https://afrjcict.net

A Survey of Some Key Characteristics of Internet of Things

Uwazie Emmanuel Chinanu[1], Abah Joel Benign[2] and Temitope Olufunmi Atoyebi[3]
Department of Computer Science,
Nasarawa State University,
Keffi,
Nigeria.
Email: [1]uwazieemmanuel@yahoo.com, [2]abahjoel08@gmail.com, [3]atoyebi.temitope@yahoo.com

ABSTRACT

With a growing dependence on data for faster and more appropriate decision making, the Internet of Things (IoT) has become indispensable for humans. This is because it is a network relied upon for the transfer of data from collection points to processing points and subsequent transfer of insights from the data to locations where it will be applied. IoT has permeated both the personal and professional lives of individuals and it is becoming ubiquitous in businesses and industries globally. This paper discusses the present state of the internet of things in terms of its Architecture, Applications, Data Processing technologies, Connectivity, Security Issues and its future prospects.

Keywords: *Internet of Things, Data, Cloud, Security, Network, Architecture*

African Journal of Computing & ICT Reference Format:

Uwazie Emmanuel, Abah Joel Benign and Temitope Olufunmi Atoyebi (2020), A Survey of Some Key Characteristics of Internet of Things, *Afr. J. Comp. & ICT*, Vol.13, No. 1, pp. 62 - 75.

I. INTRODUCTION

IoT is gaining increased popularity as devices are getting less expensive, connectivity is becoming more pervasive and battery life is lasting much longer. Cisco Internet Business Solutions Group predicts that in 2020, there will be 50 billion things connected to the internet [7]. Table 1 shows the estimated number of connected devices at selected years between 1990 and 2025.

YEAR	NUMBER OF CONNECTED DEVICES
1990	0.3 million
1999	90.0 million
2010	5.0 billion
2013	9.0 billion
2025	1.0 trillion

Table 1. IoT prospects as estimated by Hewlett Packard (HP) [33]

This paper seeks to give a complete description of the concept of Internet of Things IoT, while bringing to light its features, implications and prospects. The objectives are:
i. To describe the Internet of Things
ii. Explain the nature of IoT
iii. Describe the essence of IoT
iv. Mention the applicability of IoT
v. Analyse the threat IoT faces
vi. Mention predictions about the future of IoT

Some previous papers discuss IoT in terms of its definition, potentials, and societal role [1], the Wireless Communication Technologies for IoT [50], The Security threat to IoT Architectural layers [16], but none like this one gives an all-encompassing detail of IoT covering its Definition, Architecture, Applications, Data Processing technologies, Connectivity, Security Issues and its future prospects.

The term 'Internet of Things' (IoT) was first used in 1999 by Pioneer of British Technology Kevin Ashton [1], in terms of supply chain management [6]. According to him, the Internet of Things refers to the system of physical objects that have sensors and are connected to the internet.

When an everyday object has a sensor attached to it for sensing its environment, it is connected to a network so that it can send the data captured to other devices and it has actuators with which it can act on its environment based on information it receives from services on other systems on the network, that object becomes an Internet of Things device.

According to the 2020 conceptual Framework, the Internet of things is expressed with the simple formula:

IoT= Services + Data + Networks + Sensors [1]

Other IoT formulas still exist. A typical IoT Equation is represented as:

Internet of Things = Internet + Controller, Sensor and Actuators + Physical objects [2]

Both equations presented above still have short comings in their representation of Internet of Things.

The conceptual framework fails to show that several sensors don't stand alone but are attached to everyday objects which make the IoT relevant. Also, actuators were not mentioned even though they are part of many IoT devices. Controllers for activating both the sensors and actuators and transferring data from sensors to the network or transferring information from the network to the actuators are also absent. However, the conceptual framework correctly identifies Sensors, networks, Data and Services (which might include Cloud, Edge, Fog and Mist services).

The Typical IoT Equation rightly identifies Controllers, Sensors and Actuators added to Physical objects and the internet as components of IoT. However, it fails to realize that without services (like storage and processing) dealing with the data collected by sensors, IoT will gain little applicability.

Therefore, to represent IoT in a manner which leaves no important factor out, the Holistic Equation is very useful and is given by equation (1)

IoT = Sevices + Data + Networks + Controller, Sensor and Actuator + Physical Object (1)

A sensor detects changes in its environment and obtains data about that change while an actuator acts on its environment by moving or controlling something. Actuators are of the following types: electrical, pneumatic (uses air pressure), hydraulic (uses fluid pressure) and mechanical. Table 2 shows the type of data collected, sensors, applications and IoT devices involved.

IoT Eco system includes Objects, Data [8], People, Places, Time, Network and operations/services [14].

Key features of IoT include:

(i) Instrumentation: Sensors like in-vehicle transponders, Infrared sensors, RFID, CCTV Cameras, GPS Sensors, Pneumatic tubes, Inductive loops, Piezo-electric strips, Passive acoustic, etc are needed for the collection of various data. Actuators are also needed in some IoT devices to effect changes in the external environment. These sensors and actuators are attached to physical objects – the "things" that make up the "Internet of Things" [60] - like fridges, cars, clothes, etc used by individuals and businesses.

(ii)Interconnectedness: IoT devices are networked with each other at different scales, ranging from Local Area Networks to Wide Area Networks so that they can communicate with each other [60].

(iii)Intelligence: With IoT, objects have become smart since they are involved in the collection and processing of data to obtain meaningful information for more efficient processes and decision making that improve businesses and the society [60]. System intelligence is key in the development of IoT both now and in the future [59].

