Overview of the Internet of Things (IoT)

Nadir Abdelrahman Ahmed Farah
Information Systems
University of Bisha
Alnamas, Saudi Arabia
Email: nadiraaf [AT] hotmail.com

Abstract— **One of the modern topics in the Information Technology is the Internet of Things (IoT). The future is for Internet of Things, which will convert the real world objects into intelligent virtual objects . it defined as a technological development which provides the visibility of connected world of Things. The internet of things deals with Devices, people , systems, and other systems connected to it. Also it includes computers, smart phones and tablets which collect and exchange data with one another's over Internet. All these items are linked to the wired and wireless network to mutually create, collect, share, and use the information. All the things which are connected may generate data. The data sometimes may be used immediately and in some cases has to be processed and stored for future use. So, the compose of communication from human-human is now become, human-things and things- things. Variety of platforms are nowadays available that can support the whole development to deployment of IoT applications and systems. the paper aims to provide a comprehensive overview of the IoT. The paper start with the introduction of IoT then discuss its vision, its Characteristics, Architecture, Requirements, various platforms, Internet of Things middleware, integration of internet of things and cloud computing, various communications models, Smart home, Smart cites, social and ethical behavior, internet of things malware, various challenges, and costs of internet of things.**

Keywords- ***internet of things, platform, Middleware, RFID, Smart Cities***

Introduction

The internet of things is the most hyped concept in the IT field.

The term "Internet of Things" (IoT) was first used in 1999 by the pioneer British technologist , Kevin Ashton to describe a system in which objects in the physical world could be connected to the Internet by sensors[2].

Internet of Things is a new technology of connecting "everything" that can hold minimum memory for storage and requires very less computational power through internet so that the connected things can communicate anytime, and anywhere across world by analyzing the basic concepts of IoT. It provides services for societies, communities, governments, and individuals. It invite to a new concept of communication which expand the existent interactions between humans and computer applications to things. Things are objects of the physical world referred to as physical things, or the information world referred to as virtual things.

The Internet of Things mainly works with two components. First, is the nodes and the other is data aggregator (any device which is capable of collecting and storing data). Node is any communicating device which is present in the network. All the things or resources connected may create data or use it to be processed and stored for further computations. Whenever the data is required to be stored, data aggregator can be used.

Internet of thing is like a visibility which every object on a network can uniquely be determined, its status and position can be known, it is accessible to the network and also services and intelligence are added to network.

A number of modern techniques (such as intelligent sensors, wireless communication, networks, data analysis , cloud computing, etc.) have been developed to fulfill the potential of the IoT with different intelligent systems [1].

I. CONCEPTS AND COVERAGE OF THE INTERNET OF THINGS

1.1 IoT vision

The vision of Future Internet based on standard communication protocols meditate the combine of computer networks, Internet of Media (IoM), Internet of Services (IoS), and the Internet of Things (IoT) into a joint global IT platform of seamless networks and networked "things". IoS is an indicate to a software-based component that will be transfer via different networks and Internet. [4].

1.2 Characteristics of IoT

A. Interconnectivity: as to the IoT, anything can be interconnected with the worldwide data and correspondence messages.

B. Things-related services: The IoT is suitable for giving thing related administrations inside the imperatives of things, for example, security assurance and semantic consistency between essential tools and their related virtual things.
C. Heterogeneity: The instrument inside the IoT are heterogeneous as in view of various equipment stages and systems. They can connect with different instrument or administration stages through various systems.
D. Dynamic changes: The condition of instrument change gradually, e.g., set at rest and awakening, associated and additionally separated and also the setting of instrument including area and speed. Additionally, the quantity of instrument can change powerfully.
E. Enormous scale: The quantity of instrument that should be supervised and that speak through every one extra will be no less than a request of enormity bigger than the devices associated with the current Internet [5].

1.3 Architecture of IoT

IoT considers six layers design. Figure(1), The six layers of IoT are described below [5]:

