASFAA'15)*, pages 498–513. IEEE, April 2015.
[132] Thanh Dinh and Younghan Kim. Information centric sensor-cloud integration: an efficient model to improve wireless sensor networks lifetime. In *Proceedings of the IEEE International Conference on Communications (ICC'17)*, pages 1–6. IEEE, April 2017.
[133] Zeyuan Yan, Yanyan Tan, Wei Zheng, Lili Meng, and Huaxiang Zhang. Leader recommend operators selection strategy for a multiobjective evolutionary algorithm based on decomposition. *Information Sciences*, 550:166–188, 2021.
[134] Werner Kurschl and Wolfgang Beer. Combining cloud computing and wireless sensor networks. In *Proceedings of the 11th International Conference on Information Integration and Web-based Applications & Services (iiWAS '09)*, pages 512–518. ACM, December 2009.
[135] Chunsheng Zhu, Victor Leung, Laurence Yang, Xiping Hu, and Lei Shu. Collaborative location-based sleep scheduling for wireless sensor networks integrated with mobile cloud computing. *IEEE Transactions on Computers*, 64(7):1844–1856, July 2015.
[136] Navroop Kaur and Sandeep Sood. An energy-efficient architecture for the internet of things (iot). *IEEE Systems Journal*, 11(2):796–805, June 2017.
[137] Zheshi Chen, Chunhong Li, and Wenjun Sun. Bitcoin price prediction using machine learning: An approach to sample dimension engineering. *Journal of Computational and Applied Mathematics*, 365:1–13, 2020.
[138] Antonio Rafael Sabino Parmezan, Vinicius MA Souza, and Gustavo EAPA Batista. Evaluation of statistical and machine learning models for time series prediction: Identifying the state-of-the-art and the best conditions for the use of each model. *Information Sciences*, 484:302–337, 2019.
[139] Myriam Hernández-Álvarez, Edgar A Torres Hernández, Sang Guun Yoo, et al. Stock market data prediction using machine learning techniques. In *Proceedings of the International Conference on Information Technology & Systems (ICITS'19)*, pages 539–547. Springer, 2019.
[140] Chapoulade Elodie, Talon Aurélie, Chateauneuf Alaa, Breul Pierre, Hermand Guillaume, and Leconte Marc. Sensors position optimization for monitoring the convergence of radioactive waste storage tunnel. *Nuclear Engineering and Design*, 367:1–10, 2020.
[141] Subarna Chatterjee and Sudip Misra. Optimal composition of a virtual sensor for efficient virtualization within sensor-cloud. In *Proceedings of the IEEE International Conference on Communications (ICC'15)*, pages 448–453. IEEE, June 2015.
[142] Changsheng You, Kaibin Huang, and Hyukjin Chae. Energy efficient mobile cloud computing powered by wireless energy transfer. *IEEE Journal on Selected Areas in Communications*, 34(5):1757–1771, May 2016.
[143] Jiming Chen, Songyuan Li, Shuo Chen, Shibo He, and Zhiguo Shi. Q-charge: a quadcopter-based wireless charging platform for large-scale sensing applications. *IEEE Network*, 31(6):56–61, November 2017.
[144] Yisheng Zhao, Victor Leung, Chunsheng Zhu, Hui Gao, Zhonghui Chen, and Hong Ji. Energy-efficient sub-carrier and power allocation in cloud-based cellular network with ambient rf energy harvesting. *IEEE Access*, 5:1340–1352, February 2017.
[145] Tian Wang, Yuzhu Liang, Yaxin Mei, Muhammad Arif, and Chunsheng Zhu. High-accuracy localization for indoor group users based on extended kalman filter. *International Journal of Distributed Sensor Networks*, 14(11):1–10, 2018.
[146] Ahmed Latif, Bassem Atty, and Shamim Hossain. Secure quantum steganography protocol for fog cloud internet of things. *IEEE Access*, 6:10332–10340, March 2018.
[147] Maria Fazio and Antonio Puliafito. Cloud4sens: a cloud-based architecture for sensor controlling and monitoring. *IEEE Communications Magazine*, 53(3):41–47, March 2015.
[148] Azadeh Neiat, Athman Bouguettaya, Timos Sellis, and Hai Dong. Spatio-temporal composition of sensor cloud services. In *Proceedings of the IEEE International Conference on Web Services (ICWS'14)*, pages 241–248. IEEE, December 2014.
[149] Mohamed Guezguez, Slim Rekhis, and Noureddine Boudriga. A sensor cloud for the provision of secure and qos-aware healthcare services. *Arabian Journal for Science and Engineering*, 2:1–24, November 2017.
[150] Abbas Javed, Hadi Larijani, Ali Ahmadinia, and Des Gibson. Smart random neural network controller for hvac using cloud computing technology. *IEEE Transactions on Industrial Informatics*, 13(1):351–360, February 2017.

[151] Zhihua Xia, Xinhui Wang, Liangao Zhang, Zhan Qin, Xingming Sun, and Kui Ren. A privacy-preserving and copy-deterrence content-based image retrieval scheme in cloud computing. *IEEE Transactions on Information Forensics and Security*, 11(11):2594–2608, November 2016.

