SN Computer Science (2021) 2:277
https://doi.org/10.1007/s42979-021-00677-7

SURVEY ARTICLE

Distributed Intelligence in the Internet of Things: Challenges and Opportunities

Tariq Alsboui[1] · Yongrui Qin[1] · Richard Hill[1] · Hussain Al-Aqrabi[1]

Received: 23 January 2021 / Accepted: 3 May 2021 / Published online: 19 May 2021

Abstract

Widespread adoption of smart IoT devices is accelerating research for new techniques to make IoT applications secure, scalable, energy-efficient, and capable of working in mission-critical use cases, which require an ability to function offline. In this context, the novel combination of distributed ledger technology (DLT) and distributed intelligence (DI) is seen as a practical route towards the decentralisation of IoT architectures. This paper surveys DI techniques in IoT and commences by briefly explaining the need for DI, by proposing a comprehensive taxonomy of DI in IoT. This taxonomy is then used to review existing techniques and to investigate current challenges that require careful attention and consideration. Based on the taxonomy, IoT DI techniques can be classified into five categories based on the factors that support distributed functionality and data acquisition: cloud-computing, mist-computing, distributed-ledger-technology, service-oriented-computing and hybrid. Existing techniques are compared and categorized mainly based on related challenges, and the level of intelligence supported. We evaluate more than thirty current research efforts in this area. We define many significant functionalities that should be supported by DI frameworks and solutions. Our work assists system architects and developers to select the correct low-level communication techniques in an integrated IoT-to-DLT-to-cloud system architecture. The benefits and shortcomings of different DI approaches are presented, which will inspire future work into automatic hybridization and adaptation of DI mechanisms. Finally, open research issues for distributed intelligence in IoT are discussed.

Keywords Internet of Things (IoT) · Distributed intelligence (DI) · Cloud-computing · Mist-computing · Distributed-ledger technology · Service-oriented-computing · Hybrid

Introduction

The Internet of Things or the IoT, is an emerging worldwide network of interconnected physical-heterogeneous smart objects (e.g., wearable-sensors, environmental sensors and connected devices) that are uniquely addressable, and are available through networking technologies such as WiFi, Bluetooth and others. By 2030, the study predicts that IoT will rise exponentially, for example, by about 125 billion connected devices to the internet [1–3]. As a result, this poses several challenges in terms of providing timely delivery, data volume, speed, confidentiality and scalability [4, 5].

There are several features available for IoT applications: First, *sensing* the environment; Second, *communication* between objects for efficient data transfer; and Third, *computation* typically carried out to produce necessary raw data information.

The advent of the IoT enables a new paradigm that binds the physical objects on the Internet to form pervasive networks that allow sensing and medicating environments to respond to dynamic stimuli [6], often known as cyber-physical systems (CPS) [7]. IoT was also demonstrated by the Auto-ID centre that immediately recognises physical objects in the supply chain via radio-frequency identification RFID technology and electronic goods codes (EBC). These systems have shown the ability to improve the way of living by

✉ Tariq Alsboui
tariq.alsboui@hud.ac.uk

Yongrui Qin
y.qin2@hud.ac.uk

Richard Hill
r.hill@hud.ac.uk

Hussain Al-Aqrabi
h.al-aqrabi@hud.ac.uk

[1] School of Computing and Engineering, University of Huddersfield, Huddersfield, UK

transforming traditional cities into *smart* cities [8], *smart* homes [9], smart regions, *smart* campuses [10].

Despite the fast adoption of IoT in industry, scalability, resilience, energy efficiency, and security, are the main challenges of adopting IoT [11]. In fact, the researchers reported [12] that security is one of the top ten IoT challenges along with challenging issues of privacy [13] and the security of devices [14].

Enhancing CPS capabilities to schedule, analyse, including solve goal-directed issues allows complex IoT systems to be managed and ultimately optimised [15]. Such systems often require significant computational power.

Given the potential benefits of distributed intelligence (DI), a number of issues related to general DI approaches, such as distrust, lack of scalability, energy-efficiency, and poor identification of potential participants, where the privacy of the participants still need to be solved [16]. Traditional approaches to DI, e.g., those using Cloud Computing, are inadequate for dynamic IoT environments. The vague clauses in cloud-computing service agreements and unclear technical specifications may result in consumers of cloud services to be unable to discover trustworthy cloud services. Consequently, DI in conjunction with DLT, has been proposed to address these kinds of issues.

DI technology support for IoT applications can be categorised into five broad categories: sloud-computing, mist-computing, distributed- ledger-technology, service-oriented-computing and hybrid. The major differences among these categories are described as follows. In cloud computing, DI processing functionality and data is controlled by single entities and only sent to the cloud for further processing. With mist computing, part of DI processing functionality and data is processed at the extreme edge of a network that typically consists of micro-controllers and sensors. By working at the extreme edge, mist computing can harvest resources such as computation and communication capabilities available on sensor nodes. With distributed ledger technology, the processing functionality and data is distributed among all participant nodes. With service-oriented computing, processing components are provided as services and distributed at all levels of the system. Eventually, the hybrid method is a combination of two or more of the four categories listed above.

Comparison with Other Related Surveys

In recent research, many proposed solutions have appeared to enable distributed intelligence in IoT with different application scenarios. Several survey articles have attempted to review DI approaches in varied degrees of depth and scopes. The authors in [17] have discussed the role of distributed intelligence in the automation domain. The main idea of their survey paper was the identification of applications, key product and service requirements. The authors in [18] have surveyed distributed intelligence from the perspective of Wireless Sensor Networks under eight themes, namely, coding, storage of data, allocation of channel, aggregation of data, etc, whereas we provide a comprehensive survey of the specific distributed intelligence approaches in the IoT.

A comprehensive survey that analyzes the use of edge computing in improving the performance of IoT networks is presented in [19]. It describes the strengths and limitations of edge computing and categorizes edge computing architectures into groups, whereas our survey article focuses on the challenges faced in support of distributed intelligence. A survey in [20] provides a detailed study with the aim of analyzing the existing and evolving edge computing architectures and techniques for smart healthcare. It focuses on edge intelligence that targets health data classifications with the tracking and identification of vital signs using state of the art deep learning techniques. The study also presents a comprehensive analysis of the use of cutting-edge artificial intelligence-based classification and prediction techniques employed for edge intelligence. In comparison, this article does not provide a survey on edge computing, however, this survey article reviews contributions that attempts to build a distributed intelligence techniques in IoT by utilizing various technologies, such as cloud-computing, and mist-computing.

Another detailed survey in [21], which focuses on the research efforts in edge intelligence. It overviews the background and motivation for artificial intelligence running at the network edge. They also review the architectures, frameworks, and emerging key technologies for deep learning model, whereas we primarily focuses on distributed intelligence in IoT, presenting main techniques, frameworks, and research approaches in the domain. We also compare more than thirty representative distributed intelligence approaches. Most recently, a comprehensive survey is presented in [22] in which the focus is on integrating edge computing and artificial intelligence, which is formed as edge intelligence. They divide Edge Intelligence into artificial intelligence for edge (intelligence-enabled edge computing) and artificial intelligence on edge (artificial intelligence on edge). In comparison, this survey article provides a new classifications of distributed intelligence approaches under five categories and evaluates each distributed intelligence approach according to the identified IoT technical challenges.

In the following, we summarise the contributions of this survey article.

- We present related distributed intelligence challenges in the IoT, and categorize distributed intelligence approaches into different groups including: cloud-computing, mist-computing, distributed-ledger-technology, service-oriented-computing, and hybrid.

- We compare and evaluate the performance of each distributed intelligence approach according to the IoT technical challenges in terms of resource constraints, scalability, security, privacy, offline capability, and interoperability.
- Based on thorough studies of distributed intelligence approaches, we discuss the potential ability for integrating components from several technologies, such as network function virtualization, multi-agent system, and distributed ledger technology to develop a new hybrid distributed intelligence approaches.

Reviewing the relevant literature to distributed intelligence are fourfold: (1) to understand how the DI framework can be used on top of the IoT infrastructure to build sustainable IoT applications; (2) to define the important roles of the optimal DI framework; (3) how we can apply DI techniques from several technologies to solve real-world issues in the IoT domain; and (4) to outline current challenges and present potential future directions for research with respect to developing DI approaches and platforms to support a broader range of application scenarios.

This paper is structured as follows: "Distributed Intelligence in the IoT" defines the inspiration and obstacles that underlie the use of DI in the IoT. We also briefly describe the need for DI. In "State-of-the-Art Distributed Intelligence in IoT", we present a summary of several representatives DI research deployments according to the following categorization: cloud-computing, mist-computing, distributed-ledger-technology (DLT), service-oriented-computing and hybrid, followed by an evaluation of DI approaches. In "Hardware-Based Security Primitives for IoT", we present hardware-based security primitives with recent approaches. In "Challenges and Opportunities", we discuss future research opportunities, followed by the conclusion in "Conclusions".

Distributed Intelligence in the IoT

In this section, we outline the DI and illustrate the need for DI in the IoT by identifying a number of the critical factors that determine the challenges of the IoT. We then explain how the IOTA platform may be used to achieve distributed intelligence. Furthermore, we categorise DI approaches into four broad categories, and cast these categories in a detailed taxonomy. Figure 1 graphically illustrates the dimensions we have identified. Note that, DI is one of the most critical efforts to use the ever-increasing amount of data brought back by IoT nodes deployed with sensors to achieve a detailed and expensive task of finding, analysing and identifying the information needed.

