Egypt. J. of Appl. Sci., 34 (1) 2019 *81-95*

INTERNET OF THINGS-IOT: DEFINITION, ARCHITECTURE AND APPLICATIONS

Talal Sultan

Information Technology Engineering Department, Faculty of Engineering, Kalamoon University, Syria

Eng.talalsultan@gmail.com

ABSTRACT

Internet of Things is the concept of connecting any device to the Internet and to other connected devices. The IOT is a giant network of connected things and people, all of which collect and share data about the way they are used and the environment around them. Experts estimate that the IOT will consist of about 30 billion objects by 2020. This survey presents a study based on IOT and its applications in different fields of science and technology, and also discusses the architecture and elements of the IOT along with its different applications.

1. INTRODUCTION

Internet of Things is a platform where every day devices become smarter, every day processing becomes more intelligent, and every day communication becomes informative. We are talking about a new revolution in the Internet. Objects make themselves recognizable and they obtain intelligence by making or enabling context-related decisions thanks to the fact that they can communicate information about themselves. They can access information that has been aggregated by other things, or they can be components of complex services [1].

In present days, the IOT paradigm is applied to an ever increasing number of devices in several application fields from transportation to industrial sectors. Thus, IOT extends the capabilities of smart objects by enabling the user to monitor complex systems, such as intelligent transportation system (ITS), smart industry, and city and so on, from remote sites. The development of this kind of IOT systems requires designing several sub-systems from the network to data processing.

Based on above discussion the future of the IOT will be on many applications. Its applications will range from smart grid, smart city, intelligent automobiles, smart Energy etc.

In this survey, we briefly discussed what IOT is, how IOT enables different technologies, its architecture and applications.

2. DEFINITION OF IOT

Internet of Things common definition is: a network of physical objects. The internet is not only a network of computers, but also it has evolved into a network of devices of all types and sizes such as vehicles, smart phones, home appliances, toys, cameras, medical instruments, industrial systems, animals, people, and buildings, all connected, communicating and sharing information based on stipulated protocols in order to achieve smart reorganization, positioning, tracing, personal real time online monitoring, process control and administration [2].

We can say that the aim of the IOT is to allow physical and virtual ’Things’ to be connected anytime, anyplace, with anything and anyone ideally using any path/network/service, to achieve the goal of Internet of Things (IOT). There is a mixture of different hardware, software and communication technology integrated together to provide solutions which allow objects to be sensed or controlled remotely across existing network infrastructure.

Table 1- Comparison between the existing communication technologies

Parameters	Wi-Fi	Wi-MAX	LR-WPAN	Mobile communication	Bluetooth
Standard	IEEE 802.11 a/c/b/ d/g/n	IEEE 802.16	IEEE 802.15.4 (ZigBee)	2G-GSM, CDMA 3G-UMTS, CDMA2000 4G-LTE	IEEE 802.15.1
Frequency band	5–60 GHz	2–66 GHz	868/915 MHz, 2.4 GHz	865 MHz, 2.4 GHz	2.4 GHz
Data rate	1Mb/s– 6.75 Gb/s	1Mb/s–1 Gb/s (Fixed) 50–100 Mb/s	40–250 Kb/s	2G: 50–100 kb/s 3G: 200 kb/s 4G: 0.1–1 Gb/s	1–24 Mb/s
Transmission Range	20–100 m	<50Km	10–20 m	Entire cellular area	8–10 m
Energy Consumption	High	Medium	Low	Medium	Bluetooth: Medium BLE: Very Low
Cost	High	High	Low	Medium	Low

There is a heterogeneous mix of communication technologies, which need to be adapted in order to address the needs of IOT applications such as energy efficiency, speed, and cost. In this context, it is possible that the level of diversity will be scaled to a number of manageable connective technologies that address the needs of the IOT applications which are adopted by the market. They have already proved to be serviceable, supported by a strong technology alliance. Examples of standards in these categories include technologies like WI-FI, Bluetooth, ZigBee, and Mobile communication. Table-1 shows a comparison between these communication technologies.

