INTERNET of THINGS (IoT): A REVIEW

Dr. Owais Ahmed

Lecturer at Dept. of Management Studies, North Campus, University of Kashmir, JK, India.

salsaabiill@yahoo.com

ABSTRACT - The world of technology has taken a giant leap in recent past, especially, in data communication and networking field namely, machine learning, data mining, artificial intelligence and internet of things. Internet of Things (IoT) though, in its nascent stage, has lead to the creation of a global network that allows communication between human-to-human, human-to-things and things-to-things, by providing unique identity to each and every object. IoT represents a blend of multiple technologies, real-time analytics, machine learning, commodity sensors, and embedded systems. The current study would throw some light on Internet of Things (IoT), technologies associated with IoT, implications, challenges and future of IoT.

KEYWORDS: Internet of Things, IoT, RFID, IPv6, EP, NFC

I.INTRODUCTION

The Internet of things (IoT) is the network of devices such as vehicles, and home appliances that contain electronics, software, actuators, and connectivity which allows these things to connect, interact and exchange data. IoT involves extending Internet connectivity beyond standard devices, such as desktops, laptops, smart phones and tablets, to any range of traditionally *dumb* or non-internet-enabled physical devices and everyday objects. Embedded with technology, these devices can communicate and interact over the Internet, and they can be remotely monitored and controlled. Internet of Things is maturing and continues to be the latest, most hyped concept in the IT world. Over the last decade, the term Internet of Things (IoT) has attracted attention by projecting the vision of a global infrastructure of networked physical objects, enabling anytime, anyplace connectivity for anything and not only for any one [7]. The Internet of Things can also be considered as a global network which allows the communication between human-to-human, human-to-things and things-to-things, which is anything in the world by providing unique identity to each and every object [1]. IoT describes a world where just about anything can be connected and communicates in an intelligent fashion that ever before. Most of us think about "being connected" in terms of electronic devices such as servers, computers, tablets, telephones and smart phones. In what's called the Internet of Things, sensors and actuators embedded in physical objects—from roadways to pacemakers—are linked through wired and wireless networks, often using the same Internet IP that connects the Internet. These networks churn out huge volumes of data that flow to computers for analysis. When objects can both sense the environment and communicate, they become tools for understanding complexity and responding to it swiftly. What's revolutionary in all this is that these physical information systems are now beginning to be deployed, and some of them even work largely without human intervention. The "Internet of Things" refers to the coding and networking of everyday objects and things to render them individually machine-readable and traceable on the Internet [2]Much existing content in the Internet of Things has been created through coded RFID tags and IP addresses linked into an EPC (Electronic Product Code) network [6].

Internet of things has evolved due to convergence of multiple technologies, real-time analytics, machine learning, commodity sensors, and embedded systems. 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. Coke vending machine at Carnegie Mellon University becoming the first Internet-connected appliance, able to report its inventory and whether newly loaded drinks were cold. 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 [3]. 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. Internet-of-things devices additionally will benefit from the stateless address auto-configuration present in

