Internet of Things Architecture: Recent Advances, Taxonomy, Requirements, and Open Challenges

Ibrar Yaqoob, Ejaz Ahmed, Ibrahim Abaker Targio Hashem, Abdelmuttlib Ibrahim Abdalla Ahmed, Abdullah Gani, Muhammad Imran, and Mohsen Guizani

Abstract

Recent years have witnessed tremendous growth in the number of smart devices, wireless technologies, and sensors. In the foreseeable future, it is expected that trillions of devices will be connected to the Internet. Thus, to accommodate such a voluminous number of devices, scalable, flexible, interoperable, energy-efficient, and secure network architectures are required. This article aims to explore IoT architectures. In this context, first, we investigate, highlight, and report premier research advances made in IoT architecture recently. Then we categorize and classify IoT architectures and devise a taxonomy based on important parameters such as applications, enabling technologies, business objectives, architectural requirements, network topologies, and IoT platform architecture types. We identify and outline the key requirements for future IoT architecture. A few prominent case studies on IoT are discovered and presented. Finally, we enumerate and outline future research challenges.

Introduction

In recent years, the Internet of Things (IoT) has emerged as a new computing paradigm, in which a continuum of devices and objects are interconnected with a variety of communication solutions such as Bluetooth, WiFi, ZigBee, and GSM, to name a few. These communication technologies enable connectivity among heterogeneous IoT devices that can help improve the living standard of citizens. It is anticipated that more than 50 billion devices, ranging from smartphones, laptops, sensors, and game consoles, will be connected to the Internet through several heterogeneous access network technologies such as RF identification (RFID) and wireless sensor networks. As identified by [1], IoT can be recognized in three paradigms: Internet-oriented, sensors, and knowledge. Normally, it can be realized that the implementation of IoT technology is very close to modern society, where people and things are integrated virtually to information systems via wireless sensors [2].

The purpose of connecting devices and objects is to serve as the backbone for ubiquitous computing, enabling smart environments to recognize and identify objects and retrieve information [3]. Moreover, ubiquitous technologies like RFID and sensor networks will rise to address these emerging challenges, which center on embedding information and communication systems within our environment. Figure 1 illustrates the architecture of IoT. It also provides a blueprint for data abstraction and the quality of "quadruple" trust, which includes protection, security, privacy, and safety." Furthermore, this standard provides a reference architecture that builds upon the reference model.

Although several studies on IoT [1, 4, 5] have been conducted, none of them is specifically focused on architectural components of IoT. With the aim of exploring IoT network architectures, this study is conducted. Thus, this work is motivated by the need for network architectures, as will be required in the future to accommodate trillions of devices. The contributions of the article are numerous:

- First, we investigate, highlight, and report premier research advances made in IoT architecture recently.
- Then we categorize and classify IoT architectures and devise a taxonomy.
- We identify and outline the key requirements for future IoT architecture.
- A few prominent case studies on IoT are discovered and presented.
- Finally, we enumerate and outline future research challenges.

These contributions are given in separate sections, and the conclusion is then provided.

Motivation

With the rapid adaptation of modern smart technologies, IoT has gained much attention from industry and the IT community in terms of networking and communication aspects. IoT devices depend completely on network connection, which demands high speed, high reliability, and availability. However, existing networking architectures cannot provide smooth connectivity to the voluminous amount of devices, as in the IoT paradigm different types of networks are involved that can cause serious problems. The motivation for new IoT architectures can be seen in [6], which presents how much demand for new network architectures is in the

Ibrar Yaqoob, Ejaz Ahmed, Ibrahim Abaker Targio Hashem, Abdelmuttlib Ibrahim Abdalla Ahmed, and Abdullah Gani are with the Centre for Mobile Cloud Computing Research, Faculty of Computer Science and Information Technology, University of Malaya.

Muhammad Imran is with King Saud University.

Mohsen Guizani is with the University of Idaho.

Digital Object Identifier:
10.1109/MWC.2017.1600421

market, as in the future, the existing architectures will not be fully applicable to provide ideal services.

In the foreseeable future, the number of connected devices to the Internet will be huge in numbers. Cisco predicted that the number of connected devices will rise to 50 billion by the end of 2020.[1] IDC predicted that global spending on the IoT will also rise to US$1.7 trillion by 2020.[2] Telefonica estimated that 90 percent of cars will be connected to the Internet by 2020.[3] Gartner estimated that by 2020, a quarter billion vehicles will be connected to the Internet with the aim of enabling new vehicle services while having the capabilities of automated driving.[4] As the statistics have revealed that the voluminous number of devices will be connected to the Internet, existing network architectures are no longer able to accommodate the IoT devices. Thus, scalable, flexible, interoperable, lightweight, energy-aware, and secure network architectures will be required in the future for IoT. The involvement of heterogeneous devices that have multi-radio capabilities can cause interference problems.The existing networking architectures were only designed to support a limited number of devices.

