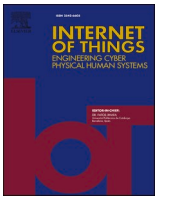
Internet of Things 20 (2022) 100632

Contents lists available at ScienceDirect

Internet of Things

journal homepage: www.sciencedirect.com/journal/internet-of-things



Review article

A survey on device fingerprinting approach for resource-constraint IoT devices: Comparative study and research challenges

Rajarshi Roy Chowdhury *, Pg Emeroylariffion Abas

Faculty of Integrated Technologies, Universiti Brunei Darussalam, Jalan Tungku Link, BE1410 Brunei, Darussalam

ARTICLE INFO

Keywords:
Internet IoT things (IoT)
Network traffic traces
Radio signals
IEEE 802.11 MAC Frames
Device fingerprinting (DFP)
Machine learning (ML)
Deep learning (DL)

ABSTRACT

Modernization and technological advancement have made smart and convenient living environments, including smart houses and smart cities, possible, by combining the Internet of Things (IoT), data, and internet-based services over various communication protocols. IoT is the next generation of the Internet. However, commonly resource-constraint IoT devices that are designed to perform a specific purpose, impose new security challenges, including node forgery, unauthorized access of data, and denial of services. They are more susceptible to being compromised by adversaries as opposed to general-purpose computing devices, and are exposed to different kinds of attacks, including spoofing and botnet attacks. Device identification is one of the promising approaches for improving network security. Devices can be identified either using explicit identifiers (internet protocol/media access control addresses) or implicit identifiers (network traffic and radio signal features), with implicit identifiers being more reliable, robust, and secure for device fingerprinting (DFP). In this paper, DFP methods have been studied in detail, with features generated from their communication traffic characteristics, including network traffic traces, IEEE 802.11 MAC frames, and radio signals, discussed. Additionally, key limitations and research challenges have been studied in the context of the IoT paradigm. Research challenges within the context of DFP and the future of IoT technologies are also discussed to shape future directions of work in the area. The key contribution of this study is the identification of different DFP research scopes in the domain of the IoT paradigm, which can be designed and implemented toward the development of IoT network security.

1. Introduction

Internet of Things (IoT), which enhances pervasive connectivity between the physical and digital worlds, is a technological elevation after the Internet. The term IoT was first coined by the Auto-ID Center in 1999. Using a radio frequency identification (RFID) tag, which consists of tiny and low-cost microchips and antennas [1–3] and hence, allowing it to be used as a unique contactless identifier, they envisioned the association of a globally unique identifier to every physical world object. This allows interaction with individual objects over the network, including for the purpose of object tracking and querying an object in real-time [1]. Thus far, IoT network has been gradually expanding in usage and incorporated into heterogeneous technologies, objects, applications, and communication protocols (wireless fidelity (WiFi), Ethernet, and Bluetooth) to allow the provision of various services from the cloud servers/services [4, 5]. Consequently, the availability of a large number of interconnected IoT and non-IoT devices has brought new

* Corresponding author.
E-mail address: 19h0901@ubd.edu.bn (R.R. Chowdhury).

https://doi.org/10.1016/j.iot.2022.100632

Available online 22 October 2022

opportunities for human beings to their doorstep.

However, IoT devices, such as smart cameras, water sensors, motion sensors, smart plugs, smart watches, and smart bulbs, are commonly designed and built for specific-purposes and are inherently resource-constraint in terms of their limited processing power, memory, and energy [1, 6, 7]. This is in contrast to general-purpose computing devices, referred to as non-IoT devices [8, 9], such as computers, laptops, smartphones, and tablets, which are commonly equipped with ample resources. Fortune Business Insights reported that the market value of IoT was $250.72 billion in 2019 and is growing with a 24.7% compound annual growth rate (CAGR) between 2019 to 2027. It is expected to reach a $1102.6 billion market value in 2027 [10]. In terms of the number of devices, the total number of IoT devices is expected to reach approximately 30.9 billion by the year 2025, in contrast to non-IoT devices with only 10.3 billion devices, despite its larger initial proportion [11]. Similarly, IHS Markit has estimated that the number of connected IoT devices will surge to approximately 125 billion by the year 2030 [12].

Specific-purpose IoT devices are fabricated with key characteristics, including sensing ability, connectivity, and exchange of data. These devices have been successfully incorporated rapidly into various aspects of everyday life, ranging from home automation to health-fitness services [13, 14], due to the remote sensing, controlling, and monitoring capability of these IoT devices over the networks. Different types of IoT network architectures [15, 16] are available. For a given IoT network, its architecture is normally chosen based on the characteristics of the demand brought about by the intended applications, with the 3-layer architecture providing the base framework [16].

The relatively new IoT ecosystem has, however, brought new challenges to cyberspace, including data and network security, data analysis (big data), energy, connectivity, and service, and consequently, these challenges have stimulated many research interests from industry to academia in the last few years. Researchers have highlighted that the proliferated growth of heterogeneous IoT devices with different functionalities is facing security and privacy challenges, including device management [17], anomaly detection [18], security rules enforcement [19], authentication [20], attack detection [21], faulty device identification [22], and location tracking [23]. These are partly due to the resource-constraint nature of IoT devices [24], forcing the IoT devices to be connected to the Internet with naive security configurations [15]. This allows adversaries in the network to take advantage of such vulnerabilities to perform various types of malicious attacks, including denial of service (DoS) and spoofing. For instance, the Mirai (a malware) botnet [25] had used millions of compromised IoT devices, which are commonly configured only using the default password, to launch distributed denial of service (DDoS) attacks. Similarly, its variant, Persirai [26] and Hajime [27], have affected IoT networks on numerous occasions.

To mitigate these issues, many researchers have proposed different approaches, including device identification, traffic flow identification, anomaly detection, and log prediction, based on the analysis of network traffic traces or signal processing, either using different machine learning (ML) or deep learning (DL) algorithms. Both ML and DL algorithms have been used to automate various processes, including device classification and decision-making, based on input data or observations. Device identification plays a key role in securing an IoT network. Traditionally, network-connected devices are identified using internet protocol (IP) and medium access control (MAC) addresses, also known as explicit or user-defined identifiers. Whilst necessary to facilitate inter-network and intra-network communications, unfortunately, these identifiers have been proven to be vulnerable to different kinds of attacks, including spoofing, DoS, and MAC address randomization, by utilizing many easily accessible malicious software, such as MAC address changer [28], and IP spoofing [29]. Additionally, device mobility significantly affects IP-based device identities, with IP addresses changing as the devices move from network to network. Device fingerprinting (DFP), also known as implicit identifiers [30], has been touted as a solution to the device identification problem. DFP uses network traffic traces, including network packets, MAC frames, and radio signals, to extract device-unique identifiers from different layers of the communication models [31]. This can be done actively by probing devices to send feedback communication traffic or passively, through passive observation of traffic exchanges between devices.

An extensive review of IoT device fingerprinting approaches is given in this paper. The paper first described IoT technology and network security from different perspectives, including device fingerprinting (DFP), data security and privacy, applications, and architectures of IoT. This provides a good foundation for the IoT paradigm and assists in understanding the future directions of the technology. It also highlights different research approaches, including device fingerprinting, sensor networks, and device management, for improving network security. Additionally, this paper signifies key research challenges, including DL and ML learning models, datasets (optimal size of training dataset), and communication protocols (Bluetooth and IP-enabled devices used different sets of communication protocols), toward the future development of IoT technology, which is the main contribution of this study.

The key contributions of this paper are as follows:

- Ø To provide a brief description of IoT technologies in terms of applications and network architectures.
- Ø To describe the different types of existing device fingerprinting (DFP) schemes, including data collection, data pre-processing, fingerprint/signature generation processes, and features engineering.
- Ø To discuss key limitations and research challenges in the new era of the IoT ecosystem, to guide the readers and research communities towards the future direction of work in IoT and DFP.

The rest of the paper is organized as follows. Section 2 describes the usage of IoT technologies and the basic architectures of IoT networks. Device fingerprinting methods, as well as data collection and pre-processing, network, and radio signal features from different layers of the communication models and state-of-the-art machine learning approaches, are presented in Section 3. The future development of IoT technologies is described briefly in Section 4. Section 5 briefly discusses IoT and DFP model's research challenges toward the development of IoT and ML/DL technologies, and finally, a conclusion is given in Section 6.

2. Internet of Things (IoT)

IoT is the next advancement of Internet technology. The adoption of this technology has been rising sharply worldwide due to its availability, affordability and usability. In reference [32], the authors utilized the MaxMind GeoIP database [33] (which provides a mapping service between IP addresses and their geographical locations using free or commercial products) to characterize the geographical distribution of IoT devices in the world to give an approximate list of the top 18 countries with the largest total number of IoT devices, which is presented in Fig. 1. It can be seen that the top 18 countries account for nearly 12 million IoT devices for various purposes, with the United States (US) having the largest number of IoT devices.

Researchers from academic and industrial domains have studied IoT technologies from different perspectives, including application, architecture, data security, and privacy. However, there is yet to be a commonly accepted standard or definition, with researchers from different domains, including home automation, agriculture, and medical science, defining IoT from their respective perspectives. Typical definitions of IoT from the various standard organizations are listed in Table 1. These definitions are generally based on three crucial characteristics: sensing capability, connectivity, and exchange of data.

2.1. Architecture of IoT network

An IoT network architecture is designed to provide different services by utilizing the devices' basic characteristics, including sensing, networking, and data communication. It consists of different layers, forming a multi-layer network, with the architecture describing communication structures between the physical and the logical worlds. However, there is yet to be a single universally accepted consensus on what constitutes an IoT architecture [16]. Different researchers have proposed various IoT network architectural frameworks, including a 3-layer [15, 16, 51, 53, 57–59], 4-layer [60], and 5-layer [16, 61, 62] architectures to reflect their different research perspectives, be it a public project or an academic research. However, a 3-layer architecture is commonly adopted [63] due to its high-level framework (or base framework) that can be used for different approaches. Fig. 2 depicts a typical representation of a 3-layer IoT network architecture, including the perception/sensing, network, and application layers. Devices, including IP cameras, smart bulbs, and smart locks, are configured to connect with a network access point (gateway or other devices) using WiFi or Ethernet interfaces to provide different services from the cloud servers. Device-specific application programming interface (API) is used to control and operate individual devices, allowing access to devices locally and from a remote location over the network.

Perception Layer: In a 3-layer architecture, the perception layer represents the physical layer, where sensors are attached to objects (or things) for collecting data on the surrounding environment. There is a wide range of sensors for various purposes, including visionary, temperature, air quality, speed, humidity, pressure, flow, motion, and electricity sensors [13]. The perception or sensing layer also converts information, which is in analogue form, into digital form for convenient data transmission over the network [57].

Network Layer: This layer is responsible for connecting smart objects to network devices, such as access points and servers, to allow the transmission and processing of sensor data from the perception layer. It uses different types of networking technologies, including wireless-fidelity (WiFi), Ethernet, Bluetooth [64], ZigBee [65], Z-Wave [6], near-field communication (NFC) [66, 67], and Infrared [68], for communication [57].

Fig. 1. Geographical distribution of IoT devices (top 18 countries) [32].

Table 1
Typical definitions of IoT.

Year	Organization	IoT Definition
2009	Coordination and Support Action for Global RFID-related Activities and Standardisation (CASAGRAS) - An EU Framework 7 [50]	A global network infrastructure, linking physical and virtual objects through the exploitation of data capture and communication capabilities.
2012	International Telecommunication Union- Telecommunication (ITU-T) [51]	A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving inter-operable information and communication technologies.
2014	International Organization for Standardization/ International Electrotechnical Commission Joint Technical Committee 1 (ISO/IEC JTC 1) [52]	An infrastructure of interconnected objects, people, systems, and information resources together with intelligent services to allow them to process information of the physical and the virtual world and react.
2015	The Institute of Electrical and Electronics Engineers (IEEE) [53]	A network of items which is connected to the Internet, each embedded with sensors.
2021	Oracle [54]	The Internet of Things (IoT) describes the network of physical objects-"things"-that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the Internet. These devices range from ordinary household objects to sophisticated industrial tools.
2021	The Internet Engineering Task Force (IETF) [55]	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.
2021	Gartnet [56]	The Internet of Things (IoT) is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment.

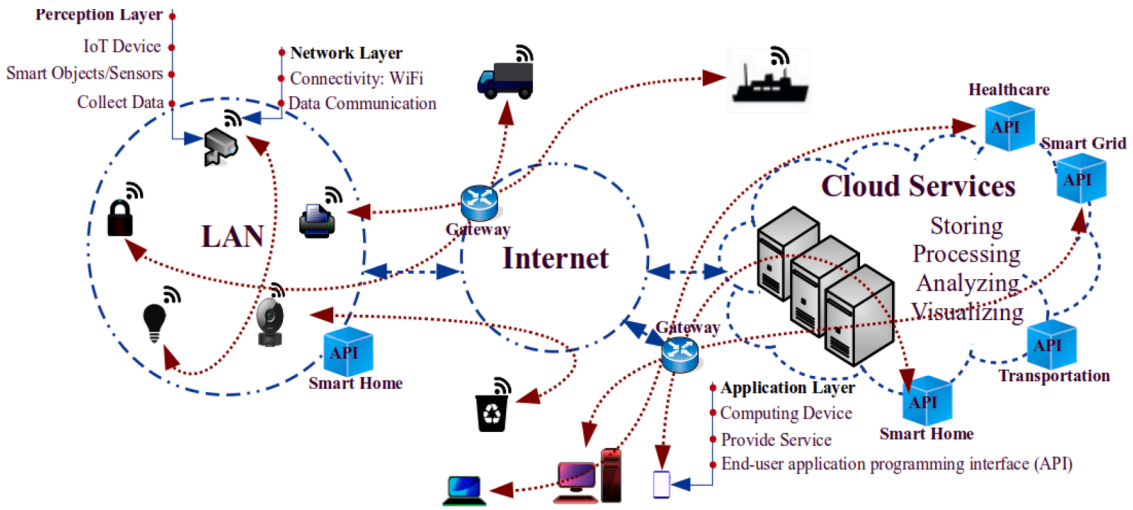


Fig. 2. A typical representation of IoT network architecture (3-layer).

Application Layer: The application layer provides specific services to end-users according to their demands or usages. This layer uses processed data from the network layer, which it receives from the perception layer, and acts as the front-end in the IoT architecture [69]. Via the application layer, end-users are able to control different objects, such as turning on/off a light bulb, and smart home IoT devices, using different applications. Examples of end-user applications in the application layer are mydlink Lite [70], and Smart Life [71].

2.2. Applications of IoT devices

Heterogeneous IoT devices with diverse sensing, controlling, and monitoring capabilities make possible the development of smart applications in different domains [72, 73], including education, research, data mining, automation, and healthcare. Subsequently, the adoption of these different IoT technologies has improved the quality of life of the population, making it more convenient. All these applications can be generally grouped into the following domains: smart city, smart home, smart agriculture, smart transportation, smart health and fitness, and security [13, 16, 59], as depicted in Fig. 3. These smart technologies have been successfully adopted for personal usage, smart industries, and smart businesses due to their simplicity, usability, affordability, open-source applications, including web and smartphone applications, and trustworthiness in terms of security and safety. For instance, smart applications such as Smart Life [71] allow the remote control of IoT devices (IP camera for monitoring home or office, smart door lock) over a network

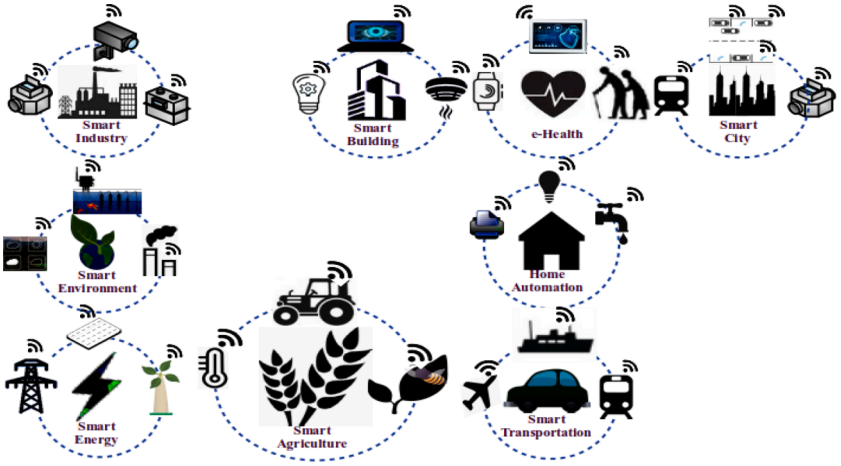


Fig. 3. Application of IoT technologies in different domains.

via end-user devices: computer, smartphone, and tablet.

2.3. Security of IoT devices

The fast adoption of IoT devices for various purposes has brought new security challenges to cyberspace. Depending on their application, IoT devices are commonly compact, miniature devices with limited computational resources, and subsequently, they are prone to different kinds of attacks. Table 2 provides an overview of different IoT systems, highlighting the different security perspectives that need to be taken into consideration. Confidentiality, integrity, authenticity, availability and non-repudiation of data, as well as authentication and management of IoT devices, are some of the security challenges that are faced with the implementation of IoT systems.

