Fondamenti di Cybersecurity

- Docente: **Jocelyne Elias**
  - Email: jocelyne.elias**@unibo.it**
  - Website: https://www.unibo.it/sitoweb/jocelyne.elias/

- Ricevimento:
  – Da concordare via mail

Piattaforma didattica

- Virtuale

  e verrà costantemente aggiornato con:
  - Informazioni
  - **Materiale didattico (slides)**
  - **Annunci**

Materiale didattico

- **Slide** caricate su Virtuale del corso
- Testi consigliati:
  - William Stallings, Lawrie Brown,
    Computer Security Principles and Practice
  - William Stallings,
    Cryptography and Network Security: Principles and Practice
  - Jean-Philippe Aumasson,
    Serious Cryptography: A Practical Introduction to Modern Encryption.
  - Bruce Schneier,
    Applied Cryptography: Protocols, Algorithms, and Source Code in C.
  - Dan Boneh, Victor Shoup,
    A Graduate Course in Applied Cryptography. (approccio matematico)

Esame

- Prova scritta
- Voto finale = Scritto + Successo laboratori
    - Scritto: 24/25 pt
    - Laboratori: max 8 pt
    - NO orali

- Date esami: consultare il sito del Dipartimento
    - **Tre** appelli nella sessione estiva (**giugno-luglio**)
    - **uno** appello nella sessione autunnale (**settembre**)
    - **due** appelli nella sessione invernale (**gennaio/febbraio 2025**)

Roadmap

❑ Introduction to Cybersecurity
❑ Cryptography
❑ Passwords and authentication
❑ Systems security
❑ Internet security
❑ Wireless security
❑ Privacy: anonymous communication, data privacy
❑ Web security?

What is Cybersecurity?

Cybersecurity refers to any technology, measure or practice for preventing **cyberattacks** or mitigating their impact. Cybersecurity aims to protect individuals' and organizations' systems, applications, computing devices, sensitive data and financial assets against simple and annoying computer viruses, sophisticated and costly ransomware attacks, and everything in between.

A **cyberattack** is any intentional effort to steal, expose, alter, disable, or destroy data, applications or other assets through unauthorized access to a network, computer system or digital device.

https://www.ibm.com/topics/cybersecurity

https://www.ibm.com/topics/cyber-attack

Cybersecurity is the practice of deploying **people, policies, processes,** and **technologies** to protect organizations, their **critical systems and sensitive information** from **digital attacks**.

https://www.gartner.com/en/topics/cybersecurity

What is a cyberattack?

https://www.gartner.com/en/topics/cybersecurity

The most common and notable types of cybersecurity attacks include:

- **Phishing and social-engineering-based attacks.**
  Attackers trick legitimate users with proper access credentials into taking action that opens the door for unauthorized users, allowing them to transfer information and data out (data exfiltration).
- **Internet-facing service risks (including cloud services).**
  These threats relate to the failure of enterprises, partners and vendors to adequately secure cloud services or other internet-facing services (for example, configuration management failure) from known threats.
- **Password-related account compromises.**
  Unauthorized users deploy software or other hacking techniques to identify common and reused passwords they can exploit to gain access to confidential systems, data or assets.

The most common and notable types of cybersecurity attacks include:

- **Misuse of information.**
  Authorized users inadvertently or deliberately disseminate or otherwise misuse information or data to which they have legitimate access.

- **Network-related and man-in-the-middle attacks.**
  Attackers may be able to eavesdrop on unsecured network traffic or redirect or interrupt traffic as a result of failure to encrypt messages within and outside an organization’s firewall.

- **Supply chain attacks.**
  Partners, vendors or other third-party assets or systems (or code) become compromised, creating a vector to attack or exfiltrate information from enterprise systems.

Supply chain attacks

- ❑ ARS Tecnica, 16 February 2021 “New type of supply-chain attack hits Apple, Microsoft and 33 other companies”
- ❑ Last week, a researcher demonstrated a new supply-chain attack that executed counterfeit code on networks belonging to some of the biggest companies on the planet, Apple, Microsoft, and Tesla included
- ❑ The so-called *dependency confusion* or *namespace confusion* attack starts by placing malicious code in an official public repository such as NPM (JavaScript), PyPI (Python), or RubyGems. By giving the submissions the same package name as dependencies used by companies such as Apple, Microsoft, Tesla, and 33 other companies, Birsan was able to get these companies to automatically download and install the counterfeit code
- ❑ …

The most common and notable types of cybersecurity attacks include:

- **Denial-of-service attacks (DoS).**
  Attackers **overwhelm** enterprise systems and cause a temporary shutdown or slowdown. Distributed DoS (DDoS) attacks also flood systems, but by using a network of devices.
  - Thousands of DDoS attacks are now reported each day, and cyber attackers are capable of increasing the scope of the attack - DDoS attacks continue to rise in complexity, volume and frequency. This presents a growing threat to the network security of even the smallest enterprises.

- **Ransomware.**
  This malicious software infects an organization’s systems and restricts access to encrypted data or systems <u>until a ransom is paid</u> to the perpetrator. Some attackers threaten to release data if the ransom isn’t paid.