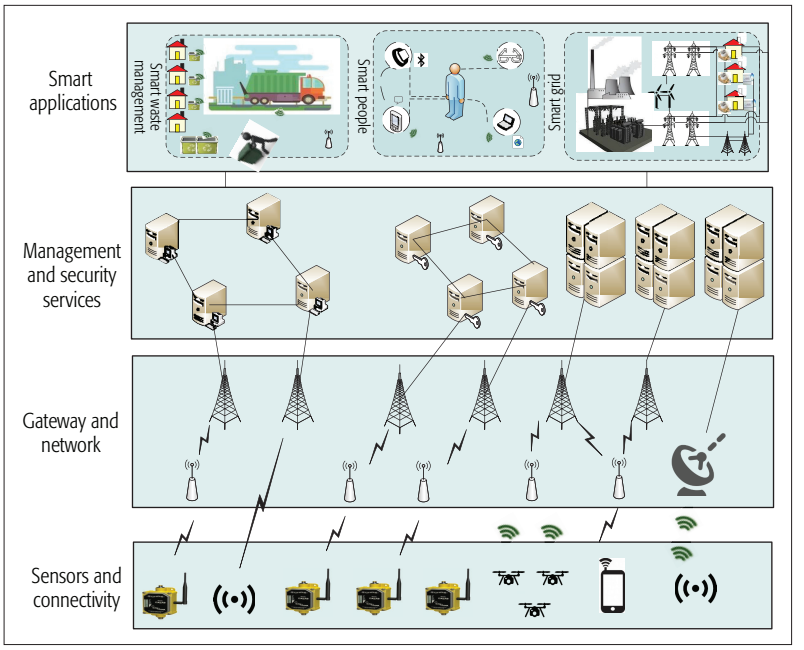

FIGURE 1. Architecture of the Internet of Things.

RECENT RESEARCH EFFORTS

This section reviews recent research efforts directed at IoT network architecture.The aim of the section is to critically investigate the existing solutions.

GENERAL ARCHITECTURE

A generic IoT architecture consists of three layers: application, transport, and sensing. The application layer employs intelligent computing technologies (e.g., data mining, cloud computing) to extract valuable information from processing voluminous data and provides an interface between users and IoT. The transport layer deals with network operations, whereas the sensing layer is responsible for collecting the information. Despite advantages such as easier problem identification and management and flexibility, the lack of application layer security is a prime limitation.

A scalable and self-configuring peer-to-peer-based architecture for a large-scale IoT network has been proposed in [7]. The objective was to provide automated services and resource discovery mechanisms that demand no human intervention for their configuration. The solution is based on local and global service discovery, which allows successful interaction and maintaining mutual independence. The main importance of this solution is that its experiments are conducted on real-world devices, which make the results more trustworthy. However, the possibility of an error occurring is the main factor in needing a more reliable solution in terms of IoT architecture.

SOFTWARE-DEFINED NETWORK-BASED ARCHITECTURE

Z. Qin *et al.* [8] designed a software-defined network (SDN)-based architecture for the IoT with the objective of providing high-level quality of service (QoS) to the different IoT tasks in heterogeneous wireless network environments. Although the proposed architecture provides many benefits — flexibility, effectiveness, and efficient management in terms of flow and task resources — the management of the layer designed by the controller is difficult to manage for heterogeneous IoT multinetworks. On the other hand, several existing studies also reveal that wireless SDN-based architecture can help to meet the objectives of IoT in terms of better QoS, scalability, quick and easy deployment of resources, and context-aware semantic information retrieval.

3G-PLC

A new IoT architecture called 3G-PLC has been proposed in [9]. The architecture combines two sophisticated communication networks: power line communication (PLC) and the third generation (3G) network. The motivation behind using these two networks was the scalability factor. The objective of this work was to integrate the IoT framework layers, such as the perception layer, aggregation layer, network layer, and application layer. Although the proposed architecture offers notable merits such as reduced cost of network construction and improved services compared to backhaul network competitors, the lack of incorporation of network heterogeneity parameters is one of the prime limitations.

MOBILITYFIRST

In [10], the authors showed that by using name-based future Internet architecture (FIA) called MobilityFirst can help address many challenges associated with mobile phones when acting as spontaneous gateways of wireless sensor networks (WSNs) in IoT systems. The capacity of the system is analyzed and compared to the sensor data rate at a given hotspot. Although the proposed work can provide many benefits such as high security and ad hoc services, the lack of incentive mechanisms for mobile contributors to the system is a disadvantage.

CLOUDTHINGS

J. Zhou *et al.* [11] presented an IoT-enabled smart home scenario to analyze the IoT application requirements. In this context, CloudThings architecture has been proposed based on the cloud-based IoT platform. The architecture accommodates CloudThings platform as a service (PaaS), software as a service

[1] http://www.fool.com/investing/general/2016/01/18/internet-of-things-in-2016-6-stats-everyone-should.aspx.

[2] http://www.marketwatch.com/story/internet-of-things-market-to-reach-17-trillion-by-2020-idc-2015-06-02-8103241.