3. Device fingerprinting

Device fingerprinting (DFP) is a process of identifying (or classifying) devices using device-specific signatures [30]. The method exploits the communication characteristics of the devices, which the devices utilize for communication over the networks, including network packet traces [8, 19, 74, 75], MAC frames [76, 77], and radio signal (or wave) [44, 78–80], to generate fingerprints or signatures. A signature or fingerprint can be represented as a vector, image, or hash value. Effective DFP must assure two properties: (i) generated signatures are hard to forge, and (ii) signatures remain stable even when devices move from one network to another network [30]. DFP approaches can be categorized into two broad categories based on the feature generation methods: active and passive device fingerprinting, as presented in Fig. 4.

In a passive DFP approach, inbound and outbound communication traffic traces of the target systems are observed passively by a profiler to generate device-specific signatures without making particular queries to individual devices. On the other hand, in an active DFP approach, target devices are probed with crafted packets. Subsequent responses from the devices are then captured and analyzed for fingerprinting generation. Key differences between active and passive DFP methods are listed in Table 3.

A DFP model may be an active or passive fingerprinting approach based on the data collection process. To further advance the development of fingerprinting technologies, some researchers have published their datasets for the research community in the same domain. Subsequently, researchers have proposed different methods of selecting subsets of features for the classification task to reduce computational complexity and improve classification accuracy. These feature sets have been used to train and test different learning mechanisms, including ML and DL algorithms, for identifying network-connected devices and traffic types. In the following subsections, all these approaches are briefly presented.

3.1. Data collection process

Depending on the adopted approach, communication traffic traces (network packet, frame, or radio signal) need to be captured for the generation of device fingerprints. A conceptual framework of the data collection process is presented in Fig. 5, where data captured can be in the forms of packets [8, 19, 84], MAC frames [84, 87], and radio signals [88, 89], to be kept for further analysis. Communication traffic traces (data) can be captured using both active and passive approaches from different layers of the communication model. In a network, IoT and non-IoT devices are commonly configured to associate to an access point (AP), either using WiFi or Ethernet interfaces for providing network services. A monitoring station (MS) connects with the target AP to sniff the communication traffic traces for further analysis. MS running an operating system (OS), such as Windows, Linux, or Mac OS, along with a network traffic analyzer or sniffing tool, such as Wireshark [81], may be used to capture or record communication packet and MAC

Table 2
A brief description of the IoT ecosystem from different perspectives.

Source	Year	Research Topics	Security Perspectives	Sensor/ Communication	DFP	Observation
[34]	2010	Visions, applications, technologies, and research challenges	Device mobility, authentication, and data integrity in sensor networks	RFID	Not covered	Limited information of device identification
[35]	2012	Technologies, applications, and development challenges	Data confidentiality and privacy	RFID	Not covered	Limited information of device identification
[36]	2013	Vision, architecture, application, cloud computing and future development	Network security and privacy	RFID, WSN	Not covered	Limited information of device identification
[37]	2014	Application and future development	Identity management, network security and privacy	RFID, NFC	Not covered	Limited information
[38]	2015	Basis of IoT, applications, technologies, and architectures	Device identification	RFID, WiFi, NFC, ZigBee Bluetooth,	Not covered	Limited information
[30]	2015	Taxonomy of device fingerprinting	Device identification, DFP features	Wireless network-WiFi	■	Limited scope of IoT devices, and other networking technology
[16]	2017	Architectures and applications of IoT	Access control	Sensors, RFID, NFC, WSN, WiFi	Not covered	Traditional identifier, e.g IP, RFID tag
[39]	2017	Operation research (hard and soft) challenges, system standards	Data security and Privacy	None	Not covered	IoT technical and business research challenges
[40]	2017	Wireless network technologies	Security on LPWA (Licensed spectrum and unlicensed spectrum)	Wireless network	Not covered	Long range communication for IoT devices
[41]	2018	Vision, applications, architecture, and challenges	Identity management, device safety, data confidentiality	RFID, sensors	Not covered	Limited information
[15]	2018	Life cycle of data driven IoT networks	Access control, data security, digital forensic	Sensor network	Not covered	Explore different perspective of data security for IoT
[42]	2019	IoT architecture, applications, technology, and challenges	Secure IoT architecture, access control, data privacy, secure protocol	Sensor network	Not covered	Growth of IoT technology and social perspectives
[43]	2019	Browser fingerprinting, categories, and challenges	User privacy	Network	■	Improving online security
[44]	2020	Radio frequency fingerprinting	Device identification	Wireless devices	■	Physical layer properties for identifying wireless devices
[45]	2020	Security challenges and countermeasures in IoT	Data privacy, and mobile computing	Sensors	Not covered	Limited to data privacy
[46]	2021	Security and privacy in IoT, deep learning	Device identification, behaviour of IoT devices, and data privacy	Sensors	■	Identifying IoT devices using DL
[47]	2021	Identity methods of IoT devices	Device identification, and authentication	RFID, IP, EPC, Barcode, WSN	■	Limited information on implicit identifiers
[48]	2022	IoT and device fingerprinting	Device identification, and machine learning	Sensors	■	Limited to network packet analysis
[49]	2022	Radio signal and device fingerprinting	Device identification and learning algorithms	Wireless devices	■	Limited to radio signal analysis

Note: Wireless sensor network – WSN, Electronic product codes – EPC, Radio frequency identification – RFID, Internet protocol – IP, Near field communication - NFC, Wireless fidelity - WiFi.

frame traces. A local area network (LAN) can be setup for extending network services by configuring and incorporating additional network devices, such as a hub and switch. Wireshark allows the capture of network packets from both local (WiFi and LAN) and global networks, whilst IEEE 802.1x MAC frames can only be captured from wireless local area networks (WLAN). In WLAN, WiFi-enabled devices use IEEE 802.1x MAC frames for associating or disassociating to an access point (AP) within WiFi ranges for connection establishment. In reference [84], the collection process of network traffic traces (network packets and IEEE 802.1x MAC frames) has been described in detail. On the other hand, a software-defined radio (SDR) device, such as universal software radio peripheral (USRP) N210 [88], or RTL-SDR [90], may connect to the monitoring station for capturing radio signals for further processing to generate fingerprints. The radio signal collection process has been briefly described in reference [86]. However, the literature has shown that expensive hardware and software are required to capture radio signals as compared to network traffic traces (packets and MAC frames).

3.2. Datasets

Researchers have utilized different datasets, including public and private datasets, to evaluate the performances of different device fingerprinting models. Some of the publicly available datasets are presented in Table 4, with some consisting of network traffic traces (packet/frame) and radio signals of the IoT and mobile devices. Miettinen et al. [19] provided a dataset of 31 smart home IoT devices with 27 different types from different manufacturers; however, it only contains devices set-up phase communication traffic. In

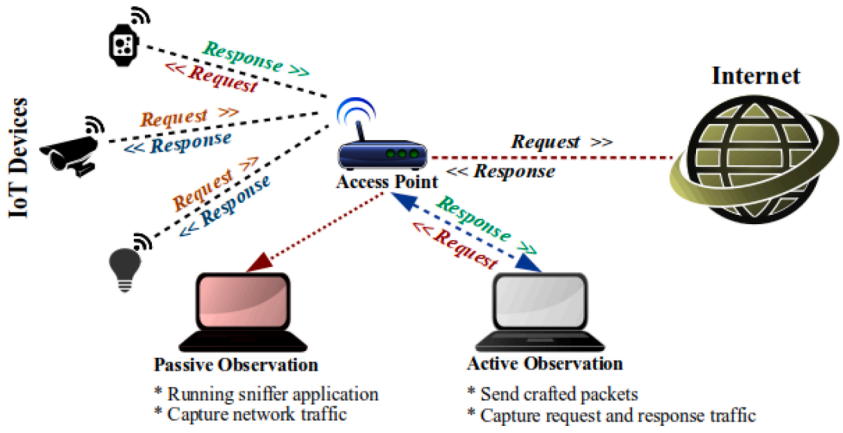


Fig. 4. An abstract view of active and passive device fingerprinting approaches.

Table 3
Comparison between active and passive fingerprinting.

Passive Fingerprinting	Active Fingerprinting
Monitor and analyze ongoing communication traffic traces from a target network.	The target system's response traffic traces are analyzed according to the crafted queries.
Does not generate additional traffic in networks.	Generate additional traffic in networks due to specific requests.
Partial information can be extracted from devices.	Provides in-depth information regarding a device.
Adversaries would not be able to detect network monitoring systems.	Network activity footprints are detectable, e.g. log analysis.
The scope of the network is limited to local ranges, e.g. local area network (LAN), and wireless local area network (WLAN).	Scope in the global range, even when devices are behind a firewall or network address translation (NAT).
Network traffic analyzer, e.g. Wireshark [81], EtherApe [82].	Active network traffic analyzer, e.g. Network mapper (Nmap) [83].

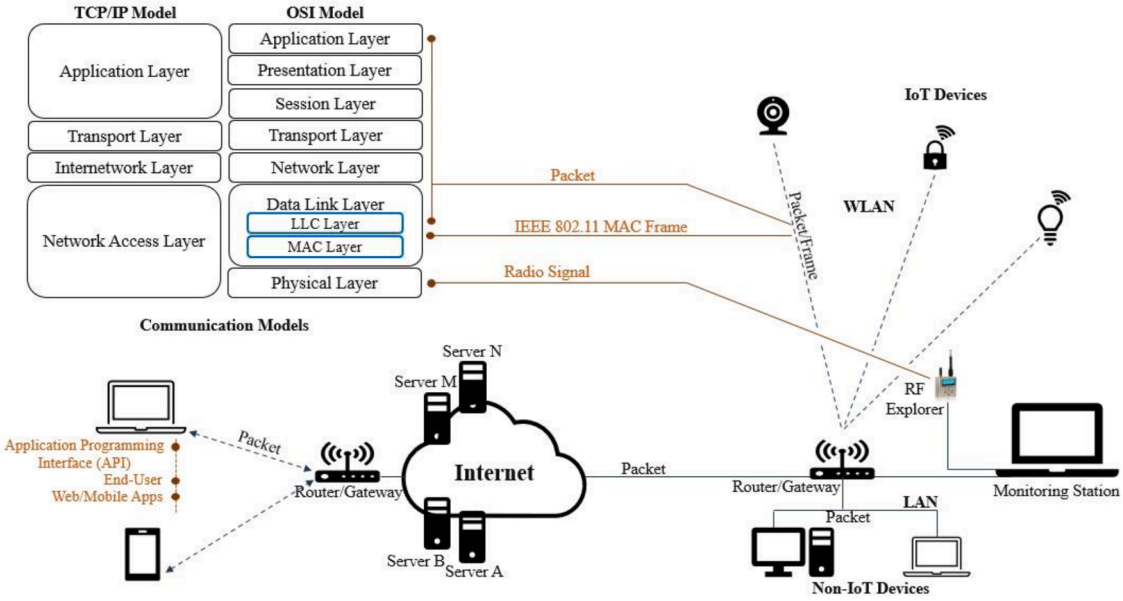


Fig. 5. A conceptual view of the data collection process [84–86].

reference [91], network traffic traces of 22 IoT devices, including smart bulbs, smart plugs, IP cameras and coffee makers, from a laboratory environment are provided. Similarly, an experimental testbed was set-up in a University of New South Wales (UNSW) laboratory to capture network traffic from both IoT and non-IoT devices for a long duration of time [8]. This UNSW dataset comes from 28 devices, including 21 IoT and 7 non-IoT devices from different manufacturers.

The D-Link IoT datasets [84] consist of both network packets and IEEE 802.11 MAC frames (probe request frame), which were

Table 4
List of publicly available datasets.

Dataset	Network Traffic		Radio Signal	Traffic Monitoring		Devices	Source
	Packet	Frame		Active	Passive		
IoT Sentinel	■	–	–	–	■	31	[19]
UNSW	■	–	–	–	■	28	[8]
LSIF	■	–	–	–	■	22	[18]
D-Link IoT	■	■	–	–	■	14	[84]
Gatech/fingerprinting (GTID)	■	–	–	■	■	30	[92]
Glimps2015	–	■	–	–	■	28,048	[87]
Sapienza/probe-requests	–	■	–	–	■	16,000	[93]
Sigcomm2008	–	■	–	–	■	–	[94]
DataIoTTrans	–	–	■	–	■	9	[95]
MonoRxSet	–	–	■	–	■	21	[96]

collected in the network systems and signal processing (NSSP) laboratory at Universiti Brunei Darussalam (UBD). 14 smart home IoT devices from the same manufacturer, i.e. D-Link, have been utilized. On the other hand, the GTID [92] dataset was collected from 30 wireless devices, including iPad, netbooks, IP cameras, kindle, etc., with the traffic traces captured actively and passively from different protocols and applications. The dataset presents the inter-arrival time (IAT) of captured packets in MATLAB file format. The glimps2015 (or hasselt/glimps2015) dataset [87] was recorded at a music festival in Ghent, Belgium. Probe request frames from about 28,048 mobile devices were captured by utilizing 8 monitoring stations (MS). Similarly, approximately 16,000 WiFi-enabled mobile devices probe request frames were collected in the Sapienza/probe-requests dataset [93]. In reference [94], the authors captured wireless network measurements (Sigcomm2008 dataset) from the Sigcomm 2008 conference at the Grand Hyatt Regency in the USA, where 8 IEEE 802.11a monitoring stations were configured to capture traffic traces. The dataIoTTrans dataset [95] comprises radio frequencies (or signals) from 9 IoT devices, with universal software radio peripheral (USRP) software used to capture IQ samples of the signals. In reference [96], the researchers collected the monoRxSet dataset from the FIT/CroteXlab testbed with a controlled environment in France, which included 21 emitters, one receiver and a scheduler for the data collection process. The emitters and the receiver used were the National Instruments USRP N2932 software-defined radio (SDR) devices, working at 5 Msample/s and 433 MHz.

3.3. Device fingerprint features

A large number of features can be extracted from the different layers, including the physical (radio signal), data link (IEEE 802.11 MAC frame), and upper layers (network packets), of the communication models [97], i.e. open systems interconnection (OSI) model or TCP/IP model, for generating device-specific signatures (or fingerprints). Individual features may carry significant information for classifying devices in the networks. Device-specific features have been grouped into the following categories: network traffic and radio signal features, as depicted in Fig. 6, with network traffic further sub-divided into network packet features and IEEE 802.11 frame features (or MAC frame features).

3.3.1. Network packet features

Communication traffic traces (or packets) are exchanged within network-connected devices over a network, with network traffic generated from two scenarios [8]: (1) autonomous traffic – traffic generated by IoT and non-IoT devices for an upgrade process and synchronization (e.g. firmware update, clock synchronization using NTP protocol), and (2) user traffic – traffic generated by the devices according to user's interaction (e.g. IP cameras, which may be used to monitor home security over networks, motion sensor to detect movement to turn on a light bulb, etc.). Different types of low-cost commodity hardware, such as USB WiFi adapters and USB

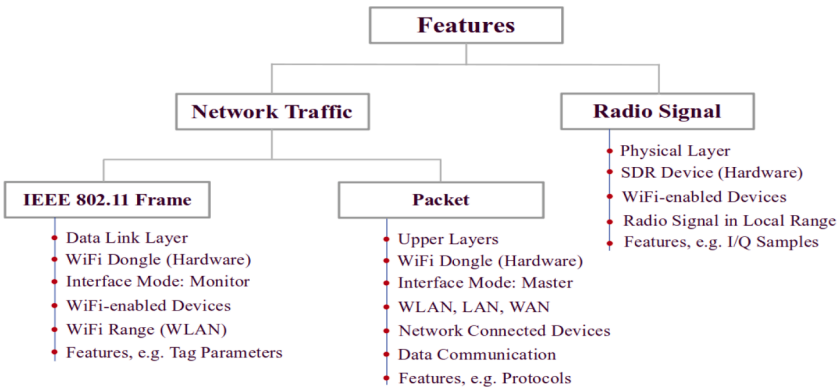


Fig. 6. Categories of DFP features.

Table 5
Categories of network packet features used for device fingerprinting.

