IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 31 January 2024, accepted 12 February 2024, date of publication 19 February 2024, date of current version 28 February 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3367118

RESEARCH ARTICLE

A Survey on Integrating Edge Computing With AI and Blockchain in Maritime Domain, Aerial Systems, IoT, and Industry 4.0

AMAD ALNAHDI[1] **AND LÁSZLÓ TOKA**[1,2,3], **(Member, IEEE)**
[1]Faculty of Electrical Engineering and Informatics, Budapest University of Technology and Economics, 1111 Budapest, Hungary
[2]HUN-REN-BME Cloud Applications Research Group, 1245 Budapest, Hungary
[3]AITIA, 1039 Budapest, Hungary

Corresponding author: Amad Alnahdi (aalnahdi@edu.bme.hu)

This work was supported in part by the Ministry of Innovation and Technology of Hungary from the National Research, Development and Innovation Fund through the ANN_20 Funding Scheme under Grant 135606, through the FK_20 Funding Scheme under Grant 135074, through the 2019-2.1.13-TÉT_IN Funding Scheme under Grant 2019-2.1.13-TÉT_IN-2020-00021, and through the 2021-1.2.4-TÉT Funding Scheme under Grant 2021-1.2.4-TÉT-2021-00058; in part by the New National Excellence Program of the Ministry for Culture and Innovation from the Source of the National Research, Development and Innovation Fund under Grant ÚNKP-23-5-BME-436; and in part by the Hungarian National Research, Development and Innovation Office, under Grant 2020-1.2.3-EUREKA-2021-000006. The work of László Toka was supported by the János Bolyai Research Scholarship of the Hungarian Academy of Sciences.

ABSTRACT In terms of digital transformation, organizations today are aware of the critical role that data and information play in their expansion and development in light of the Internet of Things. To increase network performance and stability, many applications are moving from cloud computing to edge computing (EC). However, in order to satisfy customers, applications like intelligent transportation systems, smart grids, smart cities, and healthcare call for even more effective services. This survey addresses extensive research on two aspects: firstly, we present the advancements of two application domains namely maritime areas and aerial systems in terms of integration with EC architecture. Secondly, we cover the most recent technologies, artificial intelligence (AI) and blockchain, combined into the EC paradigm by discussing several experiments conducted in various fields to demonstrate the value of utilizing them in the edge computing architecture. We analyze the results of eleven experiments in each technology from 2015 to 2023.

INDEX TERMS Edge computing, maritime domain, aerial systems, IoT, Industry 4.0, artificial intelligence, blockchain.

I. INTRODUCTION

The integration of edge computing (EC) with the most recent digital technologies, such as artificial intelligence (AI), machine learning (ML), data analytics, big data, immersive interaction technology, decentralized network ecological technology [1], and blockchain has become necessary due to the rapidly growing number of Internet of Things (IoT) devices and the massive amount of data they generate in order to improve network performance. This combination is thought to be a crucial part of the ongoing IoT revolution domain [2]. For instance, integrating AI into EC systems enables the real-time, lowest latency collection, archival, and processing of data from IoT devices, facilitating the best possible data analytics and decision-making. In fact, there is a mutually beneficial relationship between AI and EC, as AI offers EC technologies and methods to improve its performance, while EC enables its potential and scalability with the help of AI [3]. Additionally, EC provides AI with platforms and scenarios to enhance its applicability, leading to a symbiotic relationship between the two technologies. Furthermore, the combination of AI, cloud computing (CC) services and IoT is anticipated to bring about several benefits, including the emergence of advanced AI applications with greater capabilities, enhancements in quality of service (QoS), increased resource utilization, and reduced operational costs [4], [5].

Moreover, an intelligent EC system can address mobility, security, and reliability challenges while reducing bandwidth consumption and improving response time. The integration

The associate editor coordinating the review of this manuscript and approving it for publication was Mehdi Sookhak.

of EC with AI and blockchain technologies has led to the creation of innovative solutions, enabling businesses to take advantage of faster response times and lower latency. The use of AI in EC has allowed for the creation of smart devices capable of learning and adapting to new situations. As an example, Google has initiated a project for self-driving cars that utilize AI [6]. To precisely detect objects and forecast behavior, they make use of pictures, radar beams, lidar, ultrasound, GPS navigation, and central computers. The number of smart vehicles within the internet of vehicles (IoV) will rise dramatically as a result in the upcoming years. Hence, there is a need for careful consideration to efficiently manage the IoV infrastructure [7].

On the other hand, the use of blockchain technology has sparked the creation of secure, decentralized, and dependable data processing and storage platforms. The decentralized data management architecture known as the blockchain, which powers the well-known digital currency Bitcoin, has emerged as having great promise. The use of blockchain in mobile services is still sparse, despite the fact that it has been extensively employed in a variety of applications, including finance, healthcare, and logistics. This is so that blockchain users can add fresh data (a block) to the chain by resolving specified proof-of-work problems [8], [9]. In the context of aerial systems, EC is being used to process data closer to the source, reducing bandwidth requirements and increasing data transmission efficiency. Similarly, in maritime applications, EC is being used to reduce latency and improve data processing for real-time decision-making. Notable that data scarcity is a predominant issue for edge devices, for which transfer learning is a commonly recommended solution [10]. Overall, integrating EC, AI, and blockchain technologies has led to significant advancements in various industries, providing faster and more efficient services while improving security and privacy [11].

Our structured taxonomy is shown in Figure 1. We display our taxonomy under the name of the primary field in this survey which is EC, and from that, we present two branches of investigation, namely applications domains and features. We split up the features branch into two parts which are security, QoS and cost: blockchain is listed under the security part, and AI is listed under the QoS and cost. Finally, we present the most recent applications that are utilizing the EC paradigm, nevertheless, we just address four of them which are the maritime domain, aerial system, IoT, and Industry 4.0. As a future direction, we can address the remaining domains that are mentioned in our taxonomy namely, augmented reality (AR), virtual reality (VR), extended reality (XR), and telecommunications domain.

The rest of this paper is structured as follows. Section II introduces the background of EC. Section III introduces the methodology we used to collect the surveyed papers in this work and our contribution in comparison to related surveys. Section IV introduces the specification of the features of EC. Section V presents the recent application domains in EC. Section VI addresses AI and blockchain techniques deployed and applied in EC. Section VII displays the future directions. Finally, Section VIII concludes the work.

II. THE EDGE COMPUTING PARADIGM

Nowadays, using cloud computing (CC) to centrally consolidate computer tasks, storage, and network administration is typical. The usual practice in modern circumstances is the cloud computing-based centralization of network administration, storage, and computing duties. In particular, this method helps to optimize network performance in areas such as automotive networks by facilitating the provision of compute and storage resources. In this perspective, the addition of privacy-preserving reputation updating (PPRU) to CC serves as an example and enhances the overall efficiency of the network [12]. In terms of the preformance of networks, federated learning is a technique that shows promise for performing model training in Digital Twin for Mobile Networks (DTMN) virtual twins. It is always expected that the users participating in federated learning will exhibit trustworthy behaviors to enhance the model's reliability. Yet, the existing federated learning trust evaluation techniques suffer from the issues of taking into account the simplex evaluation factor and employing a coarse-grained trust computation method [13].

However, architectures solely based on a centralized cloud must contend with some difficulties as they are unable to meet the requirements of the current IoT paradigm and mobile Internet applications, and they are incapable of handling the enormous amount of data produced by these applications. This is due to the explosive growth of IoT devices and the massive data they generate at the network's edge. The issue becomes more obvious and serious as a growing number of smart devices and things are incorporated into daily life, as is the case with smart cities or the IoT. The low latency, location awareness, and mobility assistance needs cannot be met by the present CC paradigm [14].

This is due to limitations in bandwidth and constrained resources in the CC architecture. The limitations of CC have opened the door to the emergence of EC, a technology that is expected to handle the requirements of the continuously expanding IoT and mobile devices [15]. It's worth emphasizing that EC does not seek to replace CC; rather, it aims to supplement it [16]. There is no doubt that EC has recently garnered significant attention in various fields, particularly in academia and industry. By exploiting the services and resources offered by EC, it varies from traditional CC and is seen as a significant enabler for a number of promising technologies, including 6G, IoT, augmented reality, and smart cities. Additionally, the EC method allows for the processing of computationally demanding activities on IoT devices with limited resources that are unable to carry them out locally [17], [18]. Moreover, EC provides an alternative mechanism for processing and filtering large data sets at the network's edge before transferring them to the cloud. As a result, the ability to store and process data near the network's

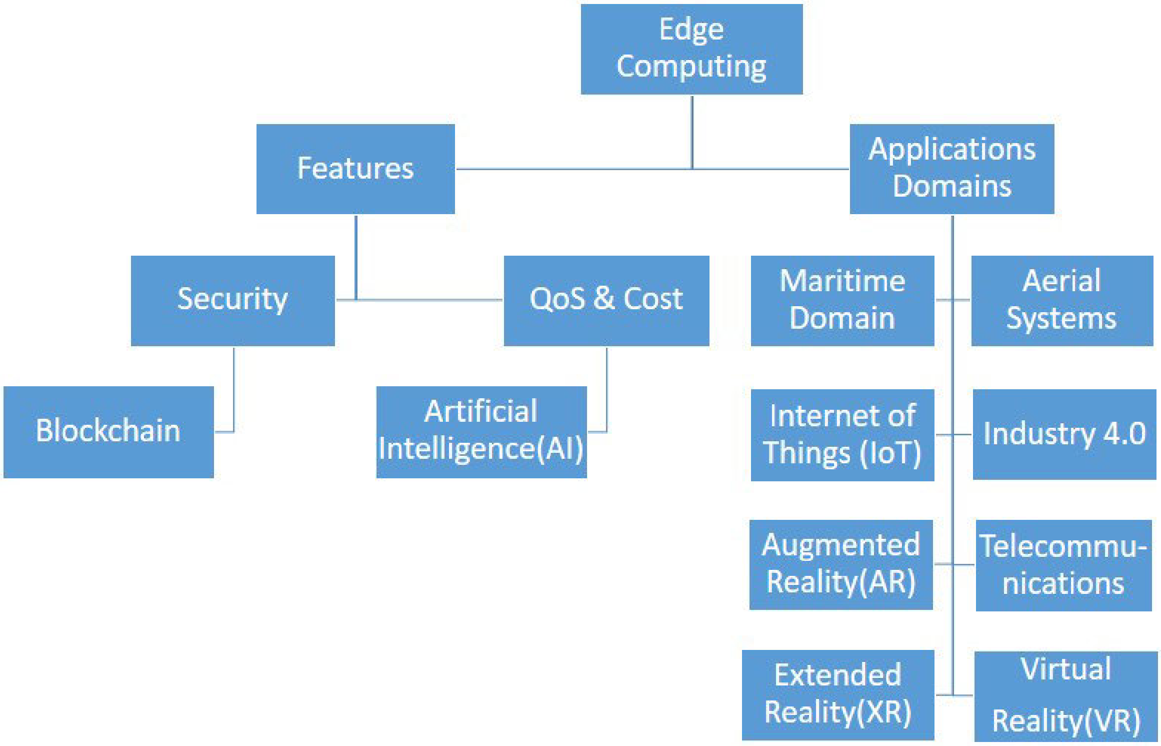

FIGURE 1. Our proposed taxonomy.

edge makes this mechanism advantageous in that it lowers bandwidth costs, storage needs, and energy usage [19], [20].

To put it another way, the core idea of EC is to shift computational data, applications, and services from the CC model to the network's edge, as seen in Fig. 2. This will bring services closer to users and shorten the time it takes for data to be processed. Since some operations that don't require the capacity of cloud servers can be handled directly by edge nodes. On the other hand, in order to relieve the bandwidth demand on the cloud server, the EC mechanism can preprocess the tasks and data that must be delivered. Additionally, by reducing the likelihood that user data will be sent on the core network, EC can improve the security and control of sensitive data as well as user privacy. This is achieved by putting encryption and anonymization systems in place at the edge [21]. Extremely low latency, large bandwidth, and real-time access to network information that can be used by numerous applications characterize the EC approach. Additionally, EC offers services and runs calculations at the network's edge to provide dependable services that satisfy industry demands for real-time data optimization, security, and privacy as well as for extremely low latency and high network bandwidth [22], [23], [24], [25].

By establishing a virtualization platform, extending the corporate service base, and providing network congestion management protocols, EC's central tenet is to improve network efficiency. By locating its computer and storage resources closer to its clients, EC dramatically decreases processing hold-ups. On the one hand, edge nodes have the ability to do some tasks independently of cloud servers. To ease the burden on the cloud server's bandwidth, these nodes can process the data and tasks that must be transferred to it. By reducing the possibility that user data will be sent over the core network and applying encryption and anonymization methods locally, EC can simultaneously

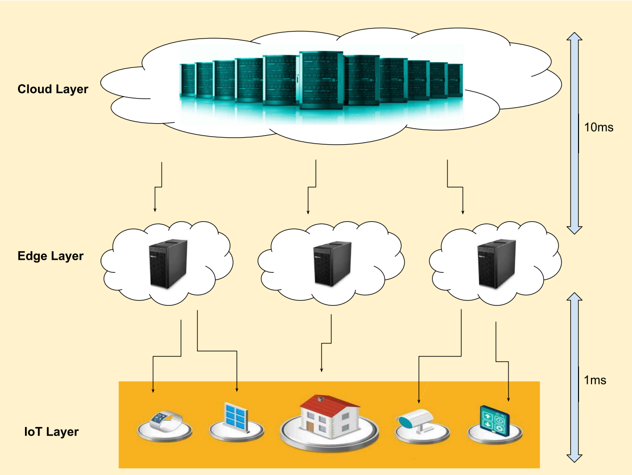

FIGURE 2. Edge computing architecture.

secure sensitive data and uphold user privacy. The aforementioned advantages have fueled the recent explosive rise of EC [21].

On the other hand, terms such as fog computing (FC) and mobile edge computing (MEC) which are related concepts have developed in recent years. The current server- and mobile-based methods either increase latency or decrease inference accuracy. Notable that deep neural networks (DNNs) are widely adopted for mobile systems, thus by dividing the (DNNs) at the right layer and operating the two components independently on the mobile and server, respectively, a hybrid solution can instead include the best features of both approaches [26], [27]. Furthermore, in order to provide delay-sensitive and context-aware apps, a CC platform is being extended to mobile base stations adjacent to mobile users in MEC, a developing architecture. Moreover, MCC is an architecture that permits users of mobile devices to outsource data processing and storage to the cloud. It was primarily developed to address applications that require intensive computing and strict latency constraints [28], [29]. On the other hand, most of the heterogeneous and decentralized fog nodes are considered to be capable of interacting and cooperating in the mechanism of fog computing to carry out data processing and storage activities without dependency on external parties. As FC can also offer improved Quality of Service (QoS) concerning energy consumption, delay, and reduced data traffic over the internet [30].

These concepts are all put out to extend the possibilities of cloud servers [31]. On the other hand, secure data processing is yet another urgent problem that a topic that EC will tackle. Typically, EC servers are used to host sensitive user data in ciphertext format. The largest obstacle in this situation is conducting a secure data search, which requires the user to find a solution for conducting a keyword search over encrypted data files. Researchers have worked to present a number of searchable encryption techniques that enable secure keyword searches over encrypted material without requiring decryption [20].

In addition to the above, there is a promising paradigm named Edge Intelligence (EI) which is a combination of EC and AI technology. The integration of AI and EC is a natural fit because there is a significant overlap between the two. The main goal of EC is to coordinate several concurrent servers and edge devices to handle the created data nearby, whereas the goal of AI is to replicate human intelligence in machines and devices by taking instructions from the data. Additionally, edge intelligence is a cutting-edge strategy that uses the potential of network edges to offer services in real-time. The advantage of fusing the AI paradigm with EC is that the servers at the intelligent edge can obtain a thorough understanding of the working surroundings, including the resource correlation between heterogeneous kinds and the viability of collaboration with neighboring nodes. Furthermore, because the services in EC frequently employ local resources to estimate the environment, edge resource scheduling does not require the full data network to be obtained from the centralized cloud. Instead of relying on resource allocation rules from far-off central AI nodes, it is more dependable to impart locally gained information to distributed AI processing entities [32], [33], [34].