[3] http://telecoms.com/272982/telefonica-90-global-connected-car-penetration-by-2020/

[4] http://www.gartner.com/newsroom/id/2970017

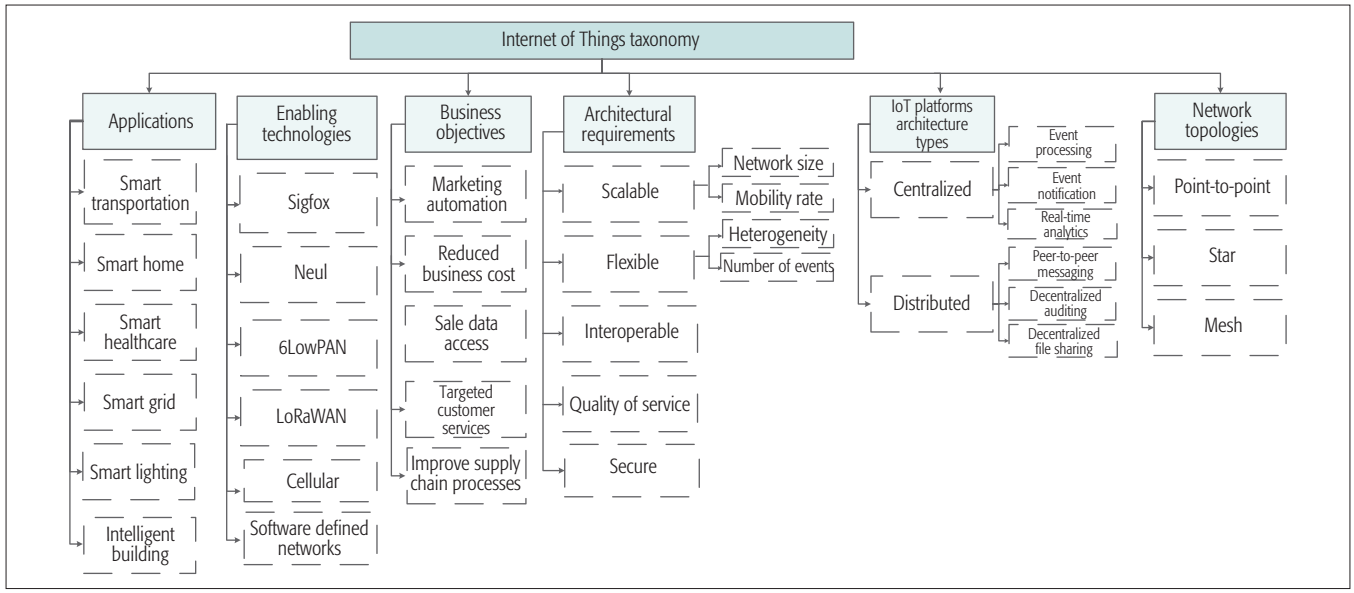

Figure 2. Taxonomy of the Internet of Things.

(SaaS), and infrastructure as a service (IaaS) to accelerate IoT applications. The integration of cloud with IoT offers a viable approach to facilitate application development. The fundamental developments for approaching CloudThings architecture are based on previously running IoT applications and composing new ones. However, the system requires dealing with the heterogeneity of the wireless network communications embedded in the IoT.

Taxonomy

Figure 2 depicts the taxonomy devised based on parameters such as applications, enabling technologies, business objectives, architectural requirements, IoT platform architecture types, and network topologies.

Applications

Some important IoT applications are smart transportation, smart home, smart healthcare, smart grid, smart lighting, and intelligent building, to name a few. These applications facilitate people in different aspects of life. The smart transportation system helps reduce traffic congestion by providing an alternate route. Moreover, the predictive analysis of smart transport data helps minimize road casualties (e.g., accidents). Smart homes allow inhabitants to remotely control appliances. Through smart healthcare applications, diseases can be diagnosed earlier, which leads to saving lives. In a smart grid environment, smart meters are used to measure energy consumption levels, and readings are automatically sent to the grid. Through smart lighting, low-cost sensors and wireless connectivity can be integrated into lamps and luminaries. Intelligent building is another important IoT application where the building is empowered by information and communication technologies (ICT). In short, IoT applications are facilitating people's daily lives.

Enabling Technologies

IoT devices cannot operate without network connectivity. To enable connectivity among heterogeneous smart devices, different networking and communication technologies are used such as Sigfox, Neul, low-power personal area network (6LowPAN), low-range wireless area network (LoRaWAN), cellular, and SDNs. Sigfox is a wide range technology, as its coverage is between those of Wifi and cellular. The objective of Sigfox is to support limited-power devices in terms of data transfer. Neul is a new, weightless wide range wireless networking technology designed to support IoT. 6LowPAN is an IP-based network protocol that defines new encapsulation and header compression mechanisms. It can be used in multiple communications platforms such as Wi-Fi, 802.15.4, and sub-1GHz ISM. LoRaWAN is also designed to target wide area networks. Moreover, it supports low-cost mobile bidirectional communication in IoT by strengthening security. To support the long distance operations of IoT applications, cellular (GSM/3G/4G) communication capabilities are used. It is considered as the most ideal for the sensor-based low-bandwidth-data projects. Software-defined networking is an emerging technology that can help to intelligently route traffic, eliminate bottlenecks, and induce efficiencies to help the data generated by IoT to be processed without placing a larger strain on the network.

