Alma STANA[1]
Silvester HASANI[2]

THE RISE OF INTERNET OF THING AND THE RISK OF THREATS

Abstract

World Wide Web has become a global driver in the information sharing from the users. Internet has changed a lot during its lifetime. The change is continuing with the rise of new technologies as well. The low cost wireless connections are making the information sharing even more persistent. Data collection has become more advanced with embedded devices connected with each other and RIFD technology used to transmit data in a continuous way.

Exactly these technologies has led to the "Internet of Things" that is a way to display web as a medium of connected devices through the world and to communicate with each other.

IoT has also faced a lot of challenges, especially when it comes to Enterprise IoT. Techniques for implementing IoT need to be developed especially in developing countries.

The challenges and threats of the IoT are described in this paper. An initial security evaluation is also shown.

Keywords: IoT, security, Web, IPv6.

1. Introduction

IoT is an emerging global Internet-based architecture used to facilitate the exchange of the information between the connected devices [1]. The whole network is a virtualization, which a group of embedded devices with sensors and each of them connected to this network. The idea is that each of this network devices can disconnect and the whole network is still operating. The list of devices

[1] University "Aleksander Moisiu" Durres – Albania

[2] University of New York Tirana– Albania; almastana@hotmail.com, silvesterhasani@unyt.edu.al

connected can be from mobiles, to air-conditioners and wearable devices. This implies that the connected devices need to access the internet using Internet Protocol version 6 (IPv6). Using his IP address these devices can transfer data over the network using IPv6. The usage of IPv6 is because of the lack of space of IPv4. One thing to note is that IoT also has devices connected that can act within that network and not only sensing devices.

2. History and Definitions

Internet of Things can be defined and described as the livable environment in the presence of mobile technologies as a powerful multimedia system [2]. IoT can be understood also by having three paradigms in mind, internet oriented IoT which is a Middleware, things oriented IoT which is created by sensors and sematic oriented IoT which is Knowledge [3].

The first real Internet of Things network was in 1999 where Massachusetts Institute of Technology, MIT wanted to develop a network and started using RFID technology to identify things on that network. This was the first step into IoT. In 2005 it was recognized as a network with things that interact by the International Telecommunication Union and in 2009 it was called Internet of Things by Cisco Internet Business Solutions Group [4].

Another definition of Internet of things is a network that objects are connected across the world and possess unique address based on a standard protocol for communication [5].

Figure 1 shows the Internet of things IoT technology perceived by the normal user as a single network that nodes interact with each other.

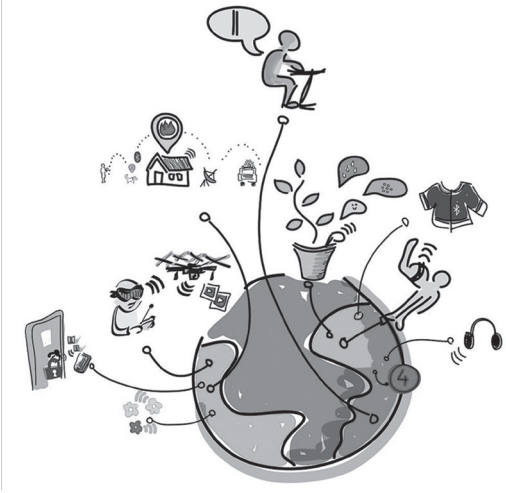

Figure 1: IoT technology

Today Internet of Things technology is following the trend of wireless sensor networks, and Google forecasts that this trend with continue and even enhance the usage of Internet of things in 2017 and ongoing [6].

3. Design of IoT

Design of an IoT is illustrated better with a classification of the parts in it, Hardware consisting of sensors, communication hardware and actuators; Middleware consisting of storage devices and tools for data analysis; and Presentation consisting of virtualization and interpretation tools that can be accessed by different platforms or applications.

Sometimes these parts are approached as three dimensions that are, Information items including all items connected to IoT such as sensors or controllers; Independent network including features of self-optimization, self-adaption or self-protection; and Intelligent applications including applications that have an intelligent behavior over the Internet [7].