	Categories		Features	H	Pa	Packet	Flow (*n* Packets)	DFP			Source
Network Packet	Value Oriented	Actual	Real-value [b, s]	■ [a, b, c, e, g, k, l, m, n, p, q, s, u, x, z, G]	■ [c, e, h, l, n, p, q, A, F]	■ [a, b, s, A]	■ [c, d, e, f, g, h, l, k, l, m, n, o, p, q, t, u, x, z, D, G]	Vector [a, b, c, d, e, g, h, j, k, l, m, o, p, q, s, u, x, z, A, B, C, D, E, G]	Image [f, n, t, F]	Hash-Value [i]	a
			Port number [c, e, k, s, D]								b
			TCP window size [d, r, s, D]								c
			Textual information [m]								d
			Data (Payload) [A, C]								e
		Custom	Integer [a, p]								f
			Binary [a]								g
			Number of protocols [c]								h
			DNS requests no [c]								i
			DNS data [v, w, x]								j
			Number of servers [c]								k
			IP address [k]								l
			Adv. channel sequence [o]								m
			IP header length [p]								n
	Time Oriented		Sleep/Idle time [c, e]								o
			Active time [c]								p
			DNS interval [c, e]								q
			NTP interval [c, e]								r
			Mean rate (Bps) [c]								s
			TTL [j, p, r]								t
			Packet timestamp [n]								u
			Burst rate [o]								v
			Burst time point [o]								w
			Adv. event interval [o]								x
			Adv. delay distribution [o]								z
			Duration [q]								A
			IAT [f, n, q, t, u, z, G]								B
	Statistic Oriented - (Data or Byte)		Packet size [c, k, q, u, G]								C
			Active volume [c]								D
			Payload entropy [d]								E
			Payload length [d, p, D]								F
			Flow volume [e, q]								G
			Flow duration [e]								
			Flow rate [e]								
			Packet length [g, l, o, r]								
			Number of bytes [g]								
			TCP-flow [h, j, F]								
			Total packets transmission								
			Number of packets [o, q]								
			Packet direction (fwd, bck) [G]								
			Entropy [E]								
	Other		Cipher suite [e]								
			Nilsima Hash [i, B]								
			Packet type [o]								

Note: Header - H, Payload - Pa, Time to live – TTL, Inter arrival time – IAT, Bits per second – Bps, Advertise – Adv, [a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z, A, B, C, D, E, F, G] - Represent relationship among filed values

Ethernet adapters, and software packet sniffing tools, such as tcpdump [98], Wireshark [99], and EtherApe [82] may be used to capture all these inbound and outbound traffic traces. Network packet features can be extracted from different layers of the communication models [97], either using information from a single packet or a group of packets (also called a packet flow or session - a group of packets with 5-tuples, including source-destination IP addresses, source-destination ports, and protocol [100–102], forming a session.). Generally, a packet consists of two-part of information: header and payload. The key purposes of the header are to distinguish each packet from another and also for error checking when delivering the individual packets to the right destination over a network, whilst the payload carries the actual content of a packet [103, 104].

Table 5 provides a list of key feature sets that many researchers have used for DFP approaches. Fingerprints may be represented as vectors (such as – one-dimensional array of integer or floating numbers [105, 124, 125]), images (such as – integer or floating numbers are converted to a bar chart or a histogram [107, 126]), and hash values (such as – the Nilsimsa hash function generates a digest from input data [120]). These feature sets can be categorized into four groups: value-oriented, time-oriented, statistical-oriented, and others, based on the assessment of the individual feature value in the DFP. Value-oriented features are either extracted from network traffic traces' actual/real value, such as port number, or custom values, which are computed according to the DFP model. For instance – in reference [19], the authors have mapped port numbers, including source and destination port numbers, to network port class, e.g. well-known port numbers ((0 – 1023) or (0 to $2^{10} - 1$)). On the other hand, time-oriented features are calculated based on timestamps available in the captured network traffic traces, such as packet sending and receiving timestamps. Statistical-oriented features are quantified based on different mathematical models, such as entropy, mean, standard deviation, and packet transmission ratio. For DFP, researchers [91, 127] have also used various hash functions, which are categorized as the other category of network packet features, in this paper.

3.3.2. MAC Frame features

WiFi-enabled communication devices, such as smartphones, laptops, and IoT devices, including IP cameras and motion sensors, IEEE 802.11 MAC frames with nearby access points (AP) to establish a connection within the local area network. These non-AP devices regularly scan the available WiFi networks within their range and send probe request frames sporadically along with other frames, such as beacon, association request, and authentication [87] frames. However, once associated with an AP, these devices start to transmit probe request frames less frequently. Similar to network packet traces, these types of communication traffic traces can be easily captured using commodity and low-cost hardware [30]. A probe request frame is preferable to be used for device identification due to key reasons: (1) a probe request frame is transmitted by WiFi-enabled devices only, and (2) information carried in a probe request frame is in the form of plain text [76]. Many researchers have proposed different DFP schemes based on the analysis of IEEE 802.11 MAC frames, as presented in Table 6.

These features can be categorized into three groups: value-oriented, time-oriented, and statistical-oriented, based on the assessment of the individual feature value, similar to network packet features. In a probe request frame, the features may consist of different types of information elements (IEs) tagged parameters: service set identifier (SSID) parameter set, supported rates, extended supported rates, high throughput (HT) capabilities, vendor-specific, interworking, robust security network (RSN) information, access point channel report, direct sequence (DS) parameter set, extended capabilities and very high throughput (VHT) capabilities [87]. Since these IEs (except SSID parameter set and supported rates [128]) are optional and vary from device to device, the set of tagged parameters may vary according to individual device configuration and capabilities. For instance, the DCS-930L (D-LinkDayCam) model device used a total of 5 tagged parameters, including SSID parameter set, supported rates, extended supported rates, HT capabilities, and vendor-specific IE, compared to the DCS-936L (D-LinkCam) model device, which only uses 4 tagged parameters: SSID parameter set, supported rates, extended supported rates, and vendor-specific IE.

Table 6
Categories of IEEE 802.1x MAC frame features used for device fingerprinting.

	Categories		Features	Type of Frame	Flow (*N Frames*)	DFP		Source
IEEE 802.1x MAC Frame	Value-Oriented	Actual	Frame size [b]	Probe Request [a, b, c, d, e, g]	■ [a, c, e, i, j]	Vector [a, d, e, h, i, j]	Image [b, c, g]	a
			[1] Field values [d]		50 [b]			b
		Custom	Jitter [h]	Beacon Frame [g, h, i, j]	1 [d]			c
			Intercept [h]		60 [g]			d
			Frame size [i]	All types [b, c]	100 [h]			e
	Time-Oriented		Medium access time [b]					f
			Transmission time [b, f, g]					g
			IAT [b, f, g]					h
			Duration field [C]					i
			Clock skew [h, j]					j
			Clock offset [h]					
	Statistical-Oriented		Information elements [a, e]					
			Transmission rate [b]					
			Ratio-total number of frames [c]					

Note: [a, b, c, d, e, f, g, h, i, j] – Represents relationship among filed values, [1] – 19 field values (check **reference** [131]), Inter arrival time – IAT, N Frames - Define n number of frames used to generate unique fingerprints, whilst frame numbers are selected using a time scale or the proposed DFP models

3.3.3. Radio signal features

With the rapid development of wireless communication technologies, wireless-enabled devices may be connected to a network for various purposes. These devices may utilize different radio frequencies (or signals) for their communication activities. Radio frequency (RF) [96, 137] may carry intrinsic features of a wireless-enabled device, which is based on the physical structure and the materials used to build the wireless circuit (e.g. WiFi chipsets) for transmission. These features inherent in the physical layer [87, 138] of the devices may allow the unique identification of the device. Conventionally, the physical layer is implemented on the hardware level of the WiFi chipsets. As such, these features, which are based on the chipsets driver or firmware, may not be easily accessible and require the use of expensive hardware-software tools (signal analyzer) and high computing power to capture raw radio signals for processing [87]. However, there are three significant advantages of using RF for device fingerprinting [138]: (1) physical layer features are hard to be replicated, (2) individual features are based on hardware characteristics, and (3) they are easy to implement for real-time processing. Table 7 presents a list of key RF features used in the literature for DFP.

RF features set can be broadly categorized into the following types: I/Q-based, Fast Fourier Transformation (FFT) based, and spectrogram-based features, with different states of a signal required to be analyzed to extract significant characteristics of the RF to generate DFP. Fig. 7 depicts an abstract view of a signal with different states [146, 150, 152], e.g. transient-state (transition from off-state to on-state of a transmitter's signal during communication, which focuses on a short period of time) and steady-state (it follows immediately after the transient-state portion of a signal). I/Q-based features represent the time-domain signal characteristics, whilst FFT-based signal characteristics are extracted from the frequency-domain [145]. Basically, FFT transforms the time-domain signal into the frequency-domain to allow extraction of significant characteristics of the signal, which are not available in the time-domain, such as I/Q FFT [155,156]. On the other hand, spectrogram-based features not only provide the frequency-domain (converts the time-domain signal to the frequency-domain) characteristics but also reveal frequency-changing patterns over time [157].

3.4. Learning mechanism

In 1959 [156], Arthur Samuel first introduced the term machine learning (ML). It is a branch of artificial intelligence (AI), which uses three key factors: data, error quantifiers (measure current and ideal behaviours distance) and feedback mechanisms for learning patterns or unique features to improve the decision-making process [156, 157,158]. One of the key objectives of AI is to construct an intelligent system for performing different tasks, including complex problem-solving (such as deoxyribonucleic acid (DNA) sequencing [160] and Covid-19 medication [161]), decision making (such as identifying network-connected devices [19] and anomaly detection [162]), and mimicking human interactions (such as in robotics [163]). AI is commonly designed to perform complex computation and mechanical tasks more efficiently and accurately within a short period of time as compared to a human being [156, 157]. Deep learning (DL) is a sub-category of ML approach and is considered the soul of modern AI. It is formed based on neural network architecture. DL models learn multilevel representations from raw or process data as input.

Representation learning (or features learning) is a set of techniques that allows a system to identify required representations automatically for prediction or classification from input data [164, 165]. Neural network architectures have been used for supervised,

Table 7
Categories of Radio Signal features used for device fingerprinting.

	Categories	Features	Sampling Rate	Number of points/ values	DFP	Source
Radio Signal	I/Q-based	I/Q samples [d, g, j, n, o, q]		1000 [a, n]	Vector [a, b, c, d, e, f, g, h, I, j, k, l, m, n, o, p, r, s, t]	a
		[ap] I/Q imbalance [e, f, I, r]	[d, q] 5 MS/s	[fd] 159,901 [b]		b
		DC offset [f, i]	[h, j] 1.92 MS/s	1024 [c,		c
		Signal spectrum [a]	[k] 1 MS/s	2048 [e]		d
		Amplitude [b, m, s, t]	[o] 20 MS/s	1200 [d]		e
		Signal error [c]	[p] 10 MS/s	256 [f, g, h]		f
		Channel information [i]	[l] 24 MHz	10,000 [j, m]		g
		LO frequency offset [I, p, s]	[s] 20 GS/s	35,000 [l]		h
		Phase offset [p, s]	[t] 25.6 – 28 MS/ s	4096 [q, t]		i
		Power amplifier [r]		600 [r]		j
	FFT-based	Amplitude [h]				k
		Phase [h]				l
		FFT [h, l]				m
	Spectrogram-based	Logarithmic compression (Mag) [k]				n
		CFO [k]				o
						p
						q
						r
						s
						t

Note: [a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t] – Represents relationship among filed values, fd – feature dimension, FFT – Fast Fourier Transformation, MS/s – Mega samples per second, GS/s – Giga samples per second, LO – Local oscillator, ap – Amplitude and phase, I/Q – In-phase and quadrature, CFO – Carrier frequency offset, MHz - Megahertz, I/Q samples – Amplitude, phase, and frequency, Mag – Magnitudes, Sampling Rate – Unit of samples per second, Number of points/values – A total number of sampling points used to represent a sample size

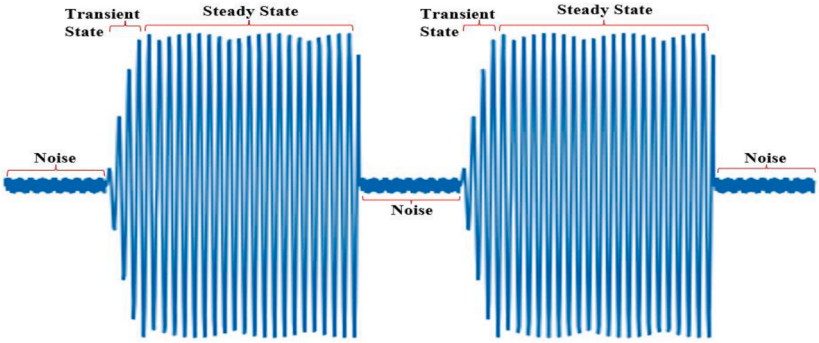


Fig. 7. An abstract view of different states of a radio frequency signal.

semi-supervised, and unsupervised learning approaches. Researchers have designed different models of neural network architectures, including convolutional neural network (CNN), recurrent neural network (RNN) – Vanilla RNN, RNN-Long short-term memory (LSTM) and RNN-Gated recurrent unit (GRU), autoencoder, and multilayer perceptron (MLP), for solving different types of problems and improve model performances. DL architectures have been used for a wide range of applications, including image recognition [166, 167], speech recognition [168, 169], anomaly detection [21, 170], device identification [19, 74, 171], robotics [172], language translation [173, 174], medical science [175], recommendation system [164], financial market prediction [176], due to its capability of solving complex tasks in different domains, e.g. science, business. All these learning mechanisms are depicted in Fig. 8, with key characteristics and applications [177,178].

Conventional ML algorithms have limited capability in processing data from raw input, with human inputs required during the data processing and feature engineering phases to learn device-specific patterns (or features) from input data [165]. Indeed, it is very challenging to perform all these tasks manually due to a large number of IoT devices with different characteristics that are connected to cyberspace. Within this context, DL techniques have significant advantages as compared to traditional ML techniques [46]: (1) deep learning architectures, such as convolutional neural network (CNN) and long short-term memory (LSTM), allow automatic learning of useful features or patterns from raw input data, (2) they can identify complex non-linear relationships between features set, and (3) DL architectures are more suitable for big-data analysis. The efficient learning capability of DL may assist in learning users' as well as devices' behaviours based on the analysis of communication traffic traces. Researchers have used both traditional ML and DL algorithms in the domain of the IoT ecosystem for solving different problems, including device fingerprinting and traffic classification.

A basic device fingerprinting architecture (or essential sections of a DFP scheme) is depicted in Fig. 9. For a DFP scheme, network data (packets, MAC frames, or radio signals) can be collected, either actively or passively, using different types of hardware-software

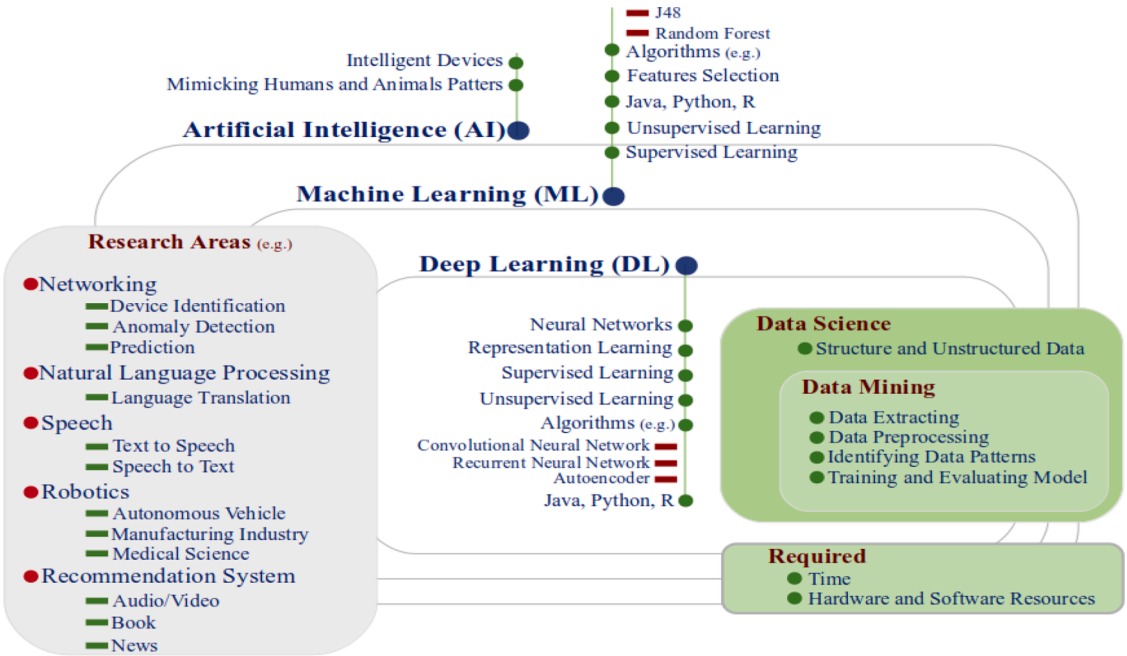


Fig. 8. Categories of learning algorithms [53, 159, 160].

resources from the network-connected devices. Then, insignificant data (missing or noisy data) are removed from the captured dataset to give a cleaner dataset, with the data converted into different forms (data scaling – transforming data into a specific range, normalization – changing data distribution into a normalized form, attribute construction – a new set of attributes is created from an existing dataset, discretization – a set of data intervals are created from a continuous data) according to the proposed fingerprinting methods. Subsequently, in the feature engineering step, either features/attributes (such as network packet features and MAC frame features [179, 180]) are extracted from the pre-processed dataset and evaluated using different attribute evaluators, or the raw dataset (such as raw I/Q samples) are utilized for further processing. DL approaches can learn significant attributes automatically from raw input data based on neural networks with representation learning [46, 165]. Finally, different ML classification models may be used to classify either devices or traffic types (benign or malicious traffic types).

