UDC 004.9:004.72 **doi:** https://doi.org/10.20998/2522-9052.2024.2.08

Heorhii Kuchuk, Eduard Malokhvii

National Technical University “Kharkiv Polytechnic Institute”, Kharkiv, Ukraine

INTEGRATION OF IOT WITH CLOUD, FOG, AND EDGE COMPUTING: A REVIEW

Abstract. Purpose of review. The paper provides an in-depth exploration of the integration of Internet of Things (IoT) technologies with cloud, fog, and edge computing paradigms, examining the transformative impact on computational architectures. **Approach to review.** Beginning with an overview of IoT's evolution and its surge in global adoption, the paper emphasizes the increasing importance of integrating cloud, fog, and edge computing to meet the escalating demands for real-time data processing, low-latency communication, and scalable infrastructure in the IoT ecosystem. The survey meticulously dissects each computing paradigm, highlighting the unique characteristics, advantages, and challenges associated with IoT, cloud computing, edge computing, and fog computing. The discussion delves into the individual strengths and limitations of these technologies, addressing issues such as latency, bandwidth consumption, security, and data privacy. Further, the paper explores the synergies between IoT and cloud computing, recognizing cloud computing as a backend solution for processing vast data streams generated by IoT devices. **Review results**. Challenges related to unreliable data handling and privacy concerns are acknowledged, emphasizing the need for robust security measures and regulatory frameworks. The integration of edge computing with IoT is investigated, showcasing the symbiotic relationship where edge nodes leverage the residual computing capabilities of IoT devices to provide additional services. The challenges associated with the heterogeneity of edge computing systems are highlighted, and the paper presents research on computational offloading as a strategy to minimize latency in mobile edge computing. Fog computing's intermediary role in enhancing bandwidth, reducing latency, and providing scalability for IoT applications is thoroughly examined. Challenges related to security, authentication, and distributed denial of service in fog computing are acknowledged. The paper also explores innovative algorithms addressing resource management challenges in fog-IoT environments. **Conclusions.** The survey concludes with insights into the collaborative integration of cloud, fog, and edge computing to form a cohesive computational architecture for IoT. The future perspectives section anticipates the role of 6G technology in unlocking the full potential of IoT, emphasizing applications such as telemedicine, smart cities, and enhanced distance learning. Cybersecurity concerns, energy consumption, and standardization challenges are identified as key areas for future research.

Keywords: Internet of Things; Cloud Computing; Fog Computing; Edge Computing; Distributed Computing; Hybrid Computing; Computational Architecture; Data Processing; IoT Applications; Scalability.

Introduction

The Internet of Things (IoT) is emerging as a pivotal advancement within the realm of Artificial Intelligence (AI), signifying a stride towards a transformative paradigm in contemporary society [1]. In this context, the term “things” pertains to tangible devices, thereby constituting a network comprised of sensors and processors facilitating data communication among these devices [2]. Within this network, two categories of nodes exist: physical nodes and virtual nodes. Physical nodes encompass sensors, actuators, transit nodes, and other wearable or embedded devices, while virtual nodes comprise virtual machines or networks utilized within wireless networks.

The architecture of IoT encompasses various components such as sensors, protocols, actuators, cloud services, and layers. The three layers within this architecture play a pivotal role in data evaluation, insights generation, identification of industrial risks, and prompt problem resolution for interconnected devices. These tasks are accomplished through the integration of three distinct architectures: cloud, fog, and edge computing. Cloud computing architecture facilitates IoT device analytics and monitoring by delivering essential application-specific services across diverse functional domains. In contrast, fog and edge computing architectures are imperative for enabling real-time data processing and computation at the network's periphery [3]. Termed utility computing, the cloud computing architecture offers flexible network access, delivering scalable, Quality of Service (QoS)-ensured services as needed.

Despite distinct developmental trajectories, the convergence of IoT and cloud computing gives rise to the conceptual framework known as the Cloud of Things. Predicated on foundational components, the IoT cloud paradigm manifests an augmented array of concurrent connectivity options, exerting an influence on the latency associated with the reception of IoT device data from the cloud system [4]. Device-to-cloud interfaces assume the role of data transmission endpoints that facilitate the exchange of information between cloud services and IoT devices. Consequently, the amalgamation of cloud and IoT services has the potential to optimize resource utilization under certain circumstances. While cloud providers facilitate seamless data transfer over the internet, thereby simplifying data navigation, fog computing empowers IoT devices to engage in processing, decision-making, and subsequent transmission of pertinent data to the cloud.

The functional alignment between fog and edge computing architectures, both serving as augmenters of cloud-based data transmission, is discernible in various scenarios, notwithstanding nuanced disparities. Fog computing operates as an intermediary between the edge and the cloud, whereas edge computing prioritizes data processing [5].

Notably, fog computing additionally facilitates the enhancement of services and the refinement of user interfaces, exemplified by accelerated responses tailored for time-sensitive applications. While cloud computing stands as a prominent approach for the analysis and derivation of results from vast datasets within the IoT, it is not without limitations, prompting exploration into mitigating solutions offered by fog and edge architectures. Recent years have seen a proliferation of studies underscoring the inadequacies of IoT systems reliant solely on a singular architecture, whether it be cloud, fog, or edge computing, as they tend to exhibit suboptimal responsiveness and limited capacity to extract actionable insights from data in real time. Notably, the evolution of edge and fog computing has been driven by the imperative to enhance the synergy between the cloud and IoT, redistributing data processing resources to the peripheries of data sources, in addition to the conventional cloud infrastructure.

The authors of many papers reported that the layered and collaborative edge–fog–cloud topology offers significant advantages since it allows the dispersion of intelligence and computation [6]. The combination of cloud, fog, and edge architecture can therefore be viewed as aiding IoT by enhancing data computation allocation and minimizing network traffic, resulting in improved operational efficiency.

Despite the integration of the three computing architectures, certain sectors within computing networks continue to grapple with several challenges. These challenges encompass issues such as faults in 5G network infrastructure, inaccuracies in data storage within industrial IoT, challenges related to resource allocation, errors in optimization processes, heightened energy consumption, and complexities in business and service models, among other concerns [7].

In the current era characterized by rapid communication systems, the role of IoT technology is indispensable across various domains, including e-commerce, industrial infrastructure, data security, the formulation of innovative business models, and other sectors.

Despite the considerable progress made in numerous IoT applications in recent years, it is crucial to recognize that the technology is still in its formative stages. This early stage of development may contribute to the persistence of the aforementioned challenges.

1. Existing IoT Architectures

Proficiency in navigating any computer network necessitates a comprehensive understanding of its underlying technology. Given that IoT devices operate within resource constraints, the services they offer necessitate adherence to stringent criteria, with security emerging as the paramount concern. Consequently, a nuanced comprehension of the fundamental architecture of IoT and its associated elements is imperative to comprehend and comply with these standards. The architecture of IoT functions as a mechanism for the flow of data from sensors embedded in “things” to a central data center or the cloud, traversing a network for processing, analysis, and storage. In the context of IoT, a “thing” may encompass structures, machines, buildings, or even human entities [8]. It is conceptualized as a virtual, physical, or hybrid system comprising various functional components such as physical objects, actuators, sensors, cloud services, bespoke IoT protocols, users, developers, communication layers, and an enterprise layer. Specialized architects play a pivotal role in the IoT infrastructure, offering a systematic approach to diverse components that culminate in solutions to interconnected problems [9].

To date, several IoT architectures have been devised, including but not limited to three-layer, four-layer, five-layer, cloud-based, Service Oriented Architecture (SOA), fog-based, and software-defined network (SDN)-based architectures [2].

Predominantly, IoT systems are cloud-based and widely accessible, with Amazon Web Services (AWS) leading the commercial cloud industry, providing an extensive array of data processing services such as AWS Lambda, Amazon S3, Amazon SQS, Amazon Kinesis, Amazon DynamoDB, and Amazon SNS. Microsoft Azure IoT Hub is another noteworthy example, featuring a reference architecture comprised of core platform services and software modules, facilitating device connectivity, analytics, data processing and management, data presentation, and business affinity. Various studies have also highlighted additional platforms, including OpenMTC, FIWARE, etc [10].

1.1. Three-layer architecture

The optimal convergence of communication and information systems at the highest speed, while ensuring authenticity and security, relies heavily on the efficiency of the IoT architecture layer. One of the prominent and foundational IoT architectures is the three-layer model (Fig. 1), comprising the perception, network, and application layers. While this architecture is practical and feasible in its implementation, it falls short of providing a comprehensive solution due to the intricate nature of IoT [11].

1.1.1. Perception layer. The perception layer, situated at the bottom and also referred to as the control layer, is primarily concerned with object recognition and the collection of data from users, requested services, and the surrounding environment. It incorporates detection equipment such as RFID, bar codes, distance sensors, and various physical objects, with the selection of monitoring devices contingent upon the specific service requirements [12].

Equipped with sensing capabilities, this layer captures signals from the environment, encompassing smart entities.

Following data collection, the perception layer conducts initial data processing and packaging, receiving control signals from the network layer to execute the necessary control actions through executive devices. Included within this layer are data sensors like Wireless Sensor Network (WSN), Reactive Sensor Network (RSN), Radio Frequency Identification (RFID), and actuators [13].

