Science and Technology Publishing (SCI & TECH)
ISSN: 2632-1017
Vol. 5 Issue 1, January - 2021

# Internet Of Things: Standardizations, Iot Elements, Protocols, Architectural Design Choices, Challenges And Future Efforts

**Dr. Osama Ahmad Salim Safarini**
Computer Science and Engineering Researcher
usama.safarini@gmail.com
Tulkarem, Palestine

***Abstract*—Internet of Things (IoT) is creating an environment of convergence in the society. This technology environment brings a paradigm shift in our professional and personal life. As a connected environment, IoT adds customer value and loyalty. Today, IoT is being implemented everywhere which is of human concern like smart city, smart environment, security, smart business process, smart agriculture, home automation and healthcare. This article discusses the evolution, advantages, Architectural design choices, Standardizations, providing an overview of some of the key IoT challenges presented in the recent literature and provide a summary of related research work. I highlighted future research directions of IoT. I Moreover, I explore the relation between the IoT and other emerging technologies including big data analytics and cloud and fog computing. I present the need for better horizontal integration among IoT services.**

***Keywords—IoT, Architectural Design Choices, IPv6, Standardization Issues, Intelligent IoT gateway, CoAP, MQTT, AMQP.***

## I. INTRODUCTION

The Internet of Things (IoT) sometimes referred to as the Internet of Objects, will change everything including ourselves. The Internet has an impact on education, communication, business, science, government, and humanity [1]. Clearly, the Internet is one of the most important and powerful creations in all of human history and now with the concept of the internet of things, internet becomes more favorable to have a smart life in every aspects [2]. Internet of Things is a new technology of the Internet accessing. By the Internet of Things, objects recognize themselves and obtain intelligence behavior by making or enabling related decisions thinks to the fact that they can communicate information about themselves [3]. These objects can access information that has been aggregated by other things, or they can added to other services [3]. Figure 1 reviews that with the internet of things, anything's will able to communicate to the internet at any time from any place to provide any services by any network to anyone. this concept will create a new types of applications can involve such as smart vehicle and the smart home, to provide many services such as notifications, security, energy saving, automation, communication, computers and entertainment [4, 5].

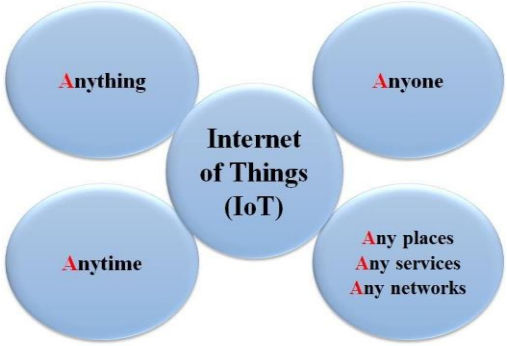


Figure 1. Internet of things Concept

By developing the IoT technology, testing and deploying products it will be much close to implementing smart environments by 2025 [6]. In the near future, storage and communication services will be highly pervasive and distributed: people, machines, smart objects, surrounding space and platforms connected with wireless/wired sensors, machine to machine (M2M) devices, RFID tags will create a highly decentralized resources interconnected by a dynamic network of networks [7]. In the IoT, the communication language will be based on interoperable protocols, operating in heterogeneous environments and platforms [8]. IoT in this context is a generic term and all objects can play an active role to their connection to the Internet by creating smart environments, where the role of the Internet has changed [9].

IoT is a concept where an object is assigned to an IP address and through that IP address we make that device identifiable on internet. A Team of International Telecommunications Union defined IoT as a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies. The network can be a combination of people-things, things-things and people-people. It happens only because of the conjugation of various technologies such as wireless communication, Micro Electromechanical System that includes wireless sensor, networks and control system. The most important elite presence of cloud space on Internet is

shaping the architecture of IoT in a feasible and rational form. Certainly, what IoT can do is beyond imagination. It connects plethora of heterogeneous object.

The outline of the contributions of this paper relative to the following:

- I provide an overview of some of the key IoT challenges presented in the recent literature and provide a summary of related research work. Moreover, we explore the relation between the IoT and other emerging technologies including big data analytics and cloud and fog computing.

- I present the need for better horizontal integration among IoT services.

## II. INTERNET OF THINGS STANDARDIZATIONS, PROTOCOLS AND ARCHITECTURAL DESIGN CHOICES

By the 2025 around 50 to 100 billion things will be connected electronically by internet [10]. Figure 2 shows the growth of the things connected to the internet from 1988 to forecast 2020. The Internet of Things (IoT) will provide a technology to creating the means of smart action for machines to communicate with one another and with many different types of information [11]. The success of IoT depends on standardization Table I, which provides interoperability, compatibility, reliability, and effective operations on a global scale [12].

Table I Standardization Efforts In Support Of the IoT

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Application Protocol** | | DDS | CoAP | AMQP | MQTT | MQTT-SN | XMPP | HTTP REST |
| **Service Discovery** | | mDNS | | | | DNS-SD | | |
| **Infrastructure Protocols** | Routing Protocol | RPL | | | | | | |
| | Network Layer | 6LoWPAN | | | | IPv4/IPv6 | | |
| | Link Layer | IEEE 802.15.4 | | | | | | |
| | Physical/ Device Layer | LTE-A | EPCglobal | IEEE 802.15.4 | | Z-Wave | | |
| **Influential Protocols** | | IEEE 1888.3, IPSec | | | | IEEE 1905.1 | | |

Today more than 60 companies for leading technology, in communications and energy, working with standards, such as IETF, IEEE and ITU to specify new IP based technologies for the Internet of Things [13].

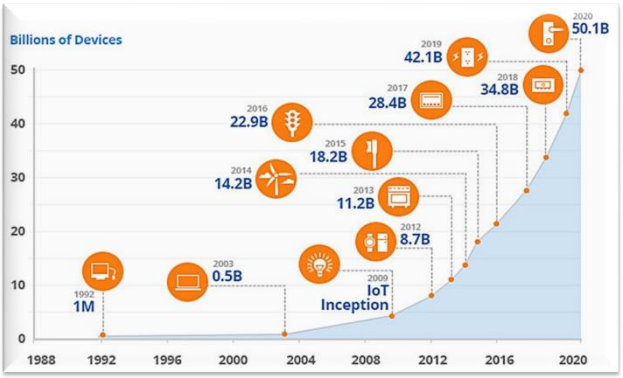


Figure 2. Internet of Things Growth

The design of the IoT standards is required to consider the efficient use of energy and network capacity, as well as respecting other constraints such as frequency bands and power levels for radio frequency communications [14, 15]. As IoT evolves, it may be necessary to Review such constraints and investigate ways to ensure sufficient capacity for expansion, for example in case of additional radio spectrum allocation as it becomes available [16].

IEEE Standards Association (IEEE-SA) develops a number of standards that are related to environment need for an IoT. The main focus of the IEEE standardization activities are on the Physical and MAC layers [17]. The IEEE provides an early foundation for the IoT with the IEEE802.15.4 standard for short range low power radios, typically operating in the industrial, scientific and medical band in addition to use ZigBee technology [18]. The IEEE-SA has an over 900 active standards and more than 500 standards under development. In its research into IoT, it has identified over 140 existing standards and projects that are relevant to the IoT. The base project related to IoT is IEEE P2413, which it is currently considering the architecture of IoT [19] [20].

