International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A Review of IoT Architectures – Internet of Vehicles, Smart healthcare, Smart Grid

Manoj Kumar Paramasivam [a], Anima Sahu [b]

[a] *Arizona State University, Tempe, Arizona, USA*
[b] *Arizona State University, Tempe, Arizona, USA*

A B S T R A C T

The Internet of Things (IoT) is the everywhere in the connected world. IoT envisions a future in which the digital and the physical entities can be connected by means of suitable information and communication technologies, to enable a whole new class of services and applications. IoT possesses huge potential which can be harnessed to improve living and make a better world. Various applications of IoT have been proposed till date in several papers, like the smart buildings and cities, smart grids for energy conservation, healthcare applications, Internet of Vehicles (IoV) etc. This paper surveys on the emerging applications of the Internet of Things, specifically IoV, Smart Healthcare and Smart grid, their architectures and related available literature. Furthermore, the paper also explores the new technical concepts for improving the present IoT architecture to provide intelligence and environmental friendly IoT in the future.

Keywords: Internet of Things (IoT), IoT applications, IoT architecture, Smart healthcare, Internet of Vehicles (IoV), Smart Grid,

1. Introduction

The Internet of Things (IoT) is a concept that accomplishes a connected network of things or objects which can communicate within them with or without human interaction. These connected nodes, which can be either wired or wireless, need to have unique addressing. In this context, the challenges faced by the research community to create a smart world are enormous. The IoT world is where the real, digital and virtual are coming closer to create smart environments. The goal of the Internet of Things is to enable things to be linked anytime, anyplace, with anything and anyone ideally, using any available path/network.

The IoT revolution has been started due to the universal expanse of the internet and the transition from IPv4 to IPv6, which can provide an almost unlimited range of unique addresses. The internet in IoT is the communication tool which provides access to information, media and services. The IoT makes use of the synergies as the consumer; business and industrial internet are merging. This forms a globally available open network connecting people, data, and things. This convergence enables cloud to connect things that can sense and transmit a broad range of data, and generating services that would not be possible without this level of connectivity and analytical intelligence. The use of platforms is being driven by the new-age technologies such as cloud and mobile computing.

The definition for IoT as formulated by the International Telecommunications Union (ITU) on the standards for next generation networks (NGN) and future networks is as follows [2]. “Internet of things (IoT): 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 IERC (European Research Cluster for Internet of things) definition states that IoT is “A dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual “things” have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network [3].”

The IoT is presently in its initial stages of development. Wireless sensor networks based home and business automation; healthcare services, industrial control of equipments, etc. are providing the background to establish this universal IoT network. This can only be possible by the conglomeration of different technologies from communication to electronics, from cloud computing to sensor networks. The IoT can be a factor which can unite the various advancing technologies and together bring us the smart world.

In this paper, we provide an extensive review of available literature on the various emerging applications of IoT, the technologies involved, their architectures and respective research trends. Moreover, we provide insights into the future research trends in development and establishing the IoT. In section 2, we describe about the IoT architecture models and the IoT-A universal functional reference model architecture. In section 3, we review the various applications of IoT, the Internet of Vehicles (IoV), Smart healthcare, Smart Grids, Finally, we conclude the paper in section 4.

2. IoT Architecture

Establishing the IoT would require several interconnected modules which should perform autonomously as well as together to provide the necessary services. The following are the various modules which are needed to make a functional IoT system as described in [4].

- Module for interaction with local IoT devices (for example embedded system in a mobile phone or smart watch and which is contactable via a short range wireless interface).

- Module for local analysis and processing of observations acquired by IoT devices.

- Module for interaction with remote IoT devices, directly over the Internet.

- Module for application specific data analysis and processing.

- Module for integration of IoT-generated information into the business processes of an enterprise.

The basic architecture of IoT is the three-layer, as shown in Fig. 1(a), which is widely accepted and is described in [5, 49]. The perception layer or sensing layer is the hardware or physical layer which is responsible for the data acquisition. The network layer is the middle layer and provides the connection between the hardware and the applications. The top application layer plays the role of providing services and / or applications that incorporate and analyze the information received from the bottom layers.

The five-layer architecture of IoT as shown in Fig. 1(b) and in [5, 49], adds the access gateway layer and the middleware layer to the three-layer architecture model. The perception layer is also called the edge layer, which is same as in the three-layer architecture. The connection between the perception and application layers is managed by the access gateway and network layer. The middleware layer provides greater flexibility to interface between the hardware and applications. The top application layer is similar to the three-layer architecture, providing services.

The general architecture of IoT, explained above can be applied for the development of simple and smart IoT environment architectures. The IoT-A (IoT-Architecture) project [6], funded by EU focuses on establishing a common architectural model for IoT. Fig. 2 shows the functional model of IoT Reference Architecture as developed by the IoT-A project [6]. This reference architecture includes all the possible functional entities or blocks for developing and establishing an IoT.

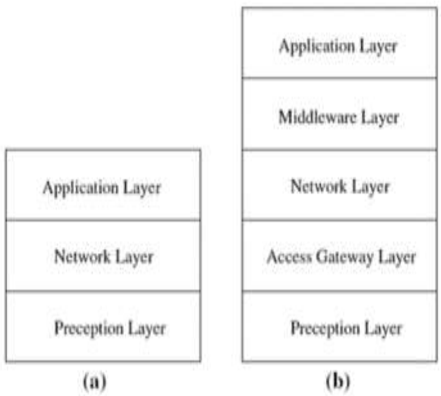

Fig. 1: General IoT architectures

This IoT Reference Architecture is, among others, designed as a reference for the generation of IoT-compliant and concrete architectures that can be tailored to one's specific needs. This model addresses the four basic IoT architecture requirements, that are, evolution and interoperability; performance and scalability; trust, security, and privacy; and availability and resilience.

