Internet of Things Security Risk and Challenges

Ms. Shevale Rupali, Ms. Priti Shinde, Ms. Gaidhani Yogita

[1]Shevale Rupali (Assistant Professor), Dept. of Computer Engineering, MVPS'S KBTCOE, Nashik, Maharashtra, India
[2]Shinde Priti (Assistant Professor), Dept. of Computer Engineering, MVPS'S KBTCOE, Nashik, Maharashtra, India
[3]Gaidhani Yogita (Assistant Professor), Dept. of Computer Science, V. K. K Menon College, Bhandup, Mumbai, Maharashtra, India

---***---

Abstract - *In the last few decades, Internet of Things (IoT) has been a focus of research. IoT is a system of interrelated computing devices, mechanical and digital machines, or people that are provided with unique identifiers (UIDs) and the ability to transfer data in all over a network without requiring human-to-human or human-to-computer interaction. With the great prospective of IoT, there is many different types of issues and challenges. Security is one of the major issues for IoT technologies, applications, and other platforms. The key requirements for any IoT security solution are IoT Device and data security, including authentication of devices and confidentiality and integrity of data. Implementing and running security operations at IoT scale. Security is the top concern for IoT developer. IoT concept is materialize and evaluated swiftly. IoT is an combination between object link via internet. Security is a big challenge in IoT. The main goal of IoT security is to preserve privacy, ensure the security of user, infrastructure, data and devices of IoT.*

Key Words: **Internet of Things (IoT), Advantages and disadvantages, applications, challenges**

1. INTRODUCTION

This document is a template. An electronic copy can be downloaded from the conference website. For questions on paper guidelines, please contact the conference publications committee as indicated on the conference website. Information about for evaluation of new technologies it use the concept of internet as "internet of computers". The Internet of things (IoT) is a set of technologies which help to create a solution which holds end point sensors translating a physical reality into electronic expand. Over the years, the number of devices connected to the internet has increased exponentially[4]. The Internet of things connected devices installed base worldwide from 2015 to 2025(in billion). IoT security as "the technology area concerned with safe guarding connected devices and networks in the Internet of Things". It refers to the precautionary measures taken to beef up the security of IoT devices and reduce their suspicious attack from unauthorized criminals.

The beginning to attract attention in embedded technologies and the Internet has enabled objects surrounding us to be interconnected with each other. In future, IoT devices will be invisibly embedded in the environment and would be generating huge amount of data. These data would have to be saved and processed to make it understandable and useful. It is been observed that IoT network are facing different security challenges including authentication, authorization, information leakage, privacy, verification. IoT is combination of object, communication network, and computer system [2].

1.1 Elements of IoT

Elements of IoT is divided into three categories:

Hardware

Middle Ware

Presentation

Hardware:-Hardware components play main role in IoT are sensors, actuators and processors[3].

Middle Ware:-

These technologies use the on demand storage and computation tools for data analytics. The main purpose is to hide the details of different complexity and it allows the programmer to develop the specific application.

Presentation:-

Only practical implementation of IoT can use in the development of smart home, smart cities, smart environment, smart countries through making the use of smart devices.

2. ADVANTAGES OF IoT

IoT is using smart sensor for monitoring the various aspects in our day to day life through various applications which can be use for saving money and time.

For communication purpose, IoT play very important role between devices. Because all physical devices is connected with IoT for communication and hence it improves the greater quality with less efficiency. Without human beings, Machines are managing, controlling all amount of information, which manage fastly and produce output timely.

With the help of IoT based application, we can increase the better and comfort management in our daily lives.

IoT increase the economic growth, new technologies, and business.

It provides better environment.

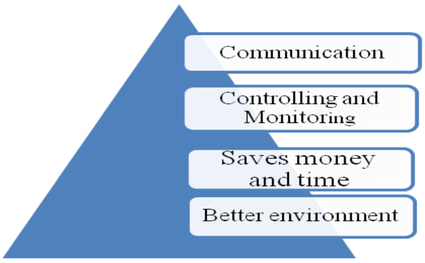

Fig -1: Advantages of IoT

3. DISADVANTAGES OF IoT

It has involvement of multiple devices and technologies and multiple companies will be monitoring it. Since a lot of Data related to the context will be transmitted by the smart Sensors, there is a high risk of losing private data.

IoT is complex network. In case any failure in the network it may cause serious issues. Even power failure also cause some inconvenience.

Daily activities can be done using automated machine so less man power is required [1].

Technology takes control of life because our life gives increasingly controlled by technology.