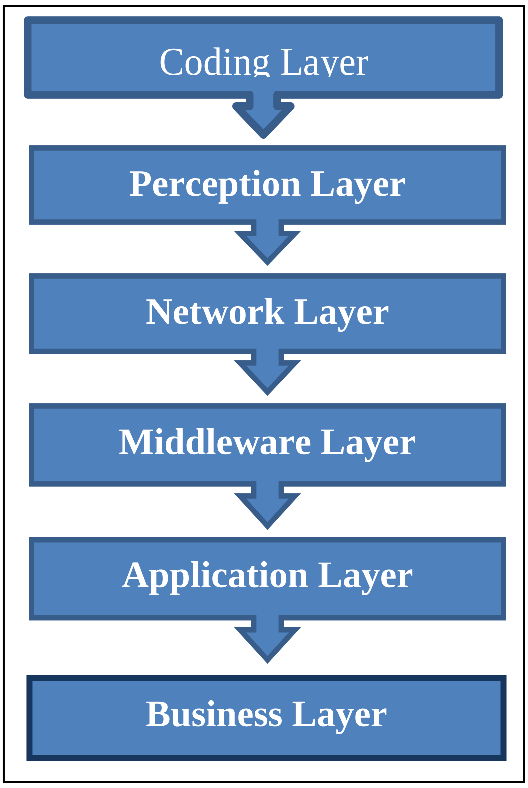

Figure 1. IoT Layers Architecture

1.3.1 Coding Layer

Coding layer is the foundation of IoT which provides identification to the objects of interest. In this layer, each object is to specify a unique ID which makes it easy to identify the objects.

1.3.2 Perception Layer

This is the device layer of IoT which gives a tangible meaning to each object. It include data sensors in different formats like RFID tags, IR sensors or other sensor networks which could sense the humidity, temperature, speed and location.

1.3.3 Network Layer

The objective of this layer is to receive the helpful information in the form of digital signals from the Perception Layer and transmit it to the processing systems in the Middleware Layer through the transmission mediums like Wi-Fi, Bluetooth, WiMaX, Zigbee, GSM, 3G etc with protocols like IPv4, IPv6, MQTT, DDS etc.

1.3.4 Middleware Layer

This layer processes the information received from the sensor devices. It includes the technologies like Cloud computing, Ubiquitous computing which include a direct access to the database to store all the requisite information in it.

1.3.5 Application Layer

This layer achieves the applications of IoT for all types of industry, based on the processed data. Because applications support the development of IoT so that the layer is very helpful in the large level development of IoT network.

1.3.6 Business Layer

This layer manages the applications and services of IoT and it is responsible for all the research related to IoT. It create different business models for efficient business strategies.

1.4 Requirements of IoT

For successful achievement of Internet of Things (IoT), we need the following [6]:

A. Effective resource demand
B. Real-time needs
C. Exponential increase of demand
D. Availability of applications
E. Data safeguard and user privacy
F. Efficient power consumptions of applications
G. Accomplish of the applications near to end users
H. Access to an open cloud system.

1.5 Internet of Things platform

1.5.1 Platform: When you are improving some applications, Platform is one of which permits you to deploy and run your application. A platform could be a hardware plus software which other applications can operate. The Platform could involve hardware above which Operating system can build. This Operating system will allow the application to work above it by providing substantial execution environment to it.
When there is only one communication to connect devices of one type with others of the same type then, a system of specific service can be establish. But in case of communication among devices of various types, there is a need for some common standard application platform which avoid heterogeneity of varied devices by providing a combined working environment to them [7].

1.5.2 various internet of Things platforms: Various IoT platforms are available, that can be used to improve IoT solutions. It has covered some popular platforms that are widely used [7].

1.5.2.1 IBM BlueMix: it is a platform as a service (PaaS) cloud which is developed by IBM. It supports programming languages like java, PHP, Python, and Node.js. Integrated DevOps allows to build, run, deploy as well as to manage applications over IBM BlueMix cloud. BlueMix platform is based on Cloud Foundry open technology [7]**.**

1.5.2.2 ThingWorx: it is the first software platform designed to build and run the connected world applications. ThingWorx focuses on reducing the time, cost, and risk required to build innovative Machine-to-Machine (M2M) and the Internet of Things (IoT) applications. [7].

1.5.2.3 Microsoft Azure Cloud: It is Intelligent System Service which composes an integrated platform and services that makeup the Internet of Things systems and applications by collecting, storing and processing data. The essence of Microsoft IoT foundation is Microsoft Azure cloud platform. It provides connectivity to millions of devices and sensors with IoT application. It provides remote access, monitoring, and content distribution and configuration management facilities for connected devices [7].

1.5.2.4 ThingSpeak: It is an application platform for the expansion of IoT systems. It can help you to build the application which works onto the data collected by sensors. ThingSpeak is an open data platform for IoT application development. it provides the ability to integrate your data with a diversity of third-party platforms, systems, and technologies [7].

