An Overview on IoT Security

Presented by
Shailendra Rathore
(rathoreshailendra@seoultech.ac.kr)

What is Internet of Things (IoT)

Past IoT Architecture

Present IoT Architecture

Future IoT Architecture
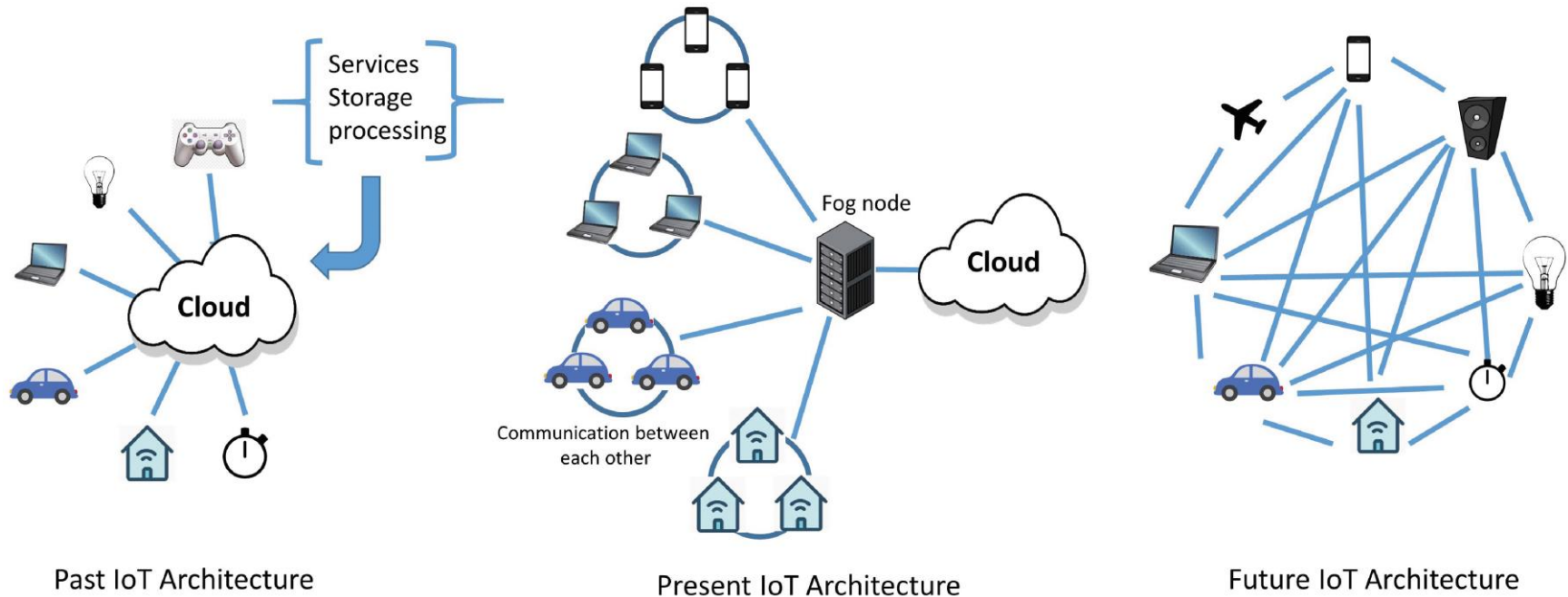
Why IoT Security

➢ Mirai attack in the last quarter of 2016 was estimated to infect around 2.5 million devices connected to the Internet and launch distributed denial of service (DDoS) attack [5].

➢ Mirai, Hajime and Reaper are the other big botnet attacks.

➢ Being low powered and less secure, provide a gateway to the adversaries for entering into home and corporate networks, thereby giving easy access to the user's data.

