Review Article

Distributed Intelligence at the Edge on IoT Networks

Tanweer Alam[1,*], Baha Rababah[2], Arshad Ali[1] and Shamimul Qamar[3]

[1]Faculty of Computer and Information Systems, Islamic University of Madinah, Saudi Arabia
tanweer03@iu.edu.sa; a.ali@iu.edu.sa
[2]Department of Computer Science, University of Manitoba, Canada
baha@cs.umanitoba.ca
[3]King Khalid University, Abha, Saudi Arabia
*Correspondence: tanweer03@iu.edu.sa

Abstract: The Internet of Things (IoT) has revolutionized innovation to collect and store the information received from physical objects or sensors. The smart devices are linked to a repository that stores intelligent information executed by sensors on IoT-based smart objects. Now, the IoT is shifted from knowledge-based technologies to operational-based technologies. The IoT integrates sensors, smart devices, and a smart grid of implementations to deliver smart strategies. Nowadays, the IoT has been pondered to be an essential technology. The transmission of information to or from the cloud has recently been found to cause many network problems to include latency, power usage, security, privacy, etc. The distributed intelligence enables IoT to help the correct communication available at the correct time and correct place. Distributed Intelligence could strengthen the IoT in a variety of ways, including evaluating the integration of different big data or enhancing efficiency and distribution in huge IoT operations. While evaluating distributed intelligence in the IoT paradigm, the implementation of distributed intelligence services should take into consideration the transmission delay and bandwidth requirements of the network. In this article, the distributed intelligence at the Edge on IoT Networks, applications, opportunities, challenges and future scopes have been presented.

Keywords: *Cloud Computing; Edge computing; Distributed Intelligence; Internet of Things; Wireless Sensor Networks*

1. Introduction

IoT keeps growing through technological inventions including solutions, embedded software, network virtualization, distributed systems and intelligence. The exponential increase in the rate of information collected through IoT sensor devices have contributed to the emergence of edge computing in which information is recorded at or close to the sources. The futuristic Internet is supposed to be powered by the proliferation of the IoT where everything could be linked. The revolutionary change towards distributed cloud storage to edge computation has grown rapidly in the IoT. Advances in Information technology have led to a considerable improvement in the ability of portable systems for data storage and processing, but that will proceed to grow at a rapid pace. Current concepts even so would not use low-level gadgets for any decision-maker. Throughout essence, smart gadgets are also used mostly for compatibility in connectivity and some storage at a minimal level. It is expected that 50 billion smart devices will be associated with the internet and the data created will be around 500 zettabytes by 2020 [1]. Wireless networking is bringing turned progressively prominent in computer organizations over the last 50 years [2]. The smart devices are increasing rapidly nowadays [3]. The smart device to smart device communication on the IoT environment can be a very useful approach to enhance the capabilities of smart devices [4].

Considering recent development in the IoT, it is becoming extremely difficult to ignore the increasing numbers of interconnected devices and a huge amount of produced data. Recent developments in network communication have heightened the need for both secure and high-performance network [5].

On the IoT, heterogeneous devices will collect the required information as input to use it in the network for many services. The service will decide to take any action in the real world based on the collected information. The IoT will have huge control in a wide range of aspects such as healthcare, industries, home automation, smart cities, and more [6]. Most IoT applications consist of six elements Recognition or identification, Sensing, Communication, Computation, Services, and Semantics [7]. Identifying such as the Electronic Product Code (EPC) is very important to name and match essential services. Using identification methods provides Clear identification for all objects in the network. IoT sensors sense data from related objects and send it to a database or cloud. IoT communication technologies connect heterogeneous nodes to provide services. Computation is usually processed at a centralized server and the information produced by processing is used by devices that act as actuators. IoT services are categorized into four classes [8]: Identity-related Services, Information Aggregation Services, Collaborative-Aware Services, and Ubiquitous Services. IoT semantic means the capability to extract knowledge smartly by different methods to offer the required services [9]. Figure 1 represents the IoT components: Recognition, Sensing, Communication, Computing, service, and semantics.

The computing decision-making paradigm in IoT systems is done by the centralized server which is usually located in the cloud. The End devices and gateway devices usually do not play any role in computation processes. This paradigm is not effective because transferring a huge amount of data might cause many problems related to delay, security, privacy, power consumption, etc. In general, real-time and fast decisions are essential for IoT applications, so distributed intelligence between edge and cloud currently attracts researchers' attention [10].

By 2020, 50 billion "things" will be connected to the Internet and move data produced by humans, machines, and things to the cloud [10]. Some IoT applications require a quick response, some contain private data, and some produce a huge amount of data which could be a weighty load for current network infrastructure. Hence, Cloud computing alone is not efficient enough to support these applications. At the same time, edge computing cannot omit cloud computing because edge computing has limited processing capabilities and it only processes local data. Hence, IoT systems should offer edge and cloud services at the same time. In other words, Distributed Intelligence should be enabled in IoT to be able to deal with the challenges were mentioned above. There have been recent efforts to present distributed intelligence in IoT, illuminate its requirements, architecture, uses cases, and potential challenges. The discussions of Distributed Intelligence in IoT are very limited.

This paper is organized as follows. In the second section, we introduce the related works with close look at the IoT, cloud computing, and edge computing, respectively. The third section represents the distributed intelligence in general. In the forth section, we go through Distributed intelligence regarding IoT. In the fifth section, we introduce some IoT applications that highlight the need for distributed intelligence. In the sixth section, we represent the main current challenges of enabling Distributed Intelligence in IoT. The seventh section shows the discussion and in the last section we explained the conclusion and future works.
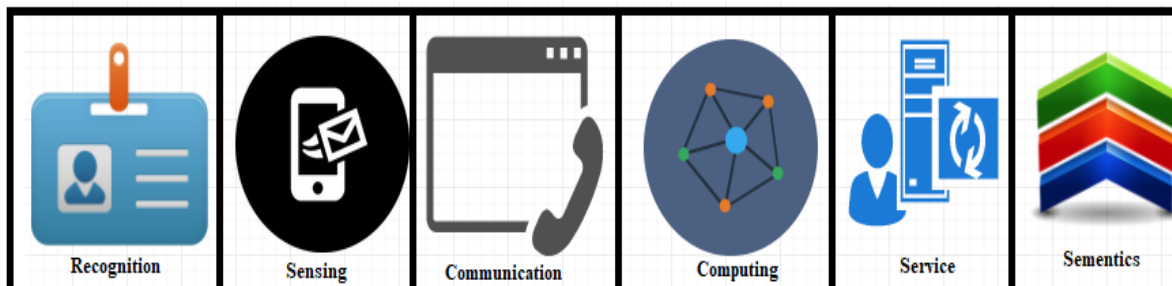

Figure 1. IoT Components [38]

2. Related Works

In 2000, M. Bonifacio published an article on the distributed intelligence [11], In this article, he discussed the distributed intelligence (DI) paradigm and he proposed a framework of multi-context systems like the specification language for distributed intelligence.

In 2004, Cecilio Angulo and Ricardo Tellez published an article on DI for smart homes [12]. In this article, they focused on the development of a framework for smart home that allows the integration of information from many sensors and actuators.

In 2007, Lynne E. Parker et.al. published an article on DI in Multi Roboting framework [13]. In this article, they were focused on three main paradigms for distributed intelligence and applied these paradigms in the multi-robot system.

In the year 2013, Gubbi, Jayavardhana, et al. published an article on IoT [14]. In this article, they present the private and public cloud interaction architecture for the IoT. They also discussed the convergence of wireless sensor networks, the Internet, and distributed computation.

In 2016, Rashid Mijumbi, et.al, published an article on Network Function Virtualization [15]. In this article, they illustrate that there is a big challenge in the management of large amounts of information exchange among IoT devices. It is therefore critical to try to find efficient methods to transfer big data over such networks. They also recommended investigating whether the existing cloud data management applications like Hadoop and Cassandra can support real-time data.

In 2017, Yuvraj Sahni, et.al, published an article on Edge Mesh. In this article, they proposed a novel approach called edge mesh that distributes the decision-making processes between edge devices to send the information to each other [6].

In 2020, Baha Rababah, et.al. published an article on distributed intelligence in IoT. In this paper, they were explained most of the concepts related to the distributed intelligence in IoT [38].

