A Brief Survey About Internet of Things (IoT) for Further Explanation

M. Heidarzade Ghareveran, and H. Asharioun, Shahid Beheshti University, Tehran, Iran.

Abstract **_The Internet of Things (IoT) is a dynamic global information network consisting of Internet-connected objects, such as radio frequency identifications, sensors, and actuators, as well as other instruments and smart appliances that are becoming an integral component of the Internet. Over the last few years, we have seen a plethora of IoT solutions making their way into the industry marketplace. Context-aware communications and computing have played a critical role throughout the last few years of ubiquitous computing and are expected to play a significant role in the IoT paradigm as well. In this paper, we examine a variety of popular and innovative IoT solutions in terms of context-aware technology perspectives. More importantly, we evaluate these IoT solutions using a framework that we built around well-known context-aware computing theories. This survey is intended to serve as a guideline and a conceptual framework for context-aware product development and research in the IoT paradigm. It also provides a systematic exploration of existing IoT products in the marketplace and highlights a number of potentially significant research directions and trends.**

Key word: Network, industrial network, internet of things, industrial internet of things.

I. INTRODUCTION

THE Internet of things (IoT) is the network of physical devices, vehicles, home appliances, and other items embedded with electronics, software, sensors, actuators, and network connectivity which enable these objects to connect and exchange data. Each thing is uniquely identifiable through its embedded computing system but is able to inter-operate within the existing Internet infrastructure. Experts estimate that the IoT will consist of about 30 billion objects by 2020. It is also estimated that the global market value of IoT will reach $7.1 trillion by 2020.

Submission date: 01 December 2017, Publication date: 31 January 2018.
Corresponding Author: (e-mail: m.heidarzade@sbu.ac.ir).

The IoT allows objects to be sensed or controlled remotely across existing network infrastructure, creating opportunities for more direct integration of the physical world into computer-based systems, and resulting in improved efficiency, accuracy and economic benefit in addition to reduced human intervention.[1] When IoT is augmented with sensors and actuators, the technology becomes an instance of the more general class of cyber-physical systems, which also encompasses technologies such as smart grids, virtual power plants, smart homes, intelligent transportation and smart cities.

As of 2016, the vision of the Internet of things has evolved due to a convergence of multiple technologies, including ubiquitous wireless communication, real-time analytics, machine learning, commodity sensors, and embedded systems. This means that the traditional fields of embedded systems, wireless sensor networks, control systems, automation (including home and building automation), and others all contribute to enabling the Internet of things.

The concept of a network of smart devices was discussed as early as 1982, with a modified Coke machine at Carnegie Mellon University becoming the first Internet-connected appliance, able to report its inventory and whether newly loaded drinks were cold. Mark Weiser's seminal 1991 paper on ubiquitous computing, "The Computer of the 21st Century", as well as academic venues such as UbiComp and PerCom produced the contemporary vision of IoT. In 1994 Reza Raji described the concept in IEEE Spectrum as "small packets of data to a large set of nodes, so as to integrate and automate everything from home appliances to entire factories". Between 1993 and 1996 several companies proposed solutions like Microsoft's at Work or Novell's NEST. However, only in 1999 did the field start gathering momentum. Bill Joy envisioned Device to Device (D2D) communication as part of his "Six Webs" framework,

presented at the World Economic Forum at Davos in 1999. [2]

The concept of the Internet of things became popular in 1999, through the Auto-ID Center at MIT and related market-analysis publications. Radio-frequency identification (RFID) was seen by Kevin Ashton (one of the founders of the original Auto-ID Center) as a prerequisite for the Internet of things at that point. Ashton prefers the phrase "Internet for things." If all objects and people in daily life were equipped with identifiers, computers could manage and inventory them. Besides using RFID, the tagging of things may be achieved through such technologies as near field communication, barcodes, QR codes and digital watermarking.

In its original interpretation, one of the first consequences of implementing the Internet of things by equipping all objects in the world with minuscule identifying devices or machine-readable identifiers would be to transform daily life. For instance, instant and ceaseless inventory control would become ubiquitous. A person's ability to interact with objects could be altered remotely based on immediate or present needs, in accordance with existing end-user agreements. For example, such technology could grant motion-picture publishers much more control over end-user private devices by remotely enforcing copyright restrictions and digital rights management, so the ability of a customer who bought a Blu-ray disc to watch the movie could become dependent on the copyright holder's decision, similar to Circuit City's failed DIVX. A significant transformation is to extend "things" from the data generated from devices to objects in the physical space. The thought-model for future interconnection environment was proposed in 2004. The model includes the notion of the ternary universe consists of the physical world, virtual world and mental world and a multi-level reference architecture with the nature and devices at the bottom level followed by the level of the Internet, sensor network, and mobile network, and intelligent human-machine communities at the top level, which supports geographically dispersed users to cooperatively accomplish tasks and solve problems by using the network to actively promote the flow of material, energy, techniques, information, knowledge, and services in this environment. This thought model envisioned the development trend of the Internet of things.[3]

Fig. 1. Applications of IoT [3]

II. APPLICATION

The applications for internet connected devices are extensive. Multiple categorizations have been suggested, most of which agree on a separation between consumer, enterprise (business), and infrastructure applications. George Osborne, the former British Chancellor of the Exchequer, posited that the Internet of things is the next stage of the information revolution and referenced the inter-connectivity of everything from urban transport to medical devices to household appliances. The ability to network embedded devices with limited CPU, memory and power resources means that IoT finds applications in nearly every field. Such systems could be in charge of collecting information in settings ranging from natural ecosystems to buildings and factories, thereby finding applications in fields of environmental sensing and urban planning. Intelligent shopping systems, for example, could monitor specific users' purchasing habits in a store by tracking their specific mobile phones. These users could then be provided with special offers on their favorite products, or even location of items that they need, which their fridge has automatically conveyed to the phone. Additional examples of sensing and actuating are reflected in applications that deal with heat, water, electricity and energy management, as well as cruise-assisting transportation systems. Other applications that the Internet of things can provide is enabling extended home security features and home automation. The concept of an "Internet of living things" has been proposed to describe networks of biological sensors that could use cloud-based analyses to allow users to study DNA or other molecules.[4]