III. OUR SURVEY METHODOLOGY AND CONTRIBUTIONS

In this survey, we adopt a systematic strategy to compile pertinent scholarly literature and research findings for this in-depth survey on the integration of EC with AI and Blockchain in the fields of aerial systems, maritime, IoT, and Industry 4.0. Our primary data source for this survey is "Google Scholar", a widely known and accessible academic search engine. We construct search queries that encompass the various facets of our research topic, ensuring they are tailored to each specific domain: maritime domain, aerial systems, IoT, and Industry 4.0. The search queries include terms related to "edge computing" which is the main field, "maritime domain", and "aerial system" as we discuss these two domains based on impact and timeliness, also we use queries of "Artificial Intelligence" and "Blockchain Technology" which are the techniques that are integrated into edge computing, and specific keywords related to each domain. As an example of the queries used to identify pertinent academic publications: edge computing into / in / with maritime, edge computing with / into aerial systems, blockchain into / with / in aerial systems, and AI technique with / into edge computing.

In addition, the search results were thoroughly examined, evaluated each publication's applicability to our research question, and retrieved pertinent data, such as significant findings, technologies, and contributions. The selected papers were then divided into groups according to their applicability to the maritime domain, aerial systems, IoT, and Industry 4.0. Furthermore, we define strict inclusion criteria for the literature found using Google Scholar in order to protect the integrity of our survey. To ensure relevance and timeliness, we only evaluate research that was published between 2015 and 2023. We also collect publications, and conference papers, that provide information on how EC, AI, and blockchain are being integrated into the aforementioned domains. We execute these queries individually and in combination with pertinent terms to get a huge selection of academic papers from journals, and conferences. To ensure the comprehensiveness of our survey, we also utilize advanced search options provided by Google Scholar, such as filtering results by publication year and relevance. Also, to validate the reliability and accuracy of the information gathered by Google Scholar, key findings and conclusions across multiple publications were undertaken. As a result, this approach ensures that our survey builds on a solid foundation of academic research.

Based on extensive research and diligent exploration that we have done to complete this work, this survey is the first one to address two aspects of the integrated EC architecture. Firstly, based on the recency, we present the advancements of two application domains namely aerial systems and maritime areas in terms of integration with EC architecture. Secondly, we cover the most recent technologies blockchain and AI that are combined into the EC paradigm by discussing several experiments conducted in various fields to demonstrate the value of using EC architecture. As we analyze the results of eleven experiments in each technology from 2015 to 2023 in order to present the benefits of utilizing EC architecture. In contrast, all prior research has been conducted differently, because all of these researches either focused on one technique or one use case with EC or applied those two techniques in different fields.

As a common pattern, a set of previous surveys summarize the application of AI within and for EC frameworks. Reference [35] Introduced the EC paradigm using the AI technique. Reference [36] Presented the use of AI and Blockchain for the sixth generation (6G) wireless communications. Reference [37] Introduced a survey on the Convergence of EC and AI for UAVs. Reference [38] Presented the use of AI in the EC paradigm. Also, [39] has overviewed the concept of integrating AI approaches and blockchain techniques for privacy-preservation, and summarized their combination along with derived privacy protection technologies. Moreover, [8] introduced the integration of blockchain technique into EC. Reference [40] Presented the combining EC and AI into the maritime domain. Also, [41] presented the combining of AI technology into EC. Reference [42] Presented the use of deep learning which is part of the AI domain utilizing the EC paradigm. Reference [43] Presented the use of EC techniques and AI with aerial systems. Also [44] presented the integration of blockchain technology into EC.

As Table 1 demonstrates, no prior survey has addressed the domains we mentioned concerning EC architecture; in contrast, our survey provides thorough work on recent developments related to two application domains namely maritime domain and aerial systems that are integrated into EC architecture. Furthermore, our survey covers the most recent technologies blockchain and AI that are combined in the EC paradigm by discussing several experiments conducted in various sectors to demonstrate the value of utilizing EC architecture.

IV. THE SPECIFICATIONS OF EDGE COMPUTING

There is no doubt that there is a similarity between CC and EC in terms of the mode and technique of processing. However, EC offers specific advantages that are included in its paradigm list, which distinguish its computing mode namely:

A. MOBILITY SUPPORT

The key to supporting mobility in EC mode is through the use of the locator ID separation protocol (LISP). In light of the increasing use of smart devices, LISP enables direct communication with the mobility of smart devices. The LISP concept entails developing a distributed directory system and divorcing the broadcast location identification from the host identity [23].

B. DENSE GEOGRAPHICAL DISTRIBUTION

The idea of EC is to deliver the service to the end user closer than CC by providing additional computer resources located at the network's edge. Therefore, the extension of geographical distribution in the environment can support certain ways as follows:

1- The network administrators can facilitate the matter of location-based mobility service without going over the entire WAS.

2- The performance of big data analytics can be quick and more accurate.

3- A large scale of real-time analytics.

C. LOCATION AWARENESS

Mobile users have network flexibility because of the location awareness of EC that allows them to access services from the closest edge server. Users are able to locate electronic devices using technologies such as GPS and cell phone infrastructure. Therefore, location awareness can be used by a range of EC applications, for instance, edge-based disaster management and fog-based vehicle safety systems.

D. LATENCY REDUCTION

EC mode involves placing services and computational resources in closer proximity to end-users. The architecture of EC is designed to minimize network latency, which is one of its primary benefits. Consequently, many applications are transitioning from cloud-based models to edge-based models to achieve low latency. This enables users to perform resource-intensive tasks with minimal delay and reduces the sensitivity of applications to resource-rich edge devices [23], [45].

E. JITTER REDUCTION

The objective of transitioning from CC models to EC models is to achieve better performance efficiency. Nevertheless, excessive jitter can adversely affect network performance, particularly in real-time applications. Hence, implementing edge-based techniques can decrease the amount of jitter as they circumvent transmitting data over the WAN network [45].

F. SECURITY AND PRIVACY

By opting for EC over CC, the level of privacy can be enhanced while the security can be compromised. The reasons for this are as follows:

1- The architecture of the CC model provides stronger physical and cyber security measures through the deployment of centralized and robust security mechanisms.

2- EC technology allows for the elimination of third-party data access because users are responsible for the storage of their own data.

TABLE 1. Our contribution in comparison to the related surveys.

References	Edge Computing	Maritime Domain	Aerial Domain	Artificial Intelligence	Blockchain
[31]	√	-	-	√	-
[20]	-	-	-	√	√
[32]	√	-	√	√	-
[33]	√	-	-	√	-
[34]	-	-	-	√	√
[35]	√	-	-	-	√
[36]	√	√	-	-	√
[37]	√	-	-	√	-
[38]	√	-	-	√	-
[39]	√	-	√	√	-
[8]	√	-	-	-	√
[Our survey]	√	√	√	√	√

The concept of an edge-based paradigm necessitates a design that incorporates flexible and lightweight security mechanisms, enabling rapid recovery from failures and attacks in a timely manner [45]. However, it is necessary to take into account the issues of privacy and security. For example, data collected by sensors deployed within a home can be accessed, potentially compromising the privacy and security of a family's daily activities. As a result, the development of EC poses critical challenges concerning data security and privacy [46].

G. PROXIMITY

The computation resources and services in the EC paradigm are supposed to be available in the proximity of the users so that the users can get a better experiment. The main benefit of having the availability of computational resources and services in the nearby area allows the end users to leverage the given information to make offloading decisions as well as usage decisions. Additionally, the service provider can take advantage of the mobility of user data by debriefing information from devices and analyzing user attitudes so that the services and resource allocation can be improved [23].

V. EMERGING APPLICATION DOMAINS IN EDGE COMPUTING

A. MARITIME INDUSTRY

The marine network (MN) is a type of broadcasting that permits multi-hop wireless connection and provides computing service when at sea. By processing a significant amount of marine cognitive data, MNs can collect worldwide oceanic observations and support and assist applications that demand low latency. Recently, the use of unmanned aerial vehicles (UAVs) in marine systems has gained international attention, and missions are in constant demand [47]. On the other hand, the emergence of IoT and CC has brought significant modifications to how we use data for the time being. However, these modifications have not yet substantially impacted the practices of condition controlling in the shipping industry, partially due to the high cost of continuous data transmission. Although many ships currently have a network of sensors on board, the continuous controlling of data is frequently not used, and land visibility is constrained.

On the other hand, it is unexpected that utilizing CC via satellite relays in the 5G or upcoming 6G network of MNs will satisfy the latency requirements of the applications of maritime, for example, the navigation of unmanned vessels or unmanned underwater vehicles (UUV), collaborative scheduling of emergency disaster rescues, maritime real-time tracking and positioning, and low-latency maritime communications, as the demand for maritime ultra-reliable low latency communications (M-URLLC) continues to increase. This is due to the fact that transitory satellite systems in MNs are frequently overwhelmed by the processing of maritime big data, which results in the limited availability of low-latency maritime applications, especially in rough weather [48]. Additionally, the demand for computation-intensive applications is rising as a result of the maritime industry's rapid expansion. Thus, MEC is being viewed as a successful solution to provide powerful computing capabilities for maritime terminals that may face resource scarcity or require low latency in order to meet the growing demand for wireless communications in the environments of maritime [49], It is noteworthy that the maritime industry is regarded as a significant area where IoT applications and EC solutions find great use [50].

Although EC introduces a potential solution to these problems, it is still challenging to maintain the accuracy levels needed for predictive maintenance. Additionally, maritime applications are computer programs created to enhance overall efficiency in the shipping domain and improve vessel operations. practically, the EC paradigm is a distributed computing paradigm that minimizes latency and boosts performance by moving computational processes and data storage closer to the devices and sensors that produce them. By combining these two technologies, maritime applications using EC can provide real-time vessel tracking, monitoring, and decision-making capabilities that can greatly enhance the safety, security, and profitability of maritime operations. Also with the EC technique, maritime applications are capable of processing and analyzing data in real-time, allowing operators to quickly identify and respond to critical events such as weather changes, security threats, or equipment failures. This can help to reduce downtime, improve fuel efficiency, and increase overall operational efficiency. Applying EC also enables maritime applications to operate in low-bandwidth or disconnected environments, which is essential for remote and offshore operations. Examples of maritime applications using EC include predictive maintenance systems, real-time cargo tracking, and intelligent navigation systems. These applications are transforming the way the maritime industry operates and helping to facilitate a new era of digitalization and automation [51]. Indeed, the companionship of IoT and EC in the maritime domain has brought numerous benefits, but it has also attracted the attention of cyber attackers. As the maritime domain has been attacked by several cyber-attacks in recent years, causing significant operational disruptions and financial losses. Therefore, it is critical to ensure the security of the data transmitted over the network, as EC can help mitigate this risk by enabling the real-time analysis of data on local devices rather than sending it to the servers that are in the center of the cloud, reducing the attack surface. However, ensuring the accuracy and reliability of these real-time analyses while minimizing latency and power consumption remains a significant challenge for maritime applications [52].

1) MARITIME DOMAIN PREDICTIONS

In the maritime domain, some predictions can be applied shortly:

- **Autonomous Shipping**: Improvements in autonomous shipping are likely going to come from a greater combination of edge computing and AI. The creation and utilization of autonomous vessels is one of the predictions for increased effectiveness and security.

- **Smart Ports**: Blockchain technology is used in order to secure data transfers, and edge computing is used for processing port activities in real-time. The marine sector might witness a broad adoption of these technologies.

- **Environmental Monitoring**: The utilization of integrated techniques has the potential to significantly improve environmental monitoring in the environments of the maritime sector. Edge computing architecture and AI techniques can be applied to analyze data about pollution, climate change, and marine life.

B. AERIAL SYSTEMS

Drones or unmanned aerial vehicles (UAVs) are aircraft that are flown remotely from the ground or by an onboard computer [37]. These UAVs are gaining more popularity for a range of industries and tasks, starting from package delivery to agricultural monitoring to search and rescue operations, as well as the military domain, business, and public sectors [53]. The market for UAVs was valued at $18 billion in 2017 and is expected to reach $ 52 billion by 2025 [54]. These systems produce enormous volumes of data, including video feeds, sensor readings, and position data, which must be processed and reviewed in real-time to enable effective decision-making. With EC technology, network speed is improved and latency is reduced by managing computation and data storage closer to the gadgets and sensors that generate them. By combining EC with aerial systems, organizations can process and analyze data on-board the drone or UAV, rather than sending it back to a centralized server for analysis. This enables real-time decision-making, faster response times, and improved efficiency.

EC can be applied in various industries and applications, and aerial systems are one of the many tools that can benefit from this technology. For instance, in agriculture, a drone equipped with sensors and cameras can fly over fields and use EC to analyze crop health, detect pests or diseases, and optimize fertilizer application rates. This enables farmers to make real-time decisions and respond to improve crop yields and minimize the use of resources. Similarly, in environmental monitoring, drones can collect data on air quality, water quality, and wildlife populations and use EC to process and analyze the data in real-time, providing valuable insights for researchers and conservationists. In infrastructure inspection, drones can be used to inspect bridges, pipelines, and buildings, detecting defects and potential issues before they become major problems. Finally, in disaster response, drones equipped with sensors and cameras can be used to quickly assess the damage and provide quick attention and care to emergency cases, enabling faster and more effective response times.

In addition to that, the integration of EC with aerial systems has the potential to operate in areas that have low bandwidth or no connectivity, which is critical for remote or hard-to-reach regions. EC enables the processing of data on the drone or UAV, thereby reducing the necessity for high-bandwidth communication links, and prolonging the operational period of aerial systems without the need for constant recharging or refueling. This combination of technologies is transforming the methods of data collection and analysis, and offering novel opportunities for advancement and development.it is notable that unmanned aerial vehicle (UAV) integration into MEC networks has recently attracted greater interest and become more widely used.

Compared to traditional terrestrial MEC networks, the technology of MEC integrating into UAV support offers a variety of advantages. For example, UAVs can do computation-related tasks as users, relays can offload computation-related activities, and MEC servers can conduct computation-related tasks. Even in challenging terrain where terrestrial MEC networks are impracticable, UAVs can be employed in a variety of applications [55], [56]. The performance of the computation part can be improved with short-range line-of-sight communications, and it can be further enhanced by optimizing the trajectory of the UAV. In addition, UAV-enabled MEC networks may be useful when natural disasters have harmed terrestrial MEC systems. Major corporations including Google, Facebook, Amazon, and Huawei have started initiatives to promote MEC networks with UAV support. As the price of UAVs drops, it is expected that UAV-enabled MEC networks will spread more widely [56], [57].

Since the random radio environment cannot be controlled, it is not taken into account by the existing method of aerial MEC optimization. However, it has been demonstrated that the unique concept of reconfigurable intelligent surfaces (RIS) can produce a smart radio environment. To change the phases and angles at which incident signals are reflected by RIS, which can boost the received signal power.

The communications of RIS-assisted UAV and aerial MEC can be used to overcome ground obstacles that may prohibit air-ground connection in realistic contexts like metropolitan regions. RIS can be used to reflect signals between the base station and customers by being broadcast from the top of buildings or installed on a UAV. However, the continually moving UAVs pose a challenge to the passive beamforming effectiveness of RIS. This is addressed in [58], which proposes a joint UAV trajectory and RIS passive beam-forming optimization to maximize the data transmission rate. In a recent study, a rotary-wing UAV was used as an MEC server, and an RIS was installed on the building's exterior to create a user-UAV interface during job offloading. To minimize the UAV's power consumption while still meeting task QoS requirements, joint improvements to the UAV trajectory, task offloading, cache, and phase-shift architecture of the RIS were made. Based on the results of the simulation, RIS passive phase-shift can elaborate the transmission environment while reducing the UAV's power requirements. The potential of RIS-assisted aerial MEC hasn't received much study, though, and more work is required to be totally understandable [59].

Many emerging applications and workable scenarios cannot be implemented on the existing computer systems, such as EC, and the reason behind that is their limitations. A comprehensive computing paradigm has been proposed to overcome these limitations, but there is a hole in the literature due to the lack of studies. To address this hole, [60] proposes a new concept called aerial computing, which combines aerial radio access networks and EC. A new comprehensive computing architecture is introduced, consisting of satellite computing platforms low-altitude computing (LAC), and high-altitude computing (HAC), in addition to conventional computing systems. The system of aerial computing provides several advantages, including comprehensive computing service, enhanced mobility, simultaneity, higher scalability, and availability. Along with vertical domain applications like smart cities, smart vehicles, smart factories, and smart grids, primary technologies that facilitate aerial computing, for example, EC, energy refilling, network softwarization, frequency spectrum, multiaccess techniques, AI, and big data, are thoroughly discussed. As mentioned above, UAV-enabled MEC systems have many benefits, but they also encounter various difficulties, these challenges include short battery life, excessive energy usage, unequal job offloading and resource allocation, delay requirements, and security concerns [61].