3.4.1. Machine learning-based DFP

ML is an advanced form of learning technique based on observations (or input) of data by automatically learning patterns, such as statistical regularities, to assist the decision-making process and enhance the overall classification task. The process can analyze a massive amount of data, either offline or online, to produce better results in the context of different research problems, including device identification, anomaly detection, application detection, operating systems (OS) identification, and location tracking [19, 182, 183]. Traditional ML-DFP offers key advantages by using commodity hardware and software tools to monitor communication traffic traces: packets, frames, and radio signals, in order to improve the network management process and security. Table 8 presents some of the existing ML-DFP models with brief information on the models.

From the literature study in the domain of DFP, it has been observed that numerous ML-based DFP schemes have been proposed by many researchers; these DFP models have demonstrated high classification performances on different datasets (either public or private datasets), with some on datasets containing both IoT and non-IoT devices from different manufacturers. However, it has been observed that classification performances may be low due to the following reasons – (1) using an experimental dataset consisting of similar types of devices from the same manufacturers, (2) the proposed DFP models are not using appropriate device-specific features for generating fingerprints, and (3) choosing an unsuitable ML algorithm from the wide varieties of ML algorithms for the classifications task. It has also been observed that researchers have used different types of ML algorithms, particularly J48, Random Forest (RF), and Support Vector Machine (SVM), for classifying devices or network traffic traces (normal and malicious traffic traces), using different sets of features derived from either network packet(s) or radio signal(s). On the other hand, the IEEE 802.1x MAC frame has not been comparatively studied in much depth to identify device-specific features that can be used for fingerprinting.

3.4.2. Deep learning-based DFP

In this study, some of the significant DL-based DFP models for device classification/identification (IoT and non-IoT devices), and anomaly detection (normal and malicious traffic traces classification) using fingerprints, are provided. A brief description of the existing DL-DFP models is presented in Table 9.

DL-based DFP models have been proposed by many researchers by utilizing the three categories of communication traffic: network packets, MAC frames, and radio signals. Either raw or processed data (captured network traffic) may be used as input in the form of a vector or image to the neural network (NN) architecture for the classification task, with hidden layers automatically extracting significant features. It has been observed that among all the different types of NN architectures, many researchers [80, 145, 203–205] have opted to use CNN-based device fingerprinting models for classifying network-connected IoT and non-IoT devices. CNNs, both

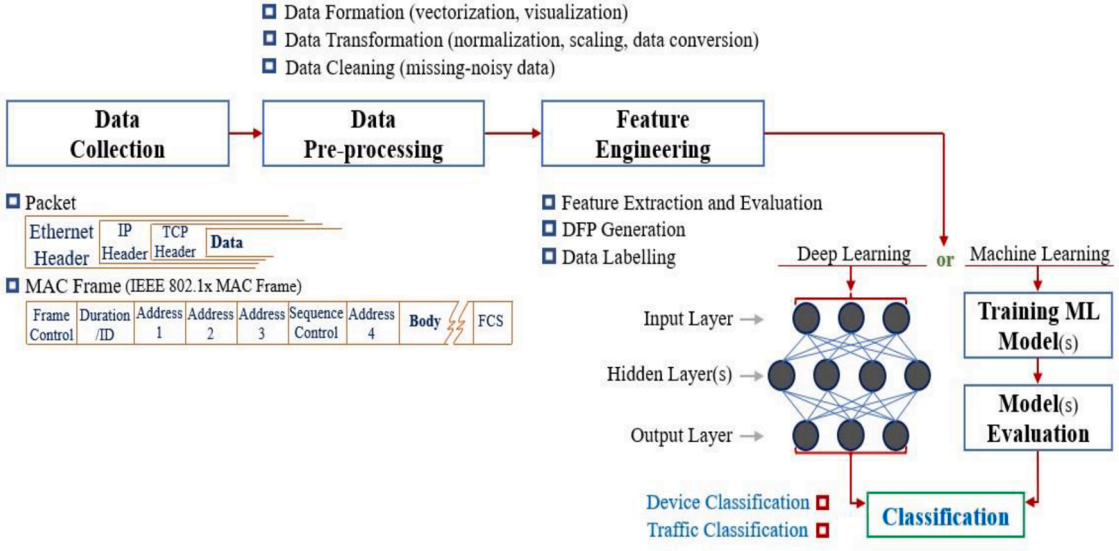


Fig. 9. The basic architecture of a device fingerprinting (DFP) scheme [125, 126, 181].

Table 8
Machine learning-based device fingerprinting approaches.

Source	Year	Problem	A/P	Packet/ Frame/ RS	Features	DFP	Devices/ Transmitters	Dataset	Accuracy	Tool/ Algorithm
Network Packet										
[115]	2017	**Device Identification**, Device category	P	200	2 (Statistics)	180	9	Private	90%	Weka (SVM)
[109]	2017	**Identification** ^{IvN}	P	Flows (K_n)	2 (Statistics)	2	12	Private	99.28%	–
[19]	2017	**Identification**, Security Enforcement	P	12	23 (Header)	12 × 23	27	Public ^{D1}	81.5%	– (RF)
[105]	2017	**Identification** ^{IvN}	P	Flows (K_n)	12 (Statistics)	12	21	Public ^{D2}	95%	Weka (RF)
[106]	2018	**Identification**, Device category	P	5	20 (Header, payload)	5 × 20	14	Private	99%	Scikit-learn (GB)
[8]	2018	**Identification** ^{IvN}	P	Flows (K_n)	8 (Statistics)	–	28	Public ^{D2}	99%	Weka (RF), Joy tool
[112]	2018	**Identification**	P	12	9 (Statistics, values)	9	53	Public ^{D5}	76.15%	– (RF)
[64]	2018	**Authentication**	P	K_n	9 (Statistics)	9	12	Private	100%	– (RF)
[101]	2018	**Device identification**, Traffic classification	P	Flows (K_n)	5 (Statistics)	13	20	Public ^{D2}	99%	– (RF)
[184]	2018	**Identification**	P	K_n (15 Min)	40 (Statistics)	40	16	Public	98%	– (RF)
[185]	2019	**Identification**	P	K_n (15 Min)	94 (Statistics)	94	15	Private	98.1%	– (Clas. tree)
[20]	2019	**Identification**	P	20	23 (Statistics, values)	166	10	Public ^{D1}	93.2%	– (TSMC-SVM)
[9]	2019	**Identification** ^{IvN}, Event identification	P	K_n (1 Sec)	3 (Statistics)	3	28	Public ^{D2}	96% ^{T} 99% ^{IvN}	Scikit-learn (RF)
[75]	2019	**Identification**	P	1	212 (Header)	1 × 212	23	Public ^{D1}	82.0%	Weka (PART)
[4]	2019	**Identification**	P	K_n (30 Min)	33 (Statistics)	33	41	Private	98.2%	– (KNN)
[102]	2019	**Identification** ^{IvN}	P	16	39 (Statistics)	39	7	Private	87.40%	Scikit-learn (RF)
[186]	2019	**Identification**	P	40-Flows (40 Min)	11 (Statistics)	11	19	Private	98.4%	Scikit-learn (RF)
[110]	2020	**Identification** ^{IvN}	P	K_n	12 (Statistics/ Values)	12	22	Private	99.99%	– (RF)
[74]	2020	**Identification**	P	1	161, 86 (Values)	161 ^{D1}, 86 ^{D1}	27 ^{D1}, 19 ^{D2}	Public ^{D1} Public ^{D2}	83.35% ^{D1} 97.78% ^{D2}	Weka (J48)
[187]	2020	**Identification** (ZigBee, Z-Wave)	P	K_n	IAT (Values)	N AUC (each bin)	39	Private	95% $^{+}$	Weka
[188]	2020	**Device identification** ^{a}, **Device categorization** ^{b}	P	Flows (K_n)	19 (Statistics)	19	43	Private	80% ^{a} 90% ^{b}	Scikit-learn
[121]	2020	**Identification**	P	Flows (K_n)	18 (Bin, Nm)	18	28	Public ^{D1} Private	97%	Scikit-learn (DT)
[189]	2020	**Identification** (Normal or anomalous traffic)	P	K_n (5 Min)	6 (Entropy)	6	5	Private	94% (50 classes)	Weka (RF)
[111]	2021	**Identification** (Four classes)	P	Flows (K_n)	13 (Statistics)	13	41	Private	99.79%	Weka (LB)
[119]	2021	**Identification** (Normal traffic)	P	1	2 (M values)	2	6	Private	92.62%	Scikit-learn (SVM)
[190]	2021	**Identification**	P	Flows (K_n)	N (Statistics)	N	21	Public ^{D2}	99.6%	Orange-ML (RF)
[123]	2021	**Identification** (Normal or anomalous traffic)	P	K_n (5 Min)	6 (Entropy)	6	5	Private	94% (50 classes)	Weka (RF)
[191]	2021	**Identification** (IoT and smartphones)	P	K_n (1 Hr)	22 (Statistics)	22	24,800	Private	95.86%	– (RF)
[192]	2021	**Identification**	P	K_n	517 (Statistics)	101	27	Public ^{D1}	92.5%	Scikit-learn (SVM)
[124]	2022	**Identification**	P	1	24 (Header)	24	8	Public ^{D3}	95.0%	Weka (J48)
[125]	2022	**Identification**	P	1	9 (Header)	9	12	Public ^{D3}	96.6%	Weka (Bagging)
[193]	2022	**Identification**	P	Flows (K_n)	83 (Statistics)	83	13	Private	78.27%	Scikit-learn (SVM)
[194]	2022	**Identification**	P	Flows (K_n)	30 (Values)	30	19	Private, Public ^{D1}	98.35%	GNB

(*continued on next page*)

Table 8 (*continued*)

Source	Year	Problem	A/P	Packet/ Frame/ RS	Features	DFP	Devices/ Transmitters	Dataset	Accuracy	Tool/ Algorithm
IEEE 802.1x MAC Frame										
–	–	–	–	–	–	–	–	–	–	–
Radio Signal										
[138]	2019	**Identification** [a], Attack Detection	P	Signal (SNR 15dB)	50 (Statistics)	50	10	Private	100% [a]	KNN
[146]	2020	**Identification** (Transient state)	P	Signal (SNR 15dB)	35,000	35,000	10	Private	100%	SVM
[147]	2020	**Device Authentication, Rogue Device Identification**	P	Signal (SNR 25dB)	10,000	10,000	10	Private	99%	SVDD (KNN)
[153]	2020	**Identification** (Transient state)	P	Signal (SNR 5-10dB)	–	27 (vet.)	20	Private	97.1%	SVM
[149]	2021	**Identification** (Steady state)	P	Signal (SNR 9-30dB)	–	348	10	Private	95.6%	Sub-Dis

Note: IoT Sentinel [19] – D1, UNSW [8] – D2, D-Link [84] – D3, LSIF [91] – D4, Intel Lab Data [112] – D5, Active – A, Passive – P, Radio Signal – RS, IoT vs Non-IoT – IvN, Packet – K, Frame – F, Number of packets - n, Number of features -N, Random Forest - RF, Gradient Boosting – GB, Support Vector Machine - SVM, Decision Tree – DT, Second – Sec, Minute – Min, Hour – Hr, IoT – T, LogitBoost – LB, Classification – Clas, Over - +, Area under the curve – AUC, Measurement – M, [a, b] – Represents relationship among filed values, Binary – Bin, Numerical value – Nm, Signal-to-noise ratio – SNR, Support vector data description - SVDD, K nearest neighbour – KNN, Subspace Discriminant – Sub-Dis, Vector – vet, Gaussian Naive Bayes - GNB

CNN and deep-CNN, are more suitable as compared to any other types of NN architectures [206] due to their ability to learn spatial as well as temporal dependency of features from images or vectors using different filtering techniques [207].

3.4.3. Alternative DFP approaches

Researchers in the DFP domain have also proposed different types of DFP methods based on various mathematical functions [17, 91, 116, 118, 129, 131], including hash, similarity and probability values, for classifying and identifying devices from their communication traffic characteristics. Table 10 presents a brief description of DFP schemes, other than those which use ML and DL algorithms. Similar to previous approaches, alternative DFP models have also been designed by utilizing the three categories of communication traffic: network packet, IEEE 802.1x MAC Frame, and radio signal. Researchers have demonstrated that the alternative DFP approaches are also able to give good classification performances using different datasets.

4. uture of IoT technologies

In the era of IoT, different technological developments have been incorporated into different objects and applications, requiring complex communication structures with different protocols for providing different services to end-users over the networks. Indeed, there is a growing trend in integrating sensors and sensor-based applications [13] with the cyber-physical system (CPS). In the near future, the expected increase in usage of IoT devices for various applications will impose new challenges to meet the demand for faster, simpler, secure, and scalable network architectures [209]. Thus far, different types of communication technologies have been utilized, including WiFi [19], ZigBee [187], BLE [64, 210], Z-Wave [19], and Ethernet [115], for short-range communication in an IoT network. Similarly, for long-range communication, different technologies, including cellular network – a global system for mobile communication (GSM) [211], long-term evolution (LTE) [212], 4th generation (4G) [213], narrowband-IoT (NB-IoT) [214], long-range (LoRa) [215, 216], and Sigfox [217], have been introduced for IoT networks.

All of these communication technologies have some limitations in terms of security, coverage, data rate, energy, latency, and reliability; despite their wide range of benefits in the development of IoT, particularly the 5th generation (5G) and next-generation technologies. The 3rd generation partnership project (3GPP) is a consortium of 7 standard organizations: ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC, as listed in Table 11, for developing protocols for mobile telecommunications [218]. It provides a complete description of the core network, radio access, and service capabilities, along with other inter-networking technologies to support the 3GPP networks. The first phase of 5G specifications has been published in Release 15 (3GPP), and new features and services are incorporated to enhance the 5G technologies [160, 200, 201].

Enhanced mobile broadband (eMBB), massive machine-type communications (mMTC) and ultra-low latency communications (URLLC) are the key advancements of the 5th generation technologies [219,220], as presented in Fig. 10, and these advancements are not available in other technologies [221, 222]. The technology presents a basic change in the wireless ecosystem, including high speed, low latency, high data rate (bandwidth), and energy-efficient connectivity for supporting the future of IoT and mobile technologies. Oxford Economics has estimated that the 5G technology will contribute to global gross domestic product (GDP) from $1.4 trillion to $3.5 trillion over the next 10-15 years [223]. The emerging development of IoT and 5G technologies are driving toward 5G-enabled IoT devices [224]. Arthur D. Little [225] has predicted that the value of 5G-enabled IoT will reach about $1.5 trillion by the year 2030.

Table 9
Deep learning-based device fingerprinting approaches.

Source	Year	Problem	A/P	Packet/ Frame/ RS	Features	Devices/ Transmitters	Dataset	Accuracy	DL
Network Packet									
[107]	2014	**Identification**	A, P	Pkt_p	IAT (Image)	37	Public [D1] Public [D2]	95% [D1] 99% [D2]	ANN
[195]	2018	**Identification** (Category)	P	Pkt_p (5 Min)	6 (Values)	15 (4 Categories)	Public [D3]	74.8%	LSTM- CNN
[196]	2018	**Identification**	P	100	IAT (Image)	2	Private	86.7%	CNN
[108]	2019	**Identification** [IvN]	P	Pkt_p	TCP-flow (50 samples)	28 [D3], 72	Public [D3] Private	66% [D3] 83%	LSTM, Auto
[122]	2020	**Identification**	P	10	21 (Values)	31 [D4], 21 [D3]	Public [D4], Public [D3]	60.7% [D4] 99% [D3]	LSTM
[197]	2020	**Identification** [IvN]	P	Pkt_p (30 Min)	96 (Values)	25	Public [D3]	99%	CNN
[100]	2020	**Identification**	P	Pkt_p (1 Session)	TCP session (Image)	10	Public [D3]	99.86%	CNN
[114]	2021	**Identification**	A, P	1000	IAT (Image)	58	Public [D1,D2]	97.7%	CNN
[198]	2021	**Identification**	p	Pkt_p	297 (Values)	10	Private	88.2%	LSTM (FL)
[199]	2022	**Identification**	p	1	Nilsimsa hash digests	22	Public [D7]	98%	MLP
[200]	2022	**Identification**	p	Pkt_p	5 (Values)	–	Public [D8,D9]	99.99%	CapsNet
IEEE 802.1x MAC Frame									
[132]	2017	**Identification**	P	F_f	Probe Request, Data frame, others – IAT [A], TT [B] (Image)	14	Public [D5]	92.3% [A] 95.8% [B]	ANN (BR)
[76]	2020	**Identification**	P	F_f	Probe Request	20	Private	99.98%	MLP
Radio Signal									
[79]	2018	**Identification**	P	Signal	Signal error	7	Private	92.29%	CNN
[142]	2018	**Identification**	P	Signal (SNR 50dB)	Raw I/Q sample	5	Private	98.00%	CNN
[143]	2018	**Identification**	P	Signal (SNR 15dB)	LO frequency offset, I/Q imbalance, DC offset, Channel info.	10,000	Private	99.00%	ANN
[144]	2018	**Identification**	P	Signal	I/Q sample	12	Private	98.70%	MST
[140, 201]	2018, 2020	**Identification**	P	Signal	I/Q imbalance, DC offset	16	Private	99.76%	CNN
[96]	2019	**Identification**	P	Signal	Raw I/Q sample	21	Public [D6]	99.90%	CNN
[202]	2019	**Identification** (Signal Classification)	P	Signal (SNR +9dB)	Radio signal (downlink signal)	3143 [a], 5157	Public	98.1% [a], 963%	In-ResNet
[141]	2020	**Identification**	P	Signal	Raw I/Q sample	16	Public	88.33%	ResNet
[139]	2020	**Identification** (Rogue Transmitter, **Known Transmitter** [a]	P	Signal (SNR 3dB)	I/Q imbalance	8	Private	99.90% 97.04% [a]	GAN, RNN-GRU [a]
[80]	2020	**Identification**	P	Signal (SNR *)	Spectrum (Magnitude and phase)	4	Private	99.99%	L-CNN
[148]	2020	**Identification**	P	Signal (SNR *)	I/Q sample	20	Private	99.56%	CNN
[154]	2020	**Identification**	P	Signal (SNR 25-28dB)	Raw amplitude	8	Private	83%	TL-LSTM
[145]	2021	**Identification**	P	Signal (SNR *)	Spectrogram, CFO	20	Private	96.44%	CNN
[151]	2021	**Identification**	P	Signal (SNR *)	I/Q sample	16	Private	98.11%	ESN
[152]	2021	**Identification**	P	Signal (SNR 20dB)	I/Q imbalance, PA	50	Private	99%	CNN (AlexNet)

Note: Deep learning – DL, Radio signal – RS, Active – A, Passive – P, Frame – F, Number of frames - f, number of packets - p , Packets – Pkt, Inter arrival time – IAT, Convolutional neural network – CNN, Artificial neural network – ANN, Multilayer perceptron – MLP, Long short-term memory – LSTM, Autoencoders – Auto, Bayesian Regularization – BR, IoT vs Non-IoT – IvN, Transmission Time – TT, Minute – Min, Federated Learning – FL, Generative adversarial network – GAN, Recurrent neural networks – RNN, Gated recurrent units – GRU, Isolated network dataset – D1, Campus network dataset – D2, UNSW – D3, IoT Sentinel – D4, Sigcomm2008 – D5, MonoRxSet – D6, LSIF – D7, [a] – represents relationship among the field values, Lightweight – L, Not defined clearly – *, Signal-to-noise ratio – SNR, Decibels – dB, In-phase and quadrature – IQ, Direct coupling – DC, Residual neural network – ResNet, Inception – In, Local oscillator – LO, Information – Info., Deep neural networks with multi-stage training – MST, Carrier-frequency offset – CFO, Echo state network – ESN, Power amplitude – PA, Transfer Learning – TL, Capsule Networks – CapsNet, GeoIP – D8, Alexa Rank – D9

Table 10
Alternative device fingerprinting approaches.

