Challenges and solutions for Internet of Things Driven by IPv6

Qazi Emad-ul-Haq[1], Hatim Aboalsamh[1], Abdelfettah Belghith[1], Muhammad Hussain[1], Wadood Abdul[2], Mostafa H. Dahshan[2] and Sanaa Ghouzali[3]

[1] Department of Computer Science, College of Computer and Information Sciences, King Saud University,
Riyadh, Saudi Arabia
[email: emadhaq@gmail.com, emadhaq@student.ksu.edu.sa, {hatem, abelgheth, mhussan}@ksu.edu.sa]
[2] Department of Computer Engineering, College of Computer and Information Sciences, King Saud University,
Riyadh, Saudi Arabia
[email: wadoodwadood@gmail.com, mdahshen@ksu.edu.sa]
[3] Department of Information Technology, College of Computer and Information Sciences, King Saud University,
Riyadh, Saudi Arabia
[email: sanaa.ghouzale@gmail.com]
*Corresponding author: Qazi Emad-ul-Haq

*Received July 8, 2015; revised August 12, 2015; accepted September 3, 2015;
published December 31, 2015*

Abstract

The IPv4 addressing scheme, which was proposed by IETF in 1981, provides 4.3 billion unique 32-bit IP addresses but has been fully exhausted in Feb, 2011. This exhaustion of unique IP addresses poses significant challenges to the addition of new devices to the Internet as well as offering new services. Internet of Things, which provides interconnected uniquely identifiable devices in the existing Internet infrastructure, will be greatly affected by the lack of unique IP addresses. In order to connect to the existing Internet infrastructure, every new device needs a uniquely identified IP address for communication. It has been estimated that by the year 2020 more than 30 billion devices would be connected to the Internet. In order to meet the challenge of such vast requirement of unique IP addresses, the devices in IoT will have to adopt IPv6, which is the latest version of Internet Protocol. IPv6 uses 128-bit IP addresses and offers 2^{128} unique IP addresses. Therefore, it expands IPv4 and provides new features of end to end connections as well as new services. In this paper, the various challenges with respect to providing connectivity, security, mobility, etc., have been discussed and how IPv6 helps in meeting those challenges.

Keywords: Internet of Things, M2M, IPv6, IPSec, Security, Mobility

This research work is supported by the Deanship of Scientific Research, King Saud University and Research Center at the College of Computer and Information Sciences, King Saud University, Riyadh, Saudi Arabia. The authors are grateful for this support.

http://dx.doi.org/10.3837/tiis.2015.12.001 **ISSN : 1976-7277**

1. Introduction

The Internet of Things (IoT), which comprise of uniquely identified interconnected devices in the Internet infrastructure, is an area of deep interest. The number of devices in this web of interconnected devices is increasing many folds. The domain of IoT is not confined only to machine to machine communication, but it is extended over a variety of protocols and applications [1]. IoT comprises smart devices, which have limited resources in terms of memory, storage, processing and energy. These devices contain identification codes and tags, which are used to uniquely identify them globally. As far as smart objects are concerned, there are various technologies that exist, e.g., Bluetooth low energy for wireless PANs, 6LoWPAN [2] for wireless sensor networks and WIFI low power for WLANs, etc [3]. For unique identification of things, the standard technologies include barcodes, used globally for simple identification of common things, matrix barcodes, for detailed identification of things. Radio Frequency Identification (RFIDs), which is used for digital identification of things and Near Field Communication (NFC), which is used to digitally identify things using smart phones and card readers. Other devices that are part of IoT include smart phones, laptops, tablet computers and industrial devices.

The concept of extending the Internet to everything is being materialized by the new version of IP protocol, IPv6, which supersedes the previous IP protocol, IPv4 [1]. The new protocol uses 128-bit addressing. Therefore, it can provide unique IP addresses to every single entity. It is based on the fundamental concept of providing secure data communication to the end users as well as providing mobility to their devices, so that the end users can always be connected. These features of IPv6 made it possible to make the web of interconnected things, i.e., Internet of Things. As such, a lot of research efforts are in progress in order to make some framework that can provide IP address to every single thing, e.g., smart devices and the related technologies, tags which are used for identification and the related legacy technologies, etc. Therefore, an integration of different technology networks can be achieved in this way. A new framework, i.e., GlowBal IPv6, has been proposed [4] for the first type of things, i.e., smart devices using technologies like Bluetooth low energy. For the second type of things, i.e., identification tags and related legacy technologies, IPv6 addressing proxy framework has been proposed [5].

It may be thought that when all the things are uniquely identified using IPv6 addresses then the things are equipped with all IP protocols like IPSec for security and MIPv6 for mobility. However, some of the protocols are not designed for all the things and are resources demanding. Therefore, not all the devices in IoT will be equipped with all the protocols [6,7,8]. Security and mobility management are two important features that will be possessed by the devices in IoT. Mobility management is a must have feature for IoT devices as it enables the devices to stay connected irrespective of their location and infrastructure. Security is another very important feature for IoT devices to have. As the more and more devices are interconnected and due to their intimate relationship with the physical world, for example, financial institutions and energy systems, security and privacy are major challenges to deal with. Another area which has serious implications with respect to security is medical environments, e.g.; security attacks such as Denial of Service (DoS) may hamper the continuous monitoring of patient’s vital signs. Therefore, meeting the challenge of security issues in IoT is of utmost importance.

As security is of major concern already in the current cyber world, there have been many proposed solutions in this respect, which can act as the foundation of the solutions for IoT devices with respect to true identity and privacy. The major challenge is how to make these solutions scalable and robust for billions of interconnected devices in IoT domain. Security is also a building block for another important feature of mobility, e.g.; the data communication may be routed to another entity claiming the identity of the true receiver. It is very important to take care of the security loopholes like man in the middle attack, data integrity, etc. Therefore, security is the fundamental building block of the entire spectrum of IoT domain. In the research community, work has been done on a secure and scalable protocol known as IPSec protocol [9], which is mandatory for IPv6 and used by MIPv6 protocol. MIPv6 ensures secure communication between the home agent and its mobile entity [10]. There are two main challenges, which are posed by IPSec protocols. The first is the cryptosuite which is to be applied. The second is related to the IPSec overhead due to its headers. To meet the first challenge, elliptic curve cryptography which provides asymmetric key cryptography is used. To tackle the issue of IPSec overhead due to its headers, a light-weight IPSec is used. In recent years, IoT has been the focus of research. Extensive research is being done in the areas of healthcare, industrial machines, transport systems and automation, among others.

In this paper, various aspects related to Internet of things are discussed. The rest of this paper is organized as follows: In Section 2, we discuss the importance of Internet of Things. Section 3 addresses the challenges in IoT, Section 4 presents the solutions based on IPv6, Section 5 discusses the future directions and Section 6 presents the conclusion.

2. Why IoT is Important?

These days the devices, sensors and other things are Internet-enabled using gateways, proxies, etc., which do not provide end-to-end connectivity. This type of topology is known as intranet of things instead of Internet of things. This intranet is being extended to the devices by the direct connections to the Internet without using the gateways or proxies. Therefore, these things will be directly connected to the Internet. The things in IoT include but are not limited to heart monitoring implants, automobiles with built-in sensors, bio chips, various sensors, etc. The applications of IoT are in vast areas, such as transport systems, automation, medical and healthcare systems, energy management, industrial applications, infrastructure management, environmental monitoring and large scale deployments. In environment monitoring, various sensors are used to monitor air or water quality, atmosphere, movement of wildlife animals, etc., in order to help in environmental protection. These devices are connected to the Internet and therefore, provide the means to assist in real time environmental monitoring. IoT plays an important role in monitoring and controlling of infrastructures like bridges, railway tracks and airport runways. By monitoring, any structural changes in these infrastructures can be detected very early and; therefore, any hazards or mishaps can be prevented. The Internet of Things showing users and applications is illustrated in **Fig. 1**. This monitoring also helps in making schedules for repairing those infrastructures and helps in coordination among stakeholders.