3. IoT Applications

The vision of Internet of Things is to make our lives simpler, smarter and safer. Towards achieving this goal, the applications pertaining to IoT are varied in nature. In this paper we discuss the most beneficial applications of IoT, the involving technologies, architecture and the corresponding research.

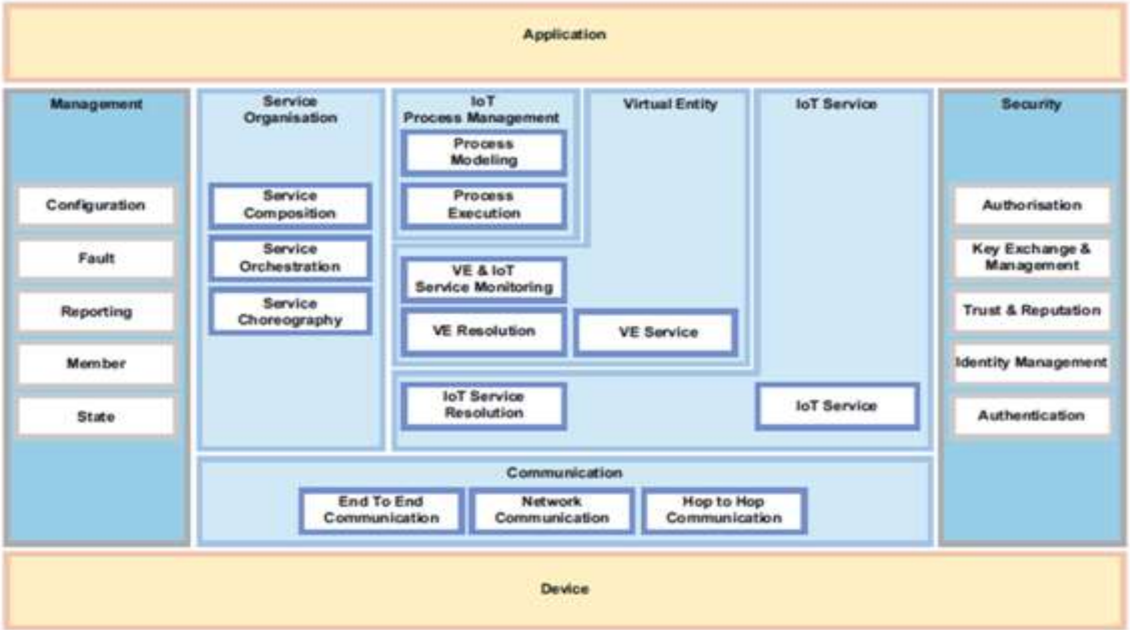

Fig. 2: Functional model of IoT Reference Architecture

3.1 Internet of Vehicles (IoV)

The IoV concept is to create a connected network of vehicles, (based on the Vehicular Ad-hoc Networks (VANETs)) which are connected to external environments and are able to send / receive data to / from the environment through internet. This will lead to the growth of automotive revolution and make path for development of the intelligent transportation systems (ITS). Internet-connected vehicles will be able to meet the demand of uninterrupted mobile data during travelling. The vehicles could also be constantly observed and they can communicate with cloud-based services which can support various applications for road safety (e.g., collision detection, lane change alert and cooperative merging), smart and efficient transportation (e.g., traffic signal control, intelligent traffic scheduling, and fleet management) and location-dependent services (e.g., route optimization) [7]. Intelligent transportation systems (ITS), in general, and vehicle area networks (VAN), in particular, are expected to grow with the goal of achieving an accident-free driving environment. The key prerequisite of VAN is efficient wireless intra- and inter-vehicle communication which will collect and exchange data among the driver, car, and road infrastructure. Analytics play a major role in the future network of smart vehicles to quickly detect unsafe situations, alert the driver and / or police, and avoid accidents and unwanted situations. Such goals require multidisciplinary analytics from signal processing, to machine learning and data mining.

The different connectivity links that need to be established for IoV architecture are Vehicle to onboard Sensor electronics (V2S), Vehicle to Vehicle (V2V), Vehicle to Road infrastructure (V2R) and Vehicle to Internet (V2I). Different communication technologies can be used to achieve the required network setup.

Vehicle to onboard Sensor electronics (V2S): The V2S connectivity is largely dependent on the embedded sensors in the vehicles. The authors in [7] state that the number of sensors in modern vehicles has increased manifold in the recent years and is likely to increase further. Intelligent intra-vehicle communication systems for detecting a vehicle's performance and like the driver's fatigue and health, is critical for driver and public safety. Machine learning techniques can be extensively used for such data classification. This sensor network also collects other vehicle information such as the speed, pressure on the brake or gas pedal, steering wheel rotation, and global positioning system (GPS) routing. It may transmit this data to a monitoring data center for additional processing and receive feedback, for example, a warning signal, for the driver. In this scenario the data reliability is essential. The sensor data and feedback control and management are a primary requirement to establish a reliable system.

The vehicular sensor networks are stationary in nature, and connected to a control unit. Generally, they do not have any energy constraint. The paper [9] lists some of the wired communication protocols for V2S – Controller Area Network (CAN), the earliest serial communication protocol, Local Interconnect Network (LIN) for ultra low cost and low speed (19.2kbps) communication and FlexRay, that provides deterministic and fault-tolerant communication up to 10Mbps. However, wired solutions are not really an alternative with the large number of onboard sensors. In case of wireless communication, the associated challenges are acute scattering and no Line-of-Sight path, interference from nearby vehicles in urban traffic situation, critical security and privacy, and low data latency and high reliability. A specialized communication network with the ability to operate in a harsh environment is required to interconnect all these onboard sensors. Some of the potential technologies for the V2S network are described in [7]. The Zigbee and RFID seem to be the most feasible solutions. A few other alternatives are Ultra Wide Band (UWB) and 60GHz Millimeter Wave.