Table 2 Comparison between the existing IOT supported hardware platforms.

Parameters	Arduino Uno	Intel-Galileo Gen 2	Beagle Bone Black	Raspberry Pi B+	ARM mbed NXP LPC1768
Processor	ATMega328P	Intel Quark SoC X1000	Sitara AM3358BZCZ100	Broadcom BCM2835 SoC based ARM1176JZF	ARM Cortex M3
GPU	————	————	Power VR SGX530 @520 MHz	Video Core IV Multimedia@ 250 MHz	————
Operating Voltage	5V	5V	3.3V	5V	5V
Bus width (bits)	8 bit	32 bit	32 bit	32 bit	32 bit
System memory	2kB	256 MB	512 MB	512 MB	32 KB
communication supported	IEEE 802.11 b/g/n, IEEE 802.15.4, 433RF, BLE 4.0, Ethernet, Serial	IEEE 802.11 b/g/n, IEEE 802.15.4, 433RF, BLE 4.0, Ethernet, Serial	IEEE 802.11 b/g/n, 433RF, IEEE 802.15.4, BLE 4.0, Ethernet, Serial	IEEE 802.11 b/g/n, IEEE 802.15.4, 433RF, BLE 4.0, Ethernet, Serial	IEEE 802.11 b/ g/n, IEEE 802.15.4, 433RF, BLE 4.0, Ethernet, Serial
Development Environments	Arduino IDE	Arduino IDE	Debian, Android, Ubuntu, Cloud9 IDE	NOOBS	C/C++ SDK, Online Compiler

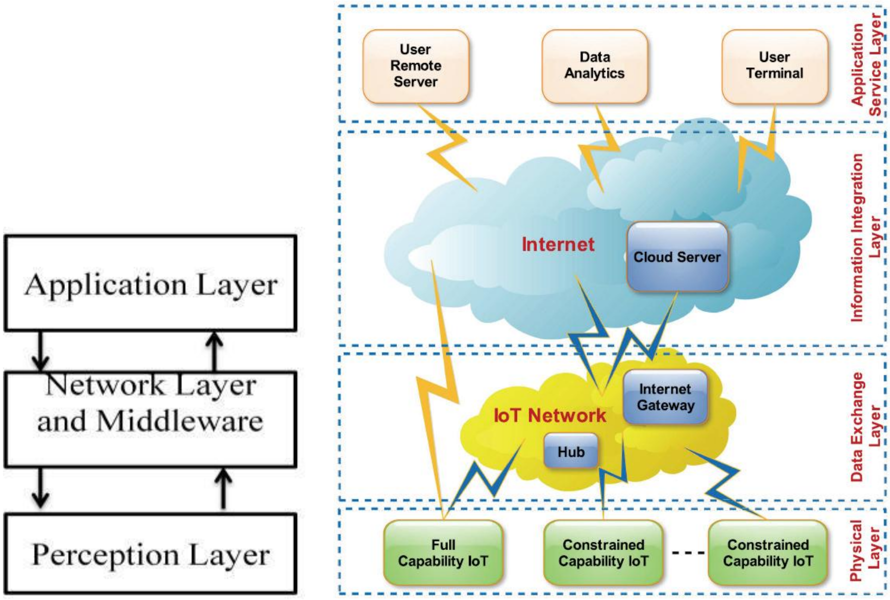
Also, there are several hardware platforms that support the needs of IOT applications and encourage the growth of them. Table-2 shows a comparison between these platforms.

In addition to hardware platform and communication Technology, we need IOT cloud platform which is designed to meant for designing IOT applications in different domains which depend on IOT cloud services which are available to be meant for particular domains such as real time data capture, visualization, data analytics, decision making, and device management related tasks through remote cloud servers[3].

We conclude from above that Internet of Things is much more than machine-to-machine communication, sensor networks, 2G/3G/4G, GSM, GPRS, RFID, WI-FI ,GPS, microcontroller, microprocessor etc. These are considered as enabling technologies that make “Internet of Things” applications possible.

