International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 4 Issue 3, April 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Insight into IoT Applications and Common Practice Challenges

Lubna Alazzawi, Jamal Alotaibi

Electrical and Computer Engineering Department, Wayne State University, Detroit, Michigan, USA

ABSTRACT

IoT caused a revolution in the technological world. Not only is the IoT related to computers, people or cell phones but also to various sensors, actuators, vehicles, and other modern appliances. There are around 14 billion interconnected digital devices across the globe i.e. almost 2 devices per human being on earth. The IoT serves as a medium to connect non-living things to the internet to transfer information from one point to another in their community network which automates processes and ultimately makes the life of human beings convenient. The subsequent result of amalgamating internet connectivity with powerful data analysis is a complete change in the way we humans work and live. The most vital characteristics of IoT include connectivity, active engagement, sensors, artificial intelligence, and small device use. All of this creates many challenges that need to be solved to keep this technology to continue expanding. In this paper, we have identified various applications of IoT based on recent technological and business trends and highlighted the existing challenges faced by IoT which need to be addressed considering the exponential acceptance of the concept globally and the way those challenges had been addressed in the past. We have also made a few comments on the way such challenges are being attempted to be resolved now. This paper presents the current status Internet of Things (IoT) in terms of technical details, and applications. Also, this paper opens a window for future work on the historical approach to study and address IoT challenges.

KEYWORDS: *IoT, challenges, applications, IoT architecture, computing devices, connectivity, security, smart city*

How to cite this paper: Lubna Alazzawi | Jamal Alotaibi "Insight into IoT Applications and Common Practice Challenges" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-4 | Issue-3, April 2020, pp.42-49, URL: www.ijtsrd.com/papers/ijtsrd30286.pdf

IJTSRD30286

1. INTRODUCTION

The industrial revolution fortified the idea of a globally connected world paving the way for the internet. Although there was a considerable rate at which computers and related accessories were connected to the internet, there was still a lack of sufficient information which could drive the world towards a much safer, efficient global machine. It was the time when very simple objects which generated information could be used to monitor and control things remotely is now known as the Internet of Things (IoT)[1]-[4]. The term IoT was given by Kevin Ashton in 1999 [5]. The idea has been straightforward yet immensely powerful. It focused on connecting things that were not connected before, such as engines, sensors, personal machines, industries, etc.

In general, the entire world became connected via the Internet platform. This idea was also presented in a refined way by Cisco which projects there would be around 500 billion devices connected to the Internet by the year 2030. Cisco predicts this will lead to the rise of smart networks, interconnected devices generating bulk of data that IoT applications use to bundle, analyze, and deliver insight, which can help drive well-informed decisions and actions[6][7].

Fig. 1 illustrates the interconnection between different technologies that together make up the concept of IoT [8].

In this paper, the topmost prominent and fast-growing IoT applications are mentioned, including Smart Spaces, Transport, Industrial IoT (IIoT), Machine to Machine and Artificial Intelligence (M2M & AI), Healthcare, Consumer Electronics, Retail, and Agriculture.

With a bigger network of devices come bigger opportunities and challenges. Also, in this paper, many of these challenges, which are still relevant today but not commonly mentioned in many publications, are addressed. Some of these challenges include connectivity, Centralization, Availability and Reliability, Scalability and Interoperability, Longevity and Upgrades, Network Latency, Energy Consumption, Regulations and Standardizations, Privacy, and Security.

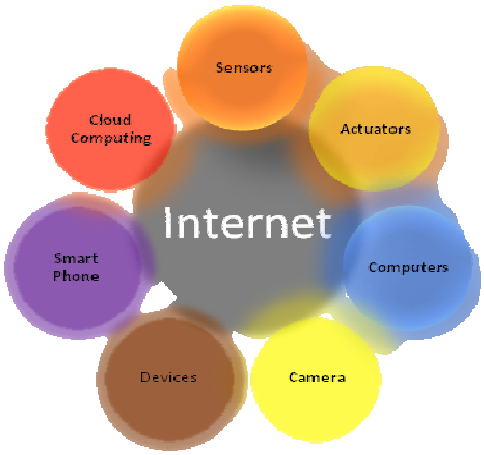

Fig. 1 Illustration of the concept of IoT

Following the introduction, the paper consists of the following sections: Section 2 discusses the related work. Section 3 describes the need for IoT. Section 4 describes the IoT layers. Section 5 presents the challenges facing IoT. Finally, the paper is concluded and ground for future works is laid in section 6.

2. Related Works

In this section, we present an insight into a multitude of research efforts that attempted to classify IoT applications and the challenges they face from different perspectives. The collated background could be envisioned as the basis for future research in IoT arena.

Mohammed et al. [9] proposed the classification of IoT services along two dimensions: relationship with the entity and based on the life cycle. The first dimension consists of: low level; resource; entity; and integrated services. Service life cycle dimension includes deployable; and operational services.