The paper [10] compares the two technologies, Zigbee and RFID, and proposes Zigbee as an advantageous alternative, except for higher cost. It states that, ZigBee is based on active technology that requires battery power, so the power loss problem seen with passive RFID is not a concern. The ZigBee technology can be deployed with off-the-shelf components as it is mainly a ready-to-use technology, while passive RFID is designed for inventory control and needs significant modifications in the design of the operating system / protocol. The paper confirms with the experimental results that link quality can be improved by some simple schemes. However, Zigbee suffers due to the vehicle engine noise and interference from Bluetooth devices which are usually present in modern vehicles.

Multihop communication has been considered as a preferable method for in-vehicle communication in [11]. The paper states that, despite its greater overhead, it can enhance overall system reliability, provide robust performance, and reduce the required energy for transmission. It uses the Collection Tree Protocol (CTP) as a multihop network layer protocol as it is the standard IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL). The results demonstrated in the paper show that the packet delivery rate of a node using single-hop topology protocol can be below 80 percent in practical scenarios, whereas CTP improves reliability performance greater than 95 percent across all sensor nodes with the reduction in RF energy consumption.

Vehicle to Vehicle (V2V): Inter-vehicle wireless links have the primary purpose of transmitting the sensor or vehicle computer's data to other vehicles present in the adhoc networks (VANETs) or the data control center. This V2V communication is utilized for traffic monitoring applications [7] and road safety like avoiding accidents and collisions. The major challenges for V2V communication are the dynamically changing networks due to fast moving vehicles, data loss due to change in network topology and Doppler Effect, and fading issues due to no LOS path. However, the paper [7] also states that the vehicular tracking would be easier by using GPS and the vehicles poses no constraint on the communication power levels.

The Dedicated Short Range Communication (DSRC) is a promising and researched technique [12] which can be used for the V2V communication. DSRC uses orthogonal frequency division multiplexing (OFDM) for communication and can support a data rate of 3-27 Mbps on a 10MHz channel. The DSRC channel allocation scheme is shown in fig. 3. The challenges associated with using DSRC as given in [13] are that reliable communication is not guaranteed when the LOS path is unavailable or there is a considerable delay spread of wireless channel. Cross-channel interference degrades the performance, when two adjacent channels are operated simultaneously; and result in gray-zone phenomenon, i.e., intermittent loss rate during the transmission. To accommodate to the requirements of vehicular environment, DSRC PHY layer is needs to keep evolving. More challenges in this evolution are discussed in [13], such as the difficulty in estimating the channel condition accurately. The OFDM system design guidelines in the DSRC PHY layer are also given in [14], such as a suggestion of a modified pilot pattern to reduce receiver complexity.

The currently used MAC protocol is based on one-hop broadcast, where the broadcast happens to all nodes in the communication network. This requires low latency and high reliability. The present version of DSRC MAC is contention based and therefore is not suitable for broadcast [7].

In the paper [15], a new wideband MIMO V2V regular-shaped geometry-based stochastic model (RSGBSM) has been proposed. This has the ability to model the Doppler spectrum and the impact of Vehicle movement on communication channel.

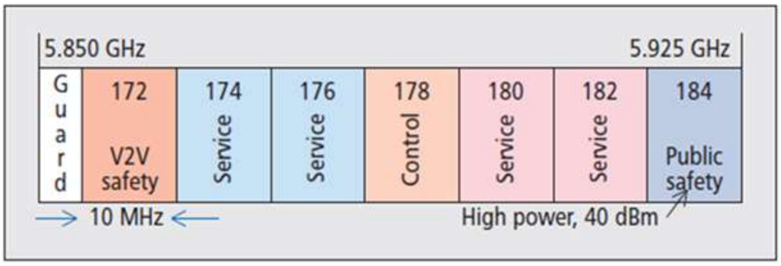

Fig. 3: DSRC Channel Allocation

This paper also proposes a new Inter-Carrier-Interference (ICI) cancellation and two-path cancellation scheme called Precoding Based Cancellation (PBC) aided with Constant Phase Rotation (CPRA). The PBC scheme involves redundant signals by suitably applying the mapping standards and mapping functions in two OFDM blocks separated by the TDM. This can successfully cancel ICI without any measurable performance degradation unlike the self ICI cancellation. The PBC along with the CPRA improves the overall performance.

In another paper [16], optical communication technology has been proposed for V2V communication. The link is established based on LED transmitters and a camera receiver installed in the vehicle chassis. The LED transmitter is capable of sending various data by 10 Mb/s optical signals. The camera receiver has a special CMOS image sensor, the optical communication image sensor (OCI), which contains a communication pixel array for high-speed optical signal reception and a flag image output function for assisting LED detection in outdoor environments. By using the OCI, the camera receiver can obtain 10 Mb/s optical signal reception and the sensor provides precise detection capabilities.

Another challenge for V2V communication is the shortage of available frequency spectrum, due to the demand of high data infotainment activities (high quality video streaming). The dynamic spectrum access (DSA) as in [17] is a suitable alternative which can allow vehicles to communicate opportunistically on spatially and / or temporally available channels. Studies and measurements show that DSA can be the beginning of the heterogeneous spectrum allocation scheme of V2V communication.

Vehicle to Internet (V2I): Internet connectivity has become an essential requirement in the modern vehicles, mostly for infotainment applications. The cellular and WiFi access technologies are the two promising technologies for providing internet connectivity to vehicles. With the expanse of cellular networks, 3G and 4G-LTE, connecting vehicles to internet can be made ubiquitous. Connecting to cellular networks might be through the smart phones plugged into vehicles or independent modules in the vehicles to connect to the cellular networks. Though WiFi connection provides a low cost solution, the connectivity would mostly remain limited to roadside WiFi access points [7].

