ISSN No. 0976-5697

Volume 7, No. 2, March-April 2016

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Internet of Things: A Look at Paradigm Shifting Applications and Challenges

Dr.P.B.Pathak
Assistant Professor and Head, Department of Computer Science & Information Technology
Yeshwant Mahavidyalaya Nanded
Maharashtra, India

Abstract: The Internet of Things is a combination of Internet, sensors, interconnected computing devices and everyday things or objects with the ability to communicate with each other without human intervention. The Internet of Things is extending connectivity and computing capability to sensors and everyday things or objects to collect exchange and analyze data. Applications of Internet of Things are widespread and possess the potential to deliver significant benefits to users across a range of areas. Security, privacy, property and liability are serious challenges of Internet of Things. The present paper discusses the concept of Internet of Things, applications and challenges.

Keywords: Internet; Things; Sensors; Ecosystem; Security; Privacy

I. INTRODUCTION

The Internet of Things is potentially beneficial, revolutionary and fully interconnected smart world of progress, efficiency, and opportunity. The term Internet of Things refers to the extension of connectivity, computing capability to objects, devices, and sensors for data collection, analysis, and management. Internet of Things is an interconnected environment of objects having ability to communicate with each other. The Internet of Things is an ecosystem of ubiquitous computing. The Internet of Things is the combination of computers, sensors, and networks to monitor and control devices. [1,13] The recent confluence of ubiquitous connectivity, adoption of Internet Protocol, miniaturization, advances in data analytics, and cloud computing, realized the concept of Internet of Things. Internet of Things has four key elements devices, wireless networks, Internet, data storage and data analysis capability. Exponential growth in number of connected smart devices and the convergence of low cost high speed connectivity; enhanced computing and processing power; availability of large data storage, sensors and IPv6's massive address space are the factors responsible for rapid proliferation of Internet of Things. [7]

The Internet of Things is a fast emerging ecosystem with the tremendous potential to deliver significant benefits like cost efficiency, improved asset utilization, enhanced processing capability and increased productivity. Cost efficient and huge cloud storage and the data acquisition and analysis capabilities have greatly contributed to rapid expansion and adoption of Internet of Things. Two main features of an Internet of Things object are its ability to capture data via sensors and transmit data over the Internet. Interconnected devices can collect and analyze significant amounts of data in real time, helpful in decision making to maximize time and cost savings. All opportunities come with some challenges and Internet of Things is no exception. Embedded wearable devices have widespread beneficial applications as well challenges resulting from amplified connectivity. [3,9] Data losses, malware infection, unauthorized access to personal data, misuse of wearable devices, unlawful surveillance are challenges of Internet of Things. The Internet of Things raises significant challenges like security, personal data protection and privacy. Personal or commercially sensitive data can be collected analyzed used and stored by interconnected devices without appropriate consent. The Internet of Things users are installing smart devices in large number in their homes creating vulnerabilities which can be used to compromise personal information. Malfunctioning devices can create security vulnerabilities. The Internet of Things device with no ability to upgrade or, with no visibility to its working and deployed at the place with no physical security can create security vulnerability. Multiple Internet of Things devices with same characteristics can magnify the severity of security vulnerability. Significant security challenge is long term support and management to address long term vulnerabilities. [15,19]

Deployment of Internet of Things devices on massive scale with ability to establish connection and communicate with other devices on their own in an unpredictable and dynamic fashion is a security challenge. The Internet of Things devices abandoned or deployed in circumstances where it is difficult to reconfigure can create serious security problems. Considering evolving security threats, the security mechanisms that are adequate at the time of deployment may not be adequate for the full lifetime of the device. The user may not be aware sometimes that some Internet of Things devices for surveillance and tracking embedded in the environment allowing a security breach to exist. Cybercriminals can use the sophistication, ubiquity, familiarity of Internet of Things technology to harm individual physically, financially. The data source can encounter an unwanted intrusion without consent, control, choice, and awareness. [5] Interoperability, standards, protocols, and conventions are essential for widespread development and adoption of Internet of Things. Every Internet connected object is entry point for the cybercriminals. Liability and privacy become serious problems when machines replace humans as the decision makers and sensors continuously capture data. Embedded intelligent and interconnected devices pose a security challenge of intrusion and interference that can compromise personal privacy and threaten public safety. Unauthorized access and misuse of personal information by cybercriminals, attacks on systems and physical safety problems are potential security challenges. Global dependence of the highly interconnected Internet of Things devices for essential services, create increased security and resilience opportunities for cybercriminals. Though security measures are

evolving along with network evolution, a multi layered security approach is needed. [11,17]

