Internet of Things Security

Lecture 1: Introduction to IoT

Mehmoona Jabeen

Mehmoona.jabeen@mail.au.edu.pk

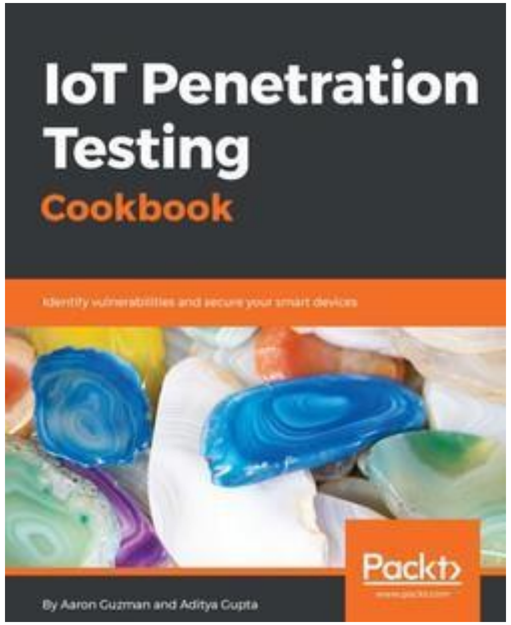
Department of Cyber Security, Air University

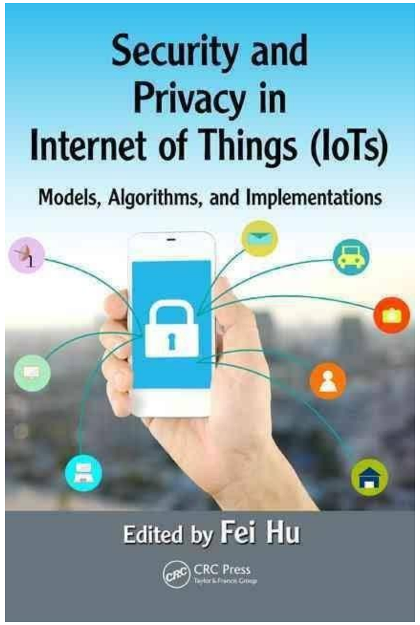
Course Outlines

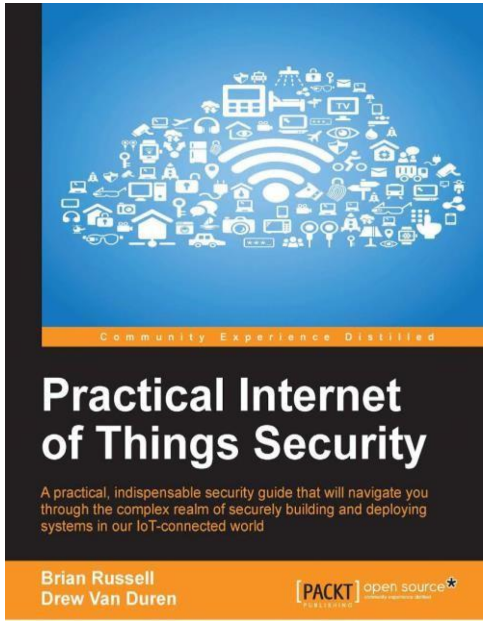
- Introduction to Internet of Things
- Hardware architectures and embedded system
- Embedded Operating systems for IoT devices
- Firmware development and management
- Communication Protocols for IoT
- IoT Attack vectors and Threat Modelling
- IoT security analysis and vulnerability assessment
- IoT Application security and their challenges
- IoT Data security and challenges
- Security issues in Edge Computing based IoT architecture

Readings

- ○ Selected research articles with each lecture
- ○ Selected chapters from the following books


IoT Penetration Testing
Cookbook
Identify vulnerabilities and secure your smart devices
Packt>
By Aaron Guzman and Aditya Gupta


Security and Privacy in Internet of Things (IoTs)
Models, Algorithms, and Implementations
Edited by Fei Hu
CRC Press
Taylor & Francis Group


Community Experience Distilled
Practical Internet of Things Security
A practical, indispensable security guide that will navigate you through the complex realm of securely building and deploying systems in our IoT-connected world
Brian Russell
Drew Van Duren
[PACKT] open source*

Class Information

- Subject:
- Internet of Things Security
- CGR Code:
- 5s5sx3n

Lecture Outlines

- What is IoT?
- Enabling technologies
- Characteristics
- Growth and Challenges
- IoT Security needs
- IoT Attack surfaces and vulnerabilities
- Common Vulnerabilities Reported
- Known Attacks in IoT

What is internet?

What is Internet?

A global network of **computers** providing a variety of information and communication facilities, consisting of interconnected networks using **standardized communication protocols**.

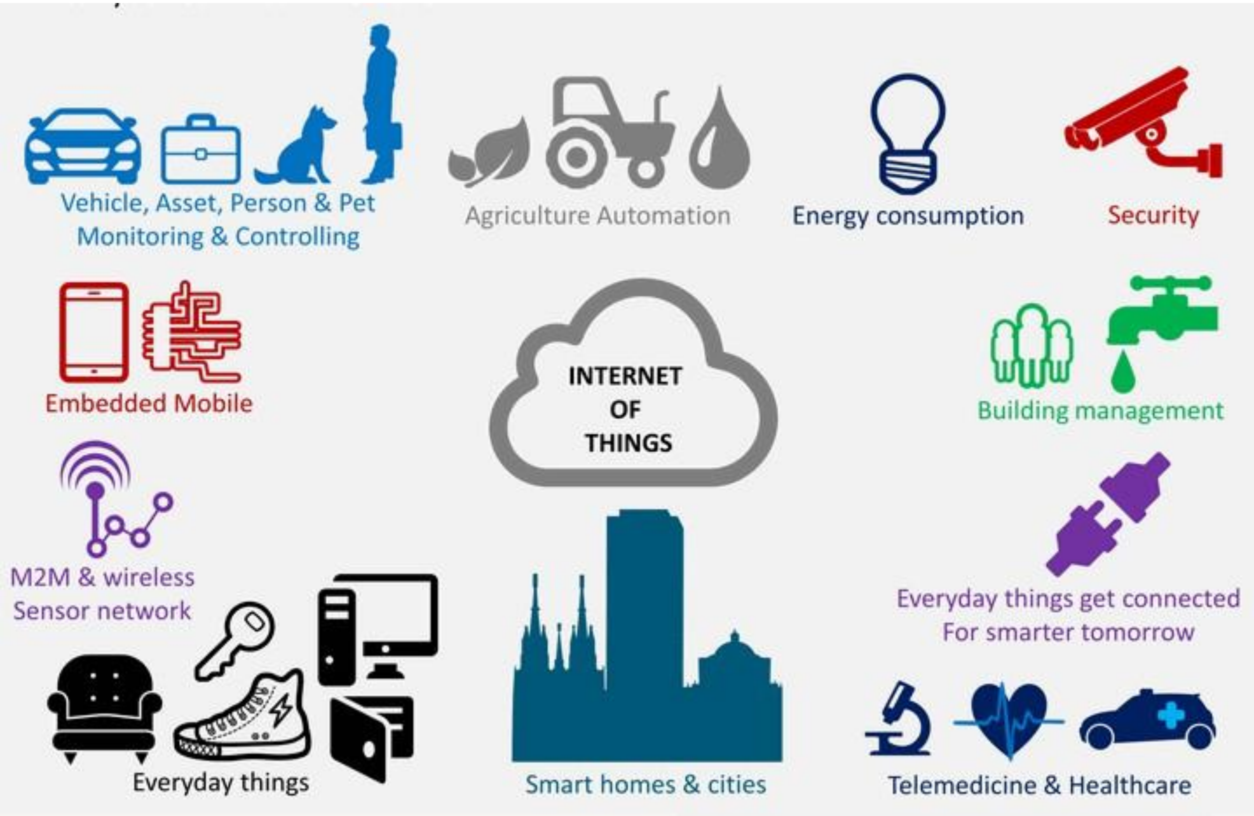
World Wide Web or *the Web* is only one of a large number of Internet services. The Web is a collection of interconnected documents (web pages) and other web resources, linked by hyperlinks and URLs.

Internet of things

- Elaboration

The **Internet of Things** (**IoT**) is the inter-networking of physical devices, vehicles (also referred to as "connected devices" and "smart devices"), buildings, and other items embedded with electronics, software, sensors, actuators,and network connectivity which enable these objects to collect and exchange data.