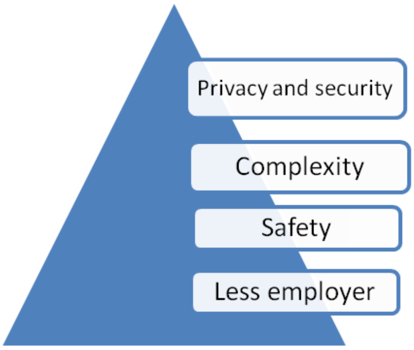

Fig -1: Disadvantages of IoT

IoT is a essential platform in the we can connect embedded devices to the internet, so we can collect the data, exchange the data between each others. It can possible interaction, collaboration and learn from each other experiences like human do [9].

4. APPLICATIONS OF IoT

Application of IoT is categories into consumer, commercial, industrial and infrastructure spaces.

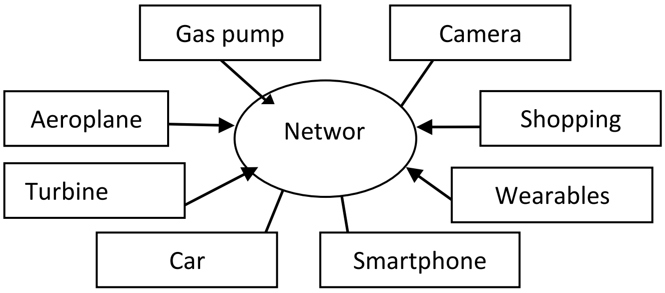

Fig –3: Applications of IoT in real life

1. Consumer application:-A growing portion of IoT devices are created for consumer use, including connected vehicles, home automation, connected health, and appliances with remote monitoring capabilities[5].

Smart home is majorly using IoT concept in home automation. Which can be include lightening, heating, conditioning, media and security system.

2. Commercial application:-

In medical and healthcare, the internet of medical things is an application of the IoT for medical and health related purposes, data gathering and analysis for research and monitoring.

It has been referenced as "Smart Healthcare. IoT is use for connecting medical resources and healthcare services.

3. Industrial applications:-

In industry IoT devices is used for acquiring and analyzing data from connected equipment, location and peoples.

In manufacturing industry, IoT can realize the seamless integration of various manufacturing devices equipped with sensing, identification, processing, communication, actuation, and networking capabilities[11].

4. Military Application:-The Internet of Military Things (IoMT) is the application of IoT technologies in the military domain for the purposes of reconnaissance, surveillance, and other combat-related objectives.

Internet of battlefield things and Ocean of things is using this IoT concept. IoT provides a network infrastructure.

This paper is based on existing researches of network security technology also it provides a new way for researchers in certain IoT application and design, through analyzing and summarizing the security of IoT.

IoT Security Risks and challenges: IoT security risk is having three categories.

Risks that are typical in any internet system.

Safety to ensure no harm is caused by misusing actuators, for instance.

Problems and security challenges:

In IoT security and privacy is the prime factors to the popularity and acceptance.

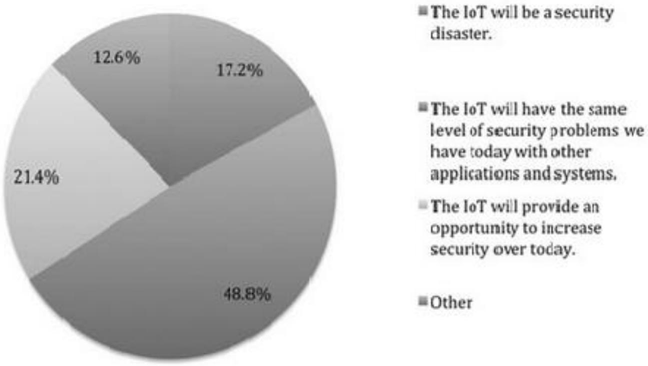

Fig -4: Characteristics of IoT in real life

This figure indicates the opinions of security personnel active in the IT space on security in the IoT, as we go back, the use and need of security and privacy in the internet would keep decreasing. Hence the security and privacy was not a part of the design of the internet. Hence the evolution of the internet into IoT, many security and privacy issue comes up. Security and privacy generally considered as augmented features.

Protocol and network security makes the IoT more secure and private. One of the biggest challenges to protection of IoT infrastructure is assortment. The highly constrained devices operating in low power and lossy network standard like IEEE 802.15.4[116], are required to open secure communication channel with more powerful devices in the internet using standard internet protocol. Lightweight cryptographic algorithms, Efficient Key Management, Standardised Security Protocols are the prime ingredients for securing such communication [8]. The cryptographic mechanism for the IoT are required to be less resource-intensive, faster, and at the same time providing the same level of security. It includes symmetric algorithms, hash functions, and random number generators.

Key Management is an indispensable element of secure network infrastructure.

The number of connected IoT devices is continuously increase, security issue are suddenly multiplied .There are many security concerns need to be considered as whole system. IoT security is the area to concentrate on protecting the connected device and network connectivity in the internet of things. Data security concern can be divided as confidentially, integrity, authenticity and data availability. All these security issue can be resolve by employing security measure. Data confidentiality means protection of data from unauthorised user. Data integrity maintains the correctness or data accuracy [7]. Authenticity makes sure that only the authorised person can access network resources. Data availability means there is no hamper of authorised access to services and applications. Different instance of IoT frameworks are smart city drones for observation frameworks, self driving vehicles etc.