The recent innovative developments of information and communication technologies related to ubiquitous communication, pervasive computing, and ambient intelligence play an essential role in IoT birth [16]. Ubiquitous Communication a concept in communication and computer networks where interconnection can be made anywhere and anytime. Pervasive computing is the improvement in smart devices including the computational feature process. Ambient Intelligence is the ability of objects to sense and respond to the physical environment. Recently, researchers have shown an increased interest in IoT. The IoT is a paradigm to connect an unlimited smart device with their unique identifications anytime and anyplace using the IoT communications protocols [17] [18] [19] [20]. The IoT objects might be mobile phones, food, clothing, machines, tables, sofas, doors, etc. [21]. The IoT impacts everyday life such as home, work, health, transportation, etc. It has many related aspects. Below, key aspects of IoT are discussed.

2.1. Radio-frequency Identification (RFID)

The RFID technology is used in IoT to identify or track the smart object electronically. It uses power from nearby RFID. It can store and/or retrieve information using electromagnetic transmission and a radio frequency (RF) compatible integrated circuit [22]. A simple RFID system consists of RFID readers and RFID tags [23] [24] [25]. To date, RFID systems have been utilized by many departments in a successful industry [26]. RFID system benefits are providing accurate, real-time information about the equipment, reducing labor costs, streamlining business processes, improving overall business efficiency. The RFID technology is widely using in organizations like strategic, production network administration, and health services checking [27], as it can be used for identification and tracking smart objects [28]. The RFID currently depends on the following two main points.
   a)   RFID Active systems with transmission
   b)   Application management techniques [29].

There are many technologies available to develop RFID-based applications [30]. In the future, researchers can develop an integrated platform with WSN and RFID together for scanning the smart objects in the real-time system. Specifically, sensor innovations are rising day by day, for example, electromagnetic sensors, biosensors, off-board sensors, and sensor gadgets, etc. These smart sensors can collect the RFID data so that researchers can develop strong IoT apps for smart organizations.

They work together with RFID systems to get the right data of their locations, movements, temperature, pressure, light, etc. It can consist of sensing objects that communicate wirelessly and hop-by-hop to gather information and detect a certain event in the physical environment [31] [32]. The WSN provides a variety of right information that is related to health informatics [33], military applications [34], farming [35], industry [36], etc. These sensors work with each other to provide different beneficial data that might be used in certain applications and services. However, sensor networks face many problems in terms of communication and resource constraints [37]. For communications, there are many issues such as short communication range, mobility, reliability, security, etc. [38].

The development of the Internet has led to interconnect objects and an intelligent environment. In this case, identifying and managing objects is very important for IoT to succeed, as it consists of a large number of objects. Addressing adds more features to IoT which are uniqueness, reliability, persistence, and scalability [39] [40] [41]. The current IPV4 is only able to identify a group of sensors based on their geographical location. But, the current requirements for IoT is to identify every sensor individually based on its identification, location, or/and functions. IPv6 able to achieve those requirements, as it has a larger address size [42] to address and manage IoT objects efficiently, the IETF standardized adaption protocol for IPv6 which is called 6LoWPAN. It represents by both RFCs 4944 [43] and 6282 [44]. It allows compression techniques to compress the IPv6 and UDP packets after deleting the excessive data from the header part.

Due to the object heterogeneity, limited storage, and processing capabilities, the middleware and application layer plays a key role, with the main objectives of functional abstraction and device communication. The Middleware is categorized in the layers such as object abstraction, service management, service composition, and application [45]. In a generic IoT system, the end devices (sensors, smart devices, etc.) usually collect specific information such as temperature, light, pressure. Etc. This information passes through limited processing locally. Then it is sent to the external gadget for computations. After that, it can transmit to the local area network until it reaches to the internet then the cloud-based services. The cloud-based service will convert received information into knowledge after some processing operations. This knowledge might need to be stored or action needs to be performed. To support IoT, middleware should handle the following challenges: interoperability between heterogeneous devices [46] [47], context awareness [48], managing data [49], privacy and security [50], and device discovery [51]. The current proposed IoT system has many challenges. We have summarised the challenges that might be handled by enabling Distributed Intelligence as follow:

2.1.1. Latency

In many IoT applications, sensors sense data then send it to the cloud to be processed. All intelligence and actions are centralized in the cloud. However, the cycle of sensing and actuating might take a specific interval of time which causes high latency. For example, self-driving car's sensors generate around one gigabyte every second [52]. Sending this amount of data to the cloud and waiting for action takes time, it might cause a crash. Most IoT applications are real-time which need to take action in an instant. Furthermore, Due to the limited Internet bandwidth and internet delay, cloud servers are unable to process coming data and take actions instantly.

2.1.2. Offline processing

In general, IoT cloud-based applications will completely be offline during an internet disconnection. For example, a self-driving car that is fully controlled by the cloud will not be able to take any decision or action, if the cloud service is unavailable.

2.1.3. Bandwidth

There is no doubt that a cloud is an efficient place for data processing as it has more powerful computing capabilities than the devices at the edge. However, network bandwidth is not currently enough to send a large quantity of data efficiently. For example, Boeing 787 generates 5-gigabyte data every second [53]. However, bandwidth between it and satellites or the base stations are not able to transmit this big amount of data.

2.2. Cloud Computing

Cloud Computing allows the users to process, access, and storage data remotely over the internet [54]. It allows sharing the resources, software, services with less effort over the networked computers that use the internet [55]. In the realism of the internet, security has been perceived as a prominent inhibitor of embracing the cloud paradigm. Since the cloud environment is a distributed architecture, which it's resource storage and management may lay in any place in the world, many concerns have been raised over its vulnerabilities, security threats, and challenges. The involvement of various parties has widened these concerns based on each party's perspective and objective. It has been determined that three dominant parties participate in the cloud environment.

i.   **Service providers:** Service providers provide services to the consumers intensified over public and hybrid cloud [56] where issues related to unauthorized access and cyber-attacks may jeopardize the service availability.

ii. **Service consumers:** Their concerns may focus on issues related to data privacy and quality of service. Besides, their concerns regard service availability and interoperability.

iii. **Service regulators:** Their concerns may focus on issues related to service standard violations. Thus, issues related to interoperability would affect them greatly. It is fair to say that all previously mentioned party concerns might be correlated and associated with other parties.
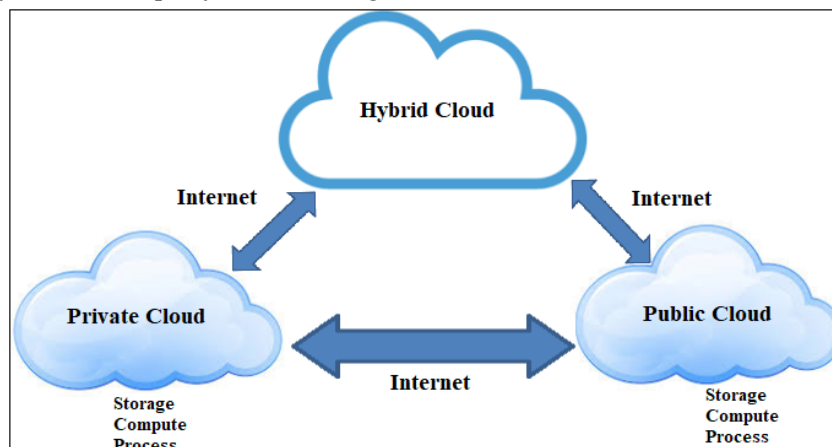

Figure 2. Cloud service and deployment model [56]

2.2.1. Public cloud

All services have been provided in a public environment where consumers can access a pool of resources that is managed by a hosted organization. Due to its nature, this type of environment may raise critical concerns over security problems [57].

2.2.2 Private cloud

Services have been provided by a third-party vendor which separates it from public access. Consequently, it is safer than the previous development model because it prevents unauthorized access [58].

2.2.3. Community cloud

Services have been provided to a specified community where all members have an equal right of accessing the shared resources [59].

2.2.4. Hybrid cloud

Services are provided as combustion of more than one cloud (public cloud, private cloud, and community cloud). It could inherit any type of vulnerability or risk that resides within the previously mentioned parties [60]. Figure 2 represents the cloud services and deployment model.