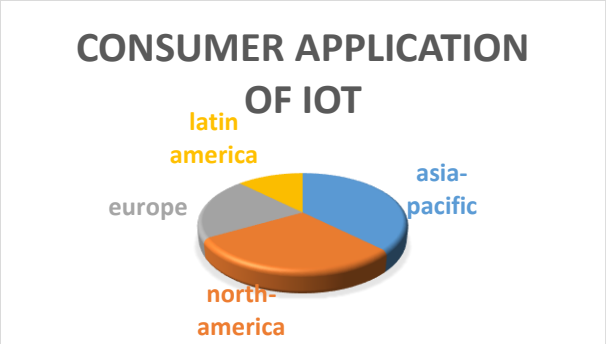

Fig. 2. Consumer application from IoT

III. CONSUMER APPLICATION

A growing portion of IoT devices are created for consumer use. Examples of consumer applications include connected car, entertainment, home automation (also known as smart home devices), wearable technology, quantified self, connected health, and appliances such as washer/dryers, robotic vacuums, air purifiers, ovens, or refrigerators/freezers that use Wi-Fi for remote monitoring. Consumer IoT provides new opportunities for user experience and interfaces. Some consumer applications have been criticized for their lack of redundancy and their inconsistency, leading to a popular parody known as the "Internet of Shit." Companies have been criticized for their rush into IoT, creating devices of questionable value, and not setting up stringent security standards. [4]

A. Smart Home

IoT devices are a part of the larger concept of home automation, also known as domotics. Large smart home systems utilize a main hub or controller to provide users with a central control for all of their devices. These devices can include lighting, heating and air conditioning, media and security systems. Ease of usability is the most immediate benefit to connecting these functionalities. [4] Long term benefits can include the ability to create a more environmentally friendly home by automating some functions such as ensuring lights and electronics are turned off. One of the major obstacles to obtaining smart home technology is the high initial cost. One key application of smart home is to provide assistance for disabled and elderly individuals. These home systems utilize assistive technology to accommodate an owner's specific disabilities. Voice control can assist users with sight and mobility limitations while alert systems can be connected directly to implants worn by hearing impaired users. They can also be equipped with additional safety features. These features can include sensors that monitor for medical emergencies such as falls or seizures. Smart home technology applied in this way can provide users with more freedom and a higher quality of life. A second application of smart home is even more sophisticated. One can guide his or her connected device at home even from far away. If one for example leaves the office, it is possible to tell a connected air conditioner device via smart phone to cool down the house to a certain temperature. Another example would be to use smart devices as for examples Amazon`s Alexa to get the most recent and most important news of the day while cutting the vegetables for the meal you are cooking at the moment. In general, Smart Home devices make life easier at home and give us the possibility to make several things at the same time. [5]

B. Media

Media use of the Internet of things is primarily concerned with marketing and studying consumer habits. Through behavioral targeting these devices collect many actionable points of information about millions of individuals. Using the profiles built during the targeting process, media producers present display advertising in line with the consumer's known habits at a time and location to maximize its effect. Further information is collected by tracking how consumers interact with the content. This is done through conversion tracking, drop off rate, click through rate, registration rate and interaction rate. The size of the data often presents challenges as it crosses into the realm of big data. However, benefits gained from the data stored greatly outweighs these challenges. [6]

C. Infrastructure Management

Monitoring and controlling operations of urban and rural infrastructures like bridges, railway tracks, on- and offshore- wind-farms is a key application of the IoT. The IoT infrastructure can be used for monitoring any events or changes in structural conditions that can compromise safety and increase risk. It can also be used for scheduling repair and maintenance activities in an efficient manner, by coordinating tasks between different service providers and users of these facilities. IoT devices can also be used to control critical infrastructure like bridges to provide access to ships.Usage of IoT devices for monitoring and operating infrastructure is likely to improve incident management and emergency response coordination, and quality of service, up-times and reduce costs of operation in all infrastructure related areas. Even areas such as waste management can benefit from

automation and optimization that could be brought in by the IoT.[6]

D. Manufacturing

Network control and management of manufacturing equipment, asset and situation management, or manufacturing process control bring the IoT within the realm of industrial applications and smart manufacturing as well. The IoT intelligent systems enable rapid manufacturing of new products, dynamic response to product demands, and real-time optimization of manufacturing production and supply chain networks, by networking machinery, sensors and control systems together. Digital control systems to automate process controls, operator tools and service information systems to optimize plant safety and security are within the purview of the IoT. But it also extends itself to asset management via predictive maintenance, statistical evaluation, and measurements to maximize reliability. Smart industrial management systems can also be integrated with the Smart Grid, thereby enabling real-time energy optimization. Measurements, automated controls, plant optimization, health and safety management, and other functions are provided by a large number of networked sensors. The term industrial Internet of things (IIoT) is often encountered in the manufacturing industries, referring to the industrial subset of the IoT. IIoT in manufacturing could generate so much business value that it will eventually lead to the fourth industrial revolution, so the so-called Industry 4.0. It is estimated that in the future, successful companies will be able to increase their revenue through Internet of things by creating new business models and improve productivity, exploit analytics for innovation, and transform workforce. The potential of growth by implementing IIoT will generate $12 trillion of global GDP by 2030. While connectivity and data acquisition are imperative for IIoT, they should not be the purpose, rather the foundation and path to something bigger. Among all the technologies, predictive maintenance is probably a relatively "easier win" since it is applicable to existing assets and management systems. The objective of intelligent maintenance systems is to reduce unexpected downtime and increase productivity. And to realize that alone would generate around up to 30% over the total maintenance costs. Industrial big data analytics will play a vital role in manufacturing asset predictive maintenance, although that is not the only capability of industrial big data. Cyber-physical systems (CPS) is the core technology of industrial big data and it will be an interface between human and the cyber world. [6] Cyber-physical systems can be designed by following the 5C (connection, conversion, cyber, cognition, configuration) architecture, and it will transform the collected data into actionable information, and eventually interfere with the physical assets to optimize processes. An IoT-enabled intelligent system of such cases was proposed in 2001 and later demonstrated in 2014 by the National Science Foundation Industry/University Collaborative Research Center for Intelligent Maintenance Systems (IMS) at the University of Cincinnati on a band saw machine in IMTS 2014 in Chicago. Band saw machines are not necessarily expensive, but the band saw belt expenses are enormous since they degrade much faster. However, without sensing and intelligent analytics, it can be only determined by experience when the band saw belt will actually break. The developed prognostics system will be able to recognize and monitor the degradation of band saw belts even if the condition is changing, advising users when is the best time to replace band saw. This will significantly improve user experience and operator safety and ultimately save on costs. [7]