Src: Wikipedia



Internet of things: introduction

The IoT has four fundamental building blocks;

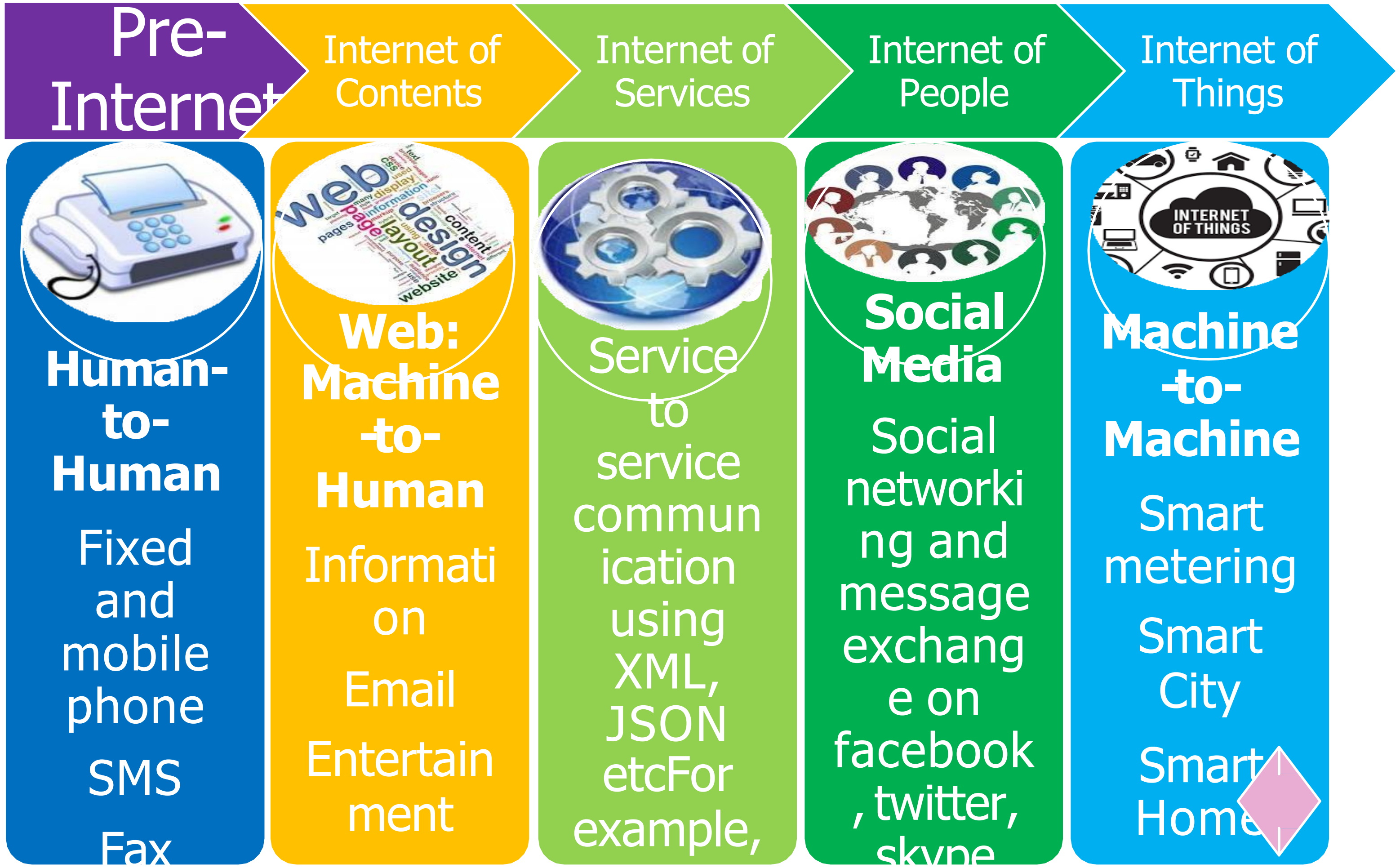
i. be identifiable (Recognizing Things)),
ii. To process (Think and Decide)
iii. to communicate (Talk to Other Devices)
iv. to interact (Take Action Based on Data)

Other terminologies

- Machine-to-Machine Communication (M2M)
- Cyber Physical System (CPS)
- Internet of Everything (IoE)

Things develop into human like society and co-work

IoT Growth Path



Pre-Internet

Human-to-Human

Fixed and mobile phone

SMS

Fax

Internet of Contents

Web: Machine-to-Human

Information

Email

Entertainment

Internet of Services

Service to service communication using XML, JSON etcFor example,

Internet of People

Social Media

Social networking and message exchange on facebook, twitter, skype

Internet of Things

Machine-to-Machine

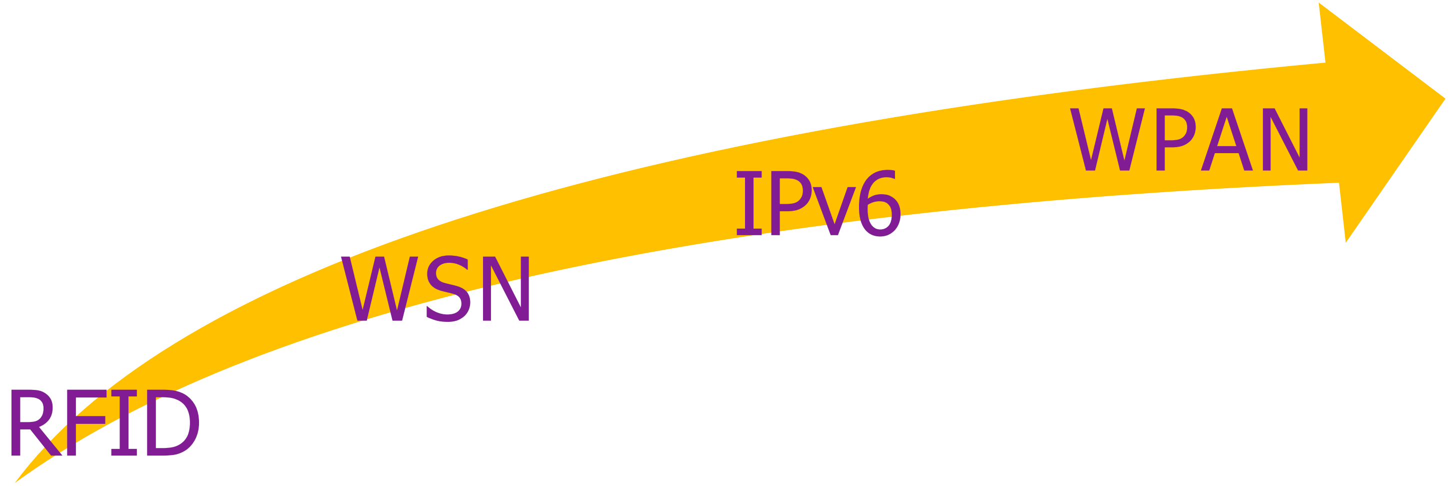
Smart metering

Smart City

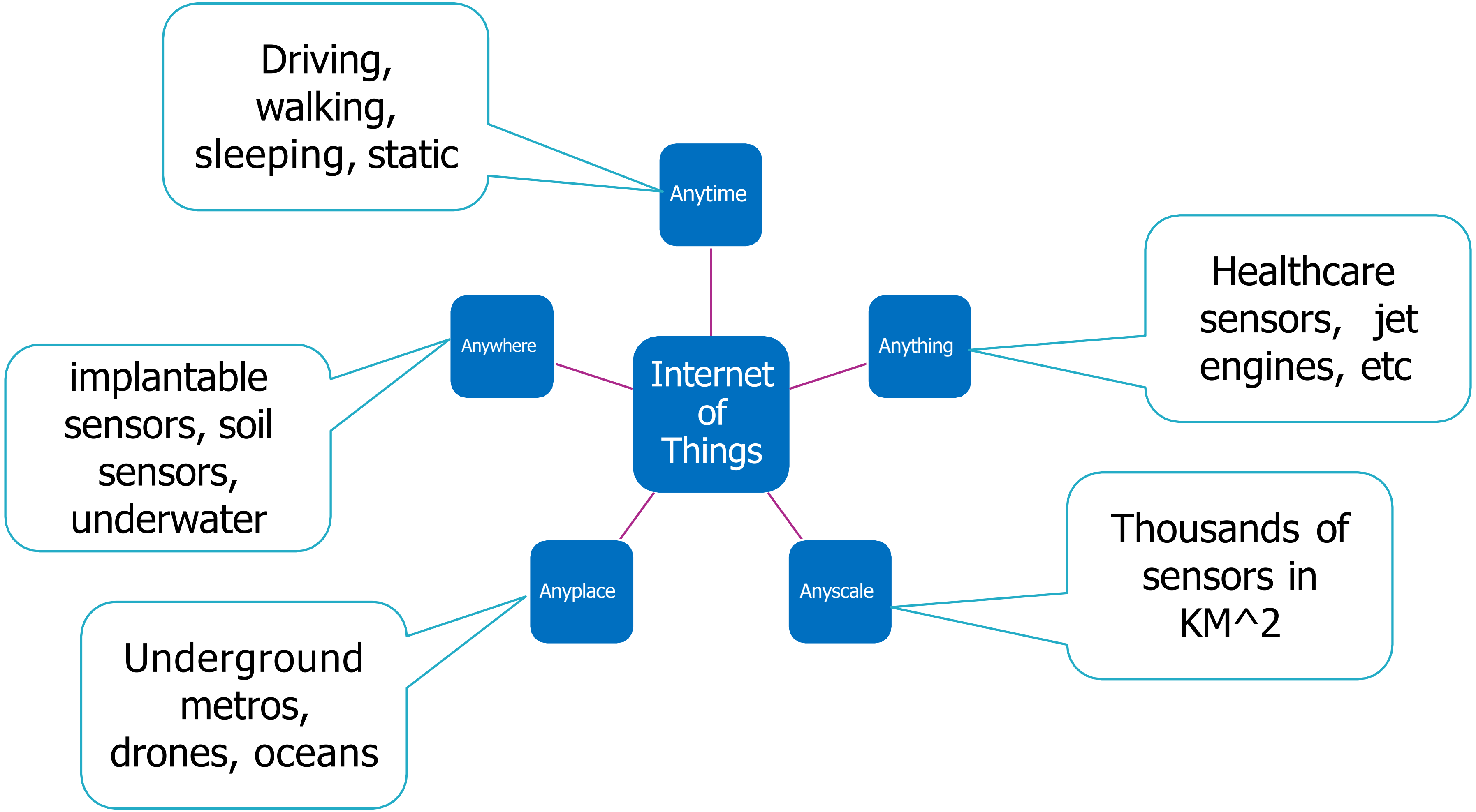
Smart Home

Enabling Technologies

- ✓ RFID for Identification and Tracking technologies.
- ✓ WSN for sensing and monitoring
- ✓ IP for addressing and networking
- ✓ WPAN for low power communication