IOT Architecture

Based on the above information about technologies, we need to enable IOT. We can say that IOT must consist of three or four layers. In general as shown in Fig. 1, we say general because IOT architecture varies from solution to solution, based on the type of solution which we intend to build. In this section, we will present original concept of a scalable and flexible IOT architecture by listing the basic element of IOT architecture and how they interact in an effective way to build an effective and applicability system.



(a) **(b)**

Fig. 1 General 3 Layer/ 4 Layer architecture for IOT

3.1. Elements of IOT Architecture

In this section, we will explain important IOT key elements [4] and how they are connected and interacted to collect, store and process data as shown in Fig. 2.

Things: A “thing” is smart objects integrated with **sensors** that gather data by measuring the physical property and convert it into a signal transferred over a network. There are many different types of them for different purposes such as temperature sensors, voltage sensors, humidity sensors, and etc. **Actuators,** that allow things to act, operates in the reverse direction of a sensor. They take an electrical input and turn it into physical action. For example, an electric motor, a hydraulic system, and a pneumatic system are all different types of actuators. This concept includes home appliance, buildings, vehicles, Industrial machinery, Medical equipment and everything else imaginable.

Gateways: Data goes from things to the cloud and vice versa through the gateways. A gateway provides connectivity between things and the cloud part of the IOT solution, enables data preprocessing and filtering before moving it to the cloud (to reduce the volume of data for detailed processing and storing), and transmits control commands going from the cloud to things. Things then execute commands using their actuators.

Cloud gateway: It’s the gateway that provides secured data transition between physical gateway and central cloud IOT servers using different protocols depending on what gateways the protocol is supported by.

Streaming data processor: It ensures distributing the data coming from sensors among relevant IOT solution's components (data lake and control applications) in effective way. No data can be lost or corrupted in this transition.