Figure 2 presents the infrastructure of IoT and the different parts of this infrastructure.

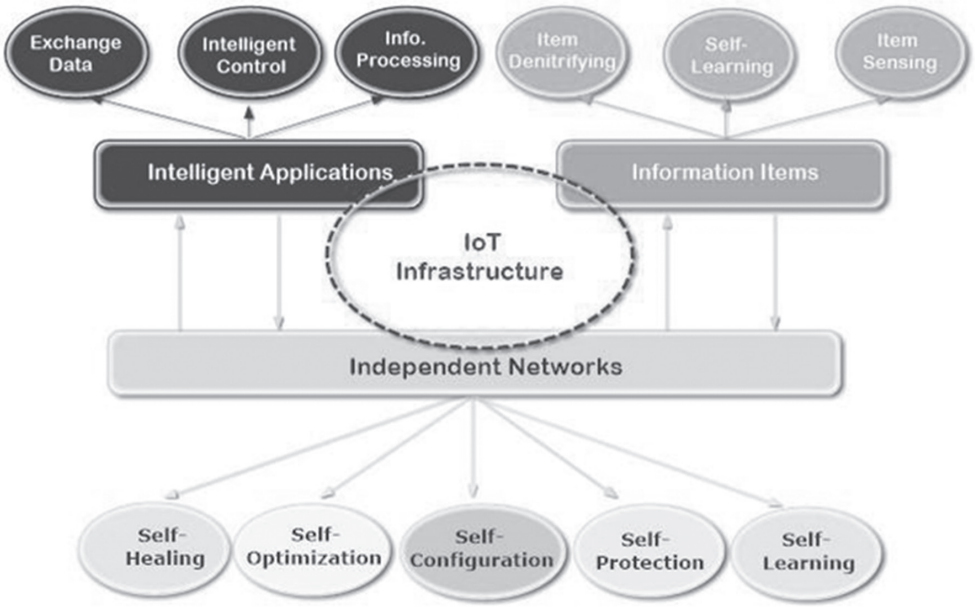

Figure 2: Infrastructure of IoT

While there are several approaches to create an IoT infrastructure, the general view of a simple IoT infrastructure is created by implementing a WSN (Wireless Sensor network) in Internet.

If IoT is compared with Internet and WSN, the communication protocol of IoT is a lightweight protocol similar to WSN while TCP/IP is used on Internet. On the other hand, the degree of the area covered by IoT is wide similar to Internet and not local like in WSN. The same can be stated about the Network Approach which is similar to the Internet with a backbone and not self-organized. The behavior of IoT is dynamic like on WSN and not fixed like the Internet. So, in general IoT is a combination of WSN on the Internet.

4. Wireless Sensor Networks (WSN)

WSN are the most important part of IoT since it's the core of the whole network. The nodes of the network work separately and autonomously. They are linked together by self-organizing. WSN supports the elements division of a sensor consisting of an external antenna, a microcontroller and an energy source [8]. Components that make up WSN are:

- WSN hardware containing a sensor interface, processing units, transceiver units and power supply.
- WSN communication stack with ad-hoc nodes.
- WSN middleware for applications with interoperable services.
- Secure data aggregation offering reliable data collection.

5. Applications of IoT

The rise of IoT effects many other existing technologies in virtually every category. The applications are usually divided using the type of network available, the coverage, the heterogeneity, the impact or the involvement of the user. The categories of the application domains are:

- Personal and Home IoT
- Enterprise IoT
- Utilities IoT
- Mobile IoT

Personal and Home IoT are applicable to individuals who own the network. For example the smartphones having Apple IOS or Google Android can measure various data and parameters into our personal network. Or the personal BANs

(body area networks) can be extended to a monitoring system through a personal network to take care of elder people. Home appliances can be controlled remotely using IoT.