DI has the potential to overcome many of the IoT technical challenges, such as scalability, resource constraints, security, privacy, and offline capability [23]. DI involves the distribution of processing functionality, cooperation, and classification of data based on the type of information held, and is concerned with identifying where functionality should be invoked.

Additional intelligence is required to optimally service a range of IoT applications and user requirements. This intelligence applies not only to data processing, but also to security, privacy, network configuration, quality of service, and many more. There is therefore no single reliable place where this intelligence is triggered or placed. It can spread from the same devices to the Cloud/DLT/Fog according to the situation. It is expected that intelligence will be distributed through various locations to achieve maximum performance or functionality. In addition, this involves both in-network processing and networking elements. As a result, DI is defined as a sub-discipline of artificial intelligence, which allows processing functionality to be distributed, enables collaboration between smart objects, and mediates data exchange to optimise communication for IoT applications. This is a description of consciousness in which the term DI is used throughout this article.

The organisation of nodes plays a crucial role in DI as it defines, along with other factors, including (1) cost, which is the amount of energy needed to collect raw data, (2) accuracy, which is the level of coverage, and (3) reliability, which includes timeliness. The organisation of nodes may be either centralised or hierarchical, data gathered by all nodes is forwarded to a gateway (e.g., Raspberry Pi, Arduino) utilising single-hop or multi-hop communication in the centralised approach [24]. Nonetheless, there is lack of scalability in this approach, which is a critical concern for IoT applications. It is unreliable, and creates traffic bottlenecks and delays in transmission or congestion, particularly in areas across gateway nodes [8, 24]. In order to overcome the problems of centralised approaches, IOTA Tangle has been introduced as a promising solution to achieve a longer network lifetime and to provide better scalability [16].

We present a taxonomy of distributed intelligence approaches in IoT. Figure 1 depicts the whole taxonomy that describes the IoT challenges. Then, it presents DI intelligence levels as low-level and high-level focusing on processing functionality and data. Finally, distributed intelligence approaches are classified into five broad categories. The following paragraphs provide a full description about the dimensions that we have identified.

– Challenges: Connected IoT devices in the coming future lead to a number of fundamental challenges, e.g., resource constraints, scalability, energy efficiency, security, privacy, offline capability, and Interoperability [5, 25, 26] as well as the massive amount of data produced by IoT.

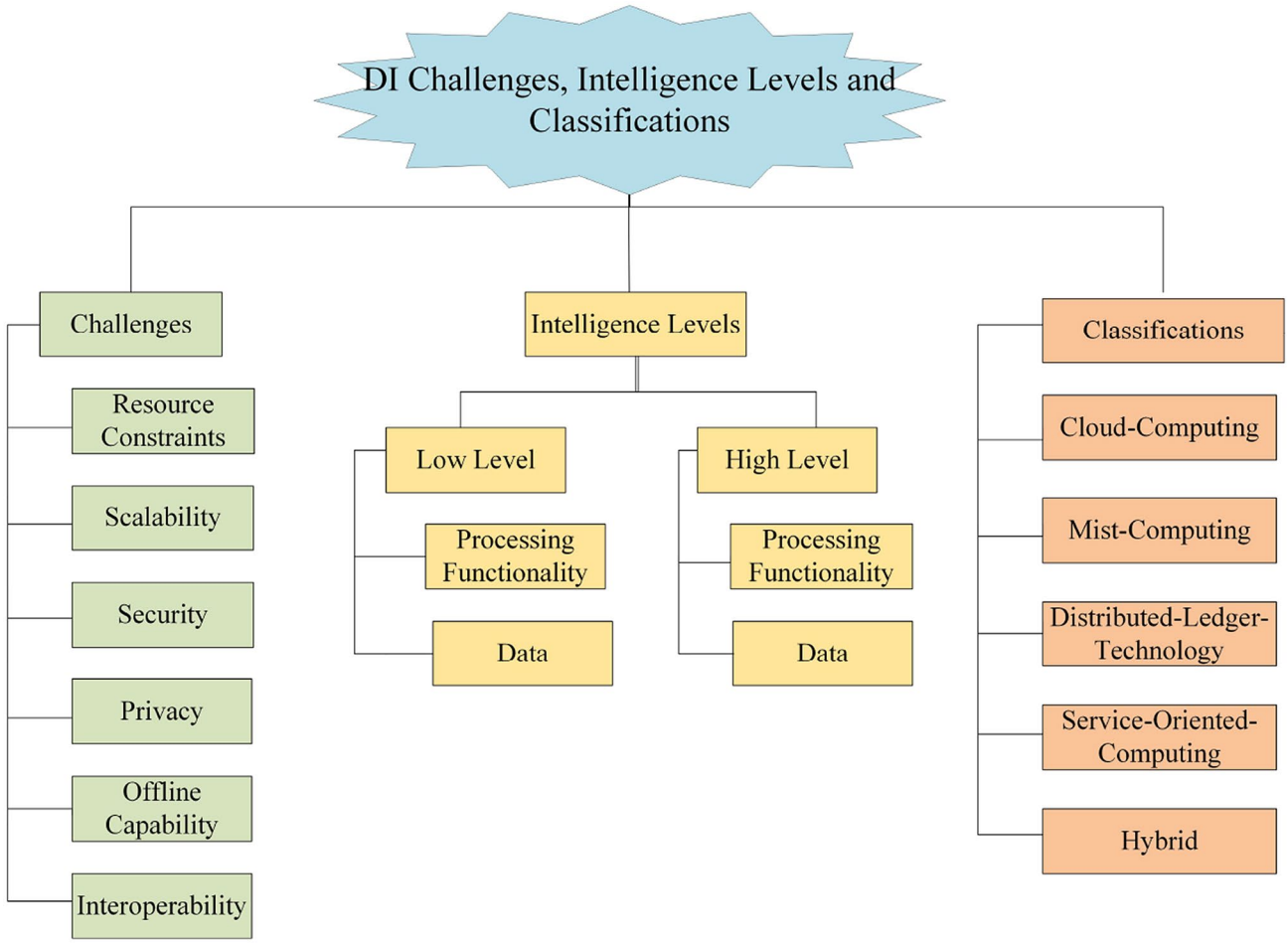

Fig. 1 A taxonomy of DI challenges, intelligence levels and Classifications in IoT

– Intelligence Levels: is classified into two parts, including low-level and high-level. The former refers to node level communications in which processing functionality is distributed among nodes in the network and data processing occurs within the network, i.e., in-network processing, whereas the latter uses high level node in the architecture, i.e., nodes with rich resources to process and handle data.
– Classifications: DI technology support for IoT applications are classified into five broad categories: cloud-computing, mist-computing, distributed-ledger-technology (DLT), service-oriented-computing and hybrid technology.

Issues and Challenges

Resource Constraints

Resource Constraints are referred to IoT devices that was specifically designed with limited power, limited storage capabilities, and limited processing. These limited resources makes DI a challenging distributed task. IoT systems generate large quantities of data, generating a high demand for network resources [26]. IoT devices tend to be small and equipped with batteries to maintain the balance between the effective span of their lifetime and the potential costs of device replacement.

As a result, these devices are typically subjected to strict constraints on their power consumption and available hardware resources. Hence. The less power consumption is universal constraint of the IoT. Efficient uses of IoT devices energy would maintain a prolonged network lifetime. A possible solutions that can be taken into consideration is energy harvesting [27], computation offloading mechanism [28], and management of the wake-up-sleep cycle [29] are important techniques that are effective in reducing energy-consumption of constrained IoT devices.

Scalability

Scalability can be defined as the ability of the network to meet the increasing demands of the network. It is a

fundamental requirement of any IoT system to handle the capability of the growing amount of work. It can be categorized as: Vertical Scaling and Horizontal Scaling. Vertical scaling is intended to upgrade the existing network devices by including more (e.g., power, RAM, CPU) [30]. For example, adding processing power to a server to increase its speed. Moreover, a system can scale a by expanding it by adding more processing, main memory, storage, and network interfaces to the node to adapt the system to handle more requests, whereas horizontal scaling, the network is designed to expand by introducing more nodes. It can be achieved by adding more machines into the group of resources and adding more IoT devices to a network, for example, adding a new IoT device to a distributed IoT network.

In line with the predictions made in [2, 3] IoT is continually changing and growing to meet ever-increasing demands. Therefore, future technologies should be very flexible in dealing with billions of things or smart objects that are inevitably connected to the Internet.

Security

Security refers to the act of securing IoT devices and the networks they are connected to. The main aim of achieving security mitigation is to preserve authentication, confidentiality, and availability to ensure the security of the users, infrastructures, data and devices of the IoT [31]. Authentication is concerned with identifying users and devices in a network and granting access to authorised persons, whereas confidentiality ensures that data is protected by preventing the unauthorised disclosure of information. Availability guarantees that an IoT system and data can be accessed by authenticated users whenever needed [32].