E. Agriculture

The IoT contributes significantly towards innovating farming methods. Farming challenges caused by population growth and climate change have made it one of the first industries to utilize the IoT. The integration of wireless sensors with agricultural mobile apps and cloud platforms helps in collecting vital information pertaining to the environmental conditions– temperature, rainfall, humidity, wind speed, pest infestation, soil humus content or nutrients, besides others – linked with a farmland, can be used to improve and automate farming techniques, take informed decisions to improve quality and quantity, and minimize risks and wastes. [7] The app-based field or crop monitoring also lowers the hassles of managing crops at multiple locations. For example, farmers can now detect which areas have been fertilised (or mistakenly missed), if the land is too dry and predict future yields. [8]

F. Energy Management

Integration of sensing and actuation systems, connected to the Internet, is likely to optimize energy consumption as a whole. It is expected that IoT devices will be integrated into all forms of energy consuming devices (switches, power outlets, bulbs, televisions, etc.) and be able to communicate with the utility supply company in order to effectively balance power generation and energy usage.

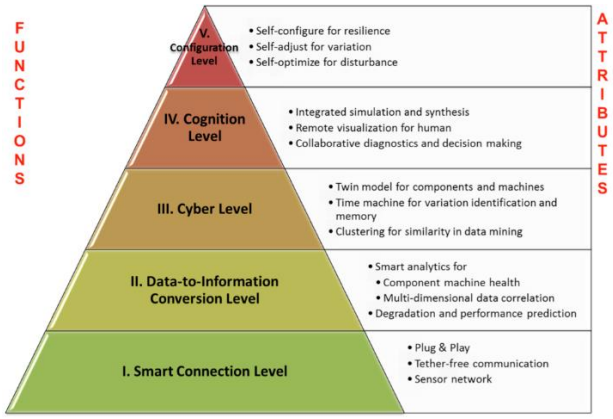

Fig. 3. Functions of IoT [7]

Such devices would also offer the opportunity for users to remotely control their devices, or centrally manage them via a cloud-based interface, and enable advanced functions like scheduling (e.g., remotely powering on or off heating systems, controlling ovens, changing lighting conditions etc.). [8]

Besides home-based energy management, the IoT is especially relevant to the Smart Grid since it provides systems to gather and act on energy and power-related information in an automated fashion with the goal to improve the efficiency, reliability, economics, and sustainability of the production and distribution of electricity. Using advanced metering infrastructure (AMI) devices connected to the Internet backbone, electric utilities can not only collect data from end-user connections but also, manage other distribution automation devices like transformers. [9]

G. Environmental Monitoring

Environmental monitoring applications of the IoT typically use sensors to assist in environmental protection by monitoring air or water quality, atmospheric or soil conditions, and can even include areas like monitoring the movements of wildlife and their habitats. Development of resource-constrained devices connected to the Internet also means that other applications like earthquake or tsunami early-warning systems can also be used by emergency services to provide more effective aid. IoT devices in this application typically span a large geographic area and can also be mobile. It has been argued that the standardization IoT brings to wireless sensing will revolutionize this area. [9]

H. Building and Home Automation

IoT devices can be used to monitor and control the mechanical, electrical and electronic systems used in various types of buildings (e.g., public and private, industrial, institutions, or residential) in home automation and building automation systems. In this context, three main areas are being covered in literature:

- The integration of the internet with building energy management systems in order to create energy efficient and IOT driven "smart buildings".
- The possible means of real-time monitoring for reducing energy consumption and monitoring occupant behaviors.
- The integration of smart devices in the built environment and how they might be used in future applications. [9]

I. Metropolitan Scale Deployments

There are several planned or ongoing large-scale deployments of the IoT, to enable better management of cities and systems. For example, Songdo, South Korea, the first of its kind fully equipped and wired smart city, is on near completion. Nearly everything in this city is planned to be wired, connected and turned into a constant stream of data that would be monitored and analyzed by an array of computers with little, or no human intervention. Another application is a currently undergoing project in Santander, Spain. For this deployment, two approaches have been adopted. This city of 180,000 inhabitants, has already seen 18,000 city application downloads for their smartphones. This application is connected to 10,000 sensors that enable services like parking search, environmental monitoring, digital city agenda among others. City context information is used in this deployment so as to benefit merchants through a spark deals mechanism based on city behavior that aims at maximizing the impact of each notification. Other examples of large-scale deployments underway include the Sino-Singapore Guangzhou Knowledge City; work on improving air and water quality, reducing noise pollution, and increasing transportation efficiency in San Jose, California; and smart traffic management in western Singapore. French company, Sigfox, commenced building an ultra-narrowband wireless data network in the San Francisco Bay Area in 2014, the first business to achieve such a deployment in the U.S. It subsequently announced it would set up a total of 4000 base stations to cover a total of 30 cities in the U.S. by the end of 2016, making

it the largest IoT network coverage provider in the country thus far. Another example of a large deployment is the one completed by New York Waterways in New York City to connect all the city's vessels and be able to monitor them live 24/7.The network was designed and engineered by Fluidmesh Networks, a Chicago-based company developing wireless networks for critical applications. The NYWW network is currently providing coverage on the Hudson River, East River, and Upper New York Bay. With the wireless network in place, NY Waterway is able to take control of its fleet and passengers in a way that was not previously possible. New applications can include security, energy and fleet management, digital signage, public Wi-Fi, paperless ticketing and others. [10,11]