Types of IoT micro controllers/processors based on performance

Based on their performance, IoT micro controllers/processors can be splitted into two categories, namely:

Low-end IoT devices: these have very low computational power and memory capacity but they require low power supply to function. Examples of such devices are Arduino, Open-Mote nodes, IoT-LAB M3 nodes, TelosB motes, Zolertia Z1 and Econotag [4].

High-end IoT devices: these are computationally powerful single-board computers like Raspberry pi, Minnowboard Max and Smartphones which run operating systems like Linux and Windows [3].

IoT interactions
There are three different types of interactions in the IoT sphere, such as [5]:

i. Machine to machine (M2M): M2M Connects a device to another [8] or the Internet, to deliver services that meet the needs of individuals and industries, with little or no direct human intervention [9].
ii. Machine to people (M2P): M2P involves the connection between a machine and a person. It facilitates the movement, manipulation, and reporting of data from machines to people for use in making informed judgments [8]. M2P communication is applied in Alarms, Health monitoring devices, Gaming, Speech recognition, Smart shopping and Biometrics authentication [10].
iii. People to people (P2P): (P2P) connections occur when information is transferred from one person to another through network of devices [8]. Such interactions are often called Collaboration.

II. GENERAL CHARACTERISTICS OF IoT

2.1 IoT Architecture
Generally, the IoT device architecture is made up of four distinct layers namely:
Perception Layer: This is the physical or device layer which collects data from the sensor nodes and other physical devices such as GPS Arduino, Barcodes and RFID [17]. It includes Endpoint devices like GPS trackers, Thermostat, door lock, Dishwasher, Refrigerator, etc

Network Layer: The main work of this layer is to collect information from the perception layer and the processing unit and securely transfer them to other layers [18]. It is the Access point that accepts data from the Endpoint and sends it to the internet. Network layer consists of Cellular networks, WLAN, Internet [49] etc.

Processing Layer: This layer does intelligent operations such as automatic information evaluation, ubiquitous computing functions and processing data based on intelligent computing [17]. This is the Back End which is a server/service on the internet where the data from the Access Point is stored and/or processed, like a Cloud Service [12].

Application Layer: This is also known as the business layer and is implemented as the top layer in IoT architecture [8]. The application layer receives the data transmitted from network layer and uses the data to provide required services or operations.

The IoT architecture is depicted in Figure 1.

2.2 IoT Application contexts and Application Domains
IoT application contexts include the following [15]:
-Consumer IoT (IoT2C)
-Enterprise IoT (IoT2B)

Consumer IoT (IoT2C)
Consumer IoT refers to things which are marketed directly to consumers [11].
Such things belong to the following categories [15]:
Home: Home automation, Home improvement, Energy efficiency
Lifestyle: Wearable computing, Entertainment and music, Family, Leisure, Pets, Toys, Drones.
Health: Fitness, Monitoring, Measurement, Diagnosis.
Mobility: Connected cars, eBikes.

Enterprise IoT (IoT2B)
Enterprise IoT refers to the things used in increasing the efficiency of an organization's systems and processes and enabling organizations to improve their services or products [11].
Enterprise IoT has the following categories [15]:
Retail: stores, shops, convenience
Health: monitoring, measurement, diagnosis, surgery, patient care
Energy: transmission & distribution, fossil, nuclear, alternative.
Mobility: Aerospace & airports, marine, rail & stations, automotive, traffic
Cities: infrastructure, water/wastewater, HVAC, Lighting, Security, Life safety
Manufacturing: Mining, Oil & Gas, discrete production, continuous production, supply chain
Public & Services: schools, universities, government, banking, insurance, administration, commercial services.
Others: environment, military, agriculture, hospitality.

IoT Application Domains

IoT is applied in several fields, including: Healthcare, Transportation, Education, Agriculture, Energy, Manufacturing, Home, Environment, City, Drilling/Mining, Government, Retail, Telecommunications, Banking and, Finance, Travel and Hospitality, Architecture/Building, Media and Entertainment, Security, Military.

2.2.1 Healthcare
IoT application to the health industry is the birth of the Smart Healthcare system which has the following benefits: disease prevention and early identification, medical research and patient-tailored healthcare [14], Greater collaboration between health care teams for enhanced performance.

A significant advancement brought about by IoT in healthcare is the introduction of Wearables like Fitness tracking devices to monitor sleep, exercise heart rate, etc or Personal Medical devices to monitor blood pressure, glucose, etc.

2.2.2 Transportation
IoT is successfully being applied to transportation bringing about the Smart Transportation paradigm shift in the following domains: • Aviation • Maritime • Rail • Roadways. Benefits of Smart Transportation are: increased safety, better passenger journeys and more efficient transport of goods [14].

2.2.3 Education
Students' books are loaded into a smart device so they don't carry heavy loads of books to school. From their smart devices students can share ideas [58] and collaborate with their peers and teachers globally. Both the young and old people can have unlimited access to lifelong education with ease from their smart devices.

Smart education enables learners to attend to their skill gaps through learner-centred education tailored towards their individual needs [58]. Through mobile education, from any location teachers/instructors can update students' records and the learners can access their records at their convenience.

With virtual classrooms provided anywhere, students are given safer and more secure physical learning environments.

2.2.4 Agriculture
IoT offers major opportunities for agriculture like: maximising yields, improving Farm collaboration with other farms, regulators, buyers and sellers, monitoring farm and animal health status, observing and tackling environmental challenges [14], etc.

2.2.5 Energy
The Internet of Things in the energy sector has led to the creation of the Smart Grid which is aimed at an automated collection of data used for analysis of the behaviour of energy consumers for efficient and economical delivery of energy, managing patterns in demand and supply, and driving innovation [14].

2.2.6 Manufacturing
It helps to connect workers in a team to foster innovation and efficient operations. It also decreases downtime and increases productivity. It aids real-time visualisation of assets and remote control of operations [54]. Smarter maintenance and dispatching decision making is achieved through it.

