IoT Device Identification

By

Dr Sandhya Aneja
Faculty of Integrated Technologies
Universiti Brunei Darussalam (UBD)

One Week Online AICTE Sponsored Short Term Training Programme
on
Internet of Things (IoT): Challenges and Applications

Outlines

- Internet of Things (IoT)
- IoT Network Architecture
- IoT Applications
- Challenges in IoT Networks
- IoT Device Identification
- Conclusion

Internet of Things (IoT)

In 1999, the Auto-ID center first introduced the term Internet of Things (IoT), which had envisioned to identify every physical world object with a globally unique identifier using RFID tag, and interact with an individual object over the Internet.

IoT has been expanding gradually and incorporating heterogeneous technologies, objects, applications and communication protocols to connect the physical world with the digital world.

IoT is the technological revolution after the Internet.

Internet of Things (IoT)

Three crucial characteristics of IoT devices: sensing ability, connectivity, and exchange data.

IETF defines IoT:

“The Internet of Things is the network of physical objects or "things" embedded with electronics, software, sensors, actuators, and connectivity to enable objects to exchange data with the manufacturer, operator and/or other connected devices.”

IoT Network Architecture

An architecture consists of different layers of technological advancement to establish a multi-layer network.

Different types of IoT network architectural frameworks have been proposed based on distinct research perspectives:

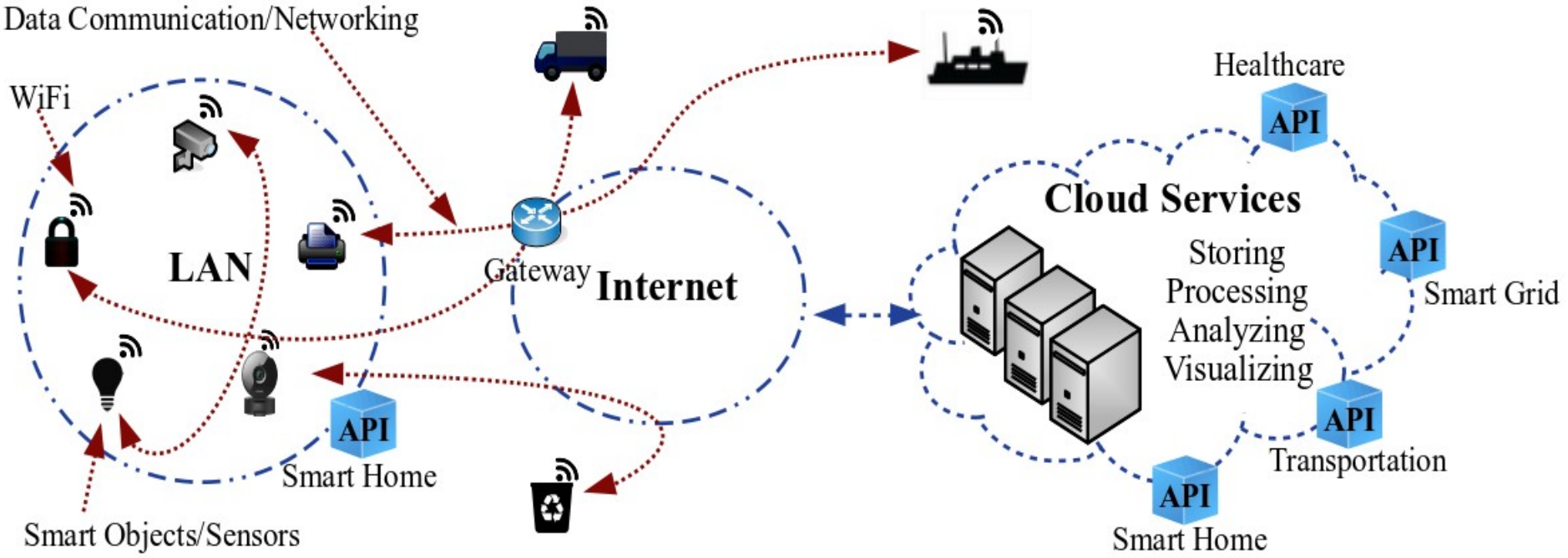
* Three layer

* Four layer

* Five layer

IoT Network Architecture

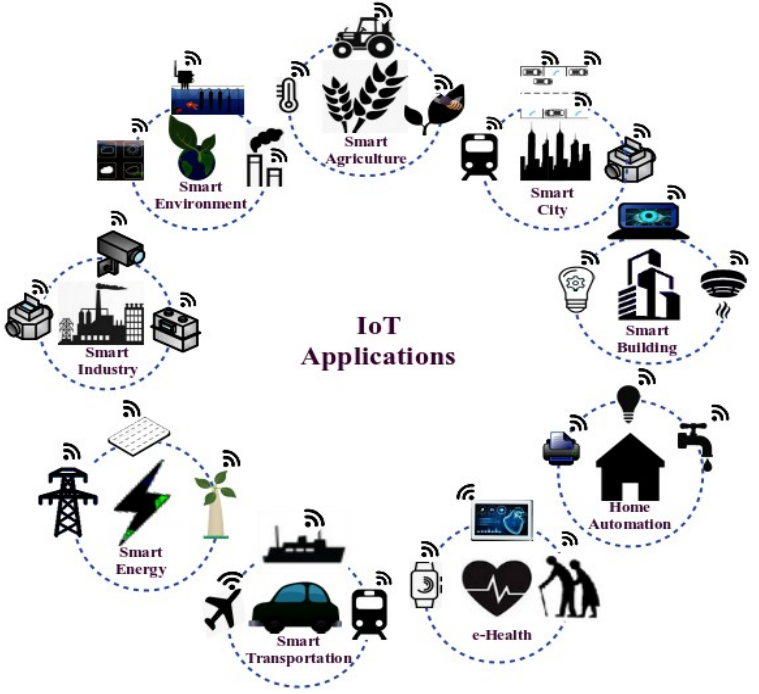
The three layer architecture provides a high-level framework (base framework) that can be used for different approaches. It includes sensing layer, network layer, and application layer.



IoT Applications

Heterogeneous IoT devices make the possibility of developing various smart applications in different domains of our everyday life. Thus, the quality of life is being improved or became more convenient using potential IoT applications.

* Smart Home
* E-Health
* Smart Agriculture
* Smart transportation
* Smart City
* Smart Energy
* Smart Industry



IoT Applications

People are adapting IoT technologies due to simplicity of usages, low cost of devices, and trust in terms of security and safety.

* Personally
* Socially
* Industry
* Business

Smartphone apps and web applications allow controlling devices locally or remotely over the network.

Examples:

* IP camera for monitoring home or office
* Smart door lock

Challenges in IoT Networks

Resource-constrained IoT devices are connected to the Internet with naive security configuration.

* Limited memory
* Low computation capabilities
* Limited Energy

Complex cryptography algorithms can not be used to secure IoT devices.

Physical threats of IoT devices always remain challenging.

* IoT devices are deployed in an open environment
* Cloning of IoT devices physical characteristics

Challenges in IoT Networks

The rapid proliferation of heterogeneous IoT devices with distinct functionalities imposes new security and privacy challenges in the cyberspace.

* Device management
* Authentication
* Security rules enforcement
* Anomaly detection
* Faulty device identification

To mitigate these issues IoT device identification plays a key role in IoT networks.

IoT Device Identification

Device identification is the process of identifying a device on the Internet without using its assigned network credentials.

* IP address
* MAC address

DFP uses implicit identifiers for device identification.

* Hardware/Software based features
* Network traffic traces
  - Network packets
  - MAC frames

IoT Device Identification

DFP exploits device-specific signature or packet information which the device uses for communication over the network.