Pervasive sensing/computing



Internet of Things

Anytime

Driving, walking, sleeping, static

Anywhere

implantable sensors, soil sensors, underwater

Anything

Healthcare sensors, jet engines, etc

Anyplace

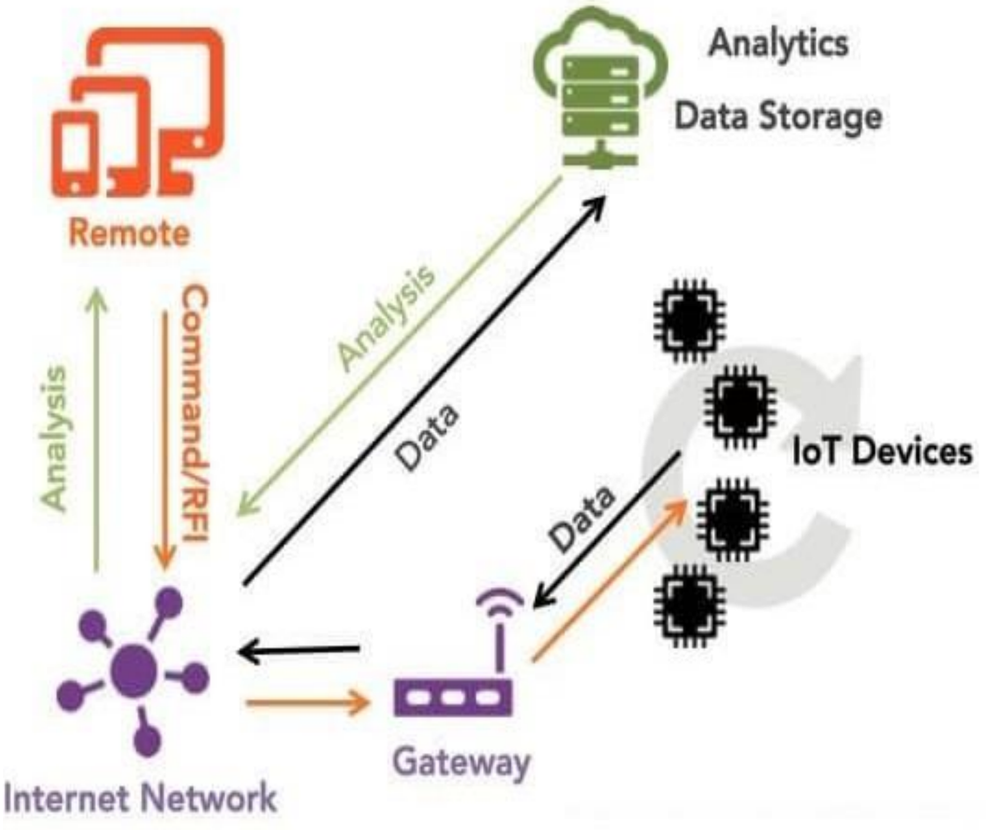
Underground metros, drones, oceans

Anyscale

Thousands of sensors in KM^2

Internet of Things Ecosystem

- **IoT Devices** embedded with sensors report **Data** to their corresponding entities (Consumers, Commercial Businesses, Governments).
- Entities send command over the Internet using **Remotes/ Interfaces** (Smartphone, tablet, etc) to actuate them.
- The Data generated by IoT Devices is stored at multiple locations including local databases, Cloud employing **Data Analytics**.



Source: BI Intelligence Report [4]

Internet of Things (IoT): Evolution

- We already have many things like Cars, Homes, Machines, Industrial equipment **connected** to **Internet**

- They can automate systems for us, allow us to communicate easier, collect data for us
- Whether we know it or not but **Internet of Things** was already there!

First IoT device

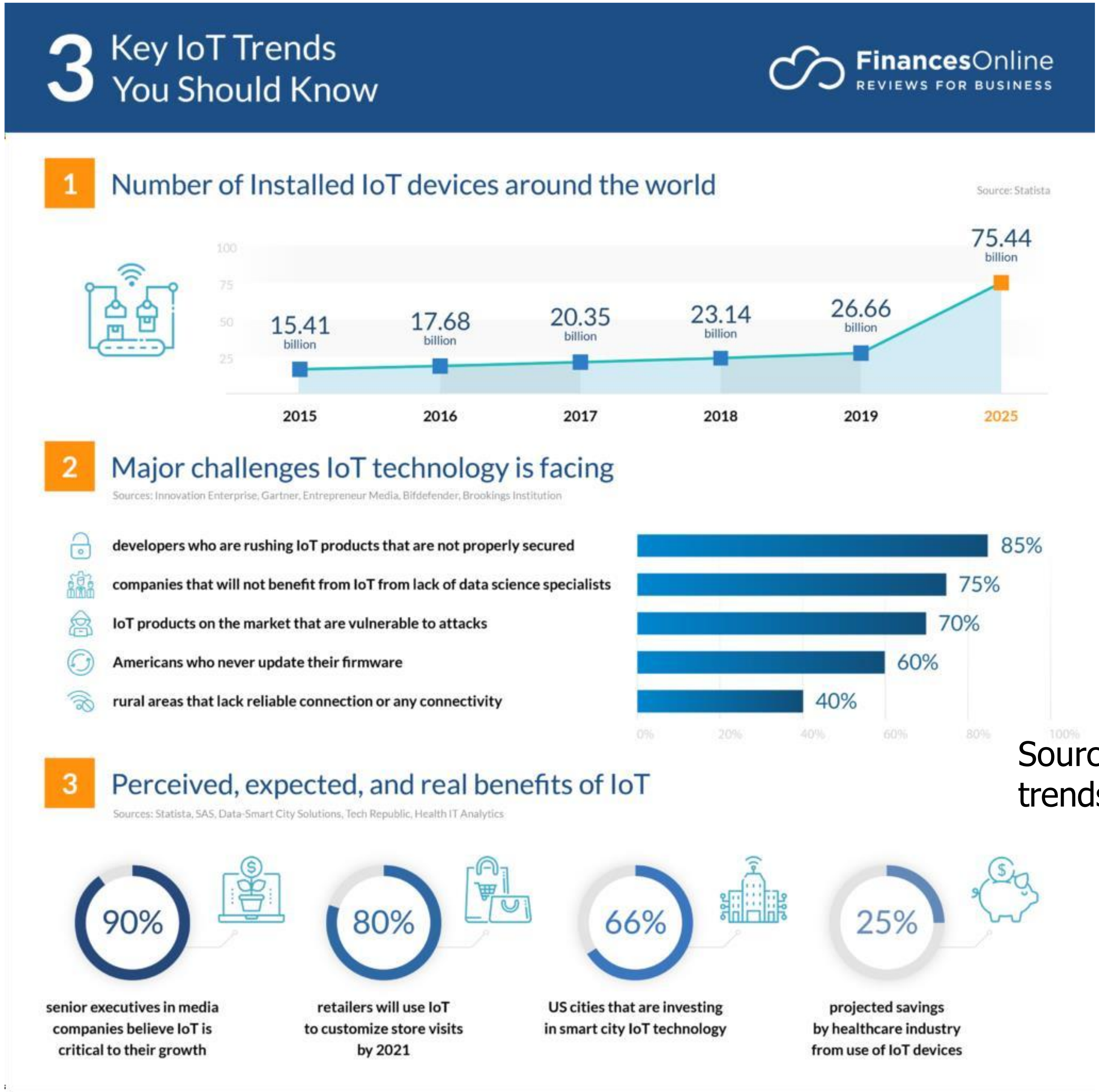
- Coke Machine Introduced in **1982** by Carnegie Mellon University students Mike Kazar, David Nichols, John Zsarnay and Ivor Durham, in the Computer Science department

```
coke$ status

ROW1 3 Bottles
ROW2 5 Bottles
… …

Total of 15 EEMPTY
```

BUT: The amount of Internet connected things is about to **EXPLODE**



3 Key IoT Trends You Should Know

FinancesOnline
REVIEWS FOR BUSINESS

1 Number of Installed IoT devices around the world

Source: Statista

2 Major challenges IoT technology is facing

Sources: Innovation Enterprise, Gartner, Entrepreneur Media, Bifdefender, Brookings Institution

developers who are rushing IoT products that are not properly secured	85%
companies that will not benefit from IoT from lack of data science specialists	75%
IoT products on the market that are vulnerable to attacks	70%
Americans who never update their firmware	60%
rural areas that lack reliable connection or any connectivity	40%

3 Perceived, expected, and real benefits of IoT

Sources: Statista, SAS, Data-Smart City Solutions, Tech Republic, Health IT Analytics

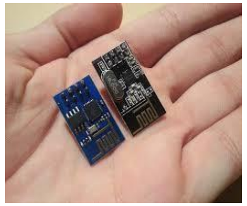
90%	senior executives in media companies believe IoT is critical to their growth
80%	retailers will use IoT to customize store visits by 2021
66%	US cities that are investing in smart city IoT technology
25%	projected savings by healthcare industry from use of IoT devices

Source: https://financesonline.com/iot-trends/

Why is it Now?