2.2.7 Home
Appliances can be controlled from remote locations to conserve energy & water [5] and to prevent accidents. Home monitoring is possible at any time, from anywhere. Intrusion detection systems would alert home owners of intruders. Increased comfort is provided with automation of house chores.
Appliances in the automated home include: Smart thermostat, connected security system, smart refrigerator, self-driving vacuum cleaner, etc.

2.2.8 Environment
Monitoring and control of emission of CO2 and toxic gases from vehicles, factories and farms and other machines. Detection of forest fire through observation of combustion gases and fire conditions [5]. Early detection of Earthquake, Landslide and Avalanche by sensors placed in tremor locations to monitor soil moisture, earth density and vibrations for detecting dangerous soil patterns. Monitoring of snow levels to get real-time information on quality of ski tracks and prevent Avalanche.

2.2.9 City
Time and weather adaptive street lights which cut energy consumption and costs. Parking spaces availability are monitored [5], reducing search time for spaces and generating revenue from the parking spaces. Monitoring vehicle and pedestrian movements for better routing to manage congestion. Waste levels in containers are monitored for proper disposal of rubbish.

Case Study of Barcelona, Spain [51].
Barcelona is a smart city people and things are connected to a city Wi-Fi, thereby creating richer experiences and increased economic opportunities for its people, businesses and partners.

Parking sensors in grounds communicate with devices in cars to help vehicle owners easily find spot to park. This reduces traffic caused by cars trying to find an available parking space. People can find information on routes for

vehicles, plus information on an area like businesses and shows, in the area.

It's installing highly efficient street lights, to save energy and optimize maintenance while providing a safe environment for its inhabitants. The city-wide network of sensors provide city officials with real-time data on the flow of citizens, pollution, traffic or weather conditions so that they can easily make decisions.

2.2.10 Building
IoT has led to the invention of Smart buildings which benefit by optimizing design, saving time, minimizing costs, increasing comfort, preserving the environment, increasing productivity, improving security and safety [14].

2.3 IoT Enabling Technologies and Connectivity
2.3.1 Enabling technologies
The following technologies are applied in processing IoT data:
-Cloud Computing for IoT
-Fog Computing for IoT
-Edge Computing for IoT

Cloud Computing
Cloud computing, is an innovation that looks to discover approaches to give less expensive and more advanced computing through the use of various remote servers on the internet to store [2], oversee and process data [12] instead of a local server or a personal computer. The cloud computing is has successfully provided reliability, high-performance, ubiquity and scalability for IoT [29].

Fog Computing
Fog computing is an architecture that offers the full Computation, Networking and Storage capabilities of Cloud computing at the Edge of IoT networks [19]. A fog node can consist of a large set of devices, including embedded servers, industrial controllers, switches, routers, and video surveillance cameras [13].

Edge Computing
An Edge is a node or network device which is in close proximity with a data source and processes the data collected before it is sent to a cloud data centre [6].

2.3.2. IoT Connectivity
2.3.2.1. Connection Protocols
2.3.2.1.1. Low-Range, High Bandwidth Protocols: These are Local Area Network (LAN) protocols which include: Ethernet, Bluetooth, Wi-Fi [11], Infrared, Thread, Zigbee [55], Z-Wave, KNX, 6LoWPAN.

Infrared: It is a simple and reliable technology which offers simplex [56] and line-of-sight transmission of signals.

Ethernet: It is a protocol for wired transmission [11] with low susceptibility for electromagnetic interference. It has a range of about 100meters [56].
Bluetooth: Has low bandwith and spans a low range [55] of about 10 meters [56]. It is weakly susceptible to electromagnetic interference so it is ideal for industrial IoT applications where there are several devices sending data. It is also good for environments where high tansmission speed is not needed and configuration is simple since Bluetooth is easy to set up. Bluetooth % is the emerging technology for IoT, which promises higher speed, signal range, broadcast messaging capacity and introduction of robust mesh networks.
Wi-Fi: Several Wi-Fi versions include 802.11a, 802.11b, 802.11g, 802.11n and 802.11ac. It provides interoperability to all Wi-Fi certified products, has a high frequency of 2.4GHz to 5GHz, transmits to a range of about 25meters [26] and consumes much power. It is ideal for IoT devices that trade distances and low power consumption for transmission speed. Emerging Wi-Fi technologies specifically for IoT include Wi-Fi HaLow (802.11ah) and HEW (802.11ax). Easy connection of third party Wi-Fi connected devices to the Local Area Network raises security concerns to enterprises. It is also susceptible to electromagnetic interference.
Thread: It is a protocol for wireless communication with a data rate of about 250kbps. An advantage of it is that there is no single point of failure [27] since if a source node is down, a destination node can get data from other nodes in the network.
Zigbee: It is based on the IEEE 802.15.4 implementation. Its network topologies include Tree, Star and Mesh topologies [56]. It has different specifications for different applications such as Zigbee LightLink which is usually used for smart lights [27] and Zigbee Green Power which is used on battery-less devices.
Z-Wave: Used mainly in smart homes, it forms a Mesh network topology [27]. Though 6 times slower than Zigbee [56], it requires less energy to cover the same range as Zigbee.
KNX: It is one of the main protocols used in Heating Ventilation and Air Conditioning [27]. Being independent of any hardware platform, it is compatible with various devices ranging from an 8-bit micro controller to a personal computer. It is installed over twisted pair, power line networking, Radio Frequency, Ethernet and Infrared [56]. It reaches a range of up to 150 meters and transmits at a rate of up to 16.385 kbps. It forms a peer-to-peer connection with several devices in a network so if one node fails, others can still communicate with each other.
6LoWPAN: This implements IP vesion 6 over Low Power Wireless Personal Area Networks. It also is based on the IEEE 802.15.4 Wireless PAN technology [57]. It is good for devices that are powered by batteries. Its advantages also include a direct connection to the

Internet and provision of IPv6 security, naming, addressing and translation. It has low data rates of 20, 40 and 250 kbps and supports Star and Mesh topologies.