Device fingerprint must assure two attributes:

* The features are hard to forge

* The DFP remains stable even when devices move from one network to another network

IoT Device Identification

An IP and MAC addresses ensuring logical and physical addresses of a particular device.

Conventional addressing schemes (IP/MAC addresses) have some constraints and limitations on being used as device identifiers or fingerprints.

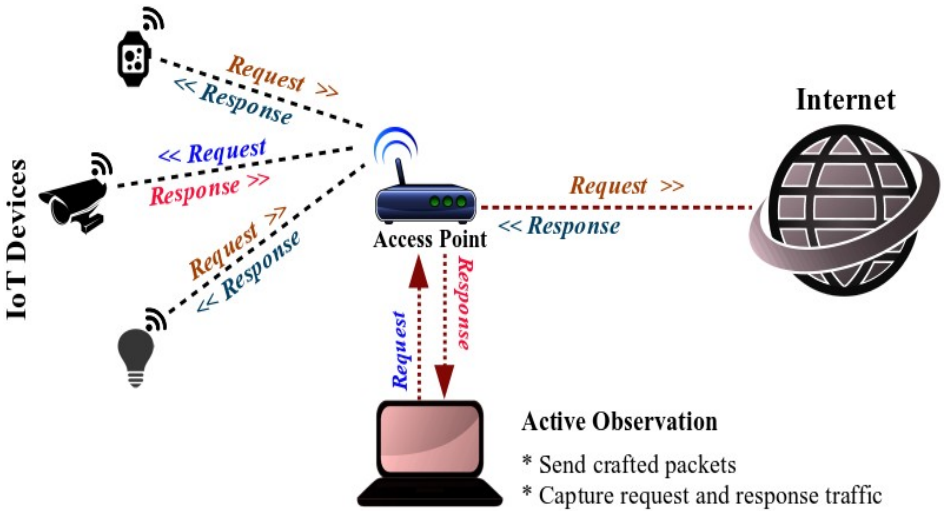
* Spoofing attack

* MAC address randomization

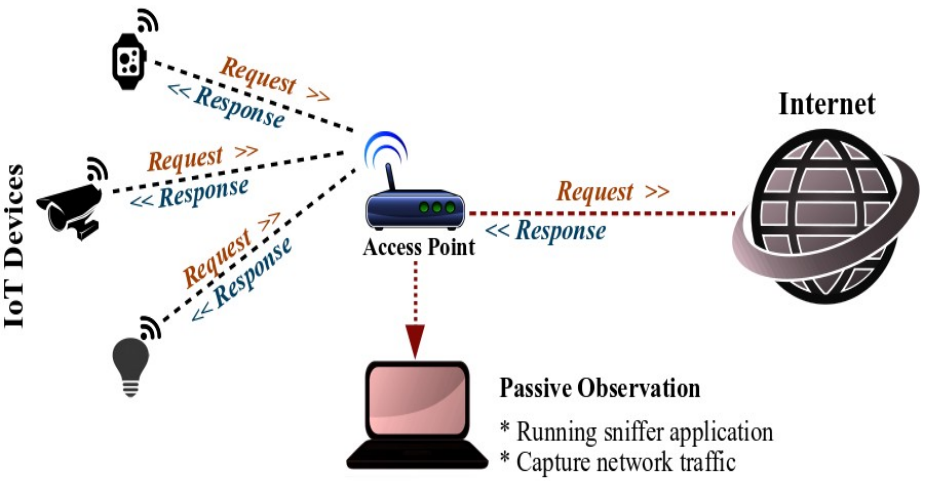
* Network-dependent IP addressing scheme

IoT Device Identification

DFP can be extracted either using active or passive fingerprinting approaches.



Active Fingerprinting Approach



Passive Fingerprinting Approach

IoT Device Identification

Passive fingerprinting has two significant benefits:

* Low-cost network resources able to capture network traffic traces
    - WiFi adapter (Monitor mode supported)
* An adversary would not be able to detect traffic monitoring system

In contrast to passive fingerprinting, active approach provides more accurate information.