Mandal et al.[10] proposed IoT application (alternatively a scenario) classification framework based on the components participating in the scenario. Components included any combination of sensors, actuators, display, controller, complex device, web service, and/or human being. An application represents the dynamics of executing interactions among its participating components. The research specified levels of interaction between components, levels of data processing, and levels of automation.

Fuqaha et al. [11] classified IoT applications based on their market direction: horizontal or vertical. The research perceives smart objects along with their supposed tasks to constitute domain specific applications (vertical markets) while ubiquitous computing and analytical services form application domain independent services (horizontal markets). So, every domain specific application is considered interacting with domain independent services, whereas in each domain sensors and actuators communicate directly with each other. Senet et al. [12] identified prominent IoT application areas almost a decade ago. Sen conceives aerospace and aviation industry to resolve the problem of suspected unapproved parts (SUP) by using RFID technology for tagging aircraft parts. Sen also identified a potential of IoT to create new services for telecommunications industry by merging of diverse telecommunication technologies. Insurance industry can benefit vehicle owners by providing technology able to record acceleration, speed, and other parameters, and communicate this information to their insurer to get a cheaper rate or premium. In the following sections, we focus on various IoT applications and their importance.

3. Need for IoT

IoT with its recent boom has seen a multitude of devices being connected for different categories of applications and will continue to see a rise in its focus on these areas.

According to IoT analytics[1], most of the IoT projects were identified in smart city (367 projects), followed by industrial settings (265) and connected building IoT projects (193). Details of the above statistical information can be found in Fig. 2.

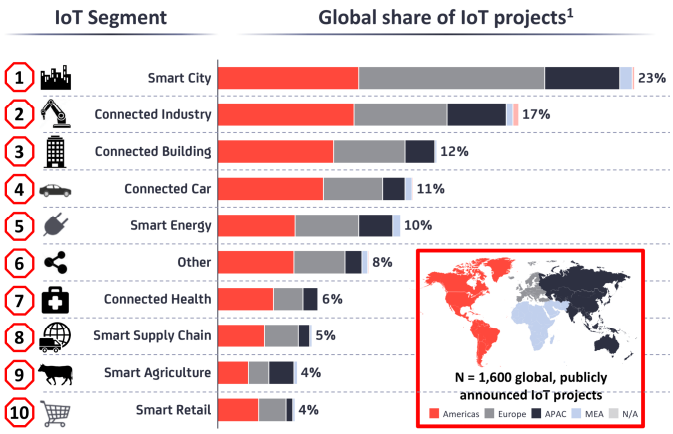

Fig.2 IoT ANALYTICS reported top 10 IoT segments in 2018

In their comparison to 2016 ranking, smart city (driven by government and municipality-led initiatives) has surpassed Connected Industry as the number one IoT segment of identified projects while Connected Building (driven by widespread uptake of building automation solutions that increase operational efficiency and reduce costs) has climbed four places to become the third biggest IoT segment.

Based on current research and market analysis valuation of IoT application domains, we dedicate this section to better understand some prominent domains of IoT, as depicted in Fig. 3, and to emphasize the importance of IoT in today's world.

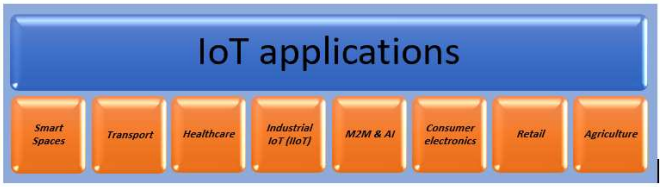

Fig. 3 Applications of IoT

3.1. Smart Spaces

Smart spaces projects mainly deal with the improvement and ease of human lifestyle by introducing automated and intelligent decision-making capabilities in private and public spaces. This can be further classified into smart homes, smart public spaces, and smart cities as shown in 0. A smart home is an application that has seen a good level of acceptance and success. It is a home which is equipped with sensors and actuators which are connected to the internet and controlled by a remote IoT application for monitoring and control of the house environment. Intelligent lighting, voice-based AI, security, entertainment, and energy management are some of the potential needs of IoT in smart homes.

Similar to smart homes is the smart public spaces application with the main difference being the setting of the application. Smart public spaces could be buildings, public-transport stations, walkways, roadways, traffic signals and networks, CCTV monitoring, smart public lighting control, or energy management. The smart city application is based on an integration of IoT in all public spaces in symbiosis to

[1]IOT ANALYTICS is a leading provider of market insights and strategic business intelligence for the Internet of Things (IoT), M2M, and Industry 4.0.

monitor and control the city as a single organism. Many countries are waking up to this idea of smart cities [13][14].

Fig. 4 IoT for smart spaces illustration

3.2. Transport

Intelligent Transport Systems (ITS) is the application of computer technology to the transport sector. ITS systems gather data about the transport system, process it, and then use the processed data to improve the management of the transport system, and/or to provide the transport user with more and better information on which to base their transport decisions [15]. It can help to tackle congestion, pollution, poor accessibility and even social exclusion. It can also help to reduce journey times and improve reliability – either in actuality, or simply by changing people's perceptions. And it can improve the efficiency with which transport systems function. Many applications of ITS are already in place for speed and incident detection, parking management, fleet and freight management, traffic signal control, tolling and access control, trip planning.0 illustrates the potential areas of implementation for ITS applications.

