A Survey And Research Challenges In Internet of Things

K.Pavithradevi[1], C.Jayapriya[2], S.Karthiga[3]
[1, 2, 3] Dept of Computer Applications
[1, 2, 3] Gnanamani College of Technology, Namakkal

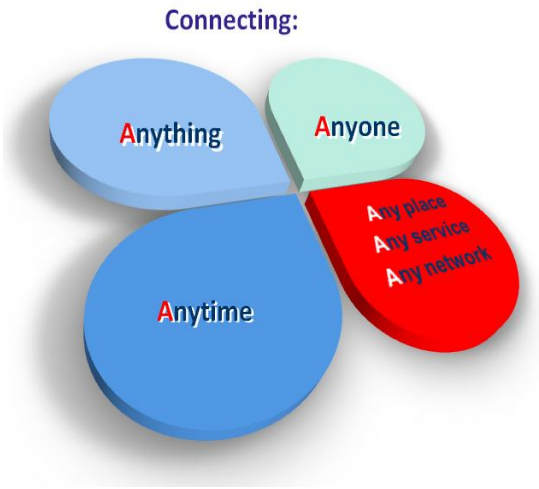
Abstract- *The terminology Internet of Things (IoT) refers to a future where every day physical objects are connected by the Internet in one form or the other, but outside the traditional desktop realm. The successful emergence of the IoT vision, however, will require computing to extend past traditional scenarios involving portables and smart-phones to the connection of everyday physical objects and the integration of intelligence with the environment. Subsequently, this will lead to the development of new computing features and challenges. The main purpose of this paper, therefore, is to investigate the features, challenges, and weaknesses that will come about, as the IoT becomes reality with the connection of more and more physical objects. Specifically, the study seeks to assess emergent challenges due to denial of service attacks, eavesdropping, node capture in the IoT infrastructure, and physical security of the sensors. The methodology paradigm used was qualitative in nature with an exploratory research design, while data was collected using the desk research method. We found that, in the distributed form of architecture in IoT, attackers could hijack unsecured network devices converting them into bots to attack third parties. Moreover, attackers could target communication channels and extract data from the information flow. Finally, the perceptual layer in distributed IoT architecture is also found to be vulnerable to node capture attacks, including physical capture, brute force attack, DDoS attacks, and node privacy leaks.*

Keywords- IoT,DDos,

I. INTRODUCTION

The internet of things is the internetworking of physical device, vehicles, buildings, and other items. Embedded with electronics, sensors, software network connectivity that enables these objects to collect and exchange data. The presence of all three aspects will be crucial in ensuring the achievement of context-aware computation and smart connectivity. At this point, the Internet will no longer only be accessible from smart-phones and laptops but will be part of such objects as cars, ovens, baby monitors, and TV sets. In addition, the IoT will become completely integrated into medical and other critical devices and pervade majority of sectors. Unfortunately, as with other major developments in the Internet era, growth in the IoT technology will be equally matched by growth in security and privacy concerns. Several researchers are pointing towards the evolving nature of challenges and vulnerabilities in various existing IoT devices. This research paper seeks to investigate the features, challenges, and vulnerabilities facing the new and dynamic realm of the IoT.

II. CONNECTING



III. CHARACTERISTICS

The IoT is a complex system with a number of characteristics. Its characteristics vary from one domain to another. Some of the general and key characteristics identified during the research study are as follows:

1. 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. 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.

2. 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. 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.

3. 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.

4. 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.

5. 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.

6. 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.

7. 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. There are a wide variety of technologies that are associated with Internet of Things that facilitate in its successful functioning. IoT technologies possess the above-mentioned characteristics which create value and support human activities; they further enhance the capabilities of the IoT network by mutual cooperation and becoming the part of the total system.

IV. IOT IS ABOUT CONNECTING DEVICES TO THE INTERNET

- Machines which have never been networked are coming online.
- Smart heating system that knows whether your home or not.
- Fridges that can tell you if you're running low on milk or a connected, self-driven car.
- The internet of things is set to change our world.

V. SENSORS

- Sensors allow the physical world to internet with computer, p
- Playing an important role in bridging the gap between the physical world and the virtual one.
- It allows a richer array of data, other than data available from keyboard and mouse input
- Currently, the internet is full of information that has been input by someone at the key board.
- But the concept of IOT will change that because we are at an inflexion point where more internet data original from sensors rather than keyboard inputs.
- A sensors is a device that can measures a physical quality and convert that physical quality into a signal that can be read by an instrument or an observer.

- The ability to detect changes in the physical status of things is also essential for recording changes in the environment.

Example:
- Sensors collect data from environment.
- Traffic control.