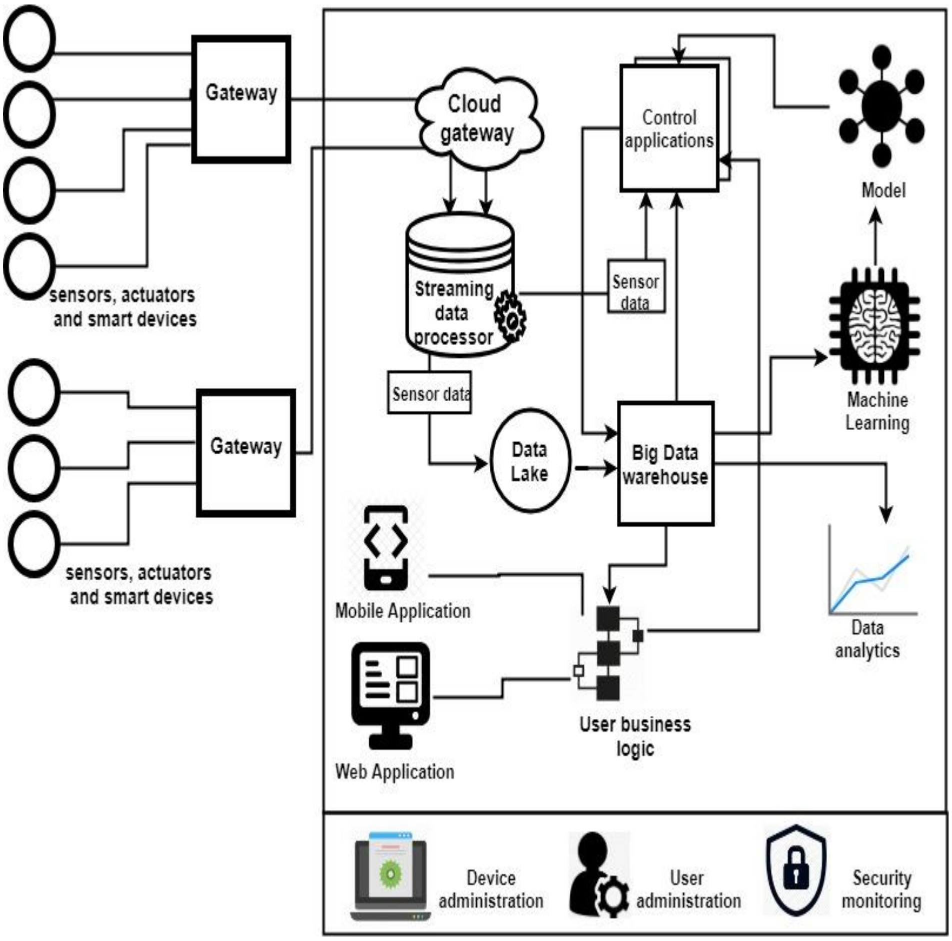


Fig 2-Basic elements of IoT architecture

Data Lake: It is used for storing raw data generated by connected sensors. Big data comes in “streams”. Then, it will be extracted and loaded to a big data warehouse for collecting valuable data.

Big data warehouse. It's contained cleaned, structured and matched data (compared to raw data stored in Data Lake). Also, data warehouse stores context information about things.

Data analytics. Data analysts can use data from the big data warehouse to find trends and gain actionable insights. At analyzing big data, we can inform about the performance of devices, know more about the efficiency of them, and try to improve an IOT system to be more reliable and oriented to do all of customers’ needs. Also, the correlations and patterns found manually can further contribute to create algorithms for control applications.

Machine learning and the models ML generates: by using machine learning, there is a chance to create more accurate and effective models for controlling applications. The models are updated regularly based on the historical data cumulated in a big data warehouse. After testing the model and ensuring that the model is applicable, effective and approved by data analysts, new models can be used by control applications.

Control applications: send automatic commands and alerts to actuators, for example, windows of a smart home can receive an automatic command to open or close depending on forecasts taken from the weather service.

When sensors show that the soil is dry, watering systems get an automatic command to water plants.

Sensors help monitor the state of industrial equipment, and in case of a pre-failure situation, an IOT system generates and sends automatic notifications to field engineers.

The commands sent by control apps to actuators can also be additionally stored in a big data warehouse. This may help investigate problematic cases (a control app sends commands which are not performed by actuators; then, connectivity, gateways and actuators need to be checked). On the other side, storing commands from control apps may contribute to security monitoring, for example, an IOT system can identify that some commands are too strange or come in too big amounts which may indicate security breaches (as well as other problems which need investigation and corrective measures).

Control applications can be either rule-based or machine-learning based. In the first case, control apps work according to the rules stated by specialists. Whereas in the second case, control apps are using models which are regularly updated (once a week or once a month depending on the specifics of an IOT system) with the historical data stored in a big data warehouse.

Although control apps ensure better automation of an IOT system, there should be always an option for users to influence the behavior of such applications, for example, in case of emergency or when it turns out that an IOT system is badly tuned to perform certain actions.

User applications: are a software component of an IOT system which enables the connection of users to an IOT system and gives options to monitor and control their smart things (while they are connected to a network of similar things, for example, homes or cars and controlled by a central system). With a mobile or web app, users can monitor the state of their things, send commands to control applications, set the options of automatic behavior (i.e. automatic notifications and actions when certain data comes from sensors).

Device management

To ensure sufficient functioning of IOT devices, it is not far enough to install them and let things go their way. Here are some procedures required to manage the performance of connected devices (facilitate the interaction between devices, ensure secure data transmission and more):

- **Device identification** to establish the identity of the device to be sure that it’s a genuine device with trusted software transmitting reliable data.
- **Configuration and control** to tune devices according to the purposes of an IOT system. Some parameters need to be written once a device is installed (e.g. unique device ID), whereas other settings might need updates (e.g. the time between sending messages with data).
- **Monitoring and diagnostics** to ensure smooth and secure performance of every device in a network and reduce the risk of breakdowns.
- **Software updates and maintenance** to add functionality, fix bugs, address security vulnerabilities.

User management

Alongside with device management, it’s important to provide control over the users having access to an IOT system.

User management involves identifying users, their roles, access levels and ownership in a system. It includes such options as adding and removing users, managing user settings, controlling access of various users to certain information, as well as the permission to perform certain operations within a system, controlling and recording user activities and more.