In [18], a dynamic optimal algorithm is proposed for connection with roadside access points (APs). The main features of the proposed scheme are 1) Optimal Access Policy Design: In case of a single AP with random vehicular traffic, it proposes a general dynamic optimal random access (DORA) algorithm which computes the optimal access policy. It further extends the results to the case of multiple consecutive APs and proposes a joint DORA (JDORA) algorithm to compute the optimal policy. 2) Low Complexity and 3) Superior Performance.

Vehicle to Road infrastructure (V2R): V2R connectivity is critical to avoid or mitigate the effects of road accidents, and to allow for the efficient management of ITSs. DSRC/WAVE is considered an important technology to facilitate connections between vehicles and ITS infrastructure, such as traffic lights, street signs, and roadside sensors. The Road Side Unit (RSU) generally, but not necessarily, serves as Internet gateway i.e. wireless infrastructures in V2I communications [7]. Optical communication using LEDs can also be used for V2R communication [16] similar to V2V communications mentioned earlier.

Vehicular Cloud: The vehicular cloud can contribute in many different ways to the vehicle grid. In [19], the authors aim to connect vehicle resources into a cloud for sensing, storage, and computing; whereas, in [20], the authors propose a cloud of (On-Board Unit) OBUs and still some propose RSUs acting as gateways to traditional clouds.

In the paper [21], a novel concept of RSU cloud is proposed as shown in fig. 4. It consists of conventional RSUs and microscale datacenters. The RSU cloud hosts services / applications to meet the changing demands from the vehicle grid. This RSU cloud architecture employs the flexibility and programmability provided by software-defined networking (SDN). In SDN, there are two communication planes, the physical data plane and the abstracted control plane. The separation of control and data planes in SDN allows for the flexibility and programmability. In RSU clouds, virtualization via virtual machines (VMs) and SDN is used to dynamically instantiate, change, and / or reproduce services and dynamically rearrange data forwarding in the network according to the changing service demands. An RSU microdatacenter, is a traditional RSU with additional hardware and software components that offer virtualization and communication resources using SDN. The microdatacenter hardware consists of a small computing device and an OpenFlow switch.

In [22], high performance vehicle streams combining control and communication architecture is presented. The framework is based on coupling transportation layer architecture with the Wireless Access in Vehicular Environment (WAVE) communication protocol. The proposed cooperative adaptive cruise control (CACC) system has the following characteristics: integrated transportation and communication protocols; heterogeneous traffic; semi-automatic operation; subplatooning; fault tolerance.

Vehicle-as-a-Resource (VaaR): The concept of VaaR is a new research domain illustrating the advantages of an intelligent vehicle. In [23], the authors present the concept of as intelligent vehicle and VaaR. With accessible mobile resources in intelligent vehicles, it can be used for many other services such as sensing, data relaying and storage, data computing, cloud, infotainment, and localization. The VaaR vision is inspired by the ubiquity of vehicles (with expected movement patterns) and readily available vehicular resources. The abundance of such on-board resources differentiates the use of a vehicle as a resource from other mobile resources, viz. smartphones, which suffer from limited resources and no trajectory prediction. It is expected by the authors that a vehicle will be a mobile provider for various resources and will be a key enabler for the revolution of the Internet of Things (IoT).

Content Distribution in IoVs: With the growth of cloud services and access to ubiquitous internet, content distribution to vehicles has become a challenging task, due to the strict constraints of maintaining connectivity, coverage, and topology of vehicles. In the paper [24], the authors propose a Bayesian coalition game-as-a-service model to solve the problem. Vehicles are assumed to be players in the game algorithm and dynamic coalition among them is done using Markov decision Process (MDP). Actions taken by players in the game are taken based on conditional probability defined by Bayes theorem. Action probability vector of the automaton is updated based on the inputs received from the environment and the vehicles.

Summary: The surveyed literature in this section provides the research trends in establishing the Internet of Vehicles (IoVs); a significant application of the IoT. The IoV requires connectivity links for V2S, V2V, V2I and V2R which are described in [7]. The Zigbee and RFID seem to be most suitable alternatives for the V2S communication. The V2V and V2R links are based on DSRC / WAVE technology. The optical communication is the new domain which needs to be explored. V2I communication requires cellular or WiFi links [16]. The Vehicular cloud architecture with SDN is proposed by [21]. Finally, the Vehicle as a Resource concept for IoT is described in [23] and the content distribution as a game model is proposed in [24]. The Internet of Vehicles envisions the future VAN integrating wireless local and wide area network technologies using portable IP-centric devices, sensors, signal processing, and behaviour analysis techniques. Ultimately, the future vehicle area networks would collect data from driver, car, and road, quickly analyze and share the information to provide a safe and secure driving environment in future networks of smart vehicles and Intelligent Transportation Systems (ITS).