J. Medical and Healthcare

IoT devices can be used to enable remote health monitoring and emergency notification systems. These health monitoring devices can range from blood pressure and heart rate monitors to advanced devices capable of monitoring specialized implants, such as pacemakers, Fitbit electronic wristbands, or advanced hearing aids. Some hospitals have begun implementing "smart beds" that can detect when they are occupied and when a patient is attempting to get up. It can also adjust itself to ensure appropriate pressure and support is applied to the patient without the manual interaction of nurses. Specialized sensors can also be equipped within living spaces to monitor the health and general well-being of senior citizens, while also ensuring that proper treatment is being administered and assisting people regain lost mobility via therapy as well. Other consumer devices to encourage healthy living, such as, connected scales or wearable heart monitors, are also a possibility with the IoT. More and more end-to-end health monitoring IoT platforms are coming up for antenatal and chronic patients, helping one manage health vitals and recurring medication requirements. The Research & Development Corporation (DEKA), a company that creates prosthetic limbs, has created a battery-powered arm that uses electricity, a device that converts muscle group sensations into motor control. The arm is nicked named Luke Arm after Luke Skywalker (Star Wars). [10,11]

K. Transportation

The IoT can assist in the integration of communications, control, and information processing across various transportation systems. Application of the IoT extends to all aspects of transportation systems (i.e. the vehicle, the infrastructure, and the driver or user). Dynamic interaction between these components of a transport system enables inter and intra vehicular communication, smart traffic control, smart parking, electronic toll collection systems, logistic and fleet management, vehicle control, and safety and road assistance. In Logistics and Fleet Management for example, The IoT platform can continuously monitor the location and conditions of cargo and assets via wireless sensors and send specific alerts when management exceptions occur (delays, damages, thefts, etc). [11]

IV. TRENDS AND CHARACTERISTICS

The IoT's major significant trend in recent years is the explosive growth of devices connected and controlled by the internet. The wide range of applications for IoT technology mean that the specifics can be very different from one device to the next but there are basic characteristics shared by most. [12]

A. Intelligence

Ambient intelligence and autonomous control are not part of the original concept of the Internet of things. Ambient intelligence and autonomous control do not necessarily require Internet structures, either.

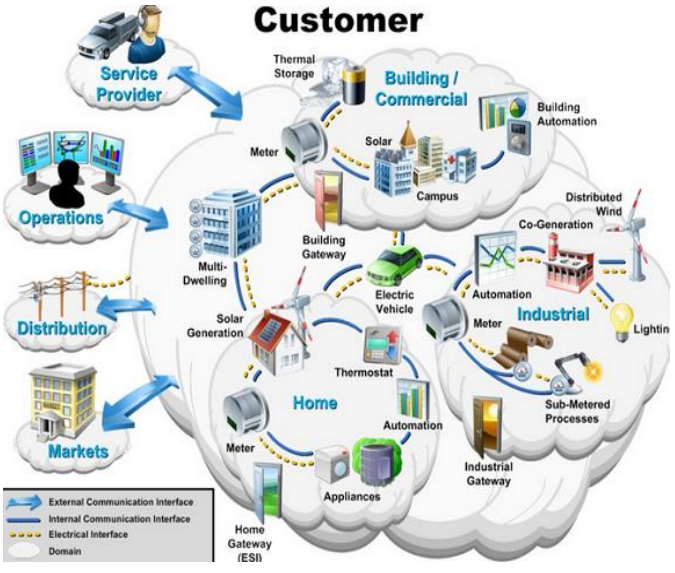

Fig. 4. Customer of IoT [11]

However, there is a shift in research to integrate the concepts of the Internet of things and autonomous control, with initial outcomes towards this direction considering objects as the driving force for autonomous IoT. In the future, the Internet of things may be a non-deterministic and open network in which auto-organized or intelligent entities (Web services, SOA components) and virtual objects (avatars) will be interoperable and able to act independently (pursuing their own objectives or shared ones) depending on the context, circumstances or environments. Autonomous behavior through the collection and reasoning of context information as well as the object's ability to detect changes in the environment (faults affecting sensors) and introduce suitable mitigation measures constitutes a major research trend, clearly needed to provide credibility to the IoT technology. Modern IoT products and solutions in the marketplace use a variety of different technologies to support such context-aware automation but more sophisticated forms of intelligence are requested to permit sensor units to be deployed in real environments. [12]

B. Architecture

The system will likely be an example of architecture, bottom-up made (based on the context of processes and operations, in real-time) and will consider any subsidiary level. Therefore, model driven and functional approaches will coexist with new ones able to treat exceptions and unusual evolution of processes (multi-agent systems, B-ADSc, etc.). In an Internet of Things, the meaning of an event will not necessarily be based on a deterministic or syntactic model but would instead be based on the context of the event itself: this will also be a semantic web. Consequently, it will not necessarily need common standards that would not be able to address every context or use: some actors (services, components, avatars) will accordingly be self-referenced and, if ever needed, adaptive to existing common standards (predicting everything would be no more than defining a "global finality" for everything that is just not possible with any of the current top-down approaches and standardizations).[12] Building on top of the Internet of things, the web of things is an architecture for the application layer of the Internet of things looking at the convergence of data from IoT devices into Web applications to create innovative use-cases. In order to program and control the flow of information in the Internet of things, a predicted architectural direction is being called BPM Everywhere which is a blending of traditional process management with process mining and special capabilities to automate the control of large numbers of coordinated devices.[13]