Business Objectives

IoT can provide many benefits to businesses. The business objectives of IoT are as follows: marketing automation, reduced cost, sale data access, targeted customer services, and improved supply chain processes. Smart IoT-enabled applications create knowledge about customers in terms of the history of a customer (e.g., buying patterns and preferences). This can allow businesses to find out in real time what the needs of customers are and in the future what products would be more demanded; in this way, marketing automation can be enabled. Through online connectivity, anything can be ordered online that can help save money by reducing traveling costs. As IoT devices generate tremendous amounts of data, by analyzing this data, business people can easily know how, why, and where products are being used and purchased, which can lead toward making the best

strategic plans for companies. Furthermore, customers, services, and supply chain processes can also be improved through analyzing the data generated by the IoT devices of each individual. In short, IoT can help meet many business objectives.

Architectural Requirements

For the existing and emerging IoT applications, it is very well known that they have different architectural requirements such as scalability, flexibility, interoperability, diverse QoS support, and security, to name a few. The term scalable means managing the connectivity among a voluminous amount of network devices without causing any performance degradation issues. Flexible means provisioning services in such a way that a given system can be flexibly programmed to optimize the performance of certain applications. Interoperability helps to enable the interoperations among heterogeneous networks. Moreover, diverse QoS is one of the most important architectural requirements for IoT, as different types of applications such as low data rate monitoring and delay-sensitive real-time applications in the smart grid are involved. The IoT architecture must be intelligent enough to handle the applications according to its requirements. Security is one of the key concerns in IoT because if someone's data is compromised once, it may undermine the user's trust in IoT. Thus, security must be a top priority when designing the architecture for IoT.

IoT Platform Architecture Types

IoT platforms are of two types, centralized and decentralized. Most of the IoT platforms are linked with the cloud architectures where a central hub is used to provide a series of backend services to smart devices. In this type of architecture, smart devices act as consumers while a central hub serves as a centralized node. The key centralized capabilities of the IoT platform are event processing, event notification, and real-time analytics, to name a few. On the other hand, in some scenarios autonomous communication between smart devices is required in the IoT paradigm without the need for a central hub. This type of architecture is a decentralized IoT platform. A few examples of decentralized IoT platforms are peer-to-peer messaging, decentralized auditing, and decentralized file sharing.

Network Topologies

The network topologies used in IoT can be classified into three categories: star, point-to-point, and mesh. In point-to-point network topology a direct connection is established between the nodes; whereas in star networks, all the devices are connected to a central hub. However, in mesh network topology all nodes can be connected to each other. An IoT application developer must consider the six networking attributes while choosing a wireless network: latency, throughput, fault resiliency, scalability, the number of hops, and range. These attributes can help in knowing the capabilities of the three IoT network topologies.

Requirements for Future IoT Architectures

This section outlines the key requirements for future IoT architectures. These requirements are elucidated in Fig. 3 and described next.

Resource Control: The smart devices participating in an IoT environment must be accessible and configurable in a remote manner. In some situations, when the administrators are not available at their particular places, controlling the resources from outside can help resolve the matter. Moreover, IoT systems must be able to balance the load in case of redundant resource availability, which can lead toward appropriate resource utilization.

Energy Awareness: The incorporation of energy awareness in the IoT paradigm, where most of the devices are resource constrained, can help avoid unnecessary energy consumption. In some cases, when the load is not too heavy, devices should put themselves into sleep mode. Moreover, the formation of lightweight communication protocols can help save the energy of smart devices. Thus, the future IoT architecture must be designed in such a way that it can minimize energy consumption.

Quality of Service: One of the requirements of IoT architectures is that they shall be able to provide quality services to users. QoS in IoT can be ensured by prioritizing the services and retrieval. Applications that require real-time processing must be given high priority to improve their performance. Moreover, in response to a query, only the required information should be retrieved. Incorporation of these suggestions in the the future IoT architecture can make it a huge success.

Interoperability: In the IoT paradigm, enabling communication among devices from different vendors is a key requirement [12]. The future IoT architecture must be able to support internetworking and seamless communication between all kinds of applications such as business, desktop, and mobile applications. In addition, to enable the communication between constrained and unconstrained devices of an IoT system, adaptation between networking protocols must be required.

Interference Management: IoT architecture must be able to handle the interference problem. In the future, when trillions of smart devices that have multi-radio capabilities will be connected to the Internet, interference will become a real problem. Therefore, the future IoT architecture must be designed in such a way that it can incorporate radio awareness. Flawless connectivity can only be ensured by addressing the interference problem. In order to achieve reliable services in the IoT environment, interference-free solutions must be developed.

Security: Strengthening security in the IoT environment has become an essential requirement [13]. The future IoT architecture must be secure enough to prevent devices being activated by unauthorized means. In addition, the security mechanisms must be lightweight as most of the devices are resource constrained. Moreover, ensuring the freshness of data is also very important. The lack of strong security support in IoT can undermine the trust of IoT users, which can lead to the failure of the technology.

Case Studies

This section briefly discusses the Microsoft Azure IoT reference architecture and highlights of a few other IoT deployments that enabled the enterprises to meet their business needs. Table 1 provides a summary of the case studies.