IoT Device Identification

Different types of features are used to generate device fingerprints or signatures:

* Network packet header information (Protocols)
* Payload
* IAT of packets
* Statistical measurements
* Raw radio signal (in-phase and quadrature streams)
* IEEE 802.11 MAC frame

IoT Device Identification

IEEE 802.11 MAC frame

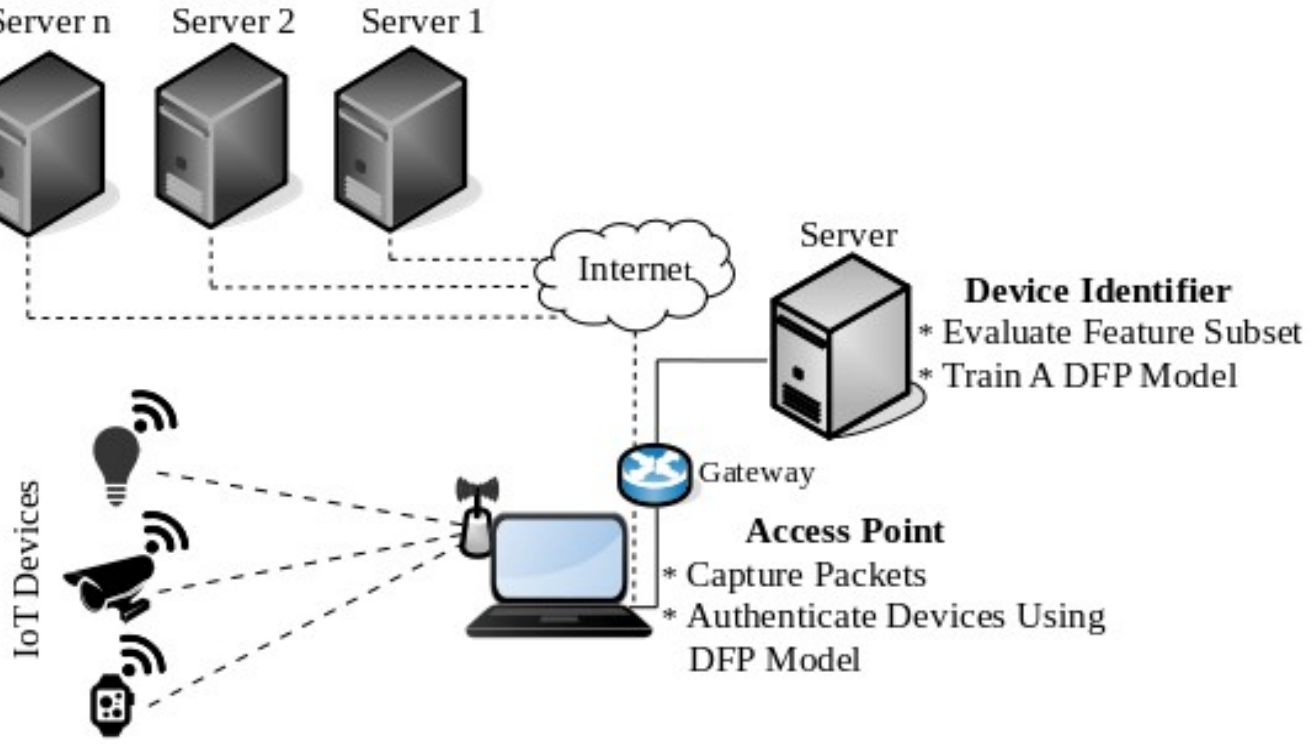
* Probe Request frame

  - Reasons:

    - Probe request frames are transmitted by the WiFi-enabled devices
    - The information carried in a probe request frame is in the form of plain text
    - Devices send probe request frame sporadically
    - Client station only sends probe request frames

