توسعه اینترنت اشیا در آزمایشگاههای تشخیص طبی در ایران: عوامل موثر، فرصتها و تهدیدها

The factors, opportunities and threats of IoT development in Iranian clinical laboratories

دکتر امید پورنیک

Dr. O. Pournik

IoT in Clinical Laboratories in Iran

Dr. O. Pournik

MD, MPH, MBA, MSc., PhD

- Faculty member of Iran University of Medical Sciences
- Head Manager at Centre For Innovation, Incubation and Entrepreneurship (IUMS)
- CEO of Health IoT Lab.
- CEO | Founder of Iran e-Health Accelerator and Innovation Center (InnoHealth)

- عضو هیئت علمی دانشگاه علوم پزشکی ایران، دانشکده پزشکی، گروه پزشکی اجتماعی
- رییس مرکز رشد و نوآوری دانشگاه علوم پزشکی ایران
- رییس آزمایشگاه ملی اینترنت اشیا در سلامت
- مدیر شتاب دهنده سلامت الکترونیک ایران

How the Internet of Things Is Affecting Laboratory Equipment

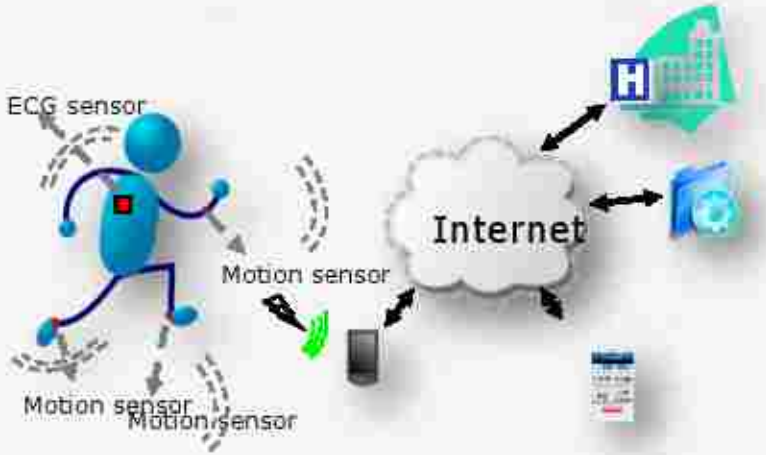
- Ready or not, you need to be planning how to deal with the internet of things (IoT);
  - Simply ignoring it is not an option. You may be able to delay its infiltration of your lab, but that will rapidly become an unfeasible option as more manufacturers incorporate the IoT into their instruments. (It is now inside the home, You don't know it)
  - A much wiser course is to embrace the IoT, but in a controlled process to reduce the risk of security breaches.

So, what is the IoT?

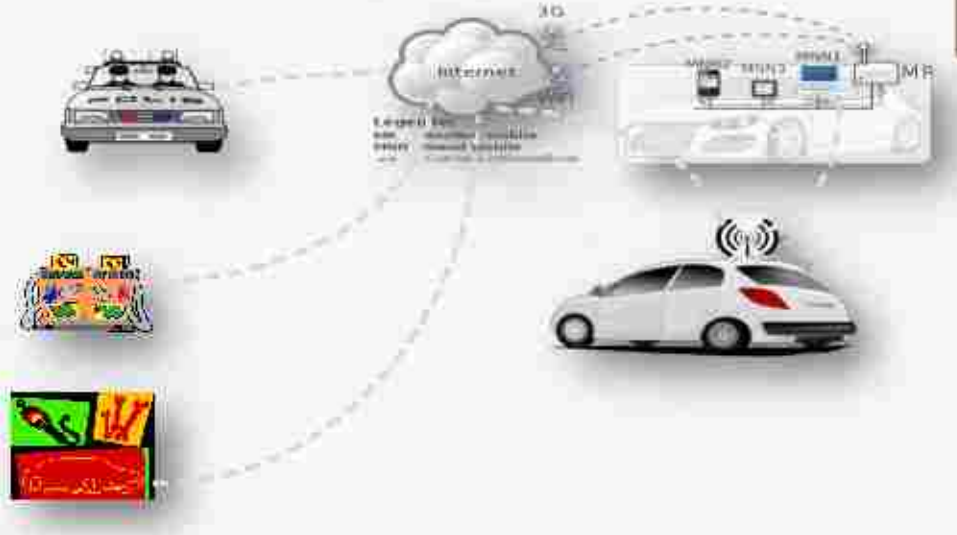
- One of the characteristics commonly cited is that it is focused on
  - Machine-to-Machine (M2M) communication.
  - Beyond that, it generally refers to any device, virtual or physical, that can be connected, either directly or indirectly, to the internet.
  - Gartner has projected that by the year 2020, the IoT will consist of approximately 2.08 x 10^{10} discrete devices, far outnumbering the internet's human users.