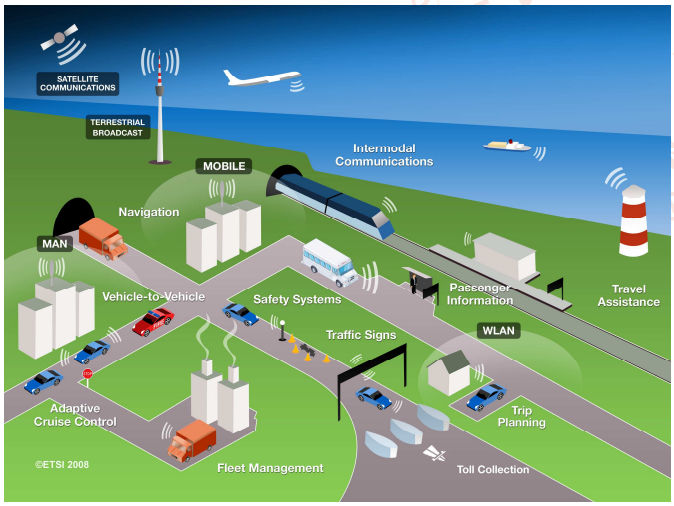

Fig.5 ITS Application Roundup[2]

Vehicular ad-hoc network (VANET) is a type of network that is created from the concept of establishing a network of cars for a specific need or situation, and providing Vehicle-to-Vehicle (V2V), Vehicle-to-Roadside, (V2R) and Roadside-to-Vehicle (V2R) Communications (See Fig. 6).

VANETs play a significant role in the establishment of ITSs. VANETs have now been established as reliable networks that vehicles use for communication purposes on highways or urban environments. Along with the benefits, there arise a large number of challenges in VANET such as provisioning of QoS, high connectivity and bandwidth and security to vehicle and individual privacy [16].

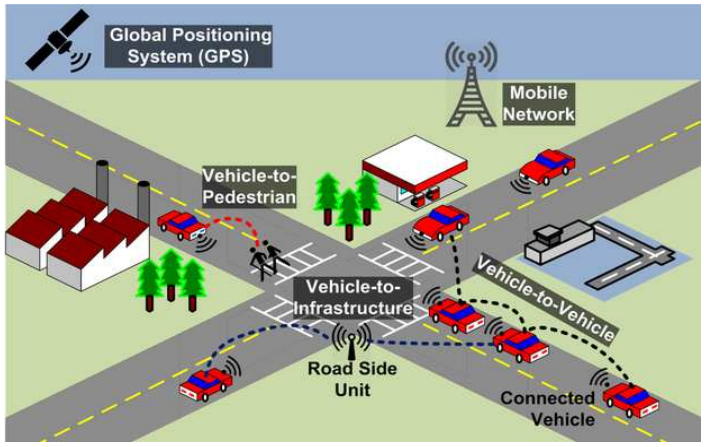

Fig. 6 VANET Main Components[3]

3.3. 2020Industrial IoT (IIoT)

IIoT is one of the fastest growing applications of IoT. It is considered as the inception of 4th Industrial Revolution. The Industrial IoT plans to take industrial or factory automation from an isolated factory to globalization of enterprises with remote control and monitoring made available with the help of the internet replacing legacy technologies. This development was focused to increase the speed of data transmission, centralize operations and control, make data analysis easier, support preemptive maintenance, uniform communication protocols and increase the efficiency of the overall manufacturing unit [17]. The industrial internet is a topic of concern for many industries and is often referred to as Industrial Internet of Things (IIoT). It is entitled industrial engineering with sensor technology including many types of sensors, software and big data analytics to create smart and brilliant machines [19]. The research leaders in the domain of IoT, like Cisco or Gartner, see the IIoT as the highest potential concept, and it has not reached all the industries as smart homes and wearable devices. IIoT holds immense capacity for fulfilling quality control and sustainable development. Applications like tracking the goods, real-time information exchange about the inventory levels among various suppliers and retailers will very well improve the efficiency of supply chains.

3.4. M2M & AI

Machine to Machine (M2M) learning and Artificial intelligence (AI) have become so intelligent that they are capable of making root level, small decisions so intelligently and that too without human involvement. The rise of IoT has opened many channels for AI and M2M applications and inversely they have found IoT applications for their support and development. This mutual relationship of the two technology segments creates an array of possibilities in smart cars, robotics, talking machines, etc. which would be capable of independently taking decisions [20]. Google's self-driving car is a good example of IoT with M2M & AI. In a comprehensive, intelligence world like today's, devices work in order to aid people in executing their day-to-day activities

[2] The European Telecommunications Standards Institute (ETSI), 2008

[3]https://www.egypt-business.com/ticker/details/1631-analysis-on-intelligent-transportation-system-market-research-report/50750

conveniently [21] and in a natural way using the information and intelligence that is concealed in the network connected devices [22]. It is distinguished by the following systems of characteristics –first, numerous devices connected through network are integrated into an environment; second, devices can be aware of an individual and their situational context; third, they can be altered as per an individual's necessity; fourth, they can transform if requested by the user; fifth, they can be prepared for an individual's desires effortlessly.

