THE APPLICATIONS OF THE INTERNET OF THINGS IN THE MEDICAL FIELD

STUDENT: CODY REPASS

FACULTY ADVISOR: DR. LIXIN WANG

COLUMBUS STATE UNIVERSITY

CAE CYBERSECURITY COMMUNITY SYMPOSIUM

JUNE 9-10, 2022

OUTLINE

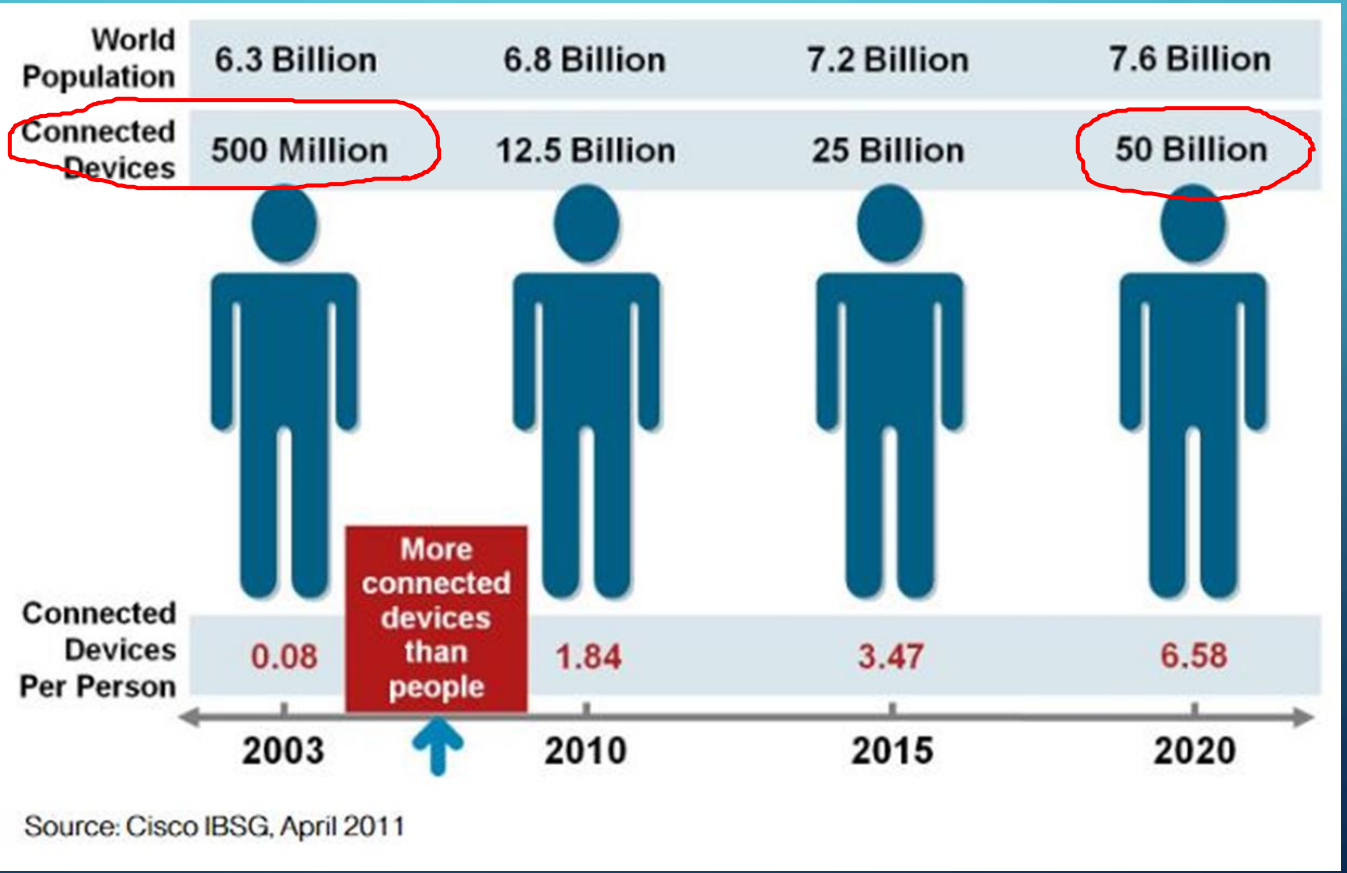
- **Intro to IoT**
- Applications of IoT in the medical field, intro to Internet of medical things (IoMT)
- Privacy and Security Concerns of IoMT
- Security countermeasures to protect IoMT devices