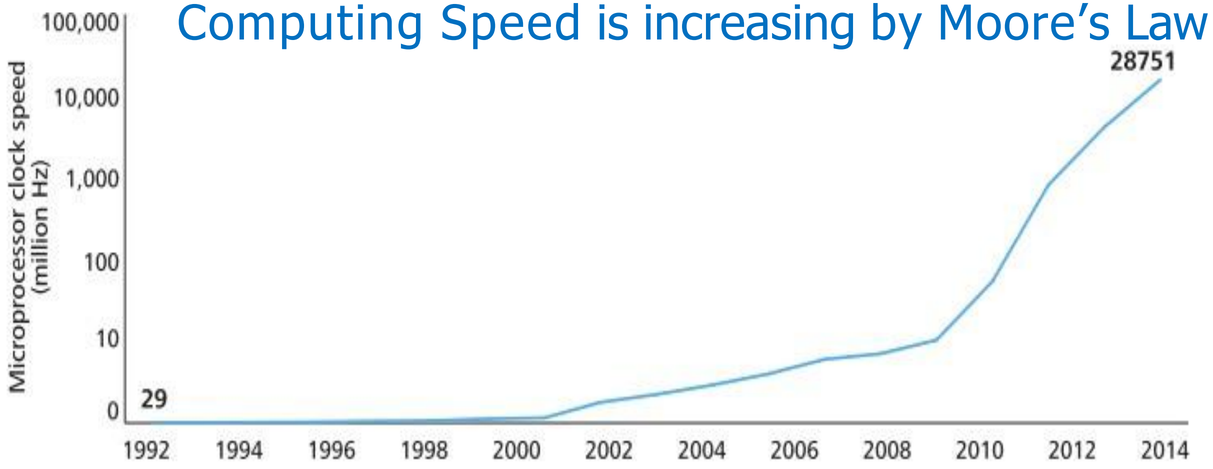
1. Fast, low-cost and small form factor silicon devices

Pentium in 1993, 60MHz @ $878



STM32 F4, 180MHz $3@

Computing Speed is increasing by Moore’s Law

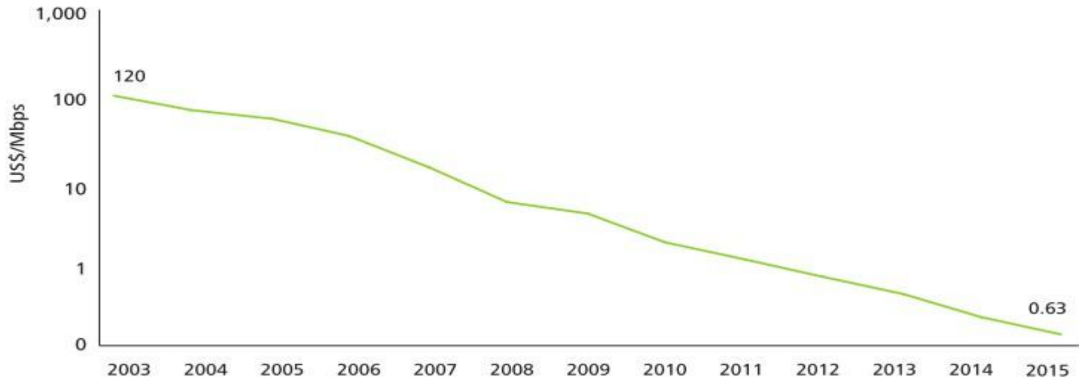


Note: Microprocessor clock speeds are plotted on a logarithmic scale.

Network capacity

2. Networking progress: more bandwidth at low cost

56K Dial-up MODEM → 150Mbps in IEEE 802.11n



Note: Transit prices are plotted on a logarithmic scale.

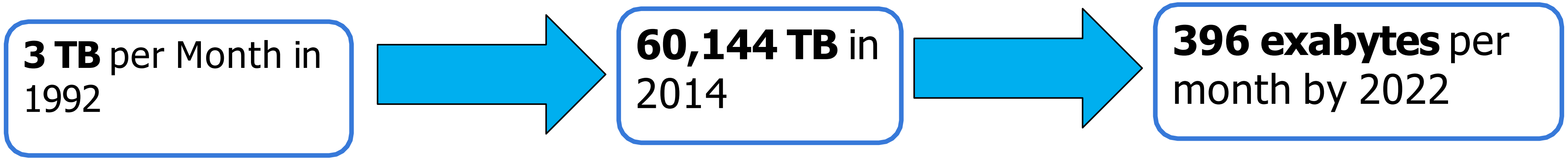
Source: DrPeering.net, http://drpeering.net/white-papers/Internet-Transit-Pricing-Historical-And-Projected.php, accessed January 21, 2015

Why is it Now?

3. IPV6 rollout: can handle 340 trillion addresses.

4. Low power wireless communication technology

Why is it Now?