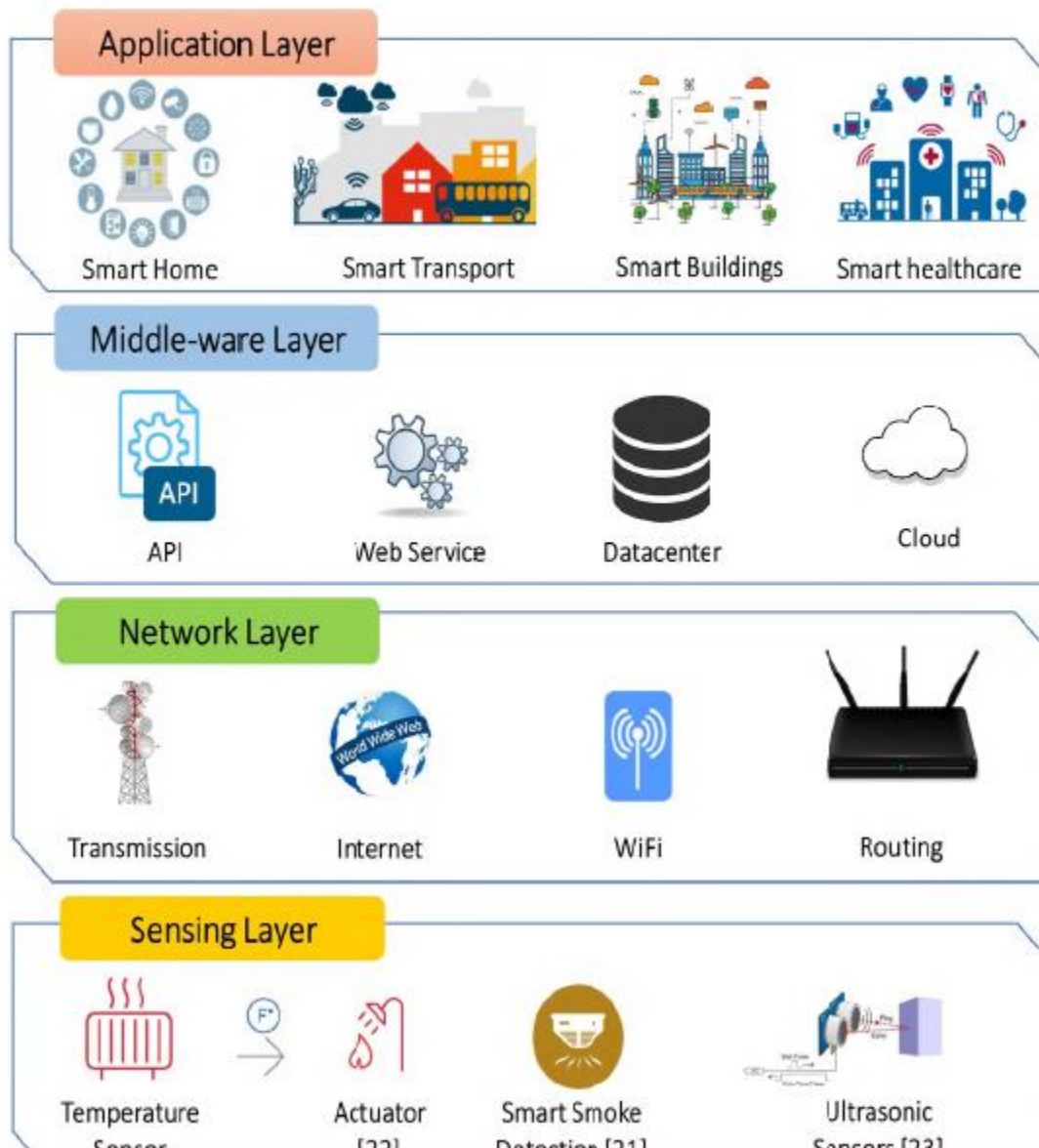➢ Implant IoT devices into the human body, particular individual or falsify data.

SeoulTech UCS Lab
Ubiquitous Computing & Security Laboratory

Why IoT Security

Widespread IT Security	IoT security
Widespread IT has devices which is resource rich	IoT devices need to be carefully provisioned with security measures
Widespread IT is based on resource rich devices	IoT system are composed of devices having limitation in terms of their software and hardware
For wide security and lower capabilities complex algorithm are implemented	only lightweight algorithms are preferred
Homogeneous technology is responsible for high security	IoT with heterogeneous technology produce large amount of heterogeneous data increasing the attack surface