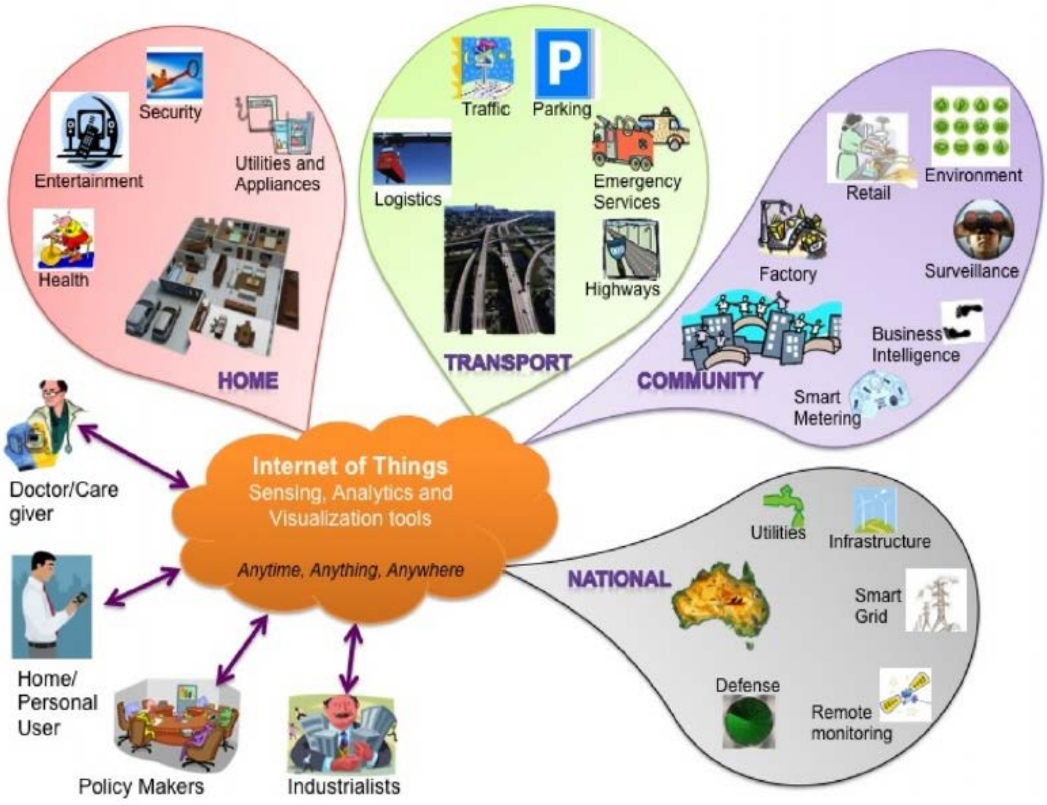

Fig. 1. Internet of Things showing users and applications, [11].

IoT infrastructure can also be used in controlling, e.g., bridges in order to let ships pass. IoT have also been game changer in industrial applications. For example, control and management of industrial processes including manufacturing, situational control and hazard management. Digital control systems, used for equipment safety and security, also come under the umbrella of IoT. In the area of energy management, the Internet connected sensors and actuators have a likely role in the optimizing of energy supply and consumption. In the near future, it is estimated that IoT devices will be an integral part of the electrical devices, such as televisions, air conditioning and heating systems, to communicate to the power generation company about the energy requirements, which will help out in the generation and supply. Users will be able to manage and control the functions of these devices, such as startup and shutdown of air conditioning and heating systems, temperature control, controlling lighting systems, etc.

One of the most important applications of IoT is in the area of healthcare and medical, where these gadgets can be utilized to remotely monitor the medical condition of patients and for automatic notifications in case of emergency. These devices can be attached to the patients and are capable of monitoring their medical conditions, such as blood pressure, heart rate, etc., and communicating back that information to the medical team. These IoT devices are especially useful in monitoring the medical conditions as well as physical location of senior citizens. Another area of IoT application is automation of homes, offices and industrial buildings, by controlling electrical and mechanical systems installed in those buildings. Therefore, lighting, heating and home security systems can be controlled using IoT devices. In the area of transportation systems, IoT devices can be used for the integration of control, communication, and information processing, among a number of transportation systems, and the domain of IoT reaches out to all the entities in the transportation systems, e.g., vehicle, user, infrastructure, etc. The communication between these entities achieves the goals of smart parking, safety, traffic control and road assistance and assistance in case of any mishap.

Nowadays, IoT is in the phase of small as well as large-scale deployments for efficient management of systems [12]. For example, Songdo, South Korea is the first city to become a smart and wired city and it is about to be completed, in which everything will be wired and connected, and the transmitted data would be analyzed automatically by the computers with little or no support from humans. Another IoT deployment project has been going on in Spain in which two methodologies are being used. An application has been developed, which has been downloaded on smart phones by the residents, and this application is connected to more than 10,000 sensors. The application assists the users in car parking across the city, monitoring of environment, etc. Another notable deployment is in New York City by New York Waterways in which all their vessels are connected and monitored at all times. By this way, they are able to control their vessels and passengers very efficiently. Due to all of these applications and their advantages, IoT has been receiving lots of attention lately. The Internet of Things in medical care is shown in **Fig. 2**.

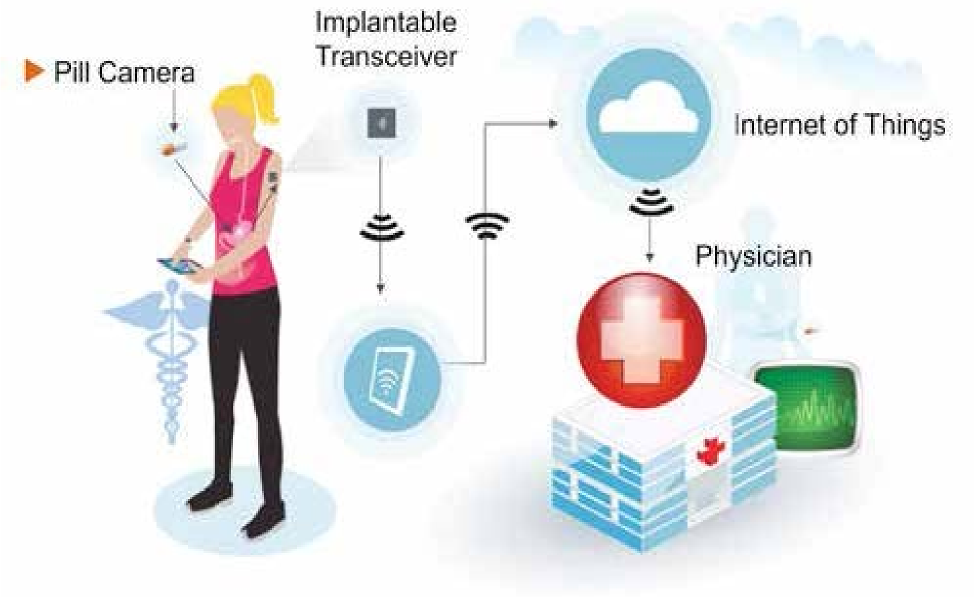

Fig. 2. Internet of Things in medical care, [13].