3 TB per Month in 1992

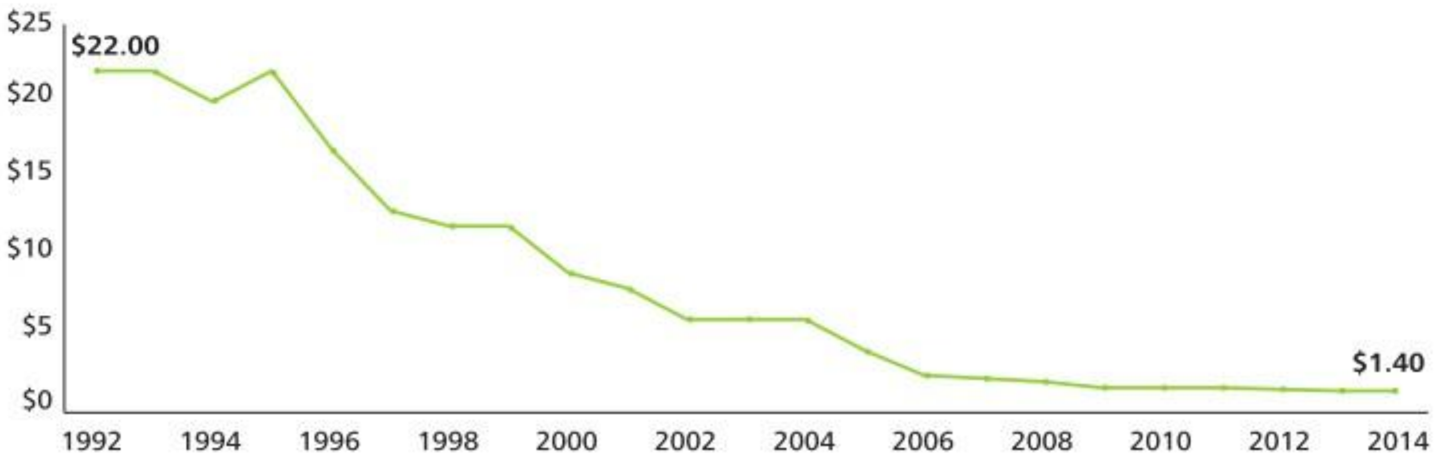
60,144 TB in 2014

396 exabytes per month by 2022

5. Big data tools available for storage and analytics e.g. Hadoop, Apache Spark, Twitter Storm etc

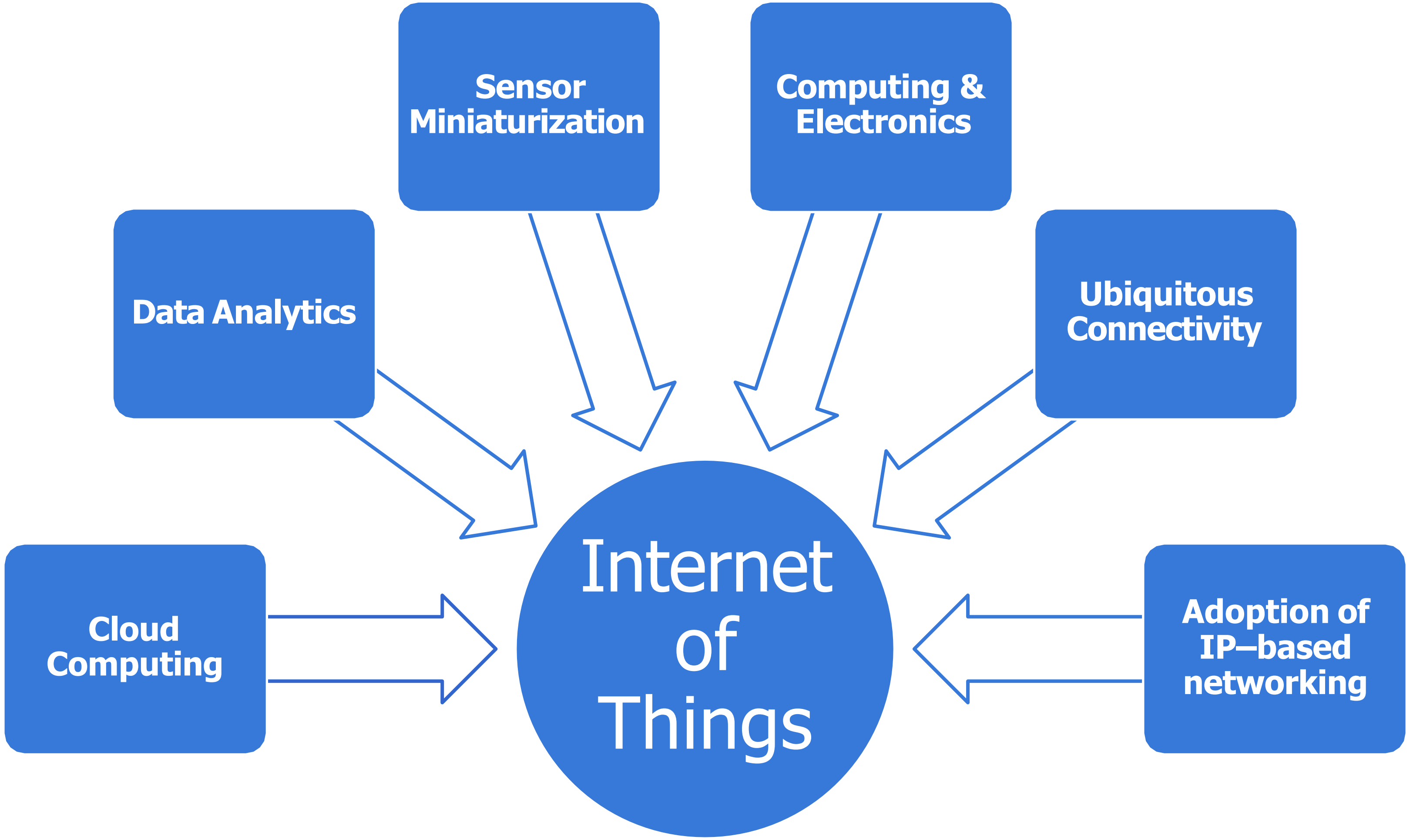
Why is it now?

- Adoption of Sensor Technology
- Cheap Sensors, e.g., the average cost of an accelerometer now stands at 40 cents, compared to $2 in 2006.



- Smaller sensors: a rapid growth in the use of smaller sensors due to Micro-electro-mechanical systems (MEMS) sensors
- Smart Sensors

Convergence of technologies



Convergence of technologies

- For IoT, number of billions of connected devices is an indicator of IoT. The **connectivity is just an enabler but the real value** of IoT is on **data** (business insight/data-driven economy)
- For Big Data, ***data collection*** is one of the main concern, and IoT can play an important role for data collection and data sharing
- For Big Data, data is nothing without real business value insight
- Cloud offers ***Everything as a Service*** business model for IOT and big data.
- **IoT is a King, Big data is a Queen and Cloud is a Palace**

Technologies: Sensors

- Types of Sensors: Potentiometer, motion sensor, Accelerometer, gyroscope, Barometer, humistor, soil moisture sensor, acoustic, infrared, Thermometer, smoke/gas sensor, blood glucose biosensor, pulse oximetry, electrocardiograph
- Size of sensor
- Cost of Sensor
- Accuracy of sensors
- Integration in different devices
- Data gathering and mining techniques
- Energy efficient algorithms and protocols

SENSORS

Wearable blood pressure sensor edges closer to reality

By **Karen Field** • Oct 5, 2020 09:34am

Technologies: networking

- **Why IP?**
- Most of the IP based technologies already exist, well known and proven to be working.
- The pervasive nature of IP networks allows use of existing infrastructure.
- **IP Address Space**
- IPv4 address space exhausted and next version IPv6 developed **BUT**
- 6LowPAN: Adoption of IPv6 for IoT
- More suitable for higher density (128 bit Address)
- Statelessness mandated
- No NAT necessary (adds extra cost to the cost prohibitive WSN)
- Possibility of adding innovative techniques such as location aware addressing
- Larger address width (Having efficient address compression schemes may alleviate this con)

Cloud storage/analytics platforms

- Amazon Web Services (AWS) IoT Platform
  - It provides device Software development Kit, a secure device gateway, registry for device recognition, device shadows (virtual devices), and rules engine
  - Cost per million messages is as low as $5
- Microsoft Azure IoT Suite
- Google Cloud Platform
  - Google Brillo is a great starting point for IoT development.
- IBM Watson IoT
- ThingSepak
- Carriots
- ThingWorx

Whats IoT Security

- An IoT attack whose goal is to (negatively) affect the interaction between a CPS and the physical world
  - Originates through any attack surface
    - cyber, physical, or any combination of cyber/physical
- IoT security concerns the development of technologies for defending against these attacks
  - e.g., discovering new vulnerabilities, techniques for detection/mitigation/recovery, ...

IoT Attack Surfaces

- Cyber attack surfaces
  - e.g., communication, networks, computers, databases, ...
- Physical attack surfaces
  - e.g., locks, hardware ports, cables, ...
- Environmental attack surfaces
  - e.g., GPS signal, electro-magnetic interference, battery draining/cycling/heating, ...
- Human attack surfaces
  - e.g., phishing, bribing, blackmail, etc.

OWASP Attack Surfaces and Vulnerabilities

Attack Surface	Vulnerability
Ecosystem Access Control	•Implicit trust between components •Enrollment security •Decommissioning system •Lost access procedures
Device Memory	•Cleartext usernames •Cleartext passwords •Third-party credentials •Encryption keys
Device Physical Interfaces	•Firmware extraction •User/admin CLI •Privilege escalation •Reset to insecure state •Removal of storage media
Device/Mobile/Cloud Web Interface	•SQL injection •Cross-site scripting •Username enumeration •Weak passwords •Known default credentials

OWASP Attack Surfaces and Vulnerabilities

Attack Surface	Vulnerability
Device Firmware	•Hardcoded credentials •Sensitive information disclosure •Encryption keys •Update sent without encryption •Updates not signed or malicious
Device Network Services	•User/Admin CLI •Denial of Service •Unencrypted Services •UPnP & Vulnerable UDP Services
Administrative Interface	•SQL injection •Cross-site scripting •Username enumeration •Weak passwords •Known default credentials •Two-factor authentication
Local Data Storage	•Unencrypted data •Data encrypted with discovered keys •Lack of data integrity checks

IoT Vulnerability Reports

- Hardware based security challenges in IoT
- Limited processing power to integrate security
  - **CVE-2018-6932** – Code vulnerable to DoS attack due to excessive system resource consumption [3]
    - IP fragment reassembly code in FreeBSD before 11.1-STABLE is vulnerable to a denial of service due to excessive system resource consumption. This issue can allow a remote attacker to send an arbitrary **IP** fragments to cause the machine to consume excessive resources.
- Device heterogeneity makes it difficult to secure
  - Same architecture but various OS functionality
  - Integrating storage and computational process
  - **CVE-2018-3619** – Information disclosure vulnerability allows attacker to recover data via physical access [4]
    - **S**torage media in systems with Intel Optane memory module with Whole Disk Encryption may allow an attacker to recover data via physical access.

IoT Vulnerability Reports

- Hardware based security challenges in IoT
- Embedded system interfaces like UART, JTAG
  - **CVE-2018-9149** – UART security failure in Wi-Fi System [5]
    - The Zyxel Multy X (AC3000 Tri-Band WiFi System) device doesn't use a suitable mechanism to protect the UART. After an attacker dismantles the device and uses a USB-to-UART cable to connect the device, he can use the 1234 password for the root account to login to the system. Furthermore, an attacker can start the device's TELNET service as a backdoor.
- Managing battery consumption and memory
  - Simultaneous application and security services
    - **CVE-2018-15671** – Hierarchical Data Format (HDF) library issue, excessive stack consumption detected in the function [6]
      - An issue was discovered in the HDF HDF5 1.10.2 library. This results in denial of service.

