EC601 A2 Product Design in Electrical and Computer Engineering (Fall 2021)

Project - 1 Summery

Name: Zhaozhong Qi

BU-ID: U35286574

Boston University

Project Topic:

Network security for IoT devices

What does the topic cover?

"The internet of things has matured out of its initial stages of very corner and incubation into a clearly defined set of use cases that deliver discernible benefits to a variety of market verticals." [1]. About the internet of things, it is an enhanced & advanced hardware network technology between machines and devices that creates a global network to connect with them. It is an incorporation of the convergence of IT and operational technology(OT) systems. The concept of the machine involves entire features that we might have already known or were unfamiliar with. It across with infrastructure within the industry to every single housekeeping around us and our society.

In another word, it covers all the communication and exchanging capabilities between machines(devices) and machines, such as security cameras, sensors, and vehicles. And also between machines & mankind, such as smart homes and security smart safety locks. Whatever Business problems across the industries around the world, or the single comprehensive device, the IoT and Network Security technology have the capability to build their specific solution to each of them in the meanwhile.

Why is it important?

When the IoT technique trying to tangibly solve pressing business problems across every walks of life. Early adopters of this technology – such as healthcare, smart cities, building management, utilities, transportation, and manufacturing – are attesting to its many benefits." [1]. There is sort of analytical data that has been contributed by IoT Threat Report, Palo Alto Networks contributor, [2] it shown thirty percent of devices on enterprise networks are IoT devices at today. The data that has been reaching collected from this research also claims, the assistance of valuable insights that aid in real-time business decision-making and accurate predictive analytics and modeling could not be divorced from the IoT science and technology.

Such domain of supply chain management, automation, even adherence to regulatory compliance of reducing expenditures and operation costs of government or capital markets. Those applications are all benefited and improved by matured out of the initial stages to advance of technology of IoT. Other areas such as the number of real-time applications(devices) that need interactions among the other tremendous devices, etc, will also inquire the sophisticated technique support from these future technologies.

What are the applications of the topic?

- Comprehensive use of Internet of Things & But Securities?

Internet of Things is recognized as one of the most important and influential technologies and gaining vast recognition in a wide range of fields, which are related to smart cities, military, education, hospitals, homeland security systems. From transpiration and autonomous connected cars, agriculture, even intelligent& remote shopping systems, or any other contemporary devices. [3] One of the most famous topics of IoT networks that seems conversant for us, the smart home applications, [Figure 1] which applied the infrastructure portion of the Internet of Things service. It used several sensors which perceive and collect the data of surroundings in order to partially or fully control various domestic appliances at the same time or asynchronous, like smart bulbs, voice recognition speakers, smart windows, temperature, and vibration sensors, etc… According to a 2019 Gartner report, enterprise IoT adoption grew 21.5% from 2018 to the end of 2019, totaling an estimated 4.8 billion devices. [4] However, in risk of Cybersecurity, those devices are actually under threat landscape.

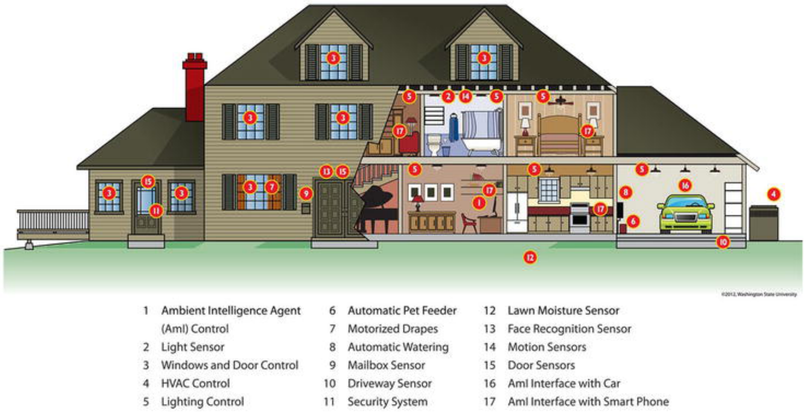
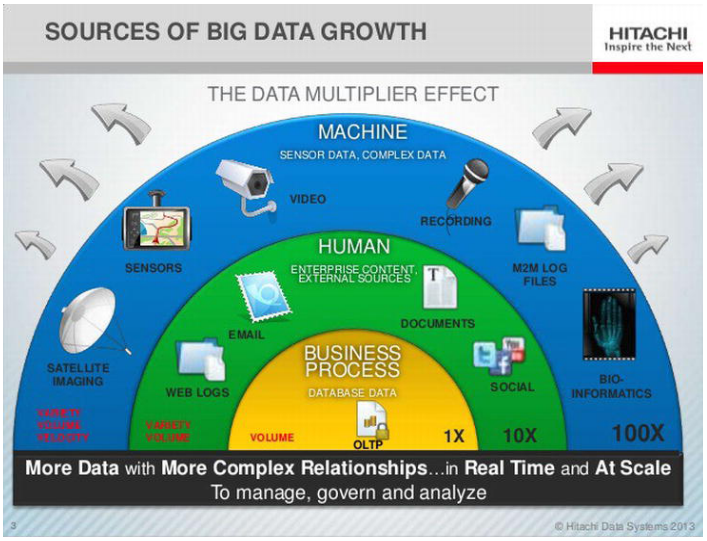