Many small devices that have limited CPU power.So need to look for new encryption scheme with less CPU power. No installation of Audio Video software. IoT also needs both encryption key management and identity management.

5. CHALLENGES in IoT

Challenge 1: Global cooperation:

Analysis of IoT globally shows the three main approaches.
Integrated approach in china is able to guide on broad investment in infrastructure, smart cities, software, applications and services.
A stakeholder approach in the EU that favors public-private partnerships and vertical investments through four-year program plans.

An opportunity investment approach in the US that is driven by short to mid-term return on investment. It is pushed by smart energy, smart cities, and RFID fueled by Department of Defense and Wal-Mart.

Challenge 2: Business models, new currencies in IoT and trust

A key area of research lies in building procedures and protocols for decision making that are not based on the premise of speed. In a real-time world there is no longer gain being the “first” to have the data. Instead, the internet of things favors a daily situation of full traceability.

Challenge 3: Ethics, control society, supervision, agreement and data driven life

This rapid diffusion of algorithms and their increasing effect, however, have result for the market and for society, consequences which include questions of ethics and rule.

Challenge 4: Technological challenges

The technological domain of the internet of things (IoT) embraces several developments, as disjointed as they are numerous. As the definition itself is still under heavy discussion, it is quite difficult, even tricky, to set boundaries, in order to determine clearly which technologies are within its range. As we know today, internet is based on a few, very simple and very meaningful principles. One of is the "end-to-end" principle: keeping the technologies in the network very simple and dealing with complexity at the end points only, allowed the Internet architecture to be very scalable[11].

Challenge 5: Searching balance between top down planning with respect to bottom up idea.

IoT application helps the current institutions and public bodies to transformed open data peacefully into a networked model, feedback on where money is going. IoT is extremely relevant in making direct feedback visible in road, furniture and applications.

IoT is a layer of data, it is open to all, through which anyone can decide by its own where they are willing to pay, and also it can get direct feedback.

6. CONCLUSION

The IoT is giving various benefits to the consumers and its potential to change the ways that consumers interact with technology in different innovative ways. From a security and privacy perspective, introduction of sensors and devices into currently intimate spaces-such as the home, the car and with wearable devices. As we are using physical object in our day to day life, for sharing observations about us, so consumer always want privacy for continuing this. In the future generation, Internet of things is likely to integrate the virtual and physical worlds together in ways that are currently difficult to understand. Hence, our future work will be focus on IoT implementation in all fields.

REFERENCES

[1] Wan, J., Yan, H., Suo, H., & Li, F. (2011). Advances in cyber-physical systems research. KSII Transactions on Internet and Information Systems, 5(11), 1891–1908.

[2] Atzori, L., Iera, A., & Morabito, G. (2010).The Internet of things: Survey.Computernetworks,54(15),2787,2805.doi:10.1016/j.comnet.2010.05.010.

[3] Abomhara, M., Koien, G.M.: Security and privacy in the Internet of things: Current status and open issues. In: International Conference on Privacy and Security in Mobile System. IEEE (2014) (2002).

[4] M. Shell. (2002) IEEE-trans homepage on CTAN. [Online].Available:http://www.ctan.org/tex-archive/macros/latex/contrib/supported/IEEEtrans.

[5] Hachem, S., Teixeira, T., & Issarny, V. (2011). Ontologies for the internet of things (pp. 1–6). New York: ACM.

[6] International Telecommunication Union. (2005). Internet reports 2005: The internet of things. Geneva: ITU.

[7] Anzelmo E, Bassi A, Caprio D, Dodson S, van Kranenburg R (2011) Matt Ratto (Internet of Things, Discussion/Position Paper. Institute for Internet and Society, Berlin, commisione.

[8] Broenink G, van Kranenburg R et al (2011) The Privacy Coach: supporting customer privacy in the internet of things. TNO. Available at: http://arxiv.org/pdf/1001.4459. Accessed 21 August 2011.

[9] van Kranenburg R (2007) The Internet of Things. A critique of ambient technology and the all-seeing network of RFID, Network Notebooks 02. Institute of Network Cultures. Available from: http://networkcultures.org/wpmu/portal/publications/network-notebooks/the-internet-of-things. Accessed 21 August 2011.

[10] Rajendra Billure, Varun M Tayur, and V Mahesh. 2015. Internet of Things-a study on the security challenges. In Advance Computing Conference (IACC), 2015 IEEE International. IEEE, 247--252.

[11] Tsai, C., Lai, C., & Vasilakos, V. (2014). Future internet of things: Open issues and challenges. ACM/Springer Wireless Networks,doi:10.1007/s11276-014-0731-0.