Source	Year	Problem	A/P	Packet/ Frame/ RS	Features	DFP	Devices	Dataset	Accuracy
Network Packet									
[116]	2018	**Identification**	P	Pkt_p	1	Server Names	25	Private	96%
[113]	2019	**Identification**	P	Pkt_p (30 Sec.)	3	20	11	Private	90%
[17]	2019	**Identification**	A, P	Pkt_p	98	BoW (Words)	33	Private	93.94%
[117]	2019	**Device Identification,** Vendor Identification	P	Pkt_p (24 Hr.)	1	List of Words	94	Private	94%
[208]	2019	**Identification** (Vendor, Series)	P	Pkt_p	SU	Word, Simhash	400	Private (Vendor [A], Service [B])	95.54% [A] 89.38% [B]
[91]	2020	**Identification**	P	Pkt_p	◆	Nilsimsa Hash	22	Public [D2]	93%
[118]	2020	**Identification**	A, P	Pkt_p	1	Server Names	25	Private	96%
[120]	2021	**Identification**	P	Pkt_p (10 min)	◆	Nilsimsa Hash	22	Public [D2]	94%
IEEE 802.1x MAC Frame									
[136]	2010	**Identification** (AP)	P	300 (LPM)	1	Values	4	Private	–
[134]	2010	**Identification** (AP)	P	100	4	Values	2	Private	–
[129]	2012	**Identification**, Similarity	P	50	5	Histogram	*	Private	◘
[130]	2013	**Device Identification**, Driver Identification	P	F_f	2	Histogram	9	Private	100%
[135]	2015	**Identification** (AP)	P	F_f (0.1 Sec)	1	Values	17	Private	100%
[87]	2017	**Identification**, Tracking	P	F_f	IE	Bit Entropy	10,000 [A], 100 [B]	Public [A, D1], Private [B]	33% [A] 80% [B]
[131]	2017	**Identification**	P	1	3	μ, σ, ε	300	Private	95%
[133]	2017	**Identification**	P	60	2	Histogram	4	Private	$75.87\%^{F.IAT}$ $67.82\%^{TT}$
Radio Signal									
[145]	2021	**Identification**	P	Signal (SNR *)	Spectrogram, CFO	Vector	20	Private	97.61%
[150]	2021	**Identification**	P	Signal (SNR 26dB)	I/Q components	Vector	54	Private	99.74% (SLOS2)

Note: Information elements tagged parameters - IE, Passive – P, Frame – F, Number of frames - f, Mean - μ, Standard deviation – σ, Energy - ε , Packet – Pkt, All values - ◆, Number of packets – p, Bag of Words – BoW, Second – Sec, Hour – Hr, Minute – min, Semi-structure and unstructured data – SU, Frame IAT – F.IAT, Transmission Time – TT, Access Point – AP, Linear Programming Method- LPM, Short range line-of-sight – SLOS, Represents relationship among filed values - [A, B], ◘ – compare individual network features performances, Glimps2015 – D1, LSIF – D2, * – Conf-1(188 devices), Conf-2 (97 devices), Office-1(158 devices), Office-2 (120 devices)

Table 11
3GPP organization partners [218].

Organization	Region
Association of Radio Industries and Businesses (ARIB)	Japan
Alliance for Telecommunications Industry Solutions (ATIS)	USA
China Communications Standards Association (CCSA)	China
European Telecommunications Standards Institute (ETSI)	Europe
Telecommunications Standards Development Society (TSDSI)	India
Telecommunications Technology Association (TTA)	South Korea
Telecommunication Technology Committee (TTC)	Japan

5. Research challenges in IoT and DFP

In the era of the IoT ecosystem, a large number of smart computing and sensing devices are being connected daily to cyberspace to provide various services over the network. This technological revolution increases automation facilities and user convenience services; however, it also intensifies network security and privacy threats. Device fingerprinting is one of the approaches which may be used by network administrators or operators to improve the network security of a newly developed or existing system. Researchers have proposed different DFP schemes using different algorithms and feature sets to improve classification performances. Nevertheless, more intense research is required. There exists a wide variety of communication environments (short and long-range communication protocols), brought about by the sharp increase in the number and types of sensing smart devices with different services and capabilities. These different communication protocols brought about potential incompatibility issues of current DFP methods, requiring the development of new DFP schemes, which are not only efficient and reliable but also dynamic enough to be able to adapt to the different

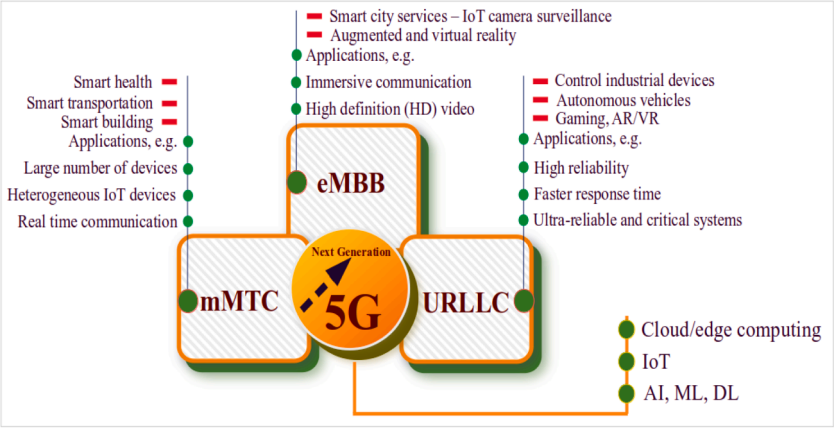


Fig. 10. 5th generation technology for IoT [160, 202].

communication protocols. Some of the key researcher challenges, in the context of DFP and IoT, are described in brief as follows: i. Definition a. A typical definition of the Internet of Things (IoT) is not clearly defined, and there is no commonly accepted definition of IoT by all the research communities and standard organizations. For instance, in references [53–55], well-established standard organizations defined IoT from different perspectives, although sensor and network connectivity are commonalities in both definitions. It is also essential to distinguish between IoT and non-IoT devices. In reference [196], some researchers have defined a smartphone as an IoT device; however, in references [8, 105, 125, 226], the researchers have identified a smartphone as a non-IoT device. ii. Communication Protocols a. Some IoT devices support multiple connectivities, including WiFi and Ethernet, with the devices changing their communication behaviours according to the available connectivity. For instance, radio signal features for DFP are only available for WiFi-enabled devices. b. Features extraction and fingerprint generation processes need to be varied based on the different types of connectivity: WiFi [19], Bluetooth [64], and ZigBee [187], since each connectivity method carries network information differently [227]. iii. Apps (Device configuration applications) a. A user requires multiple applications for configuring and accessing IoT devices from different manufacturers, for instance – *mydlink app* for D-Link IP cameras [70], *iCSee app* for 1080P PTZ Wifi IP Camera. There is no common apps available, which allows the configuration of various IoT devices either from the same or different manufacturers. iv. Datasets a. Datasets with a large number of IoT and non-IoT devices (various types) are not publicly available to the research community. b. Multiple datasets are required for analyzing IEEE 802.1x MAC frame features to generate IoT devices' fingerprints. The D-Link IoT dataset [84] (which consists of network packets and MAC frames) is currently available online for the research community for the analysis of MAC frames. In references [8, 85, 120], the researchers have published different IoT and non-IoT datasets (IoT Sentinel – 31 IoT devices, UNSW – 22 IoT and 7 non-IoT devices, and LSIF – 22 IoT Devices) for the research community. However, these datasets consist of a limited number of devices from different manufacturers, which may not cover a large number of IoT devices with different functionalities. v. Machine Learning Algorithms a. It is challenging to specify an ML algorithm suitable for DFP in terms of efficiency (less processing time) and accuracy (higher classification performances), with different classifiers showing different performances on the same dataset. In reference [125], the researchers have used different ML classifiers, including RF, J48, and RT, for the classification task with different datasets. It has been demonstrated that classification performances vary depending on the utilised classifiers on a similar dataset. b. Hyper-parameter tuning for different types of ML algorithms is challenging since each algorithm consists of a different set of properties, including confidence factor, batch size, iterations, and meta classifiers. vi. Deep Learning Algorithms a. Finding an optimal size of input data for training a DL-based DFP model, which is not only able to classify devices with higher accuracy but also efficiently within a short time scale. In reference [126], 1000 packet's information (IAT values) have been used to generate a unique fingerprint, whilst *n* number of packet's information (IAT values) from a specific time (bin size 300) frame have been used in reference [107]. Similarly, in reference [196], only 100 packets' information (IAT values) have been used for generating fingerprints. b. It is challenging to identify a set of appropriate hyper-parameters (number of hidden layers, filtering algorithm, number of epochs and activity function) suitable for DL architectures. vii. Specifying an optimal number of packets or MAC frames is required for generating fingerprints since some IoT devices generate a lot of packets (IP camera - Dropcam) within a short period of time, whilst some devices, such as Blipcare BP Meter [8, 87], generate very little packets. For instance, in reference [8], the authors have used n number packets (hourly basis) to generate fingerprints, whilst in references [85] and [75, 181, 228], the researchers have used 12 and 1 packet's information, respectively, for the classification task. viii. Identifying the optimal ratio (train:test datasets) of data sampling for training and testing DFP models with different datasets, including network packets, MAC frames, and radio signals datasets, whilst different ratios influence overall accuracy. ix. Finding an optimal range of signal–to–noise ratio (SNR) for radio signal fingerprinting imposes critical challenges for researchers. Many researchers have proposed different values: 3dB [139], 20dB [152], and 28dB [154], in their proposed DFP schemes for increasing classification accuracy.

6. Conclusion

The technological revolution has dramatically changed our daily life activities, making everyday work more convenient and smarter, from smart home services to industrial developments. After the Internet, IoT is one of the most significant technological advancements. Rightly so, it has been referred to as the future of the Internet. Resource-constraint IoT devices are integrated with other computing and non-computing devices, and traditional security approaches are not able to cope with the pursuing challenges. Device identification is one of the key challenges in improving network security. Traditional IP/MAC addresses-based identification has limitations to be used as unique identifiers, with IP/MAC addresses easily changeable using software and knowledge of networking. Additionally, these explicit identifiers are prone to spoofing attacks. Researchers have proposed different DFP methods based on implicit identifiers using similarity index, ML, or DL algorithms, by utilising different sources, including packets, frames, and radio signals, for the generation of device-specific features, to resolve this issue. But it remains a key challenge to design and develop an efficient and dynamic DFP model due to the rapid growth of technologies and usages of IoT devices. It is important that the DFP model does not require an excessively large number of packets to generate its features. Additionally, due to the resource-constrained nature of IoT devices, the features must not be overly complex to generate. Therefore, it is essential to study existing DFP works to find key research gaps and understand IoT architecture.

This study briefly discusses the basic terminologies of IoT technologies and applications to make them easily understandable. In the context of IoT network security, various aspects and challenges are also addressed related to device fingerprinting approaches in this paper, which is one of the key steps for securing network services and providing individual device security. With the growth of IoT technologies, more research is required in this field to make IoT-based services more scalable, efficient, secure, and dynamic. Overall, this study signifies critical research challenges and scopes regarding device fingerprinting approaches, communication protocols, and applications.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data Availability

No data was used for the research described in the article.

Acknowledgements

The authors are profoundly grateful to the Faculty of Integrated Technologies (FIT), Universiti Brunei Darussalam (UBD), for supporting this research work, as well as to UBD for awarding the UBD Graduate Scholarship (UGS) to the first author.

References

[1] S. K, M.S.O. Garcia-Morchon, draft-irtf-t2trg-iot-seccons-08 - Internet of Things (IoT) Security: State of the Art and Challenges, 2018. https://tools.ietf.org/html/draft-irtf-t2trg-iot-seccons-16 (accessed May 08, 2021).
[2] R.R. Chowdhury, M.A.A. Ansary, A secured mutual authentication protocol for RFID System, Int. J. Sci. Technol. Res. 3 (5) (2014) [Online]. Available: www.IJSTR.org.
[3] Y. Wang, J. Cao, Y. Zheng, Towards a low-cost software-defined UHF RFID system for distributed parallel sensing, IEEE Internet Things J (2021), https://doi.org/10.1109/JIOT.2021.3067379.
[4] S. Marchal, M. Miettinen, T.D. Nguyen, A.R. Sadeghi, N. Asokan, AuDI: toward autonomous IoT device-type identification using periodic communication, IEEE J. Sel. Areas Commun. 37 (6) (2019) 1402–1412, https://doi.org/10.1109/JSAC.2019.2904364.
[5] R.R. Chowdhury, Security in cloud computing, Int J Comput Appl 96 (15) (2014) 975–8887.
[6] L. Babun, H. Aksu, L. Ryan, K. Akkaya, E.S. Bentley, A.S. Uluagac, Z-IoT: passive device-class fingerprinting of ZigBee and Z-Wave IoT devices, in: ICC 2020-2020 IEEE International Conference on Communications (ICC), 2020, pp. 1–7.
[7] X. Chu, S. Nazir, K. Wang, Z. Leng, W. Khalil, Big data and its V's with IoT to develop sustainability, Sci. Program. (2021), https://doi.org/10.1155/2021/3780594. Hindawi Limited, 2021.
[8] A. Sivanathan, et al., Classifying IoT devices in smart environments using network traffic characteristics, IEEE Trans. Mob. Comput. 18 (8) (2018) 1745–1759, https://doi.org/10.1109/TMC.2018.2866249.
[9] A.J. Pinheiro, J. de M. Bezerra, C.A.P. Burgardt, D.R. Campelo, Identifying IoT devices and events based on packet length from encrypted traffic, Comput. Commun. 144 (May) (2019) 8–17, https://doi.org/10.1016/j.comcom.2019.05.012.
[10] Fortune Business Insights, "Internet of Things Market Size, Growth | IoT Industry Report [2020-2027]." https://www.fortunebusinessinsights.com/industry-reports/internet-of-things-iot-market-100307 (accessed May 13, 2021).
[11] L.S. Vailshery, IoT and Non-IoT Connections Worldwide 2010-2025, 2020. https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/ (accessed May 12, 2021).
[12] I.H.S. Markit, The Internet of Things: A Movement, not a Market, 2020.
[13] Libelium Comunicaciones Distribuidas S.L., 50 Sensor Applications for a Smarter World - Libelium, Libelium Comunicaciones Distribuidas S.L. (Sep. 09, 2020). https://www.libelium.com/libeliumworld/top-50-iot-sensor-applications-ranking/ (accessed May 08, 2021).
[14] C. Huang, S. Nazir, Analyzing and evaluating smart cities for IoT based on use cases using the analytic network process, Mob. Inf. Syst. 2021 (2021), https://doi.org/10.1155/2021/6674479.
[15] J. Hou, L. Qu, W. Shi, A survey on internet of things security from data perspectives, Comput. Netw. 148 (2019) 295–306.
[16] P. Sethi, S.R. Sarangi, Internet of things: architectures, protocols, and applications, J. Electric. Comput. Eng. 2017 (2017).