Security monitoring

Security is one of the top concerns in the internet of things. Connected things produce huge volumes of data, which need to be securely transmitted and protected from cyber-criminals. Another side is that the things connected to the Internet can be entry points for villains. What is more, cyber-criminals can get access to the "brain" of the whole IOT system and take control of it.

To prevent such problems, it makes sense to log and analyze the commands sent by control applications to things, monitor the actions of users and store all these data in the cloud. With such approach, it's possible to address security breaches at the earlier stages and take measures to reduce their influence on an IOT system (e.g. block certain commands coming from control applications).

Also, it's possible to identify the patterns of suspicious behavior, store these samples and compare them with the logs generated by an IOT systems to prevent potential penetrations and minimize their impact on the IOT system [5].

3. IOT Applications

Potential applications of the IOT are numerous and diverted, permeating into practically all areas of every-day life of individuals, enterprises, and society as a whole. The IOT application covers "smart" environments/spaces in domains such as: transportation, building, lifestyle, retail, agriculture, Industry, supply chain, emergency, healthcare, user interaction, culture and tourism, environment and energy. Below are some of the IOT applications:

3.1. Intelligent Transportation Systems (ITSs)

ITSs refer to a variety of traffic engineering concepts, software, hardware, and communications technologies, which are applied in an integrated pattern to the transportation system to improve its efficiency and safety. The effectiveness of ITS depends on its capability to collect a big amount of information from the transportation system (i.e. vehicles and infrastructure), then provide integrated information to the users to make decisions.

An ITS architecture is consisted as the basic elements of IOT system and we will see how these elements work together by several examples of ITS. This why, it has sensors that take data from the environment such as (photo/video cameras, GPS, speed measurement systems, distance meters) and actuators (e.g. panel signs with variable message) embedded on both the transport infrastructures and the vehicles. Wireless communications between vehicle-to-vehicle, vehicle-to-infrastructure and infrastructure-to-infrastructure are implemented, then (data analytics) analyzing information gathered with sensors and embedded information, such as incident warnings related to the infrastructure or the vehicles (e.g. vehicles accident, vehicle to infrastructure collision, and fire warning) and traffic conditions (e.g.

traffic congestion, and traffic bottleneck) to make and update the algorithms for control applications which in turn provide dispositions to the transport infrastructure supervisor, the drivers, and the rescue teams.

As the example in [6], a scalable real-time enhanced road side unit for ITS based on the concept of IOT is proposed. It aims to manage the road traffic adaptively according to the traffic levels and the pollution conditions, and to provide information about the weather. Information integration and application services are implemented in the master control center (MCC) which receives the measurements directly from the IOT sensor nodes located along the road and store them in a database. The (MCC) incorporates:

- Speed adaptive traffic control system, which provides adaptive speed limits according to the traffic conditions and the weather information.
- Pollution adaptive traffic control system, and
- Weather information system, which provides information to the road users (not only the driver) about the weather conditions.

Another example of ITS based on IOT is presented in [7]. In this case, the IOT concept is applied along the guardrails of the road infrastructure. The so called Wireless Active Guardrail System (WAGS) aims to monitor the traffic and the environmental conditions, and to detect the vehicle-guardrail impacts. The system consists of things which are: sensor/actuator nodes embedded on the guardrail that are dived into: traffic safety nodes, and environment monitoring nodes. A traffic safety node contains a speed measurement system providing measurements of vehicle speed, a proximity measurement system measuring the distance between the vehicle and the guardrail plate, an impact detection system revealing crash between vehicle and guardrail, and a signaling actuation system consisting of light or acoustic system. When a vehicle is approaching to the guardrail plates closer than a specified threshold value or when a vehicle-guardrail impact is detected, the alerting system is activated.

The environment monitoring node consists of: temperature and humidity sensors, a road surface state measurement system for detecting the conditions of dry, wet or icy asphalt, a road visibility measurement system, and an environmental pollution measurement system providing measurements related to the concentrations of CO, NO2, SO2, and particulate matter (PM).