2.3.2.1.2. Wide-Range, Low Bandwidth:
These are Wide Area Networks (WANs) that include: Low Powered Wide Area Network (LPWAN) and Cellular IoT
LPWAN: It allows for low power consumption over a long distance. A message sent over LPWAN must be small (have small bandwidth) and simple.

LPWAN technologies include: SigFox, LoRaWAN, Symphony Link, Ingenu RPMA, and Weightless.
SigFox: SigFox uses a slow modulation rate to achieve a more extended range. Making it an excellent option where a system only needs to send small and infrequent data [20].
LoRaWAN: Uses the LoRa technology, a radio frequency signal modulation scheme. LoRa is a chip, while LoRaWAN is a software that runs on the chip [20].
Symphony Link: Another software that runs on LoRa. Compared to LoRaWAN, it includes extra features like repeater capability, firmware upgrade over-the-air, removal of duty cycle limit, guaranteed message receipt and dynamic range [20].
Weightless: It is the only truly open-standard that uses the unused part of the spectrum band in and around TV transmissions [8]. Weightless has three versions that serve different purposes: **Weightless-W, Weightless-N,** and **Weightless-P [20].**

Cellular IoT: Besides serving us with the benefits of calls, sending texts, or accessing the Internet through our mobile devices, cellular networks are applied in many Internet of Things solutions [34].
Cellular IoT technologies include: Cat-1, Cat-0, Cat-M1/Cat-M/LTE-M, NB-IoT/Cat-M2, EC-GSM (formerly EC-EGPRS) and 5G-IoT.
Long Term Evolution (4G), category M1 (LTE-M): uses standard LTE connectivity while preserving resources. It has high data rates, a relatively simple front-end, and works well in roaming applications such as vehicles or drones [20].

Narrowband-IoT (NB-IoT): It uses chipsets which have simpler construction, which reduces its cost. NB-IoT works best in static assets like smart meters [20].
NB-IoT can coexist with GSM and LTE under licensed frequency bands

2.3.2.1.3. Satellite: This uses satellites to connect sensors/devices to the cloud [11]. A single satellite network is capable of effectively providing coverage to the entire planet. A device moving around the world can stay on a single satellite network. Satellite's range reaches remote areas that other communication types cannot reach.

2.4. IoT Network Topologies and Data processing Technologies

Network topologies applicable in an IoT setting include:
Star Topology: A star network has a router or access point or Gateway in the middle that connects to all the terminals or final nodes [27]. The final nodes transmit their messages to the Gateways, for onward delivery to other final nodes or Gateways
Point-to-Point (P2P) Topology: Used to connect two nodes together [27]. It is an extension of the star topology [24]. In this topology, data flows either unidirectionally or bidirectionally between two devices. P2P is not often used in IoT where a node is required to communicate with multiple nodes instead of a single node. P2P is used in traffic data systems, police or fire radios and in some SCADA systems.
Mesh Topology: it allows and facilitates direct communication between end devices [27] without the use of an intermediate element. Mesh topology is usually applied in home automation, smart HVAC control, and smart buildings.

IoT Data processing Technologies
Critical insights can be gotten from the data IoT sensors/devices collect. Data processing Technologies like data analytics and machine learning can be powerful tools in doing so.

i. Data Analytics:
Traditional data analytics is incredible at explaining data. They produce reports or models of past or present events, thereby drawing useful insights for organizations [30].
Data analytics can help in quantifying goals, making intelligent decisions, and measuring success over time.

ii. Machine Learning:
Machine learning is significant when you know the output you want but you can't select the important input variables to produce that output**.** Machine learning algorithm can be given the goal(s) and data and it would "learn" from the data which factors are essential in accomplishing that goal [30]. Machine learning is also important for accurate future prediction. While the traditional data analytics models are static, machine learning models constantly improve with time as more data is captured and learnt [30]. This makes it very applicable in the IoT domain where data is highly dynamic.

2.5. Challenges of IoT Devices

-Privacy concerns: in surveys of IoT consumers, privacy remains a major demand. The IoT ecosystem collects huge and diverse data from individuals and organisations. Privacy concerns in IoT include revelation

of location of people associated with IoT devices; personal information inference through observation of data delivered by IoT; use of real identities of users to generate their soft identities for specific applications [5]. Care must be taken to ensure that the data gets only to the parties permitted by those whose data are collected.

-Language and Culture: IoT solution providers should implement IoT solutions [31]. Much of this will relate to the social relationships that will support the use of the technology

-Legal issues: The use of IoT devices presents four legal problems – discrimination; privacy; security; and Consent [25]. There are legal questions about the existence of laws able to protect users of IoT devices. Legislative solutions should be provided to answer such questions [26].

-Intellectual property: IoT faces several issues relating to Copyright, Patents, Trade secrets and Trade mark.

i. Copyright: This is a law which protects an original work by granting its owner certain exclusive rights (with some limitations and exceptions) over the work.