ETSI produces globally applicable standards for information and communications technologies (ICT), including fixed, mobile, radio, converged, broadcast and Internet technologies, discusses a similar concept under the label of M2M communication. These standards are considered as one of the basic standards of IoT, because its associate with M2M technology, which is one of the basic techniques, related to IoT [21, 22].

Internet Engineering Task Force (IETF) is concerned with the evolution of the Internet architecture and the smooth operation of the Internet and known as large, open to international community of network designers, operators, vendors and researchers [23]. IETF provides its own description of IoT, which provides a most recognizable enhancement to support IPv6, with the 6LoWPAN [24-26]. The 6TiSCH Working Group is being formed at the IETF to address the networking piece of that unifying standard. Based on open standards, 6TiSCH will provide a complete suite protocols for distributed and centralized routing operation over the

IEEE802.15.4e TSCH MAC [27]. ITU's Telecommunication Standardization Sector (ITU-T) considered as a first organization of standards development and coordination of the Internet of Things. They buts standards to gain benefit of integrated information processing capacity, and industrial products with smart capabilities [28, 29]. In addition to make development on electronic identities that can be queried remotely, or be equipped with sensors for detecting physical changes around them.

### A. Develop and Implement Applications for IoTs

Internet and web application in IoTs are generally facilitated by open sourcing hardware and software. It is quite interesting and challenging to develop and implement applications for IoTs. One can easily develop applications using Python, html5, C and Node.js. As communication in IoT is both ways, a browser can establish communication with JavaScript API to real time web through TCP/IP. IoT enabled applications can control light, sensors and other electrical and electronics appliances. Customers provide their feedback and input before Mobile application development. Usually a prototype is prepared and tested in real time for IoT enabled mobile applications. In the current context, competition is happening between Android and iOS mobiles. Evothing Studio is a popular tool for developing IoT enabled mobile application development. This studio consists of a client, a workbench, example applications and native plugins. This platform is freely available in Internet and open source based.

## III. IoT ELEMENTS

Understanding the IoT building blocks helps to gain a better insight into the real meaning and functionality of the IoT. In the following sections, we discuss six main elements needed to deliver the functionality of the IoT as illustrated in Fig. 3. Table II shows the categories of these elements and examples of each category.


Fig. 3. The IoT elements.

### A.Identification

Identification is crucial for the IoT to name and match services with their demand. Many identification methods are available for the IoT such as electronic product codes (EPC) and ubiquitous codes (uCode) [30]. Furthermore, addressing the IoT objects is critical to differentiate between object ID and its address. Object ID refers to its name such as “T1” for a particular- Lar temperature sensor and object’s address refers to its address within a communications network. In addition, addressing methods of IoT objects include IPv6 and IPv4. 6LoWPAN [31], [32] provides a compression mechanism over IPv6 headers that makes IPv6 addressing appropriate for low power wireless networks. Distinguishing between object’s identification and address is imperative since identification methods are not glob- ally unique, so addressing assists to uniquely identify objects. In addition, objects within the network might use public IPs and not private ones. Identification methods are used to provide a clear identity for each object within the network.

### B.Sensing

The IoT sensing means gathering data from related objects within the network and sending it back to a data warehouse, database, or cloud. The collected data is analyzed to take

TABLE II Building Blocks and Technologies of the IoT

| IoT Elements | | Samples |
|---|---|---|
| Identification | Naming | EPC, uCode |
| | Addressing | IPv4, IPv6 |
| Sensing | | Smart Sensors, Wearable sensing devices, Embedded sensors, Actuators, RFID tag |
| Communication | | RFID, NFC, UWB, Bluetooth, BLE, IEEE 802.15.4, Z-Wave, WiFi, WiFiDirect, , LTE-A |
| Computation | Hardware | SmartThings, Arduino, Phidgets, Intel Galileo, Raspberry Pi, Gadgeteer, BeagleBone, Cubieboard, Smart Phones |
| | Software | OS (Contiki, TinyOS, LiteOS, Riot OS, Android); Cloud (Nimbits, Hadoop, etc.) |
| Service | | Identity-related (shipping), Information Aggregation (smart grid), Collaborative-Aware (smart home), Ubiquitous (smart city) |
| Semantic | | RDF, OWL, EXI |

specific actions based on required services. The IoT sensors can be smart sensors, actuators or wearable sensing devices. For example, com panies like Wemo, revolv and SmartThings offer smart hubs and mobile applications that enable people to monitor and control thousands of smart devices and appliances inside buildings using their smartphones [33]–[35].

Single Board Computers (SBCs) integrated with sensors and built-in TCP/IP and security functionalities are typically used to realize IoT products (e.g., Arduino Yun, Raspberry PI, Bea-gleBone Black, etc.). Such devices typically connect to a central management portal to provide the required data by customers.

### C.Communication

The IoT communication technologies connect heterogeneous objects together to deliver specific smart services. Typically, the IoT nodes should operate using low power in the presence of lossy and noisy communication links. Examples of communication protocols used for the IoT are Wi-Fi, Bluetooth, IEEE 802.15.4, Z-wave, and LTE-Advanced. Some specific communication technologies are also in use like RFID, Near Field Communication (NFC) and ultra-wide bandwidth (UWB). RFID is the first technology used to realize the M2M concept (RFID tag and reader). The RFID tag represents a simple chip or label attached to provide object's identity. The RFID reader transmits a query signal to the tag and receives reflected signal from the tag, which in turn is passed to the database. The database connects to a processing center to identify objects based on the reflected signals within a (10 cm to 200 m) range [36]. RFID tags can be active, passive or semi-passive/active. Active tags are powered by battery while passive ones do not need battery. Semi-passive/active tags use board power when needed.

The NFC protocol works at high frequency band at 13.56 MHz and supports data rate up to 424 kbps. The applicable range is up to 10 cm where communication between active readers and passive tags or two active readers can occur [37]. The UWB communication technology is designed to support communications within a low range coverage area using low energy and high bandwidth whose applications to connect sensors have been increased recently [38].

Another communication technology is Wi-Fi that uses radio waves to exchange data amongst things within 100 m range [39]. Wi-Fi allows smart devices to communicate and exchange information without using a router in some ad hoc configurations. Bluetooth presents a communication technology that is used to exchange data between devices over short distances using short-wavelength radio to minimize power consumption [40]. Recently, the Bluetooth special interest group (SIG) produced Bluetooth 4.1 that provides Bluetooth Low Energy as well as high-speed and IP connectivity to support IoT [41]. The IEEE 802.15.4 standard specifies both a physical layer and a medium access control for low power wireless networks targeting reliable and scalable communications [42].

LTE (Long-Term Evolution) is originally a standard wireless communication for high-speed data transfer between mobile phones based on GSM/UMTS network technologies [43]. It can cover fast-travelling devices and provide multicasting and broadcasting services. LTE-A (LTE Advanced) [44] is an im- proved version of LTE including bandwidth extension, which supports up to 100 MHz, downlink and uplink spatial multiplexing, extended coverage, higher throughput and lower latencies.