VI. RFID

- RFID(Radio Frequency Identification) is a system that transmit the data of an object or a person using radio waves for identifying or tracking the object or person.
- It is done by first attaching tag , known as the RFID tag , to the object or person.
- This tag will then be read by reader to determine its identification information.
- Using in some of the places are:
  1. Tracking employees at work.
  2. Monitoring bathroom breaks.
  3. Tracking students at school.
  4. Employees staying in a secure room too long.

VII. TOP APPLICATION

- Traffic monitoring
- Health
- Security
- Transport and logistics

VIII. JAWBONE UP

- Linked to an iphone application
- Not just a passive bracelet
- The application recommends to change life-style or diet.

IX. AUTO BOT

- Diagnostics service for cars
- Alert relatives in case of an accident
- Discovery service of car position
- Integrated with several web services.

X. ADVANTAGES

Data: The more the information , the easier it is to make the right decision. While you are out, without having to check on your own, not only saves times but is convenient as well.
Tracking: The computers keep a track both the quality and the viability of things at home . Eg: expiration data of product

Time: Time saved in monitoring.

Money: This technology called replaced human who are in charge of monitoring and maintaining supplies.

XI. DISADVANTAGE

Compatiability: This no standard for tagging and monitoring with sensors.

Complexity: There are several opportunities for failure with complex system.Eg : milk

Safety: There is a chance that the software can be hacked and your personal information misused. Hence, all the safety risk become the customers responsibility.

XII. CONCLUSION

In conclusion, the Internet of Things is closer to being implemented than the average person would think. Most of the necessary technological advances needed for it have already been made, and some manufacturers and agencies have already begun implementing a small-scale version of it. The main reasons why it has not truly been implemented is the impact it will have on the legal, ethical, security and social fields. Workers could potentially abuse it, hackers could potentially access it, corporations may not want to share their data, and individual people may not like the complete absence of privacy. For these reasons, the Internet of Things may very well be pushed back longer than it truly needs to be.

REFERENCES

[1] International Journal of Advanced Computer Science and Information Technology (IJACSIT) Vol. 4, No. 1, 2015, Page: 1-13, ISSN: 2296-1739-Internet of Things: Features, Challenges, and Vulnerabilities.
[2] Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions Jayavardhana Gubbi,a Rajkumar Buyya, Slaven Marusic,a Marimuthu Palaniswamia.
[3] International Journal of Software Engineering and Its Applications Vol. 9, No. 9 (2015), pp. 117-126-A Study on the Internet of Things (IoT) Applications-
Young-Mo Kang, Mi-Ran Han, Kyeong-Seok Han and Jong-Bae Kim.
[4] M. Tory, T. Moller, Rethinking Visualization: A High-Level Taxonomy, Information Visualization, 2004. INFOVIS 2004. IEEE Symposium on. (2004) 151–158.
[5] E. Welbourne, L. Battle, G. Cole, K. Gould, K. Rector, S. Raymer, et al., Building the Internet of Things Using

RFID The RFID Ecosystem Experience, IEEE Internet Computing 13 (2009) 48–55.

[6] A. Juels, RFID security and privacy: A research survey, IEEE Journal of Selected Areas in Communication 24 (2006) 381–394.

[7] A. Ghosh, S.K. Das, Coverage and connectivity issues in wireless sensor networks: A survey, Pervasive and Mobile Computing. 4 (2008) 303–334.

[8] Y. Sang, H. Shen, Y. Inoguchi, Y. Tan, N. Xiong, Secure Data Aggregation in Wireless Sensor Networks: A Survey, in: 2006: pp. 315–320.

[9] M. Zorzi, A. Gluhak, S. Lange, A. Bassi, From Today's Intranet of Things to a Future Internet of Things: A Wireless- and Mobility-Related View, IEEE Wireless Communication 17 (2010) 43–51.

[10] K.Pavithradevi, K.Ramya, S.Nandhini, G.Punitha, " History and Applications in Body Arear Network", International Journal for Research in Applied Science & Engineering Technology Vol 5, Issue II, February 2017

[11] K.Ramya and K.Pavithradevi "Effective Wireless Communication," International Journal of Advanced Research, volume4(12),pp. 1559-1562 Dec 2016.

[12] Dr.N.Muthumani, K.Pavithradevi, "Image Compression using ASWDR & 3D-Sphit Algorithms yor Satellite Data", International Journal of Scentific & Engineering Research,Volume 6, Issue 10, October-2015.Pages:289-296.

[13] T.Manjula, M.Manosakthi, C.Monika, K.Pavithradevi, "Android Application Security" ,International Journal for Research & Development in Technology, Volume 7, Issue -2, February 2017, Pages: 86 -89