[152] Ismail Butun, Salvatore D. Morgera, and Ravi Sankar. A survey of intrusion detection systems in wireless sensor networks. *IEEE Communications Surveys & Tutorials*, 16(1):266–282, May 2014.

[153] Nam Giang, Rodger Lea, Michael Blackstock, and Victor Leung. Fog at the edge: experiences building an edge computing platform. In *Proceedings of the IEEE International Conference on Edge Computing (EDGE'18)*, pages 9–16. IEEE, July 2018.

[154] Subarna Chatterjee, Ranjana Ladia, and Sudip Misra. Dynamic optimal pricing for heterogeneous service-oriented architecture of sensor-cloud infrastructure. *IEEE Transactions on Services Computing*, 10(2):203–216, March 2017.

[155] Qi Qi, Jianxin Liao, Jingyu Wang, Qi Li, and Yufei Cao. Dynamic resource orchestration for multi-task application in heterogeneous mobile cloud computing. In *Proceedings of the Computer Communications Workshops (INFOCOM WKSHPS'16)*, pages 221–226. IEEE, September 2016.

[156] Peijin Cong, Junlong Zhou, Liying Li, Kun Cao, and Keqin Li. A survey of hierarchical energy optimization for mobile edge computing: a perspective from end devices to the cloud. *Acm Computing Surveys*, 53(2):1–44, 2020.

[157] Ti, Ti, Nguyen, Vu, Nguyen, Ha, Long, Bao, Le, and Robert. Joint data compression and computation offloading in hierarchical fog-cloud systems. *IEEE Transactions on Wireless Communications*, 19(1):293–309, 2020.

[158] Tiansheng Huang, Weiwei Lin, Chennian Xiong, Rui Pan, and Jingxuan Huang. An ant colony optimization-based multiobjective service replicas placement strategy for fog computing. *IEEE Transactions on Cybernetics*, 2020:1–14, 2020.

[159] Jianhua He, Jian Wei, Kai Chen, Zuoyin Tang, Yi Zhou, and Yan Zhang. Multitier fog computing with large-scale iot data analytics for smart cities. *IEEE Internet of Things Journal*, 5(2):677–686, April 2018.

[160] Mohammad Moghaddam and Alberto Garcia. A fog-based internet of energy architecture for transactive energy management systems. *IEEE Internet of Things Journal*, 5(2):1055–1069, April 2018.

[161] Ouns Bouachir, Moayad Aloqaily, Lewis Tesng, and Azzedine Boukerche. Blockchain and fog computing for cyber-physical systems: case of smart industry. *Computer*, 53(9):36–45, 2020.

[162] Zhenyu Zhou, Haijun Liao, Xiaoyan Wang, Shahid Mumtaz, and Jonathan Rodriguez. When vehicular fog computing meets autonomous driving: computational resource management and task offloading. *IEEE Network*, 34(6):1–7, 2020.

[163] Yong Yu, Manho Au, Giuseppe Ateniese, Xinyi Huang, Yuanshun Dai, Willy Susilo, and Geyong Min. Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage. *IEEE Transactions on Information Forensics and Security*, 12(4):767–778, October 2017.

[164] Tian Wang, Jiyuan Zhou, Minzhe Huang, MD Zakirul Alam Bhuiyan, Anfeng Liu, Wenzheng Xu, and Mande Xie. Fog-based storage technology to fight with cyber threat. *Future Generation Computer Systems*, 83:208–218, 2018.

[165] Fei Chen, Fengming Meng, Tao Xiang, Hua Dai, Jianqiang Li, and Jing Qin. Towards usable cloud storage auditing. *IEEE Transactions on Parallel and Distributed Systems*, 31(11):2605–2617, 2020.

[166] Xueqiao Liu, Guomin Yang, Willy Susilo, Joseph Tonien, and Jian Shen. Privacy-preserving multi-keyword searchable encryption for distributed systems. *IEEE Transactions on Parallel and Distributed Systems*, 32(3):561–574, 2021.

[167] Yi Qian. 5g wireless communication networks: challenges in security and privacy. *IEEE Wireless Communications*, 27(4):2–3, 2020.

[168] Jindan Zhang, Rongxing Lu, Baocang Wang, and Xu An Wang. Comment on "privacy-preserving public auditing protocol for regenerating-code-based cloud storage". *IEEE Transactions on Information Forensics and Security*, 16:1288–1289, 2020.

[169] Ferucio Laurentiu Tiplea and Cristian Hristea. Puf protected variables: a solution to rfid security and privacy under corruption with temporary state disclosure. *IEEE Transactions on Information Forensics and Security*, 16:999–1013, 2021.

[170] Wentai Wu, Ligang He, Weiwei Lin, and Rui Mao. Accelerating federated learning over reliability-agnostic clients in mobile edge computing systems. *IEEE Transactions on Parallel and Distributed Systems*, 32(7):1539 – 1551, 2021.