[17] N. Ammar, L. Noirie, S. Tixeuil, Network-protocol-based IoT device identification, in: 2019 Fourth International Conference on Fog and Mobile Edge Computing (FMEC), 2019, pp. 204–209, https://doi.org/10.1109/fmec.2019.8795318.

[18] B. Charyyev, M.H. Gunes, IoT Traffic flow identification using locality sensitive hashes, in: IEEE International Conference on Communications, 2020, https://doi.org/10.1109/ICC40277.2020.9148743 vol. 2020-June.

[19] M. Miettinen, S. Marchal, I. Hafeez, N. Asokan, A.-R. Sadeghi, S. Tarkoma, IoT Sentinel: automated device-type identification for security enforcement in IoT, in: 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS, 2017, pp. 2177–2184.

[20] Y. Song, Q. Huang, J. Yang, M. Fan, A. Hu, Y. Jiang, IoT device fingerprinting for relieving pressure in the access control, in: ACM International Conference Proceeding Series, 2019, https://doi.org/10.1145/3321408.3326671.

[21] M. Hasan, Md.M. Islam, M.I.I. Zarif, M.M.A. Hashem, Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches, Internet of Things 7 (Sep. 2019), 100059, https://doi.org/10.1016/j.iot.2019.100059.

[22] J. Choi, et al., Detecting and identifying faulty IoT devices in smart home with context extraction, in: 2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2018, pp. 610–621.

[23] S. Ramnath, A. Javali, B. Narang, P. Mishra, S.K. Routray, IoT based Localization and Tracking, 2017, https://doi.org/10.1109/ICIOTA.2017.8073629.

[24] Bassam J Mohd, Hayajneh, A.V Thaier, Vasilakos, A survey on lightweight block ciphers for low-resource devices: comparative study and open issues, J. Netw. Comput. Appl. 58 (2015) 73–93.

[25] M. Antonakakis, et al., Understanding the Mirai Botnet, 2017.

[26] Y. Tim, C. Dove, L. Kenney, Persirai: New IoT botnet targets IP cameras, Trend Micro (2017). https://www.trendmicro.com/en_us/research/17/e/persirai-new-internet-things-iot-botnet-targets-ip-cameras.html. accessed May 13, 2021.

[27] S. Edwards, I. Profetis, Hajime: Analysis of a decentralized internet worm for IoT devices, Rapidity Networks 16 (2016).

[28] "Technitium MAC Address Changer | A Freeware Utility To Spoof MAC Address Instantly." https://technitium.com/tmac/(accessed Jul. 06, 2021).

[29] N. Vlajic, M. Chowdhury, M. Litoiu, IP spoofing in and out of the public cloud: From policy to practice, Computers 8 (4) (2019) 81, https://doi.org/10.3390/computers8040081.

[30] Q. Xu, R. Zheng, W. Saad, Z. Han, Device fingerprinting in wireless networks: challenges and opportunities, IEEE Commun. Surv. Tut. 18 (1) (2016) 94–104, https://doi.org/10.1109/COMST.2015.2476338.

[31] M. M. Alani, *Guide to OSI and TCP/IP Models*. 2014.

[32] K. Yang, Q. Li, L. Sun, Towards automatic fingerprinting of IoT devices in the cyberspace, Comput. Netw. 148 (2019) 318–327, https://doi.org/10.1016/j.comnet.2018.11.013.

[33] "GeoIP2 Databases | MaxMind." https://www.maxmind.com/en/geoip2-databases (accessed Jul. 16, 2021).

[34] L. Atzori, A. Iera, G. Morabito, The Internet of Things: a survey, Comput. Netw. 54 (15) (2010) 2787–2805, https://doi.org/10.1016/j.comnet.2010.05.010.

[35] D. Miorandi, S. Sicari, F. De Pellegrini, I. Chlamtac, Internet of things: vision, applications and research challenges, Ad Hoc Netw. 10 (7) (2012) 1497–1516, https://doi.org/10.1016/j.adhoc.2012.02.016.

[36] J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, Internet of Things (IoT): a vision, architectural elements, and future directions, Fut. Gener. Comput. Syst. 29 (7) (2013) 1645–1660, https://doi.org/10.1016/j.future.2013.01.010.

[37] A. Whitmore, A. Agarwal, L.Da Xu, The Internet of Things—a survey of topics and trends, Inf. Syst. Front. 17 (2) (2015) 261–274, https://doi.org/10.1007/s10796-014-9489-2.

[38] S. Madakam, R. Ramaswamy, S. Tripathi, Internet of Things (IoT): a literature review, J. Comput. Commun. 03 (05) (2015) 164–173, https://doi.org/10.4236/jcc.2015.35021.

[39] P. Ryan and R. Watson, *Research Challenges for the Internet of Things: What Role Can OR Play?*, vol. 5, no. 1. 2017. doi: 10.3390/systems5010024.

[40] N. Poursafar, M.E.E. Alahi, S. Mukhopadhyay, Long-range wireless technologies for IoT applications: A review, in: Proceedings of the International Conference on Sensing Technology, ICST, 2018, pp. 1–6, https://doi.org/10.1109/ICSensT.2017.8304507, 2017-Decem.

[41] R. Mehta, J. Sahni, K. Khanna, Internet of Things: vision, applications and challenges, Procedia Comput. Sci. 132 (January) (2018) 1263–1269, https://doi.org/10.1016/j.procs.2018.05.042.

[42] S. Kumar, P. Tiwari, M. Zymbler, Internet of Things is a revolutionary approach for future technology enhancement: a review, J. Big Data 6 (1) (2019), https://doi.org/10.1186/s40537-019-0268-2.

[43] P. Laperdrix, N. Bielova, B. Baudry, G. Avoine, Browser fingerprinting: a survey, ACM Trans. Web 14 (2) (2020), https://doi.org/10.1145/3386040.

[44] N. Soltanieh, Y. Norouzi, Y. Yang, N.C. Karmakar, A review of radio frequency fingerprinting techniques, IEEE J. Radio Freq. Identif. 4 (3) (2020) 222–233, https://doi.org/10.1109/jrfid.2020.2968369.

[45] B. Liao, Y. Ali, S. Nazir, L. He, H.U. Khan, Security analysis of IoT devices by using mobile computing: a systematic literature review, IEEE Access 8 (2020) 120331–120350, https://doi.org/10.1109/ACCESS.2020.3006358. Institute of Electrical and Electronics Engineers Inc.

[46] Y. Yue, S. Li, P. Legg, F. Li, Deep learning-based security behaviour analysis in IoT environments: a survey, Secur. Commun. Netw. 2021 (2021).

[47] S.A. Bkheet, J.I. Agbinya, A review of identity methods of Internet of Things (IOT), Adv. Internet of Things 11 (04) (2021) 153–174, https://doi.org/10.4236/ait.2021.114011.

[48] H. Jmila, G. Blanc, M.R. Shahid, M. Lazrag, A survey of smart home IoT device classification using machine learning-based traffic analysis, IEEE Access 4 (2022), https://doi.org/10.1109/ACCESS.2017.

[49] A. Jagannath, J. Jagannath, P.S.P.V. Kumar, A comprehensive survey on radio frequency (RF) fingerprinting: traditional approaches. Deep Learning, and Open Challenges, 2022 [Online]. Available: http://arxiv.org/abs/2201.00680.

[50] CASAGRAS Project, CASAGRAS final report: RFID and the inclusive model for the Internet of Things, Sci. Am. 291 (4) (2009) 10–12.

[51] T.S.S.O. ITU, Y.2060: Overview of the Internet of Thhings, International Telecommunication Union, 2012.

[52] Internet of Things (IoT) preliminary report 2014, Iso 9 (2) (2015) 1–2.

[53] R. Minerva, A. Biru, D. Rotondi, Towards a definition of the Internet of Things (IoT), IEEE Internet Initiat. (2015) 1–86.

[54] Oracle, "What Is the Internet of Things (IoT)?" https://www.oracle.com/internet-of-things/what-is-iot/#:~:text=The%20Internet%20of%20Things%20(IoT)%20describes%20the%20network%20of%20physical,and%20systems%20over%20the%20internet.&text=Oracle%20has%20a%20network%20of%20device%20partners. (accessed Jul. 17, 2021).

[55] IETF, "IETF | Internet of things." https://www.ietf.org/topics/iot/(accessed Jul. 17, 2021).

[56] Gartner, "Definition of Internet Of Things (iot) - IT Glossary | Gartner." https://www.gartner.com/en/information-technology/glossary/internet-of-things (accessed Jul. 17, 2021).

[57] M.R. Abdmeziem, D. Tandjaoui, I. Romdhani, Architecting the internet of things: State of the art. Studies in Systems, Decision and Control, vol. 36, Springer International Publishing, 2016, pp. 55–75, https://doi.org/10.1007/978-3-319-22168-7_3.

[58] I.J.H. Reynolds, IOT Architecture: 3 Layers, 4 Stages Explained, 2020. https://www.zibtek.com/blog/iot-architecture/ (accessed May 13, 2021).

[59] S. Chen, H. Xu, D. Liu, B Hu, A vision of IoT: Applications, challenges, and opportunities with china perspective, IEEE Internet Things (2014).

[60] K.K. Patel, S.M. Patel, Internet of things-IOT: definition, characteristics, architecture, enabling technologies, application \& future challenges, Int. J. Eng. Sci. Comput. 6 (5) (2016).

[61] I. Mashal, O. Alsaryrah, T. Chung, C. Yang, WH Kuo, Choices for interaction with things on Internet and underlying issues, Ad Hoc Netw. (2015).

[62] R. Zaheer, S. Khan, Future internet: The Internet of Things architecture, possible applications and key challenges, ieeexplore.ieee.org (2012) 257–260, https://doi.org/10.1109/FIT.2012.53.

[63] M. Wu, T.J. Lu, F.Y. Ling, J. Sun, H.Y. Du, Research on the architecture of Internet of Things, in: ICACTE 2010 - 2010 3rd International Conference on Advanced Computer Theory and Engineering, Proceedings 5, 2010, https://doi.org/10.1109/ICACTE.2010.5579493.

[64] T. Gu, P. Mohapatra, BF-IoT: Securing the IoT networks via fingerprinting-based device authentication, in: Proceedings - 15th IEEE International Conference on Mobile Ad Hoc and Sensor Systems, MASS 2018, 2018, pp. 254–262, https://doi.org/10.1109/MASS.2018.00047.

[65] A.I. Ali, S.Z. Partal, S. Kepke, H.P. Partal, ZigBee and LoRa based wireless sensors for smart environment and IoT applications, in: Proceedings - 2019 IEEE 1st Global Power, Energy and Communication Conference, GPECOM 2019, 2019, pp. 19–23, https://doi.org/10.1109/GPECOM.2019.8778505.

[66] E. Sutjiredjeki, N.C. Basjaruddin, D.N. Fajrin, F. Noor, Development of NFC and IoT-enabled measurement devices for improving health care delivery of Indonesian children, J. Phys. Conf. Ser. 1450 (1) (2020) 0–6, https://doi.org/10.1088/1742-6596/1450/1/012072.

[67] A. Lazaro, R. Villarino, D. Girbau, A survey of NFC sensors based on energy harvesting for IoT applications, Sensors 18 (11) (2018), https://doi.org/10.3390/s18113746.

[68] Z. Ling, C. Gao, C. Sano, C. Toe, Z. Li, X. Fu, STIR: a smart and trustworthy IoT system interconnecting legacy IR devices, IEEE Internet Things J 7 (5) (2020) 3958–3967, https://doi.org/10.1109/JIOT.2019.2963767.

[69] M.R. Abdmeziem, D. Tandjaoui, I. Romdhani, Architecting the internet of things: state of the art. Robots and Sensor Clouds, Springer, 2016, pp. 55–75.

[70] D.-L. Corporation, "mydlink Lite." 2020.

[71] Volcano Technology Limited, "Smart Life - Smart Living - Apps on Google Play." https://play.google.com/store/apps/details?id=com.tuya.smartlife&hl=en&gl=US (accessed Jul. 17, 2021).

[72] A. Ahmad, et al., Towards an improved energy efficient and end-to-end secure protocol for iot healthcare applications, Secur. Commun. Netw. 2020 (2020), https://doi.org/10.1155/2020/8867792.

[73] H. Qinxia, S. Nazir, M. Li, H. Ullah Khan, W. Lianlian, S. Ahmad, AI-enabled sensing and decision-making for IoT systems, Complex 2021 (2021), https://doi.org/10.1155/2021/6616279. Hindawi Limited.

[74] R.R. Chowdhury, S. Aneja, N. Aneja, E. Abas, Network traffic analysis based IoT device identification, in: ACM International Conference Proceeding Series, 2020, pp. 79–89, https://doi.org/10.1145/3421537.3421545.

[75] A. Aksoy, M.H. Gunes, Automated iot device identification using network traffic, in: ICC 2019-2019 IEEE International Conference on Communications (ICC), 2019, pp. 1–7, https://doi.org/10.1109/ICC.2019.8761559.

[76] X. Gu, W. Wu, X. Gu, Z. Ling, M. Yang, A. Song, Probe request based device identification attack and defense, Sensors 20 (16) (2020) 1–17, https://doi.org/10.3390/s20164620.

[77] J. Martin, et al., A study of MAC address randomization in mobile devices and when it fails, ArXiv (2017), https://doi.org/10.1515/popets-2017-0054.

[78] Y. Tu, Z. Zhang, Y. Li, C. Wang, Y. Xiao, Research on the Internet of Things device recognition based on RF-fingerprinting, IEEE Access 7 (2019) 37426–37431.

[79] K. Merchant, S. Revay, G. Stantchev, B. Nousain, Deep learning for RF device fingerprinting in cognitive communication networks, IEEE J. Sel. Top. Sign. Proces. 12 (1) (2018) 160–167, https://doi.org/10.1109/JSTSP.2018.2796446.

[80] G. Qing, H. Wang, T. Zhang, Radio frequency fingerprinting identification for Zigbee via lightweight CNN, Phys. Commun. 44 (2021), 101250, https://doi.org/10.1016/j.phycom.2020.101250.

[81] W. Foundation, "Wireshark · Wireshark 3.4.5 and 3.2.13 Released," Apr. 21, 2021. https://www.wireshark.org/news/20210421.html (accessed Jul. 01, 2021).

[82] L.F. Sikos, Packet analysis for network forensics: A comprehensive survey, Forens. Sci. Int. 32 (2020), 200892, https://doi.org/10.1016/j.fsidi.2019.200892.

[83] Nmap.org, Nmap: the Network Mapper (7.90) - Free Security Scanner, 2019. https://nmap.org/ (accessed May 15, 2021).

[84] R.R. Chowdhury, S. Aneja, N. Aneja, P.E. Abas, Packet-level and IEEE 802.11 MAC frame-level Network Traffic Traces Data of the D-Link IoT devices, Data Brief 37 (2021), 107208, https://doi.org/10.1016/j.dib.2021.107208.

[85] M. Miettinen, S. Marchal, N. Asokan, IoT Sentinel: automated device-type identification for security enforcement in IoT, in: 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS), 2017, pp. 2177–2184, https://doi.org/10.1109/ICDCS.2017.284.

[86] Y. TU, et al., Large-scale real-world radio signal recognition with deep learning, Chin. J. Aeronaut. 35 (9) (Sep. 2022) 35–48, https://doi.org/10.1016/j.cja.2021.08.016.

[87] P. Robyns, B. Bonné, P. Quax, W. Lamotte, Noncooperative 802.11 MAC layer fingerprinting and tracking of mobile devices, Secur. Commun. Netw. 2017 (January) (2017), https://doi.org/10.1155/2017/6235484.

[88] Y. Ren, L. Peng, W. Bai, J. Yu, A practical study of channel influence on radio frequency fingerprint features, in: 2018 IEEE International Conference on Electronics and Communication Engineering, ICECE 2018, 2019, pp. 1–7, https://doi.org/10.1109/ICECOME.2018.8644931.

[89] G. Li, J. Yu, Y. Xing, A. Hu, Location-invariant physical layer identification approach for wifi devices, IEEE Access 7 (2019) 106974–106986, https://doi.org/10.1109/ACCESS.2019.2933242.

[90] S. Panchenko, A. Cheranev, Interception wideband FM signals with RTL-SDR, in: 2021 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT), May 2021, pp. 0222–0224, https://doi.org/10.1109/USBEREIT51232.2021.9455110.

[91] B. Charyyev, M.H. Gunes, IoT Traffic Flow Identification using Locality Sensitive Hashes, 2020.

[92] A.S. Uluagac, CRAWDAD dataset gatech/fingerprinting (v.2014-06-09), CRAWDAD Wirel. Netw. Data Arch. (2014), https://doi.org/10.15783/C78G67.

[93] E. A. M. A. K. S. P. V. C. & S. J. Barbera M. V., "CRAWDAD dataset sapienza/probe-requests (v. 2013-09-10)." 2013.

