Pacific International Journal, Vol. 2(2), 84-88; 2019
ISSN (Print) 2663-8991, ISSN (Online) 2616-4825
DOI: 10.55014/pij.v2i2.77
https://rclss.com/index.php/pij

Inspiring Evolving Technologies in Internet of Things

Samson Hansen Sackey[1], Godwin Kobby Gapko[1], Samuel Nartey Kofie[1], Abdul Karim Armah[1]

[1]College of IOT Engineering, Hohai University, 213022, Changzhou, China

*Correspondence: kofano25@yahoo.com

In view of wireless communications, the perception of evolving technologies and opportunities in the Internet of Things (IoT) is basically wireless connectivity. Exceptionally, new features are going to bring about extraordinary growth which is reliably going to stay for a long-lasting period. However, applicable communication and information technologies in the field of IoT have great influence in involving digital and physical units together. For that reason we need to consider existing efforts, in terms of smart devices in our lives and efficient storage. In this paper, we present an analysis of evolving technologies and challenges for Internet of Things.

Keywords: Internet of Things (IoT), IoT technologies, RFID,IoT Structure, Wireless Sensor Networks.

Introduction

A network of physical objects (buildings, devices, vehicles, and other things) that are embedded with sensors, electronics, software, and network connectivity to collect and exchange data is basically known as the Internet of Things (IoT) [11]. Basically, there is exchange of data, self-regulation and secure communication in the IoT interface which exist between real world devices and applications [2]. Although this idea is evoking attention, everything and everyone will be connected [1]. The IoT still faces challenges when it comes to the development of diverse applications and services in terms of ultra large scale network of things, device and network level heterogeneity and large number of events generated [12],[13]. The presence of radio frequency identification (RFID) technology has vast influence in the theory of internet of things, which is now broadly used for tracking objects, animals, and people. It usually consist of three components: a tag, a reader, and a computer system. Also known as the transponder, the tag is made up of a microchip and a radio antenna. The chip in the tag has all information pertaining to number of items that it is either attached to or that it is inserted in it. An RFID tag is said to be functioning when its source of power is full or half in terms of its battery therefore maintaining the RFID tags circuitry and antenna. Several RFID tags contain useable batteries for years of use; others are sealed units. RFID system architecture is marked by a sharp contrast of simple RFID identifiers and an extensive infrastructure of interconnected radio frequency identification viewers .In fact, not limiting to sensing abilities and deployment controllability that are more challenging application setups required[3]. Figure 1 shows the Radio Frequency Identification (RFID) technology. It is certain that the principle supports tracking of physical entities within a well-defined boundary (storerooms) through an ideal methodology.

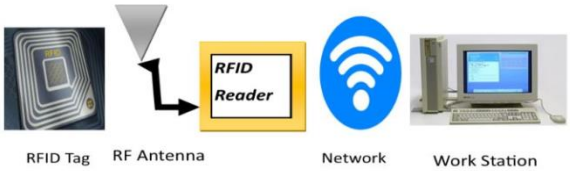

Figure 1: The RFID technology

The basic idea of IoT has much impact on several issues such as everyday life and behavioral customers. Certainly, private customer's most obvious effects on IoT will be visible in both working and domestic fields. In this context, smart households, industrial automation, Wireless Sensor Networks (WSNs), machine-to-machine (M2M) and device-to-device (D2D) technologies, assisted living, e-health, transportation, improved learning are only a few examples of possible application scenarios in which the new prototype will play a leading part in the near future [4],[14]. The most obvious significances will be equally observable in fields such as logistics, industrial manufacturing, business process management, intelligent transportation of people and goods which are most perceived by a business point of view. For instance, a community made up of smart meters will get alert of energy run down and it communicates the information efficiently to the provider. The major players in IoT are Amazon, AT&T, Bosch, Cisco, Dell, GE, Google, Hitachi Data systems, Microsoft, and Samsung.

The contribution to this paper are as follows:

[Received 03 Jan 2019; Accepted 08 April 2019; Published (online) 30 June 2019]
Publisher's Note: RCLSS stays neutral regard to jurisdictional claims published maps

i. The inspiring wide variety of new technologies of IoT are discussed.
ii. The fundamental challenges faced by the systems are indicated.
The remaining part of this paper is organized as follows. Section II describes briefly the structural interpretation of IoT. Section III forecasts possible emerging technologies of IoT. Section IV describes key challenges in the applications of IoT. Finally, Section V concludes the paper.