3. Challenges in IoT

In order to have successful deployment of IoT in practical scenarios, there are a lot of design considerations and criteria that must be met. IoT devices have their inherited constraints in the form of low memory, processing power, energy and storage. Therefore, these constraints must be kept in mind while making designs for IoT deployment. One of the important challenges being faced by IoT is that networks of diverse technologies are integrated in IP environment in order to have a robust communication network. In order to meet this challenge, IoT makes use of reliability of future architecture of the Internet along with IPv6 protocol for vast address space. Another key challenge that is being faced by IoT is to ensure privacy, integrity of data, data security and confidentiality. These important issues must be taken into account when designing the IoT deployment and appropriate mechanisms must be brought into the picture to take care of these issues. These issues pose even greater risks when the resource constrained limitation is taken into consideration.

Mobility is another challenge faced by IoT when it is considered that in near future, Internet will be mobile and ubiquitous [14]. Mobility makes the Internet more applicable in many new areas. The most applicable current trend is the availability of mobile platforms like tablet computers and cell phones, which offers a vast range of services depending on social networking and context awareness. But it is not limited to mobile platforms only. As the world is now a day mobile and moving, therefore, it is of utmost importance for IoT to support mobility to the maximum. Mobility in IoT offers continuous connectivity to the devices without any communication breakdown. For example, mobility is of great importance in hospitals where it can be achieved by the devices connected to wireless networks. Mobility is a great helping hand for the patients as they are free to move around because of the connected portable sensors attached to them, at the same time the fault tolerance is also provided by mobility as the connections to different access points are provided, which can be connected as per need. Therefore, the mobility of IoT devices has direct application in healthcare facilities where fault tolerance ensures that the connections to the patients' portable devices exist at all times and in this way, continuous monitoring can become possible.

Besides these challenges, many other challenges are also being faced by IoT. As the more and more devices get interconnected, more data streams are generated for processing, hence posing a challenge in terms of processing. Another challenge is to provide Quality of Service (QoS) as different applications have different requirements in terms of bandwidth. For example, data streams from health care facilities should have higher preference to data from other general applications. **Fig. 3** shows the significant challenges related to the implementation of Internet of Things. Now these challenges will be discussed in terms of security, mobility, heterogeneity, and connectivity and reliability.

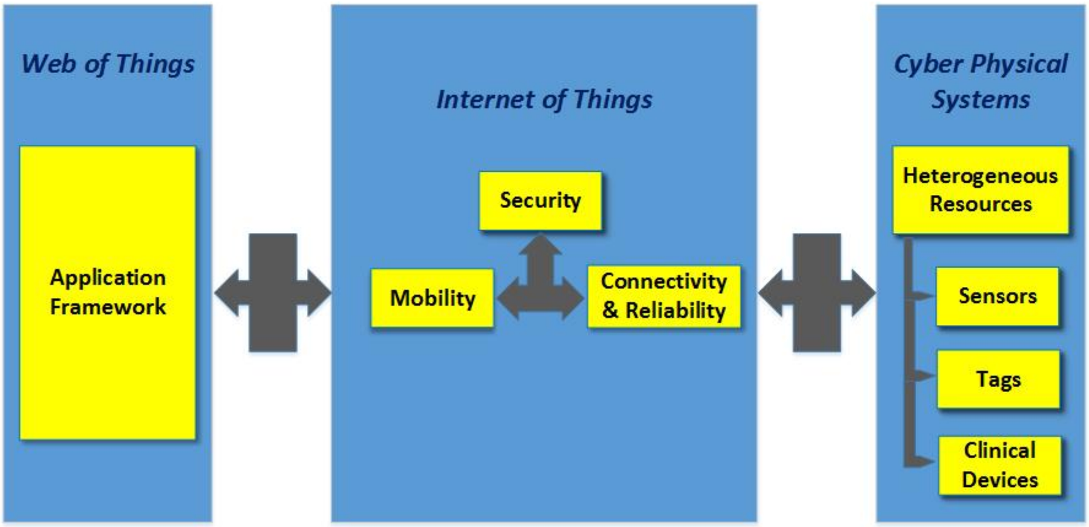

Fig. 3. Challenges faced by IoT.

A. Security

Security is a major challenge in this digital world, and it is a major area of concern in IoT. It has a vast domain that covers (1) authenticity, i.e., to ensure the identity of the end user; (2) authority, i.e., to ensure that the user has the proper rights to perform an activity; (3) integrity, i.e., the received data is in the correct form and has not been tempered with; (4) confidentiality, i.e., data communication should be in the secure form so that even if confidentiality is compromised during communication, it must be incomprehensible. All of these requirements lie in the domain of security and are fulfilled by protocols, algorithms and cryptographic measures [21].

Security for IoT is one of the hottest areas of research and is greatly emphasized because if the security is compromised in any way, then it can lead to unintended consequences. There are existing protocols that provide IPv6 security, i.e., IPSec and DTLS in the case of datagrams but security in the domain of IoT is still not easy to implement as it requires considerable effort for the configuration of IPSec and in the case of DTLS, a certificate management authority is required. As a result, most of the traffic on the Internet goes without any security protocol. The first important step for the deployment of IoT (in order to ensure the security aspects) is to have the protocols developed for key management and authentication. A network layer protocol for authentication and key management like Protocol of Carrying Authentication for Network Access (PANA) is under review in the research community. Furthermore, the IPSec protocols, e.g., Internet Key Exchange (IKE) as well as Encapsulation Protocol (ESP) is also under keen consideration. All of these protocols are based on Extensible Authentication Protocol (EAP) for the transmission of secure information [22].

With respect to IPSec, some of the initial research has been done by the research community for IoT, e.g., a light-weight form of the symmetric cryptography has been proposed, which uses 32-bit keys, which of course is very weak. Moreover, it is dependent on the keys for IPSec which are shared beforehand, and therefore, it suffers by the problem of scalability. To meet these issues, Key Management Protocol (KMP) can be taken into consideration, which has the advantage of periodically refreshing the keys. In addition, an automatic key exchange mechanism is also needed, which enables nodes to keep track of the Security Association (SA) which describes the way in which an IP flow would be security wise handled [23]. A scalable form of KMP is IKE but it lacks the criteria for a SA framework. Another issue with IPSec is the overhead incurred by IPSec packets, which has the impact on the size of the packet and can result in packet fragmentation. Therefore, extra packets would be generated and transmitted. Besides IPSec, work has been done by IETF on using the transport layer security solutions for security integration, e.g., Datagram Transport Layer Security (DTLS). Multiple steps are required to solve the security issues. The first step is to have the cryptographic primitives optimized for the aforementioned protocols. The next step should be to properly analyze how IPSec protocols would affect the resource constrained devices. The last step would be to research on new protocols that can meet the challenges of scalability and self-management.

B. Mobility

Mobility is an important characteristic for IoT to have, so that the smart devices can always be connected irrespective of their location. It poses numerous challenges to the protocols as well as the networks because mobility protocols must tackle the inherent features of IoT, such as hard duty cycles as well as resource constraints. There are two basic phases in mobility management. The first is related to the detection of movement of the device so that it can be known that the device is changing its position and therefore, new communication link is to be established with the other communication networks. Secondly, the signaling as well as control messages must know about the changing locations. The first phase is accomplished by using active scan as well as passive overhearing of other protocols' messages or by using mobility protocol's specific signaling. Solutions to mobility signaling are divided into two categories. Research based on IPv6 using the current Internet infrastructure is placed into the first category. The second category is based on proposing new architectures, which demand changes in the existing protocols. New innovative ideas are the basis of the second category, e.g., split architectures of ID/locator. Such new architectures give rise to mobility by separating session identification from the device locator, which is the prime problem in the current Internet setup. There are disadvantages of this approach as well. The main area of concern is the overhead produced by 6LoWPAN devices because one extra header for the identification layer has to be transmitted. Such disadvantages make such solutions not attractive because the current infrastructure and hardware are not designed for that [24]. For this reason, the other research based approach is followed, which is based on the current Internet infrastructure for the location as well as identification. IPv6 serves the purpose of session identification in the transport and application layers, and device locator in the network layer. Such solutions make use of the existing Internet infrastructure. The main protocol which is used in this approach is MIPv6, which uses two IPv6 addresses, one address is used for identification, and the second is used for device location.