All the nodes are powered with a photovoltaic-based system. The data exchange layer (gateway) presents wireless capabilities based on IEEE 802.15.4 standard. Furthermore, concentrator nodes are in charge of coordinating a sub-network of traffic safety and environmental monitoring nodes collecting the measured data and delivering them to the server over the Internet. The information integration layer is implemented on the server as presented in previous section about interacting the basic components among each other which provides embedded information related to the traffic and environmental conditions, and the positions and entities of the occurred vehicle-guardrail impacts. Control application is implemented to send automatic commands and alerts to actuators, in additional to user application to enable the connection of road supervisor to the system and gives him the options to show the monitored data.

3.2. Smart Energy

In a modern power grid, sensors and transducers have a significant role in monitoring and managing electrical energy in real time, according to the demand. Furthermore, the energy flow becomes bidirectional due to the presence of distributed generation plants [8]. For this reason, an implementation of smart power grids according to the IOT paradigm, allows managing and changing bidirectional flow of energy. In this way, it is possible to share information between several smart grids over Internet and to manage wide power grids. The physical layer consists of voltage and current transducers, actuators (e.g. switches and inverters), and a GPS receiver for synchronizing measurements. The voltage and current measurements have to be taken simultaneously along the monitored grid. The data exchange layer is usually implemented by means of power line communications, such as IEEE 1901.2, Ethernet or wireless communications based on Wi-Fi or cellular network. The information integration layer processes the data provided by the physical layer and provides integrated information related to the distribution system state, such as voltage, current waveforms, power quality, stationary and transient event, and supply discontinuities. By means of a control panel, the grid user or the supervisor can interact with the IOT system and monitor the grid state [8].

3.3. Smart Environment

Monitoring the environmental parameters, such as air quality, water quality and so on, is becoming more and more important due to significant impacts on the public health, and worldwide economy. To this aim, several wide distributed measurement systems have been developed according to the IOT concept. In this section, we discussed examples of IOT applications that deal with few factors of environmental monitoring. Those few factors are air quality and waste management.These factors are used in our day to day life.

In IOT Based Garbage Management System [9], ultrasonic sensor is used to detect the level of garbage in the dustbin. When the dust bins gets to its maximum level, the sensors get activated and generate a high signal which is transmitted through the Wi-Fi module. This signal is received by the server. Once the detail is received by the vehicle driver, he moves to the spot and disposes the waste from the trash bin. In this application, Cloud server is used. A cloud server is a logical server that is built, hosted and delivered. A cloud computing platform is used through the internet. Depending upon the input, the information is updated on cloud server using IOT. The main purpose of this application is to make people aware of disposing solid waste on roads and nearby places. The public user can access this website and can log in to see the location of the vehicle so that they can dispose their waste as soon as the vehicles arrive to the location. The vehicle driver has the login ID and password. If they log on site, they can get the path of the desired location of the dustbin on the Google map.

In this example, we present an air-quality monitoring system based on the IOT concept which was developed to be capable of detecting the level of pollutant gases. The sensor node consists of: the MQ135 sensor which is sensitive to variations of ammonia, sulfur, benzene, and smoke, a PM 2.5 sensors for particulate matter density measurements, and the CC2430/CC2530 embedded development board which acquires the measurements from the sensors and transmits them to a ZigBee transceiver. The sensor nodes communicate with the concentrator nodes by sending data every 20 minutes. The concentrator nodes send the acquired measurements over Internet to a server which stores the data in a database and analyze the data set using a machine learning algorithm which was based on linear regression prediction. Therefore, the system would monitor the air pollution in real time and predict the measurements in the next given time interval. A user interface shows the measurements of each node on a map and gives prediction of air pollution which helps organizations or governments to achieve better planning of cities or places.