1) AERIAL DOMAIN PREDICTIONS

In the aerial domain, some predictions can be applied shortly:

- **Integration of Drones**: The integrated Drone for a variety of purposes is anticipated to grow in the aerial realm. AI and edge computing provide real-time data processing in a variety of use cases, including emergency response, agriculture, delivery services, and the surveillance sector.

- **Air Traffic Management**: Forecasts for air traffic control indicate that cutting-edge systems driven by edge computing architecture and AI will be developed. These technologies aim to improve efficiency, security, and better airspace management.

- **Urban Air Mobility (UAM)**: As a result of technological progress, airspace may witness the rise of UAM, in which integrated edge computing architecture and AI technologies are essential to the control and optimization of air traffic in urban environments.

C. CHALLENGES IN UTILIZING EDGE COMPUTING

1) PROGRAMMABILITY

Users build their own programs and upload them to the cloud using a cloud computing paradigm; the cloud service provider decides whether or not the program processing actually happens in the cloud. They are either ignorant of the program's operation or are just partially aware of it. The fact that the end user cannot see the underlying infrastructure is one advantage of cloud computing. On the other side, edge computing offloads computation from the cloud and edge nodes are probably heterogeneous platforms. Because these nodes have vastly differing runtimes, the programmer has significant hurdles when trying to design an application that can be deployed in the architecture of edge computing.

2) NAMING

A primary assumption of edge computing is that there are an enormous number of IoT devices. On the other hand, at the edge node, a lot of apps are running at once, and each application, like any computer system, has a structure about how the service is provided. The naming method used in edge computing is crucial for a number of reasons, including but not limited to data transfer, programming, addressing, and item identification. Therefore, there is currently no standardized naming scheme designed for the edge computing paradigm. For professionals operating at the edge of their system to exchange data with its numerous components, they frequently need to become proficient in a wide range of network and communication protocols. In order to ensure privacy and security, edge computing requires a naming strategy that can handle a very large number of unreliable objects, highly dynamic network topology, and scalability. Notable that the tried-and-true techniques of naming do not function with the dynamic edge network.

3) SCHEDULING STRATEGIES

The algorithms of edge computing's scheduling are expected to optimize resource utilization, reduce energy usage, shorten reaction times, and speed up task processing. Scheduling strategies for edge computing need to work together. Completing tasks and sharing resources among nodes is similar to what happens in conventional distributed systems. However, keep in mind that, similar to cloud computing, your computer resources will probably be of different types and calibers. Moreover, one of the key challenges that users must overcome with edge computing is controlling its limited computational resources, which sets it apart from the cloud's more open environment. Since edge computing resources are diverse, scheduling strategies for Edge computing, like those for data, computing, storage, and networks, must be customized for each application. In addition, scheduling strategies must take into account the possibility of multiple distinct application types. Scheduling strategies should optimize the utilization of limited resources on edge nodes in order to improve application performance and efficiency [62]

D. SUMMARY

This section outlined the maritime sector which is the first use case we address since it is considered as one of the most recent use cases in the EC paradigm. Then we continue to demonstrate the various ways in which EC improves the network preformance in this industry. Next, we address the aerial system and the advantages of using EC in conjunction with this kind of system. After that, we present an overview of some of the applications that have been using EC in combination with aerial systems. Then we present some challenges that might be faced in the mentioned use cases. Table 2 presents the summary of the papers that have been utilized for all application domains in this survey. Notably, the two remaining domains mentioned in Table 2 which are IoT and Industry 4.0 addressed in the Appendix.

TABLE 2. **Application domains summary.**

Applications Domains	References
Maritime Industry	[40], [41], [42], [43], [44].
Aerial System	[37], [45], [46], [47], [48], [49], [50], [51], [52], [53], [54].
Internet of Things (IoT)	[22], [91], [92], [93], [94], [95], [96], [97], [98], [99], [100], [101], [102], [103], [104], [105].
Industry 4.0	[31], [35], [106], [107], [108].

VI. RECENT TECHNIQUES IN EDGE COMPUTING

It is evident that AI and blockchain techniques are deploying at a rapid rate, making them highly relevant in the current era, particularly as the fourth industrial revolution (4IR) gains huge momentum. The technological intricacy and multifaceted commercial consequences of both technologies vary.

First, AI is a modernistic science that seeks to build a machine that imitates the intelligence of a human. The intelligence is the capacity to make meaning of information. AI techniques are finding widespread use as complements to traditional methods or as parts of combined systems. They have been utilized for complex real-world issues in a variety of sectors. These techniques are also capable of learning from examples, handling noisy and incomplete data, handling nonlinear problems, and once trained can execute rapid prediction and generalization. Because of its symbolic reasoning, adaptability, and explanation capabilities, AI-based systems are being built and implemented globally in a wide range of industries such as engineering, economics, medicine, military, etc.

Second, the theory states that "since a blockchain technique is decentralized, nobody is in charge. With the technology of the blockchain, data is added to a distributed ledger and validated by network participants, each of whom contains a copy of the data. Blockchain is a revolutionary software technology that is changing many different commercial sectors, it is essentially a data structure that resembles a chain used to store transactions that have been approved by most nodes across the network. All credit for the fundamental creation of a blockchain system goes nevertheless to a group of primer developers. For example, a smart contract is essentially a collection of functions or algorithms that include a certain amount of data that are created and implemented on the blockchain by another human programmer. As a result, unfortunately, less likely to be devoid of errors and shortcomings. However, the committed transactions in the blockchain are stored at every single node, which makes it extremely difficult to alter or falsify [63], [64], [65], [66]. It is worth mentioning that security is one of the most critical criteria for any modern technology. The use of edge computing is contingent on creating safe applications and systems. As the security requirements in cloud computing are so vague, certain types of attacks can target cloud services. Because of their unique design, cloud computing services are frequently the focus of security concerns and data breaches. On the other hand, security in edge computing needs to be thoroughly defined and applied. As a result, better data security can be offered because client data is combined at specific access points near the end user [67]. More details can be found in the Appendix.

A. EDGE COMPUTING WITH ARTIFICIAL INTELLIGENCE

In general, EC devices are equipped with low capabilities of intelligence. These edge devices are in charge of local data processing such as storing and transmitting data to the cloud center.

1) THE INTEGRATION OF AI INTO EDGE COMPUTING

Recently, emerging technologies in internet protocols and computing systems have facilitated communications between different devices and made them faster. Therefore, applying the capabilities of one of these technologies which is AI with edge devices as shown in Fig. 3 to become more intelligent. Integrating the intelligence in edge devices will add the capability to analyze data, and also the capability to make decisions without the need of connecting to the cloud center. Thus, the latency will be reduced because of the added abilities.

2) THE GROWTH OF IoT INDUSTRY

In recent years, there has been a notable increase in the use of wireless communication technology recently, on the other hand, the number of IoT devices has also grown rapidly. The approximate number of IoT devices worldwide in 2020 that have connected to the internet is more than 25 billion devices. IoT devices produce large amounts of data which are really important for many modern applications for example healthcare, and smart cities. Therefore, a good approach to getting information and making decisions from the data collected is to equip these devices with intelligence. However, the answer to how to relocate the intelligence abilities from the cloud to the edge devices is still not clear. the applications that are using intelligence as a service often need sufficient computational resources and dedicated types of equipment for example GPU pools. Inversely, the current environments of edge devices are basically equipped with commercial servers with constrained resources. According to that, a denial in this matter becomes a main obstacle towards moving the feature of intelligence to the edge of the network [68], [69], [70], [71].

3) SECURITY

In terms of security aspect, edge intelligence, and edge computing security must be mutually reinforcing. The implementation of edge intelligence also hinges on the appropriate resolution of the core issues surrounding edge security, even if edge intelligence can address many of the issues facing modern edge computing security. To begin with, when training models, edge intelligence will consume a large amount of private data. It is more vulnerable to privacy breaches. Second, after being deployed to the edge, the edge intelligent model is easily stolen and cracked by hostile users, making it a valuable digital asset. Serious financial losses could come from it. When edge nodes process user-uploaded data and terminal perception data in real time, the cloud computing center must also conduct more in-depth analysis and make decisions based on the pre-processed data sets that the edge nodes upload. The security of edge intelligence is severely challenged in all areas by this process, which involves the transmission of a significant volume of sensitive data, including data, applications, networks, and equipment [21]. According to the information mentioned above, this survey presents a number of experiments to prove the aspects of improvement by integrating AI with EC as shown in Table 3.

The first experiment proposes intelligent edge devices that can be used in the coming generation in the applications of IoT. Edge device offers computing resources to be near the users. These devices are equipped with AI features in order to have the capability of making decisions in the environment where these should be deployed. This experiment proposes a cognitive snooping security system to preserve the amount of credibility of search incentive outputs, thus, precluding the commercial images from entering the web browser's image database. Applying the suggested system to the edge devices adds intelligence to the edges and the web data filtering will have the ability to detect web spam by using the services of the three different layers namely 1) data collection, 2) edge computing, 3) and the cloud. The job of the data collection layer which is at the bottom is to collect web data from various sources and transfer it to the next layer that is in charge of detecting the web spam at the edge and validating the spam detected by using deep learning models. After that the third layer which is the upper one is handling the storage in the cloud. As a result, the proposed architecture has improved the security level by barring web spam the result of this experiment is better than the existing results in the literature because the accuracy of it is 98.77% [72].

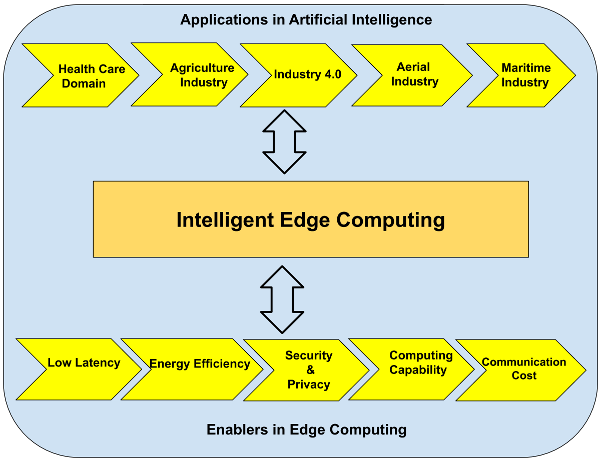

FIGURE 3. Edge computing with artificial intelligence.

Experiment number two in this survey proposes a new architecture of AI-empowered vehicular EC and caching. This architecture can dynamically link resources of EC and caching to polish the utilization of the system by applying AI-based algorithms. In addition, this new architecture can link the resources intelligently to target cross-layer offloading, cooperative multi-point caching and delivery, and V2V edge caching. Then, an integrated caching scheme with EC is presented to extend the advantage of the system by promoting a novel resource management scheme with the involvement of the developed deep reinforcement learning algorithm Deep Deterministic Policy Gradient (DDPG). In the proposed architecture, the roadside unit (RSU) is situated alongside a road, it represents the edge servers by offering communication, computing, and the capability of caching. The distinction between the current RSUs and the proposed RSUs is the capability of intelligence because RSUs in this architecture are equipped with AI functions which make them capable of providing resources for smart vehicles. The base station (BS) is in charge of providing the network to the vehicles, thus, the smart vehicles with RSUs should be located within the area that is covered by the available BS. Regarding the coverage area, usually the BS broadcasting with higher computing capability and caching resources than RSUs.

Therefore, BS can deal with the computation-intensive tasks in case RSUs are unable to handle the requirements of the computation for the smart vehicles. Moreover, the cache capability of BS is often larger than RSUs and the contents are less important in BS and the RSUs more important for example the latest news. In order to involve AI in this matter, the vehicular network is considered an environment and broadcasting the intelligence on the BS. Therefore, the capability of AI methods can be involved to recognize the feedback of the environment for instance vehicle demands, real-time behavior, and wireless channel state. In addition to that, to meet the smart vehicles requirement, the intelligent capability automatically designs developed actions due to the present state, which include cross-layer offloading, cooperative multi-point caching and delivery, and V2V edge caching. Finally, the numerical results of the proposed scheme prove that allocating resources is quick and efficient [73].

In the third experiment, deep learning (DL) technology, which represents AI, was involved with EC to enhance the network's efficiency. Basically, the EC methods have some issues such as high computing costs and high latency, it is better than the CC paradigm but these issues are critical for some applications. This experiment introduces deep learning techniques to develop the performance of EC methods.

Physical swell training has been always a hot field. Deep learning is representative of AI in various fields, especially for the academic community. The convolutional neural network (CNN) model utilizes convolution calculation, and deep reinforcement learning technology, and completes the resource allocation of EC for each trainer wearable sensor device, authorizing the deep reinforcement technique to identify EC optimization.

The CNN model is used to recognize the EC resource allocation of the IoT devices and the convolution processing is basically used to fulfill the resources rational allocation. As a result, based on the experimental analysis, the proposed method that integrates AI with EC to optimize the execution of EC methods shows an improvement in the execution of the methods in terms of having a low vacancy rate, high computing efficiency, and wide applicability. In addition to that, the suggested method has less power consumption for the server and the calculation cost can be effectively measured, the EC process is completed, thus, applying the training model can be possible for each trainer, and because of that the training is faster. Moreover, the proposed method has improved the training's quality and accuracy, therefore, the physical expansion training would be more effective [74].

The fourth experiment in this survey is using AI techniques to improve the security in the sensor network, which is one of the components of MEC that provides services for users. Applying AI technology in MEC to deal with the devices and the server's operation in such a platform is having security issues. Thus, this experiment is proposing a scheme namely Security Enhanced Traceback (SET) to enhance network performance and security. The principle behind this scheme is to divide the network into three sections namely deploy nodes in each section with a different marking probability, nodes deployed far from the sink will have a higher marking probability, while nodes deployed close to the sink will have a lower marking probability. On the other hand, selecting a tuple of data packets is not only saved in nodes but also transported to nodes far from the sink in order to stabilize the storage space of the nodes. The experimental finding indicates that both network performance and security are improved [75].

The fifth experiment is about the combination of EC and AI offers the advantage of being accessible from anywhere at any time without the need for cloud intervention. This solution is ideal for small-scale applications that require on-premises security and low-latency data processing. However, it cannot replace CC, which can handle massive data sets and connect the whole world. In the suggested model, AI-enabled EC is used to provide accurate information related to soil moisture, temperature, and humidity in the agriculture field. The use of AI-enabled edge ensures effective device monitoring, reduces unexpected failures, and increases productivity by offering accurate information at very low latency. Results show that the smart farming approach with AI-enabled edge has constrained energy consumption and takes less time to transport compared to traditional methods.

The proposed smart farming model departs from the traditional CC paradigm and adopts EC to reduce latency and communication costs. However, EC cannot replace CC, which can accommodate large-scale service utilization and data storage for numerous users. Instead, EC is a promising alternative for small-scale applications that require on-premises computation and timely solutions. Moreover, in the proposed model, EC is used in smart farming to reduce security risks, enhance efficiency, and reduce expenses. The suggested model was tested using real-time data to demonstrate the precision of the predictions. The evaluation was conducted using MATLAB to determine the maximum time required to transmit the information needed from the edge to the consumer [76].

The sixth experiment proposes a real-time monitoring system for landslides to provide early warnings to the population in case of danger. Landslides are a widespread phenomenon that causes numerous deaths and significant property damage worldwide each year. They occur when soil or rock slopes down due to gravity, and can be caused by various factors such as climate features, geological makeup, and topography of certain areas that are predisposed to a

TABLE 3. The result of using AI in edge computing.

Reference	Low Latency	Energy efficiency	Security and Privacy	Computation Capability	Communications cost
[21]	√	-	-	-	-
[22]	√	-	-	√	-
[24]	-	-	-	√	-
[23]	-	-	√	√	-
[25]	√	√	√	-	√
[27]	√	-	-	√	-
[28]	√	-	√	-	-
[29]	-	√	-	-	√
[31]	-	√	-	-	√
[33]	√	-	√	-	-
[80]	-	√	-	-	-

higher risk of landslides. The proposed system is an adaptable and distributed monitoring solution for landslides that can monitor various types of landslides using a multi-agent system (MAS) implemented on an edge heterogeneous cluster consisting of Odroid N2 and Nvidia Jaston Nano as described earlier in [77]. To minimize the utilization of cloud-based training for AI models, an NVIDIA Xavier has been added in order to enable local training into the edge. To test the proposed architecture, they deployed a weather node and multiple ground nodes at selected points on the landslides.

