Security In HealthCare

CSC 6980: Security in IOT

Presenters

Shiv Patel

Cristian Drew Wensel

Mounika Ghanta

Georgia State University

Challenges & Opportunities in IOT Healthcare

Architecture in IoT

Patients are connected with sensors which are associated with control devices, and then the data is forwarded to a health-monitoring unit.

Use of cloud technology helps to manage the high amount of data transmitted.

Security can then become an issue because this transmission allows for a loss of integrity and confidentiality.

Hybrid Cloud Environment

To reduce the complexity of in the IoT/Cloud architecture, a hybrid cloud architecture is proposed.

SMFIC - Service Management Framework for IoT Devices comprised of three layers:

- Consumer layer: collects data from smart home, patients, social network, and smart healthcare service.
- Service provider layer: provides sharing of physical resources, service management, virtualization, security & privacy.
- Middle layer: manages services between provider and consumer.

Proposed Architectures

Temporal Fuzzy Ant Miner Tree:

- Combines Ant Colony Optimization with decision tree and fuzzy rules (conditional statements)
- Collects real-time data with sensors and analyzes physical and behavioral trends in homes

Machine Learning Algorithm for Early Detection of Disease:

- Three tier architecture:
  - Collects sensor data from wearable devices
  - Stores data in cloud
  - Regression-based prediction model for heart disease
  - Also used for monitoring and detecting arthritis

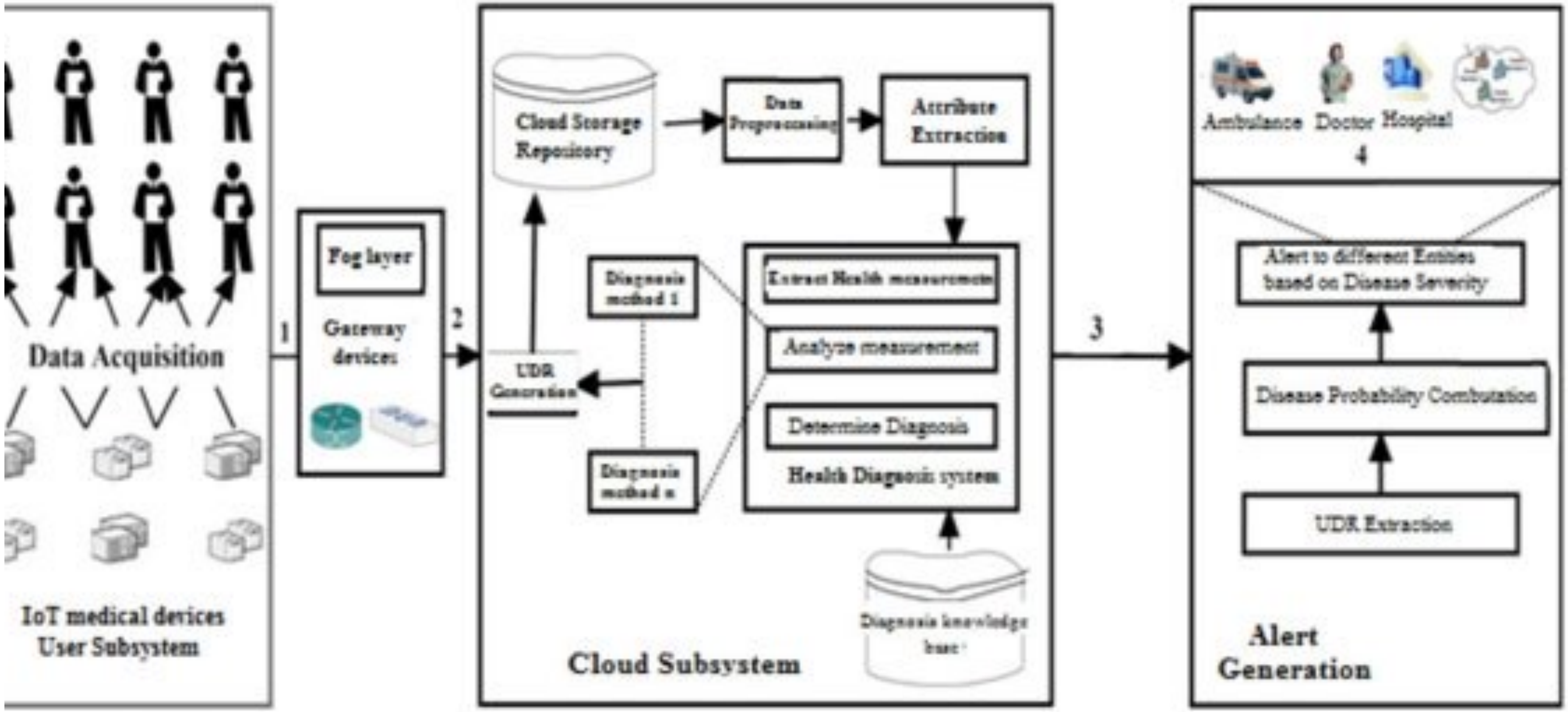
Built-in Manager
Gateway Controller
Built-in Agent
Bluetooth Module
Wire-Wireless Module
DB
Wireless Network
Mobile Communications
Wibro/LTE/Wimax
All Room Area
Camera
Speaker
Sensor
WBAN
Healthcare Device
Home Health Gateway
Home Healthcare Management Center
Operator gateway
Real-time Capture
Emergency Situation Recognition
Motion Tracking
Emergency Situation Monitoring
Move please~!
(3 Times)
Family
Social Worker
Acquaintances
Air Ambulance
Ambulance
Chronic Disease Patient Monitoring Services
Smart Home
Healthcare Management Center
Medical Center

Cloud Integration

The use of cloud technologies allows for flexibility, scalability, and higher number of resources to be used in processing the data.