New Sources of Information

People Connecting to Things
People Connecting to People



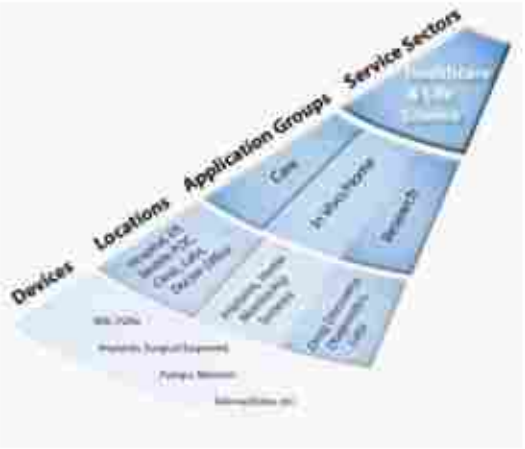
Things Connecting to Things



IoT (M2M) World of Connected Services

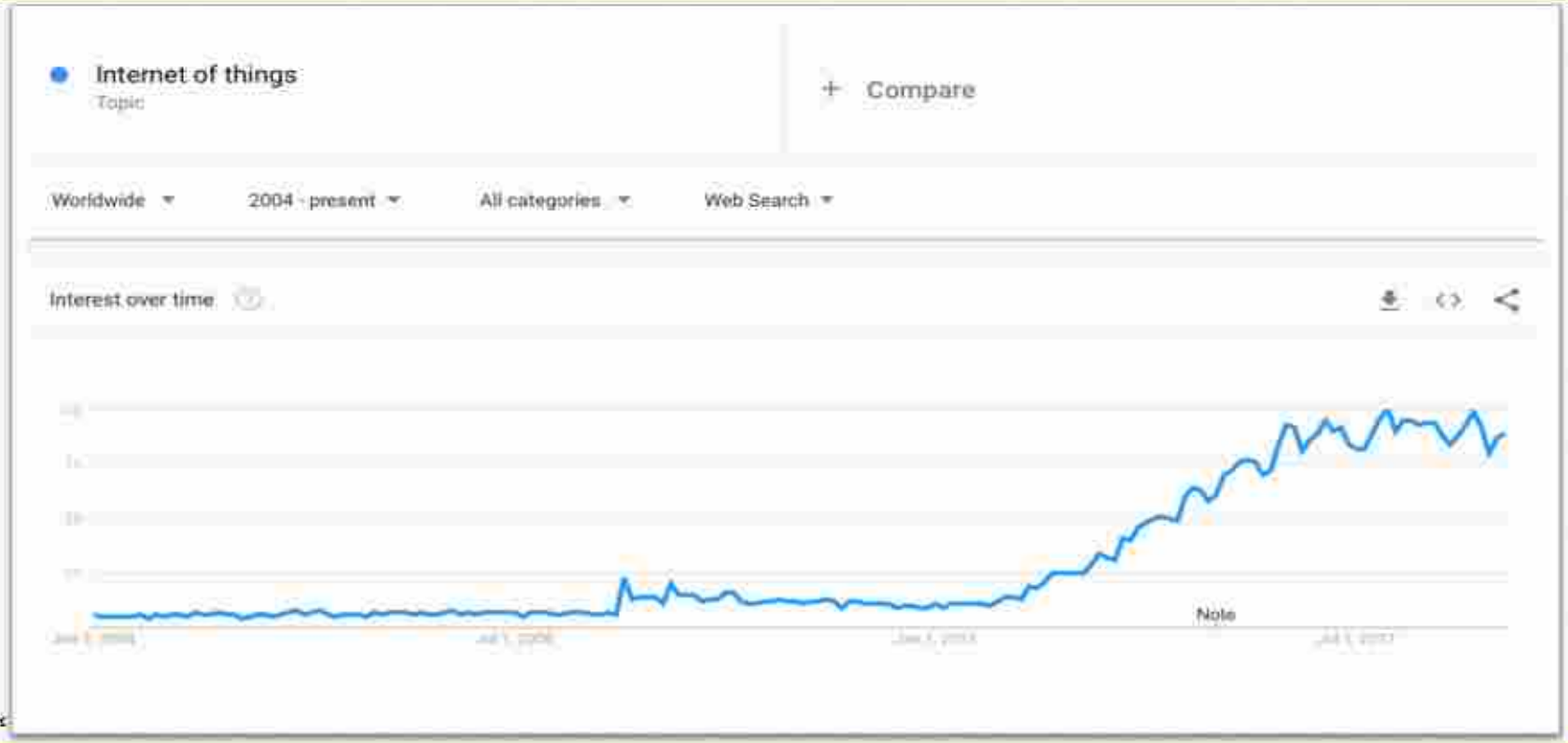
Source: Beecham Research Ltd.