### D.Computation

Processing units (e.g., microcontrollers, microprocessors, SOCs, FPGAs) and software applications represent the "brain" and the computational ability of the IoT. Various hardware plat- forms were developed to run IoT applications such as Arduino, UDOO, Friendly ARM, Intel Galileo, Raspberry PI, Gadgeteer, BeagleBone, Cubieboard, Z1, WiSense, Mulle, and T-Mote Sky. Furthermore, many software platforms are utilized to provide IoT functionalities. Among these platforms, Operating Systems are vital since they run for the whole activation time of a device. There are several Real-Time Operating Systems (RTOS) that are good candidates for the development of RTOS-based IoT applications. For instance, the Contiki RTOS has been used widely in IoT scenarios. Contiki has a simulator called Cooja which allows researcher and developers to simulate and emulate IoT and wireless sensor network (WSN) applications [45]. TinyOS [46], LiteOS [47] and RIoT OS [48] also offer lightweight OS designed for IoT environments. Moreover, some auto industry leaders with Google established the Open Auto Alliance (OAA) and are planning to bring new features to the Android platform to accelerate the adoption of the Internet of Vehicles (IoV) paradigm [49]. Some features of these operating systems are compared in Table III.

Cloud Platforms form another important computational part of the IoT. These platforms provide facilities for smart objects to send their data to the cloud, for big data to be processed in real-time, and eventually for end-users to benefit from the knowledge extracted from the collected big data. There are a lot of free and commercial cloud platforms and frameworks available to host IoT services.

TABLE III Common Operating Systems Used In Iot Environments

| Operating System | Language Support | Minimum Memory (KB) | Event-based Programming | Multi-threading | Dynamic Memory |
|---|---|---|---|---|---|
| TinyOS | nesC | 1 | Yes | Partial | Yes |
| Contiki | C | 2 | Yes | Yes | Yes |
| LiteOS | C | 4 | Yes | Yes | Yes |
| Riot OS | C/C++ | 1.5 | No | Yes | Yes |
| Android | Java | - | Yes | Yes | Yes |

### E.Services

Overall, IoT services can be categorized under four classes [50], [51]: Identity-related Services, Information Aggregation Services, Collaborative-Aware Services and Ubiquitous Services. Identity-related services are the most basic and important services that are used in other types of services. Every application that needs to bring real world objects to the virtual world has to identify those objects. Information Aggregation Services collect and summarize raw sensory measurements that need to be processed and reported to the IoT application.

Collaborative-Aware Services act on top of Information Aggregation Services and use the obtained data to make decision and react accordingly. Ubiquitous Services, however, aim to provide Collaborative-Aware Services anytime they are needed to any- one who needs them anywhere. With this categorization, we re- view some applications of the IoT in the following paragraphs. The ultimate goal of all IoT applications is to reach the level of ubiquitous services. However, this end is not achievable easily since there are a lot of difficulties and challenges that have to be addressed. Most of the existing applications provide identity- related, information aggregation, and collaborative-aware services. Smart healthcare and smart grids fall into the information aggregation category and smart home, smart buildings, intelligent transportation systems (ITS), and industrial automation are closer to the collaborative-aware category.

Smart home [52] IoT services contribute to enhancing the personal life-style by making it easier and more convenient to monitor and operate home appliances and systems (e.g., air conditioner, heating systems, energy consumption meters, etc.) re- motely. For example, a smart home can automatically close the windows and lower the blinds of upstairs windows based on the weather forecast. Smart homes are required to have regular interaction with their internal and external environments [53].

The internal environment may include all the home appliances and devices that are Internet-connected while the external environment consists of entities that are not in control of the smart home such as smart grid entities.

Smart buildings connect building automation systems (BAS) to the Internet [54]. BAS allows controlling and managing different building devices using sensors and actuators such as HVAC, lighting and shading, security, safety, entertainment, etc. Furthermore, BAS can help to enhance energy consumption and maintenance of buildings. For example, a blinking dishwasher or cooling/heating system can provide indications when there is a problem that needs to be checked and solved. Thus, maintenance requests can be sent out to a contracted company without any human intervention. Intelligent transportation systems (ITS) or Transportation Cyber-Physical Systems (T-CPS) represent integration between computation and communication to monitor and control the transportation network [55], [56]. ITS aims to achieve better re- liability, efficiency, availability and safety of the transportation infrastructure. ITS employs four main components, namely: vehicle subsystem (consists of GPS, RFID reader, OBU, and communication), station subsystem (roadside equipment), ITS monitoring center and security subsystem. Moreover, connected vehicles are becoming more important with the aim to make driving more reliable, enjoyable and efficient [57], [58]. For in-stance, Audi became the first automaker with a license for self- driving in Nevada [59]. Google is another pioneer in this area [60]. In addition, in December 2013, Volvo announced its self-driving car to drive about 30 miles in busy roads in Gothenburg, Sweden [61]. Earlier this year, the USDOT announced that it would chart a regulatory path that would require all new automobiles to be equipped with vehicle-to-vehicle (V2V) communications systems sometime in the next several years.

Industrial automation [62], [63], is computerizing robotic de- vices to complete manufacturing tasks with a minimal human involvement. It allows a group of machines to produce products quickly and more accurately based on four elements: transportation, processing, sensing and communication. The IoT is utilized in industrial automation to control and monitor production ma- chines' operations, functionalities, and productivity rate through the Internet. For instance, if a particular production machine encounters a sudden issue, an IoT system sends a maintenance request immediately to the maintenance department to handle the fix. Furthermore, the IoT increases productivity by analyzing production data, timing and causes of production issues.

Smart healthcare plays a significant role in healthcare applications through embedding sensors and actuators in patients and their medicine for monitoring and tracking purposes. The IoT is used by clinical care to monitor physiological statuses of patients through sensors by collecting and analyzing their information and then sending analyzed patient's data remotely to processing centers to make suitable actions. For example, Masimo Radical-7 monitors the patient's status remotely and reports that to a clinical staff [64]. Recently, IBM utilized RFID technology at one of OhioHealth's hospitals to track hand washing after checking each patient [65]–[67]. That operation could be used to avoid infections that cause about 90 000 deaths and losing about $30 billion annually.

Smart grids [53], [68] utilize the IoT to improve and enhance the energy consumption of houses and buildings. Employing the IoT in smart grids helps power suppliers to control and man- age resources to provide power proportionally to the population increase. For example, smart grids use the IoT to connect millions or billions of buildings' meters to the network of energy providers. These meters are used to collect, analyze, control, monitor, and manage energy consumption. The IoT enables energy providers to improve their services to meet consumers' needs. In addition, utilizing the IoT in the smart grid reduces the potential failures, increases efficiency and improves quality of services.

A smart city which could be seen as an application of ubiquitous services, aims to improve the quality of life in the city by making it easier and more convenient for the residents to find information of interest [69], [70]. In a smart city environment, various systems based on smart technologies are interconnected to provide required services (health, utilities, transportation, government, homes and buildings).

### F.Semantics

Semantic in the IoT refers to the ability to extract knowledge smartly by different machines to provide the required services. Knowledge extraction includes discovering and using resources and modeling information. Also, it includes recognizing and analyzing data to make sense of the right decision to provide the exact service [71]. Thus, semantic represents the brain of the IoT by sending demands to the right resource. This requirement is supported by Semantic Web technologies such as the Resource Description Framework (RDF) and the Web Ontology Language (OWL). In 2011, the World Wide Web consortium (W3C) adopted the Efficient XML Interchange (EXI) format as a recommendation [72].

EXI is important in the context of the IoT because it is de- signed to optimize XML applications for resource-constrained environments. Furthermore, it reduces bandwidth needs with- out affecting related resources such as battery life, code size, energy consumed for processing, and memory size. EXI converts XML messages to binary to reduce the needed bandwidth and minimize the required storage size.