SeoulTech UCS Lab
Ubiquitous Computing & Security Laboratory
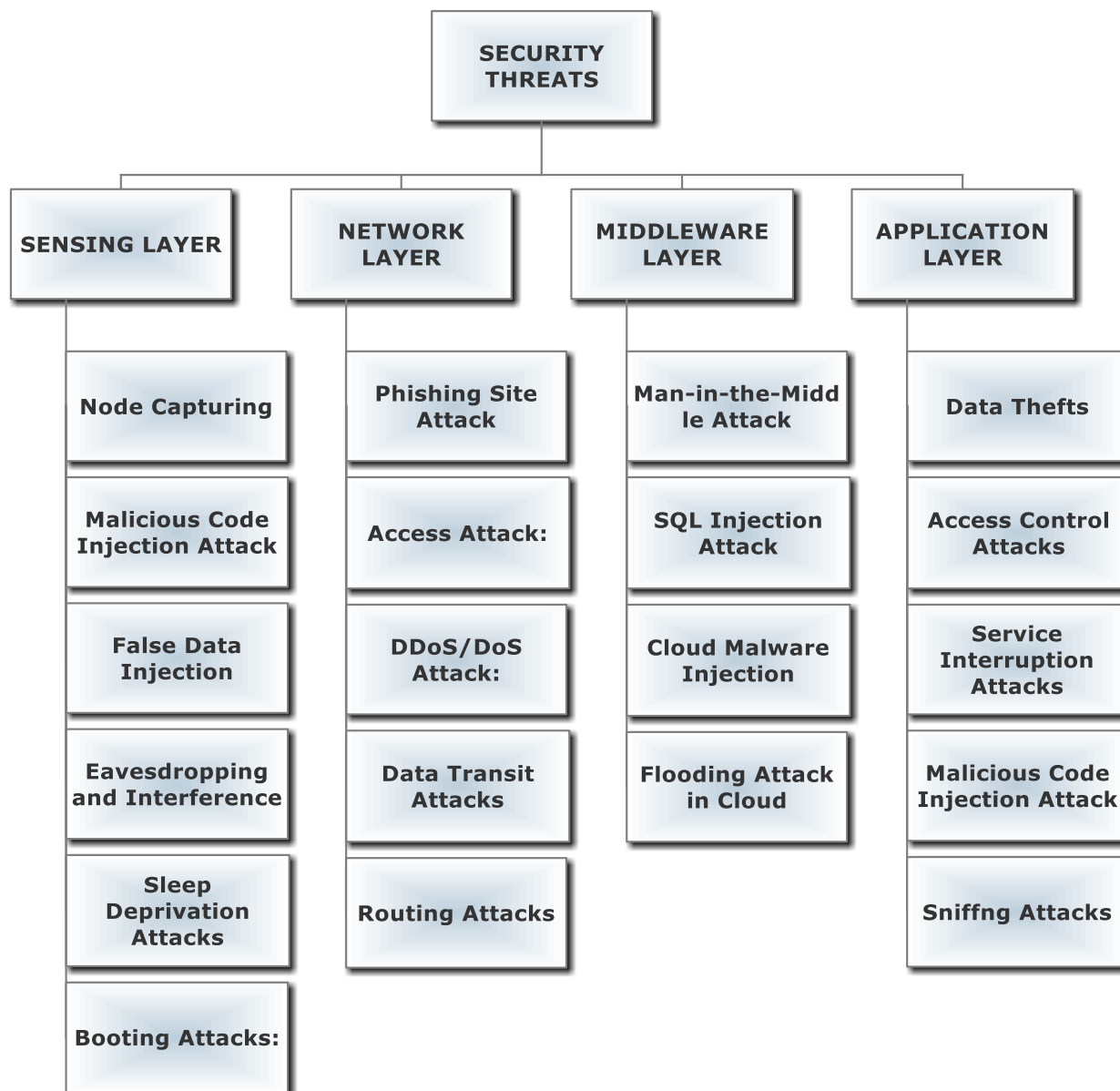
Various Security Critical IoT Applications

- **Smart Cities:** Smart card services, Smart mobility applications.

- **Smart Environment:** Fire detection, early detection of earthquakes, pollution monitoring.

- **Smart Metering and Smart Grids:** the electricity consumption is measured and monitored, monitoring of water, oil and gas levels in storage tanks and cisterns.