[94] A. Schulman, D. Levin, N. Spring, CRAWDAD dataset umd/sigcomm2008 (v.2009-03-02), CRAWDAD Wirel. Netw. Data Arch. (2009), https://doi.org/10.15783/C7J59R.

[95] G. Baldini, IoT Transient radio frequency signals, IEEE DataPort (2020). https://ieee-dataport.org/documents/iot-transient-radio-frequency-signals (accessed Aug. 14, 2021).

[96] C. Morin, L.S. Cardoso, J. Hoydis, J.M. Gorce, T. Vial, Transmitter Classification with Supervised Deep Learning, Social-Informatics and Telecommunications Engineering, LNICST 291 (2019) 73–86, https://doi.org/10.1007/978-3-030-25748-4_6.

[97] P. Ravali, A Comparative Evaluation of OSI and TCP/IP Models, Int. J. Sci. Res. (2015). https://www.ijsr.net/get_abstract.php?paper_id=SUB155737.

[98] P. Goyal, A. Goyal, Comparative study of two most popular packet sniffing tools-Tcpdump and Wireshark, in: Proceedings - 9th International Conference on Computational Intelligence and Communication Networks, CICN 2017, 2018, pp. 77–81, https://doi.org/10.1109/CICN.2017.8319360, 2018-Janua.

[99] A. Orebaugh, G. Ramirez, J. Burke, L. Pesce, J. Wright, G. Morris, Wireshark & Ethereal Network Protocol Analyzer Toolkit | ScienceDirect, Syngress (2006). https://www.sciencedirect.com/book/9781597490733/wireshark-and-ethereal-network-protocol-analyzer-toolkit#book-info (accessed Aug. 21, 2021).

[100] J. Kotak and Y. Elovici, "IoT Device Identification Using Deep Learning," *arXiv preprint arXiv:2002.11686*, 2020.

[101] M.R.P. Santos, R.M.C. Andrade, D.G. Gomes, A.C. Callado, An efficient approach for device identification and traffic classification in IoT ecosystems, Proc IEEE Symp Comput Commun (2018) 304–309, https://doi.org/10.1109/ISCC.2018.8538630, 2018-June.

[102] O. Salman, I.H. Elhajj, A. Chehab, A. Kayssi, A machine learning based framework for IoT device identification and abnormal traffic detection, Trans. Emerg. Telecomm. Technol. (August 2019) (2019) 1–15, https://doi.org/10.1002/ett.3743.

[103] J.E. Berthold, SONET and ATM. Optical Fiber Telecommunications IIIA: Third Edition, vol. A, 1997, pp. 13–41, https://doi.org/10.1016/B978-0-08-051316-4.50006-0.

[104] S.D. Meinrath, J.W. Losey, V.W. Pickard, Digital feudalism: enclosures and erasures from digital rights management to the digital divide, Adv. Comput. 81 (Jan. 2011) 237–287, https://doi.org/10.1016/B978-0-12-385514-5.00005-7.

[105] A. Sivanathan, et al., Characterizing and classifying IoT traffic in smart cities and campuses, in: 2017 IEEE Conference on Computer Communications Workshops, INFOCOM WKSHPS 2017, 2017, pp. 559–564, https://doi.org/10.1109/INFCOMW.2017.8116438.

[106] B. Bezawada, M. Bachani, J. Peterson, H. Shirazi, I. Ray, I. Ray, Behavioral fingerprinting of iot devices, in: Proceedings of the 2018 Workshop on Attacks and Solutions in Hardware Security, 2018, pp. 41–50.

[107] S.V. Radhakrishnan, A.S. Uluagac, R. Beyah, GTID: a technique for physical device and device type fingerprinting, IEEE Trans. Depend. Secure Comput. 12 (5) (2015) 519–532, https://doi.org/10.1109/TDSC.2014.2369033.

[108] J. Ortiz, C. Crawford, F. Le, DeviceMien: Network device behavior modeling for identifying unknown IoT devices, in: IoTDI 2019 - Proceedings of the 2019 Internet of Things Design and Implementation, 2019, pp. 106–117, https://doi.org/10.1145/3302505.3310073.

[109] Y. Meidan, et al., ProfilIoT: a machine learning approach for IoT device identification based on network traffic analysis, in: Proceedings of the Symposium on Applied Computing - SAC '17, 2017, pp. 506–509, https://doi.org/10.1145/3019612.3019878.

[110] K.R. Kumar, C. Hemanth, C.A. Kumar, K.M. Sahith, G.A. Prasanth, IoT device identification through network traffic analysis, Int. Res. J. Modern. Eng. Technol. Sci. 02 (06) (2020).
[111] I. Cvitić, D. Peraković, M. Periša, B.B. Gupta, Ensemble machine learning approach for classification of IoT devices in smart home (In Press), Int. J. Mach. Learn. Cybern. Ensemble (0123456789) (2021), https://doi.org/10.1007/s13042-020-01241-0.
[112] N. Yousefnezhad, M. Madhikermi, K. Framling, MeDI: measurement-based device identification framework for Internet of Things, in: Proceedings - IEEE 16th International Conference on Industrial Informatics, INDIN 2018, 2018, pp. 95–100, https://doi.org/10.1109/INDIN.2018.8472080.
[113] H. Noguchi, M. Kataoka, Y. Yamato, Device identification based on communication analysis for the internet of things, IEEE Access 7 (c) (2019) 52903–52912, https://doi.org/10.1109/ACCESS.2019.2910848.
[114] S. Aneja, N. Aneja, B. Bhargava, R.R. Chowdhury, Device Fingerprinting using Deep Convolutional Neural Networks 4951 (2021) 0–3.
[115] H. Kawai, S. Ata, N. Nakamura, I. Oka, Identification of communication devices from analysis of traffic patterns, in: 2017 13th International Conference on Network and Service Management, CNSM 2017, 2018, pp. 1–5, https://doi.org/10.23919/CNSM.2017.8256018, 2018-Janua.
[116] H. Guo, J. Heidemann, IP-based IoT device detection, in: Proceedings of the 2018 Workshop on IoT Security and Privacy, 2018, pp. 36–42.
[117] F. Le, J. Ortiz, D. Verma, and D. Kandlur, "Policy-Based Identification of IoT Devices' Vendor and Type by DNS Traffic Analysis," vol. 11550, S. Calo, E. Bertino, and D. Verma, Eds. Cham: Springer International Publishing, 2019, pp. 180–201. doi: 10.1007/978-3-030-17277-0_10.
[118] H. Guo, J. Heidemann, Detecting IoT devices in the internet, IEEE/ACM Trans. Netw. 28 (5) (2020) 2323–2336, https://doi.org/10.1109/TNET.2020.3009425.
[119] N. Yousefnezhad, A. Malhi, K. Främling, Automated IoT device identification based on full packet information using real-time network traffic, Sensors 21 (8) (2021), https://doi.org/10.3390/s21082660.
[120] B. Charyyev, M.H. Gunes, Locality-sensitive IoT network traffic fingerprinting for device identification, IEEE Internet Things J 8 (3) (2021) 1272–1281, https://doi.org/10.1109/JIOT.2020.3035087.
[121] N. Ammar, L. Noirie, S. Tixeuil, Autonomous identification of IoT device types based on a supervised classification, in: IEEE International Conference on Communications, 2020, https://doi.org/10.1109/ICC40277.2020.9148821, 2020-June.
[122] N. Najari, S. Berlemont, G. Lefebvre, S. Duffner, C. Garcia, Network traffic modeling for IoT-device re-identification, in: 2020 International Conference on Omni-Layer Intelligent Systems, COINS 2020, 2020, https://doi.org/10.1109/COINS49042.2020.9191376.
[123] H. Nguyen-An, T. Silverston, T. Yamazaki, T. Miyoshi, IoT Traffic: modeling and measurement experiments, IoT 2 (1) (2021) 140–162, https://doi.org/10.3390/iot2010008.
[124] R.R. Chowdhury, Packet-level and IEEE 802.11 MAC frame-level analysis for IoT device identification device identification, Turk. J. Electric. Eng. Comput. Sci. 30 (2022), https://doi.org/10.3906/elk-1300-0632.3915, 1–1.
[125] R.R. Chowdhury, A.C. Idris, P.E. Abas, Internet of Things device classification using transport and network layers communication traffic traces, Int. J. Comput. Digit. Syst. 12 (1) (2022), https://doi.org/10.12785/ijcds/120144, 2210–142.
[126] S. Aneja, N. Aneja, B.K. Bhargava, R.R. Chowdhury, Device fingerprinting using deep convolutional neural networks, Int. J. Commun. Netw. Distrib. Syst. 28 (2) (2022) 171–198, https://doi.org/10.1504/ijcnds.2022.10041894.
[127] V. Rao, K. v. Prema, Light-weight hashing method for user authentication in Internet-of-Things, Ad Hoc Netw. 89 (2019) 97–106, https://doi.org/10.1016/j.adhoc.2019.03.003.
[128] C. Matte, Wi-Fi Tracking: Fingerprinting Attacks and Counter-Measures, 2017.
[129] C. Neumann, O. Heen, S. Onno, An empirical study of passive 802.11 device fingerprinting, in: Proceedings - 32nd IEEE International Conference on Distributed Computing Systems Workshops, ICDCSW 2012, 2012, pp. 593–602, https://doi.org/10.1109/ICDCSW.2012.8.
[130] C. Maurice, S. Onno, C. Neumann, O. Heen, A. Francillon, Improving 802.11 fingerprinting of similar devices by cooperative fingerprinting, in: ICETE 2013 - 10th International Joint Conference on E-Business and Telecommunications; SECRYPT 2013 - 10th International Conference on Security and Cryptography, Proceedings, 2013, pp. 379–386, https://doi.org/10.5220/0004529103790386.
[131] A.K. Dalai, S.K. Jena, WDTF: a technique for wireless device type fingerprinting, Wirel. Pers. Commun. 97 (2) (2017) 1911–1928, https://doi.org/10.1007/s11277-017-4652-y.
[132] K. Kumar, A.K. Dalai, S.K. Panigrahy, S.K. Jena, An ANN based approach for wireless device fingerprinting, in: RTEICT 2017 - 2nd IEEE International Conference on Recent Trends in Electronics, Information and Communication Technology, Proceedings, 2017, pp. 1302–1307, https://doi.org/10.1109/RTEICT.2017.8256809, 2018-Janua.
[133] C. Shen, R. Lu, S. Samizade, L. He, Passive fingerprinting for wireless devices: a multi-level decision approach, in: 2017 IEEE International Conference on Identity, Security and Behavior Analysis, ISBA 2017, 2017, https://doi.org/10.1109/ISBA.2017.7947689.
[134] C. Arackaparambil, S. Bratus, A. Shubina, D. Kotz, On the reliability of wireless fingerprinting using clock skews, in: WiSec'10 - Proceedings of the 3rd ACM Conference on Wireless Network Security, 2010, pp. 169–174, https://doi.org/10.1145/1741866.1741894.
[135] B. Alotaibi, K. Elleithy, An empirical fingerprint framework to detect Rogue Access Points, in: 2015 IEEE Long Island Systems, Applications and Technology Conference, LISAT 2015, 2015, https://doi.org/10.1109/LISAT.2015.7160206.
[136] S. Jana, S.K. Kasera, On fast and accurate detection of unauthorized wireless access points using clock skews, IEEE Trans. Mob. Comput. 9 (3) (2010) 449–462, https://doi.org/10.1109/TMC.2009.145.
[137] G. Baldini, R. Giuliani, C. Gentile, G. Steri, Measures to address the lack of portability of the RF fingerprints for radiometric identification, in: 2018 9th IFIP International Conference on New Technologies, Mobility and Security, NTMS 2018 - Proceedings, 2018, pp. 1–5, https://doi.org/10.1109/NTMS.2018.8328703, 2018-Janua.
[138] Q. Tian, et al., New security mechanisms of high-reliability IoT communication based on radio frequency fingerprint, IEEE Internet Things J 6 (5) (2019) 7980–7987, https://doi.org/10.1109/JIOT.2019.2913627.
[139] D. Roy, T. Mukherjee, M. Chatterjee, E. Blasch, E. Pasiliao, RFAL: adversarial learning for RF transmitter identification and classification, IEEE Trans. Cogn. Commun. Netw. 6 (2) (2020) 783–801, https://doi.org/10.1109/TCCN.2019.2948919.
[140] K. Sankhe, M. Belgiovine, F. Zhou, S. Riyaz, S. Ioannidis, K. Chowdhury, ORACLE: Optimized Radio clAssification through Convolutional neuraL nEtworks, 2018 [Online]. Available: http://arxiv.org/abs/1812.01124.
[141] R.M. Dreifuerst, A. Graff, S. Kumar, C. Unger, D. Bray, End-to-End Radio Fingerprinting with Neural Networks, 2020 [Online]. Available: http://arxiv.org/abs/2010.05169.
[142] S. Riyaz, K. Sankhe, S. Ioannidis, K. Chowdhury, Deep learning convolutional neural networks for radio identification, IEEE Commun. Mag. 56 (9) (2018) 146–152, https://doi.org/10.1109/MCOM.2018.1800153.
[143] B. Chatterjee, S. Sen, D. Das, RF-PUF: IoT security enhancement through authentication of wireless nodes using in-situ machine learning, in: IEEE International Symposium on Hardware Oriented Security and Trust (HOST), 2018, pp. 205–208, https://doi.org/10.1109/HST.2018.8383916.
[144] K. Youssef, L. Bouchard, K. Haigh, J. Silovsky, B. Thapa, C. vander Valk, Machine learning approach to RF transmitter identification, IEEE J. Radio Freq. Identif. 2 (4) (Dec. 2018) 197–205, https://doi.org/10.1109/JRFID.2018.2880457.
[145] G. Shen, J. Zhang, A. Marshall, L. Peng, X. Wang, Radio frequency fingerprint identification for LoRa using spectrogram and CNN, in: Proceedings - IEEE INFOCOM, May 2021, https://doi.org/10.1109/INFOCOM42981.2021.9488793, 2021-May.
[146] n Y. Li, J. Jia, S. Wang, B. Ge, S. Mao, Wireless Device Identification Based on RadioFrequency Fingerprint Features, 2020.
[147] Q. Tian, Y. Lin, X. Guo, J. Wang, O. Alfarraj, A. Tolba, An identity authentication method of a miot device based on radio frequency (RF) fingerprint technology, Sensors 20 (4) (2020), https://doi.org/10.3390/s20041213.
[148] S. Wang, et al., Radio frequency fingerprint identification based on deep complex residual network, IEEE Access 8 (2020) 204417–204424, https://doi.org/10.1109/ACCESS.2020.3037206.
[149] S. Abbas, et al., Improving security of the Internet of Things via RF fingerprinting based device identification system, Neural Comput. Appl. (2021), https://doi.org/10.1007/s00521-021-06115-2.