3.5. Healthcare

A very important and slowly developing application of IoT is in the healthcare and fitness sector. The concept of telemedicine has been crudely tested by doctors around the world by remotely controlling medicinal devices for medical monitoring and operations. But IoT has leveled up the situation. The connection between the health care system and smart medical devices can prove to be a great advantage, not only for the companies but also for the well-being of general public (see 0).

IoT in healthcare has an intention to empower people to live a safe and healthy life by wearing devices which are connected through the internet. The data collected will help with personalized analysis and a solution to an individual's health plan to combat a disease. A lot of research and pilot applications are being tested in this sector which will enable doctors to make better diagnosis and treatment to patients. Some of the prominent applications include monitoring of patient's health and using the collected data to analyze and generate models for better diagnosis and treatment. Intelligent medicinal systems collect patient data, process it, and administer medicines according to AI decisions [18].

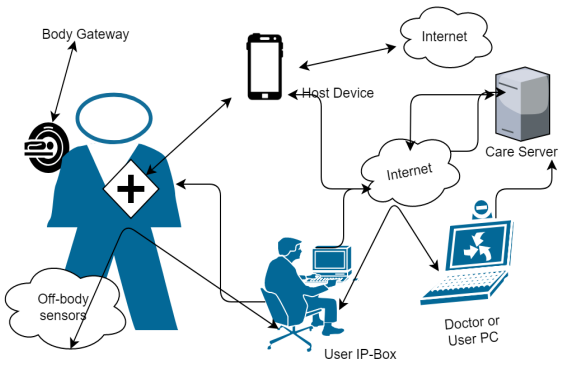

Fig. 7 Smart healthcare concept

3.6. Consumer electronics

Electronic wearables have become a popular trend in the fashion and fitness industries. Their integration with the internet opened up a whole new world of children tracking and safety devices, entertainment and fitness applications, professional development, etc. A bigger picture of this is seen in terms of wearable electronic wallets and personal IDs [23].

The wearable continue to exist as a hot topic too among potential IoT applications and there are devices with the capability to collect particular data and information about the users and are formed of sensors and required software. This collected data is later pre-processed to get the necessary information about the user. The requirement for the IoT technology enabled wearable applications is they should be highly energy efficient or consume ultra-low power and should be small sized.

3.7. Retail

The IoT has got immense opportunity in the retail sector. IoT endows an eventuality to retailers to get in touch with the customers to enhance the in-store experience. Smartphones will be used as a medium by retailers to stay connected with their customers even when not present in the store. Using the Beacon technology and the smartphones, the retailers can interact with and serve the consumers preferably. They can also track the consumer's path via a store and improvised store layout and position the premium products in dense traffic areas.

3.8. Agriculture

The smart farming is an often ignored over undermined business opportunity considering IoT as it does not exactly fit in the well-known categories like industrial, health, or mobility. However, as the farming operations are remote and requires monitoring huge quantity of livestock, the IoT could metamorphose the way farming is done. But this opinion has not yet been considered at a large scale. Farmers use meaningful intuition from the data collected to gain a meaningful return on the investment.

The sensing for soil nutrients and moisture, water usage control for the growth of plant and identifying custom fertilizer are some easy and basic uses of IoT. It can be realized that how IoT can influence all these powerful and potential applications.

4. Internet of Things Layers

As the IoT is handling millions of connected devices through the Internet, it requires a flexible layered structure or architecture [24]. The IoT's five-layered model in depicted in 0 which is most common, simple and extensively used.

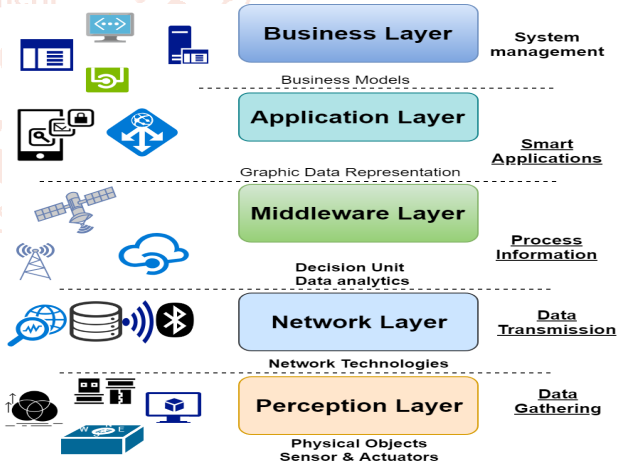

Fig. 8 The Internet of Things (IoT) Layers

4.1. Perception Layer

In the IoT architecture, the perception layer, often called the objects layer, is the first layer from the bottom, as shown in 0. It consists of various types of tangible devices that are responsible for data collection and acting in that manner, like temperatures, locations, object identifiers and, humidity measurements. The significant aspects of this layer include managing power consumption and unidirectional or bidirectional communication.