INTRO TO IOT

- IoT allows for interconnectivity among smart objects to collect, send, and receive information
- IoT is intended to give smart objects communication capability to make automated and smart decisions using the information collected and exchanged
- The IoT paradigm promises to make “things” to be accessible at anytime and anywhere
  - The “things” include a more generic set of entities such as smart devices, sensors, human beings, and any other IoT objects (aware of their context and able to communicate with other objects)

INTRO TO IOT (CONT.)

- The number of connected IoT devices increased by about100 times from 2003 to 2020



BASIC BUILDING BLOCKS OF IOT

- **Sensors** that gather information
- **Networks and gateways** for information transmission and exchange
- **Middleware** in the IoT devices lets them communicate with each other
- **A data processing and storage mechanism** (e.g., the cloud)
- **A user interface** that allows end users to interact with the IoT system

OUTLINE

- Intro to IoT
- **Applications of IoT in the medical field, intro to Internet of Medical Things (IoMT)**
- Privacy and Security Concerns of IoMT
- Security countermeasures to protect IoMT devices

APPLICATIONS OF IOT IN THE MEDICAL FIELD

- IoMT is a growing application of IoT technology
- It directly improves the life quality of patients and eases the burden on healthcare providers
  - For example, a monitor attached to an IoMT system can be sent home with a patient to measure heart rate, blood pressure, oxygen levels, etc.
  - The patient's medical information can be collected and sent to healthcare providers who can review and analyze it remotely, and then make decisions

THE PURPOSES OF USING IOMT

- IoMT consists of IoT devices specifically developed to meet the needs of patients and healthcare facilities
- The purpose of using IoMT is to make patient care much simpler and more efficient for all the people involved – patients, doctors, nurses, etc.
- Three main categories of IoMT applications
  - intensive care
  - remote patient monitoring (RPM)
  - context awareness

THE PURPOSES OF USING IOMT CONT.

- **Intensive care** refers to patients who are in ICUs and require ongoing monitoring to provide information about their conditions
- **Remote patient monitoring (RPM)** allows healthcare facilities to make the decision of sending patients home for further care
  - RPM also provides a personalized treatment plan that encourages patient/doctor interaction
  - This application is commonly used for patients with chronic conditions or diseases
- **Context awareness** gathers information about a patient's environment

THE PURPOSES OF USING IOMT CONT.

- IoMT allows patients to signal an emergency, and immediately notify healthcare providers for emergency services
- IoMT can help with diagnosing conditions through real-time monitoring
  - Continuous monitoring of a patient's physiology provides healthcare professionals with great insight into a person's health
  - IoMT eases the burden of healthcare workers by outsourcing treatment to RPM

THE PURPOSES OF USING IOMT CONT.

- IoMT also allows for easier and quicker access to patients' data
  - Electronic health records (EHR) are simpler to access with mobile apps on IoMT devices
  - Mobile apps assist healthcare providers with precise assessments, examinations, and diagnosing of patients
- Leaning on IoMT systems reduces healthcare costs for the healthcare business
  - IoMT is cost-effective for healthcare providers as well

OUTLINE

- Intro to IoT
- Applications of IoT in the medical field, intro to internet of medical things (IoMT)
- Privacy and Security Concerns of IoMT
- Security countermeasures to protect IoMT devices

PRIVACY AND SECURITY CONCERNS OF IOMT

- The Health Insurance Portability and Accountability Act (HIPAA) is a federal law created in 1996 to provide a set of standards for protecting sensitive patient information
- The goal of HIPAA is to prevent unwanted disclosure of protected health information (PHI) of patients
  - PHI consists of medical records and information that can identify an individual (age, sex, height, weight, birth date, etc.)