The main issue with MIPv6 is that it increases the overhead with respect to packets when the mobile device is roaming. The other important issue with MIPv6 is that in order to have secure communication between home agent and the mobile device, IPSec is required. Therefore, the ultimate goal with respect to mobility is the need to have new techniques for quick detection of the movement. Second important goal is to design a light MIPv6 implementation in order to have secure as well as efficient IoT mobility.

Simulation

This simulation demonstrates the overhead caused by mobility, i.e., in sending messages, requests, acknowledgement and advertisements by the router. In order to demonstrate MIPv6, four networks are used to create the internet, and each network is composed of four client machines alongwith a router as shown in **Fig. 4.** In the initial step, IP addresses are allocated to the client machines and routers in each of four networks and routing tables are formed in each of the networks. Main events, i.e., movement of a host and request for transmission, are registered into the queue and these main events when processed result in further events into the queue, and this process continues. In order to introduce the randomness and not sticking to a particular pattern of the nodes, the selection of the other networks, i.e., not the original network of the node, the mobile node and the requesting node is performed randomly. Furthermore, the number of packets to be sent are also randomly selected. Different types of delays are calculated like delay of packets between routers of two networks and the delay between a router and nodes of a network and exponential distribution is used for that purpose. After one such transmission is concluded, the mobile node comes back to its original network and the random selection of mobile node, the visiting network and the requesting node is started all over again. In order to analyze the mobility overhead in MIPv6, a number of parameters are used, which include packet delay, i.e., time needed by a packet to reach from one network to another and ratio of encapsulated packets to the number of transmitted packets. The comparison of average packet delay to the encapsulated packets is shown in **Fig. 5.** As it is evident from the figure, the packet delay is directly proportional to the encapsulated packet's percentage, i.e., the percentage of encapsulated packet's increases with the increase in packet time delay and vice versa. The reason is that as the packet time delay decreases, the packets arrive at the home agent in less time, and consequently, the binding updates will arrive at the desired node in less time and therefore, the care of address transmission will start earlier. All of this results in the decreased number of encapsulated packets.

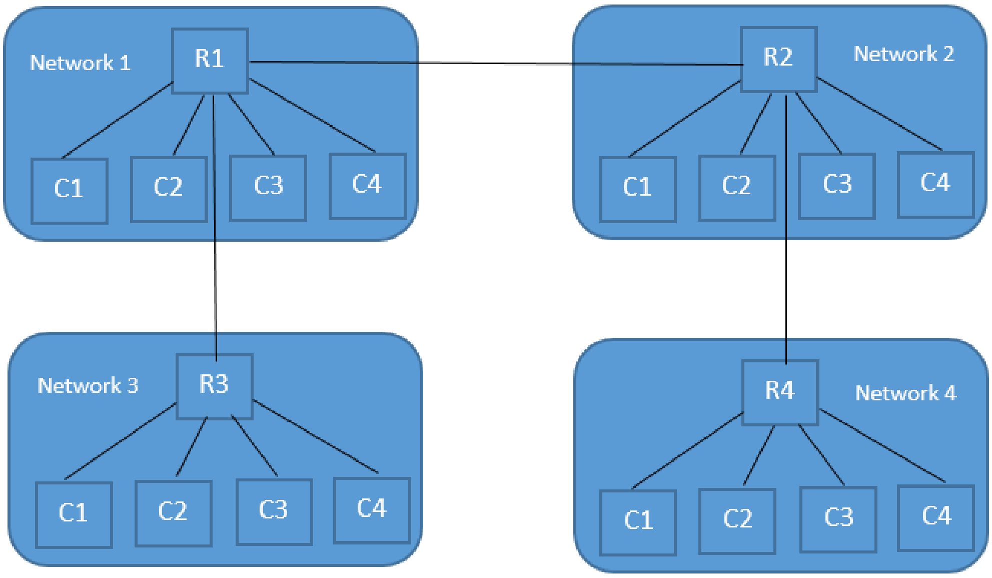

Fig. 4. Internet comprising of four networks

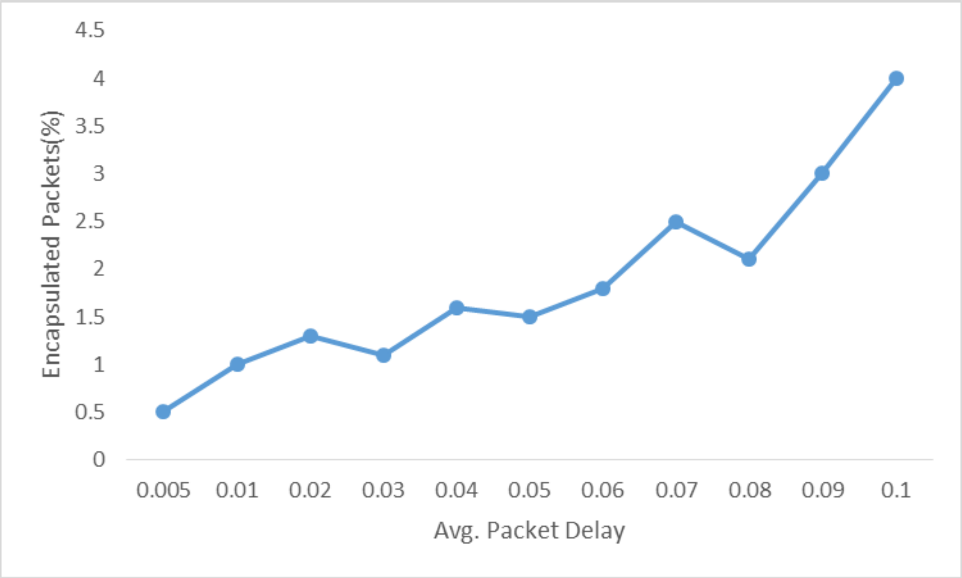

Fig. 5. Comparison of Avg. Packey Delay and Encapsulated Packets

C. Heterogeneity

Radio frequency identification (RFID) was the starting step for IoT as it is used to identify objects globally [15,16]. Lately, it has become technologically feasible that sensors and actuators get connected to IoT. Hence, a new concept of smart objects came into being in IoT which are connected through wireless sensor networks (WSN) by using protocols like 6loWPAN [3]. More and more technologies are getting under the umbrella of IoT, such as Near Field Communication (NFC), WIFI low power and Bluetooth low energy. NFC is a new form of RFID, along with latest devices like tablets, laptops and smart phones [17]. The above-mentioned technologies of RFID, WSN, etc., are not the only technologies in IoT. In addition, IoT encompasses devices, which are altogether different having diverse technologies having capabilities ranging from legacy technologies like X10, konnex, industrial devices having industrial protocols and smart grid technologies [18]. Therefore, it is technology wise very diverse kind of environment, for example; in healthcare facilities, IoT deployments comprise of different devices which range from active and passive types. Active devices include patients' wearable monitors, portable sensors and personal devices like tablets, laptops and smartphones. The passive devices may include drugs and various instruments, which have RFIDs. Hence, as any IoT deployment nowadays comprises of very different types of devices having diverse technologies. Therefore, it is necessary that IoT communication setup must facilitate such heterogeneous requirements and provides means of integration of these diverse gadgets in a common setup.