4.2. Network Layer

The second layer in IoT architecture is the network layer. As the technologies in this layer are used to transform the

traditional sensors present in the perception layer into smart and connected nodes, this layer is often referred to as infrastructure layer. The network layer technologies add recognition over the network connection (either internet or LAN) to the nodes which allows them to securely communicate with each other.

The various technologies in this layer can also be found in the first three layers of the IP suite (TCP/IP). Due to the conditioned capabilities of most IoT nodes, in order to ensure interoperability among the IoT devices, there is a need for scalable and efficient routing techniques. Pay attention that many of IoT technologies have applications in WSNs or machine to machine (M2M) communications but were certainly improvised to meet IoT requirements. Many modern devices use multiple technologies as in smart watches, which often have NFC, Wi-Fi, Li-Fi, Bluetooth, etc. in a single device [17][27]. On the basis of functionality of various technologies in the network layer, they are classified into various enabling technologies.

I. Identification

In order to enable intercommunication between nodes, a node is assigned a recognizer as soon as it connects to the network. This process of identification is important as it will limit the excessive usage of bandwidth by ensuring only the identified nodes communicate. Names and addresses are assigned to devices which makes it easier to locate them in the dense network. To identify a node easily and its functions, the nodes are named in a structured manner using specific naming conventions.

II. Communication

An identified node can communicate with other connected nodes or with the backend servers. In spite of that, depending on the capabilities of node, an appropriate communication medium is selected. Pay attention that nodes can communicate horizontally or vertically.

III. Security

The nodes in a network have limited capabilities and there are numerous nodes like these, security is an important and challenging task as a successful attack can cause severe damage to the system (for example DDoS attacks) [33]. The security may not be built into different communication technologies. Hence, various layers should provide improved security mechanisms in order to minimize the probability of attacks. Due to unsafe communication between the layers, lightweight security mechanisms are required for safe and secure communication as the attacks can occur in this layer.

IV. Routing

Knowing the destination address is not sufficient for a node to transfer the data, there is need to know the route as well. As many nodes could be connected in an ad-hoc manner, adept routing is critical in most of the IoT environments. As the capabilities of the nodes are limited, they should know the best route to be taken and to answer this problem, a special routing protocol was introduced for these environments. IPv6 is a standard routing protocol for inferior power [27]. This protocol was proposed to support dissimilar types of links, such as IEEE 802.15.4, and common traffic types, including one-to-one, many-to-one, and one-to-many. The protocol is a set of Destination-Oriented Directed Acyclic Graph (DODAG). In this type of graph, a node knows its parent and at least one path to its root node. The nodes exchange RPL messages to maintain the route to the root which is always available.

4.3. Middleware Layer

The middleware layer receives data from the network layer. It is present to manage services and data storage functionality of an IoT system. It also performs information processing and based on the results of these computations; a decision is automatically taken. The output is then transferred to the application layer.

The middleware layer is the core of (IoT) environment and can be compared to the application layer in the TCP/IP protocol. The technologies belonging to this layer are often supported by IoT platforms. This layer plays a role of decoder sort of thing. Based on the name and address, the layer enables services and programmers to communicate with miscellaneous objects, immaterial to their specific hardware setup. Depending on the received data, this layer makes judgments, and delivers demanded services.

4.4. Application Layer

The final presentation of the data is performed by this application layer which is accountable for providing demanded services to IoT users via simple interface without bothering how service requests are processed in the underlying layers.

The IoT users can request and access service (for example, tracking and managing vehicles or reading or setting temperature conditions remotely) using many platforms (for example smartwatches, laptops, and smartphones) through applications or web portals. On the basis of the IoT scenario, this layer can be categorized into four main classes as described below.

I. Identity Concerned Services

The identity concerned services are embedded to a node and a reader device called Radiofrequency Identification RFID device. These services can be either active or passive. As these services keep track of the numerous devices in large deployments in IoT applications, they are extremely important. Example of such a service is a package-tracking application[26].

II. Information Concentricity Services

The sensory measurement data collected from various sensors and networks which is to be processed and summarized to the IoT application is performed by concentricity services. An example for such a type of service is load distribution among smart grids.

III. Collaborative Cognizant Services

The layer above information concentricity services which is used to take decisions about the received data is the collaborative cognizant services. This type of service can be found in smart manufacturing, smart homes, smart agriculture, and among other applications. For instance, in a smart home, there is a security system containing thermostats to enhance the safety and security of the home.

IV. Universal Services

These services advance the collaborative services a level up by offering ubiquitous access to information anytime. And

because of such service type, this service is most profitable in IoT environment. The access and control can be set up using a smart device like a smartphone, or a computer. Example for such services is smart cities.