II Evaluation

The definition of IoT has been introduced several years ago from numerous different viewpoints and also from the large research community. For the obvious reason, the description of this type of configuration is rarely divided between two terms- The Internet and objects. Specifically, each layer comprises of protocols, devices, and modules that work effectively in converting data to information, and then to comprehensive analyses.
Device layer: The device layer is made up of devices like sensors, smart meters, wearable's, smart phones, radio frequency identification (RFID) tags, drones, etc. Even though there are many set of devices, all these devices requires a vast number of communication standards such as Hypertext Transfer Protocol (HTTP) and customized internet protocols [6] such as Zig Bee,Z-wave, User Datagram Protocol (UDP), Mod bus protocol, Transmission Control Protocol (TCP), BAC net protocol, Simple Network Management Protocol (SNMP), and Low-Level Reader Protocol (LLRP).
Data ingestion and transformation layer: In this layer, the transformed data from the device layer go esviaa number of protocols which set the benchmark for other processing. This class of data can be obtained from sensors, wearable's, actuators, connected machines, RFID, barcode, drones, GPS, smart phones, smart meters usually through TCP/IP socket communication or messaging queues like Kafka Message Bus, Advanced Message Queuing Protocol (AMQP), Constrained Application Protocol (CoAP), The Extensible Messaging and Presence Protocol (XMPP), Message Queue Telemetry Transport (MQTT),and Hypertext Transfer Protocol Secure (HTTPS) concluding with Representational State Transfer Application Programming Interface (REST API).
Data processing layer: Due to the millions of data generated by the device layer. The following meaningful visions such as systematic analytics, image exploitation, machine learning and big data analytics are few that provide the way forward for data management. For data transformation analysis such as carrying out real-time streaming analytics such as pattern matching, filtering, enhancement, correlation, and image segmentation. In this case, the complex event processor should be considered. Furthermore, we can put to use multiple APIs for localization, ticketing reporting, policy making, device provisioning, user management, communication, maps and database which assists in the formation of the control panel.
Applications layer: This layer lies on top of the IoT structure and it transfers the systems operations to the final user [5]. Bearing in mind about the availability of information that can be obtained from a set of devices. There are a series of applicative focuses which ranges from tracking and tracing, employee safety, remote monitoring, risk, fraud and warranty analytics, predictive analytics, resource efficiency, process visibility to automation. These sort of reports can be applied in diverse fields such as logistics, healthcare, agriculture, buildings, retail, smart grid, oil, mining etc.

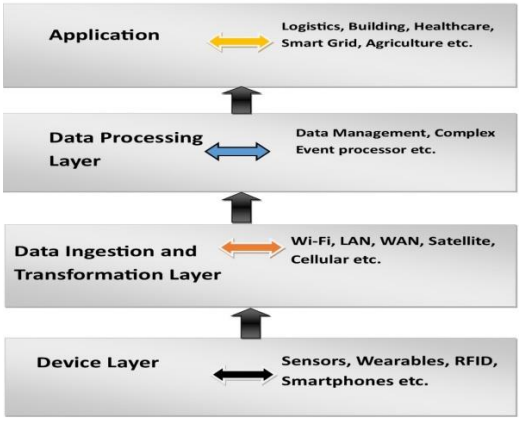

Figure 2: The IoT Structure

III Technologies

The IoT can find its technologies in almost every aspect of our daily life. Below are some of the standards.
1. IoT Analytics: Informative business prototypes in IoT gives conclusive evidence on things collected in numerous techniques, which will demand new analytic tools and algorithms. It is proposed that, over the next few years, the amount of data possessed will be increased in a tremendous way, so therefore the requirements of the IoT may diverge further from traditional analytics. Grok Engine is a software that analyses streaming data, learn from continuous data, and the ability to drive action from output data prototypes.
2. Low-Power, Short-Range IoT Networks: By the year 2025 and beyond, Low-power, short-range networks definitely take over wireless IoT connectivity, approximately more than connections making use of wide-area IoT networks. Efficient routing machines such as IPv6 Routing Protocol can be employed for Low power, short range Networks [10]. Smart Wallets and Action tags are known to be near field communications (NFC), they are short ranged ($> 10cm$) wireless technology for target sensing. On the other hand, IoT device manufacturers will still be unique in spiteof the fact that many marketable and practical trade-offs with many resolution sexist.