The specifications and details of these nodes were previously described in our earlier paper [78]. This experiment was built upon the previous work [77] by implementing AI algorithms to improve the detection of landslides using connected things. In order to reduce bandwidth and improve latency, most of the data processing has been shifted from the cloud to the edge. Due to this, the mean bandwidth has decreased from 2.63 Mbits to 249.5 Kbits, also the latency has decreased from 208 ms to 53 ms, and the amount of data transported to the cloud has decreased from 1180.06 MB per hour to 112 MB per hour. However, the execution time at the edge has increased due to the greater computing energy of our edge AI-IoT architecture compared to the cloud. While our suggested architecture has not been fully examined as there have been no landslides to date, our in-situ experimentation demonstrates the potential of our system in improving the efficiency and effectiveness of landslide monitoring [79].

The seventh experiment aims to combine AI with EC to present a forensics framework called the Efficient and Reliable Forensics Framework (ERFF), which is suitable for industrial intelligent EC that is critical for the implementation of Industry 4.0. ERFF consists of two parts, a detective module, and a validation model. The detective module observes how the client terminal interacts with the edge resource, which enables the investigator to safely collect evidence. The security-validation model integrated with ERFF is assumed to be more secure than the common key-based cryptography technique. To test the suggested framework, the researchers used the Live Digital Forensic Framework for a Cloud (LDF2C) and compared its results with other current industrial frameworks such as the Legal Reliable Forensic Framework (LRFF), Source Identification Network Forensics Framework (SINFF), and Logging Framework for Cloud Computing Forensic (LFCCF). These frameworks were created to support the digital forensic demands of industry and academia.

In other words, ERFF is a new forensics framework that leverages EC to enhance the reliability, efficiency, and precision of criminal activity detection. The framework utilizes a detective module and a validation model that collaborate to find communications between a client terminal and an edge resource. One key advantage of ERFF is its ability to spot illicit activities more faster using inexpensive edge devices.This means that investigators can obtain evidence more easily and securely, which can speed up the investigation process. In addition, ERFF uses data-collection tools including the super-timeline, information extraction, information retrieval, content, and media, all of which assist the procedures involved in forensics assault resistance. This makes the forensics statement that is given to the investigator free from attacks or illicit compromises. In comparison to other competing state-of-the-art frameworks, such as SNIF, LFCCF, and LRFF, ERFF provides better reliability, efficiency, precision, and deduction rates at the edge. ERFF's validation model is much safer than a common key-based cryptography method, and its use of EC makes it more efficient and reliable. Overall, ERFF appears to be a promising new forensics framework that could significantly improve the process of identifying criminal activities. Its use of EC and information collection features makes it more efficient and reliable, and its safety features make it more secure than other competing frameworks [80].

The main objective of the eighth experiment in this survey is to reduce the amount of energy of both edge devices and cloud services during the performing of AI of Things (AIoT) tasks. The experiment aims to achieve the objective of this experiment by formulating an optimization problem that focuses on scheduling tasks efficiently in both the edge and the cloud. To solve this problem, a new online approach has been suggested. In addition, it conducts experiments in an intelligent EC testbed and evaluates the amount of energy for various intelligent cloud services and edge devices.

Additionally, the framework for intelligent EC provided here shows how a well-designed system may handle AI tasks for AIoT applications with a significant increase in energy efficiency. A creative scheduling strategy is crucial for lowering energy use in a variety of environments. The performance evaluation results show that the reinforcement-learning-based approach is superior to alternative approaches for addressing the online scheduling issue, especially in a multilayer framework, and is better than other strategies, resulting in lower power consumption. In addition, the majority of commercial edge products exhibit sufficient performance in processing AI tasks with minimal energy consumption, indicating that intelligent EC presents a crucial opportunity for AIoT applications. As a result, the communications cost would be also reduced [81].

Experiment number nine proposes a new technology to enhance energy efficiency in the Industrial Internet of Things (IIOT). The utilization of AI technology in the IIoT presents a significant opportunity in Industry 4.0 (Fourth Industrial Revolution). However, processing complex AI tasks requires high-end servers, which results in high power consumption in IIoT environments. To address this challenge, this experiment introduces the idea of intelligent EC, a novel technology that endeavors to reduce energy usage in processing AI tasks and promote green AI computing for IIoT applications. The proposed framework has a heterogeneous architecture that offloads the majority of AI operations from servers and streamlines scheduling for various AI jobs to increase the efficiency of energy.

In order to evidence the effectiveness of the suggested solution, a little testbed is built to exhibit the energy efficiency of AI-driven IIoT applications with the intelligence of EC, as Intelligent EC offers a chance to enhance the energy efficiency of IIoT that is driven by AI, while also fulfilling the stringent demand for processing time. The intelligent edge controller is comprised of six main components: the edge node scheduler, AI model storage, task manager, AI model converter, AI processing interface, and interface management. The edge node scheduler is in charge of monitoring the status and characteristics of all edge nodes in the network, such as their workload, physical details, and software configurations. It uses a resource scheduling technique to determine the optimal edge node for handling incoming AI tasks. This procedure involves coordinating the various components to ensure efficient and effective execution. The processing of AI tasks in edge nodes relies on AI models that have been already trained.

However, these models frequently have platform-specific requirements and cannot be implemented in edge situations without modification. To address this issue, an AI model converter is used to automatically modify AI models that have been already trained to make them available for use in edge applications. The adapted AI models are designed for various heterogeneous edge devices. However, as the model conversion takes time, transforming AI models online can be challenging. To overcome this challenge, all transformed AI models are stored and controlled in an AI model storage system in preparation for future deployment. This storage system updates deployed AI models in edge nodes by storing AI models that have been trained with novel versions. Additionally, the task management module also maintains track of the resource usage, resource execution time, and edge node IDs for all of the edge nodes. The task management module's data is utilized by the edge node scheduler to plan AI jobs. To convert a task or edge node from one state to another, the task manager module regulates the statuses of those tasks and edge nodes.

The AI processes interface module offers a unified command set for the AI model storage, authorizing it to move platform- or device-related interfaces to the module's unified interface. The management interface module receives the edge node ID, task ID, and operations from the task manager module, which then transfers all operations to transmit direct orders to the specified edge node. Finally, since the industrial environment requires greater reliability than other IoT contexts, risk control mechanisms are presented to the AI-driven IIoT framework to avoid any failures. To ensure consistent service even in the event of a controller failure, the proposed framework deploys a centralized controller in a private cloud as opposed to a public cloud. In order to minimize the influence of the access network, edge nodes are linked to the controller via separate network links, and to prevent a single point of failure, the controller assigns several edge nodes to carry out important activities.

The scalability of the edge system and the scalability of AI job categories make up the scalability of the intelligent EC framework. The AI model that has been trained before can be easily added to the AI Model Storage to design a new task category for AI. The framework can distribute common AI models to a new edge node without model translation. Due to the dynamic workload of most IIoT environments, the primary goals of the work are to formulate the scheduling issues of utilizing limited computing resources in the edge to complete as many AI tasks as possible and to create an effective approach to overcome the problem in an online scenario. The proposed online scheduling technique has undergone rigorous simulation, and the findings indicate that, in most cases, it uses energy less than 80% of static scheduling and 70% of first-in, first-out (FIFO) scheduling. As a result, the communications cost is estimated to be decreased [82].

The following experiment in this survey which has number ten focuses on the security aspect and latency as well. Cyber-physical Systems (CPSs) have become more advanced and intricate, and as a result, they have been subjected to numerous unintentional and intentional disturbances, including a maximization in the number of cyber hits and the sophistication of their behaviors. For example, when fraudulent users or attackers demand the same physical nodes concurrently, this might result in service failure and constitute a security concern. Hence, a low-coupling system built on the EC platform has been created to overcome this problem.

A CPS contains different physical sensors, which are used to create virtual sensors. A virtual sensor may consist of one or more styles of physical sensors. The purpose of virtual sensors is to simplify the application of sensors by disregarding the sensor locations and criteria. However, this method may drive a coupling issue between physical and virtual sensors, which may result in the issuance of conflicting commands. For instance, if malicious consumers or attackers transmit numerous control requests to a physical sensor simultaneously, it may lead to the issuance of inconsistent commands. This is known as the coupling problem, which can be addressed using a mathematical model. To check the superiority of the proposed algorithm and mechanism, an evaluation was conducted under various parameters and the results were analyzed respectively. The same criteria were used to implement three comparison algorithms.

The first in first out (FIFO) algorithm was the first algorithm, which executes each user's requests sequentially. The second algorithm was the Shortest Job First (SJF) algorithm, which schedules each request based on the one with the shortest service time after classifying the service times of each request in ascending order. The third algorithm was the Kuhn-Munkres (KM) algorithm, which had no cache queues. Extended Kuhn-Munkres (EKM) which is the fourth algorithm, was put into practice utilizing buffer data from the physical sensors layer (EKMB). The experiment has constructed uniform distribution, normal distribution, and reversed normal distribution in eight scenes to compare to the proposed extended Kuhn-Munkres algorithm with double buffer queues (EKMDB). The eight scenes are explained in detail below. Following an arithmetic progression, the number of users rose from 100 to 450. Users to resources in the first experiment were split 1:5. In the second trial, it raised the user-to-resource ratio to 2:5, allowing the comparison of various settings.

Additionally, the numbering of edge nodes accounted for 1:4, 1:5, and 1:6 ratios (ENR) of the total number of physical nodes in various experiments. This experiment describes an intelligent method for cyber-physical systems (CPS) that uses an EC platform to optimize sensor utilization and counter-coupling problems. By emerging comparable commands and storing data from the bottom layer, the platform lowers the volume of requests from users to physical sensors. As a result, by combining comparable requests and caching data from bottom sensors, the proposed EKMDB algorithm maximizes sensor utilization in the EC layer, enabling it to rapidly respond to requests and decrease latency in parallel. The algorithm efficiently lowers scheduling and resource conflict costs, boosts resource usage, and extends the lifespan of the CPS [83].

This experiment which is no. 11 uses machine learning (ML) which is a sub-field of AI to address three typical issues in the unmanned aerial vehicles (UAV)-assisted EC system, it provides a brand-new survivable resource slice embedding technique. First, resource utilization is decreased when the resources allotted for the slices do not match the requirements of the task. Secondly, it is challenging for the UAV to supply enough supplies for the slices due to its limited resources. Third, a UAV malfunction lowers the caliber of the service. The long short-term memory (LSTM) network is proposed to predict the storage and processing needs of various slices to address these issues. Then, slices that already exist are assigned multidimensional resources. The slice embedding minimized loss function is computed based on the amount of processing and storage resources used. The interior point approach is then used to produce the slice embedding result.

The energy consumption of link re-embedding and server re-embedding is used to compute the minimized objective function of slice re-embedding in the event of a server failure. Ultimately, random rounding approaches and linear relaxation lead to the best re-embedding solution of slices. To assess the efficacy of the suggested method, this method carries out the tests on a real-world testbed by utilizing a Fifth-generation (5G) communications network trajectory dataset. Two benchmark algorithms are compared with this experiment's survivable slice embedding algorithm. It is demonstrated that the suggested algorithm may enhance the slice recovery consumption, slice acceptance ratio, and request acceptance ratio of the system [84].

B. EDGE COMPUTING WITH BLOCKCHAIN TECHNOLOGY

In recent years, several papers have presented the technique of blockchain-enabled into the EC paradigm. The primary aim of combining blockchain technique in EC as shown in Figure 4 is to provide security as it is presented in Table 4 for data processing and to support the transmission temper assistance and traceability for IoT devices [85].

1) SECURITY MECHANISM IN INTEGRATED BLOCKCHAIN EDGE COMPUTING (IBEC)

Various mechanisms can be presented in integrated blockchain edge computing (IBEC) in order to enhance the security and privacy aspect, for instance, identity authentication, and routing. It is recommended to apply smart contracts and smart oracles to create a trust management architecture that would assist the creation and use of smart applications by offering security services throughout the edge-fog-cloud computing continuum. This architecture applies smart oracles to evaluate and give targeted metrics for smart contracts, which are utilized to monitor off-chain data and choose the best edge nodes to lower costs and enhance system quality of service. A critical first step towards accomplishing safe authentication and cooperative sharing in a variety of applications is the creation of a distributed and reliable authentication system. An enhanced practical byzantine fault tolerance (PBFT) consensus mechanism is proposed for the system under description in order to make it easier to securely store logs and authentication data on the blockchain. Additionally, applying elliptic what is called curve cryptography (ECC)-based encryption and a domain name system (DNS)-based dynamic name resolution mechanism to the system under discussion adds important layers of anonymity, authentication, and security.

2) ROUTING PRIVACY

In terms of routing, the blooming filter is applied to generate new requests for the subsequent software-defined networking (SDN) controllers without exposing topology privacy. This allows for the protection of cross-domain routing privacy in multi-domain MEC networks. Three schemes are introduced in order to achieve this: a consortium blockchain-based routing verification scheme, a network-driven collaboration routing verification (NDCRV) scheme, and a cloud-driven CRV (CD-CRV) scheme. Furthermore, an ECC-based privacy-enhancement scheme (PES) with digital signature and public key random generation is designed in the IBEC environment to simultaneously accomplish both confidentiality and transparency [86].

The first experiment in this section that applies the blockchain technique is introduced by [87]. Little or medium-sized farms have never been able to participate in high-added-value farming because of the credibility of the information on organic agricultural products. Organic agriculture supply chains (OASCs) have historically been concentrated in both academic and agricultural environments. The system of OASCs is quite complex, it is responsible for the whole production process namely storage capacity, transportation speed, marketing quality, and energy consumption. The concept behind this system counts on the distribution of the database and centralized processing that are separated from each other. That way, tracing a piece of information, for instance, paper certificates or food labeling systems will be preserved by the identity of agribusiness, whether certificates or food labeling have a common fault, traceable information can be easily manipulated or even lost. Thus, this valuable data has to be stored by a trustworthy member. Hence, the blockchain technique might be the best way to fix this issue. In this case, blockchain applies a ledger called a distributed ledger technology (DLT), this ledger is preserved and controlled without any third party involved.

In OASCs, there is a need for a new computing mode to reach the goal of having unanimity and trust in the decentralized blockchain system. On the other hand, the blockchain system requires a kind of comparison between the performance and cost to master the issues of adoption and achievement by OASCs in the early stage. To obtain trust in OASCs, [87] proposes an information management framework for OASCs based on the blockchain technique and EC technology. This framework will offer a better comparison between dependencies and cost. the contribution of this experiment is distributed into three stages: 1) To achieve agreement among the different OASC structures, four key management functions for OASCs were separated and given respective roles. 2) Putting out a data-sharing architecture that utilizes blockchain in order to enable unaltered records with the intention of making OASCs far more rightful, transparent, and dependable. 3) The data platform can be shifted from a cloud-based to a local domain by adopting the technology of EC in organic agriculture. As a result, the cost of data processing will decrease and the overall response time will increase. According to the above experiment, the final result can reach the goal which is reducing the latency by avoiding the third party and adding more trust which leads to more security.

The second experiment in this survey was introduced by [5]. A reliable and efficient network can exist based on EC technology and blockchain techniques. The existing EC architecture is more practical than CC architecture, especially in terms of reducing latency, however, there are still some challenges that should take care of, firstly, in most cases there are different parties that are managing the edge devices, and there will be some trick devices among all devices, thus, these devices might deliver viruses or incorrect data to others, Secondly, the problem is how to equitably distribute computing resources among various edge nodes in order to reduce the job failure ratio for each edge device. Thirdly, the cache capacity and computing processing are low in edge devices, therefore, the safety is weak so they are easily strafe during frequent processing.

In this experiment, a three-tier architecture utilizing EC and blockchain technology is suggested. The goal of the experiment is to develop a novel group-agent technique by using trust computing, that will enhance transmission efficiency while ensuring the dependability of edge devices during communication. Additionally, a novel content model that utilizes the Zipf distribution to predict the popularity of phrases in context and symmetric searchable encryption (SSE) to encrypt hot material is being improved. The result of the simulation in this experiment shows that, in comparison to conventional approaches, the proposed technology offers higher reliability and more processing efficiency, which basically refers also to the security and latency aspects [5].