C. Network Architecture

The Internet of things requires huge scalability in the network space to handle the surge of devices. IETF 6LoWPAN would be used to connect devices to IP networks. With billions of devicesbeing added to the Internet space, IPv6 will play a major role in handling the network layer scalability. IETF's Constrained Application Protocol, ZeroMQ, and MQTT would provide lightweight data transport. "MQ" in "MQTT" came from IBM's MQ Series message queuing product line. [13]

Fog computing is a viable alternative to prevent such large burst of data flow through Internet. The edge devices' computation power can be used to analyses and process data, thus providing easy real time scalability.[14]

D. Complexity

In semi-open or closed loops (i.e. value chains, whenever a global finality can be settled) IoT will often be considered and studied as a complex system due to the huge number of different links, interactions between autonomous actors, and its capacity to integrate new actors. At the overall stage (full open loop) it will likely be seen as a chaotic environment (since systems always have finality). As a practical approach, not all elements in the Internet of things run in a global, public space. Subsystems are often implemented to mitigate the risks of privacy, control and reliability. For example, Domestic Robotics (Domotics) running inside a smart home might only share data within and be available via a local network.[14]

E. Size Considerations

The Internet of things would encode 50 to 100 trillion objects, and be able to follow the movement of those objects. Human beings in surveyed urban environments are each surrounded by 1000 to 5000 trackable objects. In 2015 there were already 83 million smart devices in people`s homes. This number is about to grow up to 193 million devices in 2020 and will for sure go on growing in the near future. [15]

F. Space considerations

In the Internet of things, the precise geographic location of a thing and also the precise geographic dimensions of a thing will be critical. Therefore, facts about a thing, such as its location in time and space, have been less critical to track because the person processing the information can decide whether or not that information was important to the action being taken, and if so, add the missing information (or decide to not take the action). (Note that some things in the Internet of things will be sensors, and sensor location is usually important.) The Geo Web and Digital Earth are promising applications that become possible when things can become organized and connected by location. However, the challenges that remain include the constraints of variable spatial scales, the need to handle massive amounts of data, and an indexing for fast search and neighbor operations. In the Internet of things, if things are able to take actions on their own initiative, this human-centric mediation role is eliminated. [15] Thus, the time-space context that we as humans take for granted must be given a central role in this information ecosystem. Just as standards play a key role in the Internet and the Web, geospatial standards will play a key role in the Internet of things. [16]

G. A Solution to "Basket of Remotes"

Many IoT devices have a potential to take a piece of this market. Jean-Louis Gassée (Apple initial alumni team, and BeOS co-founder) has addressed this topic in an article on Monday Note, where he predicts that the most likely problem will be what he calls the "basket of remotes" problem, where we'll have hundreds of applications to interface with hundreds of devices that don't share protocols for speaking with one another. There are multiple approaches to solve this problem, one of them called the "predictive interaction",where cloud or fog based decision makers will predict the user's next action and trigger some reaction. For user interaction, new technology leaders are joining forces to create standards for communication between devices. Manufacturers are becoming more conscious of this problem, and many companies have begun releasing their devices with open APIs. Many of these APIs are used by smaller companies looking to take advantage of quick integration.[16]

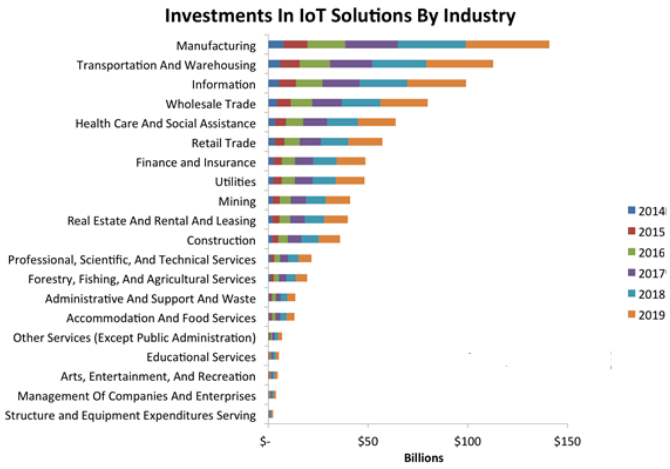

Fig. 5. Investments in Iot solutions by industry [16]

V. STANDARDS AND STANDARDS ORGANIZATION

Table 1. standards organization

Short name	Long name	Standard under development	Other notes
IEEE	Institute of Electrical and Electronics Engineers	Underlying communication technology standards such as IEEE 802.15.4	-
FDA	U.S. Food and Drug Administration	UDI (Unique Device Identification) system for unique identifiers for medical devices	-
IETF	Internet Engineering Task Force	Standards that comprise TCP/IP (the Internet protocol suite)	-
EPC-global	-	Standards for adoption of EPC (Electronic Product Code) technology	-
XSF	XMPP-Standards Foundation	Protocol extensions of XMPP (Extensible Messaging and Presence Protocol), the open standard of instant messaging	-
OMA	Open Mobile Alliance	OMA DM and OMA LWM2M for IoT device management, as well as Got-API, which provides a secure framework for IoT applications	-
Auto-ID Labs	-	Networked RFID (radiofrequency identification) and emerging sensing technologies.	-
MT-Connect Institute	-	MT-Connect is a manufacturing industry standard for data exchange with machine tools and related industrial equipment. It is important to the IIoT subset of the IoT.	-
OCF	Open Connectivity Foundation	Standards for simple devices using Co-AP (Constrained Application Protocol)	-
GS1	-	Standards for UIDs (unique identifiers) and RFID of fast-moving consumer goods (consumer packaged goods), health care supplies, and other things	Parent organization comprises member organizations such as GS1 US