3. Low-Power, Wide-Area IoT Networks: Standard cellular networks don't transport a good combination of technical features and the carry out cost for those devices that perform actively in wide-area detection possesses fairly low bandwidth, low hardware and operating cost, good battery life, and high connection density. Wide-Area Network (WAN) technologies such as 6LoWPAN border router and Routing Protocol for Low Power and Lossy Networks (RPLLN) root node plays a vital role in connection from one end to the other. As for narrowband IoT, it's still going to surpass among all standards. EnOcean is an energy harvesting wireless technology applied in constructing automation systems; it can also be linked with micro energy converters with low power to secure wireless communication between battery less sensors, switches, and controllers.

4. IoT Device Surveillance: For IoT devices to last, there is the need for management and monitoring. Monitoring device such as benzene (C_5H_6) sensor monitors air quality. There are devices that check firmware and software updates, diagnostics, crash analysis and reporting, physical management, and security management. Some tools are useful in managing and monitoring millions of devices. Nest smart thermostat regulates room temperature based on when you're home or away for efficient saving on heating and cooling bills. We Mo switch smart plug is in control of turning on or off of devices connected to the switch, monitors how much energy, power the device is using. The Piper in Figure 3(a) can be used for both security purpose and home monitoring.

Figure 3: (a) Piper(b) Smart Meter (c) Health patch (d) UHF RFID Reader

5. IoT Security: Security technologies will be required to protect IoT devices and platforms to encode their own communications, prevent data intrusion and physical interference and also discuss new problems such as denial-of-sleep attacks that weaken batteries. IoT devices employ least processors which make it complex and operating systems that may not work with advanced security practices. August smart lock routinely operates to unlock your household when you arriver leave. Canary Smart Security System combines video, audio, motion detection, night vision, temperature, a siren, air quality sensors into a piece of device that can be guarded from your phone.

6. IoT Processors: IoT devices make use of processors and designs to check whether they are capable to resist strong encryption and security, power consumption, whether the operating system (OS) can run, and embedded device monitoring machines, and firmware renovation. Sometimes choosing a processor mandates profound professional services. Samsung Smart Things Hub manages lights, locks, plugs, thermostat, cameras, and speakers from a principal hub then from the Smartphone. It functions with other automated devices for security guidelines. Health patch Monitor is used on out-patient to get information such as ECG, respiratory rate, heart rate, skin temperature, fall detection, body posture and activity readings. Lively Personal Emergency Response System enables medication reminders, alerts doctors of any likely health problems before they arise. Figure 3(c) shows a picture of a health patch device.

7. Event Stream Processing: High percentage of data charges are needed in real time by some IoT applications. Such systems can produce tens of thousands of outcomes per second and can even produce millions of outcomes per second in extreme circumstances. Distributed stream computing platforms can handle very high-rate data streams and accomplish duties such as real-time analytics and pattern matching. Philips Hue Smart bulbs can match tones in a photo that are uploaded via a specific application, it can also be altered by choosing any color and it can go with music for a special sound-and-light party.

8. IoT Operating Systems: Old designed operating systems for example OS and Windows were not created for IoT applications. These old designed OS demands fast processors, use up more power, and lack properties such as positive real-time response. Additionally, they possess oversized memory imprint for tiny devices and may not stand the chips that IoT makers utilize. Therefore, a number of IoT operating systems has been established to fit several hardware imprints and feature requirements. Automatic Car Tracking Adapter is responsible for tracking and sending information about your car like hours driven, location, mileage, fuel efficiency and ignition status by using an in-car adapter. Riot OS is an OS designed for IoT appliances. The Riot OS structure can handle energy efficiency, high degree of modularity and hardware independent improvement.

9. IoT Platforms: Most IoT platforms contain packages with quite a few assorted wide-ranging products in it. The following are services that IoT platforms can offer: Low-level device control and processes for example communications (WiMAX), device monitoring (HTTP-CoAP proxy), security, and firmware adjustment. Ocean it laboratory Smart Cement possesses implanted nano sensor material which passes on

response to oil drilling industries by helping them recognize the reliability of the well and risk valuation.Open.Sen.se is an example of an open platform for testing state-of-the-art devices.