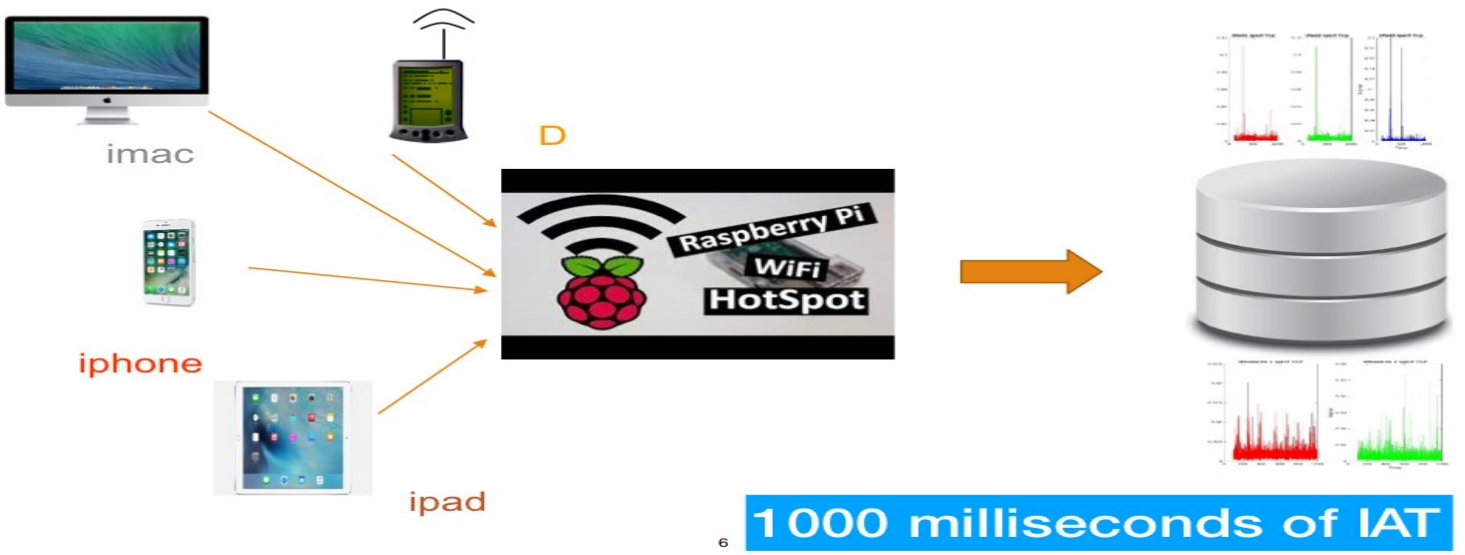
IoT Device Identification

A conceptual IoT network model.