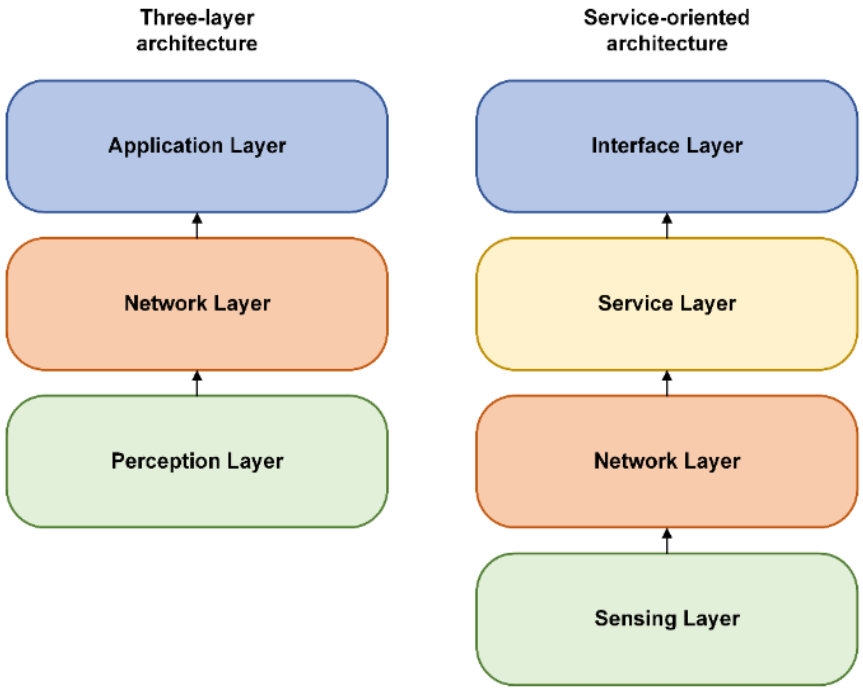

Fig. 1. Three-layer architecture and service-oriented architecture of IoT

The primary objectives of the perception layer are to detect distinct objects and engage with the received information, encompassing parameters such as humidity, location, vibration, air dust levels, pH levels, wind speed, and other variables. Subsequently, this data is transmitted through the network layer to the central information processing system for secure interaction. A significant portion of terminals instantaneously accumulates essential information and communicates it to users or forms assessments on various entities. Perception terminals face significant challenges, including the risk of secret information leakage, terminal viruses, tampering, and unauthorized copying [14]. Given that RFIDs and sensors constitute the bulk of the IoT perception layer, their constrained power consumption, storage capacity, and computational capabilities render them susceptible to diverse attacks and threats. Addressing these security concerns may involve the implementation of encryption, confidentiality measures, authentication mechanisms, and access control protocols.

1.1.2. Network layer. The network layer, often referred to as the transmission layer, serves as an intermediary, connecting the application and perception layers within the IoT architecture. Analogous to the human brain and neural network, this layer operates as a conduit, transporting data from physical objects and disseminating it through sensors. The transmission methods employed by this layer can be either wired or wireless, utilizing protocols such as Wi-Fi, 3G, UMTS, Infrared, WiMAX, Satellite, Bluetooth, and ZigBee [15].

Additionally, the network layer assumes responsibility for establishing connections among network devices, smart entities, and various networks. As a consequence, the network layer encounters significant security vulnerabilities, particularly in terms of data integrity and authentication, making it highly susceptible to various types of attacks, including:

- Denial of Service (DoS) attack obstructs authorized users' access to devices and other network resources [16].
- Man-in-the-Middle (MitM) attack poses a significant threat to online security, as it enables a hacker to intercept and manipulate data in real-time. This occurs when an attacker clandestinely intercepts or modifies the communication between a sender and recipient [17].
- In a Storage Attack, hackers target both the cloud and storage devices housing users' information, subsequently introducing erroneous modifications to the stored data. The susceptibility to threats increases when data undergo reproduction and exposure to other data by multiple individuals [18].

1.1.3. Application layer. The application layer, positioned at the top of the IoT architecture, is responsible for analyzing information sourced from the network and perception layers, ultimately generating the IoT application. Its role extends to providing application-specific support to the user. This layer defines diverse implementations for deploying IoT, such as in smart homes, smart health, smart eyewear, smart cities, and smart vehicles. It serves as the interface between IoT and various users, whether individuals or systems, with specialized needs to realize a range of intelligent IoT applications, including intelligent traffic management, intelligent buildings, intelligent logistics, security monitoring, and vehicle navigation. Given that these IoT applications heavily involve the use of information technology, the application layer ensures the validity, integrity, and confidentiality of information [11]. However, a notable drawback of this architecture is the concentration of more activities within a single layer, posing challenges for updating individual or

multiple layers [18]. Several potential threats and challenges within the application layer include:

- Malicious Code Injection is an attack that involves exploiting end-user vulnerabilities to insert malevolent code, allowing the attacker to compromise the system and pilfer information from the user.
- DoS attacks on the application layer have evolved into more sophisticated forms. These attacks serve as a diversion, creating a smokescreen for cyber attackers to infiltrate the defensive systems and compromise user data privacy, all while misleading the victim into thinking the attack is transpiring elsewhere.
- Spear-Phishing Attack is a form of e-mail spamming that targets the victim with enticing emails, aiming to lure them into opening the message, thereby providing the attacker with access to their credentials.
- In a Sniffing Attack, a hacker can install sniffer software to capture network information, potentially leading to system corruption and unauthorized access [19].

1.2. Service-oriented architecture

Service-Oriented Architecture (SOA) is a paradigm of application frameworks in which software components employ a communication protocol to serve over a network. This architectural approach enables the modeling of extensive software platforms utilizing web services, where computational components or sub-software are distributed across multiple remote servers catering to various users. SOA unifies distributed, individually controlled, and deployed software components [20]. Despite the flexibility offered by SOA, challenges persist in scaling, integrating, and fortifying resilience within IoT systems. A critical factor contributing to this integration challenge in IoT systems is the absence of an intelligent connection-aware infrastructure. While IoT is gaining popularity across various fields, the seamless integration of the physical and virtual worlds remains a substantial challenge. SOA lacks a precise definition due to its interpretation by various scholars from multiple perspectives, including technology, architecture, and business [21]. It is neither a technology, product, nor a quick solution for addressing IT complexity; instead, it is perceived as a complex system, well-defined simple entity, or a collection of subsystems. The reusable and independently manageable nature of the hardware and software components in IoT allows for effective reuse and enhancement of these subsystems [22]. In the context of SOA, the three core modules are the service provider, service requester, and service registry. These components collectively contribute to the orchestration and delivery of services within the SOA framework.

The description of SOA having four layers (Sensing, Network, Service, and Interface) with distinct characteristics and fostering device interoperability is not accurate. SOA typically refers to Service-Oriented Architecture, which is an architectural style for designing and building software applications. It is not traditionally divided into layers named Sensing, Network, Service, and Interface [20]. However, the rest of the information appears to describe the functionality of the sensing layer in IoT architecture, which is different from SOA. In IoT architecture, the sensing layer is indeed responsible for gathering information from various objects, applying identification mechanisms like IP addresses or Universal User Identifiers (UUIDs), and forwarding this data to the network layer for further processing. Considerations such as size, energy consumption, resources, deployment, accessibility, retrievability, and cost are indeed crucial when designing the sensor layer in IoT system [22].

The network layer functions as the foundational component for facilitating data transfer via both wireless and wired connections [23]. Its primary role is to ensure the smooth transmission of data within an IoT system. In contrast, the service layer is tasked with constructing and managing connections based on user and client requests. This layer plays a pivotal role in executing various service-oriented operations, encompassing tasks such as information exchange, data storage, ontology databases, communication, and search engines. The implementation of these operations adheres to standards set by different organizations, ensuring the fulfillment of requirements. Within a practical service layer, essential components include application programming interfaces (APIs), a suite of necessary applications, and protocols that support mandatory services and applications. Despite this, there is an increasing need for a universal service layer in IoT architecture to foster seamless interoperability. Meanwhile, the application layer, also known as the interface layer, focuses on data formatting and presentation. This layer encompasses mechanisms for interacting with programs, users, and other applications, incorporating information about communication strategies [20].

Services based on SOA are extensively employed in the development of large enterprises, playing a pivotal role in the domain of IoT. With the continuous emergence of new and evolving resources on the internet within the context of IoT, research focusing on SOA-based fusion applications holds significant value. Numerous studies have explored the application of SOA in various sectors, including healthcare, agriculture, activity recognition, decision-making, and the military. Some research papers recognize SOA as a primary driver of IoT [24], asserting that the integration of IoT services with SOA enhances the creation of value-added and intricate IoT applications by combining atomic services to offer distinct features [25]. Despite its recognized benefits, SOA faces challenges, including high expenses, substantial overhead, and complex service management.

2. Cloud, Edge and Fog computing architectures

IoT establishes a framework for universal computing, enabling devices with distinct addressing systems to communicate and exchange data seamlessly [8]. This unique capability allows for the interconnection of both things and individuals utilizing these devices under various conditions, regardless of

location, time, or entities involved. The communication and interaction facilitated by IoT extend to any system, network, path, service, or mode of communication. In essence, the architecture of cloud computing facilitates communication between devices and applications in the IoT, supporting device-to-device and app-to-app interactions. Additionally, fog and edge computing architectures serve as extensions of cloud networks [4]. These architectures are characterized by decentralized networks composed of a collection of computers, enhancing the scalability and efficiency of IoT communication and computation.