D. Connectivity and Reliability

The devices which are connected to the Internet are increasing manifolds by each passing day. This phenomenal increase in a number of connected devices is yielding a concept of a new version of the Internet, commonly known as Future Internet. This new form of the Internet is employing the new IPv6 protocol which uses a vast address space and, therefore, is able to uniquely identify a huge number of devices. IoT is based on this new IPv6 protocol and according to an estimate about 30 million devices will be connected to the Internet in 2020 and all this will be possible due to IPv6 protocol [19]. IPv6 provides up to 2^{128} unique IP addresses. IPv6 offers many advantages and is not limited to vast address space, but it offers excellent services of robust, scalable and extendable protocols for end to end connectivity, service and mobility, security, device discovery and group multicast addressing. While designing IPv6, security aspect was taken into keen consideration, and it offers secure communication to the end users and their devices and in this way keeps the users connected all the time.

IoT is based on IPv6 protocol, and it is only due to the services and features offered by the protocol that have made IoT possible. The prime envisioned functionality of IPv6 protocol is to integrate the communications systems that are all around us and by doing so new services can be provided to end users because the systems can get access to other systems to offer connectivity anywhere [20]. At the core of IoT, lies small devices, which are resource constrained in terms of energy, memory, processing, and communication capability. These devices are called smart objects. These resources constrained devices in the past were included in low power wireless personal area networks (LoWPANs). Some serious work has been done by IETF (Internet Engineering Task Force) group by designing IPv6 over LoWPANs, e.g. 6LoWPAN [2] in order to make these smart devices Internet enabled. 6LoWPAN provides all the benefits of IP, such as scalability and end to end connectivity. It may be thought that

6LoWPAN devices have the full capability of IP protocols such as MIPv6 (mobility protocol), SNMP management protocol, IPSec security protocol, etc., but since the smart devices are resource constrained, they do not have the capabilities of these protocols. A smart device may power down and therefore, can cause a problem in the network. The ultimate goal is to meet the challenges of reliable connectivity by adopting IPv6 for all the devices and hence achieving Internet of everything.

4. Solutions Based on IPv6

The challenges described in Section 3 can be met using the solutions based on IPv6. **Fig. 6** exhibits the advancements which provide the solutions to the previously discussed challenges through the integration of IPv6.

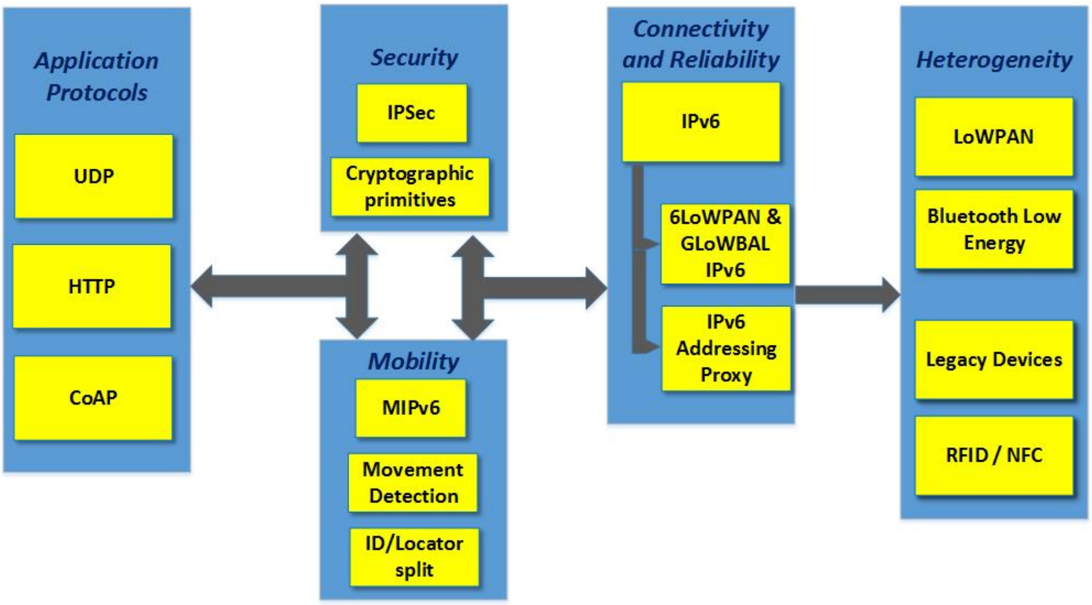

Fig. 6. Solutions for key challenges to Internet of Things.

A. Connectivity and Reliability

The primary aim of the Internet is to provide reliability and connectivity. In order to fulfil this aim, the main emphasis is on IPv6 because it is the driving force to bring together Internet of Things and the future Internet. [25] presents IPv6 architecture to achieve scalable, homogenous medium in order to integrate the devices which are altogether heterogeneous and are made using technologies like 6LoWPAN, Bluetooth low energy and legacy devices. Two solutions have been proposed in the literature to achieve reliability and ubiquitous connectivity. The first, GLoWBAL IPv6 is proposed in [4] and the second which is related to IPv6 addressing proxy is presented in [5].

In GLoWBAL IPv6, optimized global addressing for smart devices is proposed. Such devices are related to LoWPAN. GLoWBAL IPv6 minimizes the overhead related to transport and network headers by defining an access address/identifier (AAID). AAID reduces IPv6 and UDP parameters from 36 bytes to just 4 bytes identifier for communication and 1 byte for dispatch header. In this way, the headers for IPv6 and UDP are reduced. IPv6 addressing proxy [26] proposes a new transparent mechanism, intended for devices and end users, in which different addressing spaces from legacy technologies are translated to the common address space in IPv6. It provides IPv6 addressing to heterogeneous devices irrespective of the technology which is used to build them. Therefore, it proposes a scalable and homogenous solution for the devices that do not have the support of IPv6 addressing.

Let's consider a scenario take an example which describes the connectivity and reliability in a heterogeneous environment. Bring a heterogeneous gadget enabled with Bluetooth technology having the interface with low energy, for example, an advanced mobile phone integrated with the Internet through the interface of a mobile network. By using the addresses of IPv6, GLoWBAL IPv6 meets the IPv6 addressing need for any type of device connected with the advanced mobile phones through Bluetooth technology with Low Energy network by serving as the mapping protocol between the LAN and the WAN. Consequently, this device can perform effectively with IPv6 using GLoWBAL IPv6 to other smart devices by linking its Bluetooth technology using Low Energy interface. At the same time, GLoWBAL IPv6 is not an ideal solution for all gadgets that need to be enabled by IPv6 because all the gadgets are not programmable such as gateways or cell phones. Such gadgets can be found in the inherited old technologies from the building and automation areas. These business sectors display a somewhat divided arrangement of technologies. Every innovation accompanies an arrangement of specific purpose sensors and their particular application situations, which need productive interoperability among them. A few manufacturers have worked together to produce a single framework for different technologies like Konnex (KNX) for building automation. These standards do not demoralize the use of other appropriate protocols, such as, evolving ZigBee and the more established X10. Because of these standards and protocols, a framework for communication and common access dependent on IPv6 is required to deal with this heterogeneous environment. In order to meet this challenge, a solution has been suggested to deal with all existing schemes related to addressing. This solution is based on IPv6 Addressing Proxy which defines the mappings for every native addressing method. This solution performs the conversions among IPv6 addressing and its related technology addressing schemes.

IPv6 Addressing Proxy gives a straightforward system to the clients and gadgets to convert the diverse addressing schemes from different technologies to a common addressing scheme. It maps every gadget to the diverse sub-systems manufactured under the IPv6 addresses provided by the ISP (Internet Service Provider). IPv6 addressing proxy also provides homogeneous and scalable solutions to communicate with different types of devices, which have no support for IPv6 addressing. Therefore, IPv6 addressing proxy implements IPv6 addressing to all kinds of devices irrespective of the technology used by these devices.