3.4. Smart Building:

A smart building includes services offered to the occupants, resources distributed to the city, and, in case of historical buildings, information provided to municipalities about their state of health. The structural health monitoring is applied to bridges, roads, tunnels, dams, industrial plants, standard and monumental buildings and so on. In particular, the structural health monitoring (SHM) requires structure observation over time through measurements obtained with different kinds of sensors, such as accelerometers, thermometers, hygrometers, and extensometers, deployed along the whole structure. Usually, the data exchange layer consists of wireless sensor nodes that communicate with a concentrator node. The concentrator node transmits the data over

Internet to a Server. In case of structural monitoring, by using the required measurements, the integration information layer estimates parameters related to the dynamic behavior of the structure (e.g. vibration data, eigenfrequencies, damping ratios, and mode shapes). The extrapolated information is sent to the application service layer.

In [10], a structural monitoring system based on IOT is presented . The physical layer consists of: accelerometer, humidity and temperature sensors, a GPS receiver and a real-time clock circuitry. The sensors are embedded in a node, where a microcontroller acquires the measurements provided by sensors and sends them to a concentrator. Each sensor node communicates with the concentrator by means of ZigBee wireless interface. The concentrator node collects the measurements and sends them to a private data server over Internet, by means of GPRS/UMTS communication. The sensor nodes are supplied with a battery, while the concentrator is connected to an electrical network. The private data server implements the integration information layer. It processes the received data by means of fuzzy-logic algorithm and estimates the status of the structural elements.

After that, the integrated information is sent to the public data server, implementing the application service layer, where the supervisor evaluates the obtained information in order to make decisions.

In that case, an important task for implementing an IOT system for structural monitoring is related to a number of sensors to be placed on the building for obtaining a number of measurements having a spatial density that allows correcting definition of the health status of the structure, which is performed by the information integration layer. The system has to guarantee early warnings in case of dangerous damage of the structure elements.

3.5. Smart Factory

Nowadays, the advanced manufacturing technologies are changing the production mode of the manufacturing enterprises. Thus, it was raised the smart factory concept, aimed to improve the management of manufacturing resources and the quality of services.

Consequently, industrialized countries are paying more attention to the development of those manufacturing technologies in the industry. The physical layer consists of IOT nodes (e.g. smart meters, RFID tracking, etc.) with configurable logic controllers (PLCs). The data exchange layer, usually is implemented by means of wired and wireless networks. The big amount of data provided by the smart factory will be processed by cloud server and applying models generated by machine learning such as sensor data, machine log, and manufacturing process data, and provide integrated information useful for implementing active maintenance operations, to optimize the production process and providing suggestions for product designing and marketing. The application service layer allows peer to peer interaction, human-to-machine and machine-to-machine, using the integrated information provided by the previous layer. According to the application services requirements, the service layer has to guarantee real-time and high reliability capabilities [11]. An example [12] of IOT system implementation in the Industry is presented in industrial operations of oil and gas, from extraction to refining, requires efficient and reliable techniques, technologies and systems to handle critical situations in the oilfields through quick responding to them which ultimately will improve recovery and raise production.

In this system, the wellhead is designed as an IOT node which embeds acoustic, flow, temperature, pressure sensors and electrical-controlled valves. All the IOT nodes embed a transceiver for short range communication which allows data transfer to a concentrator IOT node. Each concentrator node works as a network bridge between the smart objects and the control center, over Internet. The control center analyzes the data gathered from the smart objects, generates integrated information, sorts out problems, and finally takes appropriate decisions against anomalous events. Thus, the control center aids to prevent disruptions as well as health and safety risks. In addition, the control center will analyze data to check out daily usage and production of oil and gas to the supervisor.

From the above presented example, it is obvious that the main requirements of an IOT system for implementing a smart maintenance are the reliability of the measurements, and to guarantee early warnings.

In all, the main purpose of the IOT system is to automatize the manufacturing process completely.

4. CONCLUSIONS

From this survey, it can be observed that the development of IOT applications was possible by using Information Technology, Wireless Sensor Networks, Cloud Computing, Communication Technologies and, Cognitive Sciences, and focus on consistency (giving enough attention to every element of IoT architecture and making them work together), flexibility (opportunity to add new functions and new logic), and integration with enterprise systems (teaming up new IOT solutions with previously implemented corporate IT solutions).