2.3. Edge Computing

Edge computing methodology is used to process data on the edge of networking to optimize cloud computing [61]. The performance evaluation of edge computing for data processing is better

than cloud computing (see figure 3). The previous techniques such as cloudlets [62], fog computing [63], and data center are also developed because cloud computing doesn't perform better for the process of the data on the edge of networking [64].
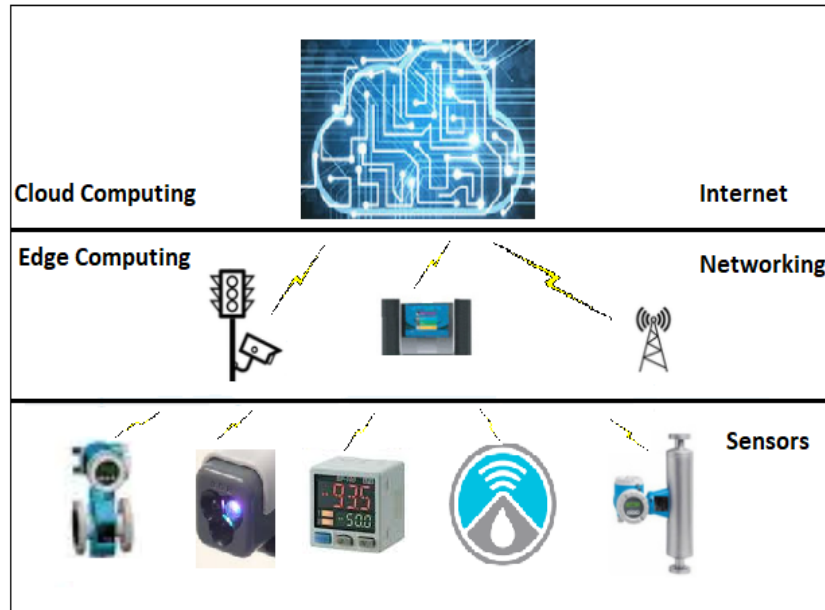

Figure 3. Edge Computing [61]

Edge computing becomes the shared technological development framework wherein device information is collected however closely to the origins as appropriate on the boundaries of the service provider. Information is the lifeline of successful corporation, offering useful financial information or encouraging actual monitoring of commercial enterprise planning and execution. Organisations are overflowing in the massive amount of data, and large quantities of data could be regularly obtained from sensors and IoT devices running in multiple locations from distant places and unfriendly situations from anywhere in the globe.

3. Distributed Intelligence

Distributed intelligence means that a group of related entities work logically together planning, solving problems, abstract thinking, understanding ideas and language, learning, and making a decision. The entity can be agents, humans, network devices, robots, sensors, and so forth where each one responsible for a specific objective. After processing the raw data will change into smart data the distributed intelligence (see figure 4). The peoples are knowing about distributed intelligence in the form of teams such as the research team consists of co-investigators, fractional staff, technical staff, and postgraduate research students. The objectives of distributed intelligence in the area of communication systems are to work together as proficiency as human teams to achieve specific many purposed tasks.
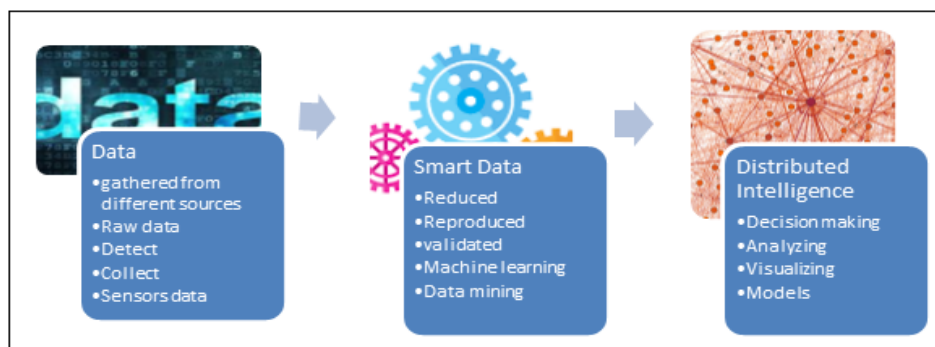

Figure 4. Distributed intelligence [65]

In general, enabling distributed intelligence solutions to help to solve certain problems that are related to time or function as enables decreasing the task completion time and decreases the

complexity for each entity. Creating a group of entities for the system enhance the robustness and reliability. Enabling distributed intelligence in computer and communication systems help to handle parallel computations, distributed systems, and multi-agent systems. There are many possible paradigms to enable distributed intelligence in the systems. Understanding the types of distributed intelligence is essential to be able to specify the appropriate paradigm for a specific type of distributed intelligence. One of the most popular ways is to understand the type of interactions between the entities in the system. The interactions between the entities can be divided into four categories: Collective, Cooperative, Collaborative, and Coordinative. Table 1 describes those categories.

Table 1. Smart devices interaction Types [65]

Collective	Cooperative	Collaborative	Coordinative
The Smart devices are not well-informed of another smart device under a network.	The Smart devices are well-informed of another smart device.	The Smart devices are well-informed of another smart device under a network.	The Smart devices are well-informed of another smart device.
The smart devices can share their actions and objective with neighborhood devices.	The smart devices can share their actions and objective with neighborhood devices.	The smart devices have individual objectives however they help each other to accomplish their objectives.	The smart devices don't share a common objective, and their actions are not helpful to neighborhood devices.
Ex. Swarm robot framework.	Ex. In the Multi-robotics system, many robots work together to accomplish a common objective.	Ex. In the multi-robot system, multiple robots depend on each other to achieve a common objective without the help of other robots.	Ex. Traffic Controlling System.

Distributed intelligence has different paradigms. Using a paradigm based on the problem's space situation allows the system designer to determine the right solution. Commonly, those paradigms are inspired by insects, animals, or human society. In general, there are three common paradigms to enable distributed intelligence in the systems:

3.1. Swarms intelligence paradigm

Bonabeau [66] defined Swarms intelligence as "any attempt to design algorithms or distributed problem-solving devices inspired by the collective behavior of social insect colonies and other animal societies". Examples in natural systems of Swarm intelligence are bee-inspired, ant colonies, fish schooling, and others [67]. In swarm intelligence, the demand for entities in the communications can be reduced. The entity can sense the right data on the local network. It is a strong approach to the application that needs the same task to be accomplished through decentralized control. Swarm intelligence paradigm can be used in the different field of computer and communications systems [68] such as Swarm Intelligence Routing [69], Swarm robotics [70], Crowd control [71], Software testing [72], Image segmentation [73], Data mining [74].

3.2. Organizational and Social paradigms

These models are used for modeling human organizational intelligence in computer and communication systems [75]. Sociology, economics, and psychology, etc. had proved to understand that the products have the capabilities of intelligent systems to work in a team to solve the complex problems.

3.3. Knowledge-based, ontological, and semantic paradigms

It is depending on share the knowledge among different entities. The purpose is to allow different entities to easily share and understand knowledge from different sources. These methods require language to represent knowledge. Knowledge systems are part of knowledge management technologies to represent knowledge application processes [76]. It is commonly used to deal with uncertain problems. This approach is using in a huge range of applications like decision support systems [77] [78]. The applications concern reusing the knowledge in more easy, effective, and

efficient. This model reduces communication by using common assumptions about vocabulary and semantics.

Currently, it is noticed that many researchers are interested in studying distributed intelligence. According to a Google Scholar search, Figure 5 represents the google trends that contain the exact phrase "distributed intelligence", IoT network, and Edge computing for the last five years. The data explicitly illustrate an increasing interest in this field, as it plays an essential role in developing computer and communication systems [79].
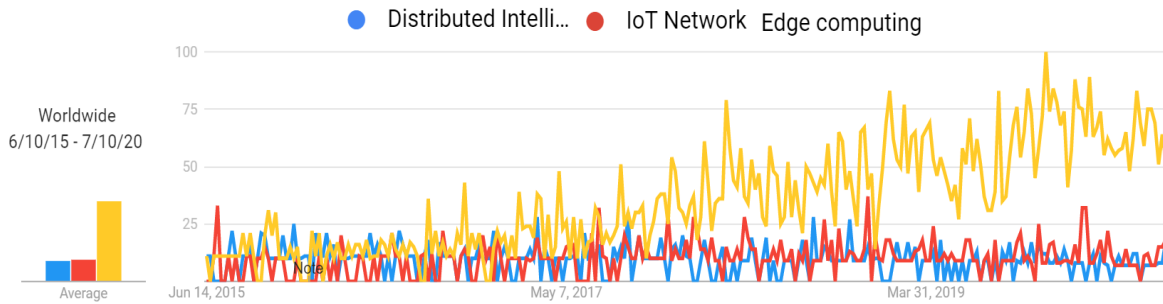

Figure 5. Distributed intelligence, Edge computing and IoT Networks in the last 5 years according to the google trends [79]

4. Distributed Intelligence in IoT

Most IoT data is generated close to the edge of the network where the things are. Usually, IoT data processing is performed close to the source. Therefore, the intelligence is distributed within IoT architecture layers. Real-time IoT data produced by a wide range of end devices such as sensors, locating, and identification devices. Those devices send data thousands of times per second. The lifecycle of produced data goes through different stages of filtering, summarizing, pattern, detection, interpreting, and processing. Understanding and processing the data locally is usually better than send them away for processing. The intelligence not only on the top layers of IoT but also there is local in the end and edge devices.