Security remains one of the most fundamental challenges [33–37]. This is believed to be the most challenging and crucial obstacle to IoT. In addition, device security is another fundamental challenge that determines successful implementation of IoT applications [14]. In such circumstances, protection is a top requirement and authentication is especially of great concern, given the harm that could occur from a possibly malicious processing device and unauthenticated device attacks (Referred to outside device attacks) in an IoT system [13]. Ensuring the robustness of any IoT system against hacking is critical.

Privacy

Privacy can be defined as the ability of the system to properly ensure that any data/information is protected and remains confidential. IoT devices must have the incompetence to send their data over the network. Hence, some IoT devices may capture private and disclose sensitive information so that they may cause vulnerability for the system [38]. According to [39] private information can be further categorized as follows: (1) personal information: Such as National Security Number. (2) Sensitive information: Such as salary. It should be ensured that these two types of data private so that individual's information cannot be revealed without appropriate permission.

One main application that requires careful design of privacy is the health care, where patient information is delicate, and user privacy is concerned. In addition, the privacy leakage of user data is usually the ultimate concern, in particular with regard to sensitive data (e.g., the location and movement trajectory information) [40]. A possible solution would be to define who can access that data and in what form the data should be.

Offline Capability

It is also referred to as resilience. It can be defined as the system's ability to operate effectively in mission-critical scenarios. For example, all capabilities do not change if the Internet is not available. Consequently, at all times, the system does not connect to the Internet and offline capability remains extremely important. IoT applications that places the intelligence in a cloud-based system will ultimately become unavailable upon the shutdown of the internet connectivity.

Creating a distributed intelligence approach that handles and processes data in the cloud is inefficient if the cloud becomes unavailable, the system should have the ability to function offline in this critical situation. Therefore, the main functionality of any IoT system should be placed within the network. This results in using simple local processing, which is still possible to have an operational system with less functionality. Hence, the distribution of intelligence is desirable and should be supported.

Interoperability

Interoperability can be defined as the ability of software to communicate with one another for effective exchange and process of information [41]. The heterogeneity of both hardware and software devices also enhances interoperability. It should be tackled through multiple layers of services to enable software and devices to interact seamlessly with each other. This ensures straightforward integration.

Interoperability is the outcome of a range of critical problems, including vendors lock-in, the difficulty of developing IoT applications that work directly in cross-domains and or cross-platforms, and also the challenges of IoT communication for non-interoperable IoT devices. Also, several manufacturers provide a wide selection of technology in its devices, and these devices on the market are unlikely to be directly compatible.

State-of-the-Art Distributed Intelligence in IoT

In this part, we review a set of recent approaches on distributed intelligence. These approaches are summarized and compared using the challenges presented in "Distributed Intelligence in the IoT".

Overview of DI Approaches

As aforementioned, we have identifies five categories of distributed intelligence approaches.

Cloud Computing DI

In cloud computing approaches to DI, generally two layers are considered: the cloud and the end devices. Data is processed in the cloud (high-level intelligence) and devices equipped with sensors, are responsible for sensing the environment (low-level intelligence). In the simplest form, data is stored, processed, and transferred to the cloud for further processing rather than connected devices [42]. The cloud is driven by a centralised design architecture and the functionality is managed in the cloud.

This is inefficient for application that requires real time-decisions. For example, for autonomous vehicles, real-time decisions are critical. To overcome some of the inherent problems, [43] have adopted AWS and introduced a framework for smart traffic control. The framework is based on a public cloud AWS IoT. The components of the system include: AWS IoT, Lambda, DynamoDB, Kinesis, and cloud watch. To be specific, AWS IoT is responsible for collecting data from the environment. DynamoDB is responsible for collecting, and storing data. This ensures what is beyond the endpoints is updated in a timely manner. Cloud watch is a platform for monitoring AWS services and responsible for debugging AWS services in run-time. The proposed framework is energy-efficient with the use of MQTT protocol, scalable and secure. However, privacy and offline capability are not supported. It also lack supporting interoperability. Similarly, a distributed intelligence approach that leverages the AWS IoT platform is proposed in [44] for connected vehicles. The approach authenticates data according to five business rules. It deploys six unique amazon services that store various details about cars health, trip, and owners. The approach is energy efficient and achieves privacy. However, it lacks support for offline capability and interoperablity.

A distributed intelligence architecture, that consists of three components has been proposed by the CARMA project [45]. Each components of the architecture is responsible for a specific task. In Carma Vehicle, various sensors are connected together that collects data. Carma edge, is responsible for processing of data via one or two machines. Finally, the CARMA Core is a cloud-based backend system that is based on public cloud resources and it supports services and information storage. The proposed framework is not suited for time-critical applications, and lacks scalability.

In [46], the author proposes a cloud-based solution, with the benefits of fog computing. The key concept is to introduce two more security features on fog gateway devices, such as Decoys and user behavior Profiling. The Decoys features involve putting the legitimate user in highly prominent locations, to identify the dubious entry. Therefore, two of the new features being added on top of the existing features of cloud security. The proposed approach achieves better security. However, other IoT related challenges such as energy-consumption, offline-capability, interoperability are not well supported.

A distributed intelligence solution, called PROTeCt-privacy architecture for IoT and CC integration, has recently been proposed in [47]. The security of the data on those IoT devices is the responsibility to detect and enforce a cryptographic method, for example, an asymmetric algorithm, to maintain the privacy prior data is exchanged to the cloud. Privacy is accomplished by the proposed technique, which is energy efficient. The technique, however, lacks scalability, and offline-capability, which is not practical for time-critical applications. Also, it does not provide any mechanism to deal with interoperability.

Similarly, the authors of [48] proposed Cloud-IoT distributed intelligence architecture, using an efficiency and security data acquisition scheme. The data collected through the terminals are divided into blocks, sequentially encrypted and processed with the corresponding access subtree until it is forwarded to the cloud in parallel. The proposed approach reduces the time, cost, and secure. It also supports interoperability. However, the approach does not take into consideration power usage of IoT devices, lacks offline-capability, and horizontal scaling.

Mist Computing DI

In mist computing approaches to DI, part of DI functionality and data is processed at the extreme edge of a network that consists of sensors and micro-controllers. By working at the extreme edge, mist computing can harvest resources with the help of computation and communication capabilities available on the sensors [49]. In the simplest form, the gateway applies functionalities and rules for monitoring the health of local nodes, execution of computationally extensive tasks, and filtering application parameters

The authors in [50] recently proposed a heterogeneous five-layer mist, fog, and cloud-based architecture (IoHT) that is responsible for managing and routing (near-real-time)

effectively. Data processing from offline/batch mode is also supported. In this framework, mist computing is responsible for checking if the data needs to be processed or not by applying certain-basic rules and the offloading mechanisms when needed. Software-defined networking (SDN) and link adaption-based load balancing are used in the heterogeneous IoHT framework. The framework ensures efficient resource utilisation while achieving optimal resource allocations.

The heterogeneous IoHT framework employs software-defined networking and link adaption-based load balancing. It ensures optimal resource allocations and efficient resource utilization. The proposed framework is energy-efficient, can eliminate redundant data, and provides fast-response to certain events. However, interoperability, and offline capability mechanisms are not well supported. Furthermore, the framework does not include how scalability is achieved in the perception layer.

A framework based on mist computing was proposed by the authors of [51]. The framework consists of four layers: the layer of data abstraction, the layer of data extraction, the transmission layer, and the layer of aggregation/integration. Where each layer is dedicated to perform a specific task. The data extraction layer is responsible for extracting data from IoT devices.

In the data abstraction, layer data is encapsulated into a JSON format rather than transmitting raw data via it. The data transmission layer is responsible for transmitting and receiving information through any radio and has a Mist Nodes where the abstracted payload of JSON-SenML Is transmitted to the microcontroller via the radio attached. The proposed framework achieves interoperability in an efficient way, and is energy efficient. However, it lacks scalability and offline capability. Furthermore, privacy and security are not supported in their design.

Another work is proposed by the authors in [52], a framework that consists of four layers, including: IoT physical devices layer, mist nodes layer, fog nodes layer, and cloud nodes layer. IoT layer sends data to the mist nodes, which are responsible for processing the data. Cloud nodes layer is responsible for heavy computation tasks. The proposed framework is energy efficient since it uses mist nodes, and has less latency. However, it lacks scalability at the physical layer, and does not support security, privacy, and offline capability.

The authors [53] have taken that work a step further by introducing an offloading computation mechanism among mist nodes using the MQTT protocol that does not require service orchestration. The authors plan as future work to investigate the performances and the partially meshed network as well as supporting interoperability as part of the system.

Similar to the above work, a generic framework based on mist computing is proposed in [54]. The framework consists of mist nodes that process data at the extreme-edge and provides mobile devices to share the networking and computational mechanisms as services in a versatile manner. The framework is called a mobile embedded platform (mePaaS) and the essence of it lies in the architecture of Enterprise Service Bus (ESB). mePaaS nodes lend their hardware resources on the basis of a service level agreement (SLA) to others. Also, it utilizes a plugin module-based method to enable nodes to perform computational processes specified through their requesters.

mePaaS is capable of implementing a workflow that makes the service modules available to complete the requesting tasks. mePaaS requests may submit a request package consisting of the process flow specified in the standard workflow model (e.g. BPMN) and input parameters with custom algorithms.