1.5.2.5 Zetta: it is an open source platform. It is developed in Node.js for creating IoT servers that run across geo-distributed servers and cloud**.** Zetta runs everywhere: It means Zetta runs in the cloud, on PCs and on single board computers**[7].**

1.5.2.6 Nimbits: The platform is used for developing hardware and software solutions that can connect to the cloud or to each other and enables send and retrieve large amounts of data from different devices, elicit events or alerts, or performance of complicated analysis [7].

1.5.2.7 Yaler: It provides a relay infrastructure which provides secure access to embedded systems and it works with any device with a TCP socket. Yaler is a cost-effective solution which is appropriate for enterprise applications [7].

1.5.2.8 Amazon Web Services (AWS): It permits Internet of Things on a global level by simplify security, services, and support. It simplifies immediate access to desirable computing power by means of Amazon Elastic Cloud Compute (EC2). it helps to perform and support big data analysis [7].

1.5.2.9 Axeda and Oracle Java Embedded: The Axeda Machine Cloud service provides M2M services, IoT connectivity services, software agents and toolkits that allow you to select communication mode and hardware which is suitable for your IoT solution. The Axeda IoT platform provides end-to-end enterprise capabilities using Java EE technology and the Oracle Database [7].

1.6 Internet of Things middleware

Middleware: It is an interface that is available to provide interaction between Internet and Things . It provides a wide type of services to the applications from outside. So the application is not limited to use its all services but only uses the necessary set of services. IoT middleware is a mechanism that connect different components of IoT systems together and offers easy communication among devices and components [7].

II. INTEGRATION OF INTERNET OF THINGS AND CLOUD COMPUTING

When internet of things gets integrated with cloud, the data gets centralized. So, the data can be stored in a cloud and can be accessed from anywhere through internet. This is one of the major requirements for integration. The integration of IoT and Cloud computing enables new services and some other services are [8]:

A. SaaS (Sensing as a Service)
B. SAaaS (Sensing and Actuation as a Service)
C. SEaaS (Sensor Event as a Service)
D. DBaaS (Data-Base as a Service)

E. EaaS (Ethernet as a Service) / NaaS (Network as a Service)
F. IPMaaS (Identity and Policy Management as a Service)
G. G. Data as a Service (DaaS)

III. INTERNET OF THINGS COMMUNICATIONS MODELS

In March 2015, the Internet Architecture Board (IAB) released a guiding architectural document for networking of smart objects (RFC 7452),39 which outlines a framework of four common communication models used by IoT devices[2].

3.1 Device-to-Device Communications: The device-to-device communication model represents two or more devices that directly connect and communicate between one another, rather than through an intermediary application server. These devices communicate over many types of networks, including IP networks or the Internet[2].

3.2 Device-to-Cloud Communications: In a device-to-cloud communication model, the IoT device connects directly to an Internet cloud service like an application service supplier to exchange data and control message traffic. This approach considerably takes advantage of existing communications mechanisms like traditional wired Ethernet or Wi-Fi connections to set up a connection between the device and the IP network, which finally connects to the cloud service [2].

3.3 Device-to-Gateway Model: In this model, the device-to-application-layer gateway (ALG) model, the IoT device connects through an ALG service as a channel to reach a cloud service. In simpler terms, this means that there is application software operating on a local gateway device, which acts as an middle between the device and the cloud service and provides security and other functionality such as data or protocol interpretation [2].

3.4 Back-End Data-Sharing Model: The back-end data-sharing model indicate to a communication architecture that enables users to export and analyze smart object data from a cloud service in combination with data from other sources. [2].

IV. SMART HOMES

IoT has huge possibility for quality living and comfort. It can dim/brighten lights as time change; it can increase/ decrease room temperature. BLE, a low-cost technology is allocated for power efficient homes. IoT can be allocatied for monitoring room air quality, open garage doors, automate all home devices, thus acting as assistance in our busy schedules [9].

V. SMART CITIES

Smart Cities are a future reality around the world. These cities will use the power of distributing communication networks, highly distributed wireless sensor technology, and intelligent management systems to solve current and future challenges and create spectacular new services. Smart City officials will be essential imaginary leaders who drive Smart City proceed using public-private co-partnership to invest in scalable projects, smart regulation to connect city laws to new digital realities. [10].