 DOI : 10.18231/2454-9150.2018.1293

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. *Short-range wireless includes* Bluetooth mesh networking – Specification providing a mesh networking variant to Bluetooth low energy (BLE) with increased number of nodes and standardized application layer (Models). Light-Fidelity (Li-Fi) – Wireless communication technology similar to the Wi-Fi standard, but using visible light communication for increased bandwidth. Near-field communication (NFC) – Communication protocols enabling two electronic devices to communicate within a 4 cm range. QR codes and barcodes – Machine-readable optical tags that store information about the item to which they are attached. Radio-frequency identification (RFID) – Technology using electromagnetic fields to read data stored in tags embedded in other items. Transport Layer Security – Network security protocol. Wi-Fi – technology for local area networking based on the IEEE 802.11 standard, where devices may communicate through a shared access point or directly between individual devices. ZigBee – Communication protocols for personal area networking based on the IEEE 802.15.4 standard, providing low power consumption, low data rate, low cost, and high throughput. *Medium-range wireless includes* LTE-Advanced – High-speed communication specification for mobile networks. Provides enhancements to the LTE standard with extended coverage, higher throughput, and lower latency. Long-range wireless includes Low-power wide-area networking (LPWAN) – Wireless networks designed to allow long-range communication at a low data rate, reducing power and cost for transmission. Available LPWAN technologies and protocols: LoRaWan, Sigfox, NB-IoT, Weightless. Very small aperture terminal (VSAT) – Satellite communication technology using small dish antennas for narrowband and broadband data. Wired includes Ethernet – General purpose networking standard using twisted pair and fiber optic links in conjunction with hubs or switches. Power-line communication (PLC) – Communication technology using electrical wiring to carry power and data. Specifications such as Home Plug or G.hn utilize PLC for networking IoT devices.

II.IMPLICATIONS

A growing portion of IoT devices are created for consumer use, including connected vehicles, home automation, wearable technology, connected health, and appliances with remote monitoring capabilities. IoT devices are a part of the larger concept of home automation, which can include lighting, heating and air conditioning, media and security systems. Long term benefits could include energy savings by automatically ensuring lights and electronics are turned off. A smart home or automated home could be based on a platform or hubs that control smart devices and appliances. For instance, using Apple's Home Kit, manufacturers can get their home products and accessories be controlled by an application in iOS devices such as the iPhone and the Apple Watch.This could be a dedicated app or iOS native applications such as Siri [5]. This can be demonstrated in the case of Lenovo's Smart Home Essentials, which is a line of smart home devices that are controlled through Apple's Home app or Siri without the need for a Wi-Fi bridge. There are also dedicated smart home hubs that are offered as standalone platforms to connect different smart home products and these include the Amazon Echo, Google Home, Apple's HomePod, and Samsung's SmartThings Hub. Smart home provides assistance for those with disabilities and elderly individuals. These home systems use 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 cochlear 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.

The Internet of Medical Things (also called the internet of health things) is an application of the IoT for medical and health related purposes, data collection and analysis for research and monitoring. This 'Smart Healthcare', as it can also be called, led to the creation of a digitized healthcare system, connecting available medical resources and healthcare services. 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. A 2015 Goldman Sachs report indicated that healthcare IoT devices "can save the United States more than $300 billion in annual healthcare expenditures by increasing revenue and decreasing cost." Moreover, the use of mobile devices to support medical follow-up led to the creation of 'm-health', used "to analyze, capture, transmit and store health statistics from multiple resources, including sensors and other biomedical acquisition systems". 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 These sensors create a network of intelligent sensors that

 DOI : 10.18231/2454-9150.2018.1293

are able to collect, process, transfer and analyze valuable information in different environments, such as connecting in-home monitoring devices to hospital-based systems. Other consumer devices to encourage healthy living, such as connected scales or wearable heart monitors, are also a possibility with the IoT. End-to-end health monitoring IoT platforms are also available for antenatal and chronic patients, helping one manage health vitals and recurring medication requirements [7].

Advances in plastic and fabric electronics fabrication methods have enabled ultra-low cost, use-and-throw IoMT sensors. These sensors, along with the required RFID electronics, can be fabricated on paper or e-textiles for wirelessly powered disposable sensing devices. Applications have been established for point-of-care medical diagnostics, where portability and low system-complexity is essential. As of 2018 IoMT was not only being applied in the clinical laboratory industry, but also in the healthcare and health insurance industries. IoMT in the healthcare industry is now permitting doctors, patients and others involved (i.e. guardians of patients, nurses, families, etc.) to be part of a system, where patient records are saved in a database, allowing doctors and the rest of the medical staff to have access to the patient's information. Moreover, IoT-based systems are patient-centered, which involves being flexible to the patient's medical conditions. IoMT in the insurance industry provides access to better and new types of dynamic information. This includes sensor-based solutions such as biosensors, wearables, connected health devices and mobile apps to track customer behaviour. This can lead to more accurate underwriting and new pricing models. The application of IOT in healthcare plays a fundamental role in managing chronic diseases and in disease prevention and control. Remote monitoring is made possible through the connection of powerful wireless solutions. The connectivity enables health practitioners to capture patient’s data and applying complex algorithms in health data analysis.