ARPANET

- 1969 – ARPANET comes online
- 1973 – Robert Metcalfe warns that ARPANET is insecure
  - High-school kids are poking around on the network
- 1983 – Fred Cohen invents the term computer **virus**
- 1983 – ARPANET adopts TCP/IP

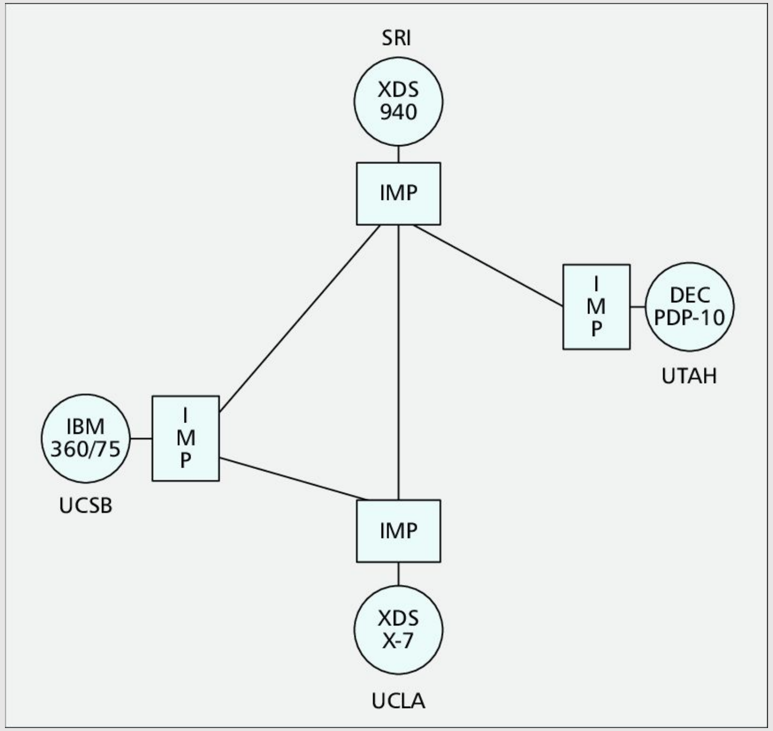


Figure of the ARPA Network (4 nodes) Dec. 1969, updated/uploaded by L. Kleinrock

First computer virus

- 1988 – Robert Morris (a 23-year-old Ph.D. student at Cornell University) inadvertently releases the first worm
  - Leveraged a bug in sendmail to remotely exploit vulnerable servers
  - Copied itself to the server
- Released as a research experiment
  - A bug in Robert's code caused the program to replicate out of control
- Crashed 10% of the computers on the ARPANET
- Morris was convicted under the CFAA (the Computer Fraud and Abuse Act), 3 years probation
- + $10k fine
- First documented use of a buffer overflow exploit

Cyber systems

Cybersecurity does not concern the security of individual computers but that of Cyber Systems

Cyber Systems integrate:

- computers,
- communications, and
- people (as users and as operators)

Additional definitions (1 / 2)

- **Vulnerability**: A weakness that can be exploited to cause damage
- **Attack**: A method of exploiting a vulnerability
- **Threat**: A motivated, capable adversary that mounts an attack

Strategies:

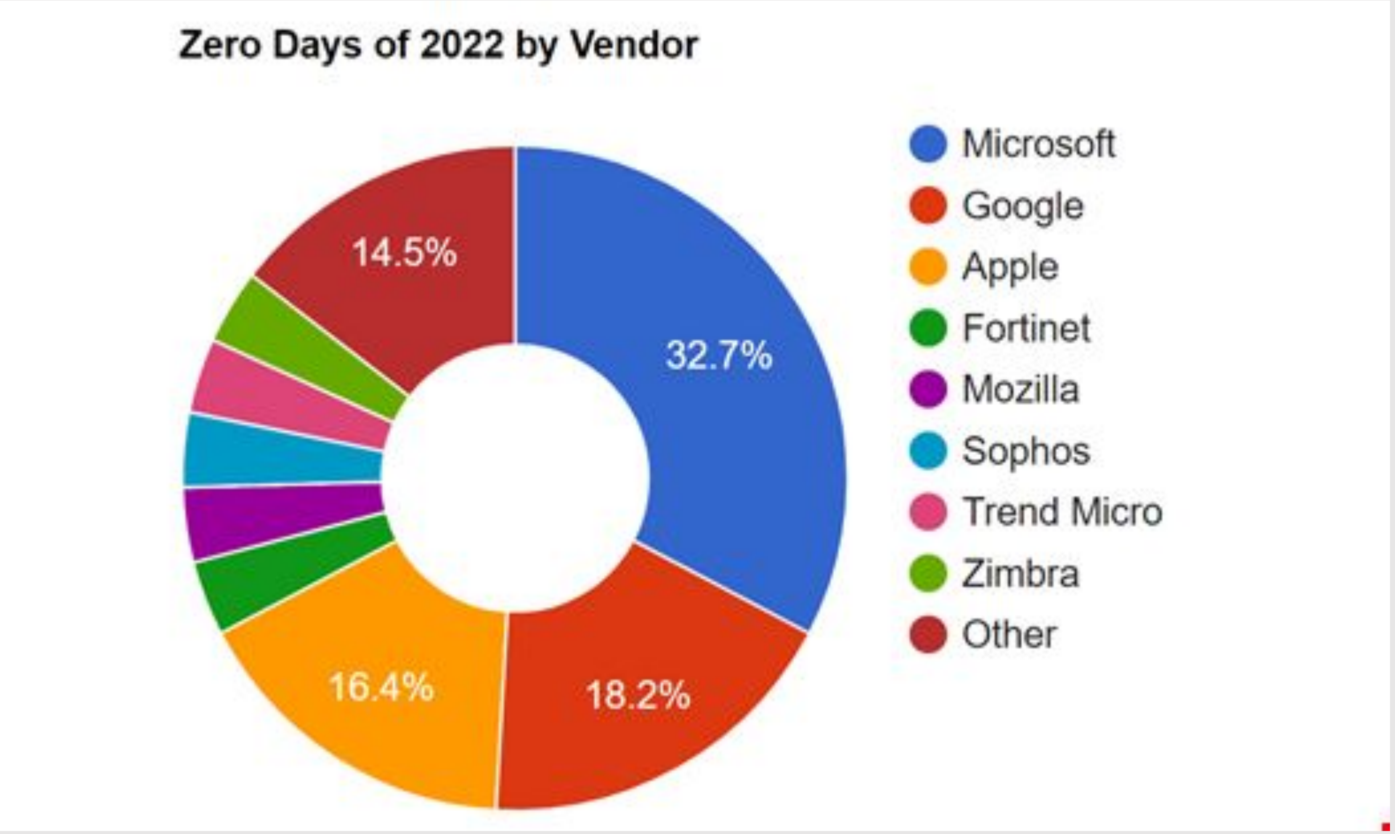
- Identify and fix each vulnerability (usually due to bugs)
- Identify attacks and eliminate those vulnerabilities that those attacks exploit