Enterprise IoT is applied to a larger scale. All the environmental information gathered is used to have track of people within a building is one example of Enterprise IoT. Various security and automated services regarding a large factory are integrated using IoT.

Utilities IoT is the gathering of the information through a network used by companies to optimize cost and profit. Energy consumption efficiency is achieved using Utilities IoT.

Mobile IoT are used widely by people and they are not aware of it. One example is the usage of Bluetooth to share information with each other. The usage of Bluetooth headphones creates a small IoT network into a car. These are examples of Mobile IoT.

6. Enterprise IoT

To develop a IoT network specifically for Enterprise level, a complete set of development tools and capabilities need to be accessed. ThingWorx is purpose-built to overcome this challenge [9]. It makes it easy to develop and deliver powerful Enterprise IoT solutions suing partners to extend smart and connected world. The economic impact of IoT is projected to be very big and the complexity of sensors, hardware providers and software vendors need to cope up with this complexity.

Creating smart, connected products requires an approach that builds on top of and integrates with the ecosystem of enterprises applications.

7. Challenges and threats of IoT

IoT has a lot of challenges facing both recently and during the years. Below are the challenges that are subject of research directions with proposed solution for each of them.

1. Networking Challenge

Networking has a great relevance in the Internet because it manages the network flow. Traffic and protocols have an impact of IoT [10]. One method to solve the issue is MANET (Mobile Ad-Hoc networks) which consists of self-organized mobile nodes using a way to maintain interconnection.

2. Routing Challenge

Routing is choosing the best path between nodes to communicate. There are many protocols used to select the best route possible. So as in Internet, even in IoT this challenge is faced.

3. Heterogeneity Challenge

IoT environment has a lot of different devices connected through the network, so the Heterogeneity challenge is faced like no other network. The best way proposed to deal with this problem is the Middleware Layer. It is a software used to interpose the technological layer with the application layer into a standard usable in real world service [3].

4. Interoperability Challenge

Interoperability is the ability to create devices cooperating with each other in an efficient way. Since IoT is a big network, the interoperability challenge is enhanced. To overcome this problem, a Semantic Interoperability Architecture to part the network into smaller groups is proposed [8].

5. QoS Challenge

QoS is the measured by the time it takes to deliver the message from the sender to the receiver. There are some standards that need to be followed to ensure the requested QoS. This challenge is faced even in IoT.

6. Scalability Challenge

Scalability is the deal with the continuous growth in an efficient way. It means that the system needs to handle the growth scale of IoT usage without effecting the performance. This challenge is dealt with Virtualization.

7. Power Efficiency Challenge

Power consumption issue is a critical point in wireless networks. Since IoT is a type of wireless network, the power efficiency is one of the critical challenges it has to face.

8. Security Challenge

Security is the biggest challenge of all the network. The threats that can attack a system can either be external threats or internal threats. In IoT environment, security is very important to ensure a reliable interaction [11]. The proposed solution is to use the RFID security protocol to make the IoT more robust.

Below are the most common threats that IoT faces:

1. Abuse of activity

The malicious abuse of the infrastructure letting a penetrator gaining confidential information about the IoT network. This may results in damage of the reputation, fraud, Denial of Service and data leak.

2. Eavesdropping

This threat is common on every type of network. This threat includes the man-in the middle attack, repudiation attack or interceptions that lead to confidential data leaking.

3. Physical attacks

Theft, vandalism or different forms of physical attacks can make the network not accessible. Even the devices are very vulnerable to natural disasters like storms, earthquakes, or corrosion. This loss of assets can lead to a disrupt data of IoT.

4. Software failure

Failure or malfunctions of software, or even bugs and design flows lead to the loss of the services of IoT.

8. Consequences of the threats

According to Microsoft [12] this is the list of consequences that affects an IoT network:

Damage to brand (DB): This leads to long-term impact of the whole business with different additional consequences like financial loss.

Financial loss (FL): From the theft of the loss of sales, the financial loss of the business can be a long-term consequence to a company.