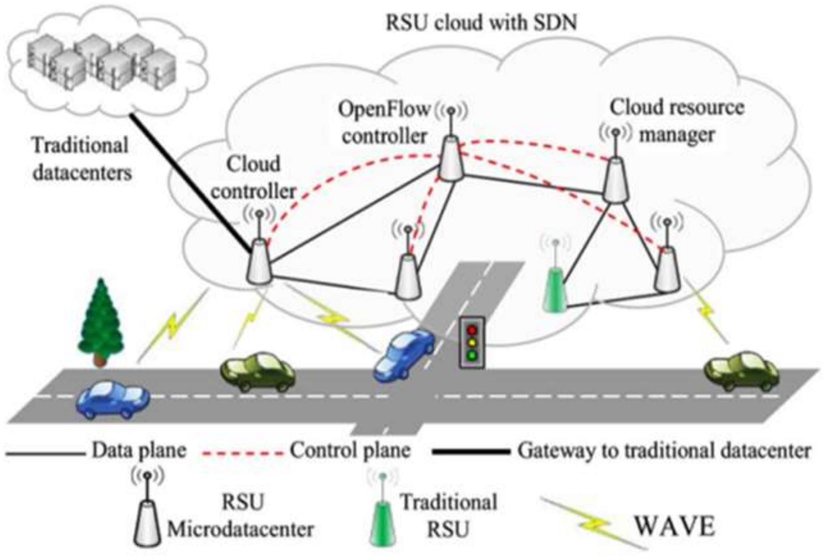

Fig. 4: RSU cloud architecture

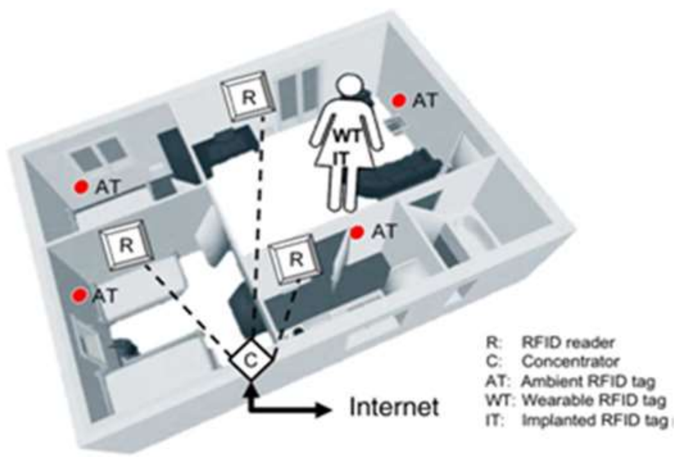

Fig. 5: RFID powered habitat for personal healthcare

3.2 Smart Healthcare

Improving the efficiency of healthcare infrastructures and biomedical systems are one of the most challenging goals of modern society. The current procedures for patient monitoring, healthcare, management, and supervision are often done manually by the nursing staff. This can result in an efficiency bottleneck which could cause errors in practice. Recent developments in the design of Internet of Thing (IoT) technologies are steering the development of smart systems to assist and improve healthcare and biomedical-related processes. Automatic identification and tracking of people and biomedical devices in hospitals, accurate drug-patient requirements, real-time monitoring of patients' physiological parameters for timely detection of health deterioration are only a few of the promising applications of smart healthcare. The two most potential technologies which can be implemented for building the smart healthcare are Ultra High Frequency (UHF) Radio Frequency Identification (RFID) and Wireless Sensor Networks (WSN).

RFID: The RFID based smart healthcare application of IoT is described in the paper [25]. The passive RFID system is made up of a digital sensing device called tag, an embedded antenna, an IC-chip with unique identification code (ID), and a radio scanner device, called reader. Readers can interact, using WiFi or Bluetooth links, with a concentrator node facilitating the interconnection with external services that carry out data processing and assistance procedures' activation. RFID systems could allow implementing, in a simple and organised way, the last few meters of the IoT for the omnipresent quantification of the person's interaction with the environment.

Passive RFID ambient sensors / tags would be able to perceive physical conditions of the environment, such as the temperature, humidity, and the presence of toxic agents, could allow to quantify the wellbeing of the environment and to analyze its association with the patient's health. Wearable and implantable tags could instead facilitate to provide implicit data regarding the presence of a person inside a room, his motion, the interaction among people and body-centric applications, to produce data about the health conditions of prosthesis or artificial organs. Data gathered from this RFID environment, e.g., generated by ambient tags or by the interaction of the user with the house, could be processed by means of data-mining algorithms to evaluate the movements and trajectories of the user, classify gestures during normal and sleep conditions, access critical events and alarm during emergencies. The entire technologic infrastructure, shown in fig. 5, has to be compliant with the electromagnetic safety standards concerning the power absorption in the human body (Specific Absorption Rate-SAR) and the emitted field strength in living environments.

The major issues pertaining to the RFID sensor systems are ascertaining of stability and accuracy of sensor data, data processing cost in the reader electronics, use of implantable electronics without any side-effects, and electromagnetic compliance of the entire system with the EMC standards.

Security requirements of RFID systems in healthcare has been analyzed and studied in [26]. This paper proposes a novel authentication scheme for the RFID in personal healthcare applications. This authentication scheme is based on Elliptic Curve Cryptography (ECC) and satisfies the security requirements. Also, it has low computational complexity and less key size as compared to RSA.

Wireless Sensor Networks (WSNs): The WSNs are another alternative which can be used for deploying the smart healthcare systems. WSNs have been used for healthcare applications like real-time monitoring and emergency-response services.

In the paper [27], a tiered architecture for WSN-based healthcare system has been described. The architecture is represented in Fig. 6. As can be seen from the proposed architecture, it is quite similar to the 3-level IoT architecture demonstrated in section II. Tier-1 is the bottom physical layer with the required wireless medical sensor nodes which forms the diverse WSN. The sensed data is collected and communicated to remote healthcare professionals via wireless infrastructure i.e tier 2 using either Internet, WiMAX, or 3G mobile communication solutions. The tier-2 is responsible for most of the transport and data processing applications. The tier-3, the top-most layer provides the interface for the doctors or nursing staff to monitor the physiological health conditions of the patient and offer the necessary and timely feedback.

The primary issue underlying the implementation of the WSNs for healthcare is the requirement of appropriate standards and protocols. The authors discuss various standards like 802.11n, BT-LE, Zigbee, 802.15.6, 802.16e and 802.22. 802.11n has the largest coverage range and can be used for community healthcare applications, whereas others are suitable for personal healthcare applications.