10. IoT Standards and Systems: Certified IoT standards and their related application programming interfaces (APIs) is beneficial because these devices connect to one another even including IoT industrial prototypes. This depends on dividing data between a lot of devices and companies. Several IoT systems will be developed, and companies assembling products may have to develop alternatives to promote the standards and systems market and also make efforts to conduct yearly maintenance to these products to extent their years as the standards evolve and new standards and APIs arise. Cisco's Connected Factory encourages companies to incorporate IoT technologies in manufacturing industries for efficient monitoring of equipment. Smart meters is an example of a weightless (SIG) product. It drives data between a base station and thousands of machines around it using wavelength radio transmission with high security guarantee. Figure 3 (c) displays a smart meter.

The IoT technologies will continuously evolve with the passage of time but it has also to face many challenges related to privacy, security, standardization, confidentiality, and sufficient continuum for connecting huge number of tagged objects or sensors etc. Some of the key challenges are addressed in section IV.

IV Challenges

The IoT has much impact in the internet world and therefore can be resourceful to the vast economic benefits that come with it but it also expressions it challenging outcomes [9]. Some of them are briefly described below.

1. Standardization: Activities involving IoT devices have grown to a point of standardization. These IoT devices have harsh concerns when it comes to networking resources and low standards. Excluding standards that monitor developers and manufactures, most designed products have complications while in use. The problem of connecting multiple vendors comes to mind when IoT devices found in a particular household have some devices suitable with a specific IoT provider but the others may not be.

2. Power Consumption: These days, the demand over robustness is done to continue the uprising decision to handle power to make daily gadgets and services run on IoT. As for system scaling and system on package (SoP), they are ways to minimizing loss of power over an increasingly small space with the factor of cost involved.

3. Security: Moreover, the part of security is an essential backbone of IoT and also the major challenge. In fact, in the next few year this difficulties will be outshined. The interest shown by IoT users will be a boosting factor for networking and communication research, industries and academic test centers. Figure 4showsthe factors that influence security and privacy [7]. Due to the numerous IoT implementations, intruders can cause destruction to these devices i.e. we need to prevent these intruders from further untrustworthy activities.

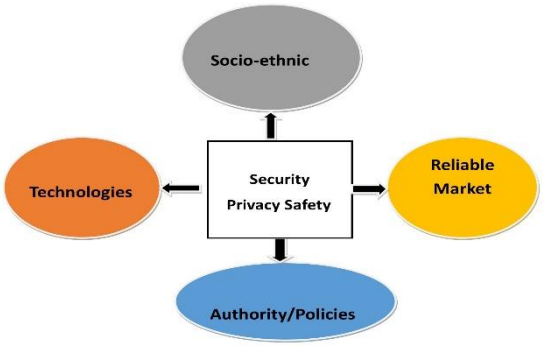

Figure 4: The structures in fluenced by security and privacy.

4. Privacy: As long as there is suspicion and as long as there is no trust that severe hazards will not be affected by protecting the privacy of IoT devices, there cannot be mutual recognition of IoT by the public. For that reason, preserving privacy should play a key role in the IoT architecture [8]. Subsequently, RFID, 2D-barcodes, sensors, and Ultra High Frequency RFID reader (in figure 3(d)) is necessary for everyday identification and therefore the tags needs to contain data of a specific entry. The necessity to preserve a particular data private should be assured to avoid unlawful access. The major players in the IoT era are conscious of these issues and an assured way forward is been taken to guarantee safety of customers and needed continuity of resources.

5. Storage capacity: As IoT is getting developed the amount of data being generated is huge. Moreover, storage allocation is made for other data to be reserved in the data centers as well as the energy and power resources. This reserved data is then organized and processed. Meaningful information is produced out of this data using Semantic Data Fusion models. Several algorithms in Artificial Intelligence can be employing to extract meaningful information from this redundant data. Furthermore, the challenge of data storage and analysis will still exist because the entire globe is going to be interconnected via IoT.

6. Monitoring: In fact, sensors are functional devices that can signal natural occurrences and processes such as temperature, wind, rainfall, and river height is very essential when it's able to sense. Sometimes, it's difficult to detect and monitor abnormal activities that could expose human or animal communication in the presence large number of devices. Therefore, the deployment of sensors to a perilous area is very important in order to make acute decision in detecting malicious activities quickly.

7. Data confidentiality: In IoT sensing or measurements, the sensor devices used works actively and carries data to the

information processing unit above the transmission system. The sensor devices functions by accurately using an encryption tool to certify the data integrity at the information processing unit. Mostly, it can be determine which data can be seen using the IoT services; hence, it is obligatory to protect the data from externals.