II. THE INTERNET OF THINGS APPLICATIONS AND CHALLENGES

The Internet of Things technology is quickly changing the way of interaction with the world. Like all technologies, the Internet of Things has applications and challenges. Despite important applications, increased connectivity, the Internet of Things may create a number of security and privacy challenges. The Internet of Things has a potential to deliver significant applications to users across wide range of sectors. The applications of Internet of Things falls in two categories one information analysis other automation and control. The Internet of Things finds its potential applications in areas such as agriculture, healthcare, manufacturing, environment, finance and insurance. Internet of Things applications benefits in ensuring safety, security, efficiency, decision making, and critical infrastructure protection. [2,8]

Wearable remote patient monitoring healthcare devices, monitor fitness exercise, sleep and other health habits allowing patients and their doctors to obtain real time access to patient's health data. Hospitals can use Internet of Things technology to collect and hold massive amounts of data to infer actionable intelligence for treatments. Internet of Things enabled scanners can give hospital stock shortages information. Embedded sensors can monitor integrity and safety of nation's critical infrastructure. Electricity smart grid technologies drive greater efficiencies in both energy production and consumption as well can streamline troubleshooting. Asset location tracking for efficient management can be done by embedding sensors into objects and using wireless connectivity. An idea of smart cities can be realized by implementing Internet of Things technology. [14,20] Internet of Things finds its application in banking and financial sector to anticipate customer's requirements and respond them. Shipping industry can use cloud based Internet of Things technology for variety of benefits including monitoring shipments, weather, sea conditions, improved sea journey optimization, ensuring safety, efficiency, coordination and communications among various control centers for fuel, engine, traffic conditions, entertainment and telemedicine. [4,10] The Internet of Things can make homes smart using communicating smart objects to provide benefit including cost; energy efficiency, selling; buying homes, ensuring protection from natural disasters like floods; fires; structural weakness, predict future problems. Aerospace industry can use Internet of Things to improve the aircraft safety and maintenance measures by capturing real time data on engine performance. In agriculture, farmers can use embedded Internet of Things technology, in their fields, to monitor and decision making of use of critical resources and crop conditions. The Internet of Things in food production and distribution are very much useful. Data collected by embedded sensors can help businesses to identify in real time inefficiencies and bottlenecks, both buyer and seller can benefit from Internet of Things. Manufacturers can use Internet of Things products to ensure the integrity, quality, safety, and security. Internet of Things devices assure to revolutionize design, security, and maintenance in sensitive area of manufacturing. Data collecting sensors embedded in instruments and equipments can communicate problems, track resources and data processing software's takes decisions and makes it easy to work more efficiently. Internet of Things possesses the ability to reduce injuries, deaths and ensures employees safety, especially those working in hazardous working conditions. Internet of Things impacts transportation on a large scale. Roadways can be monitored via sensors to keep them as safe. Governments can use the Internet of Things for improving service delivery and responsiveness to the citizens. [16,21]

Internet of Things is accelerating globally at an amazing rate raising concerns about security challenges. Commercialization is responsible for rapid spread of Internet of Things and expanded security challenges. The vast variety of Internet of Things devices and applications poses an equally vast variety of security and safety challenges. Cyberattacker use vulnerabilities such as weak passwords, insecure password recovery mechanisms, poorly protected credentials, etc. to gain access to Internet of Things device. Poorly secured Internet of Things devices and services can be potential entry points for cyberattacks. The prominent reasons for amplified security challenge include deployment of devices at very large scale, the ability of devices to automatically connect to other devices, and the deployment of these devices in unsecure physical environments. Privacy, authentication & authorization, transport encryption, cloud service & web interface, software & firmware are some security challenges of Internet of Things. [6,12] The Internet of Things presents a variety of potential security challenges that can be exploited to harm users by enabling unauthorized access and misuse of personal information, facilitating attacks on other systems and creating risks to personal safety. Rapid evolution, connectivity, interoperability, power management, security, privacy, liability, complexity, data storage, legal, regulatory and rights are some key challenges of Internet of Things. Internet of Things amplifies concerns of increased surveillance and tracking, and the strength of combining data streams from users. Personally identifiable data collected without the consent and knowledge raises serious privacy challenge. The challenge is also availability of spectrum and bandwidth for efficient communication. Internet of Things devices collecting data about people in one jurisdiction and transmitting it to another jurisdiction with different data protection laws for processing creates legal challenge of cross border data flow. [18,22]

III. CONCLUSION

The Internet of Things is continuously evolving. Though it is very difficult to define Internet of Things precisely various definitions implies that the Internet of Things as a network connectivity and computing capability extended to the collection of objects, devices, sensors, and everyday items to generate, exchange, and use data with no human intervention. Convergence of ubiquitous connectivity, adoption of the global standard Internet Protocol, availability of greater computing power at lower price, miniaturization of sensor, advances in data analysis capabilities, rise of cloud computing are some of the factors responsible for rapid proliferation of Internet of Things. The Internet of Things finds its applications and benefits to almost all sectors to make our life easier and comfortable. The Internet of Things also presents some serious challenges.