- **Security and Emergencies**

- **Smart Retail**

- **Smart Agriculture and Animal Farming**

- **Home Automation**
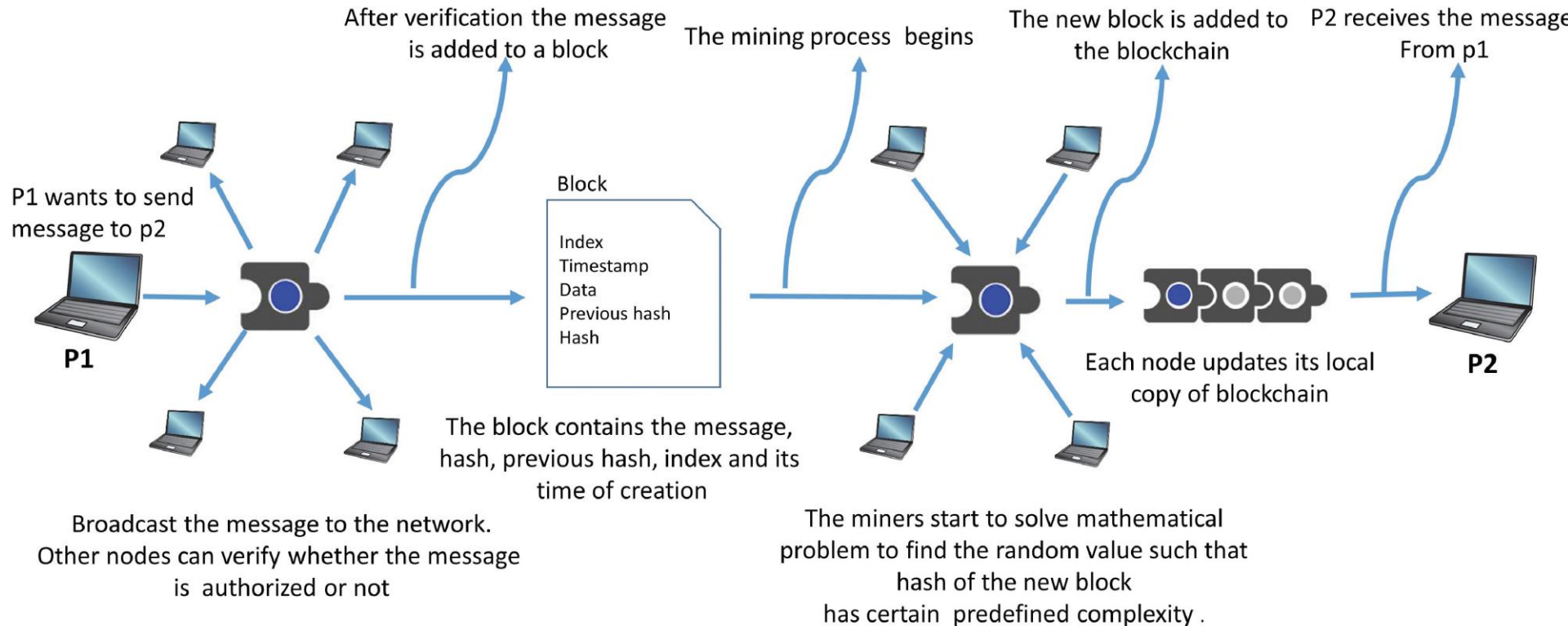
Sources of Security Threats in IoT Applications

Sources of Security Threats in IoT Applications

```
                              SECURITY
                              THREATS

     SENSING LAYER      NETWORK        MIDDLEWARE      APPLICATION
                        LAYER          LAYER           LAYER

     Node Capturing     Phishing Site  Man-in-the-Midd  Data Thefts
                        Attack         le Attack

     Malicious Code     Access Attack: SQL Injection   Access Control
     Injection Attack                  Attack          Attacks

     False Data         DDoS/DoS       Cloud Malware   Service
     Injection          Attack:        Injection       Interruption
                                                       Attacks

     Eavesdropping      Data Transit   Flooding Attack Malicious Code
     and Interference   Attacks        in Cloud        Injection Attack

     Sleep              Routing Attacks                 Sniffng Attacks
     Deprivation
     Attacks

     Booting Attacks:
```

7

IoT Security using Blockchain

➤ The IoT devices provide real-time data from sensors and blockchain provides the key for data security using a distributed, decentralized and shared ledger.