Microsoft Azure:[5] Microsoft Azure employs a

The network topologies used in IoT can be classified into three categories: star, point-to-point and mesh. In point-to-point network topology a direct connection is established between the nodes; whereas, in star networks, all the devices are connected to a central hub. However, in mesh network topology every node can be connected to each other.

[5] https://azure.microsoft.com/en-us/documentation/articles/iot-suite-what-is-azure-iot/

The future IoT architecture must be secure enough to prevent the devices being activated by unauthorized means. In addition, the security mechanisms must be lightweight as most of the devices are resource constraint. Moreover, ensuring the freshness of the data is also very important.

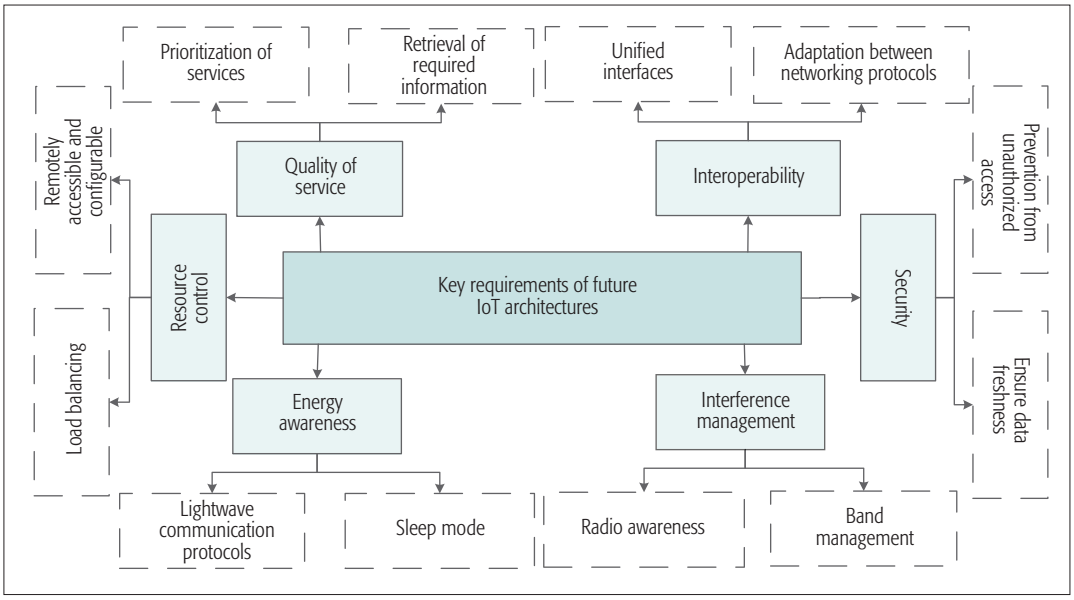

FIGURE 3. Requirement for future IoT architectures.

generic IoT solution architecture that mainly consists of four layers. In this architecture, the data collected by IoT devices is forwarded to a cloud gateway, which makes it available for processing by other back-end services. After processing, data is delivered to other presentation devices or other line-of-business applications. The solution is based on extensible preconfigured architecture that addresses common IoT scenarios such as predictive maintenance and remote monitoring. It was developed with simulated devices such as the Azure IoT Hub, events, streams, and machine learning to offer end-to-end solutions using specific management consoles. The Azure IoT Hub offers a reliable and secure bidirectional communications between devices and the cloud used in the preconfigured solution architecture.

Banco de Cordoba:[6] To train more than 3000 employees in an area that covered over 63,000 square miles with 243 branch locations, Banco de Cordoba implemented an IoT-based video solution. More than 2600 IP video cameras, a new flexible network, and a cyber security system were deployed in the service area. The designed solution was not only single-objective; it also covers many aspects of the enterprise such as security, marketing, and sales messages to customers. Banco de Cordoba claimed that with this new IoT-based system, they got rid of a major issue: sending trainers in a specific field. Moreover, staff were also free of the extra burden, which increased their productivity level in terms of electronic transactions that jumped by a factor of eight. In addition, the deployed system also helped monitor the activities and ensured the security at each location of service.

Daimler:[7] IBM is one of the leading companies that offer implementation assistance to clients, which has a huge impact in terms of increasing operational efficiency, revolutionizing business models, improving industry operations, and recasting their customers' experience. Although Daimler has faced challenges in terms of dealing with some of the internal operations using IoT technologies, these later became familiar to the system. The company uses IBM services to launch car2go, an on-demand fleet of eco-friendly smart cars that users can reserve from the mobile application. Using IoT architecture that encompasses sensors and wireless communication allows the company to monitor the vehicle performance, and provide an accessible network of vehicle and analysis data to increase the efficiency of the car.

Lukoil:[8] In Russia, the Timan-Pechora basin is home to the Varandey oil terminal. But it is located at that place where the temperature is as low as −47 degrees Fahrenheit. The owner of the facility, Lukoil, wanted to increase the production of oil. Moreover, the owner wanted to export to some other countries. To achieve this goal, Lukoil deployed IoT-based architecture called Emerson PlantWeb and employed DeltaV digital automation. The IoT-based solution helped them to protect the facility and improved the safety.