IV. REFERENCES

[1] Technology & Communications, "The Internet of Things-A Study in Hype, Reality, Disruption, and Growth",(2014), http://www.vidyo.com/wp-content/uploads/The-Internet-of-Things-A-Study-in-Hype-Reality-Disruption-and-Growt....pdf

[2] White Paper on, "The Internet of Things: Security Research Study", (2015),

https://www.veracode.com/sites/default/files/Resources/Whitepapers/internet-of-things-whitepaper.pdf

[3] Essential Guide, "IoT analytics guide: Understanding Internet of Things data" ,(2015),
http://searchbusinessanalytics.techtarget.com/essentialguide/IoT-analytics-guide-Understanding-Internet-of-Things-data

[4] Dave Evans, White paper on, "The Internet of Things How the Next Evolution of the Internet Is Changing Everything", (2011),
http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

[5] Techopedia, "Internet of Things", (2015),
https://www.techopedia.com/definition/28247/internet-of-things-iot

[6] McKinsey Global Institute, "The Internet of Things: Mapping The Value Beyond The Hype", (2015),
https://www.mckinsey.de/sites/mck_files/files/unlocking_the_potential_of_the_internet_of_things_full_report.pdf

[7] "The Internet of Things: Evolution or Revolution?",(2015),
http://www.aig.com/Chartis/internet/US/en/AIG%20White%20Paper%20-%20IoT%20English%20DIGITAL_tcm3171-677828_tcm3171-698578.pdf

[8] White Paper on, "Security in the Internet of Things-Lessons from the Past for the Connected Future", (2015),
http://www.windriver.com/whitepapers/security-in-the-internet-of-things/wr_security-in-the-internet-of-things.pdf

[9] "The Internet of Things: An Overview-Understanding the Issues and Challenges in More Connected World", (2015),
https://www.internetsociety.org/sites/default/files/ISOC-IoT-Overview-20151014_0.pdf

[10] Pew Research Center, "The Internet of Things Will Thrive by 2025", (2014),
http://www.pewinternet.org/2014/05/14/internet-of-things/

[11] Daniel Castro & Jordan Misra, "The Internet of Things", (2013),
www2.datainnovation.org/2013-internet-of-things.pdf

[12] Lopez Research, "An Introduction to the Internet of Things (IoT)", (2013),
http://www.cisco.com/c/dam/en_us/solutions/trends/iot/introduction_to_IoT_november.pdf

[13] "Internet of Things-Privacy & Security in a Connected World", (2015),
https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

[14] Ovidiu Vermesan, Peter Fries, "Internet of Things-From Research and Innovation to Market Deployment", (2014)
http://www.internet-of-things-research.eu/pdf/IoT-From%20Research%20and%20Innovation%20to%20Market%20Deployment_IERC_Cluster_eBook_978-87-93102-95-8_P.pdf

[15] "The Working Party on the Protection of Individuals With Regard to the Processing of Personal Data", (2014),
http://ec.europa.eu/justice/data-protection/article-29/files/tasks-art-29_en.pdf

[16] Ovidiu Vermesan, Peter Fries, "Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems", (2013),
http://www.internet-of-things-research.eu/pdf/Converging_Technologies_for_Smart_Environments_and_Integrated_Ecosystems_IERC_Book_Open_Access_2013.pdf

[17] White paper on "Realizing the Potential of The Internet of Things: Recommendations to Policy Makers", (2015),
https://www.tiaonline.org/sites/default/files/pages/TIA-White-Paper-Realizing_the_Potential_of_the_Internet_of_Things.pdf

[18] Jim Chase, The White Paper on, "The Evolution of the Internet of Things", (2013),
http://www.ti.com/lit/ml/swrb028/swrb028.pdf

[19] "Reaping the Benefits of the Internet of Things", (2014),
http://www.cognizant.com/InsightsWhitepapers/Reaping-the-Benefits-of-the-Internet-of-Things.pdf

[20] "The Internet of Things-Research Study", (2015),
http://www8.hp.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf

[21] P.B.Pathak, "Internet of Things: An Overview of the Emerging Technology", IJNRCSSE, Volume 3, Issue 1, pp: (167-170), Month: January-April (2016)

[22] P.B.Pathak, "Internet of Things: Understanding the Security Concerns", IJARCET, Volume 5, Issue 3, pp: (820-822), Month: March (2016)