The physiologically based attributes of patients are measured, and the information is stored in the cloud. Once the user subsystem has completed the data collection from IoT medical devices, the data is sent to the cloud subsystem for diagnosis.

The greatest challenge posed in this architecture, is the network delay.


Data Acquisition
IoT medical devices
User Subsystem
1
Fog layer
Gateway devices
2
Cloud Storage Repository
Data Preprocessing
Attribute Extraction
UDR Generation
Diagnosis method 1
Diagnosis method n
Extract Health measurements
Analyze measurement
Determine Diagnosis
Health Diagnosis system
Diagnosis knowledge base
Cloud Subsystem
3
Ambulance
Doctor
Hospital
4
Alert to different Entities based on Disease Severity
Disease Probability Combutation
UDR Extraction
Alert Generation

Security in IoT Healthcare

Hackers and attackers have easy access to sensor data

IDP (IoT-oriented Data Placement):

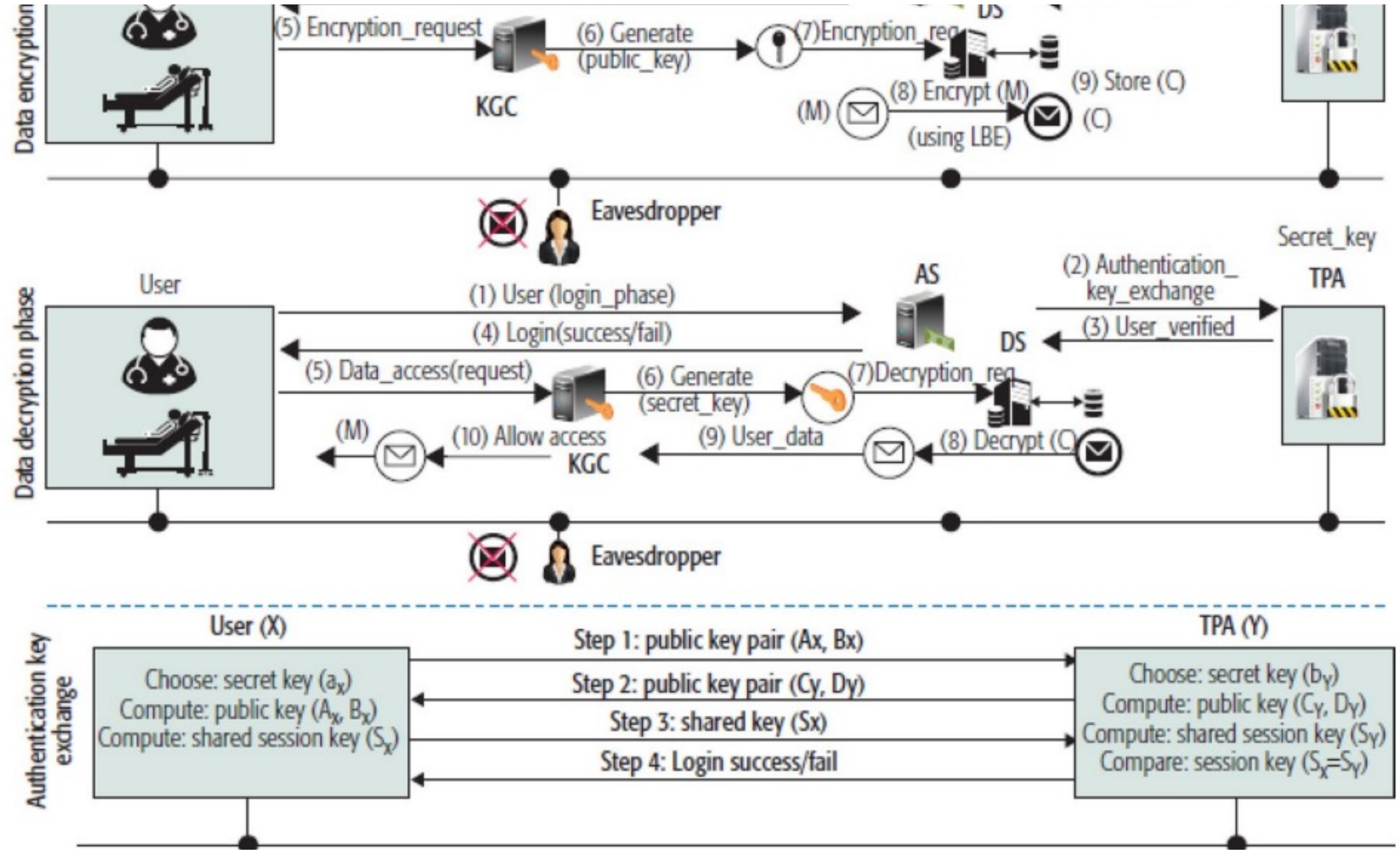
- Optimize data access time
- Increase resource utilization
- Reduce energy consumption
- All while maintaining data privacy
- Achieved using Non-dominated Sorting Genetic Algorithm II (NSGA-II)

NSGA-II

- Processes data on user's health profile
- Recommendation is processed at the cloud healthcare recommender service.
- RFID encryption is used to provide security of the medical data
- Cloud Service Provider (CSP) consists of three servers:
  - Authentication Server
  - Key Generation Center
  - Database Server

Lattice-based Secure Cryptosystem

- Four phases:
  - Setup phase
  - Key generation phase
  - Data encryption phase
  - Data decryption phase
- The three phases, the lattice polynomial vectors are used as input in the first phase and the KGC is generated i.e., the private and public key, in the second phase and shared with the Database Server (DS). In the last phase, the message is used as an input parameter and combines it with the random polynomial. If any user sent a request to access the medical data, the KGC transfers the secret key pair to the DS using a secure channel. The DS process the plaintext message using the input parameters and the secret key pair.