B. Mobility and Security

In order to meet the challenges of mobility and scalable security, a communication framework is required. The mobility issue is resolved using IPv6 based Mobile IPv6 protocol (MIPv6). It employs two IPv6 addresses, i.e.; the first address is names as home address and is used as identifier and the second address is in the network which is visited and is called Locator. MIPv6 protocol makes use of signaling messages and IPv6 header extensions to take care of the association between these two addresses. Furthermore, it also gives rise to security mechanisms to tackle the issue of identity impersonation as well as man in the middle attacks.

The suitability of MIPv6 for the resource constrained devices in IoT was first explored in [1]. It was concluded that MIPv6 yields high overhead when the device is roaming. Furthermore, MIPv6 is dependent on IPSec in order to provide the secure and trustworthy relation between the home agent and the mobile node. The security of this communication between these two entities is utmost important and is the important requirement of MIPv6. An issue with IPv6 is the encapsulation of one IPv6 packet inside another. Therefore, it faces the problem of compression and optimization of the inner header. The inner header of 40 bytes cannot be minimized. In keeping view of the above, new research work has been proposed in [27,28] which explores in detail the effect of MIPv6 together with IPSec on 6LoWPAN networks. It is further proposed that in order to have feasible integration of mobility and MIPv6, route optimization has to be eliminated, and IPSec has to be used only for tunneling or encapsulation. This way, the header of the inner packet can be compressed, and the overhead will be reduced. However, there is a disadvantage too that there may be some security loop holes because of insecurity of application layer. To tackle this disadvantage, the work also explores the possibility of using IPSec ESP in order to make the encapsulated packet secure and in turn avoid the security loop holes.

C. Application Protocol

During the previous few years, the researchers in the field of IoT have focused more on the need to enable devices with limited resources by using different protocols and functions of Internet-enabled gadgets. The starting step for this purpose is to develop a light weight version of the current protocols to increase the abilities of IoT gadgets and also to reduce the design issues in IPv6 for different types of technologies. The main advantage of light weight version of application protocols is that they keep being interoperable to the full usage and implementation. For example, the compression of the header of Ipv6 is done through the 6LoWPAN protocol [27] with the goal to achieve connectivity to the Internet.

Moreover, Web Services using the RESTFul framework have also been used for IoT devices by implementing the compact and lightweight version of the protocol, for example, Constrained Application Protocol (CoAP) [8,28], which is equivalent to HTTP. Due to constraint issues of IoT gadgets, CoAP has the ability to be mapped to HTTP and provides a same level of services to the clients. However, in some scenarios, it provides better solutions due to its design and implementation, which cater for IoT demands and constraints. Web services and IPv6 provide the primitives to construct application protocols for various scenarios. The main reason of this development of the communication framework is to ease its usage and exploitation for diverse applications and scenarios. However, this needs the parameters of resources from various applications and scenarios on the top of IPv6/CoAP. Due to this reason, profiles of applications and rules are being defined like Open Mobile Alliance Lightweight Device Management for M2M (OMA LWM2M) [29] in connection to the oneM2M for mobile networks and IPSO application rules [30] for local networks.

5. Future Directions

This section of the paper presents the current and future research work to keep improving the capability of the IoT and its diverse application in mHealth, eHealth and Smart Cities.

A. Interoperable Internet of Things

The main objective of IoT is to offer interconnectivity and join the things to the Internet. When integration is accomplished, we have to adapt to heterogeneity and enable a consistent interoperability among distinct elements. For this reason, the current diverse types of gadgets have been moving towards IPv6. In particular, this coordination at the integration level is accomplished with arrangements like 6LoWPAN [27], and also the important role from IPv6 Addressing Proxies and GLoWBAL IPv6. When the connection is established, a common mechanism / protocol is needed for transport and application layer. The application which is most used on the Internet is WWW (World Wide Web) and resultantly, the information exchange protocol implemented for the Web is Hypertext Transport Protocol (HTTP). The abilities to provide a homogeneous application platform in HTTP have been reduced by the Web Services. Due to this reason, the next phase in IoT would be to link the devices to the Web. The present business sector of IoT is interested to connect the devices vertically. For this purpose, applications and particular sensors have been developed to address specific necessities and focus on a particular application or scenario. On the other hand, IoT needs the integration in the horizontal direction containing resources and numerous abilities moving towards a larger community.

So, IoT is not only defined for communication, but it is also about interoperability and integration. Therefore, semantic is the real driver. The other challenge after the Web of Things, is to construct a Semantic Web of Things (SWoT). The reason is to guarantee which assets would have the capacity to coordinate, connect, can be shared and joined keeping in mind the end goal to construct complex structures. Consequently, the Internet of Things will give increased value of the current and developing markets, which would provide the tremendous capability of everything linked with each other being controllable and exchanging information constantly from all around. Therefore, SWoT can be used to provide wide-scale interoperability that permits the re-utilization of things and sharing. There are several difficulties involved in moving from WoT/IoT towards SWoT. Some of these are to characterize a typical elaboration that permit information to be generally comprehensible by making detailed annotations, i.e. from insignificant semantic depictions towards more comprehensive ones and to accept a list of semantic explanations.

B. Distributed Trust and Security

In future, the work should be carried out for confidence building and trust verification in M2M / IoT by using different mechanisms like capabilities based access control [28,29]. Therefore, novel methodologies can be characterized in the light of temporal access. For instance, a house administrator with an entrance control mechanism like door lock based on intelligent system has the capacity to offer temporal entry to his neighbor for the purpose of irrigation of plants and feeding the pets during the time 15:00 to 18:00 as the owner goes outside for some task. The systems need to offer secure arrangements that make use of IoT abilities amid regular human movements where gadgets and physical assets need to be updated.

Consequently, these new procedures and arrangements will encourage the presentation of IoT as a feature of the Internet-enabled society. For example, the misuse of a regular and disconnected correspondence mediums. In this case, the individual gadget and articles can be connected with the Internet through any correspondence medium, and communication is to be carried out among the devices using end-to-end communication through IP protocol. Accordingly, it is not necessary that the smart device and individual gadget use same mechanism to build up the correspondence. These dispersed security situations are being investigated with different procedures in light of IP abstracted technology and direct connection.

C. Ubiquitous and Mobile Internet of Things

IoT and M2M are being enabled and built from the perspective of cellular and capillary networks. Currently, the light weight IPv6 protocol has been investigated regarding mobile IoT for capillary networks. On the other hand, mobility and ubiquitous link built on several networks for mobile IoT which is dependent on cellular networks. In case of capillary networks, mobile IoT offers major challenges regarding the accessibility of coverage in the large-scale area. Moreover, another challenge is the absence of agreements between different network providers. Consequently, the IoT dependent on cellular networks is getting more attractions as it gives extensive coverage area and homogeneous technology around the world. Specifically, integration of M2M / IoT gadgets is defined by the standard is named as Long Term Evolution-Advanced (LTE-A). The disadvantage of the mobile networks is higher cost, more power consumption and the need of subscription. Due to this reason, the need is arisen to investigate the mobility protocols using vertical handoff between various technologies. This gives the best opportunity regarding the reliability, communication costs and availability.

D. Valuable Internet of Things

The main difficulty for IoT is to exhibit its importance to clients. The capability of the convergence and end-to-end network connection with the Web and the Internet protocols are offering very significant advantages with respect to design and implementation. The main advantages include the cost effectiveness for design and development of flexible solutions because of the re-utilization of existing protocols, significant interoperability due to the same communication mechanisms, control and checking abilities, to construct services based on physical and cybernetic resources and real adaptability. On the other hand, these benefits may not be sufficient from the client's view point with respect of IoT because some of them may not be directly relevant to their interests. The ideal arrangements or applications of IoT are yet to come, which may show the capabilities and capacities of IoT to the customers.