REFERENCES

[1] **Santucci, G. (2010).** The internet of things: Between the revolution of the internet and the metamorphosis of objects. Vision and Challenges for Realising the Internet of Things, pp.11-24.

[2] **Stankovic, J.A. (2014).** Research directions for the internet of things. IEEE Internet of Things Journal, 1(1): 3-9.

[3] **Sintef, O.V. and P.F. Norway (2014).** Internet of things–From research and innovation to market deployment. In River Publishers' Series in Communication, pp.1-5.

[4] **Rai, R. ; C. Lepcha ; P.P. Ray and P. Chettri (2013).** GDMA: generalized domain model architecture of internet of things. In Proceedings of National Conference on Applied Electronics (NCAE), AIT Kolkata., pp: 65-68.

[5] **Mosenia, A. and N.K. Jha (2017).** A comprehensive study of security of internet-of-things. IEEE Transactions on Emerging Topics in Computing, 5(4): 586-602.

[6] **Sukuvaara, T. and P. Nurmi (2009).** Wireless traffic service platform for combined vehicle-to-vehicle and vehicle-to-infrastructure communications. IEEE Wireless Communications, 16(6):54-61.

[7] **Daponte, P. ; L. De Vito ; F. Picariello ; S. Rapuano and I. Tudosa (2014).** Prototype design and experimental evaluation of wireless measurement nodes for road safety. Measurement, 57: 1-14.

[8] **Bikmetov, R. ; M.Y.A. Raja and T.U. Sane (2017),** September. Infrastructure and applications of Internet of Things in smart grids: A survey. In 2017 North American Power Symposium (NAPS) (pp. 1-6). IEEE.

[9] **Medvedev, A. ; P. Fedchenkov ; A. Zaslavsky ; T. Anagnostopoulos and S. Khoruzhnikov (2015).** August. Waste management as an IoT-enabled service in smart cities. In Conference on smart spaces (pp. 104-115). Springer, Cham.

[10] **Barsocchi, P. ; P. Cassara ; F. Mavilia and D. Pellegrini (2018).** Sensing a city's state of health: structural monitoring system by Internet-of-Things wireless sensing devices. IEEE Consumer Electronics Magazine, 7(2): 22-31.

[11] **Chen, B. ; J. Wan ; L. Shu ; P. Li ; M. Mukherjee and B. Yin (2018).** Smart factory of industry 4.0: key technologies, application case, and challenges. IEEE Access, 6: 6505-6519.

[12] Aalsalem, M.Y. ; W.Z. Khan ; W. Gharibi and N. Armi (2017). October. An intelligent oil and gas well monitoring system based on Internet of Things. In 2017 International Conference on Radar, Antenna, Microwave, Electronics, and Telecommunications (ICRAMET) (pp. 124-127). IEEE.

انترنت الأشياء تعريفه،بنيته وتطبيقاته

طلال سلطان

قسم هندسة المعلوماتية –كلية الهندسة – جامعة القلمون –سوريا

يعتبر مفهوم إنترنت الأشياء IOT الجيل الجديد المتطور والمتنامي في شبكة الانترنت والذي يزيد من قدرة الأشياء المادية (الأدوات والأجهزة المختلفة)على الاتصال بشبكة الانترنت وكذلك اتصالها مع بعضها البعض وتنظيم عملية التفاهم وتبادل البيانات بين هذه الأشياء المادية المترابطة مع بعضها والمتصلة عبر بروتوكول الانترنت. حيث يمكن أن نعبر عن انترنت الأشياء على أنه شبكة عملاقة من الأشياء والأشخاص المتصلين مع بعضهم يقومون بمشاركة بياناتهم وبيانات البيئة المحيطة بهم.ويتوقع الباحثونٍ بأن IOT ستضم أكثر من 30 مليار كائن بحلول عام 2020.سنقدم في هذه الدراسة تعريفاً لمفهوم انترنت الأشياء وتطبيقاته في مختلف المجالات،كما سنوضح العناصر الأساسية لتطبيقات انترنت الأشياء وآلية تفاعلهاوالتقنيات اللازمة لبناء هذه التطبيقات.