4.5. Business Layer

The business layer, as the name implies, is a service offered to make money out of the services provided. In this layer, service data and IoT environmental data, i.e. the business models, graphs, and flowcharts, can be accessed. This type of services is more equipped with business related tools. The output of layers so far is analyzed by this layer to improvise the services and enhance user privacy by providing users with power to design, monitor, analyze, implement, evaluate, and develop new IoT systems.

5. Challenges Facing IoT

Every new philosophy or new technology faces lots of challenges upfront, and IoT was also not exempt from them. Some of these challenges are still pertinent while others have been addressed to a great extent. On a broader level, the issues are related to security, privacy and infrastructure related challenges. However, this paper attempts to mention the most important uncategorized challenges to take the reader's attention to the roots of the problem listed.

Fig. 9 Challenges Facing IoT

5.1. Connectivity

This challenge refers to the connectivity of network-dependent remote-location solutions that deploy sensors and control devices that require connectivity to the internet. The biggest hurdle in this aspect is the dependency on mobile networks for internet connection.

It is a known fact that there isn't well-established universal connectivity of mobile networks' coverage and even lesser for internet-based bands like 2G, 3G, 4G/LTE or higher bands. Connectivity can be evaluated at various levels like Frequency allocations, MAC Protocols, Network Protocols, Transport Protocols, and Mobility Protocols. This challenge has been resolved to some extent by utilizing the lower bands of cellular networks that have larger coverage areas but limit the scale and speed of data that can be transmitted over the network [32].

5.2. Centralization

In the wake of the development of centralized computing and storage systems into cloud computing, a lot of IoT solutions and service providers tend to subscribe to these systems with or without the consent of their customers.

The cyber-attacks that have been witnessed in recent years have shown the vulnerability of centralized systems which could jeopardize the information sitting on these systems and bring forth issues of data privacy and security. A lot of efforts are being made to resolve this challenge as it is not unique to IoT but to many other services that depend on these systems like banking, hospitality, logistics, defense, etc. [28].

5.3. Availability and Reliability

The availability of the IoT must be realized in the hardware and software levels to provide sustained services for customers. The availability of software refers to the ability of the IoT applications to provide services for everyone at different places simultaneously. Hardware availability refers to the existence of devices all the time that are compatible with the IoT functionalities and protocols [30]. Redundancy for critical devices and services is one solution to achieve high availability of IoT services.

The reliability refers to the proper working of the system based on its specification [31]. Reliability aims to increase the success rate of IoT service delivery, and it has a close relationship with availability as by reliability, accessibility to information and services can be assured.

5.4. Scalability and Interoperability

The scalability of the IoT refers to the ability to add new devices, services and functions for customers without negatively affecting the quality of existing services [30].

End-to-end interoperability is yet another challenge for the IoT due to its inherent nature of embedding heterogeneous components that belong to different platforms and layers. Interoperability should be considered by both application developers and IoT device manufactures to ensure the delivery of services for all customers regardless of the specifications of the hardware platform that they use.

5.5. Longevity and Upgrading

Since the advent of connected devices over private networks and eventually the internet, thousands of devices and objects remain hooked up to the present IoT services and solutions sector. These legacy devices which are still functional pose challenges in data interpretation due to their outdated protocols. Some of these devices consume a lot more energy compared to their modern competitors, risking unexecuted failures which could prove disastrous if they are a critical part of a safety system. Another aspect of the sensors and objects connected on the IoT is their longevity in terms of product life-cycle and energy sustainability. A lot of these devices are battery powered and give rise to challenges of device blackouts. These challenges can be resolved with properly planned replacement of legacy devices with modern ones, via technologies such as development of 'over the air' or 'over the internet' updateable devices, better product design with longer life spans, and wireless over the air electricity.

5.6. Network Latency

This challenge normally arises with the difference in speeds of data transmission, network handshakes, and cloud

computing systems that create programmed delays in data flow due to heavy traffic and network issues.

A seamless and quick flow of data would require higher speeds of operation of cloud computing systems, predetermined resolution of network issues, and data traffic hurdles which involve a lot of cost and energy investment. Some solutions have been proposed to resolve this challenge. The most feasible ones involve private network level AI algorithms that filter and prioritize data and take decisions locally with efficient utilization of the local computing resources while only data with higher priority that needs to be processed on the cloud will be selectively transmitted outside the local network [28].

5.7. Regulations and Standardization

There lies a great deal of confusion among the consumers of IoT products and services due to the diverse range of products, formats of data, data protocols, security protocols, network protocols and integration. The lack of a governmental or non-governmental body to regulate and standardize IoT products and services is the main reason behind this challenge. The world is slowly waking to the call of the future to embrace IoT and the governments of a lot of countries are slowly making attempts to solve this challenge. This challenge can't be completely resolved unless all stakeholders contribute a part to these discussions on regulations and standardizations [28].