Remarks: In this section, the main components of the IoT were identified along with their related standards, technologies and realizations. The variety of standards and technologies in these elements and the way they should interoperate is a main challenge that can impede the development of IoT applications. The heterogeneity of the IoT elements needs a thorough solution to make ubiquitous IoT services a reality. Section VIII addresses this problem by proposing an architectural model that alleviates the interoperability issues caused by the diversity of protocols and technologies utilized in the context of the IoT.

## IV. INTERNET OF THINGS CHALLENGES

The fact that Internet of things applications and scenarios outlined above are very interesting which provides technologies for smart every things. , but there are some challenges to the application of the Internet of Things concept in cost of implementation. The expectation that the technology must be available at low cost with a large number of objects. IoT are also faced with many other challenges [73, 74], such as:

- **Scalability:** Internet of Things has a big concept than the conventional Internet of computers, because of things are cooperated within an open environment. Basic functionality such as communication and service discovery therefore need to function equally efficiently in both small scale and large-scale environments. The IoT requires a new functions and methods in order to gain an efficient operation for scalability.

- **Self-Organizing:** Smart things should not be managed as computers that require their users to configure and adapt them to particular situations. Mobile things, which are often only sporadically used, need to establish connections spontaneously, and able to be organize and configure themselves to suit their particular environment.

- **Data volumes:** Some application scenarios of the internet of things will involve to infrequent communication, and gathering information's form sensor networks, or form logistics and large-scale networks, will collect a huge volumes of data on central network nodes or servers. The term represent this phenomena is big data, which is, requires many operational mechanism in addition to new technologies for storing, processing and management.

- **Data interpretation:** To support the users of smart things, there is a need to interpret the local context determined by sensors as accurately as possible. For service providers to profit from the disparate data that will be generated, needs to be able to draw some generalizable conclusions from the interpreted sensor data.

- **Interoperability:** Each type of smart objects in Internet of Things have different information, processing and communication capabilities. Different smart objects would also be subjected to different conditions such as the energy availability and the communications bandwidth requirements. To facilitate communication and cooperation of these objects, common standards are required.

- **Automatic Discovery:** In dynamic environments, suitable services for things must be automatically identified, which requires appropriate semantic means of describing their functionality.

- **Software complexity:** A more extensive software infrastructure will be needed on the network and on background servers in order to manage the smart objects and provide services to support them. That because the software systems in smart objects will have to function with minimal resources, as in conventional embedded systems.

- **Security and privacy:** In addition to the security and protection aspects of the Internet such in communications confidentiality, the authenticity and trustworthiness of communication partners, and message integrity, other requirements would also be important in an Internet of Things. There is a need to access certain services or prevent from communicating with other things in IoT and business transactions involving smart objects would need to be protected from competitors' prying eyes.

- **Fault tolerance:** Objects in internet of things is much more dynamic and mobile than the internet computers, and they are in changing rapidly in unexpected ways. Structuring an Internet of Things in a robust and trustworthy manner would require redundancy on several levels and an ability to automatically adapt to changed conditions.

- **Power supply:** Things typically move around and are not connected to a power supply, so their smartness needs to be powered from a self-sufficient energy source. Although passive RFID transponders do not need their own energy source, their functionality and communications range are very limited. Hopes are pinned on future low power processors and communications units for embedded systems that can function with significantly less energy. Energy saving is a factor not only in hardware and system architecture, but also in software, for example the implementation of protocol stacks, where every single transmission byte will have to justify its existence.

- **Wireless communications:** From an energy point of view, established wireless technologies such as GSM, UMTS, Wi-Fi and Bluetooth are far less suitable; more recent WPAN standards such as ZigBee and others still under development may have a narrower bandwidth, but they do use significantly less power.

- **Regulatory Issues**: Lack of Support of the regulatory bodies, Government agencies and ubiquitous connectivity are barriers to device integration. Even quality and cost of receiving data from multiple sources are still with issues. Companies like IBM, Cisco, GE and Amazon have decided to add Swarm and fog layers. This effort reduces the difficulty of connecting IoT devices and the cost of integrating these devices. However, Applications like home monitoring systems, wearable devices along with consumer-oriented products are the center of attention of Internet of Things domain, Enterprise IT professionals are still with issues to apply these concepts from the context of generating business values.

## V. INTERNET OF THINGS AND RELATED FUTURE TECHNOLOGIES

Many new technologies are related to IoT to prove the integration of wired as well as wireless control, communication and IT technologies together, which are responsible for connecting several subsystems and things, which operate under a unified platform, controlled and managed smartly.

### A. Cloud Computing

The two worlds of Cloud and IoT have seen a rapid and independent evolution. These worlds are very different from each other, but their characteristics are often complementary in general, in which IoT can benefit from the virtually unlimited capabilities and resources of cloud to compensate its technological constraints for example storage, processing, and communication [75]. Cloud can offer an effective solution for IoT service management and composition as well as for implementing applications and services that exploit the things or the data produced by them .On the other hand, cloud can benefit from IoT by extending its scope to deal with real world things in a more distributed and dynamic manner, and for delivering new services in a large number of real life scenarios. In many cases, Cloud can provide the intermediate layer between the things and the applications, hiding all the complexity and functionalities necessary to implement the latter. This will affect future application development, where information gathering, processing, and transmission will generate new challenges, especially in a multi cloud environment or in fog cloud [76]. Cloud facilitates for IoT application to enabling data collection and data processing, in addition to rapid setup and integration of new things, while maintaining low costs for deployment and for complex data processing [77]. Cloud is the most convenient and cost effective solution to deal with data produced by IoT and, in this respect, it generates new opportunities for data aggregation, integration, and sharing with third parties. Once into Cloud, data can be treated as homogeneous through well-defined APIs, can be protected by applying top-level security, and can be directly accessed and visualized from any place [78].

### B. Big Data

What makes big data an important asset to businesses is that it makes it possible to extract analytics and consequently knowl- edge, by which a business can achieve competitive advantage. There are some platforms for big data analytics like Apache Hadoop and SciDB. However, these tools are hardly strong enough for big data needs of IoT [79]. The amount of IoT data generally is too huge to be fed and processed by the available tools. In support of the IoT, these platforms should work in real- time to serve the users efficiently. For example, Facebook has used an improved version of Hadoop to analyze billions of mes- sages per day and offer real-time statistics of user actions [80]. In terms of resources, besides the powerful servers in data centers a lot of smart devices around us offer computing capabilities that can be used to perform parallel IoT data analytic tasks [81].

Instead of providing application specific analytics, IoT needs a common big data analytic platform which can be delivered as a service to IoT applications. Such analytic service should not impose a considerable overhead on the overall IoT ecosystem.

A recent research has proposed such an IoT big data analytics service known as TSaaaS using time series data analytics to per- form pattern mining on a large amount of collected sensor data [82]. Their analytic service relies on the Time Series Database service and is accessible by a set of RESTful interfaces. Their evaluations show that TSaaaS can perform pattern searches quicker than the existing systems. They also reported that 0.4% of the original data volume was needed as the overhead space for index storage of the service provider.

One viable solution for IoT big data is to keep track of just the interesting data only. Existing approaches can help in this field like principle component analysis (PCA), pattern reduc- tion, dimensionality reduction,

feature selection, and distri- buted computing methods [79].

### C. Security and Privacy

Due the fact that IoT applications able to access the multiple administrative domains and involve to multiple ownership regimes , there is a need for a trust framework to enable the users of the system to have confidence that the information and services being exchanged can indeed be relied upon [84]. The trust framework needs to be able to deal with humans and machines as users, for it needs to convey trust to humans and needs to be robust enough to be used by machines without denial of service. The development of trust frameworks that address this requirement will require advances in areas such as lightweight public key infrastructures (PKI) as a basis for trust management [85]. Lightweight key management systems is used to enable trust encryption materials using minimum communications and processing resources, as is consistent with the resource constrained nature of many IoT devices [86].