2.1. Cloud computing

Cloud computing offers a suite of computer services, including servers, networks, software, databases, and data analytics, delivered over the internet. It provides rapid deployment and flexible tools and resources, constituting a software system primarily application based [26]. Data is stored on remote servers accessible worldwide via the internet, and these services are administered by third-party organizations. Cloud computing operates through diverse service models and deployment methods tailored to meet the specific needs of customers. In terms of deployment methods, the cloud encompasses private, community, public, and hybrid models, catering to private users, the general public, single organizations, and multiple organizations, respectively [27]. This versatility makes cloud computing infrastructure advantageous for a broad user base. Key attributes of cloud computing include on-demand services, a substantial resource pool, mobility, scalability, and multitenancy, all packaged in a cost-effective solution, rendering it suitable for both public and organizational use. Despite its merits, some researchers have highlighted potential drawbacks in cloud computing. Concerns include the possibility of critical components being unavailable during times of need due to regional and business regulations. Additionally, the shared resource concept may pose risks to security, integrity, and confidentiality. Nevertheless, cloud computing has demonstrated its advantages in diverse fields such as e-learning, e-governance, research, and data storage [27].

In cloud computing, the inherent lack of trustworthiness in cloud servers necessitates ensuring the confidentiality of information and classifiers. Addressing this concern, a paradigm for privacy-preserving outsourced classification has been developed [28]. This paradigm incorporates a proxy homomorphic encryption mechanism based on Gentry’s scheme, designed to safeguard sensitive data. In this mechanism, multiple data suppliers outsource fully homomorphic ciphertexts (encrypted data) to the evaluator (“S”), responsible for storing and processing these ciphers. The collaboration between the evaluator “S” and the cryptographic service provider results in the creation of a classification algorithm that operates on data encrypted with distinct public keys. This model is subsequently encrypted and stored in evaluator “S”, serving as a basis for providing clients with a secure prediction platform.

The proposed algorithm has demonstrated semantic efficiency in both the encryption and prediction of data, ensuring security. However, the scheme lacks clarity in illustrating the interaction between the cryptographic service provider (CSP) and evaluator “S”, and the communication cost is deemed less favorable.

In the realm of cloud computing, the diverse array of service providers poses a significant challenge for enterprises in selecting an appropriate cloud service that aligns with their requirements. In response to this challenge, a neutrosophic multi-criteria decision analysis (NMCDA) method [29], grounded in the analytic hierarchy process (AHP), has been proposed for evaluating the quality of various cloud services. This method assists clients in estimating different cloud services by considering various factors crucial for evaluating a service provider. The selection of a multi-criteria decision analysis approach is motivated by the need to account for multiple factors in the evaluation of a service provider. In a previous study, researchers engaged a panel of expert decision-makers and enhanced the consistency degree of the metric by modeling an induced bias matrix within a neutrosophic setting. The cloud service estimation method employed triangular neutrosophic numbers, with various linguistic variables in the comparison matrices representing these numbers. As a result, the proposed neutrosophic multi-criteria decision analysis method offers several advantages in handling unclear and inconsistent data, with many organizations confirming its practical applicability. However, given its novelty, the level of adoption by companies remains low, and the broader assessment of its results is yet to be fully determined.

2.2. Edge computing

Edge computing is a comprehensive platform that integrates network, processing, storage, and application capabilities at the edge of a network, physically proximate to the data source [30]. The location where edge analysis occurs is termed an edge node, which can be positioned anywhere between the data-generating source and the central cloud with processing and network capabilities [31]. In practical use cases, mobile phones and gateways have been cited as examples of edge nodes [32]. T

he first type connects an individual to the cloud center, while the second links a smart home to the cloud center. The functionality of edge computing involves three layers: the end layer, cloud layer, and edge layer. The cloud layer, the initial layer, is responsible for scheduling both nodes and cloud computing centers, adhering to a control policy for efficient client service. Unlike other paradigms, it ensures that data and computing are shared within the network during decision-making rather than being transmitted to a central server. Researchers highlighted the pivotal role of the edge layer, serving as the focal point for all nodes and extending cloud services to the network's edge, connecting both the cloud and the end layer. This layer is continuously involved in transferring information to the cloud layer and fulfills low latency and high traffic

demand through three essential functions: data caching, localization computing, and wireless access. The end layer, the final tier closest to end-users and comprising devices, takes the data from these devices and forwards it to the other layers for processing [33].

Edge computing operates both at the network's edge and within the network itself. By distributing tasks among edge nodes and cloud centers, edge computing effectively reduces the data load on the central cloud, enhancing security. The approach is inherently more secure because it diminishes the level and volume of data exposed to potential risks, with the majority of data processed on edge nodes rather than centralized cloud centers. Consequently, any data compromise at the end devices has a limited impact on the centralized data. This decentralized processing also alleviates the data burden on cloud centers, contributing to an improved overall data flow [34].

While edge computing presents notable advantages, some researchers have discussed its underutilization in service management and proposed enhancements in cloud computing related to service management, data abstraction, and user security. One suggested improvement involves implementing a standardized naming scheme for applications, ensuring a consistent structure and service methodology in edge computing. This is deemed necessary for effective communication, programming, addressing, object identification, and data transmission.

Additionally, there is a need for advancements in programmability within edge computing due to the presence of heterogeneous edge nodes in the network, making application deployment challenging for users within this paradigm.

In contemporary applications, edge computing finds utility in diverse domains, including mobile and data safety, attack detection, privacy preservation, vehicle and transportation safety, and resource management [35]. Additionally, it is employed in real-time and context-aware scenarios such as emergency healthcare and service recommendations. Despite its prevalent use, edge computing, like other data distribution and storage systems, faces challenges related to the growing volumes of data in today's digital era. To address concerns about latency-aware data distribution at the edge of a network, researchers [36] have proposed a distributed information dissemination strategy. This strategy relies on the dynamic creation, replacement, and removal of data replicas through continuous analysis of data requests received from edge network nodes. The process [36] comprises two versions, namely the source and edge versions. The source version operates solely in the node housing the central storage, producing copies of data items in that proximate node. On the other hand, the edge version operates in nodes with at least one copy, being deactivated when no replicas remain, and includes a messaging system for replica location. The results indicate that the proposed model achieves a 26% reduction in delay with a 14% lower incremental cost compared to nonreplicated data sources with client-side caching. Moreover, communication inefficiencies and misunderstanding errors induced by replica deployment and detection are deemed insignificant. However, the proposed scheme lacks assurance in real-time performance, which may limit its effectiveness in scenarios such as emergency healthcare systems or self-driving cars.

In the context of edge computing, the transportation of massive data at the edge introduces latency, conflicting with the immediacy required by many ubiquitous applications. To address this challenge, a data management technique has been introduced for edge computing environments, which separates the task of data placement from “task scheduling” [37].

This scheme employs a multi-level scheduler that allocates data to the system’s resource providers, considering various contextual factors. The scheduler assigns tasks based on the current context and continuously monitors the system’s state during runtime. The system dynamically adjusts the number of data copies to optimize the trade-off between execution latency and additional expenditure for data management.

The context-aware multi-level scheduler integrates four data placements, three task scheduling, and three runtime adaptation methods. Results indicated that a context-aware replication technique, coupled with task scheduling based on performance awareness and dynamically changing runtime adaptation, outperforms existing models. This combined approach achieved a task response time comparable to complete replication but with reduced data overhead. While promising, this approach has not yet been widely implemented to evaluate its full efficacy at scale.

2.3. Fog computing

The architecture of fog computing encompasses computing, processing, storage, and networking services distributed across multiple end devices, marking a departure from traditional cloud computing [38]. It serves as a conduit that brings the cloud and end devices into closer proximity, achieved by deploying computing, storage, and networking resources in close proximity to end devices [39]. In essence, fog computing complements cloud computing by performing some processing tasks near the edge of the network, proximate to end-users. This paradigm operates on a topology characterized by geographically dispersed nodes that execute computational tasks while providing networking and storage functions [39]. The devices integrated into the network are termed fog nodes and can be deployed wherever there is a network connection. To qualify as a fog node, a device must fulfill three essential functions: computing, storage, and connectivity [40].

Fig. 2 shows the difference in the combination of cloud and edge computing architectures with or without for computing architecture. Consequently, the effective implementation of an IoT solution, representing a fully integrated bundle of technologies aimed at addressing a problem or creating new organizational value, requires the utilization of all three architectures — cloud, fog, and edge.