5.8. Privacy

This challenge is tied with the data and network security challenges which is mainly concerned about the privacy of the information flowing over public networks. A lot of private information about a person or business entity can be collected without the entity's awareness.

A few of the solutions solve both privacy issues and these challenges. There are solutions that are trying to provide the owner of the data or the end client the control of their data and to selectively choose which data they would like to allow over the internet [29].

5.9. Security

According to IoT analytics, this challenge can be broadly broken down into 4 layers (device, communication, cloud, and application) as depicted in (Fig. 10).

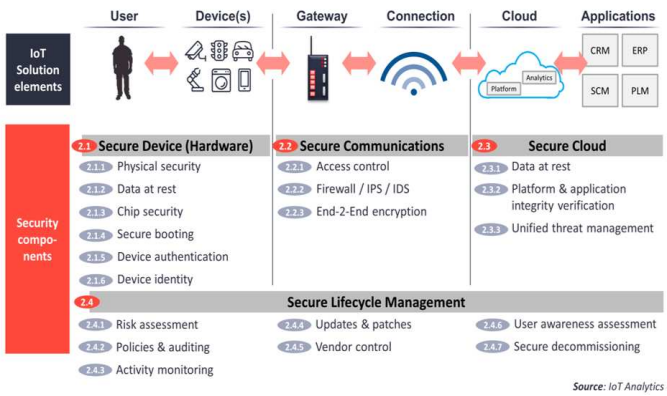

Fig. 10 IoT Security Levels

IoT security spending is on the rise. IoT ANALYTICS released market research depicting IoT security spending to be currently estimated at $703M for 2017 and the fast growing market (Compound Annual Growth Rate-CAGR of 44%) is forecast to become almost a $4.4B opportunity by 2022 (see 0).

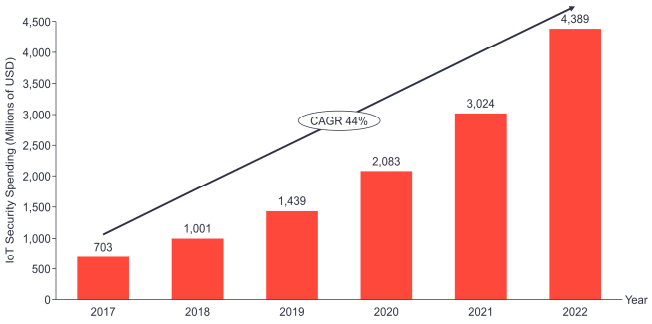

Fig. 11 IoT Security Market Expected Growth

The analysis also shows the most common IoT breaches that happened in the last years. Between 2015-2017 most of the breaches were caused by malware (24%), followed by human's factor "man in the middle" (22%), brute force (18%) and denial of service (15%). Physical tempering with devices and hacking encryption has smaller footprint in reported security breaches.

6. CONCLUSION AND FUTURE WORK

The objectives of this paper were to highlight some important facts about IoT systems with a focus on its applications and open challenges.

The scale of implementation of IoT in today's world creates opportunities for everyone to be part of this coming industrial revolution, leading to many diverse applications, developers, businesses and end users. The diversity of this digital and hardware ecosystem via IoT and the speed of its implementation are creating much vulnerabilities which need to be addressed through a historical analysis of all similar challenges faced by other technological concepts.

In this paper, we surveyed the layer of IoT, classification, ecosystem and applications in this newly emerging area, also highlighted some of the most important challenges. The main theme of this paper is to overview the big-picture to readers of this emerging area.

References

[1] Akan, Ozgur B., Sergey Andreev, and Ciprian Dobre. "Internet of Things and Sensor Networks." *IEEE Communications Magazine* 57.2 2019: 40-40.

[2] Mahmud, Sadi, Safayet Ahmed, and Kawshik Shikder. "A Smart Home Automation and Metering System using Internet of Things (IoT)." *2019 International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST)*. IEEE, 2019.

[3] Sethi, Pallavi, and Smruti R. Sarangi. "Internet of things: architectures, protocols, and applications." *Journal of Electrical and Computer Engineering*", 2017.

[4] Qian, Yi, et al. "The internet of things for smart cities: Technologies and applications." *IEEE Network* 2019: 4-5.

[5] Ashton, Kevin. "That 'internet of things" RFID journal 22.7 2009: 97-114.

[6] Al-Shdifat, Ali, and Christos Emmanouilidis. "Development of a Context-aware framework for the Integration of Internet of Things and Cloud Computing for Remote Monitoring Services." Procedia Manufacturing 16 2018: 31-38.

[7] Lee, In, and Kyoochun Lee. "The Internet of Things (IoT): Applications, investments, and challenges for enterprises." Business Horizons 58.4 2015: 431-440..

[8] Thoma, Matthias, et al. "On IoI-services: Survey, classification and enterprise integration." 2012 IEEE International Conference on Green Computing and Communications. IEEE, 2012.

[9] Mohammed, Farah Hussein, and Roslan Esmail. "Survey on IoT services: classifications and applications." Int J Sci Res 4 2015: 2124-7.