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, 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.). This can only be possible with the IoT and its seamless connectivity among devices. Sensors such as GPS, Humidity, Temperature, send data to the IoT platform and then the data is analyzed and send further to the users. This way, users can track the real-time status of vehicles and can make appropriate decisions. If combined with Machine Learning then it also helps in reducing traffic accidents by introducing drowsiness alerts to drivers and providing self driven cars too [8].

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 to know who to be used in future applications.

III.CHALLENGES

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 Android devices vulnerable.

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 privacy of households could be compromised by solely analyzing smart home network traffic patterns without dissecting the contents of encrypted

 DOI : 10.18231/2454-9150.2018.1293

application data, yet a synthetic packet injection scheme can be used to safely overcome such invasion of privacy.

A challenge for producers of IoT applications is to clean, process and interpret the vast amount of data which is gathered by the sensors. There is a solution proposed for the analytics of the information referred to as Wireless Sensor Networks. These networks share data among sensor nodes that are sent to a distributed system for the analytics of the sensory data.

Another challenge is the storage of this bulk data. Depending on the application, there could be high data acquisition requirements, which in turn lead to high storage requirements. Currently the Internet is already responsible for 5% of the total energy generated, and a "daunting challenge to power" IoT devices to collect and even store data still remains.

IoT systems are typically controlled by event-driven smart apps that take as input either sensed data, user inputs, or other external triggers (from the Internet) and command one or more actuators towards providing different forms of automation. Examples of sensors include smoke detectors, motion sensors, and contact sensors. Examples of actuators include smart locks, smart power outlets, and door controls. Popular control platforms on which third-party developers can build smart apps that interact wirelessly with these sensors and actuators include Samsung's SmartThings, Apple's Home Kit, and Amazon's Alexa, among others.

A problem specific to IoT systems is that buggy apps, unforeseen bad app interactions, or device/communication failures, can cause unsafe and dangerous physical states, e.g., "unlock the entrance door when no one is at home" or "turn off the heater when the temperature is below 0 degrees Celcius and people are sleeping at night". Detecting flaws that lead to such states, requires a holistic view of installed apps, component devices, their configurations, and more importantly, how they interact. Recently, researchers from the University of California Riverside have proposed IotSan, a novel practical system that uses model checking as a building block to reveal "interaction-level" flaws by identifying events that can lead the system to unsafe states. They have evaluated IotSan on the Samsung SmartThings platform. From 76 manually configured systems, IotSan detects 147 vulnerabilities (i.e., violations of safe physical states/properties).

The Electronic Frontier Foundation has raised concerns that companies can use the technologies necessary to support connected devices to intentionally disable or "brick" their customers' devices via a remote software update or by disabling a service necessary to the operation of the device. In one example, home automation devices sold with the promise of a "Lifetime Subscription" were rendered useless after Nest Labs acquired Revolv and made the decision to shut down the central servers the Revolv devices had used to operate. As Nest is a company owned by Alphabet (Google's parent company), the EFF argues this sets a "terrible precedent for a company with ambitions to sell self-driving cars, medical devices, and other high-end gadgets that may be essential to a person's livelihood or physical safety." Owners should be free to point their devices to a different server or collaborate on improved software. But such action violates the United States DMCA section 1201, which only has an exemption for "local use". This forces tinkerers who want to keep using their own equipment into a legal grey area. EFF thinks buyers should refuse electronics and software that prioritize the manufacturer's wishes above their own. Examples of post-sale manipulations include Google Nest Revolv, disabled privacy settings on Android, Sony disabling Linux on PlayStation 3, enforced EULA on Wii U.