Additional definitions (2 / 2) - ZERO DAY

- ❑ **Zero-day vulnerability**: A vulnerability that is unknown to those who should be interested in mitigating it
- ❑ **Window of Opportunity**: Time from when a software exploit first becomes active to the time when a patch is released by the affected vendor and applied to the affected system
- ❑ **Zero-day attack**: an attack that occurs during the window of opportunity
- ❑ In 2005, the average length of a window of opportunity was 54 days
- ❑ In 2014, the average length of a window of opportunity had grown to almost 12 months

Where Do Zero-Day Vulnerabilities Come From?

The Big Tech companies, which develop nearly all the operating systems used worldwide (Windows, Android, iOS and MacOS) are generally the leading ‘purveyors’ of zero-day vulnerabilities – unintentionally, of course …



Source: https://www.infosecurity-magazine.com/news-features/guide-zero-day-vulnerabilities/

Zero-Day Exploit Examples (2023)

The 10 Worst Attacks Ever (more details at https://softwarelab.org/blog/zero-day-exploit-examples/):

- **Code Red Worm** (2001): Exploited a buffer overflow vulnerability in Microsoft's Internet Information Services (IIS) web server.
- **Heartbleed** (2014): This bug affected the OpenSSL cryptography library, which is widely used in the transport layer security protocol.
- **Shellshock** (2014): A vulnerability in the Unix Bash shell that was often used for remote code execution.
- **Petya/NotPetya** (2017): Ransomware that exploited a vulnerability in Microsoft's Windows operating system, which was initially exposed by the EternalBlue exploit.
- **WannaCry** (2017): This ransomware also exploited the same vulnerability in Microsoft's Windows operating system as Petya/NotPetya.

Example of **IoT cybersecurity**

Internet of Things (IoT) Cybersecurity Research: A Review of Current Research Topics, Yang Lu, and Li Da Xu, IEEE Internet of Things Journal, vol.6, no. 2, April 2019.

https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8462745

…..