After verification the message is added to a block

The mining process begins

The new block is added to the blockchain

P2 receives the message From p1

P1 wants to send message to p2

Block

Index
Timestamp
Data
Previous hash
Hash

P1

P2

Each node updates its local copy of blockchain

The block contains the message, hash, previous hash, index and its time of creation

Broadcast the message to the network. Other nodes can verify whether the message is authorized or not

The miners start to solve mathematical problem to find the random value such that hash of the new block has certain predefined complexity .

IoT Security using Fog Computing

➢ The data generated by IoT devices locally for better management.

➢ Decentralized infrastructure for analysis of data and computing.

➢ Can be used to store and process time-sensitive data efficiently and quickly.

➢ Goal is to enhance security, prevent data thefts, minimize the data stored on the cloud and to increase the overall efficiency of IoT applications.

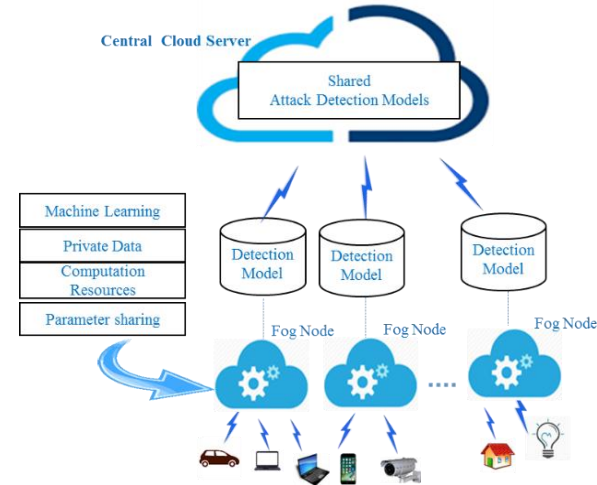➢ The latency in fog computation is less than cloud computation.