[171] Cuixian Lu, Guolong Feng, Yuxin Zheng, Keke Zhang, Han Tan, Galina Dick, and Jens Wickert. Real-time retrieval of precipitable water vapor from galileo observations by using the mgex network. *IEEE Transactions on Geoscience and Remote Sensing*, 58(7):4743–4753, 2020.

[172] Hanguang Luo, Guangjun Wen, and Jian Su. Lightweight three factor scheme for real-time data access in wireless sensor networks. *Wireless Networks*, 26(2):955–970, 2020.

[173] Kang Liao, Chunyu Lin, Yao Zhao, and Moncef Gabbouj. Dr-gan: automatic radial distortion rectification using conditional gan in real-time. *IEEE Transactions on Circuits and Systems for Video Technology*, 30(3):725–733, 2020.

[174] Tian Wang, Jiandian Zeng, Yongxuan Lai, Yiqiao Cai, Hui Tian, Yonghong Chen, and Baowei Wang. Data collection from wsns to the cloud based on mobile fog elements. *Future Generation Computer Systems*, 105:864–872, 2020.

[175] Iftikhar Ahmad, Samreen Ayaz, Syed Yasser Arafat, Faisal Riaz, and Humaira Jabeen. Qos routing for real time traffic in mobile ad hoc network. In *Proceedings of the 7th International Conference on Ubiquitous Information Management and Communication (ICUIMC'13)*, pages 1–6, 2013.
[176] Dabin Kim and Young-Bae Ko. A novel message broadcasting strategy for reliable content retrieval in multi-hop wireless content centric networks. In *Proceedings of the 9th International Conference on Ubiquitous Information Management and Communication (IMCOM'15)*, pages 1–8, 2015.
[177] Zhangbing Zhou, Deng Zhao, Lu Liu, and Patrick Hung. Energy-aware composition for wireless sensor networks as a service. *Future Generation Computer Systems*, 80:299–310, March 2018.
[178] Wenwen Gong, Lianyong Qi, and Yanwei Xu. Privacy-aware multidimensional mobile service quality prediction and recommendation in distributed fog environment. *Wireless Communications and Mobile Computing*, 4:1–8, April 2018.
[179] Hui Guo, Lan Lan Rui, and Zhi Peng Gao. A zone-based content pre-caching strategy in vehicular edge networks. *Future Generation Computer Systems*, 106:22–33, 2020.
[180] Amelec Viloria, Nelson Alberto Lizardo Zelaya, and Nohora Mercado-Caruzo. Design of a network with wireless sensor applied to data transmission based on ieee 802.15.4 standard. *Procedia Computer Science*, 175:665–670, 2020.
[181] Omar Abdel Wahab, Azzam Mourad, Hadi Otrok, and Tarik Taleb. Federated machine learning: Survey, multi-level classification, desirable criteria and future directions in communication and networking systems. *IEEE Communications Surveys & Tutorials*, 23(2):1342–1397, 2021.
[182] Jinfang Jiang, Guangjie Han, Lei Shu, Sammy Chan, and Kun Wang. A trust model based on cloud theory in underwater acoustic sensor networks. *IEEE Transactions on Industrial Informatics*, 13(1):342–350, December 2017.
[183] Tian Wang, Guangxue Zhang, Md Zakirul Alam Bhuiyan, Anfeng Liu, Weijia Jia, and Mande Xie. A novel trust mechanism based on fog computing in sensor–cloud system. *Future Generation Computer Systems*, 109:573–582, 2020.
[184] David Airehrour, Jairo A Gutierrez, and Sayan Kumar Ray. Sectrust-rpl: A secure trust-aware rpl routing protocol for internet of things. *Future Generation Computer Systems*, 93:860–876, 2019.
[185] Qussai Yaseen, Firas AlBalas, Yaser Jararweh, and Mahmoud Ayyoub. A fog computing based system for selective forwarding detection in mobile wireless sensor networks. In *Proceedings of the IEEE International Workshops on Foundations and Applications of Self Systems (FAS-W'16)*, pages 256–262. IEEE, September 2016.
[186] Sarder Fakhrul Abedin, Md. Golam Rabiul Alam, S. M. Ahsan Kazmi, Nguyen H Tran, Dusit Niyato, and Choong Seon Hong. Resource allocation for ultra-reliable and enhanced mobile broadband iot applications in fog network. *IEEE Transactions on Communications*, 67(1):489–502, 2019.
[187] Xi Zheng, Lei Pan, and Erdem Yilmaz. Security analysis of modern mission critical android mobile applications. In *Proceedings of the Australasian Computer Science Week Multiconference (MOBILESoft'14)*, pages 1–9. ACM, January 2017.
[188] Sancheng Peng, Guojun Wang, Yongmei Zhou, Cong Wan, Cong Wang, Shui Yu, and Jianwei Niu. An immunization framework for social networks through big data based influence modeling. *IEEE Transactions on Dependable and Secure Computing*, 16(6):984–995, 2019.
[189] Harish Radhappa, Lei Pan, James Xi Zheng, and Sheng Wen. Practical overview of security issues in wireless sensor network applications. *International journal of computers and applications*, 40(4):202–213, 2018.