IoT based systems require a quality of information for metadata, which can be used to provide an assessment of their liability of IoT data. A novel method is required for IoT based systems for assessing trust in people, devices and data. One of the most methods used are trust negotiation that allows two parties to automatically negotiate, on the basis of a chain of trust policies, the minimum level of trust required to grant access to a service or to a piece of information. Internet of things uses methods for access control to prevent untrusted data breaches by control the process of ensuring the correct usage of certain information according to a predefined policy after the access to information is granted [87].

Recently, the IoT becomes a key element of the future internet, the need to provide adequate security for the IoT infrastructure becomes ever more important. A large-scale applications and services based on the IoT are increasingly vulnerable to disruption from attack or information theft. Many advanced security methods are required in several areas to make the IoT secure from attacks, thefts and many other security problems such as DoS/DDOS attacks, compromised nodes, and malicious code hacking attacks, that because the IoT is susceptible to such attacks and will require specific techniques and mechanisms to ensure that transport, energy, city infrastructures cannot be disabled or subverted [88].

The IoT requires a variety of access control and associated accounting schemes to support the various lization and usage models that are required by users. The heterogeneity and diversity of the devices/gateways that require access control will require new lightweight schemes to be developed [89]. The IoT needs to handle virtually all modes of operation by itself without relying on human control. New techniques and approaches for example like machine learning are required to lead to a self-managed IoT. Cryptographic techniques is also very important in IoT based systems for enable a means of protection for data to be stored processed and shared, without the information content being accessible to other parties. Technologies such as homomorphic and searchable encryption are potential candidates for developing such approaches [90].

### D. Distributed Computing

Distributed computing uses groups of networked computers for the same computational goal. Distributed Computing has several common issues with concurrent and parallel computing, as all these three fall in the scientific computing field. Nowadays, a large amount of distributed computing technologies coupled with hardware virtualization, service oriented Architecture and autonomic and utility computing have led to cloud computing. Internet of Things with distributed computing represents a vision in which the Internet extends into the real world embracing everyday objects. Physical items are no longer disconnected from the virtual world, but can be remotely controlled and can act as physical access points to Internet services [91].

### E. Fog Computing

Fog computing is related to the edge computing in the cloud. In contrast to the cloud, fog platforms have been described as dense computational architectures at the network's edge. Characteristics of such platforms reportedly include low latency, location awareness and use of wireless access. While edge computing or edge analytics may exclusively refer to performing analytics at devices that are on, or close to, the network's edge, a fog computing architecture would perform analytics on anything from the network center to the edge. IoT may more likely be supported by fog computing in which computing, storage, control and networking power may exist anywhere along the architecture, either in data centers, the cloud, edge devices such as gateways or routers, edge equipment itself such as a machine, or in sensors [92].

## VI. THE NEED FOR BETTER HORIZONTAL INTEGRATION BETWEEN APPLICATION LAYER PROTOCOLS

IoT devices can be classified into two major categories; namely: resource-constrained and resource-rich devices. We de- fine resource-rich devices as those that have the hardware and software capability to support the TCP/IP protocol suite. On de- vices that support the TCP/IP protocol suite, IoT applications are implemented on top of a variety of application level protocols and frameworks including REST, CoAP, MQTT, MQTT-SN, AMQP and others. On the other hand, devices that do not have the required resources to support TCP/IP cannot interoperate easily with resource-rich devices that support the TCP/IP suite. For ex- ample, microcontroller based appliances and gadgets should have the capability to interoperate with other IoT elements that are TCP/IP enabled. Beyond the interoperability issues between devices that support

TCP/IP and those that do not, TCP/IP enabled devices utilize a variety of protocols leading to a myriad of interoperability issues that limit the potential applications of the IoT. This fragmentation between the protocols utilized for communication within and across resource-constrained and resource-rich devices is not foreseen to change in the near future. This gloomy picture for interoperation between IoT devices calls for a protocol gateway that allows for better horizontal in- tegration between these diverse technologies. Several attempts have been made in the recent literature to address this issue. Paramount amongst these attempts is Ponte [93] which was initially developed as QEST [94]. Ponte offers uniform open APIs for the programmer to enable the automatic conversion be- tween the various IoT application protocols such as CoAP and MQTT. Ponte is developed under the Eclipse IoT project [95] which contains other sub projects to ease the development of IoT solutions for the consumers.

There are other academic research efforts that propose partial solutions to the problem or they have been designed for specific applications or protocols or need specific hardware. For example, the authors in [96] propose a Gateway to cover the gap between ZigBee and GPRS protocols to facilitate data transmission between wireless sensor networks and mobile communication networks. This architecture assumes the use of TCP/IP protocols.

Authors in [97] present a communication model to support multiple protocols in a medical IoT application. Their purpose is to prevent conflict between the medical wireless transmission systems and increase the throughput of those devices in hospitals and medical environments. They used the Software Defined Radio (SDR) technology as part of their platform to sense and transform the wireless signals in the frequency spectrum. Ademo is also presented in [98] in which the SDR technology is used to build a communications infrastructure for IoT applications.

An approach based on software-defined networking is pro- posed for IoT tasks in [99]. In their research, the authors developed a middleware with a layered IoT SDN controller to manage dynamic and heterogeneous multi-network environments.

From the anecdotal data that we collected so far about the di- verse needs of IoT applications and the capabilities of the under- lying hardware, it is evident to us that the strategy used by Ponte to bridge the gap between the different IoT protocols is not sufficient and a more intelligent solution is needed. To be specific, while Ponte has the capability to perform any-to-any automatic protocol conversion this conversion comes at a price as the underlying packet communication tends to be more verbose in order for it to be application agnostic. Furthermore, Ponte as many other protocol gateways that have been presented in the literature assumes the underlying devices to be TCP/IP enabled. While this “one size fits all” approach shields programmers from having to write multiple instances of the same application to support different protocols, the underlying wire-protocol can- not be controlled by the programmer and consequently leading to performance issues and inefficiencies. Yet more importantly, resource-constrained devices are treated as second-class citizens and not considered at all in this solution.

Therefore, we are motivated by the following three main observations to content for the need of a new intelligent IoT gateway:

Programmers should always be in control and they should have the flexibility to control the wire protocol. IoT devices can be resource-constrained and using application agnostic messaging leads to unnecessary packet exchanges. An intelligent gateway should allow for programmers to control the wire protocol traffic as needed to optimize the performance based on the specific needs of the given application.

Resource-constrained devices should not be treated as second-class citizens. An intelligent gateway should allow for true interoperability between resource-rich and resource-constrained devices.

Can the introduction of a protocol gateway into the IoT provide a new opportunity? An intelligent gateway should be opportunistic to create new opportunities out of the gloomy picture caused by the market fragmentation between IoT protocols.

## CONCLUSIONS

Internet of things is a new technology, which provides many applications to connect the things to things and human to things through the internet. Each objects in the world can be identified, connected to each other through internet taking decisions independently. All networks and technologies of communication are used in building the concept of the internet of things such technologies are mobile computing, RFID, wireless sensors networks, and embedded systems, in addition to many algorithms and methodologies to get management processes, storing data, and security issues. IoT requires standardized approach for architectures, identification schemes, protocols and frequencies will happen parallels, each one targeted for a particular and specific use. by the internet of things many smart applications becomes real in our life , which enable us to reach and contact with every things in addition to facilities many important aspects for human life such as smart healthcare, smart homes, smart energy , smart cities and smart environments.