VI. ENABLING TECHNOLOHIES FOR IOT

There are many technologies that enable IoT. Crucial to the field is the network used to communicate between devices of an IoT installation, a role that several wireless or wired technologies may fulfill:

A. Addressability

The original idea of the Auto-ID Center is based on RFID-tags and unique identification through the Electronic Product Code, however, this has evolved into objects having an IP address or URI. An alternative view, from the world of the Semantic Web focuses instead on making all things (not just those electronic, smart, or RFID-enabled) addressable by the existing naming protocols, such as URI. The objects themselves do not converse, but they may now be referred to by other agents, such as powerful centralized servers acting for their human owners. Integration with the Internet implies that devices will use an IP address as a unique identifier. Due to the limited address space of IPv4 (which allows for 4.3 billion unique addresses), objects in the IoT will have to use the next generation of the Internet protocol (IPv6) to scale to the extremely large address space required.[98] Internet-of-things devices additionally will benefit from the stateless address auto-configuration present in IPv6, as it reduces the configuration overhead on the hosts, and the IETF 6LoWPAN header compression. To a large extent, the future of the Internet of things will not be possible without the support of IPv6; and

consequently, the global adoption of IPv6 in the coming years will be critical for the successful development of the IoT in the future. [16]

VII. GOVERNMENT REGULATION ON IOT

One of the key drivers of the IoT is data. The success of the idea of connecting devices to make them more efficient is dependent upon access to and storage & processing of data. For this purpose, companies working on IoT collect data from multiple sources and store it in their cloud network for further processing. This leaves the door wide open for privacy and security dangers and single point vulnerability of multiple systems. The other issues pertain to consumer choice and ownership of data and how it is used. Presently the regulators have shown more interest in protecting the first three issues identified above. IoT regulation depends on the country. Some examples of legislation that is relevant to privacy and data collection are: the US Privacy Act of 1974, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data of 1980, and the EU Directive 95/46/EC of 1995. [16]

Current regulatory environment:

A report published by the Federal Trade Commission (FTC) in January 2015 made the following three recommendations:

- Data security – At the time of designing IoT companies should ensure that data collection, storage and processing would be secure at all times. Companies should adopt a "defence in depth" approach and encrypt data at each stage.
- Data consent users should have a choice as to what data they share with IoT companies and the users must be informed if their data gets exposed.
- Data minimization IoT companies should collect only the data they need and retain the collected information only for a limited time. [16]

However, the FTC stopped at just making recommendations for now. According to an FTC analysis, the existing framework, consisting of the FTC Act, the Fair Credit Reporting Act, and the Children's Online Privacy Protection Act, along with developing consumer education and business guidance, participation in multi-stakeholder efforts and advocacy to other agencies at the federal, state and local level, is sufficient to protect consumer rights. [16]

A resolution passed by the Senate in March 2015, is already being considered by the Congress. This resolution recognized the need for formulating a National Policy on IoT and the matter of privacy, security and spectrum. Furthermore, to provide an impetus to the IoT ecosystem, in March 2016, a bipartisan group of four Senators proposed a bill, The Developing Innovation and Growing the Internet of Things (DIGIT) Act, to direct the Federal Communications Commission to assess the need for more spectrum to connect IoT devices. [16,17]

Several standards for the IoT industry are actually being established relating to automobiles because

most concerns arising from use of connected cars apply to healthcare devices as well. In fact, the National Highway Traffic Safety Administration (NHTSA) is preparing cybersecurity guidelines and a database of best practices to make automotive computer systems more secure. [17]

A. Platform Fragmentation

IoT suffers from platform fragmentation and lack of technical standards a situation where the variety of IoT devices, in terms of both hardware variations and differences in the software running on them, makes the task of developing applications that work consistently between different inconsistent technology ecosystems hard. Customers may be hesitant to bet their IoT future on a proprietary software or hardware devices that uses proprietary protocols that may fade or become difficult to customize and interconnect. IoT's amorphous computing nature is also a problem for security, since patches to bugs found in the core operating system often do not reach users of older and lower-price devices. One set of researchers say that the failure of vendors to support older devices with patches and updates leaves more than 87% of active devices vulnerable. [17]

B. Privacy, Autonomy and Control

Philip N. Howard, a professor and author, writes that the Internet of things offers immense potential for empowering citizens, making government transparent, and broadening information access. Howard cautions, however, that privacy threats are enormous, as is the potential for social control and political manipulation. Concerns about privacy have led many to consider the possibility that big data infrastructures such as the Internet of things and data mining are inherently incompatible with privacy. Writer Adam Greenfield claims that these technologies are not only an invasion of public space but are also being used to perpetuate normative behavior, citing an instance of billboards with hidden cameras that tracked the demographics of passersby who stopped to read the advertisement.

The Internet of Things Council compared the increased prevalence of digital surveillance due to the Internet of things to the conceptual panopticon described by Jeremy Bentham in the 18th Century. The assertion was defended by the works of French philosophers Michel Foucault and Gilles Deleuze. In Discipline and Punish: The Birth of the Prison Foucault asserts that the panopticon was a central element of the discipline society developed during the Industrial Era. Foucault also argued that the discipline systems established in factories and school reflected Bentham's vision of panopticism. In his 1992 paper "Postscripts on the Societies of Control," Deleuze wrote that the discipline society had transitioned into a control society, with the computer replacing the panopticon as an instrument of discipline and control while still maintaining the qualities similar to that of panopticism. [17]

The privacy of households could be compromised by solely analyzing smart home network traffic patterns without dissecting the contents of encrypted application data, yet a synthetic packet injection scheme can be used to safely overcome such invasion of privacy.