IoT Vulnerability Reports

- Firmware security concerns in IoT
- Secure Boot to verify firmware integrity at device startup
  - **CVE-2018-18653** – User can bypass secure boot restrictions [7]
    - Ubuntu 18.10 when booted with UEFI Secure Boot enabled, allows privileged local users to bypass intended Secure Boot restrictions and execute untrusted code by loading arbitrary kernel modules.
- Hard-coded credentials like password, e-mails etc.
  - **CVE-2018-15781** – Remote attacker can reverse engineer cryptosystem used by Dell Wyse Password Encoder [8].
    - The Dell Wyse Password Encoder in ThinLinux2 versions prior to 2.1.0.01 contain a Hard-coded Cryptographic Key vulnerability.
- Firmware update mechanism
  - **CVE-2018-9232** – Lack of firmware authentication can lead attacker to craft a malicious firmware and use as an update [9]

IoT Vulnerability Reports

- Firmware security concerns in IoT
- Exploitation of backdoors left by product developers
  - **CVE-2018-9919** – Factory backdoor allows vendor to extract confidential information via remote root SSH access [10]
- Default password for various login interfaces
  - Web interface and telnet access
    - **CVE-2019-8950** – Network device allows attacker to login to admin account via Telnet [11]

Exploiting Vulnerabilities in IoT

- A ThingBot is a botnet consisting of devices within the Internet of things.
- Vulnerable or infected appliances that are connected to the Internet can potentially pose a risk to corporate networks.
- Number of attacks against Routers, SmartTV, network-attached storage devices, gaming consoles and various types of set-top boxes is increasing.
- Many set-top boxes runs on embedded linux or apache operating systems of ARM-like microcomputers

Principle abuses of IoT Devices

- Computational capabilities, increasing capabilities of microcomputers and Internet connection makes IoT devices a privileged attack tool for hackers.
- IoT devices could be used to:
  - Send Spam.
  - Coordinate an attack against a critical infrastructure.
  - Serve a malware.
  - Work as entry point within a corporate network.

One of the first cases observed

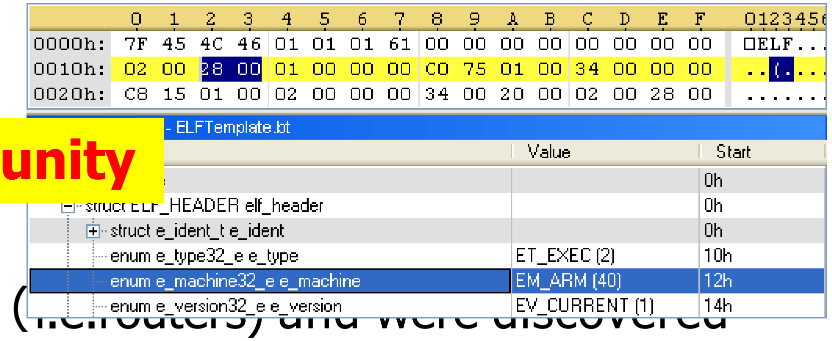
- Proofpoint discovered more than 750,000 Phishing and SPAM Emails Launched From “Thingbots”
- Thingbots could be used in an attack against a critical infrastructure from anywhere in the globe
- Cyber criminals sent in bursts of 100,000, three times per day, targeting Enterprises and ir

Exploited the strength of large number of IoT devices

- More than 100,000 Refrigerators, Smart TVs and other smart household appliances have been hacked.
- No more than 10 emails were initiated from any single IP address.

A Linux worm designed to target IoT devices

- In November 2013 Symantec detected the worm Linux.Darlloz exploiting the PHP vulnerability CVE-2012-1823 to propagate itself.



```
         0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456
0000h:  7F 45 4C 46 01 01 01 61 00 00 00 00 00 00 00 00   ELF...
0010h:  02 00 28 00 01 00 00 00 C0 75 01 00 34 00 00 00   ..(...
0020h:  C8 15 01 00 02 00 00 00 34 00 20 00 02 00 28 00   ......
```

- ELFTemplate.bt

	Value	Start
		0h
struct ELF_HEADER elf_header		0h
struct e_ident_t e_ident		0h
enum e_type32_e e_type	ET_EXEC (2)	10h
enum e_machine32_e e_machine	EM_ARM (40)	12h
enum e_version32_e e_version	EV_CURRENT (1)	14h

Wow .... a new business opportunity

- The Linux.Darlloz infected Home Internet kits with x86 chips (i.e.routers) and were discovered variant for ARM, PPC, MIPS and MIPSEL architectures.

- The worm:
  - generates random IP addresses and attempts to use commonly used credentials to log into the target machine.
  - It sends HTTP POST requests specifically crafted, once compromised the target it downloads the worm from a C&C server and starts searching for other targets.
  - Once the worm has compromised a device, it kills off access to any Telnet services running.

- Change default settings, adopt strong password, keep updated the software and firmware.

Spike botnet runs DDoS from IoT devices

- Akamai spotted a Spike malware which is used to run DDoS attacks through desktops and IoT devices.
- Spike toolkit is able to to generate an ARM-based payload
- The spike botnet was composed by routers, smart thermostats, smart dr and other IoT devices.
- Spike botnet composed by 12,000 -15,000 devices (sept 2014).

Oops … my refrigerator is sending spam messages

- SNORT signature analysis suggested to mitigate application-layer GET f

Hacking Wearable devices

- Data sent between the Smart watch and an Android mobile phone could be intercepted.
- An attacker that could be able to decode users' data, including text messages to Google Hangout chats and Facebook conversations.
- Bluetooth communication between most Smart watches and Android devices relies on a six digits PIN.
- Easy to crack with a brute-force attack.
- Mitigate the attack with NFC pairing procedure in pin code exchange or the use of passphrases.
- PoC with Samsung Gear Live smart watch and Google Nexus 4

Hacking Smart Meters

- Smart meters can be hacked to hit the National power network
- In Spain, millions of Smart meters, are susceptible to cyber attack due to lack of proper security controls.
- 8 million smart meters are deployed in Spain (30 percent of households).
- Attackers could cause a blackout or conduct fraudulent activities (i.e. billing frauds).
- Poorly protected credentials stored in the smart meters.
- Attackers could modify device unique ID to impersonate other customer or use the smart meter for launching attacks against the power network.

More Attacks

Mirai botnet

This botnet infected numerous IoT devices, then used them to flood DNS provider Dyn with a DDoS attack. It took down Etsy, GitHub, Netflix, Shopify, SoundCloud, Spotify, Twitter, and a number of other major websites

Cold in Finland

In November 2016, cybercriminals shut down the heating of two buildings in the city of Lappeenranta, Finland. This was another DDoS attack; in this case, the attack managed to cause the heating controllers to continually reboot the system

Brickernet

that it relied upon a DDoS attack and users not changing the default username/password of their devices. The biggest difference between Brickerbot and Mirai botnet is that Brickerbot simply kills the device.

BrickerBot malware destroys firmware to form a Permanent Denial-of-Service (PDoS) botnet.

Botnet barrage

more than 5,000 discrete systems were found to be making hundreds of DNS lookups every 15 minutes. The botnet spread via brute force attack to break through weak passwords on IoT devices.

Securing IoT

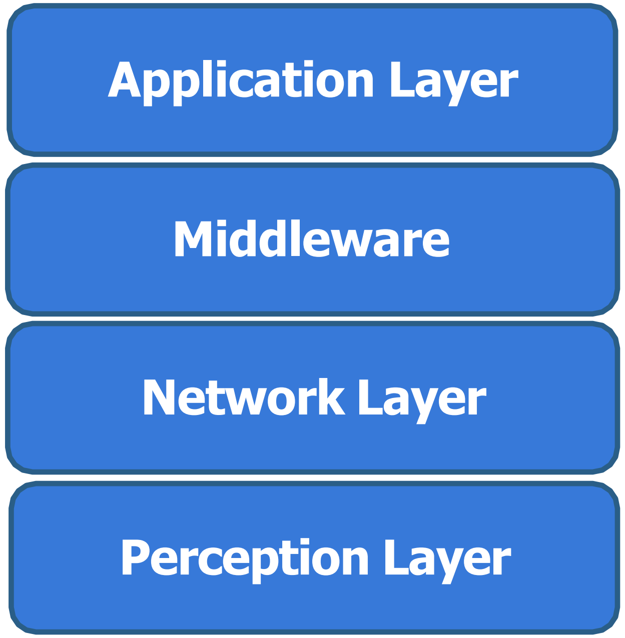
- Demand of connectivity for the Internet of Things(IoT) exploding.
- The global network must be able to securely and efficiently handle all these connections.
- Lack of standardization in the IoT market.
- Every single connection could make networks vulnerable.
- Every connected device has a network address. Internet Protocol (IPv6) extends the addressing space
- DNS will play an even more central role with the diffusion of M2M connections.
- Organizations will need to improve security and prevent DDoS and cache poisoning attacks.