[10] Mandal, Sankalita, et al. "A Classification Framework for IoT Scenarios." International Conference on Business Process Management. Springer, Cham, 2018.

[11] Al-Fuqaha, Ala, et al. "Internet of things: A survey on enabling technologies, protocols, and applications." IEEE communications surveys & tutorials 17.4 2015: 2347-2376.

[12] Bandyopadhyay, Debasis, and Jaydip Sen. "Internet of things: Applications and challenges in technology and standardization." Wireless personal communications 58.1 2011: 49-69.

[13] He, Jianhua, et al. "Multitier fog computing with large-scale IoT data analytics for smart cities." IEEE Internet of Things Journal 5.2 2017: 677-686.

[14] Lynch, Casey R., and Vincent J. Del Casino Jr. "Smart Spaces, Information Processing, and the Question of Intelligence." Annals of the American Association of Geographers 110.2 2020: 382-390.

[15] Heredia, Xavier Calle, et al. "Monitoring System for Intelligent Transportation System Based in ZigBee." 2019 UNSA International Symposium on Communications (UNSA ISCOMM). IEEE, 2019.

[16] ur Rehman, Sabih, et al. "Vehicular ad-hoc networks (VANETs)-an overview and challenges." Journal of Wireless Networking and Communications 3.3 2013: 29-38.

[17] Mumtaz, Shahid, et al. "Massive Internet of Things for industrial applications: Addressing wireless IIoT connectivity challenges and ecosystem fragmentation." IEEE Industrial Electronics Magazine 11.1 2017: 28-33.

[18] Li, Wei, Cheolwoo Jung, and Jongtae Park. "IoT Healthcare Communication System for IEEE 11073 PHD and IHE PCD-01 Integration Using CoAP." KSII Transactions on Internet & Information Systems 12.4 2018.

[19] Arumugam, Senthamiz Selvi, et al. "Accelerating Industrial IoT Application Deployment through Reusable AI Components." 2019 Global IoT Summit (GIoTS). IEEE, 2019.

[20] Mehmood, Yasir, et al. "M2M communications in 5G: state-of-the-art architecture, recent advances, and research challenges." IEEE Communications Magazine 55.9 2017: 194-201.

[21] Farhan, Laith, et al. "A concise review on Internet of Things (IoT)-problems, challenges and opportunities." 2018 11th International Symposium on Communication Systems, Networks & Digital Signal Processing (CSNDSP). IEEE, 2018.

[22] Boire, Richard. "Artificial intelligence (AI), automation, and its impact on data science." 2017 IEEE International Conference on Big Data (Big Data). IEEE, 2017.

[23] Barros, Tiago, et al. "A Multi-Radio Gateway Architecture and Implementation for Consumer Electronics." 2019 IEEE International Conference on Consumer Electronics (ICCE). IEEE, 2019.

[24] Tan, Lu, and Neng Wang. "Future internet: The internet of things." 2010 3rd international conference on advanced computer theory and engineering (ICACTE). Vol. 5. IEEE, 2010.

[25] Khan, Rafiullah, et al. "Future internet: the internet of things architecture, possible applications and key challenges." 10th international conference on frontiers of information technology. IEEE, 2012.

[26] Qu, Youyang, et al. "Privacy of things: Emerging challenges and opportunities in wireless Internet 7of Things." IEEE Wireless Communications 25.6 2018: 91-97.

[27] Perwej, Yusuf, et al. "Some drastic improvements found in the analysis of routing protocol for the Bluetooth technology using scatternet." arXiv preprint arXiv: 2012:1205.3959.

[28] P. Nelson, "Industrial IoT faces big challenges," Network World, 2018.

[29] Jain, Samyak, and K. Chandrasekaran. "Industrial Automation Using Internet of Things." Security and Privacy Issues in Sensor Networks and IoT. IGI Global, 2020: 28-64.

[30] Yaqoob, Ibrar, et al. "Internet of things architecture: Recent advances, taxonomy, requirements, and open challenges." IEEE wireless communications 24.3 2017. 10-16.

[31] Siddiqui, Shams Tabrez, et al. "Security Threats, Attacks, and Possible Countermeasures in Internet of Things." Advances in Data and Information Sciences. Springer, Singapore, 2020. 35-46.

[32] Samuel, S. Sujin Issac. "A review of connectivity challenges in IoT-smart home." 2016 3rd MEC International conference on big data and smart city (ICBDSC). IEEE, 2016.

[33] Román-Castro, Rodrigo, Javier López, and Stefanos Gritzalis. "Evolution and trends in IoT security." Computer 51.7 2018. 16-25.

[34] Ding, Xuefeng, and Jiang Wu. "Study on Energy Consumption Optimization Scheduling for Internet of Things." IEEE Access 2019.

[35] Tabassum, Kahkashan, Ahmed Ibrahim, and Sahar A. El Rahman. "Security Issues and Challenges in IoT." 2019 International Conference on Computer and Information Sciences (ICCIS). IEEE, 2019.