Advantages of Fog Computing for IoT Security

- ➢ Man-in-the-middle attack

- ➢ Data transit attacks

- ➢ Eavesdropping

- ➢ Resource-constraint issues
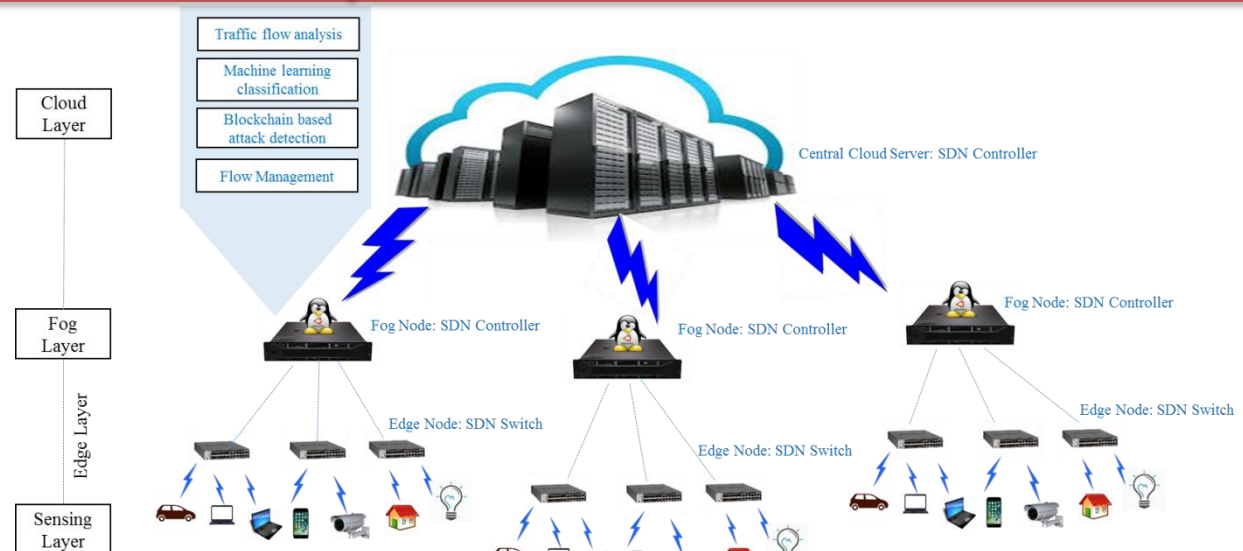
- ➢ Incident response services
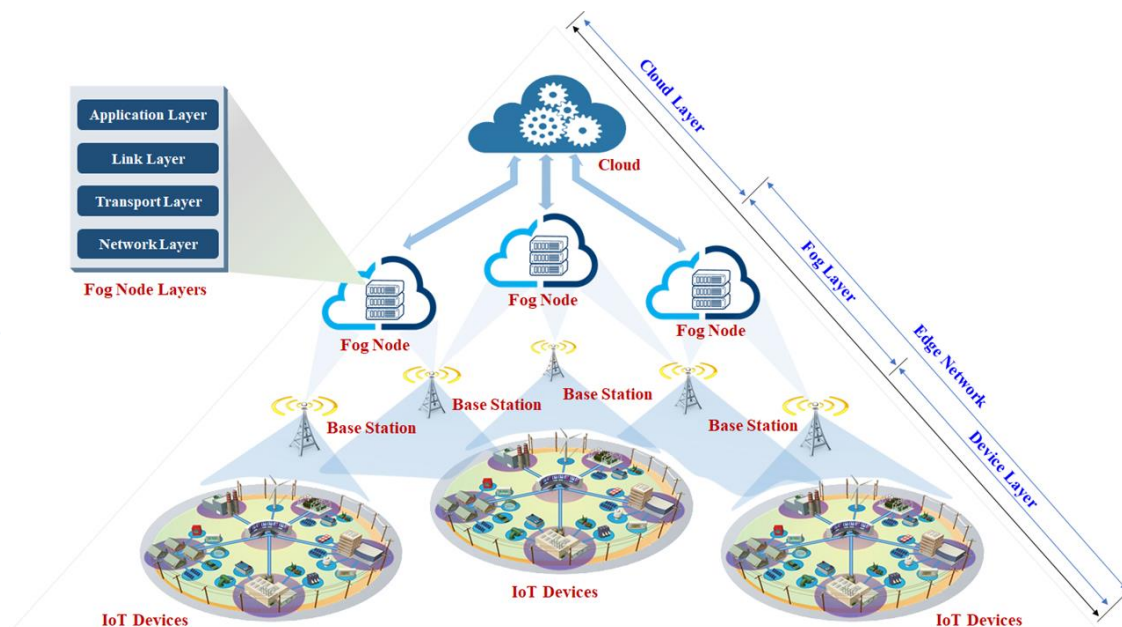
IoT Security using Machine Learning
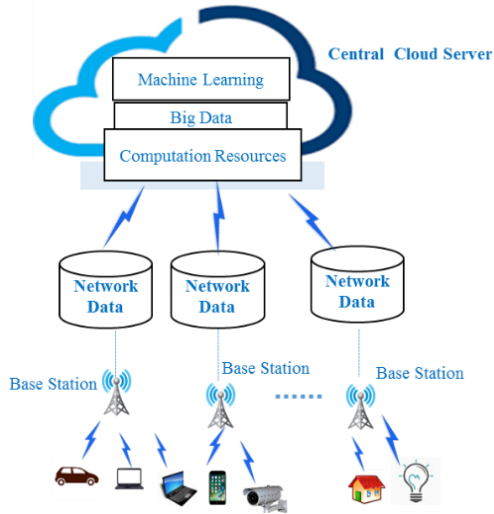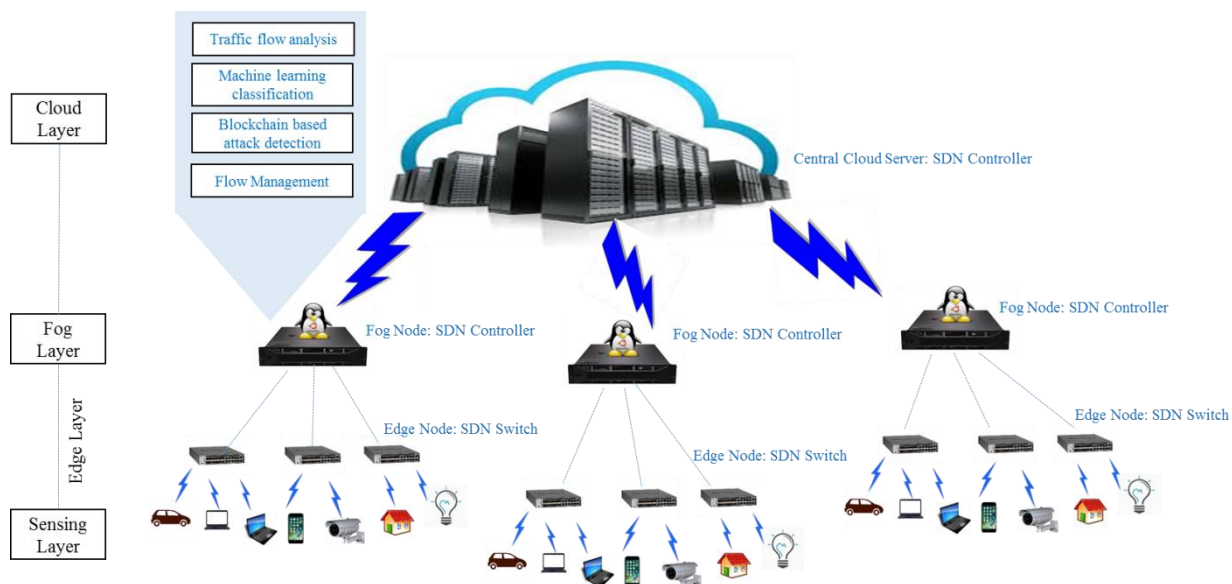