Figure 1: SMART home sensors communicate through the internet of things - (http://www.nibib.nih.gov/sites/default/files/SMART-HOUSE_2_DCook.jpg).

- Challenges and needs to improve:

“We found that the general security posture of IoT devices is declining, leaving organizations vulnerable to new IoT-targeted malware as well as older attack techniques that IT teams have long forgotten.“ – Unit 42 2020 IoT Threat Report. [4] Unit 42 threat intelligence and cyber attacks or incidents since the last two years of data investigated by IoT security experts, the information definitely demonstrating the security flaw existing throughout the network due to those unmonitored and unsecured devices who still being able to build connection in the network.

Secondly, the Tremendous growth of the devices using is increasing the risk of information security during the transmission of three basic sources of applications of Internet of Network undoubtedly. [Figure 1 shown] [2]. Meanwhile, in order to secure the stable and high accuracy transmission and exchangeable capabilities around the strange environment, the adopted smart devices would need better resilience and support of strong hardware buildings. “The expected devices to be connected together are expected to be 50 billion through the Internet of Things devices by 2020.” [2]. In order to connect such a huge number of devices will necessary required high-security levels to prevent scams, this big challenge also comes from the confidence between individuals and industries of using groups. Other challenges such as sufficient support of bandwidth, lower power consumption are still looking for some better solutions in the meantime.



SOURCES OF BIG DATA GROWTH

HITACHI
Inspire the Next

THE DATA MULTIPLIER EFFECT

More Data with More Complex Relationships…in Real Time and At Scale
To manage, govern and analyze

3

© Hitachi Data Systems 2013

Figure 2. Different sources of data growth (https://www.slideshare.net/bjorna/big-data-in-oil-and-gas).

What is the societal significance of the research?

IoT security can be understood as a security strategy or a mechanism to protect communication from cyberattacks while IoT devices exchange the information getting through the network. It is built for a fixed set of specificated functionalities to provide safeguard and vantage. Due to the properties of the IoT devices (sense and interact with an internal state to the external environment), it is easier to become targets for hackers or “Non-IT attackers” since it is always not frequently maintained by IT developers. Specifically, in addition to the different hardware, chipsets, and even operation systems, imparity works together, it can be metaphorically treated as unmanaged endpoints in the network that we are familiar with. Then be left vulnerable to exploits, for instance, account and password-targeted attacks and malware infiltration.

For the sake of those customers, all internet of things users around the world. Experts have provided several different levels of answers to resolve those layers of issues that popular exists among the world.

Examples under unmonitored data transmission, or in another word, Security Level Solutions. The *Hewlett Packard Enterprise* releases EDGE SYSTEMS: Ruggedized Edge Compute hardware. It is a device that is embedded with acquiring, analyzing, and acting upon edge data in the harshest environments with the compute power that the customer may expect from Industrial IoT service.[5] The functionality of this machine includes aggregate and filter data, while also analyzing video streams, time-series data, and translating industrial protocols. *"At the same time, it would accelerate your responsiveness to new insights and monetize data from connected devices with solutions helping transform them into an IoT-enabled, future-ready organization."* [5] [**Introduction of Ruggedized Edge Compute**]. And such a product that also innovated by this enterprise, which names "HPE Edge Center", A pre-integrated, intelligent, software-defined edge enabler that offers a rapid, standardized way to deploy and protect IT infrastructure at the edge. [5] It is also a good example that provides a fantastic way to prevent malware infiltration and enable stabilized transmission of infrastructure machines in industries.