Internet of things may face two major challenges in order to guarantee seamless network access; the first issue relates to the fact that today different networks coexist and the other issue is related to the big data size of the IoT. Other current issues, such as address restriction, automatic address setup, security functions such as authentication and encryption, and functions to deliver voice and video signals efficiently will probably be affected in implementing the concept of

the internet of things but by ongoing in technological developments these challenges will be overcome. The internet of things promises future new technologies when related to cloud, fog and distributed computing, big data, and security issues. By integrating all these issues with the internet of things, smarter applications will be developed as soon. This paper surveyed some of the most important applications of IoT with particular focus on what is being actually done in addition to the challenges that facing the implementation the internet of things concept, and the other future technologies make the concept of IoT feasible.

**Future scope**

The ongoing research in the field of IoT and its implementation in full or partial manner will definitely improve the quality of life of human civilization .Today IOT is being implemented everywhere which is of human concern like Smart city, smart environment, security and emergencies, smart business process, smart agriculture, domestic and home automation and healthcare. Search engine giant Google has already taken initiatives to mark its presence in the field of IoT. It is trying to transform the IoT by putting their enthrall concept of making the physical URL as future of IoT instead of apps which we commonly use. In this process, the browser will display a beacon style broadcast in which the nearby object will appear which will be present in the near proximity and can be communicated directly with the help of URL's according to the preference of users and signal strength of the smart object. On the other hand IBM and Libelium has launched 6LoWPAN development platform for IoT, which will enable every single sensor and devices to connect directly to the Internet using the new IPv6 protocols. China and many European countries are investing high amount of their GDP in making smart architectural infrastructure for e.g. Smart Roads and Bridges for the safety of people. In this smart bridges if corrosion or if any malfunction happens it will communicate directly so that repair work can be done at the proper time. Smart agriculture is also in research; Waspmote has taken this initiative for optimum productivity using the sensor networks to maintain monitoring capacity of crop cultivation throughout the production cycle. For example, depending on soil humidity Waspmote can send a message (through the ZigBee network or by SMS) to automatically switch off watering or to change water supply, thus contributing towards efficient water management.

Over 50 million sensors and smart watches, smart meters and smart phones, washing machines, fridges, wearable devices and many more things will be connected over internet by 2025.

**AUTHOR BIOGRAPHY**

Dr. Osama Ahmad Salim Safarini had finished his PhD. from The Russian State University of Oil and Gas Named after J. M. Gubkin, Moscow, 2000, at a Computerized Information systems Department. He obtained his BSC and MSC in Engineering and Computing Science from Odessa Polytechnic National State University in Ukraine 1995, 1996 respectively. He worked in different universities and countries.

References

[1] M. A. Ezechina, K. K. Okwara, C. A. U. Ugboaja. The Internet of Things (IoT): A Scalable Approach to Connecting Everything. *The International Journal of Engineering and Science* 4(1) (2015) 09-12.

[2] http://www.meraevents.com/event/IoT-workshop

[3] http://www.nxp.com/assets/documents/data/en/white-papers/INTOTHNGSWP.pdf

[4] Saranya C. M., Nitha K. P., Analysis of Security methods in Internet of Things. *International Journal on Recent and Innovation Trends in Computing and Communication,* Volume 3, Issue 4; April 2015.

[5] Sapandeep Kaur, Ikvinderpal Singh. A Survey Report on Internet of Things Applications. *International Journal of Computer Science Trends and Technology* Volume 4, Issue 2, Mar - Apr 2016.

[6] S. Misra et al., Security Challenges and Approaches in Internet of Things. Springer Briefs in Electrical and Computer Engineering, 2016.

[7] Suwimon Vongsingthong and Sucha Smanchat. A Review of Data Management in Internet of Things. *KKU Res. J.* 2015

[8] http://cdn2.hubspot.net/hubfs/552232/Downloads/Partner_program/Smart_Environments_Flyer.pdf?t=1458917278396

[9] http://docplayer.net/1073234-Internet-of-things-converging-technologies-for-smart-environments-and-integrated-ecosystems.html

[10] yavardhana Gubbia, Rajkumar Buyyab, Slaven Marusic, Marimuthu Palaniswami. Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems* 29 (2013) 1645-1660.

[11] https://dupress.deloitte.com/dup-us-en/focus/internet-of-things/IoT-commercial-real-estate-intelligent-building-systems.html

[12] Grandinetti, Lucio. Pervasive Cloud Computing Technologies: Future Outlooks and Interdisciplinary Perspectives: Future Outlooks and Interdisciplinary Perspectives. IGI Global, 2013.

[13] http://standardsinsight.com/IoT/IoTworkshop

[14] Debasis Bandyopadhyay, Jaydip Sen. Internet of Things - Applications and Challenges in Technology and Standardization. arvix 9 may 2011

[15] http://www.academia.edu/3276195/Internet_of_Things_Applications_and_Challenges_in_Technology_and_Standardization

[16] Adam D. Thierer. The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation. 21 Rich. J. L. & Tech. 6 (2015).

[17] Patrick Guillemin, et al., Internet of Things Position Paper on Standardization for IoT technologies. European research cluster on the internet of things; January, 2015.

[18] Patrick Guillemin et al., Internet of Things standardization - Status, Requirements, Initiatives and Organizations. Conference: Internet of Things - Converging Technologies for Smart Environments and Integrated Ecosystems 2013.

[19] http://www.standardsuniversity.org/e-magazine/march-2016/security-and-IoT-in-ieee-standards/

[20] Dr Ovidiu Vermesan, Dr Peter Friess. Internet of thing from research and innovation to market deployment, 2014 River Publishers.

[21] Sophia Antipolis. New ETSI specification for Internet of Things and Machine to Machine Low Throughput Networks. 30 September 2014; http://www.etsi.org/news- events/news/827-2014-09-news-etsi-new-specification-for-internet-of-things-and-machine-to-machine-low-throughput-networks

[22] Building the future; http://www.etsi.org/images/files/WorkProgramme/etsi-work- programme-2015-2016.pdf

[23] https://www.ietf.org/proceedings/91/overview.html

[24] http://www.ipv6forum.com/IoT/index.php/homepage

[25] http://IoT6.eu/IoT6_main_achievements

[26] Isam Ishaq et al., IETF Standardization in the Field of the Internet of Things (IoT): A Survey. *J. Sens. Actuator Netw.* 2 (2013) 235-287, doi: 10.3390/jsan2020235

[27] Nicola Accettura. Optimal and Secure Protocols in the IETF 6TiSCH communication. stack; http://telematics.poliba.it/publications/2014/Accettura ISIE2014 .pdf

[28] Gérald Santucci. Internet of things: an early reality of the future internet. May 2009. http://cordis.europa.eu/pub/fp7/ict/docs/enet/IoT-prague-workshop-report-vfinal- 20090706_en.pdf

[29] http://www.itu.int/en/ITU-T/techwatch/Pages/internetofthings.aspx

[30] N. Koshizuka and K. Sakamura, “Ubiquitous ID: Standards for Ubiqui- tous computing and the Internet of Things,” IEEE Pervasive Comput., vol. 9, no. 4, pp. 98–101, Oct.–Dec. 2010.