The proposed framework is energy-efficient because of the use of mist nodes that process data at the extreme edge. However, other related IoT challenges, such as offline capability, privacy, security and scalability, are not well considered in their design. It also lacks supporting interoperability

In [23], the authors described fog computing architecture in support of distributed intelligence in IoT. Fog nodes are considered as hardware and software architecture. In hardware, fog nodes are mainly installed on gateways, and appliances. In software, fog nodes are described as a virtual machines. Reliability, bandwidth and security are enhanced. However, it has been identified that security and privacy in fog computing remains as an issue [55–57]. In addition, how the approach is implemented and evaluated is not described. Also, it lacks a mechanism that deals with interoperability.

The work in [58] uses device-driven and human driven, to decrease energy usage and latency. Machine learning is adopted to identify user behaviors and data gathering from sensors are adjusted to decrease data transmission. Furthermore, some of the local tasks are offloaded between fog nodes in need to decrease energy usage. The proposed approach is considered to be energy-efficient and supports less latency. However, it does not support scalability, and interoperability. Furthermore, a way of exchanging information between sensor nodes is not supported.

Distributed Ledger Technology DI

In distributed ledger technology (DLT) approaches to DI, the functionality and data is distributed among all participant nodes. DLT serves as a shared, digital infrastructure for applications beyond the financial transactions. DLT enables the operation of highly, scalable, available, and append-only distributed database (known as distributed ledger) in an untrustworthy environment [59].

Recently, the authors in [60–62], have proposed an approach in support distributed intelligence. In [60], the

system focuses on privacy and security. The privacy leakage is avoided due to the fact that gateway requires the user to add consent before anyone gets access to the data. Authentication and securely managing of privacy are ensured through the developed digital signature technique. The proposed approach achieves security and privacy. However, offline-capability is not well supported in their approach, and IoT resource constraints i.e., power consummation are not taken into consideration. The approach also lacks scalability and interoperability.

Similarly, a distributed intelligence approach is proposed in [61], the architecture consists of six main components. The proposed approach is scalable, secure, energy-efficient, lightweight and supports transparency, where low-level details are hidden. However, offline-capability is not considered, and elimination of redundant data coming from WSNs still remains unsolved. It also lacks a mechanism to deal with interoperability.

IOTA tangle architecture is an evolving DLT platform aimed at addressing transaction costs, mining and scalability issues (in the context of blockchain technology) [59], that are related to IoT. The architecture of a *Tangle*, which is central to IOTA. *Tangle* has been used to achieve DI.

For example, in [63] a distributed intelligence approach that adopts the IOTA protocol is proposed. It establishes an infrastructure network for smart home paying a particular attention to ensure scalability. All of the home IoT nodes in the system are linked with neighbouring nodes to exchange information and ensure synchronization with the ledger. The approach is only suitable for small scale applications, and would lead to higher energy to be consumed in all nodes since PoW computation is performed on local IoT nodes. Offline capability is not supported and is not decentralized because it's fully based on a coordinator. The approach also does not support interoperability in the design of their architecture.

Most recently, an approach to distributed intelligence is introduced in [16]. The approach is called a Scalable Distributed Intelligence Tangle-based approach (SDIT). The approach is concerned with solving some of the IoT issues such as scalability, energy usage, and decentralization by adopting the IOTA protocol. A computation offloading mechanism has been developed to ensure that constrained IoT devices do not engage in performing heavy computation tasks. The proposed approach is scalable, energy-efficient, and decentralized. However, security and elimination of redundant data are not considered. Also, they outline to develop a mechanism to deal with interoperability, and offline capability as part of their future work.

Similar to [16, 63], the work presented in [64] in which a distributed intelligence architecture is introduced. The architecture consists of three main components, including IoT nodes, Super-node, and Masked Authenticated Messages (MAM). IoT nodes are responsible for sensing the environment. The super-nodes are mainly concerned with aggregating data and packaging them into a transaction, which then are sent to the IOTA network. Masked Authenticated Messages are mainly responsible for managing access control over the data stored in the tangle. The approach achieves privacy with the use of MAM. However, the approach lacks an offline-capability, and interoperability mechanisms that are critical to IoT applications, and is neither energy-efficient nor scalable due to the lack of an efficient clustering mechanism.

Service Oriented Computing DI

In service oriented computing approaches to DI, the functionality is supported as services that are distributed in all levels of the system. In addition, it ensures that software components are re-usable and interoperable through service interfaces.

Recent work is introduced in [65]. The LEONORE system to support distributed intelligence. LEONORE is built up using a service-oriented architecture and supports several application components in large-scale IoT deployments. The LEONORE framework works according to two phases push-based and pull-based. the Pull-based is responsible to independently propose a run time method, while provisioning of push-based, responsible for providing control for the application by providing software updates and maintains security. The proposed framework is energy-efficient, and scalable. However, offline-capability, security, and privacy are not well supported.

A service oriented computing is developed for the agriculture application in [66]. The architecture contains components that are related to farming and farmers such as monitoring of the farm and it describes how farming should utilize such components. In this way, it is likely to reduce the expenditure for farming, minimize the labor, improve the crop yielding, and suitability of crop for a particular soil. However, the proposed approach lacks scalability, offline capability, and privacy, which are fundamental requirements for IoT.

Similar to the above work, but differs by adopting micro-service is the approach proposed in [67]. The architectural style contains various patterns, including Client-server, Peer-to-Peer, and cloud computing pattern, etc, the framework proposes the adoption of micro-service. Micro-services adopts a simple APIs which are thin layered (light weighted compared to SOA). Some might argue that micro-services are similar to SOA. However, both applies service-based architecture that enables service use and reuse. The differentiation is in the way where processing functionalities are triggered, where data is processed, architectural style, architectural characteristics, service characteristics and

capabilities. The proposed approach is energy-efficient, and interoperable. However, scalability that will accommodate the growth of IoT devices is not well supported. Furthermore, other challenges such as privacy, offline capability, security are not considered.

Hybrid DI

A hybrid approach is an approach that combines two or more algorithms from different DI categories. Hybrid approaches aim to overcome some of the disadvantages of individual DI categories described above.

Most of the introduced hybrid approaches are mainly concerned with issues related to management of data, processing of data in a timely manner and privacy, by mixing different algorithms from various technologies to achieve the required goal. In early studies, distributed intelligence was achieved by integrating the architecture of WSNs at the various level of IoT in support of distributed intelligence [15]. In such approach, the aim is that wireless sensor network architecture is to be connected to the internet, and the intelligence should be distributed at several layers. These approaches are considered efficient in regards to energy usage. This is because data processing is distributed among all layers; they provide flexibility and application specific. However, they lack scalability, privacy, and offline capability, which are considered critical challenges of the IoT domain. they also lack supporting interoperability.

In [68], the authors applied fog computing as a means to support distributed intelligence by setting up an architecture that is made up of three layers. The sensing layer is concerned with transmission of data to the upper layer. A fog layer plays the role of data processing transferred from the sensor nodes. The cloud computing layer is used for heavy processing of data. The system is suitable for timely response applications and is energy efficient since processing is performed near the data source. It also provides support for interoperability. However, the approach lacks support for other IoT technical challenges such as scalability, offline capability, and privacy.

Recently, a computing paradigm called Edge Mesh is being suggested in [69] to allow distributed intelligence in IoT. Decision-making task is distributed through the network among devices, instead of data being transmitted directly to a central location for processing. Combining the use of both computation and data, tasks are exchanged with Edge Mesh through a network of routers and edge devices. The architecture of Edge Mesh comprises of several devices. First of all, the end devices are concerned with actuation and sensing purposes. Second, edge devices can be used to process and connect end devices. Third, routers are being utilized to transmit data. Finally, the cloud is increasingly being used to perform advanced analysis of data.

The incorporation of Edge Mesh could bring various benefits such as increased scalability, improved security, and privacy. Nevertheless, some will have a concern over privacy and security, but how privacy can be accomplished is not taken into account. Also, the architecture lacks support for interoperability

In comparison to the above, the research in [70] suggested an AI-based distributed intelligence solution. The solution incorporates the use of both cloud based and edge controller to enable distribute intelligence. To be specific, it has been shown that the cloud-based controller is capable of providing intelligence at a high level. The edge controller is designed to support intelligence at a low level. The advantages of their research are reducing response time and loosening rules requirements. However, the approach lacks a mechanism which allows offline capability and privacy preserving.

A hybrid distributed intelligence approach is proposed in [71]. The approach comprises of several layers, including IoT layer, fog layer, and cloud layer. The IoT layer contains WSNs that are mainly concerned with data collection from the environment, then data is transmitted to the fog layer, which is responsible for processing. The cloud layer is responsible for heavy computation. The architecture is energy-efficient, interoperable and scalable. However, it lacks an offline-capability mechanism, and does not deal with privacy.

A hybrid distributed data flow is introduced in [72, 73]. All levels of the architecture comprises of fog nodes and these fog nodes works based on their computing resources. It has Edge input/output and nodes for computing data. The input nodes are used to communicate and transmit data to the compute nodes. Computing nodes are mainly concerned with the data processing. The proposed system takes into account the scalability and energy-efficent. However, offline-capability, and privacy remains unsolved. The approach also does not support interoperability.