IoT copyright laws cover the use, ownership and access to data and software. Although some data are not included in a copyright protection, others are eligible for copyright compilation and as such, permission must be taken before they can be copied, distributed, or modified. The restricted access and modification required by copyright may protect the safety, reliability and usability of IoT devices as copyright laws deter counterfeit applications carrying malware. However, copyright protections hamper security research, thereby making consumer security and privacy difficult.

ii. Patents: For IoT to thrive, devices need to connect and communicate with each other using standard technology. Patenting these standard technologies can hamper the growth of IoT. Therefore, policymakers should ensure that patents owned by the inventors are allowed for licensing and cross-licensing to third parties [28].

iii. Trade Secrets: Although any business that doesn't protect its innovation risks losing much of the value it creates, stronger trade secrecy protections may hurt innovation. This is because innovation comes when ideas from different fields, experiences, and organizations are combined [32].

-Scalability: The IoT ecosystem is wider than the traditional Internet of Computers Ecosystem. IoT requires some new functions and methods in order to expand for large-scale adoption [61].

-Standards: To allow all actors to equally access and use IoT infrastructures and applications, services, and devices, standards should be available and open [59]. Standard protocol and languages together with consistency in design and architecture of IoT devices is necessary to increase the demand for IoT devices.

-Cybersecurity: Compared with traditional networks, IoT increases the attack surface as it connects more devices, software and networks [59]. Despite this, many organisations and individuals underestimate the security risks IoT devices pose to their businesses and lives respectively.

Cyber security attacks at the various IoT layers are [16]:

Perception Layer Attacks: Attacks on this layer usually affect the physical components of IoT. They are relatively difficult to carry out because the operations require expensive materials and also, there is need for the attacker to have physical contact with the IoT system to be attacked [17]. Examples of these attacks are: Physical Damage [17], Spoofing, Node Tampering [35], Malicious Node Injection, Malicious Code Injection [36], Tag Cloning, Unauthorized Access to the Tags, Replay Attack [37], Timing Attack [38], Eavesdropping [39], Social Engineering, etc.

Network Layer Attacks: This type of attack is targeted at the network of the IoT system. It includes the following: Wormhole attack [40], Flooding, Node Replication [41], Man-In-the-Middle Attack, Denial of Service [42], Traffic Analysis Attack, Sybil Attack, RFID Cloning, RFID Spoofing, Unauthorized Access of RFID, RF interface on RFID [43], Hello Flood Attack, Wormhole Attack, Sleep Deprivation Attack, Sinkhole Attack [44], Routing Information Attack, Selective forwarding [45], Routing Threats [17], Jamming of node in Wireless Sensor Network.

Processing Layer Attacks: Attacks in this layer are targeted at data storage and data processing technologies [16]. Common attacks in this layer are: Platform Lower Layer Attack, Unauthorized Service Access, Insider Attack, Virtualization threats [45], Shared Resources.

Application Layer Attacks: These are which use malwares like spyware, virus and worms to destroy IoT systems [16]. Common examples of application attacks are: Application layer software vulnerabilities Attack, Phishing Attack, Malicious Scripts Attack, [46] Sniffing Attack, Malicious Code Attack, Denial of Service Attack, Cryptanalysis Attack [47], Side channel Attack, Man In the Middle Attack [48].

III. DISCUSSION

Future of IoT

International Data Corporation (IDC) predictions about the IoT in 2025. IDC estimates that in 2025, there will be 41.6 billion connected IoT devices [23], generating 79.4 zettabytes (ZB) of data [21]. Data from IoT devices will grow at a compound annual growth rate (CAGR) of 28.7% over 2018 to 2025 forecast period. In that period, Video surveillance data will grow at a compound annual growth rate of 60% [21].

Deployment of 5G networks [22] (offering low latency, dense coverage, and high bandwidth) as well as analytics applications [21] for enterprise, government and consumer use will bring about the data surge. Other predictions [22] also include:
-By 2025, it is estimated that there will be more than to 21 billion IoT devices
-Cybercriminals will continue to use IoT devices to facilitate DDoS attacks
-More cities will become "smart"
-Artificial intelligence will continue to become a bigger thing
-Routers will continue to become more secure and smarter
-5G Networks will continue to fuel IoT growth
-Cars will get even smarter
-IoT-based DDoS attacks will take on more dangerous forms
-Security and privacy concerns will drive legislation and regulatory activity

IV. CONCLUSION

With the development of the Internet and Internet-based applications, it now seems impossible to operate in any scenario without interaction with the internet. The IoT would allow for the automation of everything around us in a bid to improve the quality of life. In this paper, a comprehensive survey of IoT has been presented, including its definition, components, architectures, application, enabling technologies, connectivity, network topologies, challenges, and predictions about its future. Also, new holistic IoT equation is introduced in this paper.

The main purpose of this survey is to provide a clear, comprehensive, and deep understanding of IoT, with the roles of the different components that constitute the IoT. This has been achieved by outlining the breadth of topics that IoT entails, and highlighting areas that remain unresolved. This, in turn, should provide a good foundation for researchers and practitioners who are interested to gain an insight into the IoT technologies in an effort to further promote its development.

REFERENCES

[1] L. Atzori, A. Iera, and G. Morabito, "Understanding the Internet of Things: definition, potentials, and societal role of a fast evolving paradigm," *Ad Hoc Networks*, vol. 56, pp. 122-140, 2017.

[2] Farheen Fatima, Batul Naeem Husain, Mohammed Azharuddin and Mohammed Abdul Mabood, "Internet of things: A Survey on Architecture, Applications, Security, Enabling Technologies, Advantages & Disadvantages" *International Journal of Advanced Research in Computer and Communication Engineering*, Vol. 4, Issue 12, December 2015.

[3] Abah Joshua, Uwazie Emmanuel Chinanu and Alu Esther Samuel, "Security Considerations in High-end IoT Operating Systems: Case Study of Raspbian and Windows 10 IoT Core" *International Conference on Applied ICT*, Lead City University, Ibadan, Vol. 1, pp1-8, 2017.