Data encryption
(5) Encryption_request
KGC
(6) Generate
(public_key)
(7)Encryption_req
DS
(9) Store (C)
(M)
(8) Encrypt (M)
(using LBE)
(C)
Eavesdropper
Data decryption phase
User
(1) User (login_phase)
(4) Login(success/fail)
AS
(2) Authentication_
key_exchange
(3) User_verified
Secret_key
TPA
DS
(5) Data_access(request)
(6) Generate
(secret_key)
(7)Decryption_req
(M)
(10) Allow access
KGC
(9) User_data
(8) Decrypt (C)
Eavesdropper
Authentication key exchange
User (X)
Choose: secret key (a_X)
Compute: public key (A_X, B_X)
Compute: shared session key (S_X)
Step 1: public key pair (Ax, Bx)
Step 2: public key pair (Cy, Dy)
Step 3: shared key (Sx)
Step 4: Login success/fail
TPA (Y)
Choose: secret key (b_Y)
Compute: public key (C_Y, D_Y)
Compute: shared session key (S_Y)
Compare: session key (S_X=S_Y)

Challenges in healthcare IoT

- IoT paves the way for high flexibility, i.e., the patient requires constant care, and he/she can live in the home instead of the hospital and be monitored regularly using IoT technology. Some wearable devices like sensors make uncomfortable for the patient’s body.
- The data transmitted from the sensor to the control device and further transmitted to the monitoring center, which will affect the quality of the data due to noise. Better architecture helps to transmit the data without affecting its nature. Noise removal technique can also help to enhance the data signal.

Challenges in healthcare IoT

- Most of the existing methods in ECG monitoring involve analyzing the signal in a supervised manner. This increases the cost and may produce an error in detection. Machine learning can be applied in analyzing the signal, which helps to improve efficiency and reduce expenses.
- An increasing number of sensors and the devices require higher energy to process, and it increases the power leakage and energy consumption. An optimization algorithm can be used to reduce the usage of energy.

Challenges in healthcare IoT

- Monitoring many numbers of users in the IoT requires more storage and mainframe, which can be overcome by storing the data in the Cloud. However, the IoT integrated with the cloud increases the complexity.
- Another important problem in the IoT is privacy as the devices are more vulnerable to attacks. These devices have low resource constraints which makes it difficult to apply encryption techniques on them.

cloud computing is used to handle data and provides resource sharing facilities,

Wearable technologies are efficient but demand the patience of users for their short battery lifecycle; needing to be charged regularly (if it requires nurse engagement, it sort of defeats the point

The data is very vulnerable to hackers/attackers

What are the applications of Iot devices in Healthcare?

- IoT in healthcare is the ecosystem of IoT-enabled healthcare devices connected via chips, sensors, or other related technologies to constantly monitor patient vital signs (e.g. blood pressure, heart rate, temperature, respiration rate, etc.), physician’s activity, and the overall hospital environment, to improve the efficiency of hospital equipment and staff.