The Healthcare and Life Sciences Service Sector

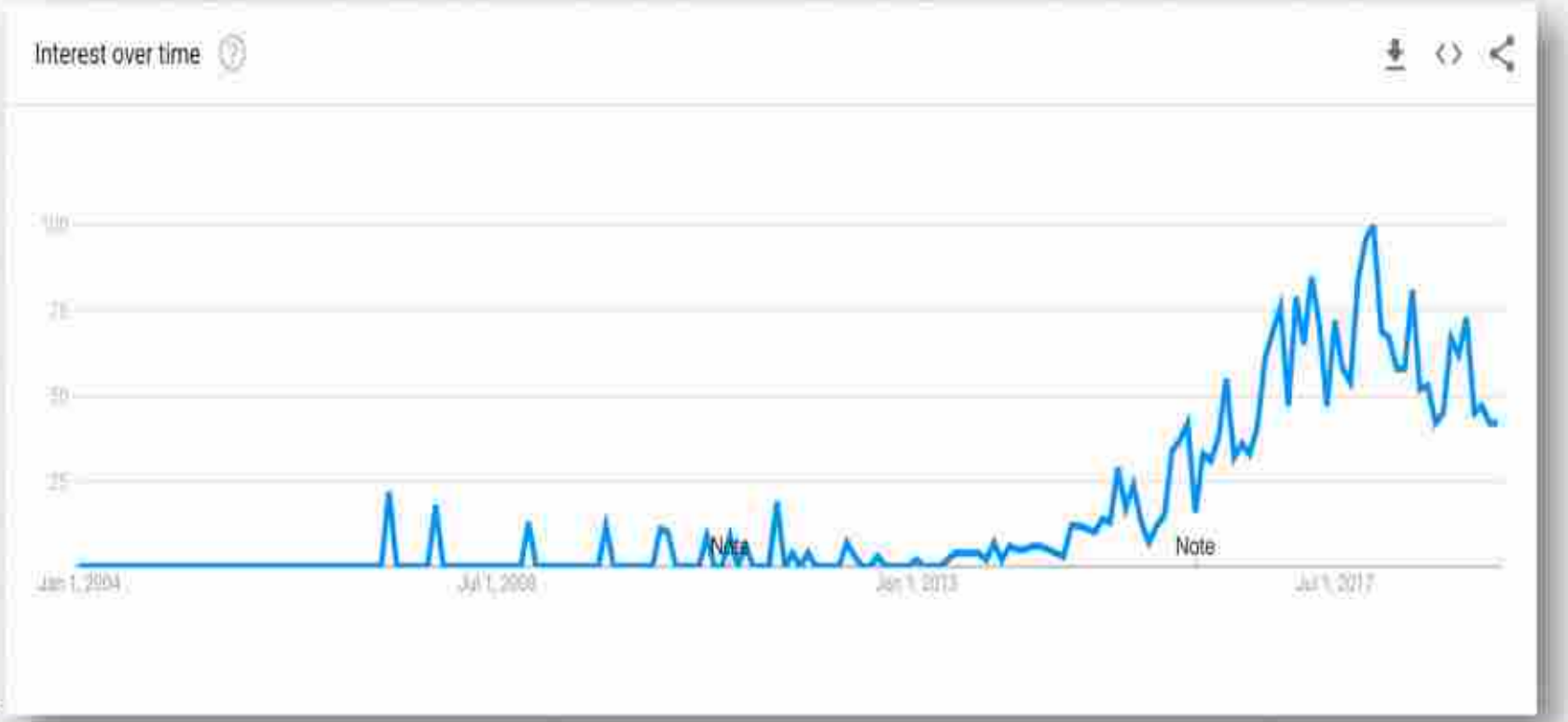


- **Care** - Hospitals, ER, Mobile POC, Clinics, Doctor Office, etc.
- **In Vivo/Home** - Implants (pace makers, etc.), Home Monitoring Systems
- **Research** - Drug Discovery, Diagnostics and Lab equipment