Open Research Challenges

The section discusses the challenges remaining to be addressed for accommodating the trillion of IoT devices. The purpose of the section is to provide the research directions for the new researcher in the domain.

Interoperability: IoT has three main types of interoperability challenges, namely technical, semantic, and pragmatic. The technical challenges have a concern with device capabilities, protocols, and relevant standards to coexist and interoperate in the same computing paradigm, whereas semantic have a concern with the capabilities of various IoT components that are responsible for processing and interpreting the exchanged data. However, pragmatic have a concern with the capabilities of the system components to observe the parties intentions. Achievement of technical interoperability can be gained by offering agent-based mediation between IoT devices and standards. Semantic interoperability is a requirement to the machine computable logic, knowledge discovery, and data federation between information systems. Pragmatic interoperability can be achieved through the creative design of predefined specifications of the

[6] http://www.networkworld.com/article/2848714/cisco-subnet/10-enterprise-internet-of-things-deployments-with-actual-results.html

[7] http://www.cbronline.com/news/internet-of-things/m2m/daimler-gets-iot-smart-by-linking-cars-to-enterprise-systems-4713572

[8] http://www.emerson.com/neverbeendone/en-us/Pages/LUKOIL.aspx

Case study	Business needs	Companies involved	Assessment	IoT-based architecture	Country
Lukoil	Process automation of oil facility	Emerson	Success	✓	Russia
Banco de Cordoba	Video collaboration and protection project	Groupo Galmes, Cisco	Success	✓	Argentina
Daimler	Driving enterprise transformation	IBM	Success	✓	Germany
Microsoft Azure	To address the common IoT scenarios such as predictive maintenance and remote monitoring	Microsoft	Success	✓	USA

TABLE 1. Summary of the case studies.

components,Äô behavior. In the future, cross-layer interoperability solutions are required.

Scalability: IoT are expected to face many challenges related to the potential unbounded number of interacting entities and substantial differences in the interaction patterns and behaviors. The existing IoT architectures need to be scaled up to accommodate the trillion of smart devices. IoT systems scalability management can be summarized into two points. First, the rapid growth has been witnessed in the IoT devices. However, current management protocols do not scale well to accommodate the requirements of IoT devices due to their limited capabilities. Second, social relationships between the owners of the devices need to be considered, where some of IoT system entities are human portable devices. In the future, scalability management protocols are expected to track social relationships between devices in order to enable ad hoc based computing services by providing some incentives.

Flexibility: Since there are numerous applications of IoT, service provisioning to the different IoT applications according to their demands has become very challenging. IoT users usually need dynamically configured, customized, value-added, and autonomous on-the-move services. Moreover, personalized, customized, autonomous, and dynamic services can be supported by constructing and utilizing the adaptive, context-aware, and reconfigurable multiple service network architecture. In the future, models of service declarative specifications are required for the construction of future network service architectures.

Energy Efficiency: Tiny devices are the backbone of IoT. However, these devices have limited processing capabilities, memory, and battery power. Consequently, compute-intensive applications and routing processes cannot run on IoT devices, as these devices are very lightweight. Consideration of energy awareness in routing protocols is still lacking. Although some protocol supports low-power communication, these protocols are in an early stage of development. In the future, energy harvesting techniques can be promising solutions to fulfill the energy requirements in IoT.

Mobility Management: Node mobility can create various challenges in terms of IoT network and protocol efficiency. The current mobility protocols of vehicular ad hoc networks (VANETs), mobile ad hoc networks (MANETs), and sensor networks cannot deal well with typical IoT devices due to severe energy and processing constraints. Mobility management is a crucial task, and has two stages. First, movement detection is needed in order to be aware of the device movement, which requires linking to a new region of a network. Second, the signaling and control messages require to be incorporated in such a way that it can help in knowing nodes' locations in a network. Movement detection can be achieved through frequent scans, via either passive messages from participating protocols or a beacon from the mobility protocol. Mobility management is one of the key issues in the IoT paradigm. Consequently, it must be considered in the future IoT architecture.

Security: The diversity of IoT applications and heterogeneity of IoT communication infrastructures results in an equally numerous variety of security challenges [14, 15]. In IoT, security can be provided in bottom-up fashion. In a bottom-up way, the system must follow a secure booting process, access control rules, device authentication procedures, and firewalling, and must be able to accept updates and patches of security software in a non-disruptive way. Since the security is a key concern in IoT, suitable security mechanisms must be applied at both the device and network levels (physically and non-physically). IoT devices must have some sort of intelligence to recognize and counteract potential threats. Fortunately, this does not require a revolutionary approach; rather, an evolution of measures that have proven successful in other networks must be adapted in the IoT paradigm by considering the processing capabilities of smart devices.

CONCLUSION

With the rapid rate of increase in smart devices, the need for future IoT network architecture has arisen. The existing network architectures cannot accommodate the voluminous number of smart devices expected in the future. With the focus on the IoT architectures, we have conducted this study. First, we have investigated, highlighted, and reported premier research advances made in IoT architecture recently. Then we have categorized and classified IoT architectures and devised a taxonomy. The key requirements for future IoT architecture have been identified and outlined. A few credible case studies have also been presented. Furthermore, several open research challenges have been discussed as future research directions. Finally, we conclude that in the foreseeable future, scalable, flexible, energy-efficient, interoperable, and secure network architectures will be required, as the existing ones can only support a limited number of devices.