IOT Healthcare Devices

Wearables

- Smartwatches
- Rings
- Vests

Monitors and sensors

- Heart monitors
- Sleep monitors
- Temperature monitors
- Air quality sensors

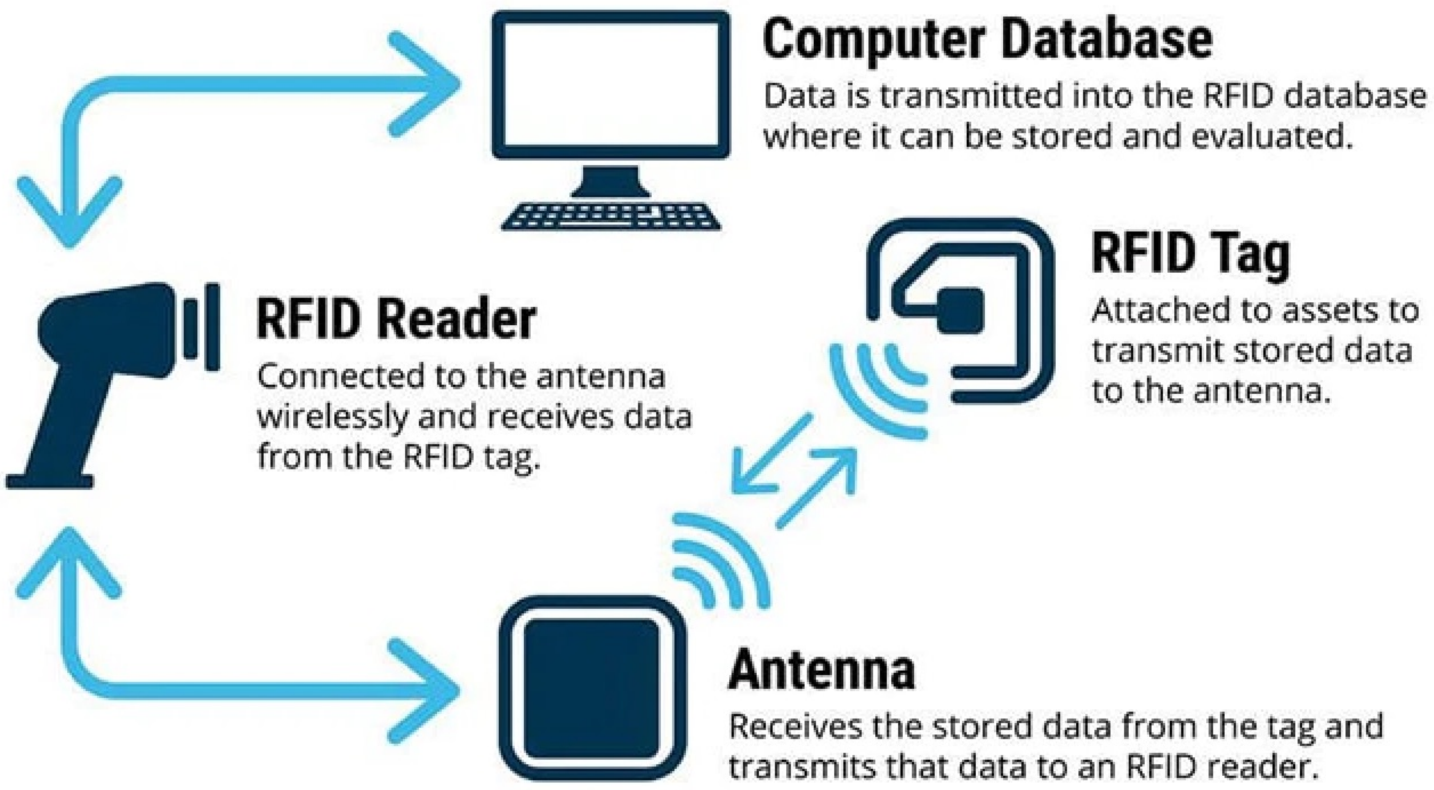
Trackers

- Medication refill reminder technology
- Drug effectiveness tracking

IOT Healthcare Methods

- Radio Frequency
- Cloud Computing
- Edge Computing
- Semantics
- Big Data
- Grid Computing
- Augmented Reality

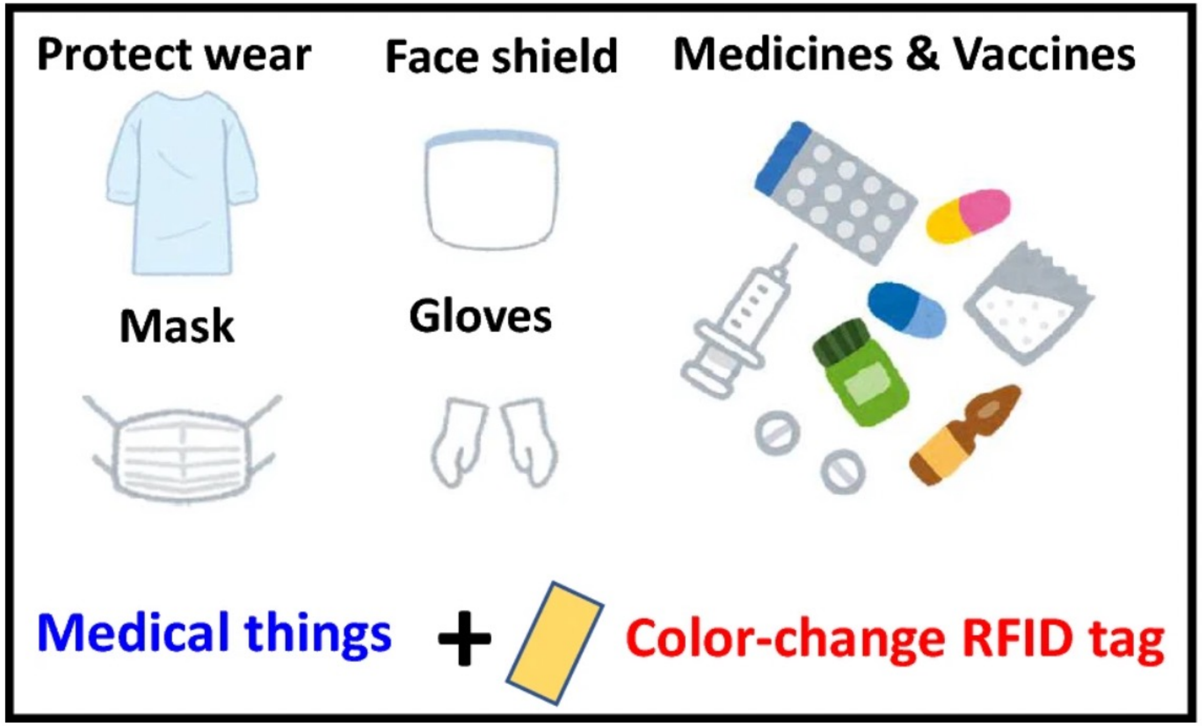
Radio Frequency Identification



- **Active RFID.** An active RFID tag has its own power source, often a battery.
- **Passive RFID.** A passive RFID tag receives its power from the reading antenna.
- The RFID reader is **a network-connected device that can be portable or permanently attached**. It uses radio waves to transmit signals that activate the tag.

RFID in Healthcare

- In healthcare, RFID technology allows the moving of medical equipment with **passive RFID** tags. Real-time location system (RTLS) enables real-time tracking of tagged objects and helps to create a system of connected devices that dynamically track and report any status change about their location, conditions, and amount.
- The RFID reader is installed in places such as medicine storerooms, check-up rooms, and sickrooms
- The color of the specific RFID tag changes as a sign of disposal, disinfection, or other treatment



Visual management of medical things using a color-change RFID tag.