The third experiment utilizing blockchain technology in EC shows off an automatic intelligent agriculture system that is capable of monitoring and providing effective use of water resources to feed plants within the maximum farming period. The main goal of Applying the technique of blockchain in EC architecture in this system is to secure the privacy of the proposed agriculture system. In such cases, after applying the technique of blockchain the information access will be more secure within the connected devices. Additionally, blockchain technology ignores and manages the proposed Intelligent Climate and Watering Agriculture System (ICWAS) by concentrating access to only trusted devices [4]. The use of the ICWAS prototype will add the capability for the system to be used by several users to control and communicate simultaneously from a distance. Android and the fuzzy logic approach were utilized to design the prototype application. The ICWAS functions according to the input data for the weather and soil parameters and decides how much water to authorize, for example, by periodically turning on or off the water tunnels.

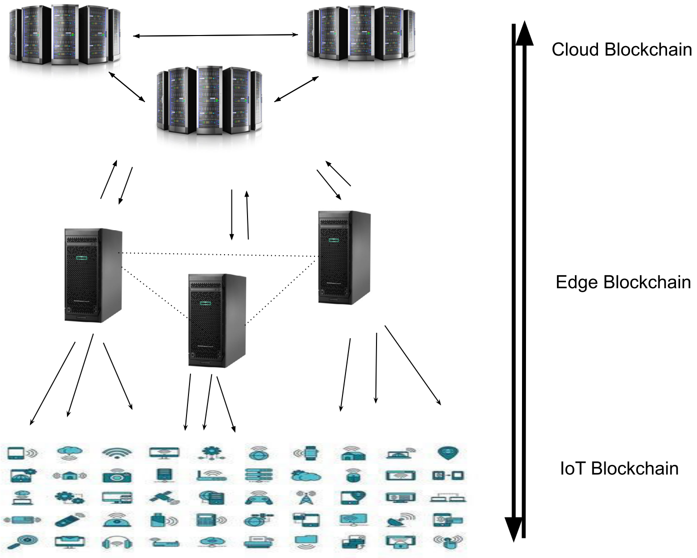

FIGURE 4. Edge computing with blockchain technology.

Moreover, the ICWAS adjusts the temperature level, humidity, weather, light intensity, and the content of the water in the soil by depleting sensors. Then the gathered data is sent to the server via WiFi in order to provide specified guidance for watering and continuously controlling the health of the plants on smart devices using the proposed application. On the other hand, the proposed system considered a limited amount of plants for modeling, and the related data is collected locally in order to monitor the health of plants accurately, and after that give recommended requirements in order to guide the farmer efficiently. In addition, the application of ICWAS is capable of intelligent monitoring and managing the quantity of water in smart devices. This experiment covers a group of plants namely onion, mint, cucumber, garlic, radish, chili, and tomato. The result of the experiment is that the suggested system has high scalability and security and it is capable of controlling the operation of watering plants, it offers multiple uses for users, and monitoring and interaction can be available remotely. The judgments were made by applying intelligent fuzzy logic according to the input parameters. it is notable that the system can also notify users in terms of turning the water off or on.

The fourth experiment in this survey is introducing a case of a smart home that is using blockchain techniques with EC. The case is about applying a Blockchain framework for IoT through EC technology. Currently, the communications in IoT architectures are complex, low level of security, and centralized. Furthermore, data reliability still has issues such as communications network overload, data missing, malicious data inserted, and the power of overload computing in the central node. This experiment is presented a novel architecture based on the blockchain with EC technology by adding a new layer in EC as well as a novel algorithm in order to enhance the quality of data and detect the failure of data. the network in the smart home is controlling all activities and all data collected should be sent and stored in the blockchain.

Thus, all available features of blockchain can be achieved. All smart devices linked to the network are equipped with sensors and Raspberry Pi to control these sensors. Each one of the smart devices is modeled by different transceivers and has the ability to capture the data and combine it in the network. The sensor combines a LIS3DH-model accelerometer that is capable of measuring acceleration across a range of values (between 0 and +/−16g). Moreover, the sensor is automatically checked for employment conditions so that accuracy may always be preserved. In terms of temperature control, integrating the TC1047A ultra-low power consumption sensor authorizes temperature management. As the system is also integrated with a positioning system that uses GNSS networks to geolocate data utilizing the MAX-M8Q model from the maker of u-blox, which can handle single signals from the GPS, Galileo, and GLONASS standards.

For the energy consumption aspect, an ATSAMR21G18A microcontroller (MCU) from Microchip company is used to control energy consumption utilizing a non-invasive Hall effect sensor. The SCT- 013-000 is capable of handling energy consumption up to 100A with a dielectric resistance of 3KV. The MCU applies the IEEE 802.15.4 communications protocol in conjunction with the ultra-low power ARM Cortex-M0+ architecture to enable interactions across the open thread network. The Raspberry Pi 3 is applied as a router for cutting-edge technology. On the other hand, in order to have communication with all sensors in the network, the Raspberry Pi 3 combines an open thread platform enabling the device the CC2652 from the manufacturer Texas Instruments that eases the functionality of all sensors in the network, and that because of its open drivers. Therefore, that's how Raspberry gathered the information from the blockchain

TABLE 4. The result of using blockchain in edge computing.

Reference	Low Latency	Energy Efficiency	Security and Privacy	Computation Capability
[5]	√	-	√	-
[4]	√	-	√	√
[3]	-	-	√	-
[2]	-	-	√	-
[20]	-	√	√	-
[34]	-	-	√	-
[35]	-	-	√	√
[36]	-	-	√	-
[37]	-	-	√	-
[38]	-	√	√	-
[95]	√	-	√	√

framework for IoT data quality by using EC architecture [3]. After all the information mentioned above, the proposed architecture is improving the data security in the system of the smart home.

The fifth experiment of using blockchain in EC aims to improve the security aspect. EC is considered as a critical tool for digitization in recent years. However, securing the data using EC technology is facing difficulties, especially in wide areas. Therefore, a new mechanism is proposed to solve the security matter, which is about combining blockchain technique and coding in EC in order to enhance security and reliability. The concept of this experiment is distributed into three stages:
1) Based on the three-tier EC architecture and the requirements of data security storage, this experiment proposed a hybrid storage architecture and a model that adapted to the paradigm of EC.
2) Concentrating on using all advantages in data storage for edge devices and the services of cloud storage. The idea here is to design a global blockchain in the cloud service layer and the terminal of the IoT there is a local blockchain technique.
3) The proposed scheme introduces a mechanism for checking the validation hash values of data to guarantee the probity of the data collected in the global blockchain. After applying the above stages the result is that the renovation coding has been used to improve the data storage reliability. Then, a second verification is done by the local blockchain that is designed on the terminals of the IoT. Finally, the data stored in the cloud might be compared to the data in the nearby blockchain for the seek of verification, thus ensuring the security of the data. Due to the remaining energy of devices, the regeneration coding selects the terminals based on who is repaired with recovering data, and as a result, the development of each device resource within the EC can be done and avoiding the waste of resources which refers to energy efficiency [88].

Experiment number six introduces an architecture to improve the quality of service in EC by applying blockchain technology. The modern network management layer considers management and orchestration as key components, with multi-domain orchestration being particularly useful for simplifying infrastructure operations and enabling the faster implementation of network services. However, resource supply, which involves optimizing the network and fulfilling multi-limitation quality of service (QoS), remains a significant challenge. This experiment proposes an architecture that addresses this challenge by using multi-domain edge orchestration (MDEO) combined with blockchain technology. The MDEO executes a dynamic end-to-end (E2E) network slicing algorithm that enables secure and isolated multi-tenant network infrastructure provisioning, based on multi-constraint QoS. The algorithm first determines the optimal network slice topology and then structures the virtual network functions accordingly while meeting the multi-constraint QoS requirements. Transparency, trust, and automated service-level agreement fulfillment are all can be possible through the utilization of smart contracts and blockchain in the telecommunication sector. The Multi-Domain Edge Orchestrator proposal was explained, including its ability to offer end-to-end (E2E) efficient services in 5G networks. However, ensuring that service level agreements (SLAs) are correctly enforced is a complex task that can lead to errors and delays if not handled correctly.

In addition, SLAs may also be interpreted in different ways, which may lead to disagreements. Transparency also requires real-time data validation, however, this is not always possible. An orchestrator component-based multi-constrained E2E method is envisaged to avoid these issues. However, in the telecommunications sector, trust connections are crucial, and some network service providers might not trust the orchestrator. To solve these problems, the proposal introduces the concept of blockchain, specifically hyperledger fabric. Blockchain will manage all records on each domain edge orchestrator (DEO) and MDEO, forming a distributed ledger. The idea additionally makes utilization of smart contracts to include legal agreements in the system, allowing for automatic fulfillment based on specified conditions. The framework includes SLA management, network slicing, multi-domain edge orchestrator, and multi-constrained E2E path on distributed ledger technique. The network slicing module distributed the physical network at an E2E level, enabling ideal traffic grouping, isolation from other tenants, and resource configuration at a macro level. SLAs are defined as utilizing smart contracts on the blockchain, and the network is distributed into categorizations based on the E2E level.

The MDEO computes all possible E2E paths and selects the best path that fulfills all constraints, finally sending data to the blockchain. Combined services and RSVP are applied to address context additive service restrictions including latency reduction, packet loss, jitter reduction, pricing, and hop count as well as non-additive service limitations like bandwidth, DEO restriction, and country restriction. A simulated experiment was conducted on the system and the proposed framework's burst and response times were examined using various distributions. The results in both instances indicate that the behavior follows a lognormal distribution [89].

The following experiment which is number seven in this survey has introduced a certificateless signcryption mechanism using blockchain with EC technology to improve security. According to the limited computing capacity and energy of EC devices, collecting information promptly while ensuring information authenticity and traceability can be challenging. The certificateless signcryption mechanism can address these concerns as it can simultaneously achieve encryption and signature, but existing mechanisms have either security problems or high computational costs. To solve these issues, a novel certificateless signcryption mechanism is proposed that incorporates a bilinear pairing operation in public key generation, reducing the computational cost and improving public key security.

Furthermore, blockchain is leveraged as a public key directory to enhance resistance to tampering with device public keys by illegal consumers. Contributions include designing a blockchain-based certificateless signcryption method that solves the key escrow problem, implementing both encryption and signature to guarantee confidentiality and unforgeability, and providing security proof under certain assumptions. The method is compared to eight related methods and demonstrated to be efficient and effective. Additionally, a lightweight blockchain is designed for EC environments and the method is embedded to demonstrate practicality. The comparative analysis indicates that the suggested scheme achieves better results in efficiency and security compared to existing schemes. The operation of signcryption and unsigncryption uses the least amount of computation, making it an appropriate option for the EC environment [90].

Experiment number eight proposes a new decentralized architecture in the smart vehicular field to enhance network performance. Smart vehicles are anticipated to possess complex, high-dimensional applications that require significant resources. These applications, including platoon control, AI-based pedestrian detection, fuel scheduling, and augmented reality gaming, serve various user preferences and boost safety and efficiency. The intensive computational requirements of these applications pose a challenge for resource-limited vehicles. Vehicular EC (VEC) networks are capable of providing cloud-like computing experiences at the edges of vehicles by using roadside units (RSUs) and MEC servers have the ability to achieve the necessary requirements of throughput and latency. Furthermore, the rapid advancements of AI algorithms have accelerated the development of intelligent VEC (IVEC) infrastructure.

Due to its centralized governance and black box computation, IVEC is capable of attacks like bogus computation feedback, unfair or biased resource allocation, and other issues. The utilization of edge consumers, such as automobiles, with a computation verification option is suggested as a way to utilize edge consumers and leverage a decentralized architecture created on blockchain to maximize resource management transparency and solve security flaws. In addition, a secure IVEC federation mode is proposed for load balancing to address the issue of unbalanced load distribution.

The main challenges associated with these solutions are highlighted, and promising research directions are briefly outlined to attract the interest of concerned stakeholders and parties within the realms of the blockchain and EC domains. The proposed decentralized system adopts a hierarchical architecture. Smart cars and other roadside devices, such as street cameras, are part of the bottom layer, referred to as the task creation layer, which continuously generates resource-intensive computing tasks for the infrastructure on the edge. This layer seeks a service offload to start the transaction operation. Every task that is offloaded is regarded as a service for edge infrastructure. A permission chain known as EdgeChain is formed by numerous RSUs/access points (APs), along with the accompanying edge servers, at the mid-layer/edge layer within a defined region. EdgeChain holds information that corresponds to each service request, including timestamps, names of linked entities, hashes of computation results, and the amount of server resource allocation.

In order to reduce human interference, this chain automates each level of the operations and ensures transparency in resource orchestration. To equilibrium loads among edge servers, an edge federation layer is designed on top of the edge servers. While the entities establish a permissioned network to store trading data into FedChain (a consortium blockchain formed by entities of the federation layer), this federation layer also holds numerous edge servers and a certificate authority (CA). As a result, the suggested architecture is based on a blockchain system and is organized hierarchically to improve impressionability in resource management and allow edge clients, such as vehicles and roadside equipment, to verify computations. Additionally, a secure computation trading model is suggested within the IVEC framework to expand edge computation capacity horizontally and manage unbalanced load distribution more effectively [91].

Experiment number nine uses blockchain with EC to improve security and privacy. The volume and variety of data in-vehicle networks are growing, allowing sophisticated applications including developed driving safety and enhancing existing services through data sharing and analysis. Mobile EC and vehicular networks can be utilized to design vehicle EC and networks (VECONs), which can offer strong computing and storage resources. However, it is not possible to totally trust roadside units acting as EC servers, creating significant security and privacy issues for these platforms. To solve these issues, consortium blockchain and smart contract technologies can be utilized for secure data storage and sharing in VECONs. These technologies avoid unauthorized data sharing and provide an efficient solution for secure and transparent transactions. Additionally, a reputation-based data-sharing scheme is proposed to guarantee high-quality data sharing among vehicles.

The reputation of vehicles is likely controlled by applying a three-weight subjective logic model. The proposed method makes use of smart contracts to guarantee the reliability and security of data sharing in the automotive blockchain. Due to their distributed nature, smart contracts are blockchain-based programs that automate multiple-step procedures and cannot be changed or halted. This improves the vehicular blockchain's reliability, effectiveness, and security. On the vehicular blockchain, two smart contracts—data storage smart contract (DSSC) and Information sharing smart contract (ISSC)—are implemented to enhance secure and decentralized data sharing.

The outcome of this experiment has led to the presentation of a secure peer-to-peer (P2P) data-sharing system for networks and computing in vehicles. In order to save and share data securely and effectively, smart contracts and consortium blockchain technology were used, avoiding the use of unlicensed second-hand data sharing. A reputation-based data-sharing scheme was proposed using the three-weight subject logic (TWSL) model, which considers interaction frequency, event timeliness, and trajectory similarity to accurately manage the reputation for high-quality data sharing among vehicles. As a result, during the data sharing process in VECONs, cars can choose the best data providers with high-quality data. This technique guarantees the security of data sharing and storage, based on the security analysis. The benefits of the proposed TWSL scheme over conventional reputation schemes in identifying aberrant vehicles to enable secure data sharing were shown by numerical results [92].

A secure and effective V2G energy commerce framework for CPSs is proposed in experiment number ten in this survey, by integrating blockchain, EC, and contract theory. The framework included a contract-based incentive method to encourage electrical vehicles (EVs) to be involved in energy commerce and energy commerce between EVs and Local energy aggregators (LEAGs), which was secured by exploiting consortium blockchain. A task offloading technique relying on EC was also suggested in order to minimize the computational strain on LEAGs and raise the likelihood that blocks will be successfully designed. On the other hand, the allocation problem of computational resources is modeled as a two-stage process: firstly, a Stackelberg leader-follower game is utilized, and secondly, the best methods are found by applying the backward induction model.

The efficiency of the suggested framework is then assessed utilizing theoretical analysis and numerical results. Theoretical research and numerical results prove that the performance of the suggested framework is improved in terms of contract viability, task offloading, and security. The experiment found that the suggested framework allowed for effective energy commerce despite information asymmetry, with the incentive-compatible contract effectively eliciting asymmetric information of the EV kind. The Convex-Concave procedure (CCP) based contract optimization algorithm successfully maximized the expected utility of the LEAG, but further research is recommended since the initial point's selection had a substantial influence on the convergence performance of CCP. Furthermore, simulation results presented that the utilization of EC might significantly increase the success probability of block generation, raising it by 124.6% with the presence of eight LEAGs [93].