Some examples of smart city solutions include[11]:

A. Parking: Smart parking monitors show parking spaces available in a city to help reduce the traffic congestion created by people looking for a parking space.
B. Traffic Flows: Traffic congestion is a significant challenge to urban residents, and smart traffic systems can monitor vehicle and pedestrian traffic to better route automobiles and pedestrians.
C. Street Lighting: Electricity from street lights is a significant municipal expense, and by better managing it, cities can save money and cut greenhouse gas emissions by reducing energy consumption.
D. Traffic Light Maintenance: Monitoring traffic lights allows municipalities to quickly respond to burned out lights, broken light poles from accidents, or malfunctioning signaling equipment.
E. Predictive Maintenance: Smart building systems can provide data that ensure structures are maintained properly by providing a predictive maintenance system. These systems can monitor vibrations and other physical conditions in buildings, bridges and historical monuments.
F. Waste Management: Collecting waste is an essential city service, but too often resources are used to collect under-filled waste containers when others are overflowing. Smart waste management systems can help detect garbage levels in containers to optimize the waste collection routes for efficiency and cost-effectiveness.
G. Noise and Air Pollution: As more people move to cities, noise and air pollution become a bigger challenge. Smart noise and air pollution monitoring can provide data that can improve citizens' well-being and detect systemic health issue correlation.

VI. SOCIAL AND ETHICAL BEHAVIOR FOR THE INTERNET OF THINGS

At current, policy and laws about online privacy and rights to information are challenging to explain and difficult to perform. As IoT technologies become more spread, personal information will become more worthy to a various set of actors that include organizations, individuals, and independent systems with the capacity to make decisions about you. Some have suggested that individuals should have a basic right to , delete, or hide their information from systems in the IoT. However, it may be impossible for an individual to control all the data generated about them by IoT systems [12].

VII. INTERNET OF THINGS MALWARE

Traditional malware lacks cross-platform capability. In heterogeneous IoT networks, different central processing unit architectures and operating systems are supported. Traditional computing environments are mainly based on X86 architecture, there exists a wide array of studies on malware propagation and analysis in X86 and/or X64 without consideration of device interaction with other architectures hence homogeneity based on specific architecture and operating system.

VIII. IoT CHALLENGES

Five key IoT issue areas are examined to explore some of the most pressing challenges and questions related to the technology. These include security; privacy; interoperability and standards; legal, regulatory, and rights; and emerging economies and development[2][13].

1- Security: While security considerations are not new in the context of information technology, the attributes of many IoT implementations present new and unique security challenges. Users need to trust that IoT devices and related data services are secure from vulnerabilities, especially as this technology becomes more pervasive and integrated into our daily lives. The interconnected nature of IoT devices means that every poorly secured device that is connected online potentially affects the security and resilience of the Internet globally. This challenge is amplified by other considerations like the mass-scale deployment of homogenous IoT devices, the ability of some devices to automatically connect to other devices, and the likelihood of fielding these devices in unsecure environments.

2- Privacy: The full potential of the Internet of Things depends on strategies that respect individual privacy choices across a broad spectrum of expectations. The data streams and user specificity afforded by IoT devices can unlock incredible and unique value to IoT users, but concerns about privacy and potential harms might hold back full adoption of the Internet of Things.

3- Interoperability / Standards: A fragmented environment of proprietary IoT technical implementations will inhibit value for users and industry. While full interoperability across products and services is not always feasible or necessary, purchasers may be hesitant to buy IoT products and services if there is integration inflexibility, high ownership complexity, and concern over vendor lock-in. In addition, poorly designed and configured IoT devices may have negative consequences for the networking resources which connect to and the broader Internet.

several other associated challenges need to be considered as well, including the followings:

A. **Thing Interaction:** There is more than one option to how things will interact with other things or the users. There exist situations where interactions with individual things are needed. On the other hand, there exist situations where the ability to query and control large groups of things at the same time is also required.
B. **Virtual Representation of Things**: How things are represented and described remains an issue unsolved or precisely unstandardized. For instance, do we need to establish a shared schema or ontology for things for greater interoperability? Which attributes should be used to describe things and how flexible and unified this descriptor system should be? Can we find appropriate ways to involve users in connecting things and resolving ambiguities based on their current operation or context?
C. **Searching, Finding and Accessing Things**: How do we search for things on the Internet? Should we be able to search for things by their unique ID, IP, location, name or/and in combination with other properties? How can we discover, search, locate or track mobile things that may move from one location or network to another? How should things be organized, deployed, managed and secured?
D. **Syntactic Interoperability between Things:** Recall that syntactic interoperability deals with the packaging and transmission mechanisms for data over a network. Thus, when all the above challenges are addressed, there will still be a need to ensure that data flow is interoperable between the various networks and among a mixture of devices.

4- Legal, Regulatory and Rights: The use of IoT devices raises many new regulatory and legal questions as well as amplifies existing legal issues around the Internet. The questions are wide in scope, and the rapid rate of change in IoT technology frequently outpaces the ability of the associated policy, legal, and regulatory structures to adapt.