It might be less familiar that we are concerned about the 5D Buiding Information Management system during the daily news in our life. But it could be familiar with the idea and topic of Smart Cities. Exactly, the Cloud-Based 5D BIM Enterprise Solution has been presented and implemented already.

During the recent research and a well-recognition received from my summer internship in 2021, there is an unprecedented idea called Germany's "Industry 4.0" before the years of 2013, that will be likely to be mentioned here. A solution, put forward by the enterprise RIB, which names "iTWO 4.0" comes out with unexpected, however, also in accordance with expectation(s). It is a cloud-based 5D BIM enterprise platform that redefines the management of building and construction business in the era of Industry 4.0. The Cloud-Based platform/ a web-based collaborative platform integrating with cloud computing, 5D BIM, big data, modular construction, smart SCM, virtual into physical technologies, etc., that connects people, machines, and data for fully digitalized management of enterprise-wide projects throughout the construction life cycle.[6] It opens up infinite opportunities for leading companies to embrace agile business and drive productivity. More details could be found in the reference link [6] at the end of the page.

Pick an area of focus that interests you in the topic (As comprehensive as you can, research the different approaches and solutions in the research community and industries)

The trend of my interest can be approached and divided into two directions, for the first one - Security, another function, Internet of Robotic Things (IoRT)/ Intelligence IoT device. The basic idea of this project could be to design an Intelligence Robots car embedded with monitoring surroundings capabilities(sensors, camera, etc.) that also can get sensor data and transmit them through a secured network, for instance, the identification of obstacles by the dependence by its own smart opinion and surroundings.

The concept of integrating IoT technology with Robotics is a brand new topic, but people are more familiar with those topics separately. It has been driven by varying yet highly related objects, but they have different focusing. “IoT focuses on supporting services for pervasive sensing, monitoring, and tracking, while the robotic communities focus on production action, interaction and autonomous behavior.” [7] While obtaining data that coming from a range of sensors that are under fused, the information will be processed locally. Then it will be distributed with an intelligence device that could make as smarter choices as it can, and making specifical functionality comes true. It will construct a pretty simple IoT-based network but could not be separated by a self-analytical unit to filtering then make a decision to achieve its intrinsic concrete value.

My expectation of building small **IoRT (Internet of Robotic Things)** devices would like to have the attributes with, it has its own way that will be able to provide the privacy and security to prevents normal cyberattacks and interference from the external world. The interference might include the attacks which contend to get access or authority to control the device(robots), different frequency band signals, replaying valid communication, etc. Meanwhile, it will determine how to respond to those signals by obeying the decision rule while it's making.

The idea is not confined to develop an intelligent robot car build interaction with several cameras around a street. Stop while meets non-moving or moving obstacles and drive without constraint in zigzag landform. This idea comes from the research of IoT Times, AI/ Machine Learning topic, [7] who is also come up with all the related articles which talk about Security Embedded IoT Devices and the framework and firmware of IoT invented by those genius contributors. The Open Source Research will give more details about how would I plan to make come true with this idea based on using the Minimum Viable Product concept.

Open Source research (Research the different open source projects that touch the topic of your interest)

1. **BG Networks' Embedded Security Software Architecture (ESSA):[10]** It is a software architecture that helps to protect your IoT Linux applications from cyber-attacks by making it much easier to check authenticity, integrity and to protect sensitive information such as Personally Identifiable Information (PII).

   Goals: **Security.** As its introduction mentioned, it is to remove the barriers of limited resources and time to adding cybersecurity to IoT.

   Implementing Language and Detailed Guide: Unknown, but free access license, details need contact with: https://bgnet.works/contact-us/

2. **PENIOT: Penetration Testing Tool for IoT [8]:** PENIOT is a penetration testing tool for the Internet of Things (IoT) devices. It helps you to test/penetrate your devices by targeting their internet connectivity with different types of security attacks.

   Goals: Security. As its introduction mentioned, it is mainly to help us to expose the device to both active and passive security attacks. Or simulate and create active security attacks to test the safeguard of the system which is a pretty useful tool.

Implementing Language: ***python***

3. **Awesome Embedded and IoT Security [9]:** In special, Bluetooth BLE Tools, UberTooth One: https://greatscottgadgets.com/ubertoothone/; Hardware Tools, J-Link https://www.segger.com/products/debug-probes/j-link/models/model-overview/

Goals: Internet of Robotic Things. Resolve Hardware connection and basic data transmission problems between Robots and IoT.