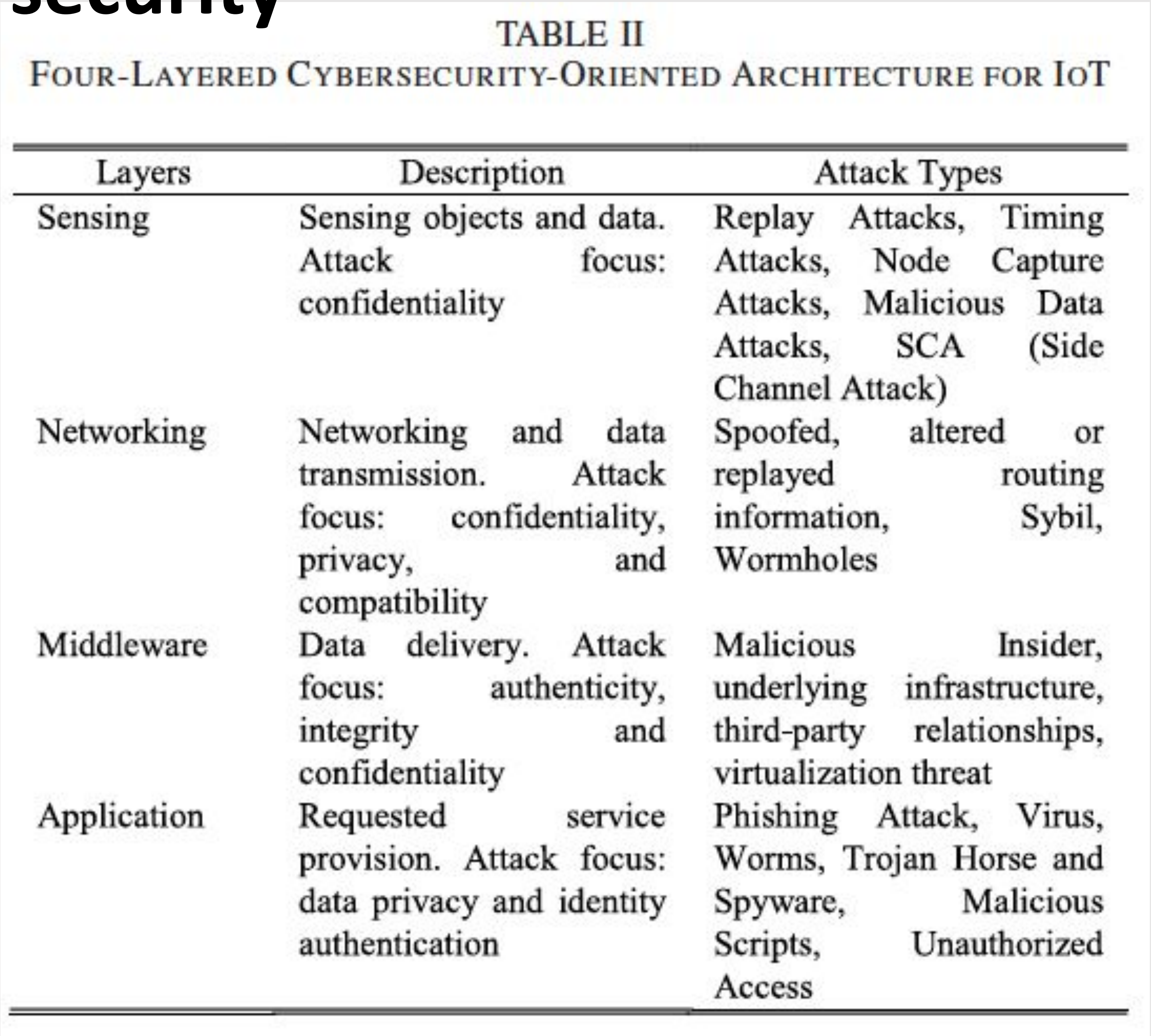
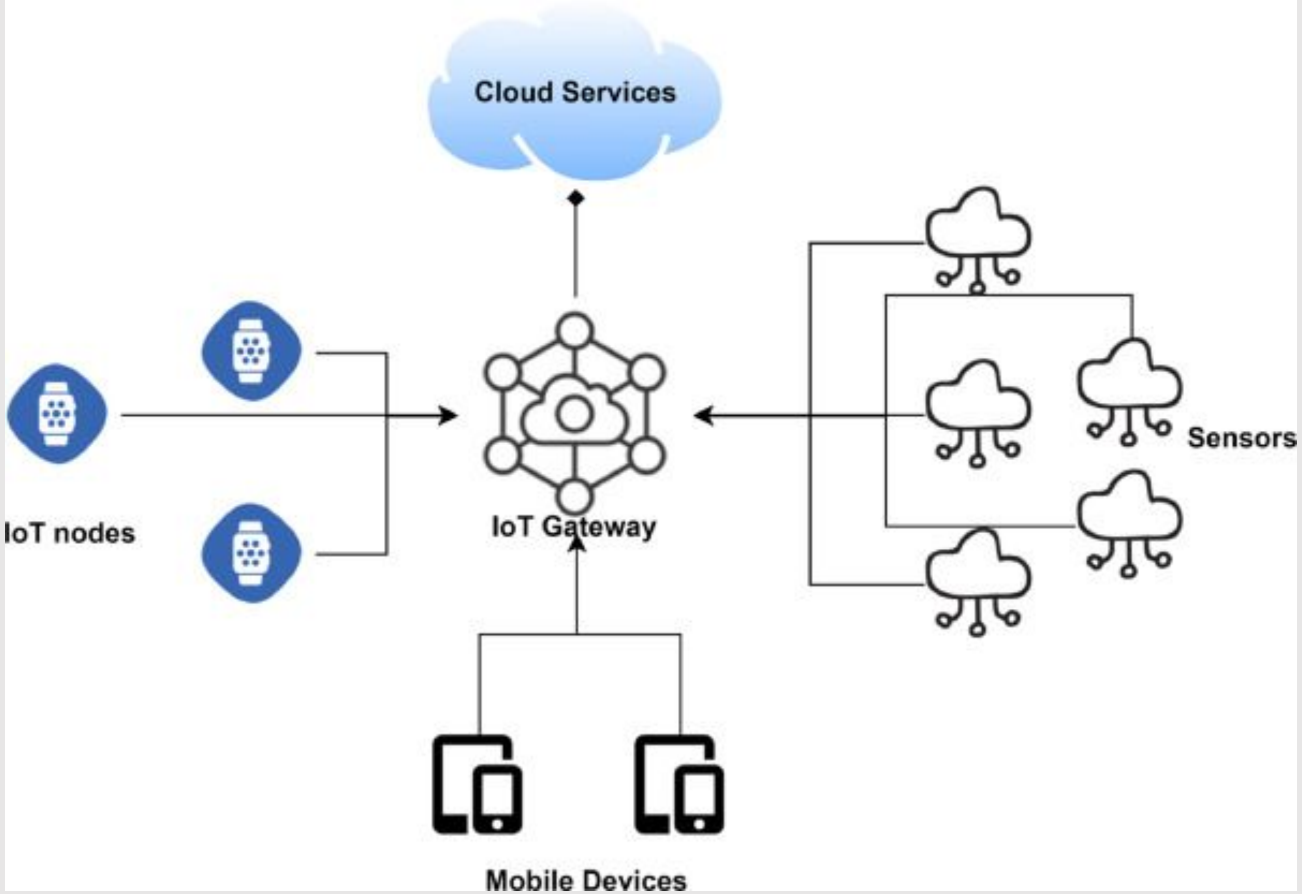