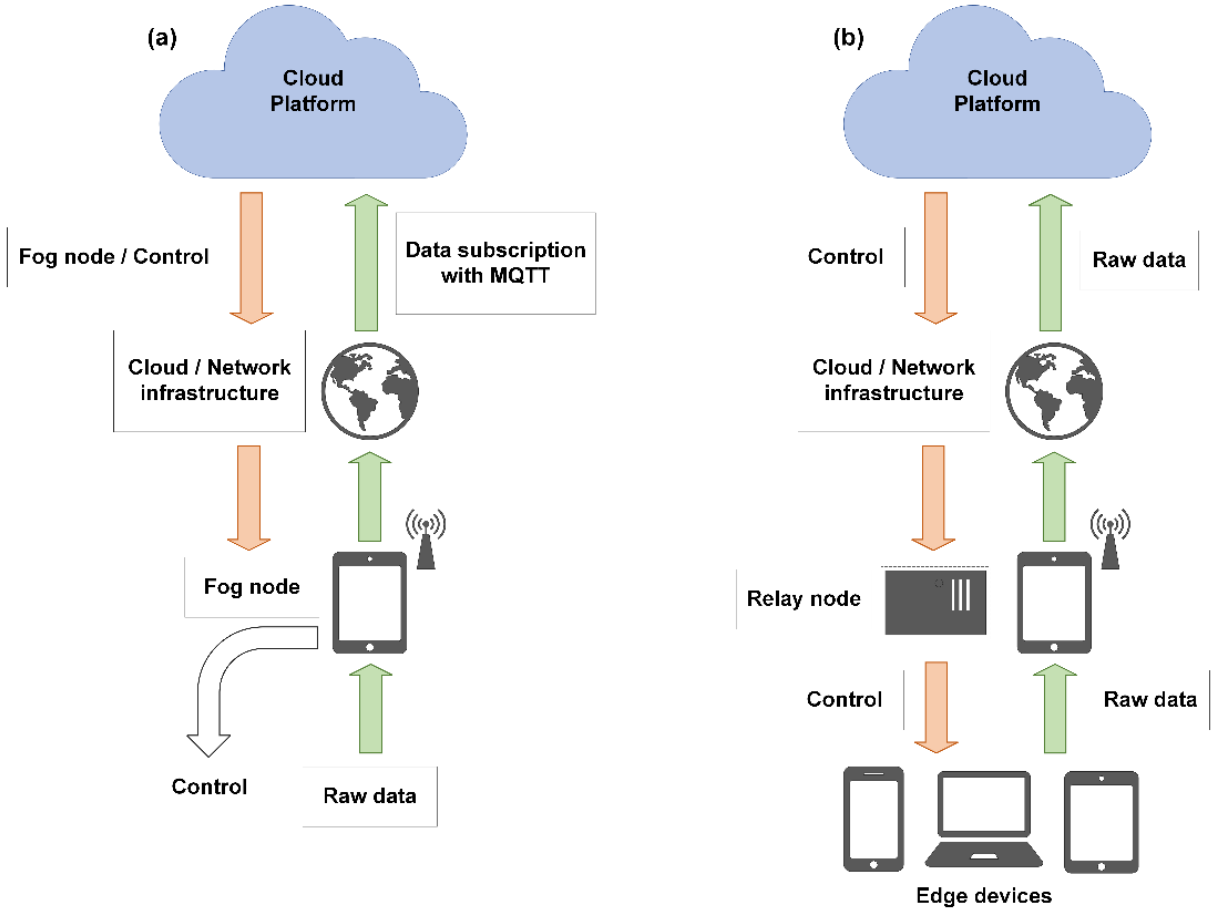

Fig. 2. Combination of cloud-edge computing architecture (a) with and (b) without fog computing architecture

Fog computing serves as an intermediary system, contributing to enhanced bandwidth and privacy by processing and responding to data locally, thereby reducing the volume of data transmitted to the central data center [40].

This approach also minimizes latency by operating in close proximity to end-users and creates opportunities for scalability. However, the proximity to the edge of the network introduces challenges, including susceptibility to intruder attacks, authentication issues, and distributed denial of service [5]. While fog computing finds applications in diverse fields such as healthcare systems, service improvement, web optimizations, road safety, video processing for surveillance, micro-data center resource management, and data processing, it encounters delays in execution time due to inefficient task scheduling and resource distribution for user tasks. To address this challenge, an innovative bio-inspired hybrid algorithm [41] has been proposed for resource management in the fog-IoT paradigm.

This approach incorporates modified particle swarm optimization (MPSO) for load distribution among fog nodes and modified cat swarm optimization (MCSO) components for maintaining available fog resources. Contrary to conventional scheduling strategies for fog computing, the results of the proposed strategy show promise in reducing energy consumption, completion time, average reaction time, and cost. However, its application in a fog-IoT environment necessitates a reframing and reinforcement of the learning strategies within the suggested model.

In fog computing paradigms, where users' data is stored on cloud servers, concerns arise regarding loss of control over data and potential privacy issues. Traditional privacy and confidentiality protection solutions are often insufficient to prevent attacks within a cloud server. To address these challenges, a three-tier storage framework [42] has been proposed, aiming to maximize the utilization of cloud storage while safeguarding data privacy.

In this framework, data is stored on the cloud server, fog server, and the local device of a user. The user's device employs the Hash-Solomon code technique to encode data, preserving fragmented data and partitioning it into distinct sections for optimal storage utilization.

Computational intelligence is utilized to estimate the distribution proportion stored on the fog, cloud, and local devices [3]. Among various coding matrices, the Cauchy matrix was identified as the most efficient. Test results indicate that this approach can successfully execute the encoding and decoding processes without compromising cloud storage efficiency, making it a potentially effective solution for maintaining security. However, the efficiency of the coding matrix with

extensive data and real-time scenarios has not been thoroughly analyzed, posing potential challenges such as storage efficiency impact and latency concerns.

3. IoT integration with cloud, fog and edge computing

The proliferation of IoT technologies has ushered in a transformative era, permeating diverse sectors with unprecedented connectivity and data generation. In tandem with this IoT revolution, the integration of cloud, fog, and edge computing has emerged as a pivotal paradigm, reshaping the landscape of computational architecture [3]. This integration represents a strategic response to the escalating demands for real-time data processing, low-latency communication, and scalable infrastructure in the IoT ecosystem.

3.1. IoT integration with cloud computing

The integration of IoT and cloud computing addresses the distinctive characteristics of each technology, aiming to leverage the strengths of both to overcome individual limitations [43]. IoT involves interconnected smart devices globally, often characterized by dispersed devices with limited processing and storage capabilities, along with potential challenges related to privacy, performance, and security [44]. On the other hand, cloud computing offers virtually unlimited resources, making it suitable for addressing technological constraints in data processing, communication, and storage. Researchers have recognized the potential synergies between IoT and cloud computing, proposing the Cloud-IoT paradigm to explore the integration of these technologies [45]. This paradigm aims to harness the flexibility and distributed nature of the cloud to manage and orchestrate IoT services, developing applications and services that make use of generated data. The cloud, in turn, benefits from IoT by expanding its capabilities to interact with physical entities in a more flexible and distributed manner. The cloud can act as an intermediary layer between models and applications, simplifying implementation and enhancing overall functionality. While studies have conducted comprehensive evaluations of the integration, some challenges and platform availability for implementing the Cloud-IoT paradigm have been highlighted [46]. However, open-platform issues were not thoroughly investigated or included in the study, leaving room for further exploration and analysis in this evolving technological landscape.

The integration of cloud computing and IoT is a subject of significant research, with studies focusing on various elements such as cloud infrastructure, platforms, and IoT middleware to create a cohesive Cloud of Things paradigm [47]. This integrated approach is seen as a solution to address constraints related to data analysis, accessibility, and computation in the context of IoT. Research has demonstrated the potential benefits of integrating cloud computing with IoT, particularly in enhancing the capabilities of embedded IoT devices. The study emphasizes the use of technologies like RFID and WSAN for information exchange and highlights how cloud computing can alleviate limitations associated with these IoT-related devices. Security concerns have been a major focus in the integration of IoT and cloud computing systems. Researchers have conducted surveys to identify common security issues and proposed algorithm models incorporating encryption methods like Rivest-Shamir-Adleman (RSA) and Advanced Encryption Standard (AES) to address these concerns. However, the long-term effectiveness of these algorithms in overcoming complex security challenges remains a topic for further exploration. While some studies have provided overviews of the development of IoT integration with cloud computing, emphasizing areas like frameworks, platforms, architecture, and middleware, challenges related to standardization and handling complex data have been acknowledged [3]. However, there is room for additional research to address other challenges and contribute to the advancement of this integrated paradigm.

3.2. IoT integration with fog computing

The integration of fog computing with IoT offers significant benefits for a variety of applications, particularly in reducing latency and enabling real-time communication among IoT devices. This integration is crucial for time sensitive IoT applications where responsiveness is a key factor [48]. Fog computing addresses challenges in existing IoT systems and provides solutions to improve efficiency and performance [49]. Research has highlighted the advantages of integrating fog computing with IoT in diverse applications such as automotive control, financial trading, and achieving low-latency communication between control modes and sensors [50]. This integration is particularly relevant for managing networks, systems, and end-user applications. Additionally, the study emphasized how fog based IoT can contribute to network scalability and enhance Radio Access Network (RAN) performance. However, challenges related to the decentralized nature of fog computing were not fully addressed in the discussed study. The constant failure of fog-based devices could pose difficulties, leading to disruptions in user activities, software, and hardware. Further research may be needed to explore strategies for mitigating these challenges and ensuring the reliability and resilience of fog based IoT systems.

Several research papers delve into the challenges and considerations related to mobility support within fog based IoT systems, particularly in the context of mobile IoT devices leveraging fog computing [51]. These studies explore potential obstacles and present three distinct scenarios illustrating the integration of IoT with fog computing, emphasizing the critical need for mobility support. Future research directions are proposed to address mobility challenges, encompassing proactive and reactive service migration, appropriate virtualization selection, and migration strategies aimed at enhancing performance and implementing effective mobility support. The exploration of integrating 5G

mobile networks is identified as a promising avenue for advancing fog-based mobility support systems. However, these studies may overlook challenges associated with mobilization and system management. Additionally, another set of researchers focuses on identifying security-related issues in existing fog computing models within IoT applications [52]. The findings reveal a tendency among applications to prioritize functionality over security, leaving various fog-based platforms vulnerable. Research concentrates on assessing the impact and significance of security challenges, proposing potential solutions for future security-based approaches in fog computing. Notably, research tends to neglect system-level difficulties intrinsic to fog computing, including aspects of service-oriented computing and resource management.