Sensor data can be read by the local processor for tens or hundreds of times per second. The local processor may, in turn, send repeated data about important status changes or events to the gateway. This may be connected to a LAN with a server at the factory level and ultimately linked to the enterprise system. The actual connection to the Internet may be away from peripheral sensors and processors. Additionally, Internet devices may be things that are intermittently connected to the network only. End devices might not be able to connect to the network all the time.
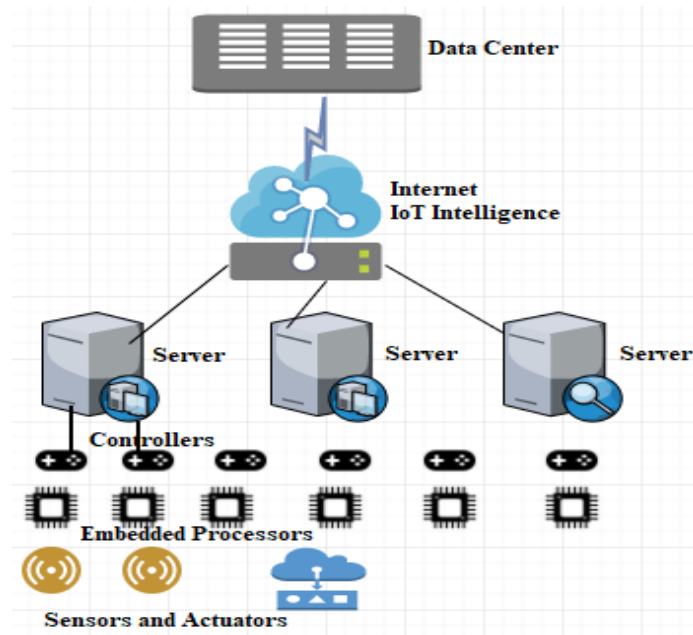

Figure 6. Distributed Intelligence in IoT

The current IoT model has many limitations to support real-time applications as it was mentioned in section 3.1. The intelligence should be everywhere from the end layer to the top of IoT depending on the case as shown in Figure 6. In many states, intelligence should be spread over several layers to achieve the right functionality and performance. The previously mentioned challenges let researchers think about the distribution of intelligence over IoT components. In general, Distributed Intelligence in IoT can be defined as a model, technique, and algorithms for collaboration between all IoT components from sensors to cloud to accomplish the desirable support of communication and application in a large scale network. It enables the communication and processing tasks to existing at the right place and time. Recently, the researchers highlight the importance of enabling Distributed Intelligence in IoT so there has been an increasing interest to support distributed intelligence in IoT.

There are a limited number of proposals for the distributed intelligence paradigm in IoT. In [80] published a white paper on distributed intelligence architecture in a wireless network.
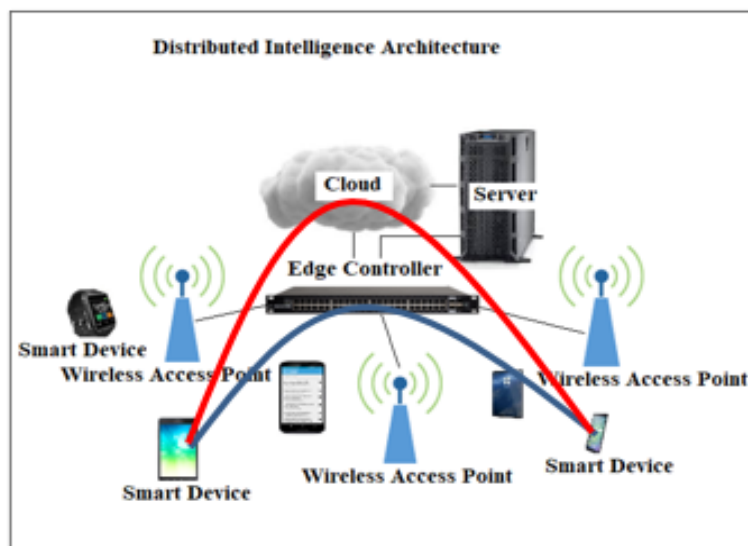

Figure 7. Distributed Intelligence at the Edge on IoT

In a traditional hub and spoke architecture, access points send all traffic to the controller that manages all network policies. This will not work well with an enormous amount of real-time data to be transmitted because it needs high bandwidth. Increased bandwidth highlights the need for a new architecture that able to increase the power of controller processing to avoid the negative impacts on real-time data. Furthermore, this architecture does not work well with the current and future 802.11 technologies. Another drawback of the traditional architecture is the failure of the controller leads the network to go down. The previously mentioned challenges force many organizations to think of a solution that supports intelligence at the edge of the network to enhance traffic flow without any negative impact on security and QoS. The proposed paradigm as shown in Figure 7 for distributed intelligence from Motorola permits optimized routing data locally or to the internet without sending traffic to the controller. Moving the intelligence and making a decision down helps the network to be dynamic, responsive, and avoid bottlenecks. This architecture improves Scalability, Reliability, Survivability; IT budgets go farther, Security, and Power consumption.

Furthermore, some researchers suggested useful methodologies to activate distributed intelligence in IoT. In [81] an architecture named sensor function virtualization to enable distributed processing is proposed as shown in. This approach offloads a specific task from limited capability nodes to unlimited capability infrastructure like a cloud, virtual gateway, etc. This approach decomposes the chosen function into smaller modules. The modules are sorted according to their functionality. For example, the module responsible for implementing 6LoWPAN compression will categorize in the network category. Once network traffic reaches a machine that runs virtualization of sensor function, the packets move up over a group of modules and move down over to an outgoing network interface. After that, all of the modules that are running on a set of machines are combined. The main feature of the approach is elasticity because some functions can be running in the cloud and it also can handle the increased load by allocating more resources to the cloud. Furthermore, the

approach does not rely on cloud infrastructure because it takes in its consideration the internet is unavailable and high latency. In [6] proposed an approach called Edge Mesh that uses edge devices for data processing as one computing paradigm. The data and reckoning tasks can be divided between edge devices.

5. IoT Applications require Distributed Intelligence

5.1. Smart Home

In the past, home automation was a science fiction idea. For example, Ray Bradbury imagined homes were interactive and ran themselves. It was terrifying until the actual benefits of home automation were considered by humans, and then the idea started to be more comfortable [83] In the 19th century, many hardware and software invention occurred that leading up to smart home automation. Besides, the X10 standard was industrialized to allow sending and receiving broadcast messages via radiofrequency. Currently, the invention of raspberry pi helps researchers to find and develop the smart home system [84]. The Raspberry Pi is a cheap, small-sized computer that plugs into an LCD, keyboard, and mouse. It has different types of communication ports such as Ethernet, USB ports, HDMI ports. It can perform all the functions of a desktop computer like word processing, internet browsing, playing the game, etc. it is currently used in a wide range of projects because of its ability to interact with the outside world [85], [86]. With raspberry pi, home automation becomes interesting. Many researchers proposed a smart home system using a raspberry pi as an edge device [87]. Home automation includes all that building automation provides door and window controls, air condition controls, multimedia controls, lights controls, cooker controls, etc. Smart home means to control home with the help of various technologies like GSM, Wi-Fi, Bluetooth, Zig bee and so on to be able to manage home remotely [88], [89], [90].

Nowadays, all the suggested proposals of smart home aim to build comfort, secure, accessible, safe system inside the home with consideration of minimizing operating energy and cost. Sensors are attached to all targeted home appliances to be considered smart objects. They can sense, process data, and communicate. These devices from time to time carry out sensing and perform basic data processing before sending the data to the hub, gateway or directly to the cloud [91]. There are many challenges with regard to smart home system design, but this paper concern of distributed intelligence only. In the traditional proposed smart home system, all data need to be transferred to the cloud where the decision is made. This strategy takes longer time and threatens security because data is shared with outside network. By applying distributed intelligence, the required data only will be transferred to the cloud. The intelligence will be distributed through several layers in order to provide the required functionality and performance so the decision will be made by cloud, edge, or any device between them depending on the situation [92]. Moreover, when internet service is not available, it is difficult to communicate with the cloud to take the decision. Enabling distributed intelligence will allow different devices within the system to share the data and decision even without the cloud. The system will be able to work offline and provide the essential coordination between the edge and end devices. In addition, real-time data is very important in an emergency.