[150] X. Zhou, A. Hu, G. Li, L. Peng, Y. Xing, J. Yu, A robust radio-frequency fingerprint extraction scheme for practical device recognition, IEEE Internet Things J. 8 (14) (Jul. 2021) 11276–11289, https://doi.org/10.1109/JIOT.2021.3051402.
[151] K. Bai, C. Thiem, N. McDonald, L. Loomis, Y. Yi, Toward intelligence in communication networks: a deep learning identification strategy for radio frequency fingerprints, in: Proceedings - International Symposium on Quality Electronic Design, ISQED, Apr. 2021, pp. 204–209, https://doi.org/10.1109/ISQED51717.2021.9424319, 2021-April.
[152] J. Zhang, R. Woods, M. Sandell, M. Valkama, A. Marshall, J. Cavallaro, Radio frequency fingerprint identification for narrowband systems, modelling and classification, IEEE Trans. Inf. Forensics Secur. 16 (2021) 3974–3987, https://doi.org/10.1109/TIFS.2021.3088008.
[153] A. Aghnaiya, Y. Dalveren, A. Kara, On the performance of variational mode decomposition-based radio frequency fingerprinting of bluetooth devices, Sensors 20 (6) (2020), https://doi.org/10.3390/s20061704.
[154] X. Wang, Y. Zhang, H. Zhang, Y. Li, X. Wei, Radio frequency signal identification using transfer learning based on LSTM, Circuits Syst. Signal Process. 39 (11) (2020) 5514–5528, https://doi.org/10.1007/s00034-020-01417-7.
[155] M. Köse, S. Ta\cscio\uglu, Z. Telatar, RF Fingerprinting of IoT devices based on transient energy spectrum, IEEE Access 7 (2019) 18715–18726.
[156] A. Al-Shawabka, et al., Exposing the Fingerprint: Dissecting the Impact of the Wireless Channel on Radio Fingerprinting, 2020, https://doi.org/10.1109/INFOCOM41043.2020.9155259.
[157] K. Choi, G. Fazekas, M. Sandler, and K. Cho, "A Comparison of Audio Signal Preprocessing Methods For Deep Neural Networks On Music Tagging," 2018. doi: 10.23919/EUSIPCO.2018.8553106.
[158] A.V Joshi, Machine Learning and Artificial Intelligence an Introduction 64 (1) (2020), https://doi.org/10.1007/978-3-030-26622-6.
[159] "What is Machine Learning? | IBM." https://www.ibm.com/cloud/learn/machine-learning (accessed Jul. 22, 2021).
[160] J.X. Zhang, et al., A deep learning model for predicting next-generation sequencing depth from DNA sequence, Nat. Commun. 12 (1) (Dec. 2021), https://doi.org/10.1038/s41467-021-24497-8.
[161] M. Ghaderzadeh, F. Asadi, Deep learning in the detection and diagnosis of COVID-19 using radiology modalities: a systematic review, J. Healthc. Eng. 2021 (2021), https://doi.org/10.1155/2021/6677314. Hindawi Limited.
[162] B.J. Radford, L.M. Apolonio, A.J. Trias, J.A. Simpson, Network Traffic Anomaly Detection Using Recurrent Neural Networks, 2018, pp. 1–7 [Online]. Available: http://arxiv.org/abs/1803.10769.
[163] R.A. Mouha, Deep learning for robotics, J. Data Anal. Inf. Process. 09 (02) (2021) 63–76, https://doi.org/10.4236/jdaip.2021.92005.
[164] S. Zhang, L. Yao, A. Sun, Y. Tay, Deep learning based recommender system: a survey and new perspectives, ACM Comput. Surv. 52 (1) (2019) 1–35, https://doi.org/10.1145/3285029.
[165] Y. LeCun, Y. Bengio, G. Hinton, Deep learning, Nature 521 (7553) (2015) 436–444.
[166] J.J. Tompson, A. Jain, Y. LeCun, C. Bregler, Joint training of a convolutional network and a graphical model for human pose estimation, Adv. Neural. Inf. Process Syst. 27 (2014) 1799–1807.
[167] S. Xie, A. Kirillov, R. Girshick, K. He, Exploring randomly wired neural networks for image recognition, in: Proceedings of the IEEE International Conference on Computer Vision, 2019, pp. 1284–1293.
[168] G. Hinton, et al., Deep neural networks for acoustic modeling in speech recognition: The shared views of four research groups, IEEE Signal Process Mag 29 (6) (2012) 82–97.
[169] M. Ravanelli, T. Parcollet, Y. Bengio, The pytorch-kaldi speech recognition toolkit, in: ICASSP 2019-2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2019, pp. 6465–6469.
[170] R.-H. Hwang, M.-C. Peng, C.-W. Huang, Detecting IoT malicious traffic based on autoencoder and convolutional neural network, in: 2019 IEEE Globecom Workshops (GC Wkshps), 2019, pp. 1–6.
[171] S. Jian, Tong, Bruno Costa Rendon, Emmanuel Ojuba, Nasim Soltani, Zifeng Wang, Kunal Sankhe, Andrey Gritsenko, Jennifer Dy, Kaushik Chowdhury, Ioannidis, Deep learning for RF fingerprinting: a massive experimental study, IEEE Internet Things Mag. 3 (2020) 50–57.
[172] J. Degrave, M. Hermans, J. Dambre, A differentiable physics engine for deep learning in robotics, Front. Neurorobot. 13 (2019) 6.
[173] E. Wali et al., "Is machine learning speaking my language? A critical look at the NLP-pipeline across 8 human languages," Jul. 2020.
[174] I. Sutskever, O. Vinyals, Q.V Le, Sequence to sequence learning with neural networks, Adv. Neural Inf. Process. Syst. 27 (2014) 3104–3112.
[175] H.Y. Xiong, et al., The human splicing code reveals new insights into the genetic determinants of disease, Science 347 (6218) (2015).
[176] T. Fischer, C. Krauss, Deep learning with long short-term memory networks for financial market predictions, Eur. J. Oper. Res. 270 (2) (2018) 654–669.
[177] I.H. Witten, E. Frank, M. a Hall, Data Mining: Practical Machine Learning Tools and Techniques (Google eBook), 2011.
[178] K. Shafique, B.A. Khawaja, F. Sabir, S. Qazi, M. Mustaqim, Internet of things (IoT) for next-generation smart systems: A review of current challenges, future trends and prospects for emerging 5G-IoT scenarios, IEEE Access 8 (2020) 23022–23040.
[179] A. Orebaugh, G. Ramirez, J. Burke, L. Pesce, J. Wright, G. Morris, Chapter 6–Wireless Sniffing with Wireshark. Wireshark and Ethereal Network Protocol Analyzer Toolkit, 2007, pp. 1–104.
[180] C. et al. Gerald, "D.2. tshark: Terminal-based Wireshark." 1998.
[181] R.R. Chowdhury, S. Aneja, N. Aneja, E. Abas, Network traffic analysis based IoT device identification, in: ACM International Conference Proceeding Series, 2020, pp. 79–89, https://doi.org/10.1145/3421537.3421545.
[182] Y. Liu, J. Wang, J. Li, S. Niu, H. Song, and S. Member, "Machine learning for the detection and identification of Internet of Things (IoT) devices : a survey," vol. 7, no. 5, pp. 1–23, 2020.
[183] T. Gu, Z. Fang, A. Abhishek, H. Fu, P. Hu, P. Mohapatra, IoTGaze: IoT security enforcement via wireless context analysis, Proceedings - IEEE INFOCOM (2020) 884–893, https://doi.org/10.1109/INFOCOM41043.2020.9155459, 2020-July.
[184] V. Thangavelu, D.M. Divakaran, R. Sairam, S.S. Bhunia, M. Gurusamy, DEFT: a distributed IoT fingerprinting technique, IEEE Internet Things J. 6 (1) (2019) 940–952, https://doi.org/10.1109/JIOT.2018.2865604.
[185] B.A. Desai, D.M. Divakaran, I. Nevat, G.W. Peter, M. Gurusamy, A feature-ranking framework for IoT device classification, in: 2019 11th International Conference on Communication Systems and Networks, COMSNETS 2019, 2019, pp. 64–71, https://doi.org/10.1109/COMSNETS.2019.8711210.
[186] L. Deng, Y. Feng, D. Chen, N. Rishe, IoTSpot: identifying the IoT devices using their anonymous network traffic data, in: Proceedings - IEEE Military Communications Conference MILCOM, 2019, pp. 1–6, https://doi.org/10.1109/MILCOM47813.2019.9020977, 2019-Novem.
[187] L. Babun, H. Aksu, L. Ryan, K. Akkaya, E.S. Bentley, A.S. Uluagac, Z-iot: passive device-class fingerprinting of zigbee and z-wave iot devices, in: ICC 2020-2020 IEEE International Conference on Communications (ICC), 2020, pp. 1–7.
[188] R. Kolcun, D.A. Popescu, A.M. Mandalari, R. Mortier, The case for retraining of ML models for IoT device identification at the edge, Assoc. Comput. Mach. 1 (1) (2020).
[189] H. Nguyen-An, T. Silverston, T. Yamazaki, T. Miyoshi, Entropy-based IoT devices identification, in: APNOMS 2020 - 2020 21st Asia-Pacific Network Operations and Management Symposium: Towards Service and Networking Intelligence for Humanity, 2020, pp. 73–78, https://doi.org/10.23919/APNOMS50412.2020.9236963.
[190] E. Ganesan, I.S. Hwang, A.T. Liem, M.S. Ab-Rahman, Sdn-enabled fiwi-iot smart environment network traffic classification using supervised ml models, Photonics 8 (6) (2021), https://doi.org/10.3390/photonics8060201.
[191] S. Hui, H. Wang, D. Xu, J. Wu, Y. Li, D. Jin, Distinguishing between smartphones and IoT devices via network traffic, IEEE Internet Things J. 4662 (c) (2021) 1–16, https://doi.org/10.1109/JIOT.2021.3078879.
[192] Q. Chen, Y. Song, A. Hu, J. Wang, Automated authentication of large-scale IoT devices with hybrid feature selection, Commun. Comput. Inf. Sci. 1424 (2021) 664–676, https://doi.org/10.1007/978-3-030-78621-2_55.
[193] Y. Wang, et al., IoT device identification using supervised machine learning, in: Digest of Technical Papers - IEEE International Conference on Consumer Electronics, 2022, https://doi.org/10.1109/ICCE53296.2022.9730354, 2022-January.

[194] V.A. Ferman, M.A. Tawfeeq, Early generation and detection of efficient IoT device fingerprints using machine learning, Int. J. Adv. Sci. Eng. Inf. Technol. 12 (1) (2022) 53–60, https://doi.org/10.18517/ijaseit.12.1.14349.
[195] L. Bia, L. Yao, S.S. Kanhere, X. Wang, Z. Yang, Automatic device classification from network traffic streams of Internet of Things, in: 2018 IEEE 43rd Conference on Local Computer Networks (LCN), 2018, pp. 1–9.
[196] S. Aneja, N. Aneja, M.S. Islam, IoT Device fingerprint using deep learning, in: Proceedings - 2018 IEEE International Conference on Internet of Things and Intelligence System, IOTAIS 2018, 2019, pp. 174–179, https://doi.org/10.1109/IOTAIS.2018.8600824.
[197] L. Fan, et al., An IoT device identification method based on semi-supervised learning, in: 16th International Conference on Network and Service Management, CNSM 2020, 2nd International Workshop on Analytics for Service and Application Management, AnServApp 2020 and 1st International Workshop on the Future Evolution of Internet Protocols, IPFutu, 2020, https://doi.org/10.23919/CNSM50824.2020.9269044.
[198] Z. He, et al., Edge device identification based on federated learning and network traffic feature engineering, IEEE Trans. Cogn. Commun. Netw. XX (XX) (2021) 1–12, https://doi.org/10.1109/TCCN.2021.3101239.
[199] J. Thom, N. Thom, S. Sengupta, E. Hand, Smart Recon: network traffic fingerprinting for IoT Device identification, in: 2022 IEEE 12th Annual Computing and Communication Workshop and Conference, CCWC 2022, 2022, pp. 72–79, https://doi.org/10.1109/CCWC54503.2022.9720739.
[200] H. Azath, M.Devi Mani, G.K.D. Prasanna Venkatesan, D. Sivakumar, J.P. Ananth, S. Kamalraj, Identification of IoT device from network traffic using artificial intelligence based capsule networks, Wirel. Pers. Commun. 123 (3) (Apr. 2022) 2227–2243, https://doi.org/10.1007/s11277-021-09236-y.
[201] K. Sankhe, et al., No radio left behind: radio fingerprinting through deep learning of physical-layer hardware impairments, IEEE Trans. Cogn. Commun. Netw. 6 (1) (2020) 165–178, https://doi.org/10.1109/TCCN.2019.2949308.
[202] S. Chen, S. Zheng, L. Yang, X. Yang, Deep learning for large-scale real-world ACARS and ADS-B radio signal classification, IEEE Access 7 (2019) 89256–89264, https://doi.org/10.1109/ACCESS.2019.2925569.
[203] W. Jo, S. Kim, C. Lee, T. Shon, Packet preprocessing in CNN-based network intrusion detection system, Electronics 9 (7) (2020) 1–15, https://doi.org/10.3390/electronics9071151.
[204] G. Baldini, R. Giuliani, An assessment of the impact of wireless interferences on IoT emitter identification using Time Frequency representations and CNN, in: 2019 Global IoT Summit (GIoTS), 2019, pp. 1–6, https://doi.org/10.1109/giots.2019.8766385.
[205] R. Mostafiz, M.S. Uddin, N.A. Alam, M.Mahfuz Reza, M.M. Rahman, Covid-19 detection in chest X-ray through random forest classifier using a hybridization of deep CNN and DWT optimized features, J. King Saud Univ. (xxxx) (2021), https://doi.org/10.1016/j.jksuci.2020.12.010.
[206] K. He, X. Zhang, S. Ren, J. Sun, Deep Residual Learning for Image Recognition, 2015 [Online]. Available: http://arxiv.org/abs/1512.03385.
[207] U. Kushwaha, S. Jha, B. Desai, Image filtering-techniques, algorithm and applications, GIS Sci. J. 7 (11) (2020) [Online]. Available: https://www.researchgate.net/publication/346583845.
[208] X. Wang, Y. Wang, X. Feng, H. Zhu, L. Sun, Y. Zou, IoTTracker: An Enhanced Engine for Discovering Internet-of-Thing Devices, 2019, pp. 1–9, https://doi.org/10.1109/wowmom.2019.8793012.
[209] H. Rahimi, A. Zibaeenejad, A.A. Safavi, A novel IoT architecture based on 5G-IoT and next generation technologies, in: 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), 2018, pp. 81–88.
[210] M. Nikodem, M. Bawiec, Experimental evaluation of advertisement-based bluetooth low energy communication, Sensors 20 (1) (2020) 107.
[211] P. Valsalan, T.A.B. Baomar, A.H.O. Baabood, IoT based health monitoring system, J. Critic. Rev. 7 (4) (2020) 739–743.
[212] H. He, H. Shan, A. Huang, Q. Ye, W. Zhuang, Edge-aided computing and transmission scheduling for LTE-U-Enabled IoT, IEEE Trans. Wirel. Commun. 19 (12) (2020) 7881–7896, https://doi.org/10.1109/TWC.2020.3017207.
[213] N. Kumar, R. Khanna, A compact multi-band multi-input multi-output antenna for 4G/5G and IoT devices using theory of characteristic modes, Int. J. RF Microwave Comput. Aided Eng. 30 (1) (2020) e22012.
[214] G. Alagarsamy, J. Shanthini, G. Naveen Balaji, A survey on technologies and challenges of LPWA for narrowband IoT. EAI/Springer Innovations in Communication and Computing, Springer Science and Business Media Deutschland GmbH, 2020, pp. 73–84, https://doi.org/10.1007/978-3-030-40037-8_5.
[215] V. Delafontaine, F. Schiano, G. Cocco, A. Rusu, and D. Floreano, "Drone-aided Localization in LoRa IoT Networks," *arXiv preprint arXiv:2004.03852*, 2020.
[216] A.M.C. Drăgulinescu, A.F. Manea, O. Fratu, A. Drăgulinescu, LoRa-based medical IoT system architecture and testbed, Wirel. Pers. Commun. (Mar. 2020) 1–23, https://doi.org/10.1007/s11277-020-07235-z.
[217] N. Poddar, S.Z. Khan, J. Mass, S.N. Srirama, Coverage Analysis of NB-IoT and Sigfox: Two Estonian University Campuses as a case study, in: 2020 International Wireless Communications and Mobile Computing, IWCMC 2020, Jun. 2020, pp. 1491–1497, https://doi.org/10.1109/IWCMC48107.2020.9148570.
[218] 3GPP, "About 3GPP Home." 2021.
[219] A. Ghosh, A. Maeder, M. Baker, D. Chandramouli, 5G evolution: a view on 5G cellular technology beyond 3GPP release 15, IEEE Access 7 (2019) 127639–127651.
[220] G. Rizzo, Internet of Things in the 5G era :opportunities and benefits for enterprises and consumers, IEEE J. Sel. Areas Commun. (November) (2019).
[221] S. Li, L.Da Xu, S. Zhao, 5G Internet of Things: a survey, J. Ind. Inf. Integr. 10 (2018) 1–9.
[222] M.A. Siddiqi, H. Yu, J. Joung, 5G ultra-reliable low-latency communication implementation challenges and operational issues with IoT devices, Electronics 8 (9) (2019) 981.
[223] O. Economics, The Economic Impact of Restricting Competition in 5G Network Equipment, 2019.
[224] G. mobile Suppliers Association and others, The road to 5G: Drivers, applications, requirements and technical development, A GSA Executive Report from Ericsson, Huawei and Qualcomm (2015).
[225] A. Lasku, H. Pichai, R. Axelsson Wadman, S. McDevitt, Realizing the Potential of the Internet of Things with 5G, 2020.
[226] A. Sivanathan, "IoT Behavioral Monitoring via Network Traffic Analysis," no. September, 2020, [Online]. Available: http://arxiv.org/abs/2001.10632.
[227] L. Ruiz-Garcia, P. Barreiro, J. Rodriguez-Bermejo, J.I. Robla, Review. Monitoring the intermodal, refrigerated transport of fruit using sensor networks, Spanish J. Agric. Res. 5 (2) (2007) 142–156, https://doi.org/10.5424/sjar/2007052-234. Ministerio de Agricultura Pesca y Alimentacion.
[228] A. Aksoy, S. Louis, M.H. Gunes, Operating system fingerprinting via automated network traffic analysis, in: 2017 IEEE Congress on Evolutionary Computation, CEC 2017 - Proceedings, 2017, pp. 2502–2509, https://doi.org/10.1109/CEC.2017.7969609.

Rajarshi Roy Chowdhury is currently pursuing his PhD in Systems Engineering under the Faculty of Integrated Technologies, Universiti Brunei Darussalam. He obtained his Master's degree in Computer Science from Universiti Sains Malaysia, Malaysia in 2012. Later, he joined Sylhet International University, Bangladesh, as a lecturer in 2012. His research interest is Internet of Things (IoT), wireless sensor networks, networking, data analysis, and machine learning.

Pg Dr Emeroylariffion Abas received his B.Eng. Information Systems Engineering from Imperial College, London in 2001, before obtaining his PhD Communication Systems in 2005 from the same institution. He is now working as an Assistant Professor in System Engineering, Faculty of Integrated Technologies, Universiti Brunei Darussalam. His present research interest are data analysis, security of info-communication systems and design of photonic crystal fiber in fiber optics communication.