Google trends (2019/02)



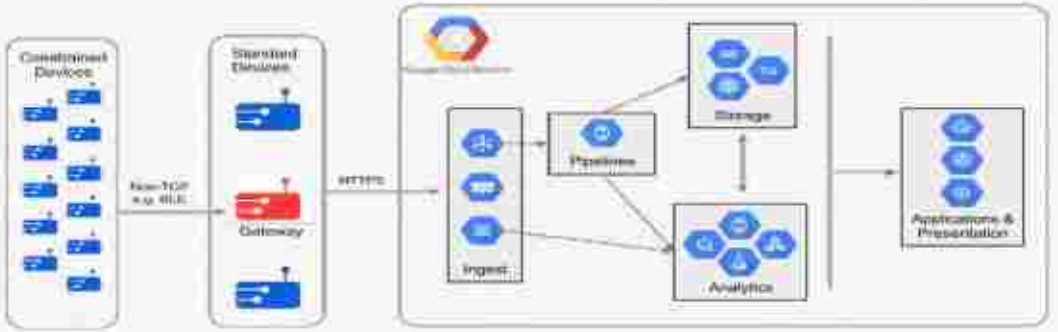
Google trends for IoT in Iran (2019/04)



Fairly simple or …

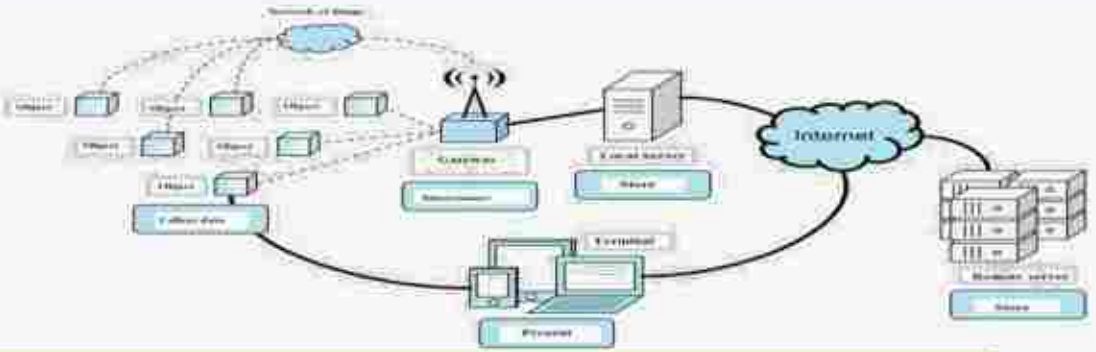
- Unfortunately, while the big picture of the IoT can be presented fairly simply, when you are in the middle of deciding how to implement and configure it, things can get pretty dirty, at least during this "frontier" period of its development.

Approaches to the IoT architecture



- There are several approaches to implementing IoT devices.
  - Currently, the most commonly used one is to implement a standard TCP/IP stack in the IoT unit and have it communicate like any other network device.
    - The advantage to this is that it uses a technology familiar to most IT groups. However, it does allow handshakes between devices, so that you can confirm that a message was received.
    - The drawback is that the cost of integrating the hardware and software to make this possible drives up the cost of the individual sensor devices.
  - An alternate approach is to use multiple inexpensive sensors with a lightweight communication protocol.
    - The trade-off is that no confirmation regarding the receipt of these Chirps is transmitted. The philosophy being that due to the low cost of the sensors, multiple redundant sensors can be distributed, so that if one reading is lost, it doesn't have any impact on operations.

Whichever approach is taken, you still need to receive the data.



- This requirement can be addressed in two ways.
  - The classic approach would be to incorporate code into your applications, such as your LIMS for an analytical laboratory or data acquisition (SCADA) for a process control system.
    - This approach requires custom modifications of the system for each sensor that you add.
  - In most situations, it is much more pragmatic to use a Web of Things gateway, which could consist of a middle ware software layer in your network or a physical hardware module.
    - The purpose of this gateway is to aggregate the data from IoT devices, filter out the unneeded information, transform it into a format that your laboratories' instruments and applications can understand, and deliver it to them. There are a number of proprietary gateways being developed by vendors. However, the basic operation of these gateways can be illustrated by the open gateway for the internet of things being developed by Mozilla[4].