ACKNOWLEDGMENTS

This work is funded by the Bright Sparks Program and the Research Grant from the University of Malaya under references BSP/APP/1689/2013,

Tiny devices are the backbone of IoT. However, these devices have limited processing capabilities, memory and battery power. Consequently, compute-intensive applications and routing processes cannot run on IoT devices, as these devices are very lightweight.

IoT devices must have some sort of intelligence to recognize and counteract against the potential threats. Fortunately, this does not require a revolutionary approach; rather an evolution of measures that have proven successful in other networks must be adapted in the IoT paradigm by considering the processing capabilities of smart devices.

RP012C-13AFR, and UM.C/625/1/HIR/MOE/FCSIT/03. Imran's work is supported by the Deanship of Scientific Research at King Saud University through Research Group No. RG # 1435-051.

References

[1] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A Survey," *Computer Networks*, vol. 54, no. 15, 2010, pp. 2787–2805.
[2] C.-W. Tsai, C.-F. Lai, and A. V. Vasilakos, "Future Internet of Things: Open Issues and Challenges," *Wireless Networks*, vol. 20, no. 8, 2014, pp. 2201–17.
[3] J. A. Guerrero-ibanez, S. Zeadally, and J. Contreras-Castillo, "Integration Challenges of Intelligent Transportation Systems with Connected Vehicle, Cloud Computing, and Internet of Things Technologies," *IEEE Wireless Commun.*, vol. 22, no. 6, Dec. 2015, pp. 122–28.
[4] A. Al-Fuqaha *et al.*, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," *IEEE Commun. Surveys & Tutorials*, vol. 17, no. 4, 2015, pp. 2347–76.
[5] C. Perera *et al.*, "Context Aware Computing for the Internet of Things: A Survey," *IEEE Commun. Surveys & Tutorials*, vol. 16, no. 1, 2014, pp. 414–54.
[6] J. Gubbi *et al.*, "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions," *Future Generation Computer Systems*, vol. 29, no. 7, 2013, pp. 1645–60.
[7] S. Cirani *et al.*, "A Scalable and Self-Configuring Architecture for Service Discovery in the Internet of Things," *IEEE Internet of Things J.*, vol. 1, no. 5, 2014, pp. 508–21.
[8] Z. Qin *et al.*, "A Software Defined Networking Architecture for the Internet-of-Things," *2014 IEEE Network Operations and Management Symp.*, May 2014, pp. 1–9.
[9] H.-C. Hsieh and C.-H. Lai, "Internet of Things Architecture Based on Integrated PLC and 3G Communication Networks," *2011 IEEE 17th Int'l. Conf. Parallel and Distrib. Systems,* 2011, pp. 853–56.
[10] J. Li *et al.*, "A Mobile Phone Based WSN Infrastructure for iot Over Future Internet Architecture," *Green Computing and Commun., 2013 IEEE and Internet of Things*, and *IEEE Int'l. Conf. Cyber, Physical and Social Computing*, 2013, pp. 426–33.
[11] J. Zhou *et al.*, "Cloudthings: A Common Architecture for Integrating the Internet of Things with Cloud Computing," *2013 IEEE 17th Int'l. Conf. Computer Supported Cooperative Work in Design*, 2013, pp. 651–657.
[12] J. Kim *et al.*, "Standard-Based IoT Platforms Interworking: Implementation, Experiences, and Lessons Learned," *IEEE Commun. Mag.*, vol. 54, no. 7, July 2016, pp. 48–54.
[13] J. L. Hernandez-Ramos, J. B. Bernabe, and A. Skarmeta, "Army: Architecture for a Secure and Privacy-Aware Life Cycle of Smart Objects in the Internet of My Things," *IEEE Commun. Mag.*, vol. 54, no. 9, Sept. 2016, pp. 28–35.
[14] X. Du and H.-H. Chen, "Security in Wireless Sensor Networks," *IEEE Wireless Commun.*, vol. 15, no. 4, 2008, pp. 60–66.
[15] X. Du *et al.*, "Defending DOS Attacks on Broadcast Authentication in Wireless Sensor Networks," *IEEE ICC*, 2008, pp. 1653–57.

Biographies

Ibrar Yaqoob (ibraryaqoob@siswa.um.edu.my) received his B.S. (Hons.) degree in information technology from the University of the Punjab, Gujranwala campus, Pakistan, in 2012. Currently, he has been pursuing his Ph.D. degree in computer science at the University of Malaya, Malaysia, since November 2013. He won a scholarship for his Ph.D. and also works as a Bright Spark Program research assistant. He has published a number of research articles in refereed international journals and magazines . His numerous research articles are very famous and among the most downloaded in top journals. His research interests include big data, mobile cloud, the Internet of Things, cloud computing, and wireless networks.