TABLE II
FOUR-LAYERED CYBERSECURITY-ORIENTED ARCHITECTURE FOR IOT

Layers	Description	Attack Types
Sensing	Sensing objects and data. Attack focus: confidentiality	Replay Attacks, Timing Attacks, Node Capture Attacks, Malicious Data Attacks, SCA (Side Channel Attack)
Networking	Networking and data transmission. Attack focus: confidentiality, privacy, and compatibility	Spoofed, altered or replayed routing information, Sybil, Wormholes
Middleware	Data delivery. Attack focus: authenticity, integrity and confidentiality	Malicious Insider, underlying infrastructure, third-party relationships, virtualization threat
Application	Requested service provision. Attack focus: data privacy and identity authentication	Phishing Attack, Virus, Worms, Trojan Horse and Spyware, Malicious Scripts, Unauthorized Access

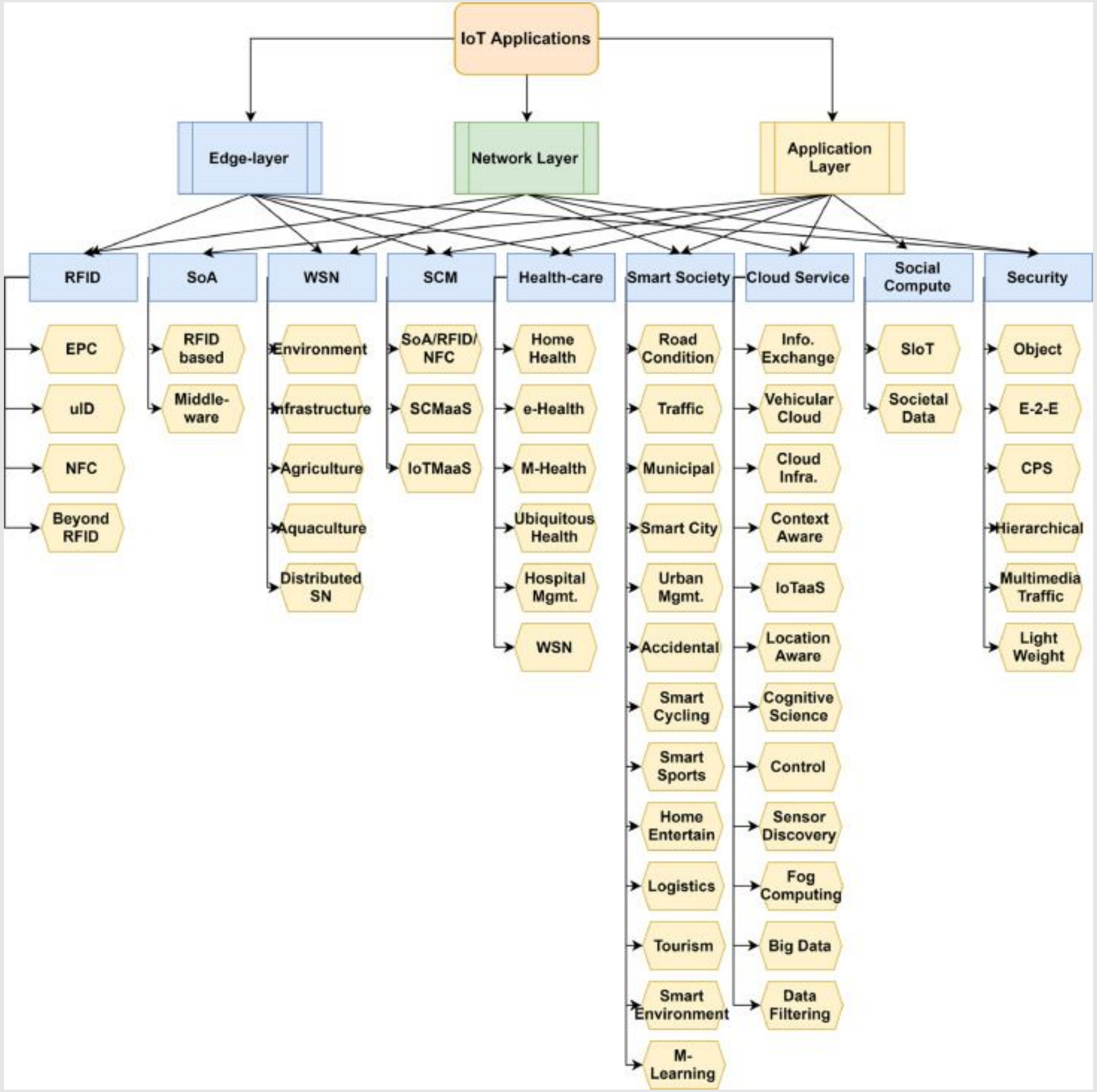
Edge (device) layer components in IoT Architecture