5.2. Internet of Vehicles

According to the Victoria Transport Policy Institute's Urban Mobility Report (UMR), the congestion cost will reach $199 billion by 2020 due to the increasing number of vehicles [83]. Internet of Vehicles (IoV) or sometimes called Intelligence Transportation System is an IoT application domain for sensing, analysis, control and communications technologies to vehicle transportation to enhance safety, flexibility, privacy, security, latency and reduce the cost [84]. IoV is a group of applications for Information processing and sharing to ease overcrowding, enhance traffic management, reduce environmental influence, and increase revenue for transport to business users and the public [85]. It is an advanced technology with the integration of sensors, internet, wireless communication, protocols for exchanging information among fast speed vehicles.

IoV should be able to process real-time data efficiently. But, the traditional system with central data processing and communication experience many significant challenges such as Connectivity

and coverage, Communication and energy cost, Congestion, Coordination and implementation, and Traffic incident notification. It cannot efficiently deal with real-time data, as each vehicle will transfer a big size of generated data to the cloud through the internet. A large number of vehicles will impact the network as it will cause a bottleneck. Furthermore, the traditional system may cause privacy problems because the current location of vehicles is shared. They also share the beginnings and journey's end of tours with the cloud server. In fact, enabling distributed intelligence in IoV will reduce the delay and enhance safety. Most of the IoV applications will benefit from distributed intelligence. For example, rerouting vehicles in the traffic management system for congestion avoidance needs the information to be shared between vehicles from different road areas. This shared information is used to re-route the vehicles. Sharing information between vehicles will prevent shifting the congestion from one route to another.

5.3. An Autonomous Agriculture Intelligent Machinery

Given the state of precision agricultural technology, this technology can allow accurate cultivation of agricultural machinery, strict application of fertilizers and pesticides, robotic welding, precision parallel grain's harvesting, and yield control (see figure 8). Precision farming equipment usually uses GPS with an accuracy of a few centimeters for automatic machine steering and when and where to apply specific amounts of seeds, fertilizers, and pesticides [96].

The data from GPS, GIS, and On-board sensors are combined with each other to enable the machine making real-time decisions and tunings. The onboard sensors measure plant biomass, chlorophyll content, soil nitrogen content, etc. For example, when using pesticides, the system may use sensor data and GIS data to adjust the height of the boom, the flow of the nozzle, and the size of the droplet.
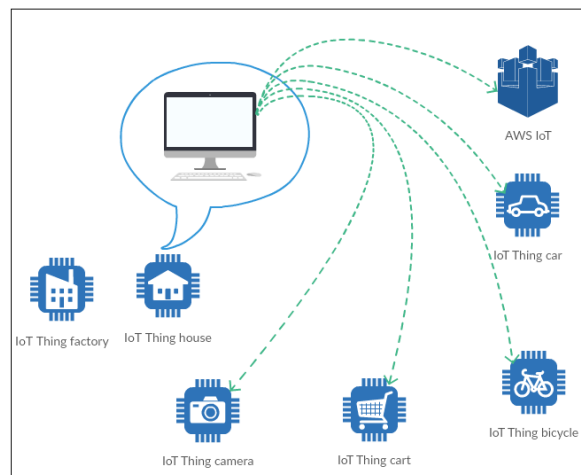
Figure 8. Agriculture Intelligent Machinery

Farming, fertilizing or harvesting machines download GIS data to guide the course and limits of their activities. GIS data may also specify areas of skipping or areas that should receive different types or levels of treatment. The incoming data from the sensor is used to direct the device in real time, but a brief copy of the data is also recorded and returned to the central farm register. External information and data, such as weather forecasts and crop prices, can also be provided to help the system improve profitability. Therefore, we can see a number of two-way communication layers for intelligent IoT in a modern farm environment.

5.4. Smart Mine

One of the fast-growing areas in IoT is the heavy equipment used in construction, mining, agriculture, and logging. Mining equipment provides some possible examples of IoT. Working with those enormous and powerful machines is dangerous. If a worker does not be careful, the result might be fatal. So, the essential role of IoT in this environment is enhancing safety through warning technology like location sensors, cameras, and RF locating devices. **A**utonomous Operation reduces

the chances that a worker is hurt as no need to be in a dangerous environment. There are autonomous continuous mining machines such as Joy Global's Longwall System. It has 7,000 sensors, actuators and controllers to direct its shearer with its armored face conveyor, belt conveyor, powered roof support system, and pump stations. The system can extract 2,200 tons per hour. The system constantly transfers data to other parts of the systems and systems under the surface, this includes communication with underground transport vehicles, as well as automatic mining trucks and automatic trains on the ground, all connected to control centers hundreds of miles away. Joy turns data generated by the sensor into actions to make real-time decisions on the system. For example, decreasing the idle time of huge wall systems for one hour can reduce the operation costs of mine operators. Again, you can combine complex multi-level machines into a cohesive and coordinated environment for several interconnected systems [97].

6. Key Challenges

6.1. Heterogeneity

IoT is a heterogeneous system as it has different hardware, architecture, infrastructure, and technologies [98]. IoT devices would be able to understand the incoming data to accomplish reliable communication. IoT devices support communications protocols with the low data rate, packet losses, and stochastic channel variations [99]. Enabling distributed intelligence means some tasks should be performed on edge nodes. But edge and end nodes are most heterogeneous. In this case, it will be difficult to deploy the tasks between those nodes.

6.2. Security and privacy

IoT brought many challenges related to security and privacy such as identification, authentication, access control, etc. [100]. Possible attacks should be expected during tasks distributions and data communication. Heterogeneous Devices are distributed to interact with each other which make it complicated to apply protection mechanisms [101].

6.3. Resource and Tasks management

The huge numbers of IoT devices, network, and traffic complexity, and the capability of constrained devices increase resource and task's management difficulty. The tasks are typically divided between edge devices. However, as the cloud has the capability to process a large amount of data, it should take part in big data analysis and management [102]. Thus, the tasks should be distributed between a group of devices based on application requirement and resources availability. The main challenge with this issue is to distribute the tasks between edge devices as it needs computation and communication joint optimization. Edge devices should manage access control, resource, Quality of Service, privacy and security, and data. Using Edge devices to manage all tasks at the same time is not an easy task because these devices are heterogeneous, resource constrained and distributed. In addition, as the IoT devices are heterogeneous, they might not be able to support the same type of tasks. The device might not be able to support some tasks because it has not enough resources.

6.4. Distributed computing Algorithms

In fact, distributing tasks between IoT devices is also a big challenge [103]. The traditional distributed computing algorithms cannot be directly applied for distributed intelligence in IoT as communications and computations tasks should be taken into consideration together. The decision should not also totally central based. Distributed intelligence requires implementation of advanced algorithms that can enable local processing and decision when it is needed. On the other words, the algorithm should enable the components to communicate and negotiate without central influence [104].

6.5. Standardization and interoperability

Another critical challenge with distributed intelligence and task assignment is changing the current code for various devices and application. Lack of standardization also prevents devices to communicate and work with each other to share data and tasks. Standardization is the key to the success of IoT especially with enabling distributed intelligence. Standardized guidelines include data acquisition protocols, data communications, task allocation and others [105].

6.6. Scalability and automation

The scalability is a major challenge associated with IoT. In order to get all the benefits of Distributed Intelligence in IoT, it should be able to manage millions of IoT devices. It is challenging to control, configure, and monitor millions of devices [106]. In addition, IoT with distributed intelligence will only be scaled, if all the functions can be automated. Thus, enabling of distributed intelligence based on the automation of processes.

7. Discussion

The secret to the growth of the IoT and the capacity to identify, evaluate providing huge information in the cloud is edge computing, the new scientific model wherein information is recorded from edges of the network. Edge Computing is attracted prominence as being one of the top competitive technological advancements in the last two years and it has a creative possibilities. This offers reduced waiting time periods, low latency rates, and much more reliable information security than cloud services. Technological advances, in general, are increasingly integrating edge computing. Throughout this paper we have presented the terms, contexts, and benefits and drawbacks of distributed intelligence, explain how it works and organize it structurally with distributed intelligence techniques, provide details of its applications in various areas, and finally propose several changes and address the key challenges of its implementation.

Edge computing is a modern innovation which has already recently gained interest, and there is space for development to promote effective distributed intelligence computation. Through analyzing information from edge, decreasing reply time and enhancing performance, a larger amount of users can shift from the clouds to the edges computing. There are three issues with cloud, they are delivery delays, high computation loads and infringements of data; cutting-edge communication technologies could be used to address this challenge. Edge computing is a smart move for true controlled activities with complex field features and is independent from the data center. These are considered to be a significant key element on the business when we use different technologies like artificial Intelligence and Data Analytics and IoT in a structured way to achieve the performance goals.