(a) Centralized machine learning architecture

(b) Distributed machine learning architecture

Blockchain-Based Decentralized Security Architecture for IoT Network

SeoulTech UCS Lab
Ubiquitous Computing & Security Laboratory

12

Benefits of Machine Learning for IoT Security

➢ DoS Attack

➢ Eavesdropping

➢ Spoofing

➢ Privacy Leakage

➢ Incident response services

IoT Security using Edge Computing

> The main difference between cloud, fog and edge computing is the location of intelligence and power computation.

> The computation and analysis power is provided at the edge itself.

> Low communication cost.
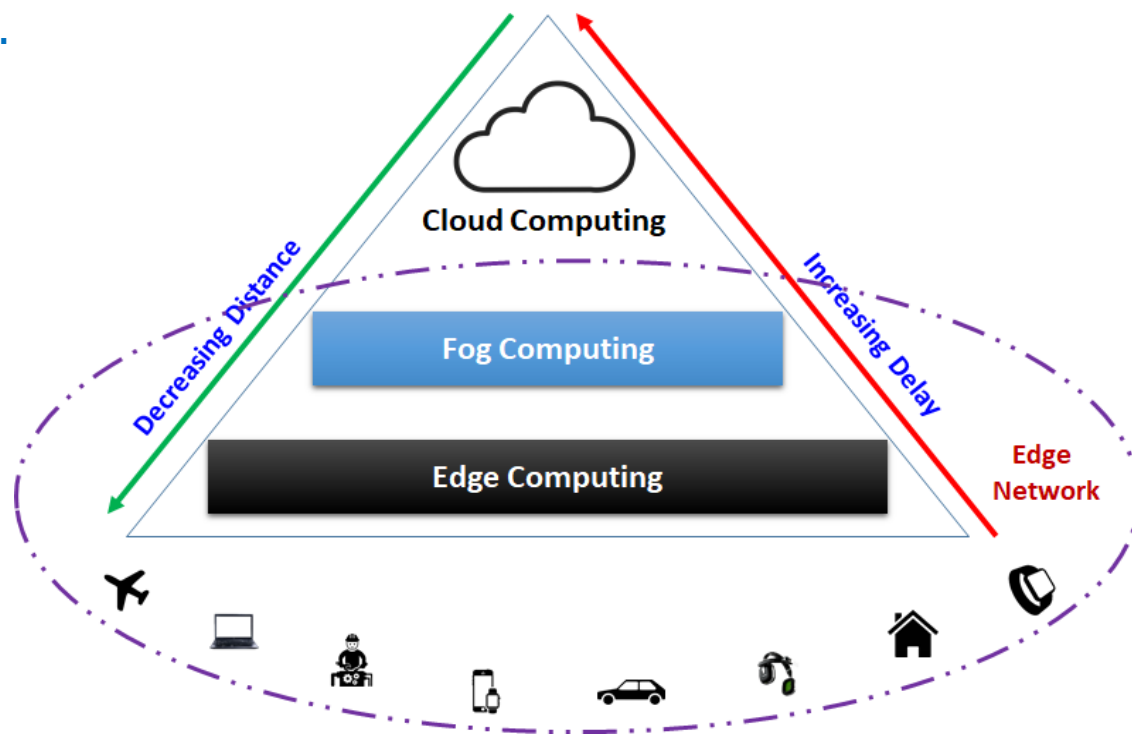
IoT Security and Edge Computing