3.3. IoT integration with edge computing

There is a noticeable evolution in both IoT and edge computing systems, and the integration of these technologies has become crucial for addressing complex challenges and enhancing performance. IoT, with its demand for rapid responses, extensive computational requirements, and substantial storage needs, finds a suitable ally in edge computing [53]. Edge computing provides the necessary computational capacity, storage space, and quick response times required by IoT applications. In this symbiotic relationship, IoT can contribute to enhancing the structure of edge computing frameworks, ensuring compatibility with the flexibility of edge computing nodes. Edge nodes, in turn, can leverage devices with residual computing capability or IoT-based devices to provide additional services [54]. While some studies have explored the use of cloud computing to support IoT, edge computing often outperforms cloud computing, especially as the number of IoT devices continues to rise. In one experiment, researchers evaluated edge computing and its relevance to mobile gaming technologies, focusing on a resource-intensive three-dimensional application [55]. The study demonstrated the significance of edge computing in meeting latency requirements for augmented and virtual reality systems. However, the study did not address the integration challenges associated with edge computing systems, which are characterized by heterogeneity. Edge computing, involving various platforms, servers, and network topologies, can be complex to program and manage resources and data transmission effectively across diverse applications running on heterogeneous platforms [56].

Edge computing plays a crucial role in addressing the latency issues inherent in IoT systems. Latency, or delay, in applications is influenced by two main components: computing latency, which is the time required to process data, and computing capability [57]. Transmission of data between servers and embedded devices introduces transmission latency [58]. Over the past decade, numerous studies have sought solutions to minimize the latency of IoT systems by integrating edge computing. One notable approach involves computational offloading in mobile edge computing systems [59]. This scheme identifies suitable virtual machines on mobile devices to efficiently execute tasks, resulting in reduced execution time and power consumption. The outcome is energy savings and a decrease in transmission delay through edge networks [60]. While this approach has shown promising results in recognizing various online activities, further research is necessary to assess the broader applicability of the proposed framework.

The substantial amount of data generated by IoT, owing to the increasing number of sensors, poses challenges for direct transmission to cloud servers without compression or processing. Transmitting this massive data volume to remote cloud servers without addressing transmission delays would require extensive network bandwidth [61].

To overcome this challenge, IoT gateways perform data pre-processing and aggregation before transmitting data to cloud servers. The goal is to efficiently manage traffic flow by automating data processing, reducing end-user bandwidth requirements, and preserving data quality [62].

Several studies have addressed bandwidth issues in IoT. For instance, researchers proposed an extension to the framework for stream processing by deploying edge computing [63].

This extended architecture considers interactions with users, databases, and other entities, referred to as topology-external interactions.

The proposed architecture aims to reduce bandwidth usage and eliminate latency violations. However, ongoing research is essential to further reduce bandwidth consumption in the context of cloud-to-edge computing.

4. Advantages and challenges of IoT integration with Cloud, Edge and Fog computing

The integration of IoT and cloud computing brings together two powerful and evolving technologies, each with unique characteristics. IoT comprises devices connected through a global network, characterized by a dynamic infrastructure, while cloud computing boasts massive processing capacity and almost unlimited storage [64]. IoT, however, faces challenges such as limited processing ability and storage, which can be effectively addressed by integrating it with cloud computing [47]. The synergy between IoT and cloud computing proves beneficial in overcoming the limitations of IoT. Cloud computing can handle large-scale data generated by billions of connected IoT devices due to its expansive storage capabilities. Moreover, the integration of IoT with the cloud opens new possibilities for creating innovative services and products by leveraging real-world scenarios [65]. Despite the advantages, challenges arise in integrating IoT with cloud services. One prominent issue is the unreliable handling of real-world data from IoT devices when transmitted to cloud computing through cloud based IoT. Privacy concerns have become a critical issue due to the lack of strict guidelines and regulations, posing a threat to user privacy [66]. Addressing these challenges is essential to ensure the secure and efficient integration of IoT with cloud computing services.

Edge computing offers significant advantages in handling vast amounts of data, services, and computational applications, allowing for the decentralization of processing capabilities from the central hub to the edge of the network [53]. This approach leverages existing resources efficiently, managing and storing data while enabling control over various activities. In the context of IoT, edge computing becomes a valuable asset by optimizing pooled edge computing resources. The key benefit of edge computing lies in its ability to process data and store information in close proximity to end-users. This proximity facilitates faster and cost-effective data experimentation within an IoT-integrated edge computing system, enabling quick decision-making. However, the limitation of edge computing is its restricted remote usability and comparatively lower computational capabilities when compared to cloud computing [67].

Integrating IoT with cloud computing has gained popularity due to its capabilities in big data storage and accessibility. However, this combination also comes with certain challenges, particularly when it comes to handling time-sensitive applications within IoT, such as video gaming, simulations, and streaming [68]. To address these challenges, fog computing, integrated with IoT, can serve as a solution. Fog computing extends cloud computing capabilities to the edge of the network, connecting IoT devices with a diverse range of cloud computing resources. With its substantial storage capacity and robust data processing capabilities, fog computing acts as an intermediary layer between IoT devices and traditional cloud services. By providing a virtualized environment for processing, memory, and networking devices, fog computing integrated with IoT becomes adept at managing time-sensitive applications, offering significant benefits to IoT devices [69].

Fog computing addresses latency issues crucial for time-sensitive applications by facilitating instant interaction among IoT devices [5]. Its ability to scale and adapt to the growing IoT network, connecting billions of devices, is a key advantage. However, continuous adjustment of the workflow structure in response to dynamic changes in IoT can pose challenges. The efficacy of IoT may be impacted if fog computing struggles to support this dynamic nature [70]. Additionally, factors such as software and hardware degradation in portable devices can lead to changes in workflow behavior and device attributes. Thus, fog nodes may require sophisticated and automated modifications to their topological structure and resources. The random dispersal of fog nodes at the edge adds complexity to the fog networking architecture [71].

Conclusions

IoT is a rapidly evolving technology that enables the processing of large amounts of data for intelligent decision-making without human intervention. It represents a new generation of technology marked by automation and the development of artificially intelligent devices. The enabling technologies of IoT facilitate the practical implementation of IoT systems and solutions. As of 2021, there were more than 10 billion active IoT devices [72], and predictions suggest that by 2025, applications will expand to cover smart grids and smart cities, with the number of active IoT devices exceeding 25.4 billion by 2030 [72].

IoT contributes to increased data collection efficiency, helping organizations operate more effectively by reducing human errors. The integration of IoT with cloud, fog, and edge computing is becoming increasingly prevalent, providing a range of supporting technologies to achieve successful integration. IoT is considered a crucial concept for the future internet, envisioned as a set of data communication network technologies that will bring together seamless networks and networked things into a single global IT platform.

Cloud computing is seen as a backend solution for processing large data streams in a future where everything is connected through seamless networks. According to the 5G Observatory Quarterly Report of 2021, there was a 41% increase in global IoT-supported 5G connections, with 124 million new connections added between Q1 and Q2 of 2021.

This growth is attributed to the increasing usage of IoT accessed through the cloud.

Researchers highlight the critical stage of development for fog computing, emphasizing its potential to reduce operational costs and address concerns within IoT, such as latency, storage, and data traffic. The fog computing architecture is seen as essential for providing a smart platform capable of managing the distributed and real-time properties of future IoT networks [73]. Moreover, the integration of edge computing architecture into IoT, along with cloud and fog computing, is considered a solution to challenges in seamless networks. The edge computing architecture is expected to play a significant role in the future of IoT by connecting a vast number of devices generating massive data at high speeds. This integration aims to enhance efficiency, minimize latency, consume less bandwidth, and improve security. The focus is on real-time applications of IoT that demand immediate responses. Consequently, the upcoming 6th generation networking system is anticipated to greatly benefit from the integration of IoT with edge computing.

6G technology holds the potential to bring about revolutionary advancements across various industries and is considered a key enabler for unlocking the full potential of IoT. The integration of IoT in the context of 6G is envisioned to manifest in applications such as holographic teleportation, telemedicine for remote healthcare, smart cities, autonomous transportation systems, enhanced opportunities for distance learning, brain-computer interfaces, and other advanced technologies [74].

The anticipated widespread adoption of smart devices, coupled with advancements in low-cost architecture, communication technologies, and data capabilities, is expected to propel IoT from a visionary concept to practical reality. However, it is crucial to acknowledge and address the cybersecurity risks associated with IoT devices, which have been a concern over the past decades. Many IoT devices lack robust

security features and are not designed to address vulnerabilities through regular updates, exposing networks to potential risks. To tackle these issues, collaboration is needed to establish and adhere to open standards, ensuring the reliability, compatibility, and secure delivery of IoT services. Additionally, efforts should be directed towards implementing techniques that minimize energy consumption, incorporating green technology to enhance the energy efficiency of IoT devices. By addressing these challenges associated with IoT integration, advancements in terms of speed, security, and overall performance can be achieved, contributing to the realization of the potential benefits offered by 6G technology [75].