5- Emerging Economy and Development Issues: The Internet of Things holds significant promise for delivering social and economic benefits to emerging and developing economies. This includes areas such as sustainable agriculture, water quality and use, healthcare, industrialization, and environmental management, among others.

IX. COSTS OF INTERNET OF THINGS

Radio-frequency identification (RFID) uses electromagnetic field to automatically identify and track tags attached to objects[14]. The tags contain electronically stored information. In the IoT, the most basic step is RFID. The main causes for costs are tags or sensors and readers. In the case of the retail sector that started to introduce RFID, it is difficult to recover tags. Thus, the tags' prices drop will play an important role in adopting decision there for, price drops after the introduction of equipment due to the improvement of sensor technology which seems to be the main factor of spreading of the IoT. Given the decline of the overall sensor price and the low network costs, the main cost factors that the enterprises is that of taking advantage of the IoT may include costs of manpower and building up data management system by making use of IoT [14].

X. CONCLUSION

The overview paper concludes that IoT is present everywhere and anywhere. It ensues automation of our daily activities in home, education, industry, transport, agriculture, mining, healthcare and still abundant. Despite its benefits, IoT deals with various security issues, energy efficiency, availability, interoperability, reliability issues, With this context, IoT is considered as next revolution of internet. An overview of IoT is describes the technologies it encompasses, emphasis on the application layer of a flexible layered IoT architecture. Also the protocols of application layer is compared. Future papers can includes gathering and processing of sensory data, having energy efficient devices, integration of IoT with cloud computing and in social networking. IoT is an emerging paradigm; it aims at improving quality of life by connecting things around us.

REFERENCES

[1] Shancang Li and Theo Tryfonas, Honglei Li ," *The Internet of Things: a security point of view*",2016 ,Internet Research, Vol. 26 Issue: 2, pp.337-359

[2] Internet Society ,"*The internet of Things An overview : Understanding the issues and challenges of a more connected world*",2015, www.internetsociety.org

[3] Harald Sundmaeker, Patrick Guillemin, Peter Friess, Sylvie Woelfflé, " *Vision and Challenges for Realising the Internet of Things*",2010, European commission – Information Society and Media,

[4] Deepika Khambra, Ms. Poonam Dabas," *Internet of Things: A Perspective from security and privacy***",** 2017, International Journal of Advanced Research in Computer Science, Volume 8, No. 5

[5] M.U. Farooq, Muhammad Waseem, Sadia Mazhar, Anjum Khairi, Talha Kamal," *A Review on Internet of Things (IoT)*",2015,International Journal of Computer Applications, 2015, Vol. 113, No. 1, 164-173

[6] Bhumi Nakhuva, Tushar Champaneria, " *study of various internet of things platforms*" , 2015, International Journal of Computer Science & Engineering Survey (IJCSES), Vol.6, No.6

[7] T. Venkat Narayana Rao, Shaik Khasim Saheb, A. Janiki Ram Redd y, " *Design of Architecture for Efficient Integration of Internet of Things and Cloud Computing*" , 2015, International Journal of Advanced Research in Computer Science, Volume 8, No. 3

[8] Jaideep Kaur, Kamaljit Kaur," *Internet of Things: A Review on Technologies, Architecture, Challenges, Applications, Future Trends*", 2017, *I.J. Computer Network and Information Security*, 4, 57-70

[9] Ruthbea Yesner Clarke **,"***Smart Cities and the Internet of Everything: The Foundation for Delivering Next-Generation Citizen Services*", 2013, IDC Government Insights,GI243955

[10] Semtech," Smart Cities Transformed Using Semtech's LoRa Technology", *2017,www.semtech.com*

[11] Francine Berman, Vinton G. Cerf, "*Social and Ethical Behavior in the Internet of Things* ", 2017, Communications of the ACM, Vol. 60 No. 2

[12] Mahmoud Elkhodr, Seyed Shahrestani, Hon Cheung, " *The Internet of Things: New Interoperability, Management and Security Challenges* ", 2016,International Journal of Network Security & Its Applications (IJNSA), Vol.8, No.2

[13] Young-Mo Kang, Mi-Ran Han, Kyeong-Seok Han, Jong-Bae Kim," *A Study on the Internet of Things (IoT) Applications*", 2015, International Journal of Software Engineering and Its Applications, Vol. 9, No. 9, pp. 117-126

[14] RFID, Wikipedia, https://en.wikipedia.org/wiki/Radio-frequency_identification