[4] Andreas Elvstam, Daniel Nordahl. *Operating systems for resource constraint Internet of Things devices: An evaluation.* Faculty of Technology and Society Computer Engineering, Malmo University, Sweden, 2016

[5] Ovidiu Vermesan, Peter Friess, "Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems" River Publishers, 2013.

[6] Weisong Shi, Jie Cao, Quan Zhang, Youhuizi Li, and Lanyu Xu, "Edge Computing: Vision and Challenges", IEEE Internet of Things Journal, Vol. 3, No. 5, October 2016, pp. 637-646.

[7] D. Evans, "The Internet of Things: How the next evolution of the Internet is changing everything," CISCO White Paper, vol. 1, pp. 1–11, 2011.

[8] OpenLearn, "Internet of Everything", The Open University, 2019, Retrieved November 2, 2019, Available at www.open.edu/openlearn/science-maths-technology/internet-everything/content-section-overview

[9] Oluwatosin Ahmed Amodu, Mohamed Othman. "Machine-to-Machine Communication: An Overview of Opportunities", Computer Networks, Vol. 145, pp. 255-276, 2018.

[10] Machine to Human Communication, Evince Development, Retrieved February 21, 2020, Available At https://evincedev.com/machine-to-human-communication/

[11] IoT 101, "An Introduction to the Internet of Things", 2018, First Edition, Leverege LLC.

[12] Emmanuel Uwazie, Okonkwo Ogechukwu, Ambrose Nwosu, Uche Mbanaso, 2019, "Survey of Cloud Computing in Nigeria and Recommendation for Future Development", ICT FOR ALL, *International Conference on Applied ICT*, Lead City University, Ibadan, vol. 2, pp. 125-143.

[13] Computing, F. The internet of things: Extend the cloud to where the things are. In *Cisco White Paper*; Cisco: Charlotte, NC, USA, 2015.

[14] The Government Office for Science, "The Internet of Things: making the most of the Second Digital Revolution" A report by the UK Government Chief Scientific Adviser, 2014

[15] Knud Lasse Lueth, October 31, 2014 "IoT market segments – Biggest opportunities in industrial manufacturing" IoT Analytics, Retrieved September 21, 2018**,** Available at https://iot-analytics.com/iot-market-segments-analysis/.

[16] Uwazie Emmanuel Chinanu, Onoja Emmanuel Oche, Joy O. Okah-Edemoh, "Architectural Layers of Internet of Things: Analysis of Security Threats and Their Countermeasures", Academic Research Publishing Group, *Scientific Review*, Vol. 4, Issue. 10, pp: 80-89, 2018.

[17] Ioannis Andrea, Chrysostomos Chrysostomou, and George Hadjichristofi. "Internet of things: Security vulnerabilities and challenges." *Computers and Communication (ISCC), 2015 IEEE Symposium on IEEE, 2015*,

[18] D. Conzon, T. Bolognesi, P. Brizzi, A. Lotito, R. Tomasi, and M. Spirito. "The VIRTUS middleware, An XMPP based architecture for secure IoT communications." In *21st Inter. Conf.on Computer Communications and Networks, Munich, Germany.* pp. 1-6, 2012.

[19] OpenFog Architecture Team, Elements of an Open, Interoperable Architecture for Fog, Fog World Congress, Santa Clara, California, October 30, 2017.

[20] Calum McClelland, August 17, 2018, IoT Connectivity – Comparing NB-IoT, LTE-M, LoRa, SigFox, and other LPWAN Technologies, Retrieved June 21, 2019, Available at https://www.iotforall.com/iot-connectivity-comparison-lora-sigfox-rpma-lpwan-technologies/

[21] Larry Dignan, "IoT devices to generate 79.4ZB of data in 2025, says IDC", ZDNet, June 18, 2019, Retrieved August 21, 2019, Available at https://www.zdnet.com/article/iot-devices-to-generate-79-4zb-of-data-in-2025-says-idc/

[22] Steve Symanovich, "The future of IoT: 10 predictions about the Internet of Things", Norton by Symantec, Retrieved September 21, 2019, Available at https://us.norton.com/internetsecurity-iot-5-predictions-for-the-future-of-iot.html

[23] "41.6 billion IoT devices will be generating 79.4 zettabytes of data in 2025" Help Net Security, June 21, 2019, Retrieved October 21, 2019, Available at https://www.helpnetsecurity.com/2019/06/21/connected-iot-devices-forecast/

[24] Jekishan K. Parmar, Ankit Desai, "IoT: Networking Technologies and Research Challenges", *International Journal of Computer Applications* (0975 - 8887), Volume 154 - No.7, November 2016.

[25] Chike Chike, 2018/01/20, "The Legal Challenges of Internet of Things", BOOK, DOI - 10.13140/RG.2.2.31475.84004

[26] Abo Bakr, Ahmed, A. Azer, Marianne, "IoT ethics challenges and legal issues", BOOK, 2017/12/01, 233-237, DOI - 10.1109/ICCES.2017.8275309

[27] Stefan Marksteiner, Vıctor Juan Exposito Jimenez, Heribert Vallant, Herwig Zeiner, 2017, An Overview of Wireless IoT Protocol Security in the Smart Home Domain, JOANNEUM RESEARCH Forschungsgesellschaft mbH, DIGITAL - Institute for Information and Communication Technologies, Graz, Austria.

[28] Amit Aggarwal, Karan Bhutani, (Nov 2, 2016), Intellectual Property issues and Internet of Things (IoT), Effectual Services, Retrieved November 2, 2019, Available at http://www.effectualservices.com/blog/intellectual-property-issues-and-internet-of-things-iot/

[29] Farhoud Hosseinpour, Payam Vahdani Amoli, Juha Plosila, Timo Hämäläinen, and Hannu Tenhunen. 2016, "An Intrusion Detection System for Fog Computing and IoT based Logistic Systems using a Smart Data Approach." *International Journal of Digital Content Technology and its Applications (JDCTA),* vol. 10, No. 5.