Using Existing Internet Security in IoT

- IoT devices communicate among themselves with little human interaction, mutual authentication is a crucial aspect of the paradigm.
- Recent attacks like the“smart” light bulb password leaks, hacks of Foscam baby monitors, Belkin home automation systems, and hacks of smart cars systems are just the beginning.
- PKI-based solutions could help to secure exchanging information across the Internet and mutual authenticate the actors.
- PKI is already being used to address problems similar to the ones the Internet.
- TLS, IPSec, and other data integrity protocols are complex and hard to apply
- Existing DDOS and IDS are unaware of devices context.

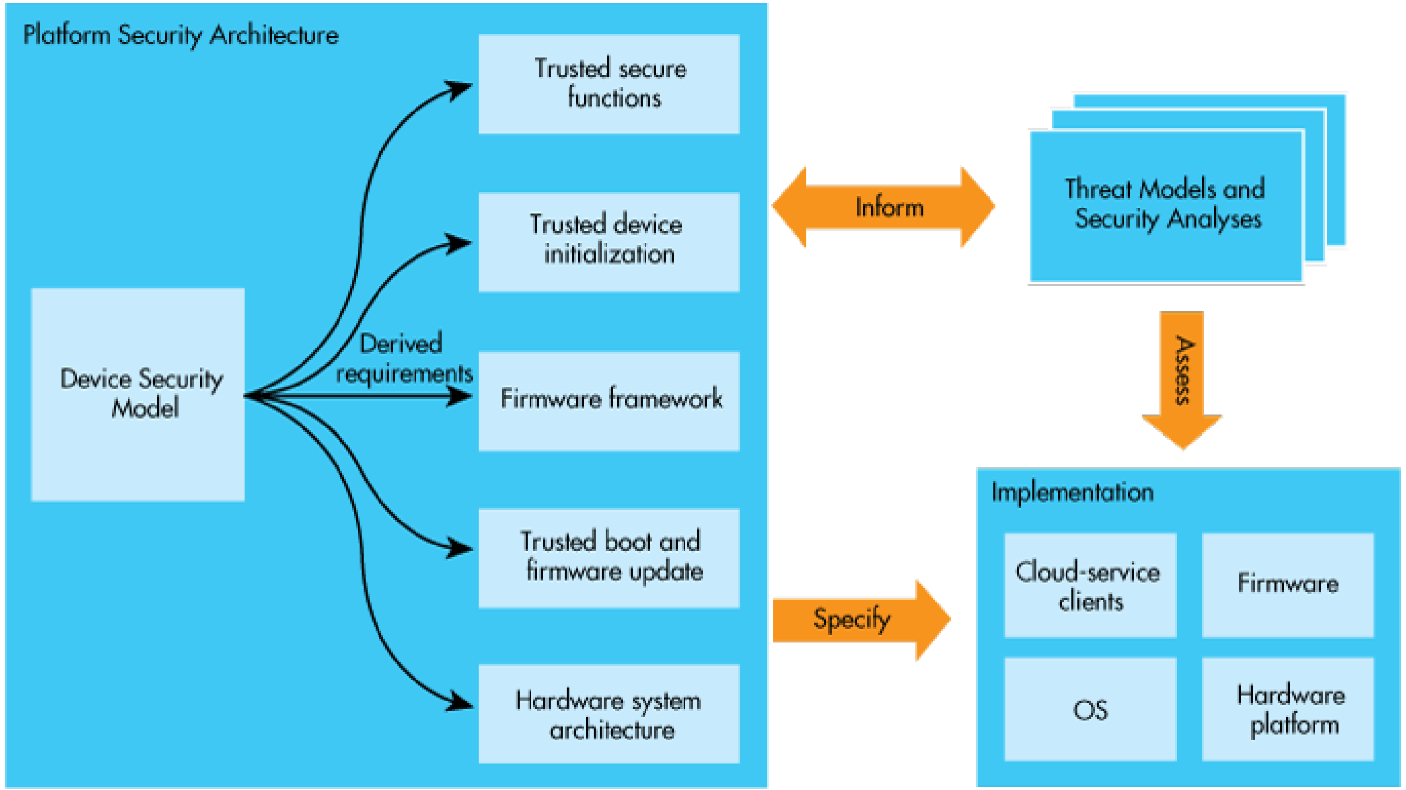
Challenges in IoT Security

- Different architecture of IoT
- Resource constrained devices
- Perception Layer
  - Device cloning, eavesdropping, spoofing, DoS, etc.
- Network Layer Challenges
  - Sybil attack, Dos attack, Man in the Middle Attack (MIMA) just like eavesdropping attack and causes Authentication assault
- Middle ware Layer Challenges
  - unauthorized access, DoS, malicious insider.
- Application Layer Challenges
  - Malicious Code Injection (Malicious code injection is another very serious software type attack in which the attacker selects a node and injects a code in the specific node which causes the shutdown of the network or seriously damages the system [7].), DoS Attack , Spear Phishing Attack (kind of email spoofing attack) and Sniffing Attack [15].



ARM Platform Security Architecture (PSA)

- PSA aims to provide end to end security of IoT devices
- PSA will simplify the process of evaluating IoT devices against security standards [14]



Traditional Security and IoT

"Traditional network security solutions are well established but due to resource constraint property of IoT devices traditional security mechanisms cannot be deployed directly for securing IoT devices from cyber attacks."

E. Gaukstern , "Cybersecurity threats targeting networked critical medical devices," 2018.

To enhance the level of security for IoT, researchers need:

1. IoT Tools
2. IoT Datasets

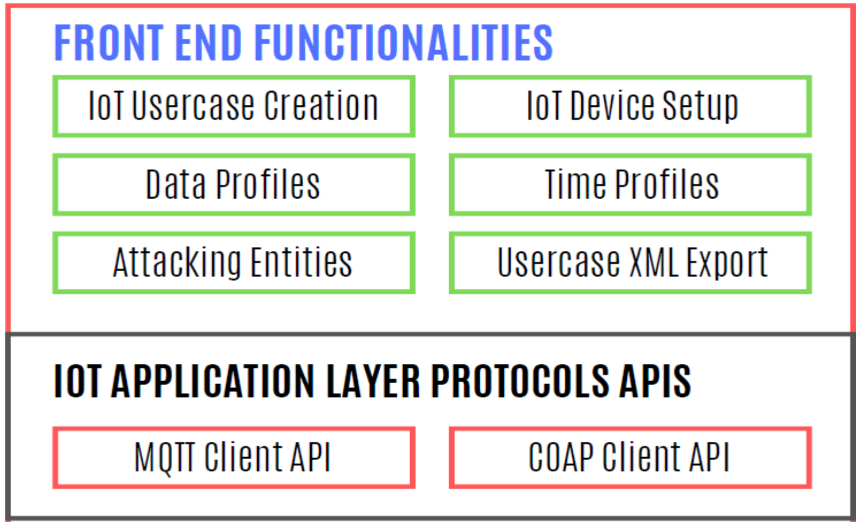
Tool 1: IoT Traffic Generator Tool

1. Open source tool with easily understandable and extendable code

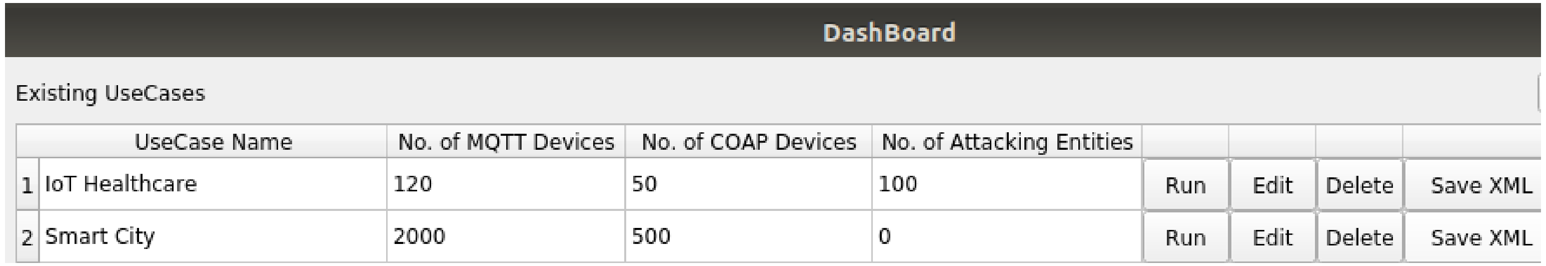
2. Link: *https://github.com/IRIL-KICS/IoT-Advanced-Data-Generator*

3. Capable of creating the real-time IoT use cases with the support of a large number of IoT devices

4. Capable of generating the latest IoT specific attacks. That is not supported yet by any other open source IoT traffic generator tools