Cloud is also an essential part of this approach where it is linked to ending nodes through edge nodes. This architecture enables distributed intelligence because all computation tasks are shared between edge devices. All those devices are connected through routers. Edge devices belong to the edge mesh network perform data processing and computation tasks. They share data through the virtual mesh network. They also proposed a task management framework to manage and distribute tasks among edge devices. The paradigm is split into three layers equivalent to end devices, edge mesh, and cloud. This paradigm enables edge devices to perform computation locally rather than transfer data to a cloud server outside the local network to perform the computation. In other words, this approach enables local data processing and distributed intelligence which enhances latency, security, reliability, scalability, fault tolerance, services, and privacy. In [82] proposed an approach for enabling distributed intelligence in IoT controller that depends on the intelligence of edge and cloud. They use an edge controller to provide intelligence close to things. They also use a cloud controller to provide a high level of intelligence. This approach includes the belief network technique for making a decision based on prior and new beliefs. Learning a new belief based on probability. It also employs reinforcement learning to learn experiences for learning and prediction. They proved that using a belief network that depends on knowledge-based management reduces the prerequisite of instructions and it also enhances processing time for the gateway (edge controller).

8. Conclusion and Future Work

This paper has presented the role of distributed intelligence at the Edge on IoT architecture, with an emphasis on its importance, latest proposed paradigms, and applications that requires it. This article alos pointed out the main challenges for enabling and develop distributed intelligence at the Edge in IoT. Distributed Intelligence in IoT plays an important role to support the exact communication and processing functions to be offered at the exact place at a certain time. The distributed intelligence combines the models, techniques, and algorithms to support decision making in a distributed environment of the IoT. Distributed Intelligence is basically related to Artificial intelligence, and there are many types of research about enabling it under artificial intelligence. Therefore, in the future, the researchers of artificial intelligence and communication networks could work together on the popular applications such as smart home, intelligence of vehicles, intelligence watering system, and so on.

References

[1]   Networking, C. V. (2016). Cisco global cloud index: Forecast and methodology, 2015-2020. white paper. Cisco Public, San Jose.

[2]   Alam, Tanweer. (2017). Fuzzy control based mobility framework for evaluating mobility models in MANET of smart devices, ARPN Journal of Engineering and Applied Sciences, 12(15), (2017) pp.: 4526-4538.

[3]   T. Alam and M. Aljohani. (2015). Design and implementation of an Ad Hoc Network among Android smart devices, International Conference on Green Computing and Internet of Things (ICGCIoT), Noida, pp. 1322-1327, doi: 10.1109/ICGCIoT.2015.7380671.

[4]   Alam, Tanweer. (2017). Middleware Implementation in Cloud-MANET Mobility Model for Internet of Smart Devices. International Journal of Computer Science and Network Security IJCSNS 17(5), pp. 86-94.

[5]   Baha Rababah, Shikun Zhou and Mansour Bader. (2018). Evaluation the Performance of DMZ. International Journal of Wireless and Microwave Technologies (IJWMT), Vol.8, No.1, pp. 1-13, DOI: 10.5815/ijwmt.2018.01.01.

[6]   Sahni, Y., Cao, J., Zhang, S., and Yang, L. (2017). Edge mesh: A new paradigm to enable distributed intelligence in internet of things. IEEE access, 5, 16441-16458.

[7]   Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., and Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. IEEE communications surveys & tutorials, 17(4), 2347-2376.

[8]   Xiaojiang, X., Jianli, W., and Mingdong, L. (2020). Services and key technologies of the internet of things. ZTE Communications, 8(2), 26-29.

[9]   Barnaghi, P., Wang, W., Henson, C., and Taylor, K. (2012). Semantics for the Internet of Things: early progress and back to the future. International Journal on Semantic Web and Information Systems (IJSWIS), 8(1), 1-21.

[10]   Cisco Systems. (2015). Fog Computing and the Internet of Things: Extend the Cloud to Where the Things Are.

[11]   Bonifacio, Matteo, Paolo Bouquet, and Alberto Manzardo, (2020). A distributed intelligence paradigm for knowledge management. AAAI Spring Symposium Series 2000 on Bringing Knowledge to Business Processes.

[12]   Angulo, Cecilio, and Ricardo Tellez. (2004). Distributed Intelligence for smart home appliances. Tendencias de la minería de datos en España. Red Española de Minería de Datos. Barcelona, España.

[13]   Tanweer Alam, and Mohamed Benaida, (2020). Blockchain, Fog and IoT Integrated Framework: Review, Architecture and Evaluation. Technology Reports of Kansai University, Volume - 62 , Issue 02.

[14]   Gubbi, J., Buyya, R., Marusic, S., and Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future generation computer systems, 29(7), 1645-1660.

[15]   Mijumbi, Rashid, Joan Serrat, Juan-Luis Gorricho, Niels Bouten, Filip De Turck, and Raouf Boutaba. (2016). Network function virtualization: State-of-the-art and research challenges. IEEE Communications Surveys & Tutorials 18, no. 1, 236-262.

[16]   Dohr, Angelika, Robert Modre-Opsrian, Mario Drobics, Dieter Hayn, and Günter Schreier. (2010). The internet of things for ambient assisted living. In Information Technology: New Generations (ITNG), 2010 Seventh International Conference on, pp. 804-809.

[17]   Doukas, C., and Maglogiannis, I. (2011). Managing wearable sensor data through cloud computing. In 2011 IEEE Third International Conference on Cloud Computing Technology and Science (pp. 440-445). IEEE.

[18]   Ganchev, Ivan, Zhanlin Ji, and Máirtın O'Droma. (2014). A generic IoT architecture for smart cities. pp. 196-199.

[19]   Komalavalli, C. (2017). Convergence of Wireless Sensor Networks, Internet of Things, Big Data: Challenges. Convergence 6, no. 6.

[20]   See, Jin-Chuan, Wai-Kong Lee, Kai-Ming Mok, and Hock-Guan Goh. (2017). Development of LLVM compilation toolchain for iot processor targeting wireless measurement applications." In Smart Instrumentation, Measurement and Application (ICSIMA), 2017 IEEE 4th International Conference on, pp. 1-4. IEEE.

[21]   Kosmatos, Evangelos A., Nikolaos D. Tselikas, and Anthony C. Boucouvalas. (2011). Integrating RFIDs and smart objects into a Unified Internet of Things architecture. Advances in Internet of Things 1.01.

[22]   Li, Heng, Greg Chan, Johnny Kwok Wai Wong, and Martin Skitmore. (2016). Real-time locating systems applications in construction. Automation in Construction 63. Pp. 37-47.

[23]   Lee, Youngjae, Jinhong Kim, W. Yu, and Kiyoung Moon. (2016). An RFID-based real-time localization of multiple AGV (Automatic Guided Vehicle) system for the guided path navigation. In Inter. Conf. on Indoor Positioning and Indoor Navigation (IPIN), Spain, pp. 1-2.

[24]   Windmann, Stefan, Oliver Niggemann, Holger Ruwe, and Friedrich Becker. (2017). A novel self-configuration method for RFID systems in industrial production environments. In Emerging Technologies and Factory Automation (ETFA), 22nd IEEE International Conference on, pp. 1-5.

[25]   Saha, Rajesh, Santanu Maity, and Nripendra Trigunayat. (2015). Enhancementof gain, bandwidth and directivity of a patch antenna by increasing dielectric layers of the substrate through micromachining technique for RFID application. In Computer Engineering and Applications (ICACEA), 2015 International Conference on Advances in, pp. 321-324.

[26]   C. Sun, (2012). Application of RFID Technology for Logistics on Internet of Things Things. AASRI Conference on Computational Intelligence and Bioinformatics, vol. 1.

[27]   Jia, Xiaolin, Quanyuan Feng, Taihua Fan, and Quanshui Lei. (2012). RFID technology and its applications in Internet of Things (IoT). In Consumer Electronics, Communications and Networks (CECNet), 2nd International Conference on, pp. 1282-1285.

[28]   Lim, Ming K., Witold Bahr, and Stephen CH Leung. (2013). RFID in the warehouse: A literature analysis (1995–2010) of its applications, benefits, challenges and future trends. International Journal of Production Economics 145.1, pp. 409-430.

[29]   M. Aljohani and T. Alam, (2015). An algorithm for accessing traffic database using wireless technologies, 2015 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), Madurai, pp. 1-4. doi: 10.1109/ICCIC.2015.7435818

[30]   Romero, D., Hermosillo, G., Taherkordi, A., Nzekwa, R., Rouvoy, R., and Eliassen, F. (2010). RESTful integration of heterogeneous devices in pervasive environments. In IFIP International Conference on Distributed Applications and Interoperable Systems (pp. 1-14). Springer, Berlin, Heidelberg.