[30] Calum McClelland, (Apr 30, 2018), "Data Analytics vs. Machine Learning", IoT For All,. Retrieved January 2, 2019, Available at https://medium.com/iotforall/data-analytics-vs-machine-learning-90d93dc06291

[31] Kim Walker, "The legal considerations of the internet of things", ComputerWeekly.com 16 Jul 2014, Available at https://www.computerweekly.com/opinion/The-legal-considerations-of-the-internet-of-things

[32] Andrea Contigiani, David H. Hsu, (January 29, 2019), "How Trade Secrets hurt innovation" Retrieved October 2, 2019, Available At https://hbr.org/2019/01/how-trade-secrets-hurt-innovation

[33] Vikrant Bhateja, João Manuel R.S. Tavares, B. Padmaja Rani, V. Kamakshi Prasad and K. Srujan Raju. *Proceedings of the Second International Conference on Computational Intelligence and Informatics*: ICCII 2017 Paperback – Jul 24 2018.

[34] Calum McClelland (May 21, 2018), "The Power of Cellular Technologies in IoT", Retrieved October 2, 2019, Available At https://medium.com/iotforall/the-power-of-cellular-technologies-in-iot-a2a65048bec8

[35] J. Jin, J. Gubbi, S. Marusic, and M. Palaniswami. "An information framework for creating a smart city through the internet of things." *IEEE Internet of Things Journal*, vol. 1, pp. 112–121, 2014.

[36] M. Leo, F. Battisti, M. Carli, and A. Neri. "A federated architecture approach for internet of things security." In *Euro Med Telco Conference (EMTC), Naples.* pp. 1-5, 2014.

[37] D. Zegzhda. and T. Stepanova. "Achieving internet of things security via providing topological sustainability." In *Science and Information Conference (SAI), London.* pp. 269-276, 2015.

[38] P. K. Manadhata and M. W. Jeannette. "An attack surface metric Software Engineering." *IEEE Transactions*, vol. 37.3, pp. 371-386, 2014.

[39] K. D. Soumya and B. Christian. "Securing datatweet IoT architecture elements." pp. 1-3, 2014.

[40] N. C. Gaitan, V. G. Gaitan and I. Ungurean. "Gradual development of an IoT architecture for real-world things." *2015 IEEE European Modelling Symposium*, pp. 344-349, 2015.

[41] Andrea Zarella and Lorenzo Vangelista. "Internet of things for smart cities." *IEEE Internet Things*, vol. 1, pp. 22-32, 2014.

[42] S. Raza, S. Dequenne, T. Chung, T. Voigt and U. Roedig. "Securing Communication in with compressed IPsec." *DCOSS. IEEE*, pp. 1-8, 2011.

[43] A. Juels. "RFID security and privacy, a research survey." *IEEE Journal on Selected Areas in Communications*, vol. 24, pp. 381- 394, 2006.

[44] D. S. G. Lessa, V. T., da, C. R. G., Guimarães, L. Z. Granville and L. M. R.Tarouco. "A DTLS-based security architecture for the Internet of Things." *IEEE Symposium on Computers and Communication (ISCC), Larnaca*, pp. 809-815, 2015.

[45] D. Singh, G. Tripathi, and A. J. Jara. "A survey of internet-of-things, future vision, architecture, challenges and services." *Proc. IEEE World Forum on Internet of Things*, pp. 287–292, 2014.

[46] M. Ma, P. Wang, and C. H. Chu. "Data management for an internet of things, challenges." In *IEEE International Conference on and IEEE Cyber, IEEE, 2013.*

[47] S. Raza, L. Seitz, D. Sitenkov, and G. Selander. "S3K, Scalable security with symmetric keys—DTLS key establishment for the internet of things." *IEEE Transactions on Automation Science and Engineering*, vol. 13, pp. 1270-1280, 2016.

[48] W. Shi. "Edge computing, Vision and challenges." *IEEE Internet of Things*, vol. 3, pp. 637-646, 2016.

[49] P. P. Ray, "A survey on Internet of Things architectures". *Journal of King Saud University – Computer and Information Sciences, 2016*, Retrieved February 23, 2020, Available At http://dx.doi.org/10.1016/j.jksuci.2016.10.003

[50] Ikenna Uzoma Ajere and Charles Ikerionwu, 'A Survey of Wireless Communication Technologies for IoT-based Healthcare Systems', *African Journal of Computing & ICT*, Vol. 12, No. 2, pp. 1-18, 2019.

[51] Curtin University, "*IoT World Forum – Barcelona"*, Cisco Video Portal. Retrieved February 23, 2020, Available At https://video.cisco.com/detail/video/2902033808001/iot-world-forum---barcelona?autoStart=true&q=barcelona

[52] Rita Sharma, "Top 15 Sensor Types Being Used Most By IoT Application Development Companies", Retrieved March 3, 2020, Available At https://www.finoit.com/blog/top-15-sensor-types-used-iot/

[53] AVSystem (August 27, 2019), "Top Sensor Types Used in IoT", Retrieved March 3, 2020, Available At https://www.avsystem.com/blog/iot-sensors-iot-actuators/

[54] K. Mekki, E. Bajic, F. Chaxel, F. Meyer, A comparative study of LPWAN technologies for large-scale IoT deployment, ICT Express (2018), https://doi.org/10.1016/j.icte.2017.12.005

[55] Rashmi Sharan Sinha, Yiqiao Wei, Seung-Hoon Hwang, "A survey on LPWA technology: LoRa and NB-IoT", ICT Express, 1 March 2017.

