

An Overview of the IOT Technology, Its Applications and Security Challenges

Mr. Ajay Lotheta

Assistant Professor, UIT, HP UNIVERSITY

Abstract

The Internet today has become ubiquitous and has touched almost every corner of the world. Its affecting human life in unimaginable ways. We are now entering an era of almost all pervasive connectivity where a wide variety of appliances will be connected to the web and will be able receive transmit data to the various systems and devices connected to each other through the various networking and transmission technologies. Out of the potential Internet of Things application areas; Smart Cities , Smart Car and mobility, Smart Home and assisted living, Smart Industries, Public safety, Energy & Environmental protection, Agriculture and Tourism as part of a future IoT Ecosystem have acquired high attention. The present paper aims at studying the IoT systems, its applications and the various security issues in the various fields.

1. IoT Ecosystem

The term IoT was first coined by Kevin Ashton in 1999 with reference to the supply chain management [1]. The concept of IoT revolves around the word “smartness” – “an ability to independently obtain and apply knowledge” Therefore, IoT refers to the “things or devices and sensors” that are smart, uniquely addressable based on their communication protocols, and are adaptable and autonomous with inherent security [2].

Atzori have characterized IoT in three visions.

1. Internet Oriented–the vision focuses on connectivity between the objects;
2. Things Oriented- the vision focuses on generic objects; and
3. Knowledge Oriented – the vision focuses on how to represent, store and organize information. These visions paved towards International Telecommunication Union (ITU) vision of IoT, which defines it as *“from anytime, anyplace connectivity for anyone; we will now have the connectivity of the smart objects”*[3][4].

2. CHARACTERISTICS OF the IoT:

Some most popular characteristics of Internet of things are: (a) Intelligence (b) Connectivity (c) Dynamic Nature (d) Enormous scale (e) Sensing (f) Heterogeneity (g) Security

(a) Intelligence

IoT comes with the combination of algorithms and computation, software & hardware that makes it smart. Ambient intelligence in IoT enhances its capabilities which facilitate the things to respond in an intelligent way to a particular situation and supports them in carrying out specific tasks[5][6]. In spite of all the popularity of smart technologies, intelligence in IoT is only concerned as means of interaction between devices, while user and device interaction is achieved by standard input methods and graphical

user interface [7][8]. Together algorithms and computer (i.e. software & hardware) provide the “intelligent spark” that makes a product experience smart. Consider Misfit Shine, a fitness tracker, compared to Nest’s intelligent thermostat. The Shine experience distributes compute tasks between a smartphone and the cloud. The Nest thermostat has more computational horsepower for the AI that make them smart.

(b) Connectivity

Connectivity empowers Internet of Things by bringing together everyday objects. Connectivity of these objects is pivotal because simple object level interactions contribute towards collective intelligence in IoT network [9]. It enables network accessibility and compatibility in the things. With this connectivity, new market opportunities for Internet of things can be created by the networking of smart things and applications. Connectivity in the IoT is more than adding a Wi-Fi module. Connectivity enables network accessibility and compatibility. Accessibility is getting on a network while compatibility provides the common ability to consume and produce data. If this sounds familiar, that’s because it is Metcalfe’s Law and it rings true for IoT [10].

(c) Dynamic Nature

The primary activity of Internet of Things is to collect data from its environment, this is achieved with the dynamic changes that take place around the devices. The state of these devices change dynamically, example sleeping and waking up, connected and/or disconnected as well as the context of devices including temperature, location and speed. In addition to the state of the device, the number of devices also changes dynamically with a person, place and time. The state of devices change dynamically, e.g., sleeping and waking up, connected and/or disconnected as well as the context of devices including location and speed. Moreover, the number of devices can change dynamically [11].

(d) Enormous Scale

The number of devices that need to be managed and that communicate with each other will be much larger than the devices connected to the current Internet. The management of data generated from these devices and their interpretation for application purposes becomes more critical.

Gartner (2015) confirms the enormous scale of IoT in the estimated report where it stated that 5.5 million new things will get connected every day and 6.4 billion connected things will be in use worldwide in 2016, which is up by 30 percent from 2015. The report also forecasts that the number of connected devices will reach 20.8 billion by 2020. The number of devices that need to be managed and that communicate with each other will be at least an order of magnitude larger than the devices connected to the current Internet. Even more critical will be the management of the data generated and their interpretation for application purposes.

(e) Sensing

IoT wouldn’t be possible without sensors which will detect or measure any changes in the environment to generate data that can report on their status or even interact with the environment. Sensing technologies provide the means to create capabilities that reflect a true awareness of the physical world and the people in it. The sensing information is simply the analogue input from the physical world, but it can provide the rich understanding of our complex world [12] [13]. We tend to take for granted our senses and ability to understand the physical world and people around us. Sensing technologies provide us with the means to create experiences that reflect a true awareness of the physical world and the people in it. This is simply the analog input from the physical world, but it can provide rich understanding of our complex world.