Recent Research on Standards: In [28], a WSN-based architecture, WSN4QoL, for healthcare applications is presented. This architecture includes another layer, “Middleware Services layer”, to the three-tiered WSN architecture. This layer is between the tier-2 and 3 and consists of three major blocks: (i) Network Coding (NC); (ii) distributed localization; and (iii) security. These blocks utilize the services provided by the underlying protocols to generate a high-level application programming interface (API) to the application developers and the users. The NC entity is responsible for providing efficiency in wireless communications. By appropriate combinations of two or more packets into a single packet and NC-aware routing mechanisms at the physical layer, a relay node can reduce the amount of traffic over the network, without losing any data.

Fig. 6: Three-tiered architecture for WSNs in healthcare

The distributed localization block carries out the online estimation of the geographical position and location of the mobile node in the environment. The relay nodes send their synch packets and thus, they play the role of an anchor or reference node. These relay nodes know their own location and they include this information in the packets. The security block monitors the acknowledgement packets transmitted / received at the network layer among the nodes to identify any potential threats or suspicious nodes and instruct the MAC layer to encrypt frames based on the security and privacy guidelines offered by the IEEE 802.15.4 standard.

The authors of the paper [29] present a novel routing protocol for healthcare applications, the Movement Aided Energy Balance (MAEB) protocol. The first step of MAEB is neighbour discovery. After neighbour discovery, the local coordinators have the movement and energy information so that they can transfer to their nearest reachable coordinators. According to this information, the local coordinator decides most suitable neighbour to forward the data packet. The MAEB forwarding considers the distance and velocity towards Access Gateway, as well as the necessary energy considerations. The simulations for MAEB show performance improvement in latency, energy consumption, packet delivery ratio, and throughput.

Global Healthcare Systems: The recent research is based on the development of a ubiquitous, pervasive and global smart healthcare system.

Integrating Mobile Cloud Computing (MCC) in Healthcare is one of the solutions to build a smart and global healthcare system as explained in [30]. Using the MCC architecture along with the WBAN / WPAN, the healthcare system can take advantage of large-scale computing, storage and software services in a scalable and virtual manner and at a low cost. This architecture will simplify the mobile devices as the major computations and data applications are carried by the cloud based services, like automatic diagnosis and alarm, geographical information system (GIS) services, location-based services, and medical decision making. However, the concept still needs a lot of research to meet the required QoS and security requirements.

Another concept of global healthcare systems is proposed in [31], using Machine-to-Machine (M2M) communication and services, utilizing the IPv6 global addressing schemes. The authors describe the global-coverage M2M healthcare system achievable by using wearable physiological sensors based on the 6LoWPAN protocol. The wearable physiological sensors are intended to sense signals on the patient's body and the M2M nodes and gateway are used to transmit the data to the central server for analysis and supervising through the internet. By combining the 6LoWPAN and IP network using IPv6 addressing scheme, the extreme extension of network and the higher accessibility of M2M node can be accomplished. The 6LoWPAN protocol stack is implemented on top of the IEEE 802.15.4 layer in the M2M nodes in higher-level protocols.

Summary: The surveyed literature in this section describes the IoT for healthcare applications, Smart Healthcare. The technologies associated for building a smart healthcare system are RFID [25] and WSNs [27]. Some additional promising technologies are also surveyed, like the WSN4QoS [28] developed on the WSN architecture for improving efficiency and security, Routing protocol MAEB [29] for improving latency, energy consumption and throughput. Finally, latest developments in the global smart healthcare system are surveyed, i.e. cloud-enabled service (MCC) [30] and the M2M communication with 6LoWPAN [31]. All of these technologies still needs significant research activities to be successfully implemented for the IoT envisioned smart healthcare systems.

3.3 Smart Grid (SG)

With the decline in the non-renewable energy resources, the focus on energy conservation and management has increased significantly. The increase in the IoT potential has led to the research on the integration of Iot and energy grids formulating the concept of smart grids. Future energy grids are characterized by a high number of scattered small and medium sized energy sources and power plants which can be combined virtually adhoc to form virtual power plants. SGs are supposed to spread the intelligence of the energy distribution and control system from the central core to the peripheral nodes in the network, which will enable accurate evaluation of energy losses as well as precise control and adaptation of energy and power distribution.

In the paper [32], the authors describe the web-enabled smart grid system. The key technologies associated with this architecture are small, cheap and resource-constrained devices and the wireless sensor and actuator networks (WSANs) area. The pervasive computing applications available in the WSANs can be effectively utilized for energy control and monitoring. The web-enabled SG should be able to interface with the generally used HTTP-based web services. IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN) for the network layer, Routing over Low-Power and Lossy Networks (ROLL) for the routing of datagrams, Constrained RESTful Environment (CoRE) for the application layer, in addition with W3C's definition for the Efficient XML Interchange specification (EXI), which is currently being finalized to generate a compressed binary representation of the Extensible Markup Language (XML) for constrained devices are all viable technologies explained in this paper. 6LoWPAN is a revised version for the general IPv6 addressing, CoAP supports easy mapping to HTTP, and EXI allows for compressed representation of XML contents. This web-based architecture is based on the deployment of a new kind of web proxy, located at the edge of the constrained network and mapping the constrained protocol stack to the other and vice versa.

In the paper [33], Machine to Machine (M2M) standards for the smart grid applications are presented. The authors describe the Global metering and Home energy management standards with respect to M2M technologies. The ETSI TC M2M standard, DLMS / COSEM, and M-bus are explained for the global metering and IEEE 802.15.4, ZigBee and ISA 100.11a for home energy management. This paper addresses the critical issue of standardizing technologies for global deployment.