[31] N. Kushalnagar, G. Montenegro, and C. Schumacher, “IPv6 over Low- Power Wireless Personal Area Networks (6LoWPANs): Overview, assumptions, problem statement, and goals,” Internet Eng. Task Force (IETF), Fremont, CA, USA, RFC4919, vol. 10, Aug. 2007.

[32] G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler, “Transmission of IPv6 packets over IEEE 802.15. 4 networks,” Internet Eng. Task Force (IETF), Fremont, CA, USA, Internet Proposed Std. RFC 4944, 2007.

[33] K. Pilkington, “Revolv teams up with Home Depot to keep your house connected,” Centre National d’Etudes des Telecommunications (CNET), San Francisco, CA, USA, CNET—News, 2014. [Online]. Available: http://Ces.Cnet.Com/8301-35306_1-57616921/Revolv-Teams-Up-with-Home-Depot-to-Keep-Your-House-Connected/

[34] SmartThings | Home automation, home security, and peace of mind,” SmartThings, Palo Alto, CA, USA, Sep. 2014. [Online]. Available: http://www.smartthings.com

[35] U. Rushden, Belkin Brings Your Home to Your Fingertips With WeMo Home Automation System. Los Angeles, CA, USA: Press Room Belkin, 2012.

[36] R. Want, “An introduction to RFID technology,” IEEE Pervasive Comput., vol. 5, no. 1, pp. 25–33, Jan.–Mar. 2006.

[37] R. Want, “Near field communication,” IEEE Pervasive Comput., vol. 10, no. 3, pp. 4–7, Jul./Sep. 2011.

[38] [29]R. S. Kshetrimayum, “An introduction to UWB communication systems,” IEEE Potentials, vol. 28, no. 2, pp. 9–13, Mar./Apr. 2009

[39] E. Ferro and F. Potorti, “Bluetooth and Wi-Fi wireless protocols: A survey and a comparison,” IEEE Wireless Commun., vol. 12, no. 1, pp. 12–26, Feb. 2005.

[40] P. McDermott-Wells, “What is Bluetooth?” IEEE Potentials, vol. 23, no. 5, pp. 33–35, Jan. 2005.

[41] Press releases detail: Bluetooth technology website,” Bluetooth Tech- nol. Website, Kirkland, WA, USA, Sep. 2014. [Online]. Available: http:// www.bluetooth.com/Pages/Press-Releases-Detail.aspx?ItemID=197

[42] IEEE Standard for Local and Metropolitan Area Networks—Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs), IEEE Std. 802. 15. 4-2011, 2011.

[43] G. V. Crosby and F. Vafa, “Wireless sensor networks and LTE-A network convergence,” in Proc. IEEE 38th Conf. LCN, 2013, pp. 731–734.

[44] A. Ghosh, R. Ratasuk, B. Mondal, N. Mangalvedhe, and T. Thomas, “LTE-Advanced: Next-generation wireless broadband technology [In- vited Paper],” IEEE Wireless Commun., vol. 17, no. 3, pp. 10–22, Jun. 2010.

[45] A. Dunkels, B. Gronvall, and T. Voigt, “Contiki—A lightweight and flex- ible operating system for tiny networked sensors,” in Proc. 29th Annu. IEEE Int. Conf. Local Comput. Netw., 2004, pp. 455–462.

[46] P. Levis et al., “TinyOS: An operating system for sensor networks,” in Ambient Intelligence. New York, NY, USA: Springer-Verlag, 2005, pp. 115–148.

[47] Q. Cao, T. Abdelzaher, J. Stankovic, and T. He, “The LiteOS operating system: Towards Unix-like abstractions for wireless sensor networks,” in Proc. Int. Conf. IPSN, 2008, pp. 233–244.

[48] E. Baccelli, O. Hahm, M. Günes, M. Wählisch, and T. C. Schmidt, “RIOT OS: Towards an OS for the Internet of Things,” in Proc. IEEE Conf. INFOCOM WKSHPS, 2013, pp. 79–80.

[49] Open Auto Alliance, Oct. 20, 2014. Available: http://www. openautoalliance.net/

[50] X. Xiaojiang, W. Jianli, and L. Mingdong, “Services and key technolo- gies of the Internet of Things,” ZTE Commun., Shenzhen, China, vol. 2, p. 011, 2010.

[51] M. Gigli and S. Koo, “Internet of Things: Services and applications cat- egorization,” Adv. Internet Things, vol. 1, no. 2, pp. 27–31, Jul. 2011.

[52] D. J. Cook, A. S. Crandall, B. L. Thomas, and N. C. Krishnan, “CASAS: A smart home in a box,” Computer, vol. 46, no. 7, pp. 62–69, Jul. 2013.

[53] N. Komninos, E. Philippou, and A. Pitsillides, “Survey in smart grid and smart home security: Issues, challenges and countermeasures,” IEEE Commun. Surveys Tuts., vol. 16, no. 4, pp. 1933–1954, 4th Quart. 2014.

[54] E. Finch, “Is IP everywhere the way ahead for building automation?” Facilities, vol. 19, no. 11/12, pp. 396–403, 2001.

[55] C. Talcott, “Cyber–physical systems and events,” in Software-Intensive Systems and New Computing Paradigms, M. Wirsing, J. Banatre, M. Hölzl, and A. Rauschmayer, Eds. New York, NY, USA: Springer Sci. Business Media, 2008, pp. 101–115.

[56] L. Yongfu, S. Dihua, L. Weining, and Z. Xuebo, “A service-oriented architecture for the transportation cyber–physical systems,” in Proc. 31st CCC, 2012, pp. 7674–7678.

[57] L. Ying and Z. Lingshu, “Novel design of intelligent Internet-of-vehicles management system based on cloud-computing and Internet-of-Things,” in Proc. Int. Conf. EMEIT, 2011, pp. 3190–3193.

[58] M. Gerla, L. Eun-Kyu, G. Pau, and L. Uichin, “Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds,” in Proc. IEEE WF-IoT, 2014, pp. 241–246.

[59] A. Strange, “Toyota, Audi prepping self-driving cars,” PC, New York, NY, USA, PCMag.Com: New Product Rev. 2013. [Online]. Available: http://Www.Pcmag.Com/Article2/0,2817,2413841,00.Asp

[60] J. Markoff, “Google cars drive themselves, in traffic,” New York Times, New York, NY, USA, 2010. [Online]. Available: http://www.Nytimes.com/2010/10/10/Science/10google.Html?Pagewanted=all&_r=0

[61] A. Del-Colle, “Volvo will test autonomous cars on Sweden’s streets— Popular mechanics,” Popular Mechanics, Cars, News, New York, NY, USA, 2013.

[62] I. Ungurean, N. C. Gaitan, and V. G. Gaitan, “An IoT architecture for things from industrial environment,” in Proc. 10th Int. COMM, 2014, pp. 1–4.

[63] C. Wang, Z. Bi, and L. D. Xu, “IoT and cloud computing in automation of assembly modeling systems,” IEEE Trans. Ind. Informat., vol. 10, no. 2, pp. 1426–1434, May 2014.

[64] “Radical-7 breakthrough measurements. Radical monitor,” Masimo Corp., Irvine, CA, USA, Data Sheet Radical-7, 2013.

[65] C. Nay, “Sensors remind doctors to wash up,” IBM Res., Armonk, NY, USA, 2013.