(f) Heterogeneity

Heterogeneity in Internet of Things as one of the key characteristics. Devices in IoT are based on different hardware platforms and networks and can interact with other devices or service platforms through different networks. IoT architecture should support direct network connectivity between heterogeneous networks. The key design requirements for heterogeneous things and their environments in IoT are scalabilities, modularity, extensibility and interoperability. The devices in the IoT are heterogeneous as based on different hardware platforms and networks. They can interact with other devices or service platforms through different networks [14].

(g) Security

IoT devices are naturally vulnerable to security threats. As we gain efficiencies, novel experiences, and other benefits from the IoT, it would be a mistake to forget about security concerns associated with it. There is a high level of transparency and privacy issues with IoT. It is important to secure the endpoints, the networks, and the data that is transferred across all of it means creating a security paradigm.

4. APPLICATIONS OF INTERNET OF THINGS (IOT):

Some useful applications of Internet of Things (IOT) are:

(a) Connected Health (b) Smart City (c) Connected cars (d) Smart Home (e) Smart Farming (f) Smart Retail (g) Smart Supply Chain

(a) Connected Health Systems

Telemedicine, Health (Digital Health/Tele IoT) have various applications in healthcare, which are from remote monitoring equipment to advance & smart sensors to equipment integration. It has the potential to improve how physicians deliver care and also keep patients safe and healthy. Healthcare IoT can allow patients to spend more time interacting with their doctors by which it can boost patient engagement and satisfaction. From personal fitness sensors to surgical robots, IoT in healthcare brings new tools updated with the latest technology in the ecosystem that helps in developing better healthcare. IoT helps in revolutionizing healthcare and provides pocket-friendly solutions for the patient and healthcare professional [15][16].

The concept of connected healthcare system and smart medical devices bears enormous potential not just for companies, but also for the well-being of people in general. Research shows IoT in healthcare will be massive in coming years. IoT in healthcare is aimed at empowering people to live healthier life by wearing connected devices. The collected data will help in personalized analysis of an individual's health and provide tailor made strategies to combat illness.

(b) Smart City

Smart city is another powerful application of IoT generating curiosity among world's population. Smart surveillance, smarter energy management systems, automated transportation, water distribution, urban security and environmental monitoring all are examples of internet of things applications for smart cities.

IoT will solve major problems faced by the people living in cities like pollution, traffic congestion and shortage of energy supplies etc. Products like cellular communication enabled Smart Belly trash will send alerts to municipal services when a bin needs to be emptied [17]. By installing sensors and using web applications, citizens can find free available parking slots across the city. Also, the sensors can detect meter tampering issues, general malfunctions and any installation issues in the electricity system.

(c) Connected Cars:

The automotive digital technology has focused on optimizing vehicles internal functions. But now, this attention is growing towards enhancing the in-car experience.

A connected car is a vehicle which is able to optimize its own operation, maintenance as well as comfort of passengers using onboard sensors and internet connectivity. Connected car technology is a vast and an extensive network of multiple sensors, antennas, embedded software, and technologies that assist in communication to navigate in our complex world. It has the responsibility of making decisions with consistency, accuracy, and speed. It also has to be reliable. These requirements will become even more critical when humans give up entirely the control of the steering wheel and brakes to the autonomous or automated. Most large auto makers as well as some brave startups are working on connected car solutions. Major brands like Tesla, BMW, Apple, and Google are working on bringing the next revolution in automobiles [18].

(d) Smart Homes

Smart homes have become the revolutionary ladder of success in the residential spaces and it is predicted Smart homes will become as common as smartphones. Whenever we think of IoT systems, the most important and efficient application that stands out every time is Smart Home ranking as highest IOT application on all channels. The estimated amount of funding for Smart Home startups exceeds \$2.5bn and is ever growing. Wouldn't you love if you could switch on air conditioning before reaching home or switch off lights even after you have left home? Or unlock the doors to friends for temporary access even when you are not at home. Don't be surprised with IoT taking shape companies are building products to make your life simpler and convenient .

The cost of owning a house is the biggest expense in a homeowner's life. Smart Home products are promised to save time, energy and money. With Smart home companies like Nest, Ecobee, Ring and August, to name a few, will become household brands and are planning to deliver a never seen before experience [19].

(e) Smart Farming

Smart farming is an often overlooked IoT application. However, because the number of farming operations is usually remote and the large number of livestock that farmers work on, all of this can be monitored by the Internet of Things and can also revolutionize the way farmers work. But this idea is yet to reach a large-scale attention. Nevertheless, it still remains to be one of the IoT applications that should not be underestimated. Smart farming has the potential to become an important application field specifically in the agricultural-product exporting countries.