Peter-Paul Verbeek, a professor of philosophy of technology at the University of Twente, Netherlands, writes that technology already influences our moral decision making, which in turn affects human agency, privacy and autonomy. He cautions against viewing technology merely as a human tool and advocates instead to consider it as an active agent. [18]

Justin Brookman, of the Center for Democracy and Technology, expressed concern regarding the impact of IoT on consumer privacy, saying that "There are some people in the commercial space who say, 'Oh, big datawell, let's collect everything, keep it around forever, we'll pay for somebody to think about security later.' The question is whether we want to have some sort of policy framework in place to limit that." [18]

Tim O'Reilly believes that the way companies sell the IoT devices on consumers are misplaced, disputing the notion that the IoT is about gaining efficiency from putting all kinds of devices online and postulating that "IoT is really about human augmentation. The applications are profoundly different when you have sensors and data driving the decision making." [19]

Editorials at WIRED have also expressed concern, one stating "What you're about to lose is your privacy. Actually, it's worse than that. You aren't just going to lose your privacy; you're going to have to watch the very concept of privacy be rewritten under your nose."

The American Civil Liberties Union (ACLU) expressed concern regarding the ability of IoT to erode people's control over their own lives. The ACLU wrote that "There's simply no way to forecast how these immense powers disproportionately accumulating in the hands of corporations seeking financial advantage and governments craving ever more control will be used. Chances are big data and the Internet of things

will make it harder for us to control our own lives, as we grow increasingly transparent to powerful corporations and government institutions that are becoming more opaque to us."

In response to rising concerns about privacy and smart technology, in 2007 the British Government stated it would follow formal Privacy by Design principles when implementing their smart metering program. The program would lead to replacement of traditional power meters with smart power meters, which could track and manage energy usage more accurately. However the British Computer Society is doubtful these principles were ever actually implemented. In 2009 the Dutch Parliament rejected a similar smart metering program, basing their decision on privacy concerns. The Dutch program later revised and passed in 2011. [19]

C. Security

Concerns have been raised that the Internet of things is being developed rapidly without appropriate consideration of the profound security challenges involved and the regulatory changes that might be necessary. Most of the technical security issues are similar to those of conventional servers, workstations and smartphones, but the firewall, security update and anti-malware systems used for those are generally unsuitable for the much smaller, less capable, IoT devices. According to the Business Insider Intelligence Survey conducted in the last quarter of 2014, 39% of the respondents said that security is the biggest concern in adopting Internet of things technology. In particular, as the Internet of things spreads widely, cyber-attacks are likely to become an increasingly physical (rather than simply virtual) threat. In a January 2014 article in Forbes, cyber-security columnist Joseph Steinberg listed many Internet-connected appliances that can already "spy on people in their own homes" including televisions, kitchen appliances, cameras, and thermostats. Computer-controlled devices in automobiles such as brakes, engine, locks, hood and trunk releases, horn, heat, and dashboard have been shown to be vulnerable to attackers who have access to the on-board network. In some cases, vehicle computer systems are Internet-connected, allowing them to be exploited remotely. By 2008 security researchers had shown the ability to remotely control pacemakers without authority. Later hackers demonstrated remote control of insulin pumps and implantable cardioverter defibrillators. David Pogue wrote that some recently published reports about hackers remotely controlling certain functions of automobiles were not as serious as one might otherwise guess because of various mitigating circumstances; such as the bug that allowed the hack having been fixed before the report was published, or that the hack required security researchers having physical access to the car prior to the hack to prepare for it. The U.S. National Intelligence Council in an unclassified report maintains that it would be hard to deny "access to networks of sensors and remotely-controlled objects by enemies of the United States, criminals, and mischief makers... An open market for aggregated sensor data could serve the interests of commerce and security no less than it helps criminals and spies identify vulnerable targets. Thus, massively parallel sensor fusion may undermine social cohesion, if it proves to be fundamentally incompatible with Fourth-Amendment guarantees against unreasonable search." In general, the intelligence community views the Internet of things as a rich source of data. As a response to increasing concerns over security, the Internet of Things Security Foundation (IoTSF) was launched on 23 September 2015. IoT SF has a mission to secure the Internet of things by promoting knowledge and best practice. Its founding board is made from technology providers and telecommunications companies including BT, Vodafone, Imagination Technologies and Pen Test Partners. In addition, large IT companies are continuously developing innovative solutions to ensure the security for IoT devices. As per the estimates from KBV Research, the overall IoT security market would grow at 27.9% rate during 2016–2022 as a result of growing infrastructural concerns and diversified usage of Internet of things. In 2016, a distributed denial of service attack powered by Internet of things devices running the Mirai malware took down a DNS provider and major web sites. In May 2017, Junade Ali, a Computer Scientist at Cloudflare noted that native DDoS vulnerabilities exist in IoT devices due to a poor implementation of the Publish–subscribe pattern. While security is a concern there are many things being done to protect devices. Device data is following cryptographic standards and encryption is being used in end-to-end scenarios. To help with this scenario x.509 certificates are also being used to verify device identity. Security experts view Internet of things as a threat to the traditional Internet. Some argue that market incentive to secure IoT devices is insufficient and increased governmental regulation is necessary to make the Internet of things secure. The overall understanding of IoT is essential for basic user security. Keeping up with current anti-virus software and patching updates will help mitigate cyber-attacks. [19]

D. Environmental Sustainability Impact

A concern regarding Internet-of-things technologies pertains to the environmental impacts of the manufacture, use, and eventual disposal of all these semiconductor-rich devices. Modern electronics are replete with a wide variety of heavy metals and rare-earth metals, as well as highly toxic synthetic chemicals. This makes them extremely difficult to properly recycle. Electronic components are often incinerated or placed in regular landfills. Furthermore, the human and environmental cost of mining the rare-earth metals that are integral to modern electronic components continues to grow. With production of electronic equipment growing globally yet little of the metals (from end-of-life equipment) are being recovered for reuse, the environmental impacts can be expected to increase. Also, because the concept of Internet of things entails adding electronics to mundane devices (for example, simple light switches), and because the major driver for replacement of electronic components is often technological obsolescence rather than actual failure to function, it is reasonable to expect that items that previously were kept in service for many decades would see an accelerated replacement cycle if they were part of the IoT. For example, a traditional house built with 30 light switches and 30 electrical outlets might stand for 50 years, with all those components still original at the end of that period. But a modern house built with the same number of switches and outlets set up for IoT might see each switch and outlet replaced at five-year intervals, in order to keep up to date with technological changes. This translates into a ten-fold increase in waste requiring disposal. [19]