A novel tiered architecture to allow distributed intelligence is presented in [74]. The three-tier architecture manages gathered data from sensors. The regional Tier contains fog nodes that are mainly concerned with data combination and pre-processing. The cloud data center is hosted to deal with heavily computations of data. The proposed system reduces energy usage by utilizing fog nodes to process data. However, scalability is not well maintained within the system and privacy is not considered. Furthermore, it applies static orchestration, leading to system failure.

Most recently, the authors in [5] propose a novel approach in support of distributed intelligence. The approach consists of (1) IoT nodes; Tangle to manage transactions; (3) PoW Server, and mobile agents to gather transactions data. All of the IoT nodes in the system are linked with neighbouring nodes to exchange information. IoT devices deployed to

sense data. A PoW server contains high power resources, and deals with heavy computations. Mobile Agents are triggered to gather transactions data along their identified routes. MADIT is scalable and shares information between sensor nodes. Furthermore, the system is energy-efficient and decrease the data that needs to be collected. However, offline-capability and interoperability are not considered, but outlined as future work.

In [75], a distributed Internet Like architecture (DIAT) is introduced. The system has three main layers. The first layer mainly concerned with real-world objects such as sensor devices. Second layer, communicates and coordinates the tasks coming from the first layer. The final layer is mainly concerned with user requests and services. The system is scalable and enables interoperability. However, dealing with other challenges such as offline capability is not introduced and does not consider resource constraints posed by IoT devices.

The authors in [76] proposed an approach that relies on Mobile Cloud Computing. It was described that sensing and processing to be merged in the architecture of the network and it requires that the application workload to be shared among server side and nodes. The proposed approach allows the data to be analyzed and monitored in real time. However, these approaches do not consider the scalability of the system and they are not designed to cope with time-critical applications. Furthermore, offline capability, is not considered but outlined as future work.

Another work is introduced in [77]. The work describes system architecture that consists of data collection, self-organization, and reasoner. The data collection is to be used for gathering and communicating data to a gateway for further processing, while, self-organization is responsible for proper management such as configuration, discovery, and duplicated identification check. The publish-subscribe is responsible for disseminating/acquiring data, which can be handled by the MQTT protocol. Finally, the reasoner plays the role of extracting knowledge based on context using a naïve Bayes method. Scalablity is ensured and delay is avoided due to the use of Bayesian reasoning. However, the ability to work in critical cases is not supported.

In [78], the authors presents a hierarchical distributed computing architecture. layer one is largely used for computations. It is designed to provide centralised control purposes and wide city monitoring. The second layer consists of the intermediate computing nodes that recognise and respond to potentially dangerous activities and to act upon risks it identifies. The third layer consists of high-performance edge devices and low-powered linked to a group of sensors which manage raw data from sensors and analyses data promptly. The fourth layer is containing sensor nodes to track environmental changes. The benefits include low latency, efficient responses in real-time, and energy-efficient. Nonetheless, issues related to IoT, such as security and scalability, are not taken into account in the proposed approach.

Intelligence Levels

Intelligence-levels in DI approaches aims to provide where raw data processing occurs and where processing functionalities are triggered. In each distributed intelligence approach, the level of supported intelligence can be either low-level, high-level or both levels supported. For example, the works reported in [43–48] focuses on high-level intelligence by enabling data processing and processing functionality to occur in the cloud. Other research efforts that primarily supports high-level intelligence are proposed in [16, 60, 63, 64] in which a nodes with advanced computational resources i.e., energy and processing power are responsible for managing and handling data.

Low-level intelligence are mainly concerned with enabling data processing to occur at the edge of the network. For example, the DI approaches described in [23, 50–52, 54] in which the main idea is to provide low-level intelligence to the data at the edge. In addition, cooperation among physical IoT devices by means of data sharing. Such research efforts would lead to a significant decrease in energy-consumption since data computation is performed near the IoT devices and faster response time is obtained.

Both of the high-level and low-level intelligence are supported in all levels of the IoT system to ensure minimum resource usage. For example, the DI approaches proposed in [5, 15, 65, 69, 70, 74] focuses on enabling high-level and low-level intelligence. In these approaches, low-level intelligence is supported by enabling data to be shared among various IoT devices and perform computation to provide usefulness insight out of the data. On the other hand, high-level intelligence is supported by making use of the cloud to perform big data analytics [70].

Evaluation of Distributed Intelligence Approaches

The evaluation of distributed intelligence approaches covers 30 representative approaches. As described in Table 1, the evaluation aims to assess existing research using the categorization presented in "State-of-the-Art Distributed Intelligence in IoT" and the identified challenges in "Distributed Intelligence in the IoT".

According to Table 1, the least implemented challenges of distributed intelligence are offline capability, security, and privacy. Many research efforts support only two or three of the IoT DI challenges, which are potentially critical for many IoT applications. In terms of offline capability, It has not been implemented in most of the research efforts according to Table 1.

Table 1 Evaluation of distributed intelligence approaches

DI Categories	AP	RC	SC	SE	PR	OC	IO	IL
Cloud computing	[43]	✓	✓	X	✓	X	X	H
	[44]	✓	✓	X	✓	X	X	H
	[45]	✓	X	X	✓	X	✓	H
	[46]	✓	X	✓	✓	X	X	H
	[48]	X	X	✓	✓	X	✓	H
	[47]	X	✓	X	✓	✓	X	H
Mist computing	[50]	✓	X	✓	X	X	X	L
	[23]	✓	X	✓	X	X	X	L
	[58]	✓	X	✓	X	X	X	L
	[51]	✓	X	X	✓	X	✓	L
	[52]	✓	✓	X	X	X	✓	L
	[53]	✓	✓	X	✓	✓	X	L
	[54]	✓	✓	X	X	X	X	L
Distributed ledger technology	[60]	X	X	✓	✓	X	X	H
	[61]	✓	✓	✓	X	X	X	H
	[63]	X	✓	✓	✓	X	X	H
	[16]	✓	✓	X	X	✓	X	H
	[64]	X	X	X	✓	✓	X	H
Service oriented computing	[65]	X	X	✓	✓	X	X	H&L
	[66]	✓	✓	✓	X	X	X	H&L
	[67]	X	✓	✓	✓	X	X	H&L
Hybrid	[15]	✓	✓	X	X	✓	X	H&L
	[68]	✓	✓	✓	X	X	✓	H&L
	[69]	✓	✓	✓	X	X	X	H&L
	[70]	X	✓	X	X	X	✓	H&L
	[71]	✓	✓	✓	X	X	✓	H&L
	[72]	X	✓	X	✓	X	✓	H&L
	[73]	✓	X	✓	X	X	X	H&L
	[74]	✓	✓	✓	X	X	X	H&L
	[5]	✓	✓	X	X	✓	✓	H&L
	[75]	X	✓	✓	✓	X	✓	H&L
	[76]	✓	X	✓	X	X	X	H&L
	[77]	✓	X	✓	X	X	X	H&L
	[78]	✓	X	X	✓	X	X	H&L

AP approach, *RC* resources constraints, *SC* scalability, *SE* security, *PR* privacy, *OC* offline capability, *IO* interoperability, *IL* intelligence levels, *L* low-level, *H* high-level, *H&L* both high-level and low-level

Among these research efforts, the work proposed in [23], provides an interesting case study on applying distributed intelligence in smart factory applications. When applying the Fog computing technology, Fog nodes are described by the hardware and software architecture. Therefore, real time analysis are supported and low-latency is minimized. It has been indicated that fog computing approach is able to reduce bandwidth because processing is occurring within the network. The work proposed by the authors in [46] relates to the security issue in which a cloud-based approach is used to mitigate attack (e.g, data theft) where two additional security features are added. Consequently, better security can be achieved through the proposed built-in features in addition to existing cloud security features. In regards to the offline capability issue, the authors in [15] introduced offline-capability in their architectural design, but without giving details about the implementation and evaluation.

A Summary of Shortcomings of Existing Distributed Intelligence Approaches

From the above discussion, it can be seen that most of the current approaches to enabling distributed intelligence in IoT are subject to all the problems inherent in distributed systems. Firstly, the approaches suggested usually depend on centralised architecture for processing data [57] that offers

high cost and unacceptable delays for many distributed applications. These include health monitoring, autonomous driving, emergency response etc. Furthermore, transferring data to a central location requires high network bandwidth [8, 79].

Bottlenecks and delays are expected from the communications among the devices and the centralized system [76]. Tracing data stored in the cloud is very difficult and lacks accountability. IoT that is based on central infrastructure requires trusting third party for dealing with data, and the storage of data in the cloud has the possibility of that data to be deleted or tampered with [80]. Besides, solutions that fully relies on fog computing is considered to have problem with security and privacy [25, 55]. They also lack interoperability and interaction models [25].

Previous research recommends that IoT needs to shift away from centralization point of control [81]. Approaches based on Blockchain introduce overhead and performance issues [82, 83]. Therefore, developing a standardised approach is required to define IoT data. For example, the one provided in the IOTA Identification of Items (IDoT) [84] that aims to protect the network, too. Also, Blockchain requires transferring a big portion of data, which is the header block, leading to a wastage of resources [85].

Hardware-Based Security Primitives for IoT

The inherently distributed nature of distributed intelligence approaches provides several vulnerable points to compromise security. Consequently, it is a fundamental challenge to ensure authenticity, integrity, confidentiality and availability among various integrated devices [86, 87].