This experiment which takes no.11 in this survey presents a design named Multi-Camera Multi-Hypothesis Tracking (MC-MHT) framework that is integrated with the Multi-Camera TrackingChain (MCTChain) which is a perspective of blockchain transaction. This integration improves the limitation of the communication bottleneck and computation resources of the centralized curator and improves security and privacy compared to the traditional method named Multi-Camera Multi-Object Tracking (MCMT). The mechanism of MC-MHT is about aggregating all raw video data and distributing tracking tasks to each camera to be expanded flexibly within the EC environment to ensure efficiency and guarantee security and privacy.

In order to lower the danger of single-point failure or Byzantine behaviors, this framework creates a collaborative architecture powered by MCTChain technology that allows tracking information to be shared and tracking consensus to be conducted via dispersed multiple cameras. Furthermore, the collaborative architecture is authorized by MCTChain's technology to exchange tracking data and assume the risk of Byzantine or single-point failure. The implementation of MCTChain is done by Python code and adopting a P2P network for per communications. To verify the effectiveness of MCTChain, constructing a centralized MCMT system is done for comparison with MCTChain. The centralized system consists of multiple cameras and a powerful server, whereas the MCTChain is formed of edge devices. In order to more clearly show the latency of each round in MCTChain. This experiment splits a round into three stages: local tracking computation, which has a total time overhead, tracking transactions, and blockchain and according to the result of this experiment, the time efficiency is stable [94].

C. SUMMARY

The effects of integrating two cutting-edge technologies namely blockchain technology and AI techniques into the EC architecture are covered in this section. Eleven experiments under different circumstances and with a different application were given for each technique. Afterward, we compiled all of the experiment's findings and displayed every experiment's impact by putting them on tables to illustrate the different impacts on every field. Table 5 displays an overview of the publications that have been used in this section concerning technology.

TABLE 5. Blockchain and AI summary.

Cutting-edge Technologies	References
AI	[3], [4], [5], [70], [71], [74], [75], [76], [77], [78], [79], [80], [81], [82], [83], [84], [85], [86], [87].
Blockchain	[3], [4], [21], [22], [72], [73], [88], [89], [90], [91], [92], [93], [94], [95], [96], [97], [98], [99], [100], [101], [102], [103], [104], [105].

VII. FUTURE DIRECTIONS

In terms of future directions, by conducting a comprehensive assessment of the range of research outcomes in EC, it has been determined that there are still some crucial challenges to be investigated.

A. SECURITY AND PRIVACY

This survey outlined various types of attacks in EC and discussed the potential solutions for detecting and improving them through the use of AI and blockchain techniques. However, security and privacy still need more investigations in the EC system. Although traditional security frameworks have been extensively developed over the years and are generally effective at defending against attacks, the security terminologies used within these frameworks are not always capable of addressing the modern-day attacks that are frequently encountered in EC systems. As a result, adopting a new approach may reduce the risk of breaches [22].

B. DATA HANDLING

Data handling involves a range of activities including collecting, storing, analyzing, and sharing information, therefore, it poses numerous challenges. One major obstacle is integrating and making different data formats and structures work together. Additionally, handling large amounts of data remains a challenge, as evidenced by recent surveys that identified data overload as a key issue. Furthermore, with the rapid growth of IoT devices, massive amounts of data are being downloaded and uploaded through edge devices. This means that the capabilities of these devices must be reliable to effectively manage the huge volume of data being collected [95].

C. ENERGY EFFICIENCY

In the upcoming era, networks will become increasingly intricate and require significant energy to power billions of interconnected devices. Currently, most IoT devices are battery-powered or operate in resource-constrained environments. As a result, energy efficiency is essential to prolong battery life, reduce energy consumption, reduce operational costs, and optimize device performance. As it would be impractical to regularly change or recharge the batteries of such a vast number of devices. Consequently, energy efficiency becomes imperative for future networks and devices. Furthermore, it is worth noting that the number of IoT devices is expanding at a rapid pace, and ensuring their long-term functionality calls for a focus on energy efficiency. Additional research and investigation are necessary to adequately address the specific requirements of certain applications, for example, the military sector [96], [97].

D. MOBILITY

The mobility of IoT devices is still considered an open challenge, the quick growth in the number of mobile devices connected to the network edge has introduced critical challenges, despite the added flexibility that mobility provides to users and applications. Specifically, the disconnections between edge devices and the edge network can often be attributed to mobility, which can significantly degrade the overall quality of service by impacting key parameters such as loss, delay, and bandwidth [22].

E. HETEROGENEITY

In the current EC system, the environment has become highly heterogeneous. Due to the increasing number and diversity of connected devices with varying hardware limitations, including mobile devices such as smartphones, and unmanned vehicles in conjunction with the propagation of multiple network access technologies such as Wi-Fi, WiMAX, 4G, 5G, and beyond that aims to combine existing devices with the IoT domain [97], [98].

F. RELIABILITY

Finally, the last future direction in this survey is the reliability of the EC system, due to dynamic and unpredictable environments, resource constraints, distribution complexity, network connectivity issues, edge device failures, and the demand for real-time processing, achieving reliability in EC is still a significant challenge [99].

G. QUANTUM COMPUTING

Considering the principles of quantum physics, over the past few years, the quantum computing (QC) community has accomplished a significant milestone. Basically, QC is a cutting-edge branch of computation that makes possible tasks that were previously considered unachievable for classical computers by using quantum bits (qubits). Therefore, the integration of the current network design and QC presents several substantial challenges. Firstly, developing optimized quantum algorithms for network settings is necessary to involve quantum computers in the architecture of the network while taking into account the particular limitations of network devices. It also requires the successful fusion of network devices with quantum hardware [100]. Secondly, it is challenging to guarantee the security and privacy of a quantum system, which demands strong cryptography methods and quantum-safe protocols. lastly, network designs and protocols must be carefully considered to be capable of handling seamless interaction between quantum network devices and central QC resources [101].

H. SUMMARY

As addressed in the section, several significant challenges in the EC sector need more attention and research. Security and privacy are still primary challenges, and new strategies are frequently required because outdated frameworks are incapable of handling contemporary threats. On the other hand, handling large amounts of data and combining different formats can be challenging when it comes to data processing, especially with the rapid growth of the IoT domain. Also, with limited resources and an ever-expanding IoT device landscape, energy efficiency is essential for powering large and linked networks. Moreover, the mobility of IoT devices presents issues with service quality and disconnections which need more investigations. Heterogeneity is caused by different devices and network technologies, which makes the challenge more critical. lastly, establishing reliability in dynamic, resource-constrained, real-time EC systems is a substantial continuous difficulty. Table 6 presents the summary of the papers that have been utilized in this section in terms of the challenges.

TABLE 6. Open challenges summary.

Challenges	References
Security and Privacy	[106].
Data Handling	[31].
Energy Efficiency	[35], [107].
Mobility	[106].
Heterogeneous	[35], [108].
Reliability	[109].
Quantum Computing	[16], [110].

VIII. CONCLUSION

In summary, the involvement of blockchain and AI in edge computing architecture is expected to integrate seamlessly in the future. Applying AI technology will improve edge devices' intelligence, on the other hand, blockchain technology would offer a transparent and safe foundation for decentralized interactions. Therefore, by making edge computing applications faster, more secure, and intelligent edge computing applications made possible by this joint evolution, a number of industries could undergo a complete transformation. This survey overviewed the most recent applications domains in edge computing in recent years and presented the impact of combining them with the architecture of edge computing, these applications are the maritime domain, aerial systems, IoT domain, and Industry 4.0. Furthermore, this survey investigated the influence of integrating the techniques of AI and blockchain in the paradigm of edge computing and ended up with the results of eleven experiments in each technique in order to present the added features in the edge computing paradigm. Finally, this survey has considered some open challenges and future directions that can be investigated in the future to improve the performance and reliability of the edge computing architecture.

APPENDIX

IoT

The rise of the IoT paradigm is one of the most remarkable phenomena of the past few years. The IoT is a rapidly evolving sector of technology that combines cutting-edge protocol and communications technologies with speedy and intelligent software to analyze data and provide computing services. These services utilize cloud and EC architectures that are tailored to the needs of the customer and the level of service for a variety of use cases across different domains [102]. The ability to have a video chat with family members living on different continents was once unimaginable a few decades back, but now it has become a common occurrence. To earn a more in-depth comprehension of the scale of IoT, consider the following statistics; Around 6.1 billion people worldwide used smartphones in 2020, and there were reportedly 50 billion connected devices. In addition, it is anticipated that there will be 27 billion machine-to-machine links across various industries by 2027 [103]. The reason behind this notable transformation can be attributed to the declining cost of technology and the emergence of devices that possess new and improved capabilities. Additionally, because of the ease provided by smartphones, it is now feasible to complete things like ordering a cab, paying bills, sending emails, and transferring money with just a few clicks [104]. Furthermore, the development of different communication protocols and the miniaturization of transceivers have made it feasible to transform previously isolated devices into communicating "things" [105].

IoT industry represents a significant advancement in science and technology, monitoring the growth of electronic gadgets, the Internet, and the mobile network. The IoT enables some real-world attitudes and behaviors to become intelligent, practical, and effective by integrating virtual information with reality [106]. IoT applications are being used more and more frequently in a number of industries, such as smart factories, wearable technology, smart homes, smart surroundings, and so on [31]. The primary target of IoT technology is to simplify our daily lives and make things more convenient by saving time, money, and energy, ultimately resulting in reduced expenses for various industries. However, due to the extensive integration of IoT devices into our daily tasks, a significant volume of data is being generated from these devices [107]. The properties of data produced by IoT devices include polymorphism, heterogeneity, timeliness, extensive magnitude, accuracy, huge scale, and rich semantics [35].

The processing and storage of this data may be inefficient because IoT devices have limited resources. In order to get over these constraints, the IoT domain must use CC technology. In the context of resource-limited IoT devices, it becomes crucial to explore a new task-scheduling strategy in order to enhance performance specifically within the mobile communication network [108]. IoT devices generate a continuous stream of data from various applications, which is stored in the cloud system. However, certain applications in different industries require low latency or real-time processing, which cannot be effectively handled by CC. In the IoT domain, a viable approach has emerged to handle the sensitivity of latency and context-aware services. By relocating the competition of the data and the service supply as well from the centralization of the cloud to the edge, this solution addresses the limitations of CC [109].In the context of EC, the platform of EC offers architecture and software support for computing applications at the edge, which leads to a significant reduction in latency and improved efficiency [110].

EC is designed to fulfill these requirements by providing the necessary capabilities at the network's edge. The paradigm of EC includes several approaches such as cloudlet, FC, and MEC [15], [16] which offer comprehensive solutions to CC architecture, reducing latency at the edge of the network. In other words, the EC model is a prototype that encompasses cloudlet, FC, MEC, and micro clouds. Resources like storage, computational processing, and power are shifted closer to the edge of the network to reduce latency and increase availability, overcoming the limitations of the CC paradigm. The management of millions of sensors, devices, and related resources presents a complicated set of problems, and as the IoT sector grows rapidly, EC is proving to be a practical solution. In other words, in contrast to CC, EC moves data computation and storage to the edge of the network which is located closer to the consumers, this technique decreases traffic flows and diminishes the bandwidth requirements in IoT. Furthermore, EC reduces the latency between the edge/cloudlet servers and consumers, thus the response will be in a shorter time for real-time IoT applications compared to traditional cloud services. Additionally, by lowering the cost of workload transmission and shifting computational and communication overhead from nodes with limited battery resources to nodes with significant power resources, nodes with limited battery resources can have their lifetimes extended, thus prolonging the lifetime of the entire IoT system [111].

On the other hand, security and safety aspects have become crucial verticals in IoT applications [112]. As technology continues to advance and generate more data from sensors and high-resolution video cameras, there is an increasing demand for a scalable, adaptable, and cost-effective solution to evaluate this content in the aspect of real-time response. it is notable that due to MEC's capacity to manage enormous amounts of data locally, analytics applications can be hosted close to the data source to improve efficiency, and performance, and significantly reduce costs. For instance, the analysis of improved video enables the development and use of guidelines for different situations to awaken alertness and take appropriate action. Real-time video analysis can count the number of items as well as identify them, specify principles for elements of interest, and event-based rules like moving into or out of space. By using sound analytics and extra data from outside sources and sensors, these analytics can be further enhanced. MEC also makes it possible for a security solution that is automated, flexible, scalable, and properly priced. Therefore, the analytics function can offer flexible extensions to third parties via the integration of plug-ins, and the solution is made easy to use by permitting video processing and analytics applications to perform at their best based on technical and financial considerations [113].

APPENDIX

INDUSTRY 4.0

The fourth industrial revolution, which is known as Industry 4.0, is the digitization and automation of production processes with the target of improving flexibility, responsiveness, and data-driven decision-making. However, the industrial sector is shifting away from automation and towards autonomy, but there is currently limited availability of devices with sufficient processing power to support autonomy in industrial plants [114]. Industry 4.0 represents a holistic strategy for manufacturing that leverages the interconnectivity of the IoT, real-time data access, and cyber-physical systems. It makes it possible to quickly and affordably increase productivity. Manufacturing systems communicate, analyze, and use data in Industry 4.0 to direct intelligent operations. Additionally, it includes modern innovations like robotics, AI, augmented reality (AR), and additive manufacturing [115].

In contrast to Industry 3.0, which is also known as the digital revolution, Industry 4.0 encourages the use of cyber-physical systems (CPS) in manufacturing, which are digital assets capable of operating and interacting autonomously or with little to no human contact. The German government coined the term "Industry 4.0" in 2011, and it is expected to bring about significant changes to how production and supply chain activities have been conceptualized up until the late 1990s and early 2000s. The significant shift in the manufacturing industry, known as Industry 4.0, is supported by the latest advancements in information and communication technologies (ICTs), which are transforming our daily lives. Modern control systems are capable now of gathering and handling enormous volumes of real-time data, optimizing production procedures, and raising product quality because of the growing capability of digital technologies. Additionally, distributed manufacturing equipment makes use of communication networks to enhance production procedures, lower energy usage, and greenhouse gas emissions, and reduce production pipeline downtime by using preventive maintenance techniques [116].

By merging sophisticated information processing methods, communication technologies, and future-focused strategies, Industry 4.0 gains the capability to transform a factory into a smart facility. However, the great degree of automation, adaptability, and complexity in such an intelligent plant also presents significant reliability and security challenges. To overcome these challenges, innovative methods for predictive maintenance that increase system reliability can be created using industrial big data produced by many sources of sensors, system intercommunication, and outside-linked data [117]. On the other hand, Industry 4.0 heavily relies on the IoT and CC for monitoring and automating industrial processes. In this context, early failure detection of the assembly line equipment is crucial since it reduces downtime and boosts productivity. While time-sensitive industrial applications such as industrial robots or unmanned/guided vehicles used to deliver tools and merchandise may have strict QoS requirements, current defect detection systems are primarily cloud-centric and may not be able to satisfy those criteria. The development of fresh solutions in the complementary fields of processing and communication is being driven by this issue. While EC solutions are being looked into to minimize processing latency and conserve bandwidth, time-sensitive networking (TSN) and 5G standards are being examined to reduce data acquisition latency and ensure deterministic message delivery [118].

APPENDIX
BLOCKCHAIN CHARACTERISTICS

By using the following features in the network, the efficiency will be improved, quicken processing time, and secure the data.

A. DECENTRALIZATION

The transaction in the blockchain technique is different from the conventional mode that should be authorized by the central authority. Therefore, the advantage of using the decentralization character is to avoid the central authority and allow direct user-to-user transactions, and all information about the transaction process should be recorded, and all members in the transaction can have a copy of the record which is available anytime. In addition, the blockchain is continuously expanding since miners add new blocks to it approximately every 10 minutes to record the latest transactions [119].

B. SECURITY

In a blockchain, new blocks can only be added to the chain after they have been successfully validated by the decentralized network of nodes through a consensus mechanism. This process makes certain that the blockchain's integrity is maintained and that no fraudulent transactions are added to the ledger. The cryptography techniques used in the blockchain also ensure that the data in each block is secure and cannot be changed or tampered with. Overall, the combination of cryptography and decentralized consensus makes the blockchain a highly secure and trustworthy ledger for recording transactions [120].

C. IMMUTABILITY

One of the main characteristics of blockchain technology is immutability, which means that once data is transferred to the blockchain, it is not possible to be changed or removed. The decentralized and distributed nature of the blockchain makes it challenging for any one party to change the data without consensus from the majority of the entire network [121].