E. Application in Smart Cities, eHealth and mHealth

These smart objects along with sensors that can be coordinated in the smart driver itself offer Smart enormous potential. These sensors can also be considered as the foundation to interface and communicate to any gadget. Consequently, the coordination of the Internet and IoT-related capabilities in a street light could be used to enhance power utilization, streamline the setup and observing of platforms, which leads to major chance to construct a foundation for the remaining gadgets. This foundation can connect to the parking places, peoples' gadgets, autos, picnic spots, and any of the elements that are included in the urban environment. The smart lighting arrangement depicted for smart urban areas offers real saving in power utilization with a significant know how regarding air and acoustical contamination along with specific ultimate ambition to provide the best possible steps for improving continuity of facilities.

One more illustration worth of taking into account is eHealth/mHealth. It provides the interconnection between various distinctive gadgets. These gadgets are available for insulin therapy to the patients of type-1 diabetes for Continuous Glucose Monitoring (CGM) using the insulin pump. These gadgets start to collaborate among each another to communicate the information to the client because of the absence of intelligence in them. IoT enables the CGM and insulin pump to communicate with gadgets, for example, swatch and an advanced mobile phone that can provide insulin treatment based on the health record of the patient. Hence, the triangle between observing, treatment and patient can be implemented in an easier and a smarter way. Consequently, the client stays away from injecting the insulin manually in the insulin pump at different times each day and the insulin injection is kept in check automatically.

The mHealth based arrangements not only provide the treatment to the patients but also personal satisfaction in addition to possible health improvement. In this way, IoT proves its value through enhancement of current solutions, communication models and knowledge sharing. The IoT, therefore, is another empowering factor to enhance personal satisfaction and health.

6. Conclusion

The Internet of things envisions a digital atmosphere where objects in daily life are the Internet enabled and connected at all times, which gives the capability to control them remotely and at will. This concept of Internet of things gives rise to truly ubiquitous computing and therefore, has a huge impact on society in daily life [29,30]. At the same time, Internet of things poses many challenges in terms of security, mobility and due to the fact that the things in IoT are resource constrained devices in terms of energy, memory and processing power. Thus, it is utmost important to meet these challenges. In this paper, the work, which has been done in the research community in order to materialize the envisioned dream of IoT by using IPv6, is presented. In IoT domain, the integration of the different types of objects using diverse technologies, such as Near Field Communication (NFC) and 6LowPAN is critical. In order to achieve this integration in IoT with IPv6 common address space, protocols like GLowBAL IPv6, IPv6 addressing proxy is needed. Along with addressing, IPv6 also offers the features of scalable security and mobility, which are also the foundations of IoT, by using Mobile IPv6 (MIPv6) and IPSec protocols for mobility and security, respectively. Due to the overhead constraints, these protocols need a reduced form of MIPv6 with the support for IPSec. It may be concluded that the vision of IoT has a long way to go before it can connect things and services, but IPv6 integration is an important first phase in achieving that goal.

References

[1] A. J. Jara, R. M. Silva, J. Silva, M. Zamora and A. Skarmeta, "Mobile IPv6 over Wireless Sensor Networks (6LoWPAN) Issues and feasibility," in *Proc. of the 7th European Conference on Wireless Sensor* Networks (EWSN'10), Coimbra, Portugal, February 2010 (ISBN: 978-989-96001-3-3).

[2] G. Kortuem, F. Kawsar, D. Fitton and V. Sundramoorthy, "Smart objects as building blocks for the Internet of things," *IEEE Internet Computing*, vol. 14, no. 1, pp. 44–51, January 2010. Article (CrossRef Link).

[3] A. J. Jara, R. Silva, J. S. Silva, M. A. Zamora and A. F. Skarmeta, "Mobile IP-based Protocol for Wireless Personal Area Networks in Critical Environments," *Wireless Personal Communications*, vol. 61, no. 4, pp. 711–737, 2011. Article (CrossRef Link).

[4] A. J. Jara, M. A. Zamora and A. Skarmeta, "Glowbal IP: An adaptive and transparent IPv6 integration in the Internet of Things," *Mobile Information Systems*, vol. 8, no. 3, pp. 177–197, 2012. Article (CrossRef Link).

[5] A. J. Jara, P. Moreno, A. Skarmeta, S. Varakliotisy and P. Kirstein, "IPv6 addressing proxy: Mapping Native addressing from legacy Technologies and Devices to the Internet of Things (IPv6)," *Sensors*, vol. 13, no. 5, pp. 6687-6712, 2013. Article (CrossRef Link) .

[6] J. Zhang, J. Ma, X. Li and W. Wang, "A Secure and Efficient Remote User Authentication Scheme for Multi-server Environments Using ECC," *KSII Transactions on Internet and Information Systems*, vol. 8, no. 8, pp. 2930 - 2947, ISSN: 1976-7277, August 2014. Article (CrossRef Link).

[7] M. Avula, S. Lee and S. Yoo, "Security Framework for Hybrid Wireless Mesh Protocol in Wireless Mesh Networks," *KSII Transactions on Internet and Information Systems*, vol. 8, no. 6, pp. 1982 - 2004, ISSN: 1976-7277, June 2014. Article (CrossRef Link).

[8] A. J. Jara, M. A. Zamora-Izquierdo and A. F. Skarmeta, "Interconnection Framework for mHealth and Remote Monitoring Based on the Internet of Things," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 47–65, 2013. Article (CrossRef Link).

[9] S. Raza, S. Duquennoy, J. Hoglund, U. Roedig and T. Voigt, "Secure communication for the Internet of Things - a comparison of link-layer security and IPsec for 6LoWPAN," *Security and Communication Networks*, 2012. Article (CrossRef Link).

[10] C. Cao, R. Zhang, M. Zhang and Y. Yang, "IBC-Based Entity Authentication Protocols for Federated Cloud Systems," *KSII Transactions on Internet and Information Systems*, vol. 7, no. 5, pp. 1291 - 1312, ISSN: 1976-7277, May 2013.

[11] J. Gubbi, R. Buyya, S. Marusic and M. Palaniswami, "Internet of Things (IoT): A Vision, Architectural Elements and Future Directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645-1660, September 2013. Article (CrossRef Link).

[12] Wikipedia. [Internet] Available at: http://en.wikipedia.org/wiki/Internet_of_Things,"
[Accessed 11 Dec 2014].

[13] White paper from Arm.com, "What the Internet of Things (IoT) Needs to Become a Reality," *Document Number: INTOTHNGSWP Rev 2*, May 2014.

[14] R. Adelmann, M. Langheinrich, C. Floerkemeier, "A Toolkit for Bar Code Recognition and Resolving on Camera Phones – Jump-Starting the Internet of Things," in *Proc. of Workshop Mobile and Embedded Interactive Systems.* In: C. Hochberger, R. Liskowsky, (eds.) Informatik 2006 – GI Lecture Notes in Informatics (LNI) 94, pp. 366–373, 2006.

[15] K. Ashton, "That 'Internet of Things' Thing," *RFID Journal*, 22 July 2009.
[Internet] Available at: http://www.rfidjournal.com/article/view/4986 [Accessed 18 Dec 2014].

[16] V. Coroama, "The Smart Tachograph – Individual Accounting of Traffic Costs and its Implications," In: K.P Fishkin, B. Schiele, P. Nixon, A.J Quigley, (eds.) *Proc. Pervasive 2006, LNCS 3968, Springer*, pp. 135–152, 2006. Article (CrossRef Link).

[17] S. Duquennoy, G. Grimaud, J. Vandewalle, "Smews: Smart and Mobile Embedded Web Server," in *Proc. of Int. Conf. on Complex, Intelligent and Software Intensive Systems*, pp. 571– 576, 2009. Article (CrossRef Link).