PRIVACY AND SECURITY CONCERNS OF IOMT CONT.

- The privacy rule of HIPAA seeks to **provide adequate protection of PHI** while enabling covered entities to transmit and access necessary patient information
  - The HIPAA security rule protects all PHI collected, maintained, and transmitted in an electronic format (ePHI)
  - The security rule addresses the administrative, physical, and technical safeguards used to secure ePHI

SOME OF THE MOST COMMON HIPAA VIOLATIONS

- Snooping on ePHI/PHI
- Failure to conduct risk assessment/management on ePHI/PHI
- Denying patients' access to records
- Lack of access controls for ePHI (e.g., authorization)
- Wrongful disclosure of PHI/ePHI
- Improper disposal of PHI/ePHI

OUTLINE

- Intro to IoT
- Applications of IoT in the medical field, intro to internet of medical things (IoMT)
- Privacy and Security Concerns of IoMT
- **Security countermeasures to protect IoMT devices**

SECURITY COUNTERMEASURES

- Currently, there is a big security gap in the development of IoMT devices
  - According to a survey by a HIPAA Journal, ONLY about half of the IoMT device manufacturers stated that security was considered as a factor during the design process
  - The majority (about 82%) of the manufacturers stated that they have major security concerns and felt that safeguards were lacking to protect from attacks

SECURITY COUNTERMEASURES CONT.

- It is the manufacturer's responsibility to
  - adequately develop and prepare IoMT devices for deployment, and
  - provide certain security countermeasures innately to ensure compliances

SECURITY COUNTERMEASURES CONT.

- Having rules in place that dictate who can access what resources and for what purpose prevents unauthorized access, and reduces the likelihood of the IoMT devices or data being compromised
  - For example, only certified and authorized physicians may have access to the EHR of patients

SECURITY COUNTERMEASURES CONT.

- Network segmentation is a useful security countermeasure for the telehealth provider and the healthcare provider
  - For example, segmenting the EHR servers from the rest of a hospital's network provides additional security so that the ePHI cannot be accessed from within the main hospital network

SECURITY COUNTERMEASURES CONT.

- Network hardening refers to security countermeasures that support network security
- Network hardening can mean that firewall rules are configured more strictly to prevent additional traffic
- Closing certain ports and using demilitarized zones (DMZs) to protect the internal private network of a hospital system

SECURITY COUNTERMEASURES CONT.

- Disabling unused network services, implementing IDS and IPS are also countermeasures to harden a network
  - IDS and IPS reduce the risk of attacks like DoS, DDoS as well as break-in attacks

SECURITY COUNTERMEASURES CONT.

- An administrative countermeasure for securing IoMT is creating some means of IoMT training and education for healthcare staff
- Healthcare professionals must have awareness of the risks involved with IoMT and understand the importance to protect ePHI
  - E.g., educating staff on what email phishing looks like and how to report it can mean the difference between a hefty HIPAA fine and successfully protecting ePHI

SECURITY COUNTERMEASURES CONT.

- Lightweight security protocols have been developed to further protect information on resource constrained IoMT devices. E.g., 6LowPSec
  - A lightweight version of IPSec for IoT devices
  - end-to-end security solution for 6LowPan (IPv6 over low power wireless PAN) IoT devices
  - provides end-to-end security that reliably delivers data in resource-constrained environments, while reducing overhead and computational requirements
  - security features include data confidentiality using AES-128, and an IDS for advanced security

SECURITY COUNTERMEASURES CONT.

- The cloud can provide secure storage for IoMT data with a private cloud
- Mechanisms such as Amazon AWS simple storage service (S3) allows for scalable and secure storage of IoMT data
  - Any file can be stored in what's known as an S3 bucket
- AWS provides identity and access management to ensure safe storage of IoMT data
  - Ex. public access to S3 buckets is automatically blocked by default
- AWS CloudTrail provides detailed logs of activities

THANKS & QUESTIONS