D. SMART CONTRACT

A smart contract is another significant aspect of the blockchain, the idea is about starting into impact if the conditions and requirements are fulfilled. Smart contracts on blockchain technology can offer a safe and effective way to carry out contracts and automate procedures. Self-executing computer programs known as "smart contracts" can automatically enforce the terms of a contract between two parties without the use of a moderator or manual participation. By using blockchain technology, these smart contracts can be stored on a decentralized, tamper-resistant network, providing a high level of security and transparency [122], [123].

Blockchain as a service was first introduced in the digital currency of Bitcoin. Nowadays, because of the advantages of the blockchain, the technology has attracted various applications to improve the network's performance and to support the smart digital contract in order to improve decentralization in applications [2], [124]. Applying blockchain technology in the EC paradigm promises to add several features to the network such as improving the storage resources, security, and the capability of computation in the servers in the EC mode based on the property of consensus of the blockchain technology.

REFERENCES

[1] T. Yang, Z. Cui, C. Peng, J. Wu, F. Liu, and Y. Yang, "Integrated communication and computing maritime networks design for green metaverse," *IEEE Wireless Commun.*, vol. 30, no. 5, pp. 120–126, Oct. 2023.

[2] M. H. Ronaghi, "A blockchain maturity model in agricultural supply chain," *Inf. Process. Agricult.*, vol. 8, no. 3, pp. 398–408, Sep. 2021.

[3] R. Casado-Vara, F. de la Prieta, J. Prieto, and J. M. Corchado, "Blockchain framework for IoT data quality via edge computing," in *Proc. 1st Workshop Blockchain-Enabled Networked Sensor Syst.*, 2018, pp. 19–24.

[4] L. Ting, M. Khan, A. Sharma, and M. D. Ansari, "A secure framework for IoT-based smart climate agriculture system: Toward blockchain and edge computing," *J. Intell. Syst.*, vol. 31, no. 1, pp. 221–236, Feb. 2022.

[5] L. Zhang, Y. Zou, W. Wang, Z. Jin, Y. Su, and H. Chen, "Resource allocation and trust computing for blockchain-enabled edge computing system," *Comput. Secur.*, vol. 105, Jun. 2021, Art. no. 102249.

[6] M. M. Hassan, M. R. Hassan, V. H. C. de Albuquerque, and W. Pedrycz, "Soft computing for intelligent edge computing," *Appl. Soft Comput.*, vol. 128, Oct. 2022, Art. no. 109628.

[7] A. Hammoud, H. Sami, A. Mourad, H. Otrok, R. Mizouni, and J. Bentahar, "AI, blockchain, and vehicular edge computing for smart and secure IoV: Challenges and directions," *IEEE Internet Things Mag.*, vol. 3, no. 2, pp. 68–73, Jun. 2020.

[8] R. Yang, F. R. Yu, P. Si, Z. Yang, and Y. Zhang, "Integrated blockchain and edge computing systems: A survey, some research issues and challenges," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1508–1532, 2nd Quart., 2019.

[9] Z. Xiong, Y. Zhang, D. Niyato, P. Wang, and Z. Han, "When mobile blockchain meets edge computing," *IEEE Commun. Mag.*, vol. 56, no. 8, pp. 33–39, Aug. 2018.

[10] Q. Chen, Z. Zheng, C. Hu, D. Wang, and F. Liu, "On-edge multi-task transfer learning: Model and practice with data-driven task allocation," *IEEE Trans. Parallel Distrib. Syst.*, vol. 31, no. 6, pp. 1357–1371, Jun. 2020.

[11] V. Hassija, V. Chamola, D. N. Gopala Krishna, N. Kumar, and M. Guizani, "A blockchain and edge-computing-based secure framework for government tender allocation," *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2409–2418, Feb. 2021.

[12] Z. Liu, L. Wan, J. Guo, F. Huang, X. Feng, L. Wang, and J. Ma, "PPRU: A privacy-preserving reputation updating scheme for cloud-assisted vehicular networks," *IEEE Trans. Veh. Technol.*, early access, Dec. 8, 2023, doi: 10.1109/TVT.2023.3340723.

[13] J. Guo, Z. Liu, S. Tian, F. Huang, J. Li, X. Li, K. K. Igorevich, and J. Ma, "TFL-DT: A trust evaluation scheme for federated learning in digital twin for mobile networks," *IEEE J. Sel. Areas Commun.*, vol. 41, no. 11, pp. 3548–3560, Nov. 2023.

[14] E. Ahmed and M. H. Rehmani, "Mobile edge computing: Opportunities, solutions, and challenges," *Future Gener. Comput. Syst.*, vol. 70, pp. 59–63, May 2017.

[15] Y. Xiao, Y. Jia, C. Liu, X. Cheng, J. Yu, and W. Lv, "Edge computing security: State of the art and challenges," *Proc. IEEE*, vol. 107, no. 8, pp. 1608–1631, Aug. 2019.

[16] J. Gedeon, F. Brandherm, R. Egert, T. Grube, and M. Mühlhäuser, "What the fog? Edge computing revisited: Promises, applications and future challenges," *IEEE Access*, vol. 7, pp. 152847–152878, 2019.

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

[18] P. P. Ray, D. Dash, and D. De, "Edge computing for Internet of Things: A survey, e-healthcare case study and future direction," *J. Netw. Comput. Appl.*, vol. 140, pp. 1–22, Aug. 2019.

[19] I. Sittón-Candanedo, R. S. Alonso, Ó. García, L. Muñoz, and S. Rodríguez-González, "Edge computing, IoT and social computing in smart energy scenarios," *Sensors*, vol. 19, no. 15, p. 3353, Jul. 2019.

[20] J. Zhang, B. Chen, Y. Zhao, X. Cheng, and F. Hu, "Data security and privacy-preserving in edge computing paradigm: Survey and open issues," *IEEE Access*, vol. 6, pp. 18209–18237, 2018.

[21] H. Zeyu, X. Geming, W. Zhaohang, and Y. Sen, "Survey on edge computing security," in *Proc. Int. Conf. Big Data, Artif. Intell. Internet Things Eng. (ICBAIE)*, Jun. 2020, pp. 96–105.

[22] K. Cao, Y. Liu, G. Meng, and Q. Sun, "An overview on edge computing research," *IEEE Access*, vol. 8, pp. 85714–85728, 2020.

[23] W. Z. Khan, E. Ahmed, S. Hakak, I. Yaqoob, and A. Ahmed, "Edge computing: A survey," *Future Gener. Comput. Syst.*, vol. 97, pp. 219–235, Aug. 2019.

[24] L. Kong, J. Tan, J. Huang, G. Chen, S. Wang, X. Jin, P. Zeng, M. Khan, and S. K. Das, "Edge-computing-driven Internet of Things: A survey," *ACM Comput. Surv.*, vol. 55, no. 8, pp. 1–41, 2022.

[25] J. Pan and J. McElhannon, "Future edge cloud and edge computing for Internet of Things applications," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 439–449, Feb. 2018.

[26] J. Wu, L. Wang, Q. Pei, X. Cui, F. Liu, and T. Yang, "HiTDL: High-throughput deep learning inference at the hybrid mobile edge," *IEEE Trans. Parallel Distrib. Syst.*, vol. 33, no. 12, pp. 4499–4514, Dec. 2022.

[27] J. Wu, L. Wang, Q. Jin, and F. Liu, "Graft: Efficient inference serving for hybrid deep learning with SLO guarantees via DNN re-alignment," *IEEE Trans. Parallel Distrib. Syst.*, vol. 35, no. 2, pp. 280–296, Feb. 2024.

[28] L. Liu, C. Chen, Q. Pei, S. Maharjan, and Y. Zhang, "Vehicular edge computing and networking: A survey," *Mobile Netw. Appl.*, vol. 26, no. 3, pp. 1145–1168, Jun. 2021.

[29] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, "A survey of mobile cloud computing: Architecture, applications, and approaches," *Wireless Commun. Mobile Comput.*, vol. 13, no. 18, pp. 1587–1611, Dec. 2013.

[30] K. P. Saharan and A. Kumar, "Fog in comparison to cloud: A survey," *Int. J. Comput. Appl.*, vol. 122, no. 3, pp. 10–12, Jul. 2015.

[31] D. Liu, Z. Yan, W. Ding, and M. Atiquzzaman, "A survey on secure data analytics in edge computing," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4946–4967, Jun. 2019.

[32] Y. Dai, K. Zhang, S. Maharjan, and Y. Zhang, "Edge intelligence for energy-efficient computation offloading and resource allocation in 5G beyond," *IEEE Trans. Veh. Technol.*, vol. 69, no. 10, pp. 12175–12186, Oct. 2020.

[33] Z. Zhou, X. Chen, E. Li, L. Zeng, K. Luo, and J. Zhang, "Edge intelligence: Paving the last mile of artificial intelligence with edge computing," *Proc. IEEE*, vol. 107, no. 8, pp. 1738–1762, Aug. 2019.

[34] Y. An, F. R. Yu, J. Li, J. Chen, and V. C. M. Leung, "Edge intelligence (EI)-enabled HTTP anomaly detection framework for the Internet of Things (IoT)," *IEEE Internet Things J.*, vol. 8, no. 5, pp. 3554–3566, Mar. 2021.

[35] Z. Chang, S. Liu, X. Xiong, Z. Cai, and G. Tu, "A survey of recent advances in edge-computing-powered artificial intelligence of things," *IEEE Internet Things J.*, vol. 8, no. 18, pp. 13849–13875, Sep. 2021.

[36] Y. Zuo, J. Guo, N. Gao, Y. Zhu, S. Jin, and X. Li, "A survey of blockchain and artificial intelligence for 6G wireless communications," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 4, pp. 2494–2528, 2023.

[37] P. McEnroe, S. Wang, and M. Liyanage, "A survey on the convergence of edge computing and AI for UAVs: Opportunities and challenges," *IEEE Internet Things J.*, vol. 9, no. 17, pp. 15435–15459, Sep. 2022.

[38] R. Singh and S. S. Gill, "Edge AI: A survey," *Internet Things Cyber-Phys. Syst.*, vol. 3, pp. 71–92, Mar. 2023.

[39] Z. Li, D. Kong, Y. Niu, H. Peng, X. Li, and W. Li, "An overview of AI and blockchain integration for privacy-preserving," 2023, *arXiv:2305.03928*.

[40] N. Nomikos, P. K. Gkonis, P. S. Bithas, and P. Trakadas, "A survey on UAV-aided maritime communications: Deployment considerations, applications, and future challenges," *IEEE Open J. Commun. Soc.*, vol. 4, pp. 56–78, 2023.

[41] Z. Xu, W. Liu, J. Huang, C. Yang, J. Lu, and H. Tan, "Artificial intelligence for securing IoT services in edge computing: A survey," *Secur. Commun. Netw.*, vol. 2020, pp. 1–13, Sep. 2020.

[42] F. Wang, M. Zhang, X. Wang, X. Ma, and J. Liu, "Deep learning for edge computing applications: A state-of-the-art survey," *IEEE Access*, vol. 8, pp. 58322–58336, 2020.

[43] Q. Zhang, Y. Luo, H. Jiang, and K. Zhang, "Aerial edge computing: A survey," *IEEE Internet Things J.*, vol. 10, no. 16, pp. 14357–14374, Aug. 2023.

[44] V. Ahsani, A. Rahimi, M. Letafati, and B. H. Khalaj, "Unlocking metaverse-as-a-service the three pillars to watch: Privacy and security, edge computing, and blockchain," 2023, *arXiv:2301.01221*.

[45] Y. Mansouri and M. A. Babar, "A review of edge computing: Features and resource virtualization," *J. Parallel Distrib. Comput.*, vol. 150, pp. 155–183, Apr. 2021.

[46] M. Talebkhah, A. Sali, M. Marjani, M. Gordan, S. J. Hashim, and F. Z. Rokhani, "Edge computing: Architecture, applications and future perspectives," in *Proc. IEEE 2nd Int. Conf. Artif. Intell. Eng. Technol. (IICAIET)*, Sep. 2020, pp. 1–6.

[47] J. Guo, H. Gao, Z. Liu, F. Huang, J. Zhang, X. Li, and J. Ma, "ICRA: An intelligent clustering routing approach for UAV ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 2, pp. 2447–2460, Feb. 2023.

[48] X. Su, L. Meng, and J. Huang, "Intelligent maritime networking with edge services and computing capability," *IEEE Trans. Veh. Technol.*, vol. 69, no. 11, pp. 13606–13620, Nov. 2020.

[49] Y. Liu, J. Yan, and X. Zhao, "Deep reinforcement learning based latency minimization for mobile edge computing with virtualization in maritime UAV communication network," *IEEE Trans. Veh. Technol.*, vol. 71, no. 4, pp. 4225–4236, Apr. 2022.

[50] A.-R. Morariu, A. Ashraf, and J. Björkqvist, "A systematic mapping study on edge computing approaches for maritime applications," in *Proc. 47th Euromicro Conf. Softw. Eng. Adv. Appl. (SEAA)*, Sep. 2021, pp. 37–44.

[51] A. L. Michala, I. Vourganas, and A. Coraddu, "Vibration edge computing in maritime IoT," *ACM Trans. Internet Things*, vol. 3, no. 1, pp. 1–18, Feb. 2022.

[52] A. Munusamy, M. Adhikari, M. A. Khan, V. G. Menon, S. N. Srirama, L. T. Alex, and M. R. Khosravi, "Edge-centric secure service provisioning in IoT-enabled maritime transportation systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 2, pp. 2568–2577, Feb. 2023.

[53] W. Wu, F. Zhou, B. Wang, Q. Wu, C. Dong, and R. Q. Hu, "Unmanned aerial vehicle swarm-enabled edge computing: Potentials, promising technologies, and challenges," *IEEE Wireless Commun.*, vol. 29, no. 4, pp. 78–85, Aug. 2022.

[54] O. Bekkouche, T. Taleb, and M. Bagaa, "UAVs traffic control based on multi-access edge computing," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2018, pp. 1–6.

[55] Y. Zeng, R. Zhang, and T. J. Lim, "Wireless communications with unmanned aerial vehicles: Opportunities and challenges," *IEEE Commun. Mag.*, vol. 54, no. 5, pp. 36–42, May 2016.

[56] F. Zhou, R. Q. Hu, Z. Li, and Y. Wang, "Mobile edge computing in unmanned aerial vehicle networks," *IEEE Wireless Commun.*, vol. 27, no. 1, pp. 140–146, Feb. 2020.

[57] Y. Mao, C. You, J. Zhang, K. Huang, and K. B. Letaief, "A survey on mobile edge computing: The communication perspective," *IEEE Commun. Surveys Tuts*, vol. 19, no. 4, Dec. 2017.

[58] S. Li, B. Duo, X. Yuan, Y.-C. Liang, and M. Di Renzo, "Reconfigurable intelligent surface assisted UAV communication: Joint trajectory design and passive beamforming," *IEEE Wireless Commun. Lett.*, vol. 9, no. 5, pp. 716–720, May 2020.

[59] Z. Song, X. Qin, Y. Hao, Y. Hao, J. Wang, and X. Sun, "A comprehensive survey on aerial mobile edge computing: Challenges, state-of-the-art, and future directions," *Comput. Commun.*, vol. 191, pp. 233–256, Jul. 2022.

[60] Q.-V. Pham, R. Ruby, F. Fang, D. C. Nguyen, Z. Yang, M. Le, Z. Ding, and W.-J. Hwang, "Aerial computing: A new computing paradigm, applications, and challenges," *IEEE Internet Things J.*, vol. 9, no. 11, pp. 8339–8363, 2022.

[61] N. Fatima, P. Saxena, and M. Gupta, "Integration of multi access edge computing with unmanned aerial vehicles: Current techniques, open issues and research directions," *Phys. Commun.*, vol. 52, Jun. 2022, Art. no. 101641.

[62] R. Patel, L. Prasad, R. Tandon, and N. P. S. Rathore, "A comprehensive review on edge computing, applications & challenges," in *Security and Risk Analysis for Intelligent Edge Computing*. Cham, Switzerland: Springer, 2023, pp. 1–33.

[63] T. Marwala and B. Xing, "Blockchain and artificial intelligence," 2018, *arXiv:1802.04451*.

[64] A. Islam and S. Y. Shin, "A digital twin-based drone-assisted secure data aggregation scheme with federated learning in artificial intelligence of things," *IEEE Netw.*, vol. 37, no. 2, pp. 278–285, Mar. 2023.