[18] T. Kindberg, J. Barton, J. Morgan, G. Becker, D. Caswell, P. Debaty, G. Gopal, M. Frid, V. Krishnan, H. Morris, J. Schettino, B. Serra, M. Spasojevic, People, Places, “Things: Web Presence for the Real World,” *Mobile Networks and Applications*, vol. 7, no. 5, pp. 365–376, 2002. Article (CrossRef Link).

[19] J. Hui, D. Culler, “IP is Dead, Long Live IP for Wireless Sensor Networks,” in *Proc. of 6th Int. Conf. on Embedded Networked Sensor Systems (SenSys)*, pp. 15–28, 2008. Article (CrossRef Link).

[20] D. Guinard, V. Trifa, E. Wilde, “Architecting a Mashable Open World Wide Web of Things,” *TR CS-663 ETH Zurich*, 2010. Article (CrossRef Link).

[21] C. Frank, P. Bolliger, F. Mattern, W. Kellerer, “The Sensor Internet at Work: Locating Everyday Items Using Mobile Phones,” *Pervasive and Mobile Computing*, vol. 4, no. 3, pp. 421–447, 2008. Article (CrossRef Link).

[22] K. Kollmann, “Internet of Things,” – *Der kurze Weg zur kollektiven Zwangsentmundigung. Telepolis*, 2009. Article (CrossRef Link).

[23] C. Floerkemeier, M. Langheinrich, E. Fleisch, F. Mattern, S.E Sarma, “The Internet of Things,” *First International Conference, IOT 2008, LNCS 4952, Springer*, 2008. Article (CrossRef Link).

[24] C. Floerkemeier, F. Mattern, “Smart Playing Cards – Enhancing the Gaming Experience with RFID,” In: C. Magerkurth, M. Chalmers, S. Bjork, L. Schafer, (eds.) in *Proc. 3rd Int. Workshop on Pervasive Gaming Applications – PerGames*, pp. 27–36, 2006.

[25] A. J. Jara, S. Varakliotis, A. F. Skarmeta, and P. Kirstein, “Extending the Internet of Things to the Future Internet through IPv6 support,” *Mobile Information Systems*, vol. 10, no. 1, pp. 3-17, 2014. Article (CrossRef Link).

[26] A. J. Jara, P. Moreno, A. Skarmeta, S. Varakliotisy and P. Kirstein, “IPv6 addressing Proxy: Mapping native addressing from legacy technologies and devices to the Internet of Things (IPv6),” *Sensors*, vol. 13, no. 5, pp. 6687–6712, May 2013. Article (CrossRef Link).

[27] A. J. Jara, D. Fernandez, P. Lopez, M. A. Zamora, and A. F. Skarmeta, “Lightweight MIPv6 with IPSec support,” *Mobile Information Systems*, vol. 10, no. 1, pp. 37-77, 2014. Article (CrossRef Link).

[28] A. J. Jara, D. Fernandez, P. Lopez, M. A. Zamora and A. F. Skarmeta, “Lightweight mobile ipv6: A mobility protocol for enabling transparent ipv6 mobility in the Internet of things,” in *Proc. of IEEE Global Communications Conference (GLOBECOM)* Atlanta, *2013*. Article (CrossRef Link).

[29] European Commission: “Internet of Things – An action plan for Europe,” *COM(2009) 278*, 2009.

[30] E. Fleisch, “What is the Internet of Things? When Things Add Value,” *Auto-ID Labs White Paper WP-BIZAPP-053*, Auto-ID Lab St. Gallen, Switzerland, 2010.

Qazi Emad ul Haq received his M.S. degree from the National University of Sciences and Technology, Islamabad, Pakistan. He is currently working toward the Ph.D. degree in the Visual Computing Lab, Department of Computer Science, King Saud University, Riyadh, Saudi Arabia. His research interests include networking, pattern recognition, biometrics, watermarking, probability modeling and machine learning.

Hatim A. Aboalsamh is Chairman in the Department of Computer Science, King Saud University, Saudi Arabia. He received his Ph.D. in Computer Engineering & Science in 1987 from University of Miami, USA. Currently, he holds the following Posts:

1. Prof. of Computer Science, Chairman of Computer Science Dept. with 80 publications.
2. Editor-in-chief - Saudi Computer society Journal.
3. Fellow Member- British Computer Society (BCS) Charted IT Institute, and 3 others.
4. Senior Member -Association of Computing Machinery, USA (ACM).
5. Senior Member International Association of Computer Science and Information Technology (IACSIT), Singapore and Professional Member - IEEE.

He held the following leading posts:

1. Vice Rector for Development and Quality-King Saud University (KSA), Riyadh, KSA (2006-2009) and Dean of the college of Computer & Information Sciences.
2. Editor-in-chief, KSU-Journal of Computer Sciences and Vice President of Saudi Computer Society.

Dr. Abdelfettah Belghith received his Master of Science and his PhD degrees in computer science from the University of California at Los Angeles (UCLA) respectively in 1982 and 1987. He is since 1992 a full Professor at the National School of Computer Sciences (ENSI), University of Manouba, Tunisia. He is currently on a sabbatical leave at King Saud University, Saudi Arabia. His research interests include computer networks, wireless networks, multimedia Internet, mobile computing, distributed algorithms, simulation and performance evaluation. He runs several research projects in cooperation with other universities, research laboratories and research institutions. He is the Past chair of the IEEE Tunisia section, the chair of the IEEE ComSoc and VTS Tunisia Chapters, and the Director of the HANA Research Laboratory (www.hanalab.org) at the National School of Computer Sciences. He published more than 300 research papers in international journals and conference proceedings.

Abdul Wadood received his BE degree from COMSATS Institute of Information Technology, Islamabad, Pakistan, in 2004. He did Masters from University of Limoges, France in 2007, and PhD in signal and image processing from University of Poitiers, Poitiers, France in 2011. Currently, he is working as an Assistant Professor at the Department of Computer Engineering, CCIS, King Saud University, Riyadh, Saudi Arabia. His research interests are focused on color image watermarking, networking, steganography, fingerprinting, and biometric template protection.

Muhammad Hussain is a Professor in the Department of Computer Science, King Saud University, Saudi Arabia. He received an M.Sc. and an M. Phil., both from University of the Punjab, Lahore, Pakistan, in 1990 and 1993 respectively. In 2003, He received a Ph.D. in Computer Science from Kyushu University, Fukuoka, Japan. His current research interests include Image and Signal Processing, Pattern Recognition and Computer Graphics. His research has been funded by Japan Science and Technology Agency (JST), and National Science Technology and Innovation Plan (NSTIP) of Saudi Arabia. Dr. Hussain is an Associate Editor of Journal of Computer and Information Sciences, King Saud University and has served on the program committees of various international conferences.

Mostafa H. Dahshan has received his B.Sc. degree in Computer Engineering from Cairo University, Egypt in 1999 and his M.Sc. in Telecommunication Systems and Ph.D. in Electrical and Computer Engineering from the University of Oklahoma, United States in 2002 and 2006, respectively. He is currently an Assistant Professor of Computer Engineering at the College of Computer and Information Sciences, King Saud University, Saudi Arabia. His research interests include network optimization problems, network security and quality of service.

Sanaa Ghouzali received both the Master's and the Ph.D. degrees in computer science and telecommunications from Mohamed V-Agdal University (Rabat, Morocco) in 2004 and 2009, respectively. She was a Fulbright visiting student at Cornell University (Ithaca, NY, USA) between 2005 and 2007. She was an Assistant Professor at ENSA (the National school of Applied Sciences), within the University Abdelmalek Essaadi (Tetuan, Morocco), between 2009 and 2011. In 2012, she joined the College of Computer and Information Sciences at King Saud University (Riyadh, Saudi Arabia) where she is an Assistant Professor in the department of Information Technology. Her research interests include statistical pattern detection and recognition, Biometrics, Biometric Security and Protection.