8. Identification: The IoT will connect billions of objects to provide innovative services. These various objects holds a unique identity tag over the internet. Hence, providing an efficient way to name and identify things is needed to assign and manage distinct identity for such a large number of objects.

9. Legal and Regulatory: In relation to legal or regulatory, there is a considerable restriction because information (privacy laws) shared could definitely be breached. In adverse cases, the revision of laws and regulations are fulfilled, otherwise, there may be complications in propagating better communication.

10. Analytical real-time operation: Apparently, high data transfer rate is achieved when the bandwidth path is greater. The future of IoT is open and adjustable to fast changes of the status and settings of the systems. Then again, it is vital to response swiftly to dangerous situations such as the increasing frequency of natural disasters due to the global climate change. Infrastructure less alternatives for communication in networks or easy-to-deploy structures can help solve these problems.

V Conclusions

Conclusively, this paper introduced the developing future practice of the Internet known as "Internet of Things" that gets access to the conception of ‘‘any media, anywhere, anytime, anyone, anything”sharing. Sensor devices work independently to interconnect interchange data and take intellectual decisions in most fields of IoT. The continuous increase in the interest of IoT innovations has seen several research being conducted. Apparently, the present evolving trends discussed above are highly possible to reach a height for many years.

References

[1] J. Zheng, D. Simplot-Ryl, C. Bisdikian, and H. Mouftah, “The Internet of Things,” in *IEEE Communications Magazine, Volume: 49, Issue: 11, pp: 30-31*, 2011.

[2] T. Fan and Y. Chen, “A Scheme of Data Management in the Internet ofThings,” in 2nd IEEE International Conference on Network Infrastructure and Digital Content, Sept, 2010.

[3] R. Khan, S.U. Khan, R. Zaheer, andS. Khan,“Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges,” In 10th International Conference on Frontiers of Information Technology (FIT): Proceedings (pp. 257-260). Institute of Electrical and Electronics Engineers Inc. DOI: 10.1109/FIT.2012.53, 2012.

[4] D. Bandyopadhyay and J. Sen,“Internet of Things: Applications and Challenges in Technology and Standardization,”in Wireless Pers Comm.58:49–69DOI 10.1007/s11277-011-0288-5, 2011.

[5] L. Atzori, A. Iero, and G. Morabito, “The Internet of Things: A Survey,” in Computer Networks 54 pg. 2787–2805, 2010.

[6] M. R. Palatella, N. Accettura, X. Vilajosana, T. Watteyne, L. A. Grieco, G. Boggia, and M. Dohler, “Standardized Protocol Stack for the Internet of (Important) Things”, IEEE Communications Surveys & Tutorials, VOL. 15, NO. 3, THIRD QUARTER, 2013.

[7] D. Singh, G. Tripathi, and A. J. Jara, “A survey of Internet-of-Things: Future Vision, Architecture, Challenges and Services”, IEEE World Forum on Internet of Things (WF-IoT), 2014.

[8] D. H. Shin, “A socio-technical framework for Internet-of-Things design: A human-centered design for the Internet of Things”, Telematics and Informatics 31 pg. 519–531, 2014.

[9] G. Gang, L. Zeyong, and J. Jun, “Internet of Things Security Analysis,” in *International Conference on Internet Technology and Applications(iTAP)*, August 2011.

[10] T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, K. Pister, R. Struik, J. P. Vasseur, and R. Alexander, “RPL: IPv6 routing protocol for low-power and lossy networks”, RFC6550, s.l.: IETF Mar. 2012.

[11] F. Ganz, D. Puschmann, P. Barnaghi, and F. Carrez, “A Practical Evaluation of Information Processing and Abstraction Techniques for the Internet of Things”, IEEE Internet Things J. 2 340–354, 2012.

[12] M.A. Razzaque, M. Milojevic-Jevric, A. Palade, and S. Cla, “Middleware for internet of things: A survey”, IEEE Internet Things J. 3 70–95, 2016.

[13]Y. Ai, M. Peng, and K. Zhang, “Edge cloud computing technologies for internet of things: A primer”, *Digital Communications and Networks*, doi: 10.1016/j.dcan.07.001, 2017.

[14]A. AI-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayysah,“Internet of Things: A Survey on Enabling Technologies, Protocols and Applications”, IEEE Communication Surveys and Tutorials Vol. 17, No.4. pp. 2347-2376, Fourth Quarter, 2015.