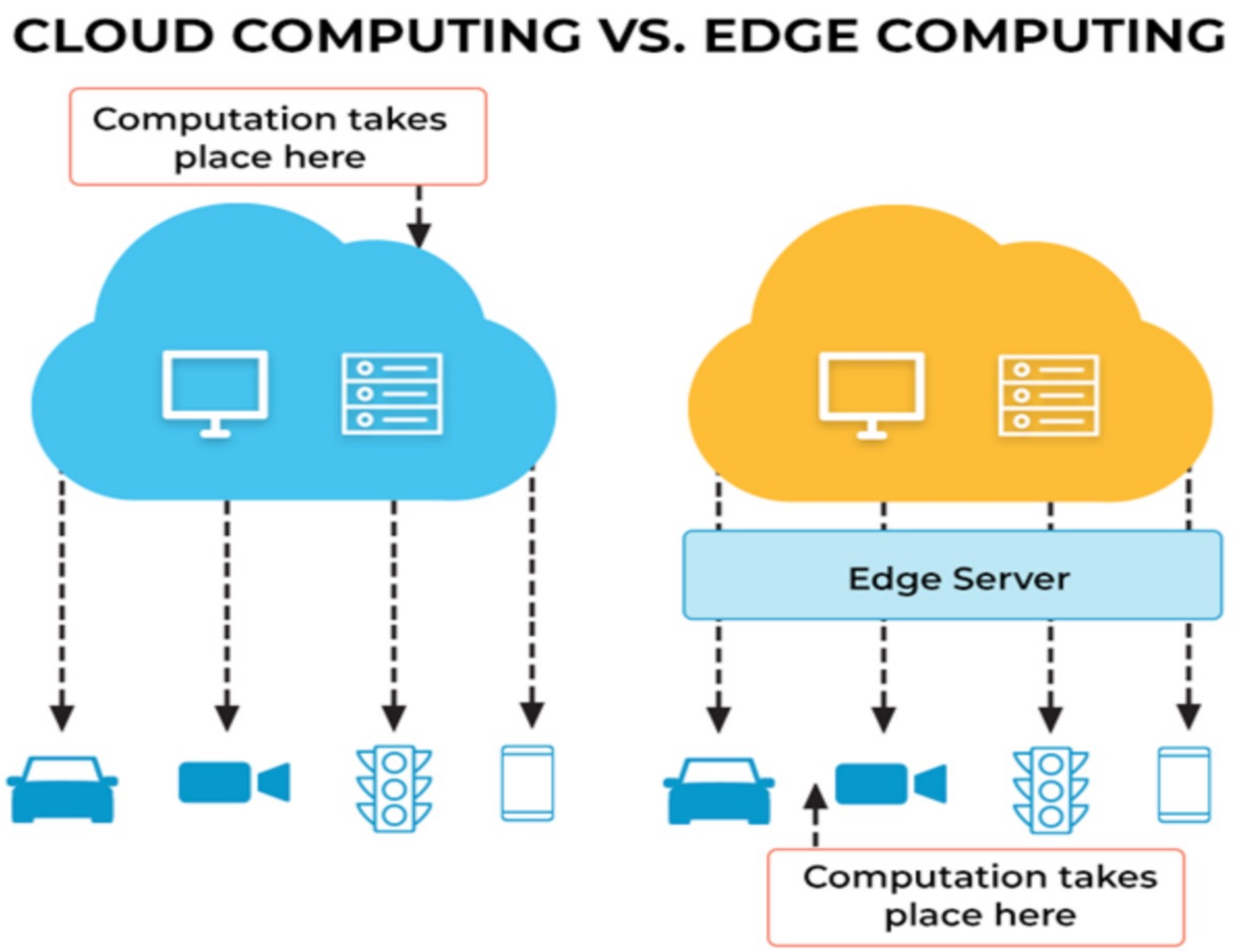
Wearables :Vests

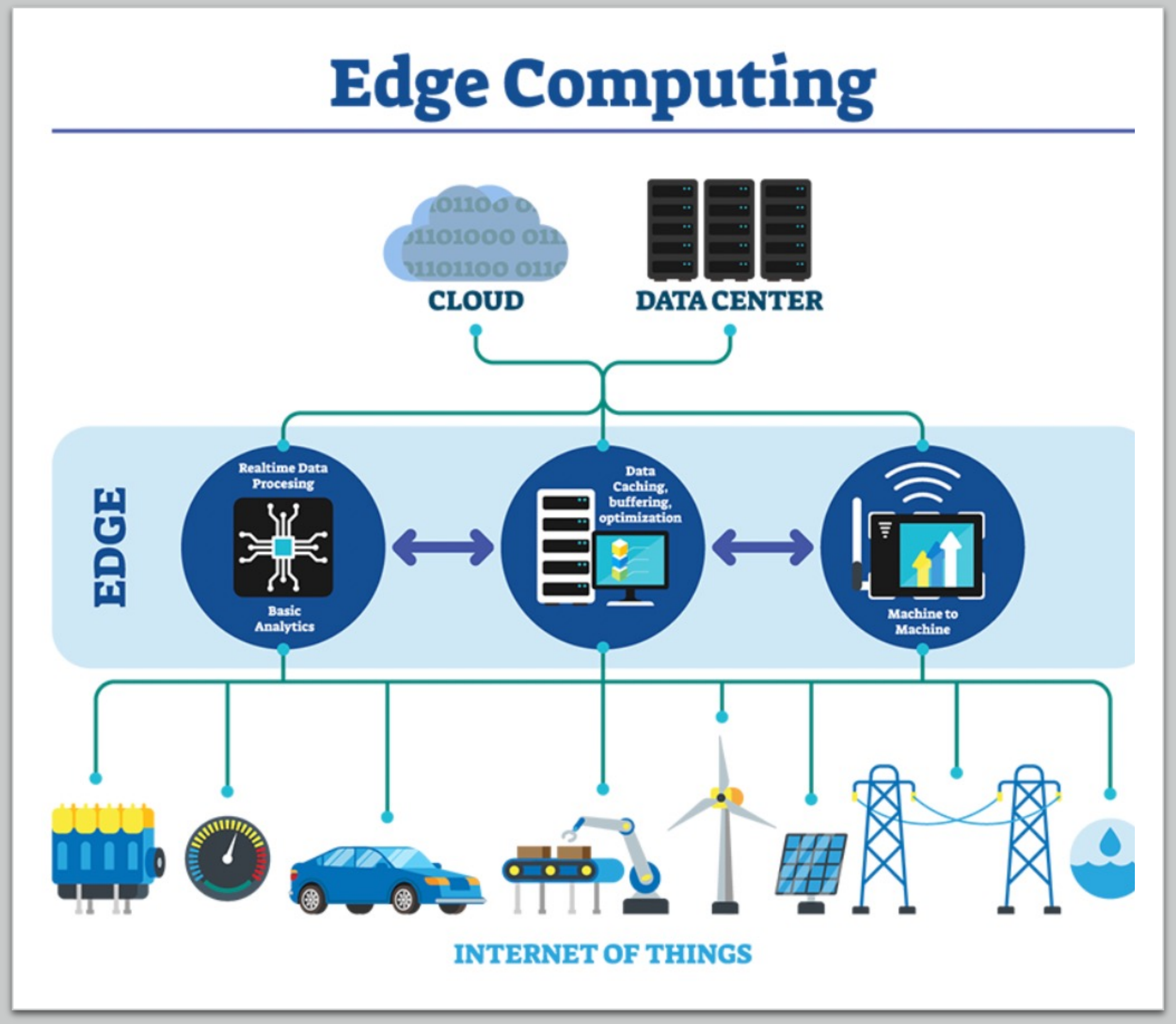
Multiple sensors working together to improve worker safety, enforcing social distancing and improving productivity

Cloud Computing in Healthcare

- Cloud computing in healthcare describes the practice of implementing remote servers accessed via the internet to **store, manage and process