The surveyed literature highlights the transformative impact of the IoT technological revolution on future quality of life, cultural diversity, and human-device interactions. As IoT integrates with cloud, fog, and edge computing, new business models and opportunities are expected to emerge. However, the successful functioning of IoT services and devices depends on well-designed underlying network infrastructure. Companies, regardless of size, are investing in IoT projects to harness its potential for improving system efficiency, effectiveness, and communication. For example, the Cloud of Things, which combines IoT and cloud computing, has the potential to address and alleviate limitations in data analysis, accessibility, and computation. Edge computing is recognized for outperforming cloud computing in various scenarios, and the integration between edge computing and IoT is expected to grow as the number of IoT devices increases.

Edge computing provides the necessary computational power, storage space, and response time to meet the requirements of IoT applications. Fog computing integrated with IoT presents a promising solution to challenges posed by cloud computing, especially in managing time sensitive IoT applications. This integration minimizes data transfers and communication delays to the cloud, addressing issues related to gaming, simulation, and streaming. Additionally, fog computing can effectively manage applications in areas like automotive, aviation financial trading, and ensure low-latency communication between control modes and sensors. The integration of fog computing with IoT involves incorporating various cloud computing hardware into the IoT infrastructure, providing significant data processing capabilities. With its ability to bring cloud computing to the network's edge, fog computing proves advantageous as the number of connected IoT devices continues to increase exponentially. However, adapting the workflow of IoT to changing circumstances remains a challenge, and further research is needed to enhance the seamless integration of fog computing with evolving IoT systems.

Acknowledgements

The study was funded by the National Research Foundation of Ukraine in the framework of the research project 2022.01/0017 on the topic "Development of methodological and instrumental support for Agile transformation of the reconstruction processes of medical institutions of Ukraine to overcome public health disorders in the war and post-war periods".

References

1. Seng, K. P., Ang, L. and Ngharamike, E. (2022), "Artificial intelligence Internet of Things: A new paradigm of distributed sensor networks", *International Journal of Distributed Sensor Networks*, 18(3), 155014772110628, doi: https://doi.org/10.1177/15501477211062835
2. Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H. and Zhao, W. (2017), "A survey on Internet of things: architecture, enabling technologies, security and privacy, and applications", *IEEE Internet of Things Journal*, vol. 4(5), pp. 1125–1142, doi: https://doi.org/10.1109/jiot.2017.2683200
3. De Donno, M., Tange, K. and Dragoni, N. (2019), "Foundations and evolution of modern computing paradigms: cloud, IoT, edge, and FOG", *IEEE Access*, vol. 7, pp. 150.936–150.948, doi: https://doi.org/10.1109/access.2019.2947652
4. Alhaidari, F., Rahman, A. and Zagrouba, R. (2020), "Cloud of Things: architecture, applications and challenges", *Journal of Ambient Intelligence and Humanized Computing*, vol. 14(5), pp. 5957–5975, doi: https://doi.org/10.1007/s12652-020-02448-3
5. Atlam, H. F., Walters, R. J. and Wills, G. (2018), "Fog Computing and the Internet of Things: a review", *Big Data and Cognitive Computing*, vol. 2(2), doi: https://doi.org/10.3390/bdcc2020010
6. Alwakeel, A. M. (2021), "An overview of fog computing and edge computing security and privacy issues", *Sensors*, vol. 21(24), 8226, doi: https://doi.org/10.3390/s21248226
7. Li, S., Da Xu, L. and Zhao, S. (2018), "5G Internet of Things: A survey", *Journal of Industrial Information Integration*, vol. 10, pp. 1–9, doi: https://doi.org/10.1016/j.jii.2018.01.005
8. Weyrich, M. and Ebert, C. (2016), "Reference architectures for the Internet of things", *IEEE Software*, vol. 33(1), pp. 112–116, doi: https://doi.org/10.1109/ms.2016.20
9. Ray, P. P. (2018), "A survey on Internet of Things architectures", *Journal of King Saud University - Computer and Information Sciences*, vol. 30(3), pp. 291–319, doi: https://doi.org/10.1016/j.jksuci.2016.10.003
10. Pierleoni, P., Concetti, R., Belli, A. and Palma, L. (2020), "Amazon, Google and Microsoft Solutions for IoT: Architectures and a Performance comparison", *IEEE Access*, vol. 8, pp. 5455–5470, doi: https://doi.org/10.1109/access.2019.2961511
11. Sethi, P. and Sarangi, S. R. (2017), "Internet of Things: architectures, protocols, and applications", *Journal of Electrical and Computer Engineering*, pp. 1–25, doi: https://doi.org/10.1155/2017/9324035
12. Rghioui, A., Sendra, S., Lloret, J. and Oumnad, A. (2016), "Internet of things for measuring human activities in ambient assisted living and e-Health", *Network Protocols and Algorithms*, vol. 8(3), p. 15, doi: https://doi.org/10.5296/npa.v8i3.10146
13. Landaluce, H., Arjona, L., Perallos, A., Falcone, F., Angulo, I. and Muralter, F. (2020), "A review of IoT sensing applications and challenges using RFID and wireless sensor networks", Sensors, vol. 20(9), 2495, doi: https://doi.org/10.3390/s20092495

14. Vashi, S., Ram, J., Modi, J., Verma, S. and Prakash, C. (2017), "Internet of Things (IoT): A vision, architectural elements, and security issues", *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)* (I-SMAC), doi: https://doi.org/10.1109/i-smac.2017.8058399
15. Ngu, A. H. H., Gutiérrez, M., Metsis, V., Nepal, S. and Sheng, Q. Z. (2016), "IoT Middleware: A Survey on Issues and Enabling technologies", *IEEE Internet of Things Journal*, vol. 1, doi: https://doi.org/10.1109/jiot.2016.2615180
16. Patil, S. B. and Chaudhari, S. (2016), "DOS attack prevention technique in wireless sensor networks", *Procedia Computer Science*, vol. 79, pp. 715–721, doi: https://doi.org/10.1016/j.procs.2016.03.094
17. Conti, M., Dragoni, N. and Lesyk, V. (2016), "A survey of Man in the middle attacks", *IEEE Communications Surveys and Tutorials*, vol. 18(3), pp. 2027–2051, doi: https://doi.org/10.1109/comst.2016.2548426
18. Ahmid, M. and Kazar, O. (2021), "A comprehensive review of the Internet of things security", *Journal of Applied Security Research*, vol. 18(3), pp. 289–305, doi: https://doi.org/10.1080/19361610.2021.1962677
19. Farooq, M. U., Waseem, M., Khairi, A. and Mazhar, S. (2015), "A critical analysis on the security concerns of internet of things (IoT)", *International Journal of Computer Applications*, vol. 111(7), pp. 1–6, doi: https://doi.org/10.5120/19547-1280
20. Gião, J., Nazarenko, A. A., Ferreira, F., Gonçalves, D. and Sarraipa, J. (2022), "A framework for Service-Oriented Architecture (SOA)-Based IoT application development", *Processes*, vol. 10(9), 1782, doi: https://doi.org/10.3390/pr10091782
21. Uviase, O. and Kotonya, G. (2018), "IoT Architectural Framework: connection and integration framework for IoT systems", *arXiv* (Cornell University), vol. 264, pp. 1–17, doi: https://doi.org/10.4204/eptcs.264.1
22. Maurya, S. and Mukherjee, K. (2019), "An Energy Efficient Architecture of IoT based on Service Oriented Architecture (SOA)", *Informatica*, vol. 43(1), doi: https://doi.org/10.31449/inf.v43i1.1790
23. Li, S., Tryfonas, T. and Li, H. (2016), "The Internet of Things: a security point of view", *Internet Research*, vol. 26(2), pp. 337–359, doi: https://doi.org/10.1108/intr-07-2014-0173
24. Chen, I., Guo, J. and Bao, F. (2016), "Trust Management for SOA-Based IoT and its application to service composition", *IEEE Transactions on Services Computing*, vol. 9(3), pp. 482–495, doi: https://doi.org/10.1109/tsc.2014.2365797
25. Wang, F., Hu, L., Zhou, J. and Zhao, K. (2015), "A data processing middleware based on SOA for the Internet of things", *Journal of Sensors*, pp. 1–8, doi: https://doi.org/10.1155/2015/827045
26. Gomathi, B., Balaji, B., Kumar, V. R., Abouhawwash, M., Aljahdali, S., Masud, M. and Kuchuk, N. (2022), "Multi-Objective optimization of energy aware virtual machine placement in cloud data center", *Intelligent Automation and Soft Computing*, vol. 33(3), pp. 1771–1785, doi: https://doi.org/10.32604/iasc.2022.024052
27. Petrovska, I., Kuchuk, H. and Mozhaiev, M. (2022), "Features of the distribution of computing resources in cloud systems", *2022 IEEE 3rd KhPI Week on Advanced Technology (KhPIWeek)*, doi: https://doi.org/10.1109/khpiweek57572.2022.9916459
28. Li, P., Li, J., Huang, Z., Gao, C., Chen, W. and Chen, K. (2017), "Privacy-preserving outsourced classification in cloud computing", *Cluster Computing*, vol. 21(1), pp. 277–286, doi: https://doi.org/10.1007/s10586-017-0849-9
29. Abdel-Basset, M., Mohamed, M. and Chang, V. (2018), "NMCDA: A framework for evaluating cloud computing services", *Future Generation Computer Systems*, vol. 86, pp. 12–29, doi: https://doi.org/10.1016/j.future.2018.03.014
30. Wang, R., Yan, J., Wang, D., Wang, H. and Yang, Q. (2018), "Knowledge-Centric edge computing based on virtualized D2D communication systems", *IEEE Comm. Magazine*, vol. 56(5), pp. 32–38, doi: https://doi.org/10.1109/mcom.2018.1700876
31. Khatatneh, K., Nawafleh, O. and Al-Utaibi, D. (2020), "The Emergence of Edge Computing Technology over Cloud Computing", *International Journal of P2P Network Trends and Technology*, vol. 10(2), pp. 1–5, doi: https://doi.org/10.14445/22492615/ijptt-v10i2p401
32. Rimal, B. P., Van, D. P. and Maier, M. (2017), "Cloudlet enhanced Fiber-Wireless access networks for Mobile-Edge Computing", *IEEE Transactions on Wireless Communications*, vol. 16(6), pp. 3601–3618, doi: https://doi.org/10.1109/twc.2017.2685578
33. Wang, F., Xu, J., Wang, X. and Cui, S. (2018), "Joint offloading and computing optimization in wireless powered Mobile-Edge computing systems", *IEEE Transactions on Wireless Communications*, vol. 17(3), pp. 1784–1797, doi: https://doi.org/10.1109/twc.2017.2785305
34. Qiu, T., Chi, J., Zhou, X., Ning, Z., Atiquzzaman, M. and Wu, D. (2020), "Edge Computing in Industrial Internet of Things: architecture, advances and challenges", *IEEE Communications Surveys and Tutorials*, vol. 22(4), pp. 2462–2488, doi: https://doi.org/10.1109/comst.2020.3009103
35. Khan, W. Z., Ahmed, E., Hakak, S., Yaqoob, I. and Ahmed, A. (2019), "Edge computing: A survey", *Future Generation Computer Systems*, vol 97, pp. 219–235, doi: https://doi.org/10.1016/j.future.2019.02.050
36. Yin, Y. and Deng, L. (2022), "A dynamic decentralized strategy of replica placement on edge computing", *International Journal of Distributed Sensor Networks*, vol.18(8), 155013292211150, doi: https://doi.org/10.1177/15501329221115064
37. Breitbach, M., Schäfer, D., Edinger, J. and Becker, C. (2019), "Context-Aware Data and Task Placement in Edge Computing Environments", *2019 IEEE Int. Conf. Pervasive Comput. Commun. PerCom*, doi: https://doi.org/10.1109/percom.2019.8767386
38. Verma, M., Bhardwaj, N. and Yadav, A. K. (2016), "Real time efficient scheduling algorithm for load balancing in FOG computing environment", *International Journal of Information Technology and Computer Science*, vol. 8(4), pp. 1–10, doi: https://doi.org/10.5815/ijitcs.2016.04.01
39. Hunko, M., Tkachov, V., Kovalenko, A. and Kuchuk, H. (2023), "Advantages of Fog Computing: A Comparative Analysis with Cloud Computing for Enhanced Edge Computing Capabilities", *2023 IEEE 4th KhPI Week on Advanced Technology*, KhPI Week 2023 - Conference Proceedings, 02-06 October 2023, Code 194480, doi: https://doi.org/10.1109/khpiweek61412.2023.10312948
40. Kraemer, F. A., Bråten, A. E., Tamkittikhun, N., & Palma, D. (2017), "FOG Computing in Healthcare–A Review and Discussion, *IEEE Access*, vol. 5, pp. 9.206–9.222, doi: https://doi.org/10.1109/access.2017.2704100
41. Rafique, H., Shah, M. A., Islam, S. U., Maqsood, T., Khan, S. and Maple, C. (2019), "A novel Bio-Inspired Hybrid Algorithm (NBIHA) for efficient resource management in Fog computing", *IEEE Access*, vol. 7, pp. 115.760–115.773, doi: https://doi.org/10.1109/access.2019.2924958