Loss of data (LD): This consequence leads to DB because the data and the intellectual property need to be protected.

Loss of control (LC): A loss of control could be extremely detrimental to business operations.

Compromise of privacy (CP): Privacy and its breach can have significant consequence to the company.

*Loss of property/ Loss of Life (LP/LL***)**: This involves either physical damage to property or a loss of property. Sometimes even the injury of humans can be a consequence from the automatization coming from IoT.

Service disruption (SD): Disruption can effect both reliability and brand of the company.

9. Security Evaluations

The evaluation of the security of IoT is a long process and it subject to further researches. Below are a few evaluation strategies to initial security evaluation:

1. Threat Modeling

Analyzing the infrastructure of IoT to discover possible threats.

2. Deployment review

Reviewing the design, deployment and development of the IoT network. This involves audits and configuration analyzing. The most important part is to maintain privacy throughout the review.

3. Access control review

This review analyzes the authentication and access control models used in the IoT network. This includes even analysis of operating system of the devices and even review of password complexity and policies.

4. Device risk analysis

This involves the analysis of device standards and regulations, to have a better standardized IoT network, and the review of the exploitations available to different devices.

5. Device firmware review

This involves reviewing the devices firmware to check if they have been updated to the latest one. A newer firmware is known to have less exploitation possibilities.

6. Network traffic analysis

There are threats that exploit the whole network from the topologies and traffic patterns, so a throughout analysis of the network helps to remove this risk.

7. Encryption review and penetration testing

Review of the encryption algorithms, a vulnerability assessment and a penetration testing can lead to a more secure IoT environment.

10. Conclusions

IoT faces many challenges starting from the most general ones like security and power efficiently to more complicated ones like scalability and

interoperability. There are a lot of applications where IoT can be used starting from personal and home usage to enterprise and industrial usage. The world is changing constantly and these challenges need to overcome to adapt the network to IoT. A lot of advancements are being made and the understanding of the infrastructure of IoT can help developing countries to implement IoT and thus advancing their technology.

References

- R. H. Weber, "Internet of Things – New security and privacy challenges," *Comput. Law Secur. Rev.*, vol. 26, no. 1, pp. 23–30, Jan. 2010.
- D. Li and Y. Chen, *Computer and Computing Technologies in Agriculture: 5th IFIP TC 5, SIG 5.1 International Conference, CCTA 2011, Beijing, China, October 29-31, 2011, Proceedings*. Springer Science & Business Media, 2012.
- L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010.
- "History of IoT | Background Information and Timeline of the Trending Topic." [Online]. Available: /internet-of-things-history/. [Accessed: 29-Apr-2017].
- D.-L. Y. F. L. Yi and D. Liang, "A Survey of the Internet of Things," *Proc ICEBI*, 2010.
- M. I. and Strategy, "Internet Of Things (IoT) Outlook For 2017," *Forbes*. [Online]. Available: http://www.forbes.com/sites/moorinsights/2017/01/03/internet-of-things-iot-outlook-for-2017/. [Accessed: 29-Apr-2017].
- H. Ning and H. Liu, "Cyber-Physical-Social Based Security Architecture for Future Internet of Things," *Adv. Internet Things*, vol. 02, no. 01, p. 1, Jan. 2012.
- Z. H., H. A., and M. M., "Internet of Things (IoT): Definitions, Challenges and Recent Research Directions," *Int. J. Comput. Appl.*, vol. 128, no. 1, pp. 37–47, Oct. 2015.
- "Enterprise IoT Solutions and Platform Technology," *ThingWorx*. [Online]. Available: https://www.thingworx.com/. [Accessed: 07-May-2017].
- B. Leal and L. Atzori, "Objects Communication Behavior on Multihomed Hybrid Ad Hoc Networks," in *The Internet of Things*, Springer, New York, NY, 2010, pp. 3–11.
- H. Ning, *Unit and Ubiquitous Internet of Things*. CRC Press, 2016.
- Microsoft.com, "Evaluating Your IoT Security," 2017.