- ➢ Data Breaches

- ➢ Data Compliance Issues

- ➢ Safety Issues

- ➢ Bandwidth Issues
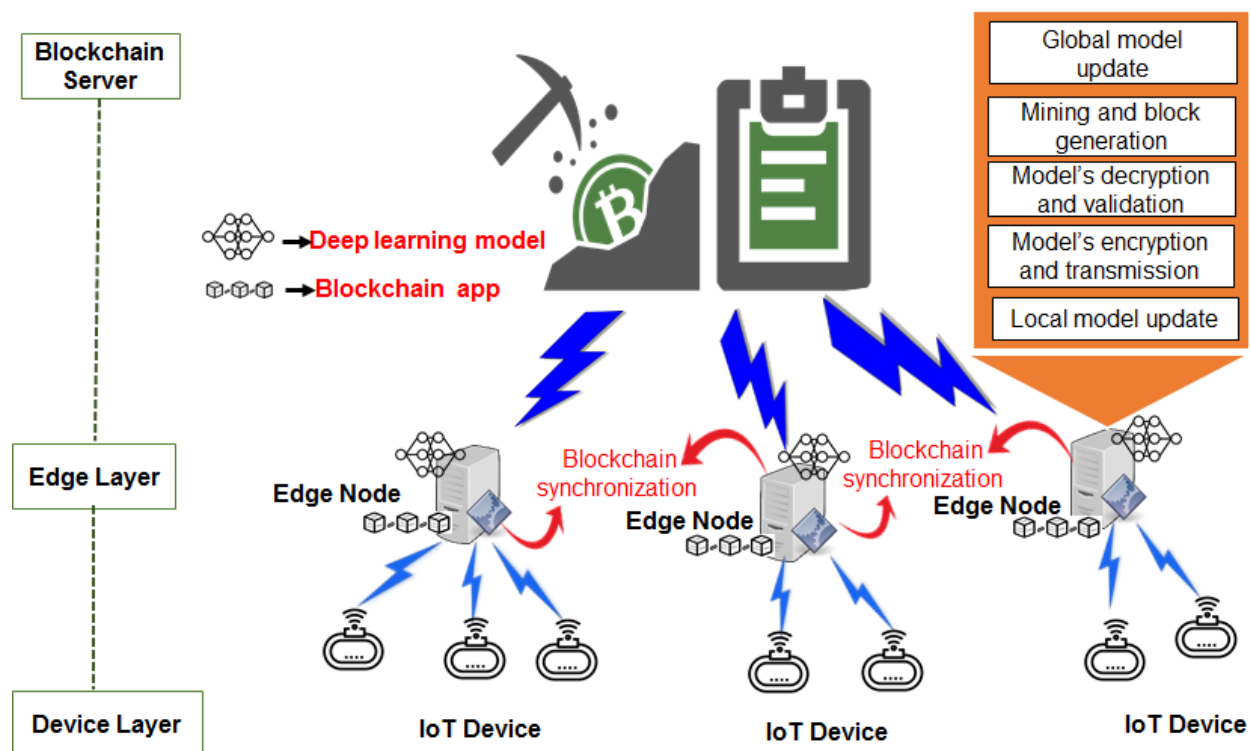
Open Research Challenges

- ➢ Scalability and availability of blockchain.

- ➢ Security and privacy continue to persist in fog computing.

- ➢ Select a proper machine learning algorithm and data set.

- ➢ Data security and user privacy.

Conclusion

➢   Provided an overview of IoT Security.

➢   Motivation behind IoT security.

➢   Studied Various security threats in IoT.

➢   Possible emerging technology for IoT security.

➢   Recent research challenges.

Reference

Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., & Sikdar, B. (2019). A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures. IEEE Access, 7, 82721-82743.