<u>Source:</u> H. HaddadPajouh, A. Dehghantanha, R. M. Parizi, M. Aledhari, H. Karimipour, ***A survey on internet of things security: Requirements, challenges, and solutions***, journal of Internet of Things, Vol. 14, June 2021.

https://www.sciencedirect.com/science/article/pii/S2542660519302288

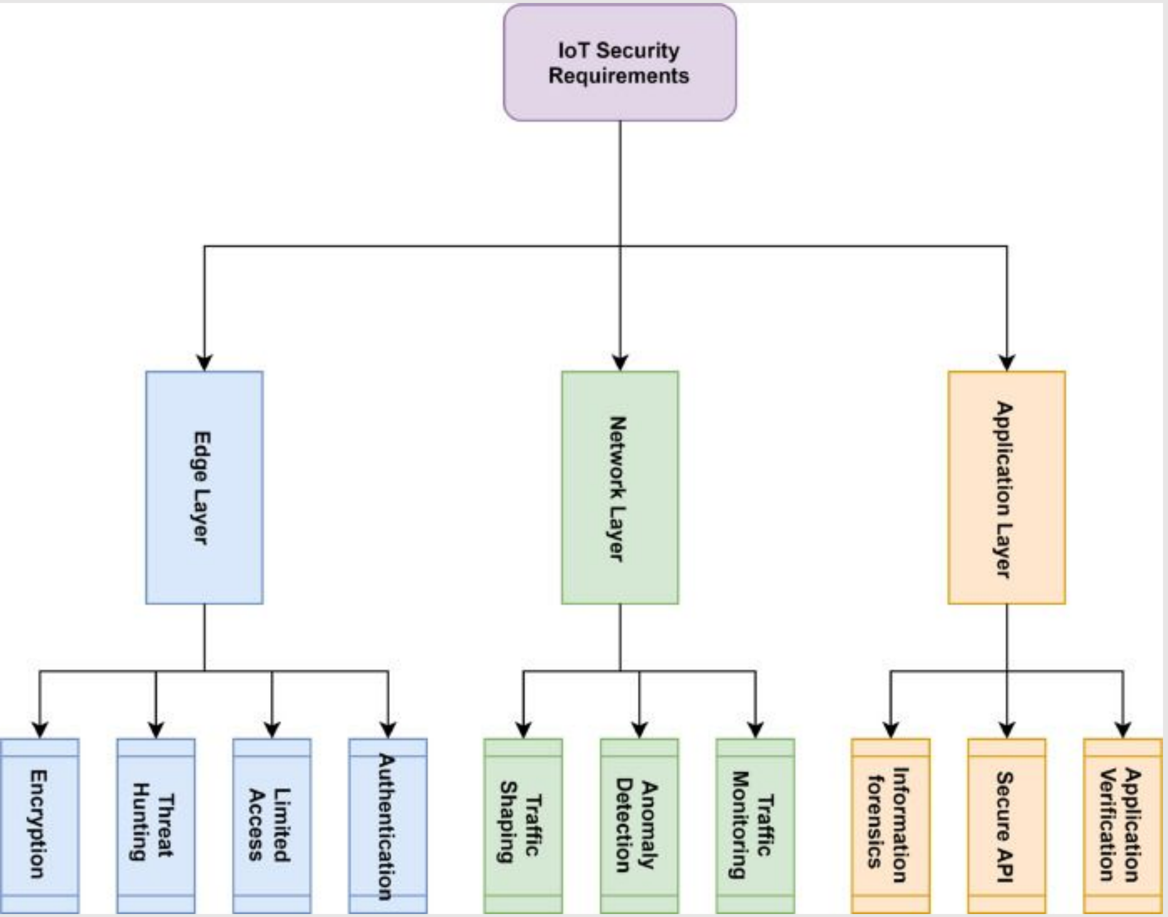
IoT Applications Taxonomy based on domain applications