E. Confusing Terminology

Kevin Lonergan at Information Age, a business-technology magazine, has referred to the terms surrounding IoT as a “terminology zoo”. The lack of clear terminology is not “useful from a practical point of view” and a “source of confusion for the end user”. A company operating in the IoT space could be working in anything related to sensor technology, networking, embedded systems, or analytics. According to Lonergan, the term IoT was coined before smart phones, tablets, and devices as we know them today existed, and there is a long list of terms with varying degrees of overlap and technological convergence: Internet of things, Internet of everything (IoE), industrial Internet, pervasive computing, pervasive sensing, ubiquitous computing, cyber-physical systems (CPS), wireless sensor networks (WSN), smart objects, cooperating objects, machine to machine (M2M), ambient intelligence (AmI), operational technology (OT), and information technology (IT). Regarding IIoT, an industrial sub-field of IoT, the Industrial Internet Consortium's Vocabulary Task Group has created a "common and reusable vocabulary of terms" to ensure "consistent terminology" across publications issued by the Industrial Internet Consortium. IoT One has created an IoT Terms Database including a New Term Alert to be notified when a new term is published. As of March 2017, this database aggregates 711 IoT-related terms, however, without any attempts to reduce terminological ambiguity and complexity. [19]

VIII. RESULT

Internet of Things (IOT) one of the important and high technology systems that all of world need to this system, description this technology is very important for all people and who work in this field of industry. Internet of Thing enter all our life and become easy to life and comfortable. But for use safe and correct about this technology, we need to understand a basic of Internet of Things (IOT).

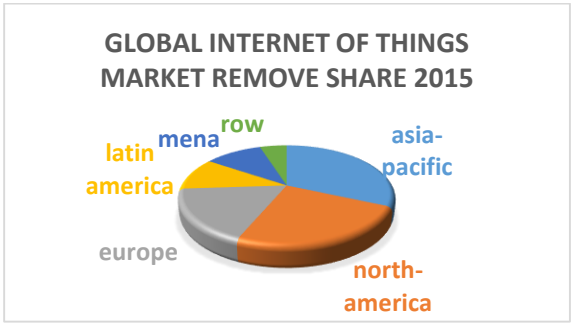

Fig. 6. Global IoT market

REFERENCE

[1] Ajit. (2014,05). Impact of Internet of Things on the Retail Industry. Scopus. 15(power & computer), 30-37.
[2] Mihta. Deo. Romascanu. (2014,03). anagement of Networks with Constrained Devices: Use Cases. IEEE Transaction Electron Devices. 13(power), 12-16.
[3] CasCard. Gemalto. Ericsson. Mitchell. Shane. (2014,01). Smart Shopping: spark deals. IEEE Transaction. Electron Devices. 12(power), 28-35.
[4] Dibo. Kyriazis. Varvarigou. Tiasoo. Rossi. White. Cooper. (2013,09). Sustainable smart city IoT applications: Heat and electricity management & Eco-conscious cruise control for public transportation. scopus. 8(power), 16-23.
[5] Arkian.(2017,11). MIST: Fog-based Data Analytics Scheme with Cost-Efficient Resource Provisioning for IoT Crowdsensing Applications. Journal of Network and Computer Applications. 33(network & computer), 152–165.
[6] Junade.(2009,3). IoT Security Anti-Patterns. SpringerLinke. 24(power & computer), 79-88.

[7] Mattern. Friedemann. Floerkemeier. Christian.(2013,06) From the Internet of Computers to the Internet of Things. SpringerLink.44(copmuter), 74-93.
[8] Weiser. Mark. (2003,12). The Computer for the 21st Century. Wiley. 63(industrial power), 243-258.
[9] Eggimann. Mutzner. Wani. Mariane. Schneider. Spuhler. Beutler. Maurer.(2017,11). The potential of knowing more – a review of data-driven urban water management. ScienceDirect. 13(digital marketing), 69-77.
[10] Lee.(2014,07). Keynote Presentation: Recent Advances and Transformation Direction of PHM. ProQuest, 36(communication), 193-212.
[11] Nordrum(2016,03). Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated. APAPsycNET. 70(network), 243-256.
[12] Klint. Finley.(2015,11). The Internet of Things Could Drown Our Environment in Gadgets.SpringerLink. 101(power), 43-56.
[13] Brown.(2014,05). Britain's Smart Meter Programme: A Case Study in Privacy by Design. IEEE transaction. 45(smart grid),105-112.
[14] Lee, Jay (1993,12). Analysis of machine degradation using a neural network based pattern discrimination model. Journal of Manufacturing Systems. 12(network), 379–387.
[15] Mahmud. Khizir. Town. Graham. Morsalin. Sayidul. Hossain. (2018,01). Integration of electric vehicles and management in the internet of energy. Renewable and Sustainable Energy Reviews. 82(computer), 4179–4203.
[16] Zhuge. (2004,03). Future Interconnection Environment – Dream, Principle, Challenge and Practice, Keynote. Wiley. 80(power), 145-160.
[17] Zhuge(2013,08). The Future Interconnection Environment. IEEE Transaction. 96 (Computer), 236-245.
[18] Gubbi. Jayavardhana. Buyya. Rajkumar. Marusic. Slaven. Palaniswami. Marimuthu. (2013,04). Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems. 29 (computer), 1645–1660.
[19] Lee. Jay. Bagheri. Behrad. Kao. Hung-An. (2015,06). A cyber-physical systems architecture for industry 4.0-based manufacturing systems. SpringerLinke. 56(power & computer), 18–23.