(f) Smart Retail

Retailers have started adopting IoT solutions and using IoT embedded systems across a number of applications that improve store operations such as increasing purchases, reducing theft, enabling inventory management, and enhancing the consumer's shopping experience. Through IoT physical retailers can compete against online challengers more strongly. They can regain their lost market share and attract consumers into the store, thus making it easier for them to buy more while saving money [20].

The potential of IoT in the retail sector is enormous. IoT provides an opportunity to retailers to connect with the customers to enhance the in-store experience. Smartphones will be the way for retailers to remain connected with their consumers even out of store. Interacting through Smartphones and using

Beacon technology can help retailers serve their consumers better. They can also track consumer's path through a store and improve store layout and place premium products in high traffic areas [21].

(g) Smart Supply Chain

Supply chains have already been getting smarter for a couple of years. Offering solutions to problems like tracking of goods while they are on the road or in transit, or helping suppliers exchange inventory information are some of the popular applications.

5. SECURITY CHALLENGES FACING IoT

IoT security is the protection of Internet of Things devices from attack. While many business owners are aware that they need to protect computers and phones with antivirus, the security risks related to IoT devices are less well known and their protection is too often neglected. Internet of Things devices are everywhere. From cars and fridges to monitoring devices on assembly lines, objects around us are increasingly being connected to the internet. The speed at which the IoT market is growing is staggering - Juniper research estimates that the number of IoT sensors and devices is set to exceed 50 billion by 2022. While consumer IoT devices allow lifestyle benefits, businesses are quickly adopting IoT devices due to high potential for savings [21].

(a) Data Integrity

Billions of devices come under the umbrella of an interlinked ecosystem that is connected through IoT. Manipulating even a single data point will result in manipulation of the entire data which is exchanged and shared back and forth from the sensor to the main server. Decentralized distributed ledger and digital signatures should be implemented in order to ensure integrity [22].

(b) Encryption Capabilities

Data encryption and decryption is a continuous process. The IoT network's sensors still lack the capability to process. The brute force attempts can be prevented by firewalls and segregating the devices into separate networks.

(c) Privacy Issues

IoT is all about the exchange of data among various platforms, devices, and consumers. The smart devices gather data for a number of reasons, like, improving efficiency and experience, decision making, providing better service, etc.; thus, the end point of data shall be completely secured and safeguarded.

(d) Common Framework

There is an absence of a common framework and so all the manufacturers have to manage the security and retain the privacy on their own. Once a common standardized framework is implemented, the individual efforts will then collectively be utilized in an expandable manner and so reusability of code can be achieved [23].

(e) Automation

Eventually, enterprises will have to deal with more and more number of IoT devices. This enormous amount of user data can be difficult to manage. The fact cannot be denied that it requires a single error or trespassing a single algorithm to bring down the entire infrastructure of the data [24].

(f) Updates

Managing the update of millions of devices needs to be adhered to, respectively. Not all the devices support over the air update and hence it requires manually updating the devices. One will need to keep a track of the available updates and apply the same to all the varied devices. This process becomes time-consuming and complicated and if any mistake happens in the process then this shall lead to loopholes in

the security later. Security Investment in securing infrastructure and network should be the first priority, which is not the case now. IoT involves the use of millions of data points and each point should be secured. Indeed, the need is for the multi-layer security, i.e., security at each and every level. From end-point devices, cloud platforms, embedded software to web and mobile applications that leverage IoT (Internet of Things), each layer should be security intact. With the set of heterogeneous devices, security becomes complex.

5. CONCLUSION

The IoT framework is vulnerable to attacks at each layer. Therefore, there are many security threats and requirements that need to be dispatched. Current state of research in IoT is mainly concentrated on authentication and access control protocols, but with the rapid growth of technology it is essential to consolidate new networking protocols like IPv6 and 5G to achieve the progressive mash up of IoT topology. Due to lack of security mechanism in IoT devices, many IoT devices become soft targets and even this is not in the victim's knowledge of being infected.. In this paper, different aspects of IoT are discussed. We hope this paper will be useful to researchers in the IoT field by helping identify the major issues in IoT.

6. ETHICS

This Research paper is original and not published in any conferences or in any journal.