The authors of the paper [34] propose a real time energy distribution algorithm for smart grids. The system includes three large domains, Customer, Power Grid Operator (PGO), and Energy Distributor (ED) as shown in fig. 7. The Customer domain signifies the power users including resident, industrial, and others. The PGO performs the duties of the operators, utility providers and managers of electricity. The ED includes the generation, transmission, and distribution of electricity. It generates power to meet local demands and stores excessive power. It also supplies power from outside to local customers when there is not enough local generation and storage.

The Smart meter (SM) in the Customer domain has the tasks of information sharing with the PGO and scheduling of the electrical appliances on the user side. The information transfers are carried using the communications network infrastructure, such as the wireless network or the power line communication system. With the energy and communication connections among the domains, the PGO can exchange information with the Customer and ED and thus it can effectively control the energy operations of the entire area. The Distributed Online Algorithm (DOA) proposed in this paper is presented as a realisable method with a highly effective variance control and peak reduction, for online energy distribution in the smart grid.

In the paper [35], the authors present the applications of communicating power supplies (CPS) wherein the device power supplies can send / receive control and energy management information with the central energy units. This Internet-connected system of CPSs can enable higher energy awareness in devices and users. The CPS concept in this paper demonstrates that this concept is valid at a reasonable price and thus can be used for quite low-cost devices. Energy awareness gives rise to new sets of interactive energy-saving behaviours where devices can control their power usage while minimizing energy consumption.

Summary: In this section, we surveyed literature concerning the smart grid application of the IoT. The SG web-enabled framework is proposed in [32], which can help in establishing the ubiquitous and global smart grid network. Then, we discussed regarding the M2M standards for SG implementation in [33]. A real time energy distribution algorithm in [34] is surveyed and finally the CPS concept in [35] is reviewed. The smart grid application of IoT holds the potential to bring significant change to the energy scenario of the world.

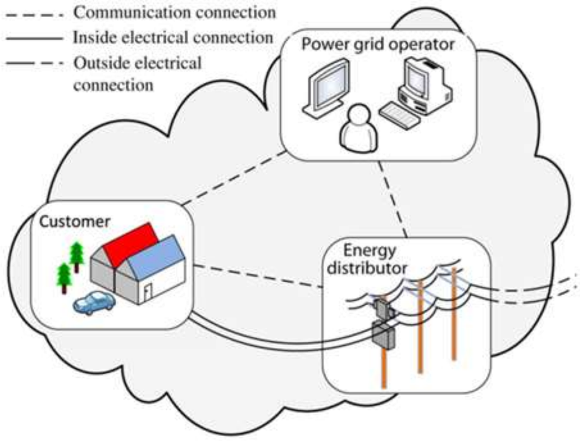

Fig. 7: Smart grid infrastructure with customer, PGO and ED

4. Conclusion

In this paper, we have provided an extensive survey on the available literature on the applications of the Internet of Things, their respective architectures and the associated technologies which are required for their deployment. The major applications of IoT which are believed to change the world are surveyed in this paper. The Internet of Vehicles focuses on enhancing the travelling experience and making it safer. Smart healthcare plans to provide ubiquitous healthcare facilities which can save many lives. Smart grid application of IoT, is the energy-aware initiative, which can offer effective electricity distribution and management solutions for the world. The Future work includes further study of emerging applications of IoT, such as smart cities, Social IoT, Green IoT and others.

References

[1] J. A. Stankovic, “Research Directions For The Internet Of Things”, IEEE Internet of Things, Vol. 1, No. 1, pp. 3-9 Feb. 2014

[2] International Telecommunication Union — ITU-T Y.2060 — (06/2012) — Next Generation Networks — Frameworks and functional architecture models — Overview of the Internet of things

[3] O. Vermesan, P. Friess, P. Guillemin, S. Gusmeroli, et al., “Internet of Things Strategic Research Agenda”, Chapter 2 in Internet of Things—Global Technological and Societal Trends, River Publishers, 2011.

[4] O. Vermesan, P. Friess, “Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems” River Publishers, 2013

[5]C. W. Tsai, C. F. Lai, A. V. Vasilakos, “Future Internet of Things: open issues and challenges”, Wireless Networks, Volume 20, Issue 8 , pp 2201-2217, Nov. 2014

[6] Internet of Things –Architecture, IoT-A Deliverable D1.5 –Final architectural reference model for the IoT v3.0, http://www.iot-a.eu/public/public-documents/d1.5/view

[7] Ning Lu, Nan Cheng, Ning Zhang, Xuemin Shen, and Jon W. Mark, “Connected Vehicles: Solutions and Challenges”, IEEE Internet of Things, Vol. 1, No. 1, pp. 289-299, Aug. 2014

[8] J. Gubbia, R. Buyyab, S. Marusic, M. Palaniswami, “Internet of Things (IoT): A vision, architectural elements, and future directions,” Future Gen. Comp. Sys., Vol. 29, Issue 7, pp. 1645–1660, Sept. 2013

[9] M. Faezipour, M. Nourani, A. Saeed, and S. Addepalli, “Progress and Challenges in Intelligent Vehicle Area Networks”, ACM Commun., Vol. 55, No. 2, pp. 90-100, Feb 2012

[10] H.-M. Tsai et al., “Zigbee-based intra-car wireless sensor networks: A case study,” IEEE Wireless Commun., vol. 14, no. 6, pp. 67–77, Dec. 2007.