[56] Experts at DEKRA, Jun 20, 2017 "Smart Home Protocols Explained Thread, Zigbee, Z-Wave, KNX and More", Retrieved March 16, 2020, Available At https://medium.com/iotforall/smart-home-protocols-thread-zigbee-z-wave-knx-and-more-71efa4b410e1

[57] Jie Lin, Wei Yu, Nan Zhang, Xinyu Yang, Hanlin Zhang, and Wei Zhao, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications", IEEE Internet of Things Journal, Vol. 4, No. 5, October 2017

[58] GSM Association, July 2014, "Understanding the Internet of Things (IoT)", Connected Living, www.gsma.com.

[59] Shanzhi Chen, Hui Xu, Dake Liu, Bo Hu, and Hucheng Wang, "A Vision of IoT: Applications, Challenges, and Opportunities With China Perspective", IEEE Internet of Things Journal, Vol. 1, No. 4, August 2014 349

[60] Bill Chamberlin (August 26, 2015), "An Intelligent Internet of Things = A Smarter Planet
", Retrieved March 26, 2020, Available At http://www.billchamberlin.com/building-a-smarter-planet-through-an-intelligent-internet-of-things/

[61] Rachita Kansal, 2018, "A Survey on Internet of Things: Related Future Technologies, Applications, Challenges and Security Risks", *IJEDR*, Volume 6, Issue 4.

Table 2: Types of data collected, sensors, Applications and IoT devices involved

S/N	TYPE	SENSORS	APPLICATIONS	IoT DEVICES
1	Sound, audio and acoustics	ultrasonic sensor, transceivers	Detecting sounds, speech recognition, measurement and location of echo, detection of presence or absence of objects and measurement of distance	Cameras, headsets, speakers
2	Temperature and thermal	Galvanic skin response sensor, infrared sensor, Thermistors, Pyrometer, Thermocouple [52]	Detecting temperature values [53] and amount of heat	Heaters, Refrigerators, Air conditioners, Cameras, wearables, smart home, connected vehicles
3	Motion and Orientation	Accelerometer, Gyroscope	Detecting motion of objects [52], measuring acceleration and reacting to velocity, sense rotation and change in orientation, camera stabilization, 3-D character animation, sports science, tracking in mobile games	Video and mobile games, smartphones, electric keyboard, Smart buildings [53]
4	Optic, light and imaging	Photoresistors, Photodiodes, Phototrasistors,	Detecting distance, absence or presence of	cameras [52], webcams, smartphones

		Image sensor for HD video data.	objects, converting light into a signal and vice versa, measuring various outputs using light, thermal imaging, video images	
5	Proximity, position and presence	Inductive sensor, Capacitive sensor, Photoelectric sensor, Ultrasonic sensor [52], GPS receiver	detecting height and width, determining the distance between objects [53], sensing UV index and ambient light, long range proximity, detecting heart rate or pulse, motion with 2-D or 3-D gestures, providing positional feedback	wearables, cameras, smartphones, game consoles, connected vehicles
6	Pressure and force	Piezoresistive transducers	detecting touch and contact pressure, sensing pressure applied [52], measuring force and weight, virtual reality, gesture recognition, video and mobile gaming	cameras, smart home, security devices, touch screen devices
7	Flow of liquid, chemical and gas	Chemiresistor, Breathalyzer [52], Hygrometer	detecting room humidity, measuring the flow of a liquid or gas, sensing and monitoring dangerous chemical elements [52]	cameras, smartphones, smart home, security systems, connected vehicles, wearables

			(carbon monoxide, radiation)	
8	Humidity/Moisture	Hygrometer	For measuring the amount of water vapour in air [52]. Applied in agriculture, supply chain, environment monitoring, health monitoring	HVAC devices [53].

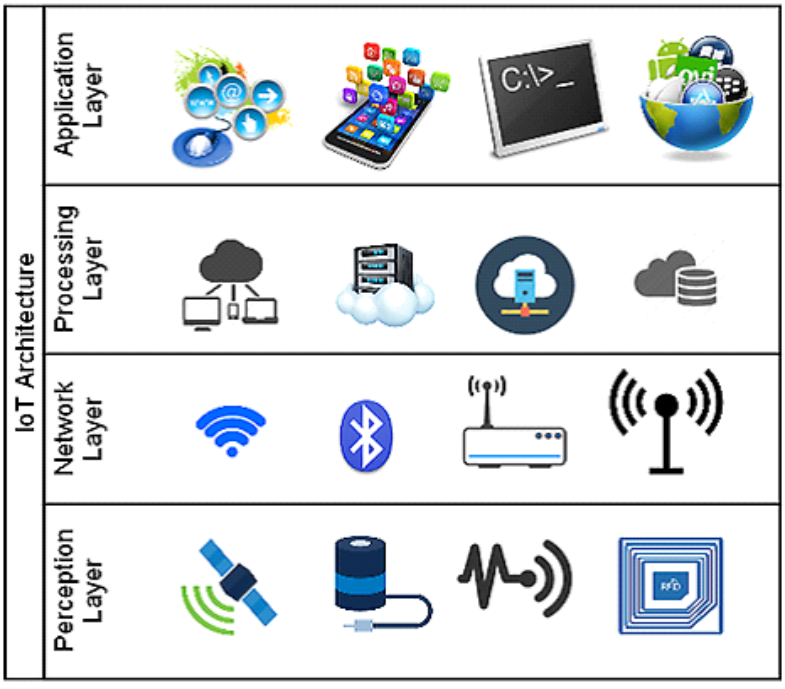

Figure 1. IoT Architecture [17]