[31]   Yetgin, Halil, Kent Tsz Kan Cheung, Mohammed El-Hajjar, and Lajos Hanzo Hanzo. (2017). A survey of network lifetime maximization techniques in wireless sensor networks. IEEE Communications Surveys & Tutorials 19, no. 2, pp. 828-854.

[32]   Rawat, Priyanka, Kamal Deep Singh, Hakima Chaouchi, and Jean Marie Bonnin. (2014). Wireless sensor networks: a survey on recent developments and potential synergies. The Journal of supercomputing 68, no. 1, pp. 1-48.

[33]   Saleh, Nayif, Abdallah Kassem, and Ali M. Haidar. (2018). Energy-Efficient Architecture for Wireless Sensor Networks in Healthcare Applications. IEEE Access, 6, 6478-6486.

[34]   Prabhu, Boselin, N. Balakumar, and A. Johnson Antony. (2017). Evolving constraints in military applications using wireless sensor networks. International Journal of Innovative Research in Computer Science & Technology (IJIRCST), 5(1).

[35]   Rodríguez, Schubert, Tatiana Gualotuña, and Carlos Grilo. (2017). A System for the Monitoring and Predicting of Data in Precision Agriculture in a Rose Greenhouse Based on Wireless Sensor Networks. Procedia Computer Science 121, pp. 306-313.

[36]   Wang, Shiyong, Jiafu Wan, Di Li, and Chunhua Zhang. (2016). Implementing smart factory of industrie 4.0: an outlook. International Journal of Distributed Sensor Networks 12, no. 1.

[37]   Alamri, A., Ansari, W. S., Hassan, M. M., Hossain, M. S., Alelaiwi, A., and Hossain, M. A. (2013). A survey on sensor-cloud: architecture, applications, and approaches. International Journal of Distributed Sensor Networks, 9(2), 917923.

[38]   Baha Rababah, Tanweer Alam, Rasit Eskicioglu. (2020). The Next Generation Internet of Things Architecture Towards Distributed Intelligence: Reviews, Applications, and Research Challenges. Journal of Telecommunication, Electronic and Computer Engineering (JTEC). Vol 12(2).

[39] Tanweer Alam and Mohammed Aljohani. (2016). Design a New Middleware for Communication in Ad Hoc Network of Android Smart Devices. In Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies (ICTCS '16). ACM, New York, NY, USA, Article 38, 6 pages. DOI: 10.1145/2905055.2905244.

[40] Liu, Wei, Qiang Liu, and Wensu Li. (2016). Research of IoT Application in Manned Spaceflight Launch Site. In Wireless Communications, Networking and Applications, pp. 517-527. Springer.

[41] Khodkari, Hourieh, S. Maghrebi, and Rey Branch. (2016). Necessity of the integration Internet of Things and cloud services with quality of service assurance approach. Bulletin de la Société Royale des Sciences de Liège 85, no. 1, pp. 434-445.

[42] Gilligan, R., Susan Thomson, Jim Bound, and W. Stevens. (1999). Basic socket interface extensions for IPv6. No. RFC 2553.

[43] Montenegro, Gabriel, Nandakishore Kushalnagar, Jonathan Hui, and David Culler. (2007). Transmission of IPv6 packets over IEEE 802.15. 4 networks. No. RFC 4944.

[44] Thubert, Pascal, and Jonathan W. Hui. (2011). Compression format for IPv6 datagrams over IEEE 802.15. 4-based networks.

[45] Aljohani, Mohammed, and Tanweer Alam. (2015). Real Time Face Detection in Ad Hoc Network of Android Smart Devices. Advances in Computational Intelligence: Proceedings of International Conference on Computational Intelligence. Springer Singapore. DOI: https://doi.org/10.1007/978- 981-10-2525-9_24

[46] Eisenhauer, Markus, Peter Rosengren, and Pablo Antolin. (2009). A development platform for integrating wireless devices and sensors into ambient intelligence systems. In Sensor, Mesh and Ad Hoc Communications and Networks Workshops. SECON Workshops' 09. 6th Annual IEEE Communications Society Conference on, pp. 1-3.

[47] Spiess, Patrik, Stamatis Karnouskos, Dominique Guinard, Domnic Savio, Oliver Baecker, Luciana Moreira Sá De Souza, and Vlad Trifa. (2009). SOA-based integration of the internet of things in enterprise services. In Web Services, 2009. ICWS 2009. IEEE International Conference on, pp. 968-975.

[48] Reiners, René, Andreas Zimmermann, Marc Jentsch, and Yan Zhang. (2009). Automizing home environments and supervising patients at home with the hydra middleware: application scenarios using the hydra middleware for embedded systems. In Proceedings of the first international workshop on Context-aware software technology and applications, pp. 9-12.

[49] Yang, Yiling, Yu Huang, Xiaoxing Ma, and Jian Lu. (2016). Enabling context-awareness by predicate detection in asynchronous environments. IEEE Transactions on Computers 65, no. 2, pp. 522-534.

[50] Park, Namje, Hongxin Hu, and Qun Jin. (2016). Security and privacy mechanisms for sensor middleware and application in internet of things (IoT).

[51] Bandyopadhyay, Soma, Munmun Sengupta, Souvik Maiti, and Subhajit Dutta. (2011). A survey of middleware for internet of things. In Recent trends in wireless and mobile networks, pp. 288-296. Springer, Berlin, Heidelberg.

[52] Van Rijmenam, Mark. (2017). Self-driving cars will create 2 petabytes of data, what are the big data opportunities for the car industry.

[53] Finnegan, Matthew. (2013). Boeing 787s to create half a terabyte of data per flight says Virgin Atlantic. Computerworld UK 6.

[54] Zhang, Qi, Lu Cheng, and Raouf Boutaba. (2010). Cloud computing: state-of-the-art and research challenges. Journal of internet services and applications 1, no. 1, pp. 7-18.

[55] Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I. and Zaharia, M., 2010. A view of cloud computing. Communications of the ACM, 53(4), pp.50-58.

[56] Fernando, Niroshinie, Seng W. Loke, and Wenny Rahayu. (2013). Mobile cloud computing: A survey. Future generation computer systems 29, no. 1,pp. 84-106.

[57] Ryan, Mark D. (2013). Cloud computing security: The scientific challenge, and a survey of solutions. Journal of Systems and Software 86, no. 9, pp. 2263-2268.

[58] Botta, Alessio, Walter De Donato, Valerio Persico, and Antonio Pescapé. (2016). Integration of cloud computing and internet of things: a survey. Future Generation Computer Systems 56, pp. 684-700.

[59] Whaiduzzaman, Md, Mehdi Sookhak, Abdullah Gani, and Rajkumar Buyya. (2014). A survey on vehicular cloud computing. Journal of Network and Computer Applications 40, pp. 325-344.

[60] Rahimi, M. Reza, Jian Ren, Chi Harold Liu, Athanasios V. Vasilakos, and Nalini Venkatasubramanian. (2014). Mobile cloud computing: A survey, state of art and future directions. Mobile Networks and Applications, Vol 19, no. 2, pp. 133-143.

[61] Shi, W., Cao, J., Zhang, Q., Li, Y., and Xu, L. (2016). Edge computing: Vision and challenges. IEEE internet of things journal, 3(5), 637-646.

[62] Tanweer Alam. (2020). Internet of Things: A Secure Cloud-Based MANET Mobility Model. International Journal of Network Security. Vol 22(3). DOI: 10.6633/IJNS.202005_22(3).17

[63] Bonomi, F., Milito, R., Zhu, J., and Addepalli, S. (2012). Fog computing and its role in the internet of things. In Proceedings of the first edition of the MCC workshop on Mobile cloud computing (pp. 13-16).

[64] Mao, Yuyi, Changsheng You, Jun Zhang, Kaibin Huang, and Khaled B. Letaief. (2017). A survey on mobile edge computing: The communication perspective. IEEE Communications Surveys & Tutorials 19, no. 4, pp. 2322-2358.

[65] Parker, Lynne E. (2008). Distributed intelligence: Overview of the field and its application in multi-robot systems. Journal of Physical Agents 2.1, pp. 5-14.

[66] Zhang, S., Lee, C. K., Yu, K. M., and Lau, H. C. (2017). Design and development of a unified framework towards swarm intelligence. Artificial intelligence review, 47(2), 253-277.