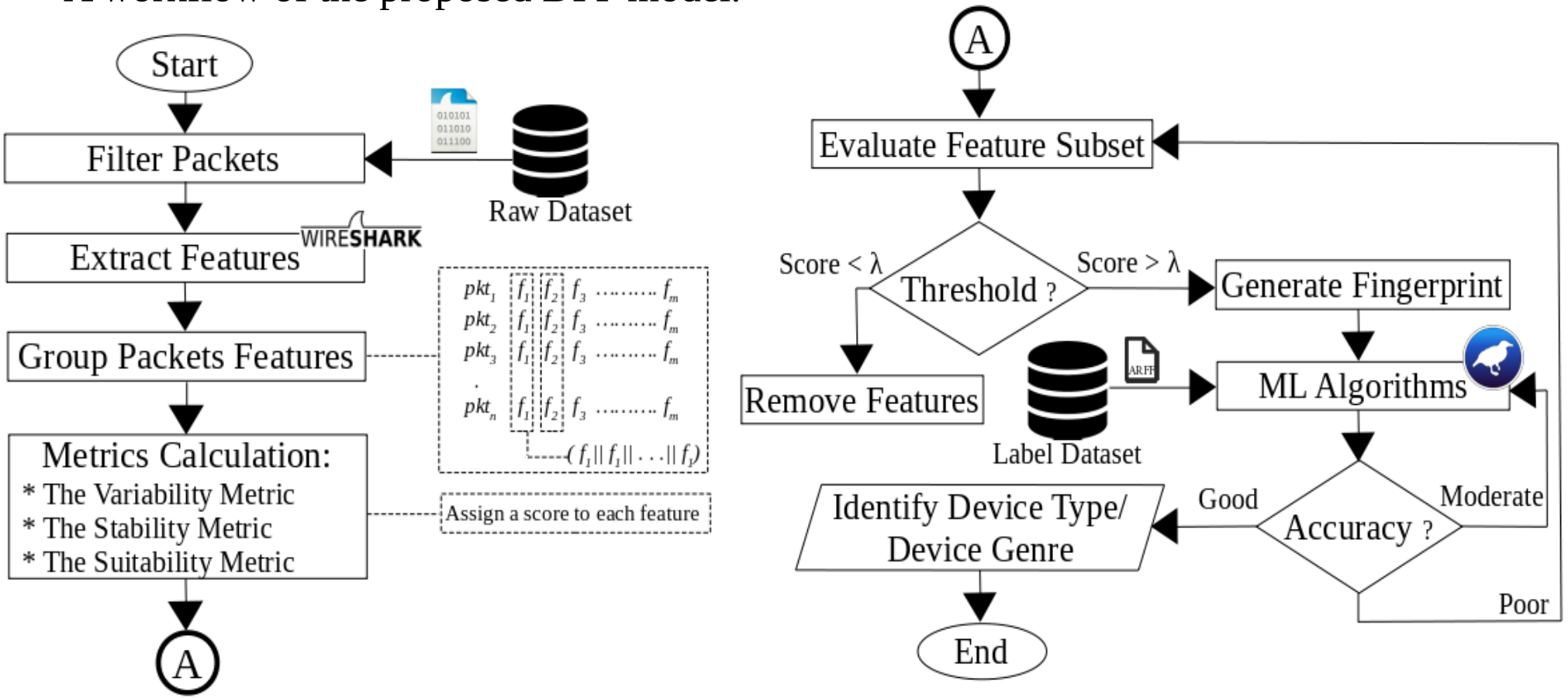
IoT Device Identification

A workflow of the proposed DFP model.



IoT Device Identification

A workflow of the proposed DFP model.



IoT Device Identification

Extracted device-specific features are used to train different DFP models for various perspectives.

* Identify individual IoT devices
* Identify IoT devices vendors
* Communication patterns

DFP models are designed based on traditional machine learning and deep learning techniques to identify IoT devices accurately.

* Random Forest
* C4.5 (J48 Decision Tree)
* PART
* CNN
* RNN

IoT Device Identification

ML is an advance form of learning techniques based on observations or input data to learn patterns.

ML helps for better decision making in the future or enhance overall performance.

It allows analyzing a massive amount of data offline or online to produce better results in the context of different domains:

* Device identification
* Anomaly detection
* Application detection
* Location tracking

IoT Device Identification

ML schemes are required a significant amount of time and resources for better training to generate models.

Traditional ML:

* Conventional ML algorithms have limited capability to process natural data from raw input

* It requires expertise for feature engineering to learn patterns or features from input data

IoT Device Identification

DL has some significant advantages compared with traditional ML techniques:

* Deep learning architectures allow to learn useful features or patterns automatically from raw input data

* It can identify complex non-linear relationships between features or attributes

* Deep learning is suitable for big data analysis

Conclusion

DFP has emerged a significant solution for IoT device identification due to its resistance against vulnerabilities such as node forgery or masquerading in IoT networks.

ML algorithms help to investigate comprehensive behaviour of IoT devices to deploy AL-enabled secure IoT networks.

Challenges:

* To identify device-specific features

* Design resource-efficient DFP models for IoT device identification