IoT Traffic Generator Tool Screens

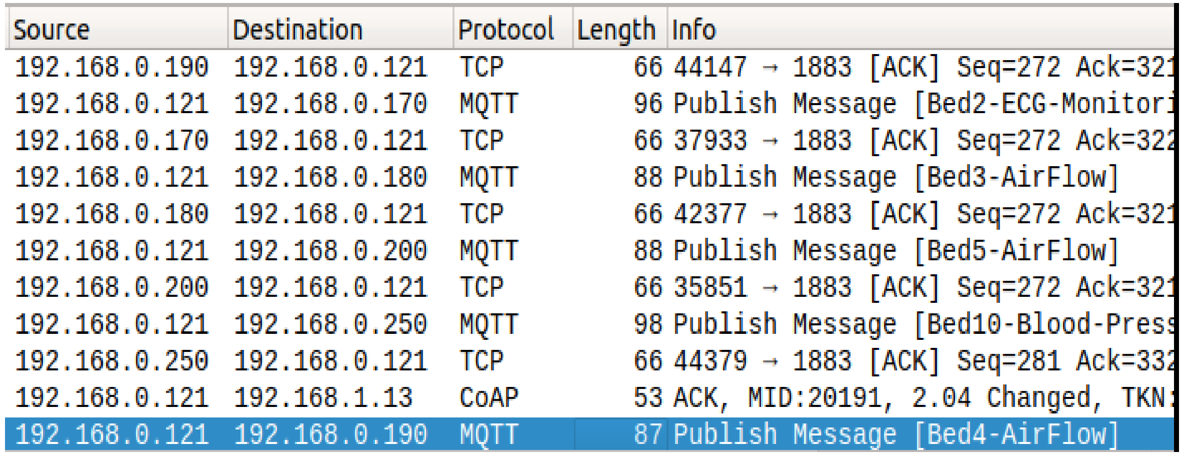


DashBoard

Existing UseCases

	UseCase Name	No. of MQTT Devices	No. of COAP Devices	No. of Attacking Entities				
1	IoT Healthcare	120	50	100	Run	Edit	Delete	Save XML
2	Smart City	2000	500	0	Run	Edit	Delete	Save XML

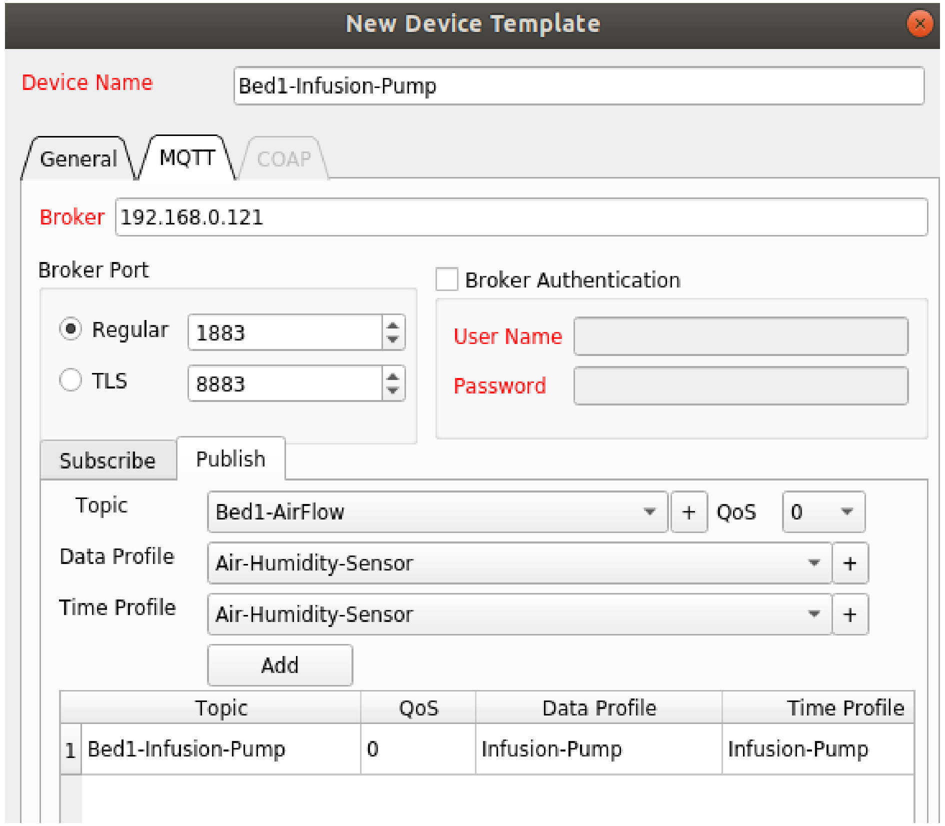
Screen 1: Dashboard of IoT Use Cases



Source	Destination	Protocol	Length	Info
192.168.0.190	192.168.0.121	TCP	66	44147 → 1883 [ACK] Seq=272 Ack=321
192.168.0.121	192.168.0.170	MQTT	96	Publish Message [Bed2-ECG-Monitori
192.168.0.170	192.168.0.121	TCP	66	37933 → 1883 [ACK] Seq=272 Ack=322
192.168.0.121	192.168.0.180	MQTT	88	Publish Message [Bed3-AirFlow]
192.168.0.180	192.168.0.121	TCP	66	42377 → 1883 [ACK] Seq=272 Ack=321
192.168.0.121	192.168.0.200	MQTT	88	Publish Message [Bed5-AirFlow]
192.168.0.200	192.168.0.121	TCP	66	35851 → 1883 [ACK] Seq=272 Ack=321
192.168.0.121	192.168.0.250	MQTT	98	Publish Message [Bed10-Blood-Press
192.168.0.250	192.168.0.121	TCP	66	44379 → 1883 [ACK] Seq=281 Ack=332
192.168.0.121	192.168.1.13	CoAP	53	ACK, MID:20191, 2.04 Changed, TKN:
192.168.0.121	192.168.0.190	MQTT	87	Publish Message [Bed4-AirFlow]

Screen 2: IoT Traffic Captured with Wireshark

IoT Traffic Generator Tool Screens



Device Name: Bed1-Infusion-Pump

Broker: 192.168.0.121

Broker Port

● Regular 1883

○ TLS 8883

□ Broker Authentication

User Name

Password

Topic: Bed1-AirFlow

QoS: 0

Data Profile: Air-Humidity-Sensor

Time Profile: Air-Humidity-Sensor

	Topic	QoS	Data Profile	Time Profile
1	Bed1-Infusion-Pump	0	Infusion-Pump	Infusion-Pump

Screen 3: IoT Device Setup Screen

IoT Healthcare System Dataset

1. Created IoT healthcare dataset with more than 200 IoT devices data.
2. First dataset with IoT protocols specific features.
3. Dataset consist of both Normal & Malicious traffic
4. Ideal for developing Intrusion Detection Systems (IDS) for IoT

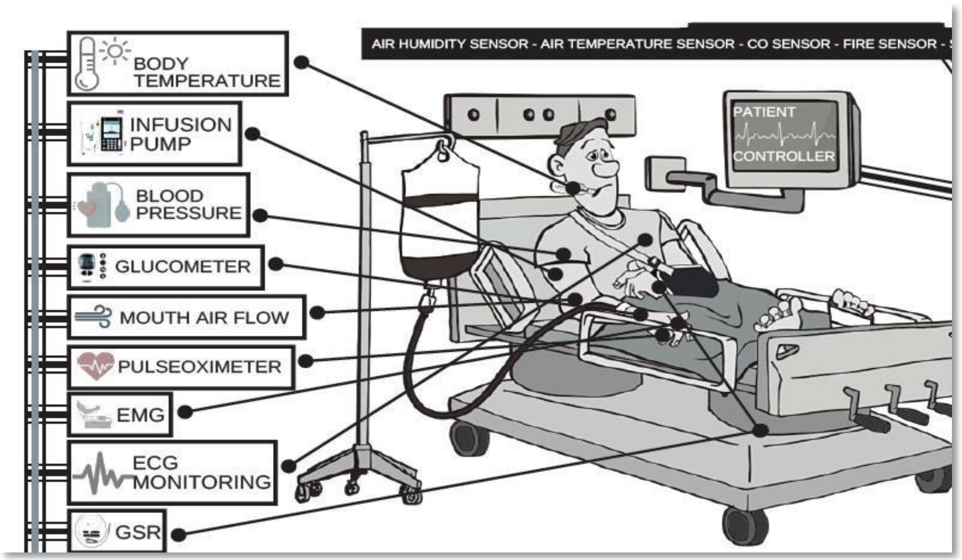


Fig 2: IoT Healthcare Dataset

Tool 2: IoT Firewall

The traditional security mechanisms are deployed at two levels i.e. network level or host level. IoT devices are resource constrained, so the host level security mechanisms cannot be deployed on them.

L. Santos, C. Rabadao, and R. Gonc ̧alves, “Intrusion detection systems in internet of things: A literature review,” in 2018 13th Iberian Conference on Information Systems and Technologies (CISTI). IEEE, 2018, pp. 1–7.

References

1 https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/

2 Baseline Security Recommendations for IoT – ENISA

3 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-6923

4 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-3619

5 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-9149

6 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-15671

7 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-18653

8 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-15781

9 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-9232

10] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-9919

11 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8950

12 William J. Buchanan, Shancang Li & Rameez Asif (2017) Lightweight cryptography methods, Journal of Cyber Security Technology, 1:3-4, 187-201, DOI: 10.1080/23742917.2017.1384917

13 DDoS in the IoT: Mirai and other Botnets

14 ARM Platform Security Architecture Overview Whitepaper