healthcare-related data**. This is in contrast to establishing an on-site data center with servers, or hosting the data on a personal computer.

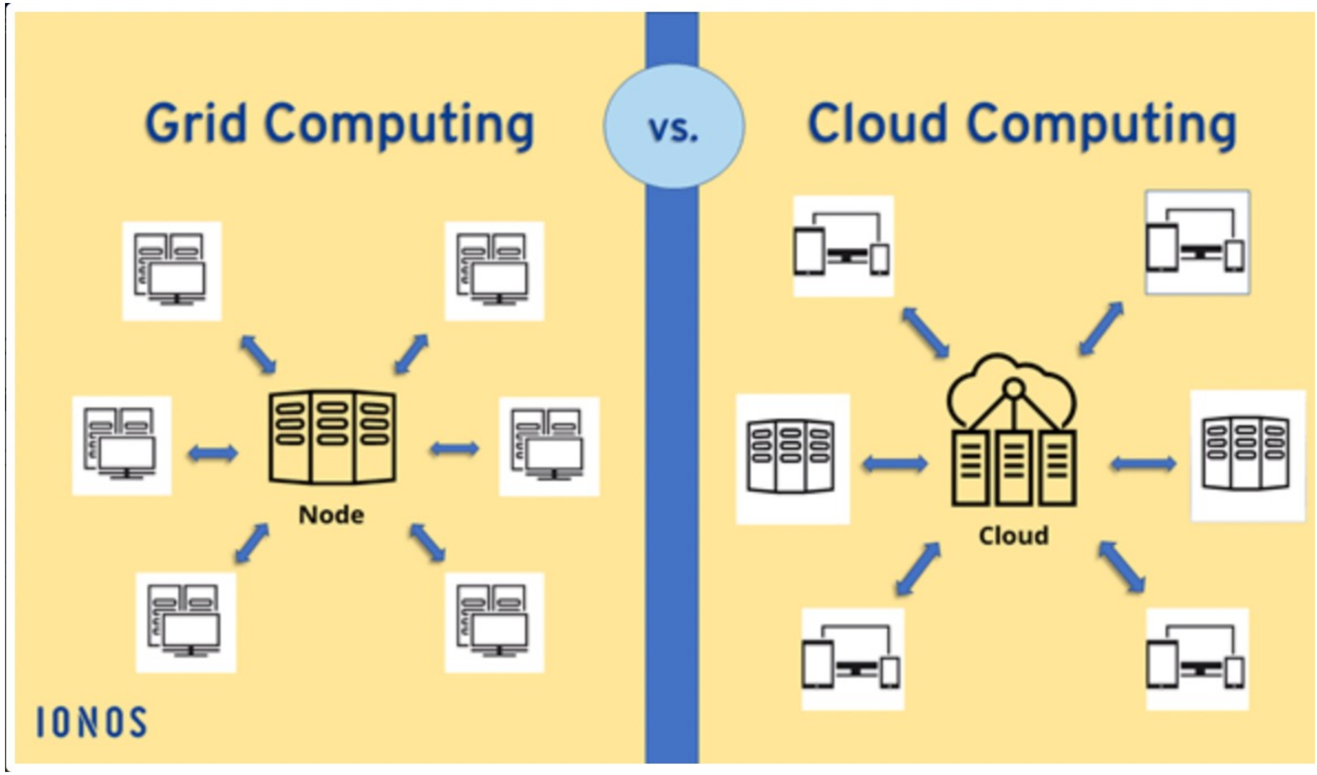
- Electronic Medical Record(EMR)
- Reduce data storage cost
- Offers superior data security
- Enhances Patient Safety
- Streamlines Collaborative Patient Care
- Medical Research
- Paves the Way for Big Data Applications