REFERENCES

1. R.Vignesh and 2A.Samydurai ans1 Student, 2Associate Professor Security on Internet of Things (IOT) with Challenges and Countermeasures in 2017 IJEDR | Volume 5, Issue 1 | ISSN: 2321-9939.
2. N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of computation*, vol. 48, 203-209, 1987.
3. J.-Y. Lee, W.-C.Lin, and Y.-H. Huang, "A lightweight authentication protocol for internet of things," in *Int'l Symposium on Next-Generation Electronics (ISNE)*, 1-2, 2014.
4. Y. Xie and D. Wang, "An Item-Level Access Control Framework for Inter-System Security in the Internet of Things," in *Applied Mechanics and Materials*, 1430-1432, 2014.
5. B. Anggorojati, P. N. Mahalle, N. R. Prasad, and R. Prasad, "Capability-based access control delegation model on the federated IoT network," in *Int'l Symposium on Wireless Personal Multimedia Communications (WPMC)*, 604-608, 2012.
6. M. Castrucci, A. Neri, F. Caldeira, J. Aubert, D. Khadraoui, M. Aubigny, et al., "Design and implementation of a mediation system enabling secure communication among Critical Infrastructures," *Int'l Journal of Critical Infrastructure Protection*, vol. 5, 86-97, 2012.
7. R. Neisse, G. Steri, and G. Baldini, "Enforcement of security policy rules for the internet of things," in *Int'l Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, 165-172, 2014.
8. Mirza Abdur Razzaq and Muhammad Ali Qureshi "Security Issues in the Internet of Things (IoT): A Comprehensive Study" by (IJACSA) *International Journal of Advanced Computer Science and Applications*, Vol. 8, No. 6, 2017. [9] J. S. Kumar and D. R. Patel, "A survey on internet of things: Security and privacy issues," *International Journal of Computer Applications*, vol. 90, no. 11, 2014.
9. M. Abomhara and G. M. Køien, "Security and privacy in the internet of things: Current status and open issues," in *Privacy and Security in Mobile Systems (PRISMS)*, *International Conference on*.

- IEEE, 2014, pp. 1–8.
10. S. Chen, H. Xu, D. Liu, B. Hu, and H. Wang, “A vision of iot: Applications, challenges, and opportunities with china Published by, www.ijert.org 6 Volume 7, Issue 12 International Journal of Engineering Research & Technology (IJERT) Special Issue - 2019 ISSN: 2278-0181 NCRIETS – 2019 Conference Proceedings perspective,” IEEE Internet of Things journal, vol. 1, no. 4, pp. 349–359, 2014.
 11. L. Atzori, A. Iera, and G. Morabito, “The internet of things: A survey,” Comput. Netw. vol. 54, no. 15, pp. 2787–2805, Oct 2010.
 12. M. M. Hossain, M. Fotouhi, and R. Hasan, “Towards an analysis of security issues, challenges, and open problems in the internet of things,” in Services (SERVICES), 2015 IEEE World Congress on. IEEE, 2015, pp. 21–28.
 13. L. Da Xu, W. He, and S. Li, “Internet of things in industries: A survey,” IEEE Transactions on industrial informatics, vol. 10, no. 4, pp. 2233–2243, 2014.
 14. L. M. R. Tarouco, L. M. Bertholdo, L. Z. Granville, L. M. R. Arbiza, F. Carbone, M. Marotta, and J. J. C. de Santana, “Internet of things in healthcare: Interoperability and security issues,” in Communications (ICC), IEEE International Conference on. IEEE, 2012, pp. 6121–6125.
 15. A. Mohan, “Cyber security for personal medical devices internet of things,” in Distributed Computing in Sensor Systems (DCOSS), 2014 IEEE International Conference on. IEEE, 2014, pp. 372–374.
 16. Mohamed Abomhara and Geir M. Køien” Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks”.
 17. S. De, P. Barnaghi, M. Bauer, and S. Meissner, “Service modelling for the internet of things,” in Computer Science and Information Systems (FedCSIS), 2011 Federated Conference on. IEEE, 2011, pp. 949–955.
 18. G. Xiao, J. Guo, L. Xu, and Z. Gong, “User interoperability with heterogeneous iot devices through transformation,” 2014.
 19. J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of things (iot): A vision, architectural elements, and future directions,” Future Generation Computer Systems, vol. 29, no. 7, pp. 1645–1660, 2013.
 20. M. Zorzi, A. Gluhak, S. Lange, and A. Bassi, “From today’s intranet of things to a future internet of things: a wireless-and mobility-related view,” Wireless Communications, IEEE, vol. 17, no. 6, pp. 44–51, 2010.
 21. C. Hong song, F. Zhongchuan, and Z. Dongyan, “Security and trust research in m2m system,” in Vehicular Electronics and Safety (ICVES), 2011 IEEE International Conference on. IEEE, 2011, pp. 286–290.
 22. I. Cha, Y. Shah, A. U. Schmidt, A. Leicher, and M. V. Meyerstein, “Trust in m2 communication,” Vehicular Technology Magazine, IEEE, vol. 4, no. 3, pp. 69–75, 2009.
 23. J. Lopez, R. Roman, and C. Alcaraz, “Analysis of security threats, requirements, technologies and standards in wireless sensor networks. Published by, www.ijert.org