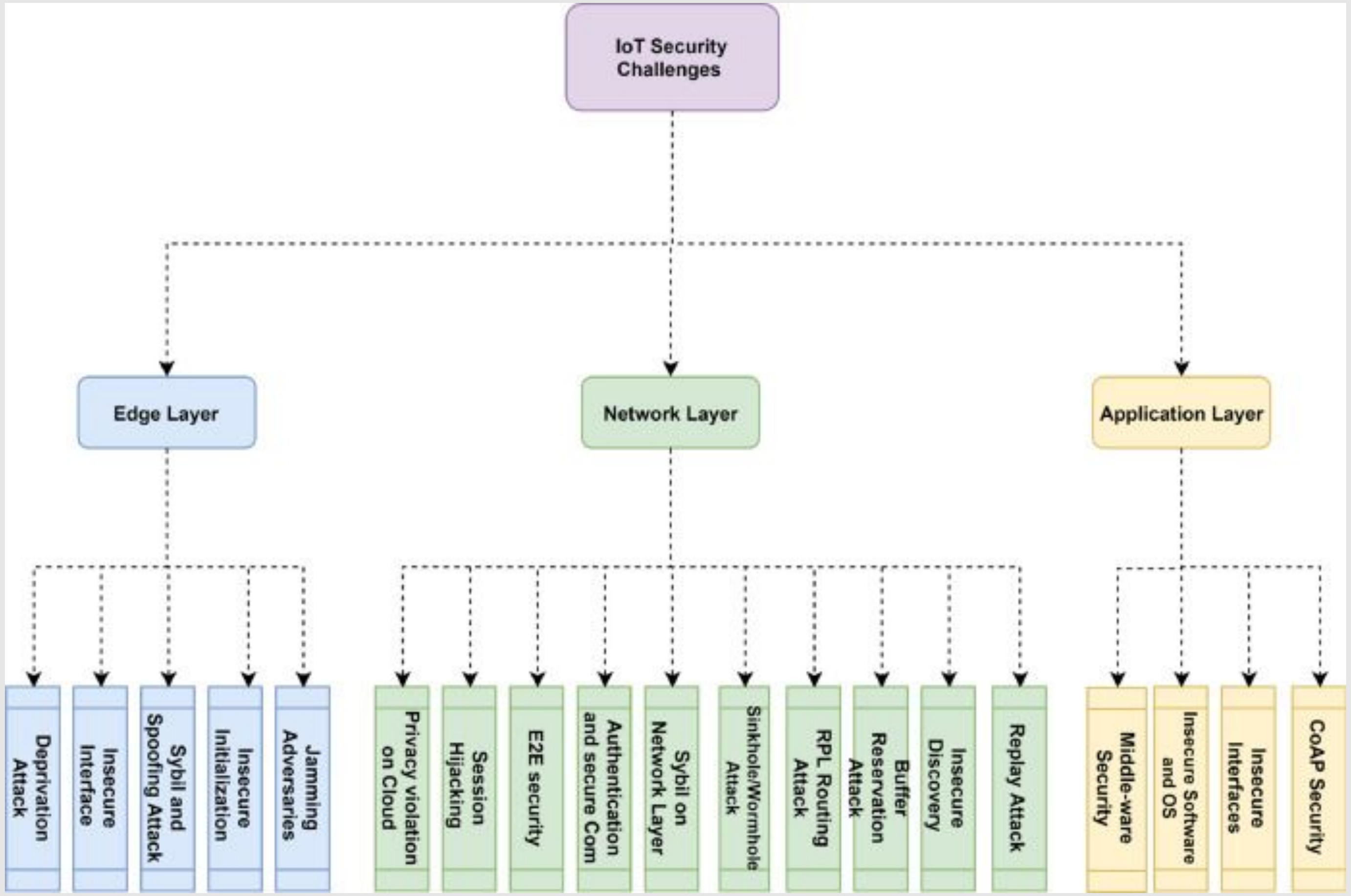


Source: H. HaddadPajouh, A. Dehghantanha, R. M. Parizi, M. Aledhari, H. Karimipour, ***A survey on internet of things security: Requirements, challenges, and solutions***, journal of Internet of Things, Vol. 14, June 2021.

https://www.sciencedirect.com/science/article/pii/S2542660519302288

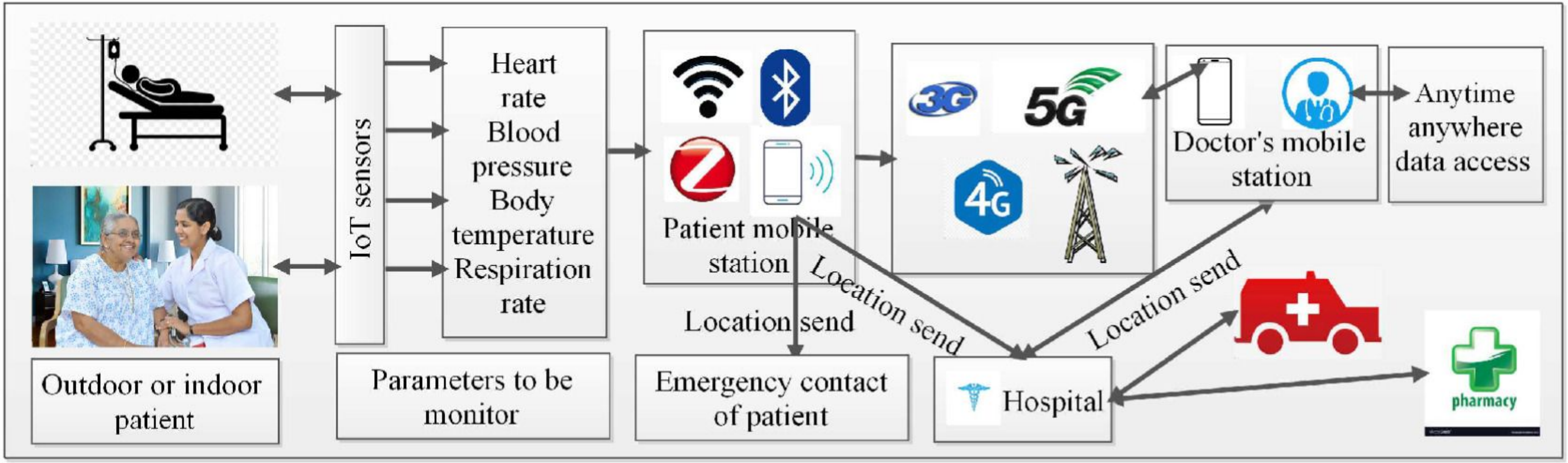
IoT security requirements/challenges taxonomy based on layered architecture