CLOUD COMPUTING VS. EDGE COMPUTING
Computation takes place here
Edge Server
Computation takes place here



- Edge computing is a distributed computing paradigm that brings computation and data storage closer to the sources of data. This is expected to improve response times and save bandwidth.
- **Healthcare Devices:** Health monitors and other wearable health care devices can keep an eye on chronic conditions for patients. It can save lives by instantly alerting caregivers when help is required.
- Robots assisting in surgery must be able to quickly analyze data in order to assist safely, quickly, and accurately. If these devices rely on transmitting data to the cloud before making decisions, the results could be fatal.

Grid Computing



- Grid computing is the use of widely distributed computer resources to reach a common goal. System **that allocates a set of computer nodes running in a cluster to jointly perform a given task.**
- A group of networked computers which work together as a virtual supercomputer to perform large tasks, such as analysing huge sets of data.

Security

Security Requirements

Security Challenges

Threat model

Attack Taxonomy

Security Requirements

- Scalability
- Communications Media
- Multiplicity of Devices
- Multiprotocol Network
- Attacks based on Information Disruption- Interruption,Confidentaility,Modification,Replay.
- Attacks based on Host properties – User,Hardware,Software compromise.

Security Requirements

- Confidentiality
- Integrity
- Authentication
- Availability
- Data Freshness
- Non Repudation
- Authorization
- Resiliency
- Fault Tolerence
- Self-Healing

Security Reqirements

- Denial-of-Service(DoS)
- Unauthorised access
- confidentiality of data
- Making trusted platforms
- Authenticity
- Data transmission control

Security Challenges

- Restriction Computation
- Memory Limitations
- Uncertanity
- Maintain the standardization
- Interaction with Internet
- Connect the scalable networks
- Integrate the data management
- Control security protocol
- Embedded devices with software
- Integrate with analyzed health data

Applications & Services

- IOT Healthcare Applications (few examples)
- Telehealth
- Tracking of information
- Drug Management
- Food Management