Ejaz Ahmed [S'13] (ejazahmed@ieee.org) is a senior researcher in the High Impact Research project at Centre for Mobile Cloud Computing Research (C4MCCR), University of Malaya. Before that, he worked as a research associate in the Cognitive Radio Network (CogNet) Research Lab SEECS, NUST Islamabad from December 2009 to September 2012, and in Center of Research in Networks and Telecom (CoReNet), MAJU, Islamabad, from January 2008 to December 2009. His research experience spans over more than nine years. He is an Associate Editor of *IEEE Communication Magazine*, *IEEE Access*, and *Wiley Wireless Communications and Mobile Computing*. He has also served as a Lead Guest Editor/Guest Editor of *Elsevier Future Generation Computer Systems*, *Elsevier Computers & Electrical Engineering*, *IEEE Communications Magazine*, *IEEE Access*, *Elsevier Information Systems*, and *Wiley Transactions on Emerging Telecommunications Technologies*. His areas of interest include mobile cloud computing, mobile edge computing, the Internet of Things, cognitive radio networks, and smart cities. He has successfully published his research work in more than 30 international journals and conferences.

Ibrahim Abaker Targio Hashem (targio@siswa.um.edu.my) is currently a Ph.D. degree candidate in the Department of Computer Systems and Technology, University of Malaya. He received his M.S. degree in computing in 2012 at the same university and his B.E. degree in computer science in 2007, Sudan. He obtained professional certificates from Cisco (CCNP, CCNA, and CCNA Security) and the APMG Group (PRINCE2 Foundation, ITIL v3 Foundation, and OBASHI Foundation). He worked as a tutor at Cisco Academy, University of Malaya. His main research interests include big data, cloud computing, distributed computing, and networking.

Abdelmuttlib Ibrahim Abdalla Ahmed (abdelmuttlib@siswa.um.edu.my) received his B.Sc. degree in computer science from OIU, Sudan, and his M.S. degree in computer science from IIUI, Pakistan. He is currently pursuing a Ph.D. degree at the University of Malaya. His research Interest areas include trust and reputation systems, security and digital forensics, Internet of Things, mobile and cloud computing, and vehicular networks.

Abdullah Gani [M'01, SM'12] (abdullahgani@ieee.org) is a full professor in the Department of Computer System and Technology, University of Malaya. He received hiis Bachelor's and Master's degrees from the University of Hull, United Kingdom, and his Ph.D from the University of Sheffield, United Kingdom. He has vast teaching experience due to having worked in various educational institutions locally and abroad: schools, teaching college, the Ministry of Education, and universities. His interest in research started in 1983, when he was chosen to attend a Scientific Research course in RECSAM by the Ministry of Education, Malaysia. More than 150 academic papers have been published in conferences and respectable journals. He actively supervises many students at all levels of study — Bachelor, Master, and Ph.D.. His research interests include self-organized systems, reinforcement learning, and wireless-related networks. He worked on mobile cloud computing with a High Impact Research Grant for the period of 2011–2016.

Muhammad Imran (cimran@ksu.edu.sa) is an assistant professor in the College of Computer and Information Science, King Saud University. His research interests include mobile ad hoc and sensor networks, WBANs, IoT, M2M, multihop wireless networks, and fault-tolerant computing. He has published a number of research papers in peer reviewed international journals and conferences. His research is financially supported by several grants. He is serving as a Co-Editor-in-Chief for *EAI Transactions on Pervasive Health and Technology*. He also serves as an Associate Editor for the *Wireless Communication and Mobile Computing Journal* (Wiley), the *Inderscience International Journal of Autonomous and Adaptive Communications Systems*, *Wireless Sensor Systems* (IET), and the *International Journal of Information Technology and Electrical Engineering*. He has served/serves as a Guest Editor for *IEEE Communications Magazine*, *IJAACS*, and the *International Journal of Distributed Sensor Networks*. He has been involved in a number of conferences and workshops in various capacities such as a Program Co-Chair, Track Chair/Co-Chair, and Technical Program Committee member. These include IEEE GLOBECOM, ICC, AINA, LCN, IWCMC, IFIP WWIC, and BWCCA. He has received a number of awards such as an Asia Pacific Advanced Network fellowship.

Mohsen Guizani [S'85, M'89, SM'99, F'09] (mguizani@ieee.org) received all of his degrees from Syracuse University, New York, in 1984, 1986, 1987, and 1990, respectively. He is currently a professor and the Electrical and Communications Engineering Department Chair at the University of Idaho. He has served in a number of academic positions in the United States. His research interests include wireless communications, mobile computing, computer networks, cloud computing, IoT, security, and smart grid. He currently serves on the Editorial Boards of several international technical journals, and is the founder and Editor-in-Chief of *Wireless Communications and Mobile Computing* (Wiley). He is the author of nine books and more than 400 publications in refereed journals and conferences. He has been a Guest Editor of a number of Special Issues in IEEE journals and magazines. He has also served as a TPC member, Chair, and General Chair of a number of international conferences. He was selected as the Best Teaching Assistant for two consecutive years at Syracuse University. He was the Chair of the IEEE Communications Society Wireless Technical Committee and the TAOS Technical Committee. He served as an IEEE Computer Society Distinguished Speaker from 2003 to 2005. He is a Senior Member of ACM.