Hardware security primitives has been put forward as a promising security primitive to achieve security. It is referred to hardware devices that are used as fundamental building blocks to create security solutions [87]. It consists of Physically Unclonable Functions (PUFs) and True Random Number Generator (TRNG). On one hand, PUFs is considered as an integrated circuit, which has the ability to generate secret responses and cryptographic keys by applying inherent physical variations from manufacturing [88]. In PUFs, inputs are referred to "challenges" and outputs are "responses." A challenge and its associated response are known as challenge-response pair (CRP). On the other hand, TRNG are hardware components that is responsible for producing random bits according to the outcome of unpredictable physical processes such as device's internal thermal noise [89].

Recent research focused on exploiting the benefits of hardware security primitives for Cyber-Physical System (CPS) [88, 90–92]. The authors in [90] have proposed a novel integrated TRNG-PUF architecture based on Photovoltaic (PV) solar cells. The proposed architecture works according to two phases including: Training phase and Run phase. The training phase is mainly concerned with learning the entropic nature of PV solar cells and sets an optimal sampling interval, which is a vital step to set optimum TRNG throughput. The run phase is mainly responsible for obtaining sensor response in either dynamic (large variation) response to produce TRNG output or static (stable) response to generate PUF output. The proposed integrated architecture can be beneficial in space-limited CPS.

Another PUF design that is specifically targeted for use in IoT applications is proposed in [92]. The architecture of the proposed PUF consists of a microcontroller, eight piezo sensors, eight 100 K resistors, and an ac voltage source each of which is responsible for performing a specific task. The proposed PUF should be considered a weak PUF as it is designed to have only one possible challenge-response pair (CRP). The reason there should only be one pair is because the response generated by the PUF is a result of comparing intrinsic characteristics of the piezo sensors. The proposed PUF approach can be incorporated into IoT devices as a cybersecurity solution.

A novel solar cell based PUF that leverages the intrinsic variations present in solar cells is introduced in [88]. The proposed design utilizes a microcontroller to read the open-circuit voltages (Voc) of a selection of solar cells and generate an associated response. The proposed design was implemented using amorphous silicon solar cells, monocrystalline solar cells, and polycrystalline solar cells. A microcontroller is responsible for capturing voltages output and converts them to digital values. The PUF uses these values to generate a 128 bit response by comparing the voltages in a pre-determined pattern. Each bit in the generated response is a direct result of a comparison made between the output voltages from two different groups of solar cells. The proposed approach ensures security of IoT devices without adding hardware.

A novel weak PUF design using thermistor temperature sensors is proposed by the authors in [91]. The design uses the differences in resistance variation between thermistors in response to temperature change. The approach is based on eight thermistor temperature sensors. Each sensor is connected to a microcontroller in the configuration. A microcontroller is used to compare readings from groups of thermistor temperature sensors to generate a weak response. An algorithm is used to process the individual voltage data and construct a 128-bit response. It produces a response by making a series of comparisons between total output readings for predetermined groups of a given component. It assumes that each component should have the same reading, and any differences are solely due to their intrinsic variations. The approach have shown an improved overall reliability with regards to changes in temperature.

Challenges and Opportunities

We have discussed several issues, and challenges that are important in a distributed intelligence approach. Also, we have examined over 30 research efforts to evaluate distributed intelligence approaches. these challenges are research fields that needs to be further investigated. We have giving the related references for each challenge in which the interested reader can use to further look into a specific challenge.

In the following, we provide the needs of a DI approach/platform that could potentially support all of the challenges in this article.

- Both DI and DLT are still in their early stages and requires further experimentation. Distributed intelligence is considered to be very critical in determining the success of almost any IoT applications such as smart parking. The main reason behind it is that it requires the placement of where methods should be invoked/triggered and where data should be processed. This needs an effort to where distributed intelligence should be put and activated. This process requires several stages such as business logic, energy efficient, and computation efficient. Distributed ledger technology (DLT), will change the infrastructure for the Internet of Things into collaborative distributed participants. IOTA Tangle will tackle many of the IoT issues by enabling scalablity, efficient processing of data, security, and privacy [5, 16].
- There is an overall lack of a DI platform and approach, which can provide an efficient framework for other researchers to test alternative approaches, and distributed algorithms. For example, in order to design and develop a *new hybrid* DI approach that is mixed up from various technologies such as Network Function Virtualization (NFV) [93], Mobile cloud Computing [94], Multi-Agent system [95, 96], Distributed Leger technology [97], is yet to be developed.
- IOTA DLT Masked Authentication Messaging comprises of three modes including public, private, and restricted that could potentially provide a way of enabling multiparty authentication scenarios [4], and access control. Moreover, location privacy [13] that focuses on how to effectively select reasonable dummy locations and avoid having the real locations. These are considered as important issues for providing an effective IoT privacy [25]. The first IOTA-based project towards achieving better privacy, i.e. end to end encryption is called Untangle care as described in [98], which has an interesting vision as your body, your health, and your data. The project considers the development of a virtual health assistant platform that puts users in control of their own health data and enables them to have a more active role side-by-side with their healthcare stakeholders.
- Device security is regarded as an important challenge, which provides support to successfully implement many IoT applications that can be affected by cyber-attack. For example, cyber attacks to IoT devices, IOTA nodes/IoT gateways can mislead the functioning of these IoT devices, and introduces potential risks that could fail in the services that is provided to, for example, smart parking system, and leading to providing faulty decisions in response to critical situations. Network security ensures that the DI system is protected from several network attacks such as jamming and sniffer. Cyber security [14] would be regarded as a crucial enhancement to any IoT systems. This is where the IOTA MAM plays an important role to ensure security and privacy in data transfer.
- The issue of the offline capability can be tackled by the IOTA ***Tangle***. This issue is not related to the configuration of the network, rather it is concerned with clustering the network. Consequently, the Tangle can overcome this particular issue by generating offline ***Tangles***, in which part of the nodes can be in an offline mode and exchange transactions between each other's. Ultimately, this does not require an internet connection when the tangle is offline. Then, all of the transactions that occurred when the ***Tangle*** was offline can be attached to the online one.
- The IOTA Tangle offers benefits that can be applied to Wireless Sensor Networks (WSNs). The energy efficiency, and scalability issues are the main concerns of a WSN and these issues should be considered. In addition to that, generating an effective routing protocol using the ***Tangle*** by considering an important metrics such as quality of service is another direction to be considered. Moreover, an investigation of the probability of applying it to support information Extraction (IE) methods in WSNs such as Threshold-based, periodic and query-based would be an efficient way of performing Information Extraction in an interactive mode. Consequently, the advantages of IOTA ***Tangle*** will not be restricted to a particular problem.
- Ensuring where to place the intelligence is a major research question that should be taken into consideration when developing distributed intelligence approach. Other related research questions that should be investigated including: How IoT devices should cooperate with each other to support low-level intelligence? Where heavy computations should be invoked? Who is responsible for the distribution of tasks between devices? When to trigger data processing and where?. These are all research questions that needs to be investigated further. The computation tasks should be distributed among various devices depending

on the available resources of each device. For example, IoT devices with higher resources can perform data processing on behalf of constrained IoT devices. Therefore, the tasks should be distributed among different devices depending on the application requirement and resources available on the devices. Mist computing can work on the edge of the network and can deal with issues related security, data processing, and access control etc. This requires mist devices to be robust and flexible. It is a challenge to manage all the tasks concurrently when developing distributed intelligence approaches.

Conclusions

As the use of Internet of Things (IoT) appliances have increased in recent years, mainly due to improvements in sensor technologies and an overall costs is reduced, the ability of sensing is considered to be become pervasive as they are integrated into everyday objects. Since IoT devices are generally resource-constrained, there is an assumption that they shall connect to centralised infrastructure to provide additional application functionality, facilitating the smart revolution. The reliance upon cloud nodes to process sensor data, for knowledge discovery, results in being unsuitable way for many IoT applications. To overcome these issues, distributed intelligence and DLT paradigms are being investigated. Industrial development of IoT platforms, such as INFORMA London, MAERSK UPS, FEDEX, AND BNSF RAILWAY JOIN BITA ALLIANCE etc, are now moving toward utilizing DLT analytics. Distributed intelligence is suitable for resource constraints IoT devices and describes where functionality should be invoked and where data should be processed while DLT will change the entire infrastructure of IoT to many IoT applications. We have studied the research efforts related to distributed intelligence to identify critical functions that DI platform/approach should support. We have provided a discussion about distributed intelligence techniques. It has been identified that there is a lack of lightweight solution that enables distributed intelligence according to the identified limitations of the summarized approaches.

Declaration

Conflict of Interest On behalf of all authors, the corresponding author states that there is no conflict of interest.