IV.FUTURE

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. IoT creates opportunities for more direct integration of the physical world into computer-based systems, resulting in efficiency improvements, economic benefits, and reduced human exertions. The number of IoT devices increased 31% year-over-year to 8.4 billion in the year 2017 and it is estimated that there will be 30 billion devices by 2020. The global market value of IoT is projected to reach $7.1 trillion by 2020. 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 and intelligent cyber-physical systems to be deployed in real environments.

V.CONCLUSIONS

IoT literally, has changed the landscape, of data communication and transfer. Emerging breakthroughs like IoT has made a mark of its own across different disciplines like health, education, logistics, communication, technology, manufacturing, services etc. IoT offers a sea of

 DOI : 10.18231/2454-9150.2018.1293

opportunities to all stakeholders like technologists, scientists, practioners, marketers, academicians, analysts, programmers, , engineers etc . Simply, IoT has been a forerunner in integrating different disciplines like computer science, business management, industrial engineering, information technology, networking, electronics, etc. IoT has been gradually making our life simpler and more comfortable, though various technologies and applications. To create a vast, reliable IoT network we need compatible standards. Connected objects need to be able to speak to each other to transfer data and share what they are recording. If they all run on different standards, they struggle to communicate and share. "Additional needs are emerging for standardisation,". If standardisation happens it will let more devices and applications be connected. Microsoft has introduced its own system for IoT devices known as IoT Central. The system gives businesses a managed central platform for setting up IoT devices. Microsoft claims the system will simply the creation of IoT networks. The Hypercat standard is now supported by ARM, Intel, Amey, Bae Systems and Accenture and the firms are currently agreeing on a format for "exposing collections" of URLs, for example. "In the short term, IoT will impact on anything where there is a high cost of not intervening for example simpler day-to-day issues – like finding a car parking space in busy areas, linking up your home entertainment system and using your fridge webcam to check if you need more milk on the way home. "Ultimately what makes it exciting is that we don't yet know the exact use cases and just that it has the potential to have a major impact on our lives.

The IoT can realize the seamless integration of various manufacturing devices equipped with sensing, identification, processing, communication, actuation, and networking capabilities. Based on such a highly integrated smart cyber physical space, it opens the door to create whole new business and market opportunities for 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. Though, IoT has abundant benefits, there are some flaws in the IoT governance and implementation level. Universal standardizations are required in architectural level. Technologies are varying from vendor-vendor, so needs to be interoperable.

REFERENCES

[1]Aggarwal, R. and Lal Das, M. (2012) RFID Security in the Context of "Internet of Things". First *International Conference* on Security of Internet of Things, Kerala, 17-19 August 2012, 51-56. http://dx.doi.org/10.1145/2490428.2490435

[2]Biddlecombe, E. (2009). UN Predicts,"Internet of Things".

[3] Burgess, M. (2018). What is the Internet of Things, WIRED explains

[4]Drew, H. (2015). *"The Trouble with the Internet of Things", London Datastore. Greater London Authority*.

[5]Eric, B. (2016). "Who Needs the Internet of Things?", *Linux.com.*

[6]Graham, M. and Haarstad, H. (2011). Transparency and Development: Ethical Consumption through Web 2.0 and the Internet of Things.

[7]Kosmatos, E.A., Tselikas, N.D. and Boucouvalas, A.C. (2011) Integrating RFIDs and Smart Objects into a Unified Internet of Things Architecture. Advances in Internet of Things: Scientific Research, 1, 5-12. http://dx.doi.org/10.4236/ait.2011.11002

[8]Wigmore, I. (2014). "Internet of Things (IoT)". *TechTarget.*

 DOI : 10.18231/2454-9150.2018.1293