Benefits of the IoT

- The IoT promises a major paradigm shift in the way we work and think about equipment.
- Common illustrating applications might include:
  - Monitoring chemical/reagent inventories, and automatically reordering.
  - Monitoring controlled environments, such as server rooms or reagent storage areas, for over/under temp conditions.
  - Monitoring equipment for regulatory or operational compliance. This could range from monitoring incubators or freezers to ensure that they remain within their optimal temperature range.
  - Safety tracking and remote communication with employees.
  - Monitoring sample temperatures, whether collected internally or externally, to ensure that there are no excursions outside of the regulatory temperature storage range.
  - Possibly even capturing the actual sample collection point.

Benefits of the IoT

- Other laboratories will have more unique requirements, with highly variable degrees of overlap. These are illustrated by:
  - Monitoring the identity, location, and condition of patients.
  - Allowing notes and observation entries, as well as treatment orders via smart pens.
  - Capture of data from freestanding instruments.
  - Monitoring the status and location of employees in lone operator situations via wearable devices.
  - At this point in time, we've only scratched the surface regarding the impact of IoT-enabled devices. In the future, there will be an ever-expanding range of uses, limited only by our imagination.

The dark side of the IoT

- Some of these issues are due to errors in device design or programming. Other issues concern the privacy and confidentiality of the data collected.
- However, the above is minor in comparison to active attacks on the IoT.
  - Some of the largest denial-of-service attacks encountered so far have been launched using perverted internet security cameras and other IoT devices.
  - In some instances, this co-opting of devices has been managed by breaching the devices' security by brute force attacks, though in the majority of cases the exploit was frequently due to the owners not changing the default password on the devices.
- This is not the only risk, as once the security of a single device is penetrated, that can be leveraged to launch attacks against other components in the network.
  - to capture internal data, inject erroneous data, or actively sabotage equipment

Best practices

Steps that you, as the laboratory manager, can do to minimize this risk:

- Change the default password on all IoT devices before installation. If the manufacturer has a fixed password that cannot be changed, go with a different vendor.
- Ensure that any unused ports and protocols on the device are disabled.
- Ideally, all data transfers should be encrypted, with each device using a different encryption key.
- Where possible, purchase equipment that supports over-the-air (OTA) firmware updates.
- Don't purchase equipment with known security issues, even if you must forfeit some features.
- Security practices are different for IoT systems and traditional networks, so IT personnel will potentially be unfamiliar with the differences. While probably not in a position to ensure that proper procedures are followed, you can strongly suggest that your IT support personnel learn through some ways.
- Ensure that a compliance monitoring program is set up for the IoT, to ensure that your security remains in compliance.

Summary

- We have seen how an IoT implementation can revolutionize your laboratory operations, but that it does have risks.
- Particularly as manufacturers and IT support teams explore this new paradigm, it is not unlikely that at least some of the IoT devices already inside your organization have been compromised, so you need to coordinate with IT to ensure that all devices have been locked down, both to ensure the security of your operations and to remove potential legal liability.
- Approached proactively, the IoT allows you to reengineer many processes, improving both data quality and productivity.

Threat vs. Opportunity

The IoT is propelled by an exceptional convergence of trends: mobile phone ubiquity, open hardware, big data, Artificial Intelligence, cloud computing, 3D printing, and crowdfunding

- The world is rapidly evolving to where just about everything will be connected
- The number of cyber attacks will rapidly increase
- Privacy and security must be fully addressed

So…

- If misunderstood and misconfigured, IoT poses risk to data, privacy, and safety

But…

- If understood & secured, IoT will enhance communications, lifestyle, and delivery of services

Who cares? No need? Just a luxury?

2019 TRENDS IN Health Sector

Clinical Laboratory that do not consider their entire infrastructure when implementing devices may find themselves with devices

that don't function properly or aren't secure.

- Dr. O. Pournik
- MD, MPH, MSc., MBA, PhD in Medical Informatics
- Founder and Director of Health Internet of Things laboratory
- Iran University of Medical Sciences
- pournik.o@iums.ac.ir