References

1. Cisco. Internet of things at a glance. (1); 2016.
2. Gartner. Gartner says the internet of things installed base will grow to 26 billion units by 2020. (1); 2013.
3. API Research. More than 30 billion devices will wirelessly connect to the internet of everything in 2020. (1); 2013.
4. Al-Aqrabi H, Pulikkakudi JA, Hill R, Lane P, Liu L. A multi-layer security model for 5g-enabled industrial internet of things. In: 7th International Conference on Smart City and Informatization (iSCI 2019), Guangzhou, China, November 12–15, 2019, Lecture Notes in Computer Science, Switzerland; 8 2019. Springer International Publishing AG.
5. Alsboui T, Qin Y, Hill R, Al-Aqrabi H. Enabling distributed intelligence in the internet of things with iota and mobile agents. Computing; 01 2020.
6. Luigi A, Antonio I, Giacomo M. The internet of things: a survey. Comput Netw. 2010;54(15):2787–805.
7. Carlos C, Samuel SNC. Agent-oriented engineering for cyber-physical systems. Helping Teachers Dev Res Inf Pract. 2019;02:93–102.
8. Perera C, Qin Y, Estrella JC, Reiff-Marganiec S, Vasilakos AV. Fog computing for sustainable smart cities: a survey. ACM Comput Surv. 2017;50(3):32:1-32:43.
9. Doan TT, Safavi-Naini R, Li S, Avizheh S, Muni VK, Fong PWL. Towards a resilient smart home. In: Proceedings of the 2018 Workshop on IoT Security and Privacy, IoT S&P '18, pages 15–21, New York, NY, USA; 2018. ACM.
10. De Angelis E, Ciribini ALC, Tagliabue LC, Paneroni M. The brescia smart campus demonstrator renovation toward a zero energy classroom building. Procedia Eng. 2015;118:735–43.
11. Al-Aqrabi H, Johnson AP, Hill R, Lane P, Alsboui T. Hardware-intrinsic multi-layer security: a new frontier for 5g enabled iiot. Sensors. 2020;20(7):1963.
12. Armbrust M, Fox A, Griffith R, Joseph AD, Katz RH, Konwinski A, Lee G, Patterson DA, Rabkin A, Stoica I, Zaharia M. A view of cloud computing. Commun ACM. 2010;53(4):50–8.
13. Sun G, Chang V, Ramachandran M, Sun Z, Li G, Hongfang Y, Liao D. Efficient location privacy algorithm for internet of things (IoT) services and applications. J Netw Comput Appl. 2017;89:3–13 (**Emerging Services for Internet of Things (IoT)**).
14. Sohal AS, Sandhu R, Sood SK, Chang V. A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments. Comput Secur. 2018;74:340–54.
15. Van den Abeele F, Hoebeke J, Teklemariam GK, Moerman I, Demeester P. Sensor function virtualization to support distributed intelligence in the internet of things. Wirel Person Commun. 2015;81(4):1415–36.
16. Alsboui T, Qin Y, Hill R. Towards a scalable iota tangle-based distributed intelligence approach for the internet of things. In: Intelligent Computing, Advances in Intelligent Systems and Computing. Springer Verlag; 10 2019.
17. Terzic I, Zoitl A, Favre B, Strasser T. A survey of distributed intelligence in automation in European industry, research and market. In: 2008 IEEE International Conference on Emerging Technologies and Factory Automation; 2008. pp. 221–228.

18. Shu L, Lloret J, Rodrigues JJPC, Chen M. Editorial—distributed intelligence and data fusion for sensor systems. IET Commun. 2011;5(12):1633–6.
19. Wei Y, Liang F, He X, Hatcher WG, Chao L, Lin J, Yang X. A survey on the edge computing for the internet of things. IEEE Access. 2018;6:6900–19.
20. Amin SU, Shamim HM. Edge intelligence and internet of things in healthcare: a survey. IEEE Access. 2021;9:45–59.
21. Zhi ZX, Chen EL, Zeng L, Luo K, Zhang J. Edge intelligence: paving the last mile of artificial intelligence with edge computing. Proc IEEE. 2019;107(8):1738–62.
22. Deng S, Zhao H, Fang W, Yin J, Dustdar S, Zomaya AY. Edge intelligence: the confluence of edge computing and artificial intelligence. IEEE Internet Things J. 2020;7(8):7457–69.
23. Byers CC, Wetterwald P. Fog computing distributing data and intelligence for resiliency and scale necessary for IoT: the internet of things (ubiquity symposium). Ubiquity. 2015;4(1–4):12.
24. Michael V, Johannes S, Christian I, Schahram D. A scalable framework for provisioning large-scale IoT deployments. ACM Trans Internet Technol. 2016;16:1–20.
25. Dizdarevic J, Carpio F, Jukan A, Masip X. A survey of communication protocols for internet of things and related challenges of fog and cloud computing integration. ACM Comput Surv 04 2018. 51.
26. Siow E, Tiropanis T, Hall W. Analytics for the internet of things: a survey. ACM Comput Surv. 2018;51(4):74:1-74:36.
27. Klinefelter A, Roberts NE, Shakhsheer Y, Gonzalez P, Shrivastava A, Roy A, Craig K, Faisal M, Boley J, Oh S, Zhang Y, Akella D, Wentzloff DD, Calhoun BH. 21.3 a 6.45 w self-powered IoT soc with integrated energy-harvesting power management and ulp asymmetric radios. In: 2015 IEEE International Solid-State Circuits Conference - (ISSCC) Digest of Technical Papers; 2015. pp. 1–3.
28. Elsts A, Mitskas EOG. Distributed ledger technology and the internet of things: a feasibility study. Proc 1st Workshop Blockchain-Enabled Netw Sens Syst. 2018;11:7–12.
29. Haimour JA-SO. Energy efficient sleep/wake-up techniques for IoT: a survey. JEEIT. 2019;04:478–84.
30. Bondi AB. Characteristics of scalability and their impact on performance. In: Workshop on Software and Performance; 2000. pp. 195–203.
31. Noor MM, Hassan WH. Current research on internet of things (IoT) security: a survey. Comput Netw. 2019;148:283–94.
32. Sha K, Wei W, Andrew YT, Wang Z, Shi W. On security challenges and open issues in internet of things. Future Gener Comput Syst. 2018;83:326–37.
33. Granjal J, Monteiro E, Sá SJ. Security for the internet of things: a survey of existing protocols and open research issues. IEEE Commun Surv Tutor. 2015;17(3):1294–312.
34. Nastase L. Security in the internet of things: a survey on application layer protocols. In: 2017 21st International Conference on Control Systems and Computer Science (CSCS); 2017. pp. 659–666.
35. Sha K, Andrew YT, Wei W, Davari S. A survey of edge computing based designs for IoT security. Digit Commun Netw; 2019.
36. Tedeschi S, Mehnen J, Roy R. Iot security hardware framework for remote maintenance of legacy machine tools. In: Proceedings of the Second International Conference on Internet of things and Cloud Computing, ICC 2017, Cambridge, United Kingdom, March 22–23, 2017; 2017. pp. 43:1–43:4.
37. Mohan S, Asplund M, Bloom G, Sadeghi A-R, Ibrahim A, Salajageh N, Griffioen P, Sinopoli B. The future of iot security: special session. In: Proceedings of the International Conference on Embedded Software, EMSOFT 2018, Torino, Italy, September 30–October 5, 2018; 2018. p. 16.
38. Gao C, Cheng Q, Li X, Xia S. Cloud-assisted privacy-preserving profile-matching scheme under multiple keys in mobile social network. Clust Comput. 2019;22.
39. Mehdi G, Quoc-Viet P, Mamoun A, Xiaobo Z, Christian F-C, Gautam S. Eca: an edge computing architecture for privacy-preserving in IoT-based smart city. IEEE Access. 2019;7:155779–86.
40. James B, Immanuel B, Navin R. Authenticating health activity data using distributed ledger technologies. Comput Struct Biotechnol J. 2018;16:257–66.
41. Jussi K, Alfredo DE, Francesco M, Pasi H, Janne T-M, Arto Y, Juha-Pekka S, Tullio C. Semantic interoperability architecture for pervasive computing and internet of things. Access IEEE. 2014;2:856–73.
42. Buyya R, Yeo CS, Venugopal S, Broberg J, Brandic I. Cloud computing and emerging it platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Gener Comput Syst. 2009;25(6):599–616.
43. Tärneberg W, Chandrasekaran V, Humphrey M. Experiences creating a framework for smart traffic control using aws iot. In: 2016 IEEE/ACM 9th International Conference on Utility and Cloud Computing (UCC); 2016. pp. 63–69.
44. Seniro S, Rec C, Nishar H, Horton T. Aws connected vehicle solution: Aws implemnation guide; 06 2017.
45. Katsaros K, Stevens A, Dianati M, Han C, McCullough, Alexandros M, Maple C, Fallah S. Cooperative automation through the cloud: the carma project; 06 2017.
46. Stolfo SJ, Salem MB, Keromytis AD. Fog computing: Mitigating insider data theft attacks in the cloud. In: 2012 IEEE Symposium on Security and Privacy Workshops; May 2012. pp. 125–128.
47. Pacheco LAB, Alchieri EAP, Barreto PASM. Device-based security to improve user privacy in the internet of things. In: Sensors; 2018.
48. Guan Z, Li J, Wu L, Zhang Y, Du X. Achieving efficient and secure data acquisition for cloud-supported internet of things in smart grid. IEEE Internet Things J. 04 2017. p. 1.
49. Yogi MK, Chandrasekhar K, Vijay Kumar G. Mist computing: principles, trends and future direction; 2017. arXiv:1709.06927.
50. Asif RM, Afsana F, Mahmud M, Shamim KM, Ahmed M, Kaiwartya O, James-Taylor A. Towards a heterogeneous mist, fog, and cloud based framework for the internet of healthcare things. IEEE Internet Things J. 10 2018. p. 1.
51. Pratik T, Lenka RK, Nayak GK, Kumar A. An architecture to support interoperability in IoT devices. In: 2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN); Oct 2018. pp. 705–710.
52. Battistoni P, Sebillo M, Vitiello G. Experimenting with a fog-computing architecture for indoor navigation. In: 2019 Fourth International Conference on Fog and Mobile Edge Computing (FMEC); June 2019. pp. 161–165.
53. Battistoni P, Sebillo M, Vitiello G. Computation offloading with mqtt protocol on a fog-mist computing framework; 10 2019.
54. Liyanage M, Chang C, Srirama S. Adaptive mobile web server framework for mist computing in the internet of things. Int J Pervasive Comput Commun. 11 2018. 14.
55. Esposito C, Castiglione A, Pop F, Choo KR. Challenges of connecting edge and cloud computing: a security and forensic perspective. IEEE Cloud Comput. 2017;4(2):13–7.
56. Yi S, Li C, Li Q. A survey of fog computing: concepts, applications and issues. In: Proceedings of the 2015 Workshop on Mobile Big Data, Mobidata 15, pages 37–42, New York, NY, USA; 2015. ACM.
57. Gillam L, Katsaros K, Dianati M, Mouzakitis A. Exploring edges for connected and autonomous driving. In: IEEE INFOCOM 2018 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS); April 2018. pp. 148–153.