42. Wang, T., Zhou, J., Chen, X., Wang, G., Liu, A. and Liu, Y. (2018), "A Three-Layer privacy preserving cloud storage scheme based on computational intelligence in FOG computing", *IEEE Transactions on Emerging Topics in Computational Intelligence*, vol. 2(1), pp. 3–12, doi: https://doi.org/10.1109/tetci.2017.2764109
43. Petrovska, I. and Kuchuk, H. (2023), "Adaptive resource allocation method for data processing and security in cloud environment", *Advanced Information Systems*, vol. 7, is. 3, pp. 67–73, doi: https://doi.org/10.20998/2522-9052.2023.3.10
44. Dang, L. M., Piran, M. J., Han, D., Min, K. and Moon, H. (2019), "A survey on internet of things and cloud computing for healthcare", *Electronics*, vol. 8(7), 768, doi: https://doi.org/10.3390/electronics8070768
45. Darwish, A., Hassanien, A. E., Elhoseny, M., Sangaiah, A. K. and Muhammad, K. (2017), "The impact of the hybrid platform of internet of things and cloud computing on healthcare systems: opportunities, challenges, and open problems", *Journal of Ambient Intelligence and Humanized Computing*, vol. 10(10), pp. 4151–4166, doi: https://doi.org/10.1007/s12652-017-0659-1
46. Botta, A., De Donato, W., Persico, V. and Pescapè, A. (2016), "Integration of Cloud computing and Internet of Things: A survey", *Future Generation Computer Systems*, vol. 56, pp. 684–700, doi: https://doi.org/10.1016/j.future.2015.09.021
47. Díáz, M., Martin, C. L. and Rubio, B. (2016), "State-of-the-art, challenges, and open issues in the integration of Internet of things and cloud computing", *Journal of Network and Computer Applications*, vol. 67, pp. 99–117, doi: https://doi.org/10.1016/j.jnca.2016.01.010
48. Liu, Y., Fieldsend, J. E. and Min, G. (2017), "A framework of FOG Computing: architecture, challenges, and optimization", *IEEE Access*, vol. 5, pp. 254.45–254.54, doi: https://doi.org/10.1109/access.2017.2766923
49. Kuchuk, N., Mozhaiev, O., Haichenko, A., Semenov, S., Kuchuk, H., Tiulieniev, S., Mozhaiev, M., Davydov, V., Brusakova, O. and Gnusov, Y. (2023), "Devising a method for balancing the load on a territorially distributed foggy environment", *Eastern-European Journal of Enterprise Technologies*, vol. 1(4 (121)), pp. 48–55, doi: https://doi.org/10.15587/1729-4061.2023.274177
50. Chiang, M. and Zhang, T. (2016), "Fog and IoT: An Overview of Research Opportunities", *IEEE Internet of Things Journal*, vol. 3(6), pp. 854–864, doi: https://doi.org/10.1109/jiot.2016.2584538
51. Puliafito, C., Mingozzi, E. and Anastasi, G. (2017), "Fog Computing for the Internet of Mobile Things: Issues and Challenges", *2017 IEEE Int. Conf. Smart Comput*, doi: https://doi.org/10.1109/smartcomp.2017.7947010
52. Khan, S., Parkinson, S. and Qin, Y. (2017), "Fog computing security: a review of current applications and security solutions*", Journal of Cloud Computing*, vol. 6(1), doi: https://doi.org/10.1186/s13677-017-0090-3
53. Hamdan, S., Ayyash, M. and Almajali, S. (2020), "Edge-Computing Architectures for Internet of Things Applications: A survey", *Sensors*, vol. 20(22), 6441, doi: https://doi.org/10.3390/s20226441
54. Li, Y., Qi, F., Wang, Z., Yu, X. and Shao, S. (2020), "Distributed edge Computing offloading algorithm based on deep reinforcement learning", *IEEE Access*, vol. 8, pp. 85.204–85.215, doi: https://doi.org/10.1109/access.2020.2991773
55. Premsankar, G., Di Francesco, M. and Taleb, T. (2018), "Edge Computing for the Internet of Things: a case study", *IEEE Internet of Things Journal*, vol/ 5(2), pp. 1275–1284, doi: https://doi.org/10.1109/jiot.2018.2805263
56. Xue, H., Huang, B., Qin, M., Zou, H. and Yang, H. (2020), "Edge Computing for Internet of Things: A Survey", *2020 Int. Conf. Internet Things IEEE Green Comput. Commun. IEEE Cyber*, Phys. Soc. Comput. IEEE Smart Data IEEE Congr. Cybermatics, IEEE, doi: https://doi.org/10.1109/ithings-greencom-cpscom-smartdata-cybermatics50389.2020.00130
57. Ketykó, I., Kecskes, L. J., Nemes, C. and Farkas, L. (2016), "Multi-user computation offloading as Multiple Knapsack Problem for 5G Mobile Edge Computing", *2016 Eur. Conf. Networks Commun.*, IEEE, doi: https://doi.org/10.1109/eucnc.2016.7561037
58. Liu, J., Mao, Y., Zhang, J. and Letaief, K. B. (2016), "Delay-optimal computation task scheduling for mobile-edge computing systems", *2016 IEEE Int. Symp. Inf. Theory*, IEEE, doi: https://doi.org/10.1109/isit.2016.7541539
59. Rehman, M. H. U., Sun, C., Wah, T. Y., Iqbal, A. and Jayaraman, P. P. (2016), "Opportunistic Computation Offloading in Mobile Edge Cloud Computing Environments", *2016 17th IEEE Int. Conf. Mob. Data Manag.*, IEEE, doi: https://doi.org/10.1109/mdm.2016.40
60. Wang, Y., Sheng, M., Wang, X., Wang, L. and Li, J. (2016), "Mobile-Edge computing: Partial computation offloading using dynamic voltage scaling" *IEEE Transactions on Communications*, 1, doi: https://doi.org/10.1109/tcomm.2016.2599530
61. Abdelwahab, S., Hamdaoui, B., Guizani, M. and Znati, T. (2016). Replisom: Disciplined Tiny Memory Replication for Massive IoT Devices in LTE Edge Cloud. IEEE Internet of Things Journal, 3(3), 327–338, doi: https://doi.org/10.1109/jiot.2015.2497263
62. Kuchuk, N., Ruban, I., Zakovorotnyi, O., Kovalenko, A., Shyshatskyi, A. and Sheviakov, I. (2023), "Traffic Modeling for the Industrial Internet of NanoThings", *2023 IEEE 4th KhPI Week on Advanced Technology*, KhPI Week 2023 - Conference Proceedings, 194480, doi: https://doi.org/10.1109/khpiweek61412.2023.10312856
63. Παπαγεωργιου, A., Poormohammady, E. and Cheng, B. (2016), "Edge-Computing-Aware Deployment of Stream Processing Tasks Based on Topology-External Information: Model, Algorithms, and a Storm-Based Prototype", *2016 IEEE Int. Congr. Big Data*, doi: https://doi.org/10.1109/bigdatacongress.2016.40
64. Zhou, J., Leppänen, T., Harjula, E., Ylianttila, M., Ojala, T., Chen, Y., Jin, H. and Yang, L. T. (2013), "CloudThings: A common architecture for integrating the Internet of Things with Cloud Computing", *2013 IEEE 17th Int. Conf. Comput. Support. Coop. Work Des. CSCWD 2013*, doi: https://doi.org/10.1109/cscwd.2013.6581037
65. Suciu, G., Vulpe, A., Halunga, S., Fratu, O., Todoran, G. and Suciu, V. (2013), "Smart Cities Built on Resilient Cloud Computing and Secure Internet of Things", *19th Int. Conf. Control Syst. Comput. Sci. CSCS 2013*, doi: https://doi.org/10.1109/cscs.2013.58
66. Atlam, H. F., Alenezi, A., Alharthi, A., Walters, R. J. and Wills, G. (2017), "Integration of Cloud Computing with Internet of Things: Challenges and Open Issues", *2017 IEEE Int. Conf. Internet Things*, IEEE Green Comput. Commun. IEEE Cyber, Phys. Soc. Comput. IEEE Smart Data, doi: https://doi.org/10.1109/ithings-greencom-cpscom-smartdata.2017.105
67. Naveen, S. and Kounte, M. R. (2019), "Key Technologies and challenges in IoT Edge Computing", *2019 Third International Conference on I-SMAC* (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), doi: https://doi.org/10.1109/i-smac47947.2019.9032541
68. Mouradian, C., Naboulsi, D., Yangui, S., Glitho, R., Morrow, M. and Polakos, P. (2018), "A comprehensive survey on FoG Computing: State-of-the-Art and Research challenges", *IEEE Communications Surveys and Tutorials*, vol. 20(1), pp. 416–464, doi: https://doi.org/10.1109/comst.2017.2771153