Implementing Language: ***C, C++***

4. **ROS (Robot Operating System)[11]:** The Robot Operating System (ROS) is a flexible framework for writing robot software. It is a collection of tools, libraries, and conventions that aim to simplify the task of creating complex and robust robot behavior across a wide variety of robotic platforms.

Goals: Internet of Robotic Things（IoRT). Resolve Robots Intelligent and its kernel judge mechanism while receives different signals from networks.

Implementing Language: ***python, C++***

References Link: (Network Security and IoT)

1. Palo Alto Networks. (2020, March). *What is iot security?* Palo Alto Networks. Retrieved September 20, 2021, from https://www.paloaltonetworks.com/cyberpedia/what-is-iot-security?utm_source=google-search&utm_medium=paid-search&utm_term=iot&utm_campaign=CDSS-AMER-EN-Search-Lead_Gen-US%2FCA-IoT&utm_content=536282648795-c&utm_network=&sfdcid=7014u000001ZDRYAA4&_bt=536282648795&_bm=p&_bn=g&gclid=Cj0KCQjwnJaKBhDgARIsAHmvz6eJJBdQfVCxBQJ0VelR7nELCgb0GUv5XA6I9tEBpSySDEO_gHGrgxAaAqkaEALw_wcB.
2. Ismail, Y. (2019, November 27). *Introductory chapter: Internet of things (iot) importance and its applications*. IntechOpen. Retrieved September 20, 2021, from https://www.intechopen.com/chapters/69788.
3. Tim. (2019, February 18). *The internet of THINGS (iot): 5 reasons why the world needs it*. Medium. Retrieved September 20, 2021, from https://medium.com/zeux/the-internet-of-things-iot-5-reasons-why-the-world-needs-it-125fe71195cc.
4. 1,2,3 2020 Unit 42 IoT Threat Report, Palo Alto Networks, March 2020, Global cybersecurity leader. Palo Alto Networks. Retrieved September 20, 2021, from https://start.paloaltonetworks.com/unit-42-iot-threat-report.
5. HPE. (n.d.). *Internet of Things (IoT) infrastructure & security solutions*. HPE. Retrieved September 20, 2021, from https://www.hpe.com/us/en/solutions/internet-of-things.html?chatsrc=ot-en&jumpid=ps_1246dipurz_aid-520023673&ef_id=Cj0KCQjwnJaKBhDgARIsAHmvz6d5bKwOthhQMa55nxw8hRAiyLWLJyGdlIu_j3C2r_9prn_K8GuOPgEaAi0cEALw_wcB%3AG%3As&s_kwcid=AL%2113472%213%21495320731362%21b%21%21g%21%21%2Biot+%2Btechnology%211352653387%2154044576117&gclsrc=aw.ds&gclid=Cj0KCQjwnJaKBhDgARIsAHmvz6d5bKwOthhQMa55nxw8hRAiyLWLJyGdlIu_j3C2r_9prn_K8GuOPgEaAi0cEALw_wcB.
6. RIB. (n.d.). RIB Americas. Retrieved September 20, 2021, from http://ribamericas.com/.
7. Matthews, K. (2019, November 14). The internet of robotic things: How iot and robotics tech are evolving together. IoT Times. Retrieved September 20, 2021, from https://iot.eetimes.com/the-internet-of-robotic-things-how-iot-and-robotics-tech-are-evolving-together/.

Open Source Project Reference:

8. yakuza8, @yakuza8 (B. C. (2019). Yakuza8/Peniot: PENIOT: Penetration testing tool for IoT. GitHub. Retrieved September 20, 2021, from https://github.com/yakuza8/peniot.
9. Fkie-Cad, F. (2019). *Fkie-Cad/Awesome-Embedded-And-Iot-Security: A curated list of awesome embedded and iot security resources.* GitHub. Retrieved September 20, 2021, from https://github.com/fkie-cad/awesome-embedded-and-iot-security.
10. Selvan, D. D. (2021, June). *Bgnetworks/Meta-Bgn-Essa: Yocto meta layer for Winsystem ITX-P-C444 With MENDER integration AND HAB*. GitHub. Retrieved September 20, 2021, from https://github.com/bgnetworks/meta-bgn-essa./https://bgnet.works/download-essa-user-guide/?gclid=Cj0KCQjwnJaKBhDgARIsAHmvz6e_c48KwAXSsQ98hEMI4aA5C81XGC6KUltuWa

Fz5J-RoOWOFgtE69waAl-kEALw_wcB

11. *Powering the world's robots*. ROS.org. (n.d.). Retrieved September 20, 2021, from https://www.ros.org/.