[11] M. Hashemi, W. Si, M. Laifenfeld, D. Starobinski, and A. Trachtenberg, “Intra-Car Multihop Wireless Sensor Networking: A Case Study”, Vol. 52, Issue 12, pp. 183-191, IEEE Commun. Magazine, Dec. 2014

[12] K. Chang, C. Consulting, “Wireless communications for vehicular safety”, IEEE Wireless Commun., Vol. 22, Issue 1, pp. 6-7, Feb. 2015

[13] X. Wu et al., “Vehicular communications using DSRC: Challenges, enhancements, and evolution,” IEEE J. Sel. Areas Commun., vol. 31,no. 9, pp. 399–408, Sep. 2013

[14] C. F. Mecklenbrauker et al., “Vehicular channel characterization and its implications for wireless system design and performance,” Proc. IEEE, vol. 99, no. 7, pp. 1189–1212, Jul. 2011.

[15] X. Cheng, et. al., “Wideband Channel Modeling and Intercarrier Interference Cancellation for Vehicle-to-Vehicle Communication Systems,” IEEE J. Sel. Areas Commun. Vol. 31, No. 9, pp. 434-448, Sept 2013

[16] I. Takai, et. al., “Optical Vehicle-to-Vehicle Communication System Using LED Transmitter and Camera Receiver,” IEEE Photonics Jour., Vol. 6, No. 5, Oct. 2014

[17] E. Bozkaya and B. Canberk, “Robust and continuous connectivity maintenance for vehicular dynamic spectrum access networks,” Adhoc Networks, Vol. 25, Part A, pp. 72-83, Feb. 2015

[18] M. H. Cheung, F. Hou, V.W.S. Wong, and J. Huang, “DORA: Dynamic Optimal Random Access for Vehicle-to-Roadside Communications,” IEEE J. Sel. Areas Commun., vol. 30, no.4, pp. 792–803, May, 2012

[19] E. Lee, E.-K. Lee, and M. Gerla, “Vehicular cloud networking: Architecture and design principles,” IEEE Commun. Mag., vol. 52, no. 2, pp. 148–155, Feb. 2014.

[20] K. Mershad and H. Artail, “Finding a STAR in a vehicular cloud,” IEEE Intell. Transport. Syst. Mag., vol. 5, no. 2, pp. 55–68, Apr. 2013.

[21] M. A. Salahuddin, A. Al-Fuqaha, and M. Guizani, “Software-Defined Networking for RSU Clouds in Support of the Internet of Vehicles,” IEEE Internet of Things, Vol. 2, No. 2, pp. 133-144, Apr. 2015

[22] P. Kachroo, N. Shlayan, S. Roy, and M. Zhang, “High-Performance Vehicle Streams: Communication and Control Architecture,” IEEE Trans. Vehi. Tech., Vol. 63, No. 8, pp. 3560 – 3568, Oct 2014

[23] S. Abdelhamid, H. S. Hassanein, and G. Takahara, “Vehicle as a Resource (VaaR),” IEEE Network, Vol 29, Issue 1, pp. 12.17, Jan.-Feb. 2015

[24] N. Kumar, J. J. P. C. Rodrigues, and N. Chilamkurti, “Bayesian Coalition Game as-a-Service for Content Distribution in Internet of Vehicles,” IEEE Internet of Things, Vol. 1, No. 6, pp. 544-555, Dec. 2014

[25] S. Amendola, R. Lodato, S. Manzari, C. Occhiuzzi, and G. Marrocco, “RFID Technology for IoT-Based Personal Healthcare in Smart Spaces,” IEEE Internet of Things, Vol. 1, No. 2, pp. 144-152, Apr. 2014

[26] D. He and S. Zeadally, “An Analysis of RFID Authentication Schemes for Internet of Things in Healthcare Environment Using Elliptic Curve Cryptography,” IEEE Internet of Things, Vol. 2, No. 1, pp. 72-83, Feb. 2015

[27] Y. Zhang, L. Sun, H. Song, and X. Cao, “Ubiquitous WSN for Healthcare: Recent Advances and Future Prospects,” IEEE Internet of Things, Vol. 1, No. 4, pp. 311-318, Aug. 2014

[28] S. Tennina, et. al., “WSN4QoL: A WSN-Oriented Healthcare System Architecture,” Int. Jour. Distri. Sens. Nets. Vol. 2014

[29] H. Su, Z. Wang, and S. An, “ MAEB: Routing Protocol for IoT Healthcare,” Adv. Internet of Things, Vol. 3, pp. 8-15, Jun. 2013

[30] J. Wan, et. al., “Cloud-Enabled Wireless Body Area Networks for Pervasive Healthcare,” IEEE network, Vol. 27, Issue 5, pp. 56-61, Sept.-Oct. 2013

[31] S. Jung and W. Chung, “Non-Intrusive Healthcare System in Global Machine-to-Machine Networks,” IEEE Sens. Jour., Vol. 13, No. 12, pp. 4824-4830, Dec. 2013

[32] N. Bui, A. P. Castellani, P. Casari, and M. Zorzi, “The Internet of Energy A Web-Enabled Smart Grid System,” ,” IEEE network, Vol. 26, Issue 4, pp. 39-45, Jul.-Aug. 2012

[33] Z. Fan, R. J. Haines, and P. Kulkarni, “M2M communications for e-health and smart grid: an industry and standard perspective,” IEEE Wireless commun., Vol.21, Issue 1, pp. 62-69, Feb. 2014

[34] Y. Wang, S. Mao, and R. M. Nelms, “Distributed Online Algorithm for Optimal Real-Time Energy Distribution in the Smart Grid,” IEEE Internet of Things, Vol. 1, No. 1, pp. 70-80, Feb. 2014

[35] S. Lanzisera, A. R. Weber, A. Liao, D. Pajak, and A. K. Meier, “Communicating Power Supplies: Bringing the Internet to the Ubiquitous Energy Gateways of Electronic Devices,” IEEE Internet of Things, Vol. 1, No. 2, pp. 153-160, Apr. 2014