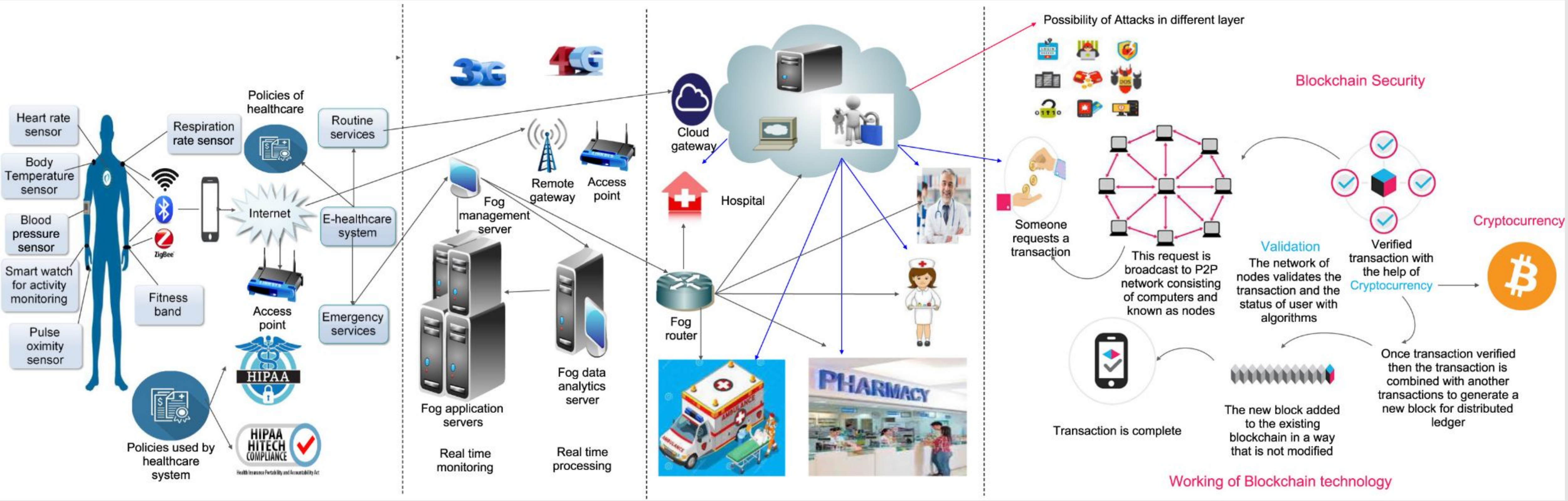
<u>Source:</u> H. HaddadPajouh, A. Dehghantanha, R. M. Parizi, M. Aledhari, H. Karimipour, ***A survey on internet of things security: Requirements, challenges, and solutions***, journal of Internet of Things, Vol. 14, June 2021.
https://www.sciencedirect.com/science/article/pii/S2542660519302288

Mobile based data exchange between caregivers in **Healthcare 4.0**



<u>**Source:**</u> Jigna J. Hathaliya, Sudeep Tanwar, ***An exhaustive survey on security and privacy issues in Healthcare 4.0***, Elsevier Computer Communications journal, vol. 153, March 2020.

Security and privacy issues in Healthcare 4.0


Heart rate sensor
Body Temperature sensor
Blood pressure sensor
Smart watch for activity monitoring
Pulse oximity sensor
Respiration rate sensor
Fitness band
ZigBee
Policies of healthcare
Internet
Access point
HIPAA
Policies used by healthcare system
HIPAA HITECH COMPLIANCE
Routine services
E-healthcare system
Emergency services
3G
4G
Remote gateway
Access point
Fog management server
Fog application servers
Fog data analytics server
Real time monitoring
Real time processing
Cloud gateway
Hospital
Fog router
PHARMACY
AMBULANCE
Possibility of Attacks in different layer
Blockchain Security
Someone requests a transaction
This request is broadcast to P2P network consisting of computers and known as nodes
Validation
The network of nodes validates the transaction and the status of user with algorithms
Verified transaction with the help of Cryptocurrency
Cryptocurrency
Once transaction verified then the transaction is combined with another transactions to generate a new block for distributed ledger
The new block added to the existing blockchain in a way that is not modified
Transaction is complete
Working of Blockchain technology

Source: Jigna J. Hathaliya, Sudeep Tanwar, ***An exhaustive survey on security and privacy issues in Healthcare 4.0***, Elsevier Computer Communications journal, vol. 153, March 2020.