[67] Mavrovouniotis, Michalis, Changhe Li, and Shengxiang Yang. (2017). A survey of swarm intelligence for dynamic optimization: Algorithms and applications. Swarm and Evolutionary Computation 33, pp. 1-17.

[68] Saggu, Amrit, Pallavi Yadav, and Monika Roopak. Applications of Swarm Intelligence. (2013). International Journal of Computer Science and Mobile Computing, Vol. 2, Issue. 5, pp. 353 – 359.

[69] Zahedi, Zeynab Molay, Reza Akbari, Mohammad Shokouhifar, Farshad Safaei, and Ali Jalali. (2016). Swarm intelligence based fuzzy routing protocol for clustered wireless sensor networks. Expert Systems with Applications 55, pp. 313-328.

[70] de Sá, Alan Oliveira, Nadia Nedjah, and Luiza de Macedo Mourelle. (2016). Distributed efficient localization in swarm robotic systems using swarm intelligence algorithms. Neurocomputing 172, pp. 322-336.

[71] Lin, Ying-yin, and Ying-ping Chen. (2007). Crowd control with swarm intelligence. In Evolutionary Computation. CEC 2007. IEEE Congress on, pp. 3321-3328.

[72] Mahmoud, Thair, and Bestoun S. Ahmed. (2015). An efficient strategy for covering array construction with fuzzy logic-based adaptive swarm optimization for software testing use. Expert Systems with Applications 42, no. 22, pp. 8753-8765.

[73] Mandal, Devraj, Amitava Chatterjee, and Madhubanti Maitra. (2017). Particle Swarm Optimization Based Fast Chan-Vese Algorithm for Medical Image Segmentation. In Metaheuristics for Medicine and Biology, pp. 49-74. Springer, Berlin, Heidelberg.

[74] Djenouri, Youcef, Asma Belhadi, and Riadh Belkebir. (2018). Bees swarm optimization guided by data mining techniques for document information retrieval. Expert Systems with Applications 94, pp. 126-136.

[75] Castelfranchi, Cristiano. (1998). Modelling social action for AI agents. Artificial Intelligence 103, no. 1-2, pp. 157-182.

[76] R. Maier, (2007). Knowledge Management Systems, 3rd ed. New York: Springer.

[77] Uriarte, Filemon A.(2008). Introduction to knowledge management: A brief introduction to the basic elements of knowledge management for non-practitioners interested in understanding the subject. ASEAN Foundation.

[78] Das, Aditi, and Ravi Prakash Gorthi. (2015). Knowledge Based Routing Protocols in Wireless Sensor Networks. In Computational Intelligence, Communication Systems and Networks (CICSyN), 2015 7th International Conference on, pp. 35-38.

[79] Google Trends, (2020). https://trends.google.com/trends/explore?cat=174&date=2015-06-10%202020-07-10&q=Distributed%20Intelligence,IoT%20Network,Edge%20computing

[80] Motorola, (2011). Distributed intelligence: The Future of Wireless Networking Architecture.

[81] Van den Abeele, F., Hoebeke, J., Teklemariam, G. K., Moerman, I., & Demeester, P. (2015). Sensor function virtualization to support distributed intelligence in the internet of things. Wireless Personal Communications, 81(4), 1415-1436.

[82] R. R. Hasibur Rahman, (2017). Enabling distributed intelligence assisted Future Internet of Things Controller (FITC), Applied Computing and Informatics.

[83] Tanweer Alam. Abdulrahman A. Salem. Ahmad O. Alsharif and Abdulaziz M. Alhujaili, (2020). Smart Home Automation Towards the Development of Smart Cities. Computer Science and Information Technologies. Vol 1(1). DOI: 10.11591/csit.v1i1.p17-25.

[84] Tanweer Alam and Mohamed Benaida. (2018). The Role of Cloud-MANET Framework in the Internet of Things (IoT). International Journal of Online Engineering. Vol 14(12). DOI: 10.3991/ijoe.v14i12.8338

[85] Tanweer Alam. (2019). IoT-Fog: A Communication Framework using Blockchain in the Internet of Things. International Journal of Recent Technology and Engineering (IJRTE). Vol. 7(6).

[86] Tanweer Alam, Shamimul Qamar, Amit Dixit, and Mohamed Benaida. (2020). Genetic Algorithm: Reviews, Implementations, and Applications. International Journal of Engineering Pedagogy (iJEP). Vol 10(6).

[87] Richardson, M., and Wallace, S. (2012). Getting started with raspberry PI. O'Reilly Media, Inc.

[88] Tanweer Alam.(2020). Efficient and Secure Data Transmission Approach in Cloud-MANET-IoT Integrated Framework., Journal of Telecommunication, Electronic and Computer Engineering. Vol 12(1).

[89]   Tanweer Alam and Mohamed Benaida. (2018). CICS: Cloud–Internet Communication Security Framework for the Internet of Smart Devices. International Journal of Interactive Mobile Technologies (iJIM). Vol 12(6). DOI: 10.3991/ijim.v12i6.6776

[90]   Alam, T. (2020). CMI Computing: A Cloud, MANET, and Internet of Things Integration for Future Internet. Jambura Journal of Informatics, 2(1), 1-22.

[91]   Beck, Michael Till, and Marco Maier. (2014). Mobile edge computing: Challenges for future virtual network embedding algorithms. In Proc. The Eighth International Conference on Advanced Engineering Computing and Applications in Sciences (ADVCOMP 2014), vol. 1, no. 2, p. 3.

[92]   Kulkarni, B. P., Joshi, A. V., Jadhav, V. V., and Dhamange, A. T. (2017). IoT based home automation using Raspberry PI. International Journal of Innovative Studies in Sciences and Engineering Technology (IJISSET), 3(4).

[93]   Nellore, Kapileswar, and Gerhard P. Hancke. (2016). A survey on urban traffic management system using wireless sensor networks. Sensors 16.2.

[94]   Pan, Juan Susan, Iulian Sandu Popa, and Cristian Borcea.(2017). Divert: A distributed vehicular traffic re-routing system for congestion avoidance. IEEE Transactions on Mobile Computing 16, no. 1, pp. 58-72.

[95]   M. Rouse, (2017). Intelligent Transportation System (ITS). 03 Available: http://whatis.techtarget.com/definition/intelligent-transportation-system.

[96]   Bill McBeath, (2014). Distributed Intelligence in the IoT. chainlink, URL: http://www.clresearch.com/research/detail.cfm?guid=4E088DB8-3048-79ED-9964-69B73742171B

[97]   Earley, Seth. (2015). Analytics, machine learning, and the internet of things. IT Professional 17.1, pp. 10-13.

[98]   Sanaei, Zohreh, Saeid Abolfazli, Abdullah Gani, and Rajkumar Buyya. (2014). Heterogeneity in mobile cloud computing: taxonomy and open challenges. IEEE Communications Surveys & Tutorials 16, no. 1 pp. 369-392.

[99]   Borgia, Eleonora. (2014). The Internet of Things vision: Key features, applications and open issues. Computer Communications 54, pp. 1-31.

[100] Roman, Rodrigo, Jianying Zhou, and Javier Lopez. (2013). On the features and challenges of security and privacy in distributed internet of things. Computer Networks 57, no. 10, pp. 2266-2279.

[101] Xu, Ke, Yi Qu, and Kun Yang. (2016). A tutorial on the internet of things: From a heterogeneous network integration perspective. IEEE Network 30, no. 2, pp. 102-108.

[102] Mansour Bader, Andraws Swidan, Mazin Al-Hadidi, and Baha Rababah. (2016). A Binary to Residue Conversion Using New Proposed Non-Coprime Moduli Set. Signal & Image Processing: An International Journal (SIPIJ) Vol 7(3).

[103] T. Alam and M. Aljohani. (2015). An approach to secure communication in mobile ad-hoc networks of Android devices, International Conference on Intelligent Informatics and Biomedical Sciences (ICIIBMS), Okinawa, Japan, 2015, pp. 371-375. doi:10.1109/ICIIBMS.2015.7439466.

[104] Parker, Lynne E. (2008). Distributed intelligence: Overview of the field and its application in multi-robot systems. Journal of Physical Agents 2.1, pp. 5-14.

[105] Stronks, H. C., Mitchell, E. B., Nau, A. C., and Barnes, N. (2016). Visual task performance in the blind with the BrainPort V100 Vision Aid. Expert review of medical devices, 13(10), 919-931.

[106] Al Nuaimi, Klaithem, Nader Mohamed, Mariam Al Nuaimi, and Jameela Al-Jaroodi. (2012). A survey of load balancing in cloud computing: Challenges and algorithms. In Network Cloud Computing and Applications (NCCA), 2012 Second Symposium on, pp. 137-142.