Applications & Services

Determination of glucose Level

Monitoring of Electrocardiogram

Monitoring of Blood pleasure

Monitoring of oxygen saturation

Challenges & Open Issues

Standardization

Security

Cost

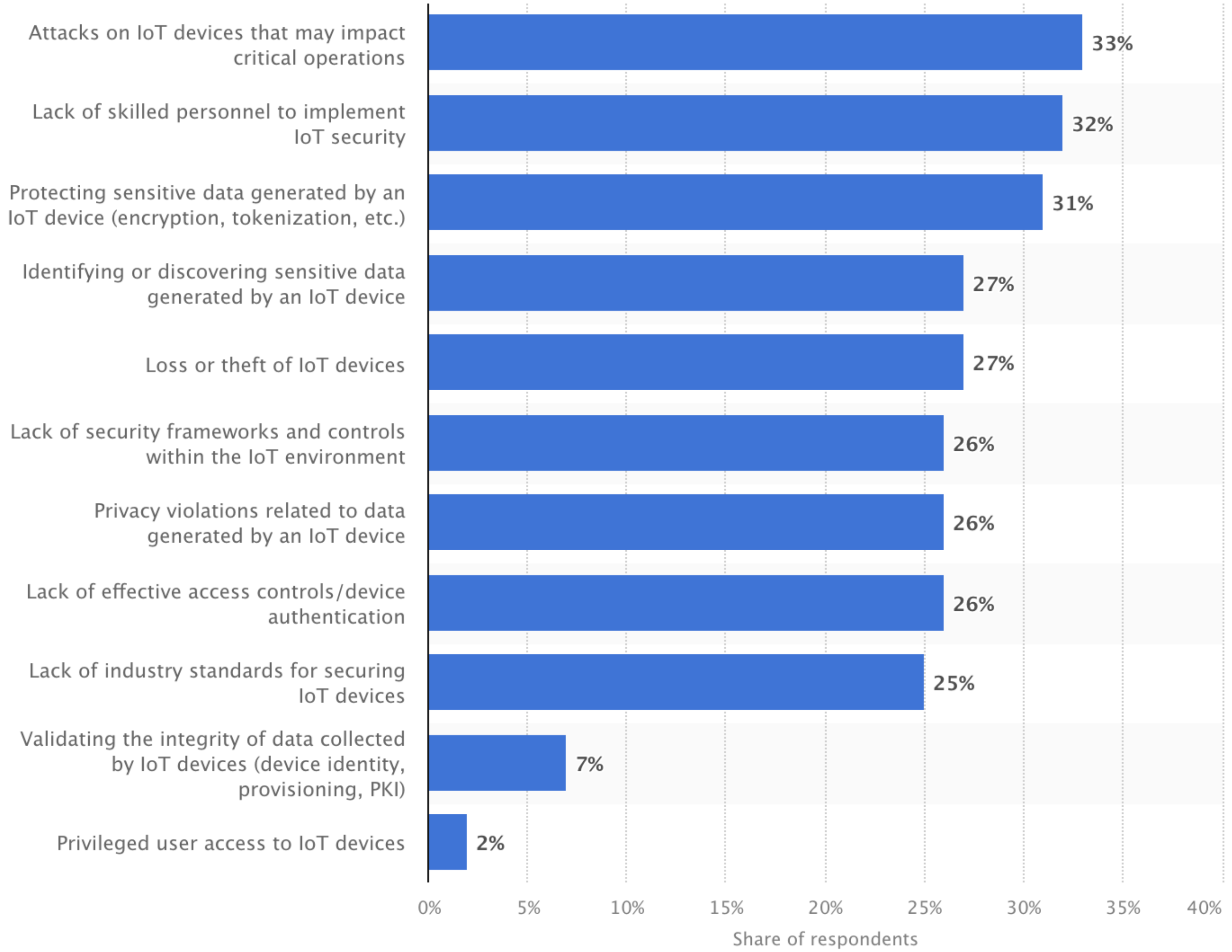
Quality of Service

Network Architecture

Technology Transition

Power Consumption

Data Protection


Attacks on IoT devices that may impact critical operations
33%
Lack of skilled personnel to implement IoT security
32%
Protecting sensitive data generated by an IoT device (encryption, tokenization, etc.)
31%
Identifying or discovering sensitive data generated by an IoT device
27%
Loss or theft of IoT devices
27%
Lack of security frameworks and controls within the IoT environment
26%
Privacy violations related to data generated by an IoT device
26%
Lack of effective access controls/device authentication
26%
Lack of industry standards for securing IoT devices
25%
Validating the integrity of data collected by IoT devices (device identity, provisioning, PKI)
7%
Privileged user access to IoT devices
2%
0%
5%
10%
15%
20%
25%
30%
35%
40%
Share of respondents

Future Scope

- We can implement light weight crypto algorithms instead of AES, DES, Hashing, RC-4.
- Less memory
- Less computing resource
- Less power supply to provide security solution that can work over resource-limited devices.

Holochain for Distributed Security in IoT Healthcare

- This article talked about blockchains and how they are an important key in the healthcare.
- Blockchains consists of blocks that contain data which the nodes themselves contain the transaction of the person.
- The issue with block chain is that it consumes to much data and memory.
- Holochain overcomes the above mentioned weakness.

Holochain

- Saves memory and time then blockchain by storing essential data in the nodes.
- Better preventing unwanted attacks.
- More efficient then block chain when it comes to large networks.
- Cheaper to maintain

Holochain

- IoT, perception layer, application layer and network layer

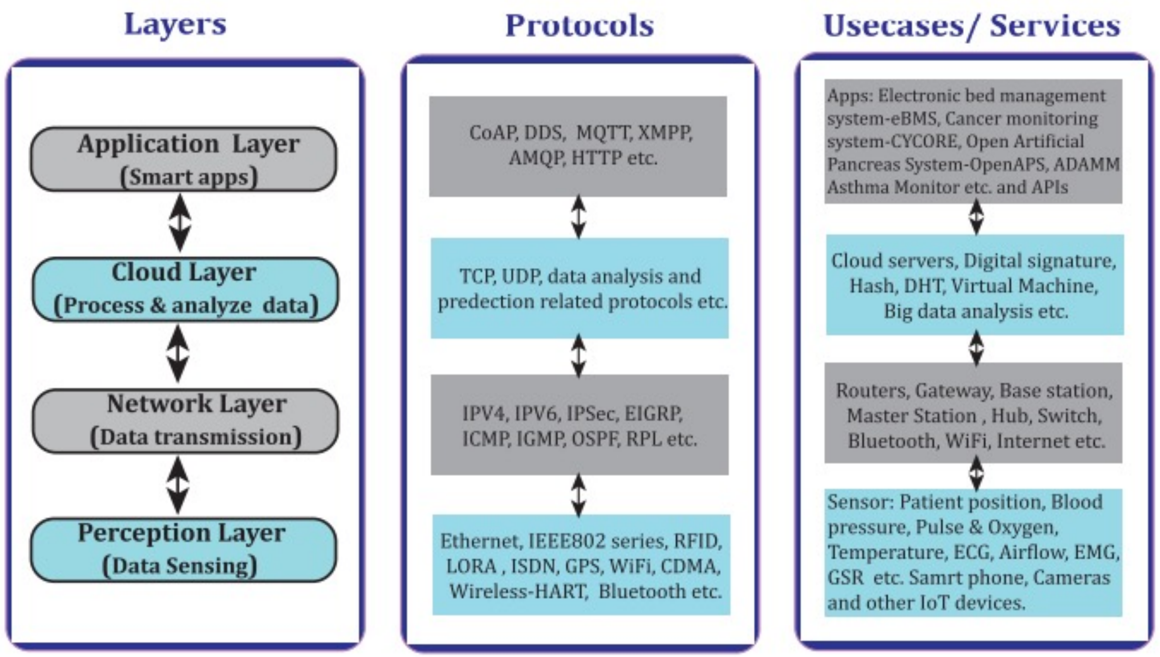


FIGURE 3. Layer-wise protocols and technologies of the IoT healthcare architecture.

Structure of Holochain

- DNA, Genesis, and Transactions
- DNA consists of the over overall structure of Holochain.

Genesis contains hash to make sure the DNA blocks follows the rules.

It also creates a happ which will have the code for it to follow.

Holochain

- Holochain, Holofuel , Hashchain, and DHT.
- Holofuel deals with online currency to support the hosts.
- Hashchain makes sures none of the data gets changed.
- DHT is a network where users can transmit information through the nodes.

Future Scope

- Holochain has many advantages over blockchains
- It can save time and resources in the healthcare system
- There are still risk such as DDos attacks, manipulating data with bad intent and MitM
- Over time Holochain will become dominant in the healthcare field.