58. La Quang D, Ngo Mao V, Dinh TQ, Quek Tony QS, Shin H. Enabling intelligence in fog computing to achieve energy and latency reduction. Digit Commun Netw. 2019;5(1):3–9 (**Artificial Intelligence for Future Wireless Communications and Networking**).
59. Zhang K, Jacobsen H. Towards dependable, scalable, and pervasive distributed ledgers with blockchains. In: 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS); July 2018. pp. 1337–1346.
60. Cha S-C, Chen J-F, Su C, Yeh K-H. A blockchain connected gateway for ble-based devices in the internet of things. IEEE Access; 01 2018. p. 1.
61. Novo O. Blockchain meets IoT: an architecture for scalable access management in IoT. IEEE Internet Things J. 2018;5(2):1184–95.
62. Dorri A, Kanhere SS, Jurdak R. Towards an optimized blockchain for IoT. In: 2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI); April 2017. pp. 173–178.
63. Fan C, Khazaei H, Chen Y, Musilek P. Towards a scalable dag-based distributed ledger for smart communities. In: 2019 IEEE 5th World Forum on Internet of Things (WF-IoT); April 2019. pp. 177–182.
64. Odysseas L, Dionisis P, John G. A novel combination of distributed ledger technologies on internet of things: use case on precision agriculture. Appl Syst Innov. 2019;2:30.
65. Vögler M, Schleicher J, Inzinger C, Nastic S, Sehic S, Dustdar S. Leonore – large-scale provisioning of resource-constrained IoT deployments; 03 2015.
66. Kashif D, Amir T, Harun B, Frank E, Kurt G. A resource oriented integration architecture for the internet of things: a business process perspective. Pervasive Mobile Comput. 2015;20:145–59.
67. Uviase O, Kotonya G. IoT architectural framework: connection and integration framework for IoT systems. In: ALP4IoT@iFM; 2017.
68. Klonoff David C. Fog computing and edge computing architectures for processing data from diabetes devices connected to the medical internet of things; 2017.
69. Sahni Y, Cao J, Zhang S, Yang L. Edge mesh: a new paradigm to enable distributed intelligence in internet of things. IEEE Access. 2017;5:16441–58.
70. Hasibur R, Rahim R. Enabling distributed intelligence assisted future internet of things controller (fitc). Appl Comput Inform. 2018;14(1):73–87.
71. Aazam M, Huh E. Dynamic resource provisioning through fog micro datacenter. In: 2015 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops); March 2015. pp. 105–110.
72. Giang NK, Blackstock M, Lea R, Leung VCM. Developing iot applications in the fog: a distributed dataflow approach. In 2015 5th International Conference on the Internet of Things (IOT); Oct 2015. pp. 155–162.
73. Muthanna A, Ateya AA, Khakimov A, Gudkova I, Abuarqoub A, Samouylov K, Koucheryavy A. Secure IoT network structure based on distributed fog computing, with sdn/blockchain. 2019.
74. Tran M-Q, Nguyen DT, Le VA, Nguyen DH, Pham TV. Task placement on fog computing made efficient for IoT application provision. Wirel Commun Mobile Comput. 2019.
75. Sarkar C, Nambi AUNS, Prasad RV, Rahim A, Neisse R, Baldini G. Diat: a scalable distributed architecture for IoT. IEEE Internet Things J. 2015;2(3):230–9.
76. Mora H, Pont MT, Gil D, Johnsson M. Collaborative working architecture for IoT-based applications. Sensors. 2018;18:1676.
77. Hasibur R, Rahim R, Theo K. The role of mobile edge computing towards assisting IoT with distributed intelligence: a smartliving perspective. Cham: Springer International Publishing; 2019. p. 33–45.
78. Tang B, Chen Z, Hefferman G, Wei T, He H, Yang Q. A hierarchical distributed fog computing architecture for big data analysis in smart cities. In: Proceedings of the ASE BigData & SocialInformatics 2015, ASE BD&SI '15, pages 28:1–28:6, New York, NY, USA, 2015. ACM.
79. Bellur U, Patel P, Chauhan S, Qin Y. A semantic-enabled framework for future internet of things applications. In: 2017 IEEE World Congress on Services (SERVICES); 2017. pp. 106–113.
80. Ali MS, Vecchio M, Pincheira M, Dolui K, Antonelli F, Rehmani MH. Applications of blockchains in the internet of things: a comprehensive survey. IEEE Commun Surv Tutor. 2019;21(2):1676–717.
81. Perera C, Zaslavsky A, Christen P, Georgakopoulos D. Context aware computing for the internet of things: a survey. IEEE Commun Surv Tutor. 2014;16(1):414–54.
82. De Aguiar EJ, Faiçal BS, Krishnamachari B, Ueyama J. A survey of blockchain-based strategies for healthcare. ACM Comput Surv. 2020;53(2):1–27.
83. Pahl C, El Ioini N, Helmer S. A decision framework for blockchain platforms for IoT and edge computing; 03 2018.
84. IOTA Foundation. Iota development roadmap. (1); Dec 2016. (visited on 2-01-2019).
85. Danzi P, Kalør AE, Sørensen RB, Hagelskjær AK, Nguyen LD, Stefanović Č, Popovski P. Communication aspects of the integration of wireless IoT devices with distributed ledger technology; 2019.
86. Grujic M, Rozic V, Johnston D, Kelsey J, Verbauwhede I. Invited: design principles for true random number generators for security applications. In: 2019 56th ACM/IEEE Design Automation Conference (DAC); 2019. pp. 1–3.
87. Carson L, Himanshu T. Hardware security primitives for vehicles. IEEE Consumer Electron Mag. 2019;8(6):99–103.
88. Labrado C, Dinesh Kumar S, Badhan R, Thapliyal H, Singh V. Exploration of solar cell materials for developing novel pufs in cyber-physical systems. SN Comput Sci. 2020;1(6):313.
89. Hao J, Daniel B, Sergey S, Siyan L, Zhongrui W, Yunning L, Saumil J, Rivu M, Can L, Mingyi R, Mark B, Qing W, Jianhua JY, and Qiangfei X. A novel true random number generator based on a stochastic diffusive memristor. Nat Commun. 10 2017. 8.
90. Degada A, Thapliyal H. An integrated trng-puf architecture based on photovoltaic solar cells. IEEE Consumer Electron Magazine. 2020. p. 1.
91. Labrado C, Thapliyal H, Prowell SJ, Teja KP. Use of thermistor temperature sensors for cyber-physical system security. Sensors. 2019;19(18):3905.
92. Carson L, Himanshu T. Design of a piezoelectric-based physically unclonable function for iot security. IEEE Internet Things J. 2019;6(2):2770–7.
93. Zhao D, Ren J, Lin R, Xu S, Chang V. On orchestrating service function chains in 5g mobile network. IEEE Access. 2019;7:39402–16.
94. Noor T, Zeadally S, Alfazi A, Sheng Q. Mobile cloud computing: challenges and future research directions. J Netw Comput Appl. 05 2018. 115.
95. Venetis IE, Gavalas D, Pantziou GE, Konstantopoulos C. Mobile agents-based data aggregation in wsns: Benchmarking itinerary planning approaches. Wirel Netw. 2018;24(6):2111–32.
96. Alsboui T, Alrifaee M, Etaywi R, Jawad MA. Mobile agent itinerary planning approaches in wireless sensor networks- state of the art and current challenges. In: Maglaras LA, Janicke H, Jones K, editors. Industrial networks and intelligent systems. Cham: Springer International Publishing; 2017. p. 143–53.
97. Rauchs M, Glidden A, Gordon B, Pieters G, Recanatini M, François R, Kathryn V, Bryan Z. Distributed ledger technology systems: a conceptual framework. SSRN Electron J. 01 2018.
98. ChaoZhou A, Felandil. Untangle care. (1); October 2019.