[65] A. Mellit and S. A. Kalogirou, "Artificial intelligence techniques for photovoltaic applications: A review," *Prog. Energy Combustion Sci.*, vol. 34, no. 5, pp. 574–632, Oct. 2008.

[66] Z. Zheng, H.-N. Dai, and J. Wu, "Blockchain intelligence: When blockchain meets artificial intelligence," 2019, *arXiv:1912.06485*.

[67] N. Hassan, S. Gillani, E. Ahmed, I. Yaqoob, and M. Imran, "The role of edge computing in Internet of Things," *IEEE Commun. Mag.*, vol. 56, no. 11, pp. 110–115, Nov. 2018.

[68] K. Hazelwood, S. Bird, D. Brooks, S. Chintala, U. Diril, D. Dzhulgakov, M. Fawzy, B. Jia, Y. Jia, A. Kalro, J. Law, K. Lee, J. Lu, P. Noordhuis, M. Smelyanskiy, L. Xiong, and X. Wang, "Applied machine learning at Facebook: A datacenter infrastructure perspective," in *Proc. IEEE Int. Symp. High Perform. Comput. Archit. (HPCA)*, Feb. 2018, pp. 620–629.

[69] X. Shang, Y. Huang, Z. Liu, and Y. Yang, "NVM-enhanced machine learning inference in 6G edge computing," *IEEE Trans. Netw. Sci. Eng.*, early access, Sep. 3, 2021, doi: 10.1109/TNSE.2021.3109538.

[70] M. S. Mahdavinejad, M. Rezvan, M. Barekatain, P. Adibi, P. Barnaghi, and A. P. Sheth, "Machine learning for Internet of Things data analysis: A survey," *Digit. Commun. Netw.*, vol. 4, no. 3, pp. 161–175, 2018.

[71] M. G. S. Murshed, C. Murphy, D. Hou, N. Khan, G. Ananthanarayanan, and F. Hussain, "Machine learning at the network edge: A survey," *ACM Comput. Surv.*, vol. 54, no. 8, pp. 1–37, Nov. 2022.

[72] A. Makkar, U. Ghosh, and P. K. Sharma, "Artificial intelligence and edge computing-enabled web spam detection for next generation IoT applications," *IEEE Sensors J.*, vol. 21, no. 22, pp. 25352–25361, Nov. 2021.

[73] Y. Dai, D. Xu, S. Maharjan, G. Qiao, and Y. Zhang, "Artificial intelligence empowered edge computing and caching for Internet of Vehicles," *IEEE Wireless Commun.*, vol. 26, no. 3, pp. 12–18, Jun. 2019.

[74] Z. Liu, "Analysis of physical expansion training based on edge computing and artificial intelligence," *Mobile Inf. Syst.*, vol. 2021, pp. 1–9, Jun. 2021.

[75] Y. Liu, T. Wang, S. Zhang, X. Liu, and X. Liu, "Artificial intelligence aware and security-enhanced traceback technique in mobile edge computing," *Comput. Commun.*, vol. 161, pp. 375–386, Sep. 2020.

[76] D. D. Sivaganesan, "Design and development AI-enabled edge computing for intelligent-IoT applications," *J. Trends Comput. Sci. Smart Technol.*, vol. 2019, no. 2, pp. 84–94, Dec. 2019.

[77] O. Debauche, S. Mahmoudi, S. A. Mahmoudi, P. Manneback, and F. Lebeau, "A new edge architecture for AI-IoT services deployment," *Proc. Comput. Sci.*, vol. 175, pp. 10–19, Jan. 2020.

[78] M. E. Moulat, O. Debauche, S. Mahmoudi, L. A. Brahim, P. Manneback, and F. Lebeau, "Monitoring system using Internet of Things for potential landslides," *Proc. Comput. Sci.*, vol. 134, pp. 26–34, Jan. 2018.

[79] M. Elmoulat, O. Debauche, S. Mahmoudi, S. A. Mahmoudi, P. Manneback, and F. Lebeau, "Edge computing and artificial intelligence for landslides monitoring," *Proc. Comput. Sci.*, vol. 177, pp. 480–487, Jan. 2020.

[80] A. Razaque, M. Aloqaily, M. Almiani, Y. Jararweh, and G. Srivastava, "Efficient and reliable forensics using intelligent edge computing," *Future Gener. Comput. Syst.*, vol. 118, pp. 230–239, May 2021.

[81] S. Zhu, K. Ota, and M. Dong, "Energy-efficient artificial intelligence of things with intelligent edge," *IEEE Internet Things J.*, vol. 9, no. 10, pp. 7525–7532, May 2022.

[82] S. Zhu, K. Ota, and M. Dong, "Green AI for IIoT: Energy efficient intelligent edge computing for Industrial Internet of Things," *IEEE Trans. Green Commun. Netw.*, vol. 6, no. 1, pp. 79–88, Mar. 2022.

[83] T. Wang, Y. Liang, Y. Yang, G. Xu, H. Peng, A. Liu, and W. Jia, "An intelligent edge-computing-based method to counter coupling problems in cyber-physical systems," *IEEE Netw.*, vol. 34, no. 3, pp. 16–22, May 2020.

[84] G. Wu, B. Zhang, and Y. Li, "Intelligent and survivable resource slicing for 6G-oriented UAV-assisted edge computing networks," *Comput. Commun.*, vol. 202, pp. 154–165, Mar. 2023.

[85] D. Liu, Y. Zhang, D. Jia, Q. Zhang, X. Zhao, and H. Rong, "Toward secure distributed data storage with error locating in blockchain enabled edge computing," *Comput. Standards Interfaces*, vol. 79, Jan. 2022, Art. no. 103560.

[86] H. Xue, D. Chen, N. Zhang, H.-N. Dai, and K. Yu, "Integration of blockchain and edge computing in Internet of Things: A survey," *Future Gener. Comput. Syst.*, vol. 144, Jul. 2023.

[87] S. Hu, S. Huang, J. Huang, and J. Su, "Blockchain and edge computing technology enabling organic agricultural supply chain: A framework solution to trust crisis," *Comput. Ind. Eng.*, vol. 153, Mar. 2021, Art. no. 107079.

[88] Y. Ren, Y. Leng, Y. Cheng, and J. Wang, "Secure data storage based on blockchain and coding in edge computing," *Math. Biosci. Eng.*, vol. 16, no. 4, pp. 1874–1892, 2019.

[89] V. K. Rathi, V. Chaudhary, N. K. Rajput, B. Ahuja, A. K. Jaiswal, D. Gupta, M. Elhoseny, and M. Hammoudeh, "A blockchain-enabled multi domain edge computing orchestrator," *IEEE Internet Things Mag.*, vol. 3, no. 2, pp. 30–36, Jun. 2020.

[90] G. Xu, J. Dong, C. Ma, J. Liu, and U. G. O. Cliff, "A certificateless signcryption mechanism based on blockchain for edge computing," *IEEE Internet Things J.*, vol. 10, no. 14, pp. 11960–11974, Jul. 2023.

[91] S. Islam, S. Badsha, S. Sengupta, H. La, I. Khalil, and M. Atiquzzaman, "Blockchain-enabled intelligent vehicular edge computing," *IEEE Netw.*, vol. 35, no. 3, pp. 125–131, May 2021.

[92] J. Kang, R. Yu, X. Huang, M. Wu, S. Maharjan, S. Xie, and Y. Zhang, "Blockchain for secure and efficient data sharing in vehicular edge computing and networks," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4660–4670, Jun. 2019.

[93] Z. Zhou, B. Wang, M. Dong, and K. Ota, "Secure and efficient vehicle-to-grid energy trading in cyber physical systems: Integration of blockchain and edge computing," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 50, no. 1, pp. 43–57, Jan. 2020.

[94] S. Wang, H. Sheng, Y. Zhang, D. Yang, J. Shen, and R. Chen, "Blockchain-empowered distributed multi-camera multi-target tracking in edge computing," *IEEE Trans. Ind. Informat.*, vol. 20, no. 1, pp. 369–379, Jan. 2023.

[95] P. Sukruta, K. Chetana, and A. Khalid, "Analysis of data handling challenges in edge computing," *Int. J. Performability Eng.*, vol. 18, no. 3, p. 176, 2022.

[96] S. Shukla, P. K. Jha, and K. C. Ray, "An energy-efficient single-cycle RV32I microprocessor for edge computing applications," *Integration*, vol. 88, pp. 233–240, Jan. 2023.

[97] J. Liu, P. Yang, and C. Chen, "Intelligent energy-efficient scheduling with ant colony techniques for heterogeneous edge computing," *J. Parallel Distrib. Comput.*, vol. 172, pp. 84–96, Feb. 2023.

[98] S. Niu, H. Shao, Y. Su, and C. Wang, "Efficient heterogeneous signcryption scheme based on edge computing for industrial Internet of Things," *J. Syst. Archit.*, vol. 136, Mar. 2023, Art. no. 102836.

[99] Q. Vu Khanh, V.-H. Nguyen, Q. N. Minh, A. Dang Van, N. Le Anh, and A. Chehri, "An efficient edge computing management mechanism for sustainable smart cities," *Sustain. Comput., Informat. Syst.*, vol. 38, Apr. 2023, Art. no. 100867.

[100] A. D. Córcoles, A. Kandala, A. Javadi-Abhari, D. T. McClure, A. W. Cross, K. Temme, P. D. Nation, M. Steffen, and J. M. Gambetta, "Challenges and opportunities of near-term quantum computing systems," *Proc. IEEE*, vol. 108, no. 8, pp. 1338–1352, Aug. 2020.

[101] A. S. Cacciapuoti, M. Caleffi, F. Tafuri, F. S. Cataliotti, S. Gherardini, and G. Bianchi, "Quantum Internet: Networking challenges in distributed quantum computing," *IEEE Netw.*, vol. 34, no. 1, pp. 137–143, Jan./Feb. 2019.

[102] S. Naveen and M. R. Kounte, "Key technologies and challenges in IoT edge computing," in *Proc. 3rd Int. Conf. I-SMAC (IoT Social, Mobile, Anal. Cloud) (I-SMAC)*, Dec. 2019, pp. 61–65.

[103] M. Moh and R. Raju, "Machine learning techniques for security of Internet of Things (IoT) and fog computing systems," in *Proc. Int. Conf. High Perform. Comput. Simul. (HPCS)*, Jul. 2018, pp. 709–715.

[104] A. Ghosh, D. Chakraborty, and A. Law, "Artificial intelligence in Internet of Things," *CAAI Trans. Intell. Technol.*, vol. 3, no. 4, pp. 208–218, Dec. 2018.

[105] A. Mosenia and N. K. Jha, "A comprehensive study of security of Internet-of-Things," *IEEE Trans. Emerg. Topics Comput.*, vol. 5, no. 4, pp. 586–602, Oct. 2017.

[106] B. Zheng, Z. Mei, L. Hou, and S. Qiu, "Application of Internet of Things and edge computing technology in sports tourism services," *Secur. Commun. Netw.*, vol. 2021, pp. 1–10, May 2021.

[107] V. K. Sarker, J. P. Queralta, T. N. Gia, H. Tenhunen, and T. Westerlund, "A survey on LoRa for IoT: Integrating edge computing," in *Proc. 4th Int. Conf. Fog Mobile Edge Comput. (FMEC)*, 2019, pp. 295–300.

[108] X. Huang, W. Fan, Q. Chen, and J. Zhang, "Energy-efficient resource allocation in fog computing networks with the candidate mechanism," *IEEE Internet Things J.*, vol. 7, no. 9, pp. 8502–8512, Sep. 2020.

[109] J. Ren, Y. Pan, A. Goscinski, and R. A. Beyah, "Edge computing for the Internet of Things," *IEEE Netw.*, vol. 32, no. 1, pp. 6–7, Jan. 2018.

[110] H. Ning, Y. Li, F. Shi, and L. T. Yang, "Heterogeneous edge computing open platforms and tools for Internet of Things," *Future Gener. Comput. Syst.*, vol. 106, May 2020.

[111] W. Yu, F. Liang, X. He, W. G. Hatcher, C. Lu, J. Lin, and X. Yang, "A survey on the edge computing for the Internet of Things," *IEEE Access*, vol. 6, pp. 6900–6919, 2017.

[112] A. Islam, A. Al Amin, and S. Y. Shin, "FBI: A federated learning-based blockchain-embedded data accumulation scheme using drones for Internet of Things," *IEEE Wireless Commun. Lett.*, vol. 11, no. 5, pp. 972–976, May 2022.

[113] D. Sabella, A. Vaillant, P. Kuure, U. Rauschenbach, and F. Giust, "Mobile-edge computing architecture: The role of MEC in the Internet of Things," *IEEE Consum. Electron. Mag.*, vol. 5, no. 4, pp. 84–91, Oct. 2016.

[114] A. Carvalho, N. O'Mahony, L. Krpalkova, S. Campbell, J. Walsh, and P. Doody, "At the edge of Industry 4.0," *Proc. Comput. Sci.*, vol. 155, pp. 276–281, Jan. 2019.

[115] M. Khadmaoui-Bichouna, G. Golcarenarenji, I. Martinez-Alpiste, and J. M. A. Calero, "Edge computational offloading for corrosion inspection in Industry 4.0," *IEEE Internet Things Mag.*, vol. 5, no. 4, pp. 116–120, Dec. 2022.

[116] D. Stadnicka, J. Sęp, R. Amadio, D. Mazzei, M. Tyrovolas, C. Stylios, A. Carreras-Coch, J. A. Merino, T. Żabiński, and J. Navarro, "Industrial needs in the fields of artificial intelligence, Internet of Things and edge computing," *Sensors*, vol. 22, no. 12, p. 4501, Jun. 2022.

[117] J. Yan, Y. Meng, L. Lu, and L. Li, "Industrial big data in an Industry 4.0 environment: Challenges, schemes, and applications for predictive maintenance," *IEEE Access*, vol. 5, pp. 23484–23491, 2017.

[118] L. Bacchiani, G. De Palma, L. Sciullo, M. Bravetti, M. Di Felice, M. Gabbrielli, G. Zavattaro, and R. D. Penna, "Low-latency anomaly detection on the edge-cloud continuum for Industry 4.0 applications: The SEAWALL case study," *IEEE Internet Things Mag.*, vol. 5, no. 3, pp. 32–37, Sep. 2022.

[119] D. Tse, B. Zhang, Y. Yang, C. Cheng, and H. Mu, "Blockchain application in food supply information security," in *Proc. IEEE Int. Conf. Ind. Eng. Eng. Manag. (IEEM)*, Dec. 2017, pp. 1357–1361.

[120] R. Zhang, R. Xue, and L. Liu, "Security and privacy on blockchain," *ACM Comput. Surv.*, vol. 52, no. 3, pp. 1–34, 2019.

[121] F. Hofmann, S. Wurster, E. Ron, and M. Böhmecke-Schwafert, "The immutability concept of blockchains and benefits of early standardization," in *Proc. ITU Kaleidoscope, Challenges Data-Driven Soc. (ITU K)*, Nov. 2017, pp. 1–8.

[122] A. Jain and D. S. Jat, "Supply chain management using blockchain, IoT and edge computing technology," in *Innovative Supply Chain Management via Digitalization and Artificial Intelligence*. Singapore: Springer, 2022, pp. 87–98.

[123] B. K. Mohanta, S. S. Panda, and D. Jena, "An overview of smart contract and use cases in blockchain technology," in *Proc. 9th Int. Conf. Comput., Commun. Netw. Technol. (ICCCNT)*, Jul. 2018, pp. 1–4.

[124] P. Mendki, "Blockchain enabled IoT edge computing," in *Proc. Int. Conf. Blockchain Technol.*, Mar. 2019, pp. 66–69.

AMAD ALNAHDI was born in 1978. He received the bachelor's degree in computing field from Salalah College of Education, Oman, in 2002, and the master's degree in computer engineering from the European University of Lefke, North Cyprus, in 2015. He is currently pursuing the Ph.D. degree in computer engineering with Budapest University of Technology and Economics, Budapest, Hungary.

LÁSZLÓ TOKA (Member, IEEE) received the Ph.D. degree from Telecom ParisTech, in 2011. He was with Ericsson Research, from 2011 to 2014. He joined the academia with a research focus on software-defined networking, cloud computing, and artificial intelligence. He is currently an Associate Professor with Budapest University of Technology and Economics, the Vice-Head of the HSN Laboratory, and a member of the HUN-REN-BME Network Cloud Applications Research Group.