69. Agarwal, S., Yadav, S. and Yadav, A. K. (2016), “An efficient architecture and algorithm for resource provisioning in Fog computing”, *International Journal of Information Engineering and Electronic Business*, vol. 8(1), pp. 48–61, doi: https://doi.org/10.5815/ijieeb.2016.01.06
70. Luan, T. H., Gao, L., Li, Z., Xiang, Y., Wei, G. and Sun, L. (2015), “Fog Computing: focusing on mobile users at the edge”, *arXiv* (Cornell University), doi: https://doi.org/10.48550/arxiv.1502.01815
71. Sabireen, H. and Venkataraman, N. (2021), A” Review on Fog Computing: Architecture, Fog with IoT, Algorithms and Research Challenges”, *ICT Express*, vol. 7(2), pp. 162–176, doi: https://doi.org/10.1016/j.icte.2021.05.004
72. Majid, M., Habib, S., Javed, A. R., Rizwan, M., Srivastava, G., Gadekallu, T. R. and Lin, J. C. (2022), “Applications of wireless sensor networks and Internet of Things Frameworks in the Industry Revolution 4.0: A Systematic Literature review”, *Sensors*, vol. 22(6), 2087, doi: https://doi.org/10.3390/s22062087
73. Gedeon, J., Brandherm, F., Egert, R., Grube, T. and Mühlhäuser, M. (2019), “What the fog? Edge Computing revisited: promises, applications and future challenges”, *IEEE Access*, 7, pp. 152.847–152.878, doi: https://doi.org/10.1109/access.2019.2948399
74. Malik, U. M., Javed, M. A., Zeadally, S. and Islam, S. U. (2022). Energy-Efficient FOG Computing for 6G-Enabled Massive IoT: Recent trends and future opportunities. IEEE Internet of Things Journal, 9(16), 14572–14594, doi: https://doi.org/10.1109/jiot.2021.3068056
75. Imoize, A. L., Adedeji, O., Tandiya, N. and Shetty, S. (2021). 6G Enabled Smart Infrastructure for Sustainable Society: Opportunities, Challenges, and Research Roadmap. Sensors, 21(5), 1709, doi: https://doi.org/10.3390/s21051709

Received (Надійшла) 22.01.2024
Accepted for publication (Прийнята до друку) 24.04.2024

ВІДОМОСТІ ПРО АВТОРІВ/ ABOUT THE AUTHORS

Кучук Георгій Анатолійович – доктор технічних наук, професор, професор кафедри комп’ютерної інженерії та програмування, Національний технічний університет “Харківський політехнічний інститут”, Харків, Україна;
Heorhii Kuchuk – Doctor of Technical Sciences, Professor, Professor of Computer Engineering and Programming Department, National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine;
e-mail: kuchuk56@ukr.net; ORCID ID: http://orcid.org/0000-0002-2862-438X;
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=57057781300.

Малохвій Едуард Едуардович – аспірант, кафедра комп’ютерної інженерії та програмування, Національний технічний університет “Харківський політехнічний інститут”, Харків, Україна;
Eduard Malokhvii – PhD Student of Department of Computer Engineering and Programming Department, National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine;
e-mail: malokhvii.ee@gmail.com; ORCID ID: http://orcid.org/0009-0008-0311-6400.

Інтеграція IoT із хмарними, туманними та периферійними обчисленнями: огляд

Г. А. Кучук, Е. Е. Малохвій

Анотація. Мета огляду. Стаття містить поглиблене дослідження інтеграції технологій Інтернету речей (IoT) із парадигмами хмарних, туманних і периферійних обчислень, досліджуючи трансформаційний вплив на обчислювальні архітектури. **Підхід до огляду**. Починаючи з огляду еволюції IoT та його стрімкого поширення в усьому світі, документ підкреслює зростаючу важливість інтеграції хмарних, туманних і периферійних обчислень для задоволення зростаючих вимог до обробки даних у реальному часі, зв’язку з низькою затримкою та масштабованої інфраструктури в екосистема IoT. Опитування ретельно аналізує кожну обчислювальну парадигму, підкреслюючи унікальні характеристики, переваги та проблеми, пов’язані з IoT, хмарними обчисленнями, периферійними обчисленнями та туманними обчисленнями. Обговорення заглиблюється в індивідуальні переваги та обмеження цих технологій, розглядаючи такі проблеми, як затримка, споживання пропускної здатності, безпека та конфіденційність даних. Крім того, у статті досліджується взаємодія між IoT і хмарними обчисленнями, визнаючи хмарні обчислення серверним рішенням для обробки великих потоків даних, створених пристроями IoT. **Результати огляду.** Визнаються проблеми, пов’язані з ненадійною обробкою даних і проблемами конфіденційності, наголошується на необхідності надійних заходів безпеки та нормативної бази. Досліджується інтеграція периферійних обчислень з IoT, демонструючи симбіотичні відносини, коли крайові вузли використовують залишкові обчислювальні можливості пристроїв IoT для надання додаткових послуг. Висвітлено проблеми, пов’язані з неоднорідністю периферійних обчислювальних систем, і в статті представлено дослідження обчислювального розвантаження як стратегії мінімізації затримки в мобільних периферійних обчисленнях. Проміжна роль Fog Computing у збільшенні пропускної здатності, зменшенні затримки та забезпеченні масштабованості для програм IoT ретельно досліджується. Визнаються проблеми, пов’язані з безпекою, автентифікацією та розподіленою відмовою в обслуговуванні в туманних обчисленнях. У документі також досліджуються інноваційні алгоритми вирішення проблем управління ресурсами в середовищах fog-IoT. **Висновки.** Опитування завершується розумінням спільної інтеграції хмарних, туманних і периферійних обчислень для формування цілісної обчислювальної архітектури для IoT. Розділ про перспективи передбачає роль технології 6G у розкритті повного потенціалу IoT, акцентуючи увагу на таких програмах, як телемедицина, розумні міста та покращене дистанційне навчання. Питання кібербезпеки, споживання енергії та проблеми стандартизації визначені як ключові сфери майбутніх досліджень.

Ключові слова: Інтернет речей; хмарні обчислення; туманні обчислення; периферійні обчислення; розподілені обчислення; гібридні обчислення; обчислювальна архітектура; обробка даних; програми IoT; масштабованість.