[66] K. Michaelsen, J. L. Sanders, S. M. Zimmer, and G. M. Bump, “Overcoming patient barriers to discussing physician hand hygiene: Do patients prefer electronic reminders to other methods?” Infection Con- trol, vol. 34, no. 9, pp. 929–934, Sep. 2013.

[67] S. Jain et al., “A low-cost custom HF RFID system for hand wash- ing compliance monitoring,” in Proc. IEEE 8th ASICON, 2009, pp. 975–978.

[68] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, “A survey on smart grid com- munication infrastructures: Motivations, requirements and challenges,” IEEE Commun. Surveys Tuts., vol. 15, no. 1, pp. 5–20, 1st Quart. 2013.

[69] T. Gea, J. Paradells, M. Lamarca, and D. Roldan, “Smart cities as an appli- cation of Internet of things: Experiences and lessons learnt in Barcelona,” in Proc. 7th Int. Conf. IMIS Ubiquitous Comput., 2013, pp. 552–557.

[70] J. Jin, J. Gubbi, S. Marusic, and M. Palaniswami, “An information framework for creating a smart city through Internet of Things,” IEEE Internet Things J., vol. 1, no. 2, pp. 112–121, Apr. 2014.

[71] P. Barnaghi, W. Wang, C. Henson, and K. Taylor, “Semantics for the Internet of Things: Early progress and back to the future,” Proc. IJSWIS, vol. 8, no. 1, pp. 1–21, Jan. 2012.

[72] T. Kamiya and J. Schneider, “Efficient XML Interchange (EXI) Format 1.0,” World Wide Web Consortium, Cambridge, MA, USA, Recommend. REC-Exi-20110310, 2011.

[73] Ron Davies. The Internet of Things Opportunities and challenges. May 2015. http://www.europarl.europa.eu/RegData/etudes/BRIE/2015/557012/EPRS_BRI(2015)5 57012_EN.pdf

[74] Friedemann Mattern and Christian Floerkemeier. From the Internet of Computers to the Internet of Things. https://www.vs.inf.ethz.ch/publ/papers/Internet-of-things.pdf

[75] Alessio Botta, Walter de Donato, Valerio Persico, Antonio Pescap´e. On the Integration of Cloud Computing and Internet of Things. http://wpage.unina.it/walter.dedonato/pubs/IoT_ficloud 14.pdf

[76] Yu Liu, Beibei Dong, Benzhen Guo, Jingjing Yang and Wei Peng. Combination of Cloud Computing and Internet of Things (IOT) in Medical Monitoring Systems. *International Journal of Hybrid Information Technology* 8(12) (2015) 367-376.

[77] Isna Khan, Prof S.D. Sawant. A Review on Integration of Cloud Computing and Internet of Things. *International Journal of Advanced Research in Computer and Communication Engineering* Vol. 5, Issue 4, April 2016.

[78] http://www.csi-india.org/communications/SeptDec2015.pdf

[79] C. Tsai, C. Lai, M. Chiang, and L. T. Yang, “Data mining for Internet of Things: A survey,” IEEE Commun. Surveys Tuts., vol. 16, no. 1, pp. 77– 97, 1st Quart. 2014.

[80] D. Borthakur et al., “Apache Hadoop goes realtime at Facebook,” in Proc. 2011 ACM SIGMOD Int. Conf. Management Data, 2011, pp. 1071–1080.

[81] A. Mukherjee, H. S. Paul, S. Dey, and A. Banerjee, “ANGELS for dis- tributed analytics in IoT,” in Proc. IEEE WF-IoT, 2014, pp. 565–570.

[82] X. Xu, S. Huang, Y. Chen, K. Browny, I. Halilovicy, and W. Lu, “TSAaaS: Time series analytics as a service on IoT,” in Proc. IEEE ICWS, 2014, pp. 249–256.

[83] Rebecca Sawyer. The Impact of New Social Media on Intercultural Adaptation. University of Rhode Island, 2011. http://digitalcommons.uri.edu/cgi/viewcontent.cgi?article=1230&context=srhonorsprog

[84] Odulaja, G.O., Security issues in internet of the things. *Computing, Information Systems, Development Informatics & Allied Research Journal*, Vol. 6, No. 1, March 2015.

[85] P. Saichaitanya1, N. Karthik, D. Surender. Recent trends in IoT. International Journal of Electrical and Electronics Engineering, Vol. 8, Issue 2, December 2016.

[86] Shahid Raza. Lightweith security solutions for the internet of things. Mälardalen University Press Dissertations, 2013. http://www.diva-portal.org/smash/get/diva2:619066/FULLTEXT02

[87] Jaydip Sen. Security and privacy issues in cloud computing. Innovation Labs, Tata Consultancy Services Ltd., Kolkata, India. https://arxiv.org/ftp/arxiv/papers/1303/1303.4814.pdf

[88] http://www.cloud-council.org/deliverables/CSCC-Cloud-Security-Standards-What-to-Expect-and-What-to-Negotiate.pdf

[89] https://www.ntia.doc.gov/files/ntia/publications/marcus_response_to_IoT_rfc_rin_0660x c024 0.pdf

[90] Paula Fraga-Lamas, et al., A Review on Internet of Things for Defense and Public Safety. *Sensors* (Basel) 2016 Oct., 16(10), 1644.

[91] Virendra Dilip Thoke. Theory of distributed computing and parallel processing with applications, advantages and disadvantages. *International Journal of Innovation in Engineering, Researchand Technology.* http://www.ijiert.org/admin/papers/1452798652_ICITDCEME%E2%80%9915.pdf

[92] https://www.rtinsights.com/what-is-fog-computing-open-consortium/

[93]Ponte—M2M Bridge framework for REST developers, Eclipse, Ottawa, ON, USA, Sep. 25, 2014. [Online]. Available: http://eclipse.org/proposals/technology.ponte/

[94]M. Collina, G. E. Corazza, and A. Vanelli-Coralli, “Introducing the QEST broker: Scaling the IoT by bridging MQTT and REST,” in Proc. IEEE 23rd Int. Symp. PIMRC, 2012, pp. 36–41.

[95]Eclipse IoT, Sep. 25, 2014. [Online]. Available: https://projects.eclipse. org/projects/iot

[96]Q. Zhu, R. Wang, Q. Chen, Y. Liu, and W. Qin, “IOT gateway: Bridging wireless sensor networks into Internet of Things,” in Proc. IEEE/IFIP 8th Int. Conf. EUC, 2010, pp. 347–352.

[97]X. Wang, J. T. Wang, X. Zhang, and J. Song, “A multiple communication standards compatible IoT system for medical usage,” in Proc. IEEE FTFC, 2013, pp. 1–4.

[98]Y. H. Lin, Q. Wang, J. S. Wang, L. Shao, and J. Tang, “Wireless IoT plat- form based on SDR technology,” in Proc. IEEE Int. Conf. IEEE Cyber, Phys. Soc. Comput. GreenCom, iThings/CPSCom, 2013, pp. 2245–2246.

[99]Z. Qin, G. Denker, C. Giannelli, P. Bellavista, and N. Venkatasubramanian, “A software defined networking architecture for the Internet-of-things,” in Proc. IEEE NOMS, 2014, pp. 1–9.

BIOGRAPHY

Dr. Osama Ahmad Salim Safarini had finished his PhD. from The Russian State University of Oil and Gas Named after J. M. Gubkin, Moscow, 2000, at a Computer-Aided Information Control system Department. He obtained his BSC and MSC in Engineering and Computing Science from Odessa Polytechnic National State University in Ukraine 1995, 1996 respectively. He worked in different universities and countries.