Physical Security and Safety of IoT Equipment: A Survey of Recent Advances and Opportunities

Xing Yang, *Student Member, IEEE*, Lei Shu, *Senior Member, IEEE*, Ye Liu, *Member, IEEE*, Gerhard Petrus Hancke, *Senior Member, IEEE*, Mohamed Amine Ferrag, and Kai Huang

***Abstract*—The connectivity and intelligence of Internet of Things (IoT) equipment offer improved services, but several technical challenges have emerged in recent years that hinder the widespread application of IoT, e.g., security and safety. Cyber-security and privacy countermeasures are widely used in IoT equipment, and many studies have been conducted. However, an important aspect that is often overlooked in security literature is IoT equipment's physical security and safety, namely, preventing IoT equipment from vandalism and theft. Therefore, this article provides an overview of IoT equipment's physical security and safety to draw attention to new research opportunities in this area. Afterward, we discuss, among other aspects, antitheft and antivandalism schemes along with circuit and system design, additional sensing devices, biometry and behavior analysis, and tracking methods. Besides, we summarize the artificial intelligence solutions for the physical security and safety of IoT equipment. Finally, we conclude with four future research opportunities.**

Manuscript received July 14, 2021; revised October 10, 2021 and November 30, 2021; accepted January 4, 2022. Date of publication January 7, 2022; date of current version April 13, 2022. This work was supported in part by the National Natural Science Foundation of China under Grant 62072248, in part by the High-End Foreign Experts Recruitment Plan of the Ministry of Science and Technology China under Grant G2021145009L, in part by Jiangsu Modern Agricultural Machinery Equipment and Technology Demonstration and Promotion Project under Grant NJ2021-11, in part by the International Cooperation Capacity Enhancement Plan of Nanjing Agricultural University under Grant 2021-PY-10, and in part by China Scholarship Council (CSC) under Grant 202106850023. Paper no. TII-21-2981. *(Corresponding author: Lei Shu.)*

Xing Yang is with the College of Artificial Intelligence, Nanjing Agricultural University, Nanjing 210031, China, and also with the School of Engineering,University of Lincoln, LN67TS Lincoln, U.K. (e-mail: harryyangx@gmail.com).

Lei Shu is with the College of Artificial Intelligence, Nanjing Agricultural University, Nanjing 210031, China, and also with the School of Engineering, University of Lincoln, LN67TS Lincoln, U.K. (e-mail: lei.shu@njau.edu.cn).

Ye Liu is with College of Artificial Intelligence, Nanjing Agricultural University, Nanjing 210031, China (e-mail: yeliu@njau.edu.cn).

Gerhard Petrus Hancke is with the Department of Computer Science, City University of Hong Kong, Hong Kong (e-mail: gp.hancke@cityu.edu.hk).

Mohamed Amine Ferrag is with the Department of Computer Science, Guelma University, Guelma 24000, Algeria (e-mail: ferrag.mohamedamine@univ-guelma.dz).

Kai Huang is with the National Engineering and Technology Center for Information Agriculture, Nanjing Agricultural University, Nanjing 210095, China, and also with the School of Artificial Intelligence, Nanjing Agricultural University, Nanjing 210095, China (e-mail: kai_huang@njau.edu.cn).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TII.2022.3141408.

Digital Object Identifier 10.1109/TII.2022.3141408

***Index Terms*—Behavior analysis, deep learning, Internet of Things (IoT), physical security and safety.**

I. Introduction

BACKGROUND: A growing number of Artificial Intelligence (AI) chips, sensors, and wireless communication devices are embedded in traditional equipment. With more Internet of Things (IoT) devices, the number of smart devices will increase to 3.5 billion in 2024 [1], [2]. International Data Corporation predicted that the collective sum of the world's data will grow from 33 ZB in 2018 to 175 ZB in 2025, where 90 ZB of data will be created on IoT devices by 2025 [3]. To reduce data transmission and improve executive efficiency, part computing and storing functions are implemented in IoT equipment based on the edge computing concept, which enhances the potential value and importance of this equipment. However, IoT equipment is usually deployed in remote and insecure spaces, which indicates that attackers can easily access the devices and perform physical attacks. In general, physical attacks can be divided into signal/radio jamming, eavesdropping, node capture/tampering attack, node replication attack, environment tampering, and physical damage [4], [5]. Unlike other physical attacks, attackers perform physical damage and harm the IoT equipment directly by theft or vandalism rather than remote intrusion or interference. Theft and vandalism require attackers to reach areas containing IoT equipment; thus, this type of physical attack is hard to achieve. However, the rising number of smart devices, the popularity of edge computing technology, and increasing attention to cyber-security issues force attackers to benefit from the theft or vandalism of available IoT equipment. Theft and vandalism would result in abnormal operation of infrastructures [6]. For instance, underground cable theft costs the South African economy five billion annually and leads to interruptions of transportation and telecommunication [7]. In addition, losses of individual property caused by physical damage cannot be ignored, e.g., one out of ten US smartphone owners suffered from phone theft, and 68% of them cannot find their phone after being stolen [8]. In particular, physical damage may be a stepping stone for other attacks. By stealing IoT equipment, attackers can access credentials to the IoT system and then utilize other connected devices to cause physical harm to users [9], [10]. Consequently, IoT equipment must be sufficiently secure to prevent such attacks and reduce the impact of unexpected equipment failures on the whole system.

1551-3203 © 2022 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See https://www.ieee.org/publications/rights/index.html for more information.

Authorized licensed use limited to: Account Rajalakshmi Institute of Technology - Chennai. Downloaded on February 22,2023 at 07:25:32 UTC from IEEE Xplore. Restrictions apply.

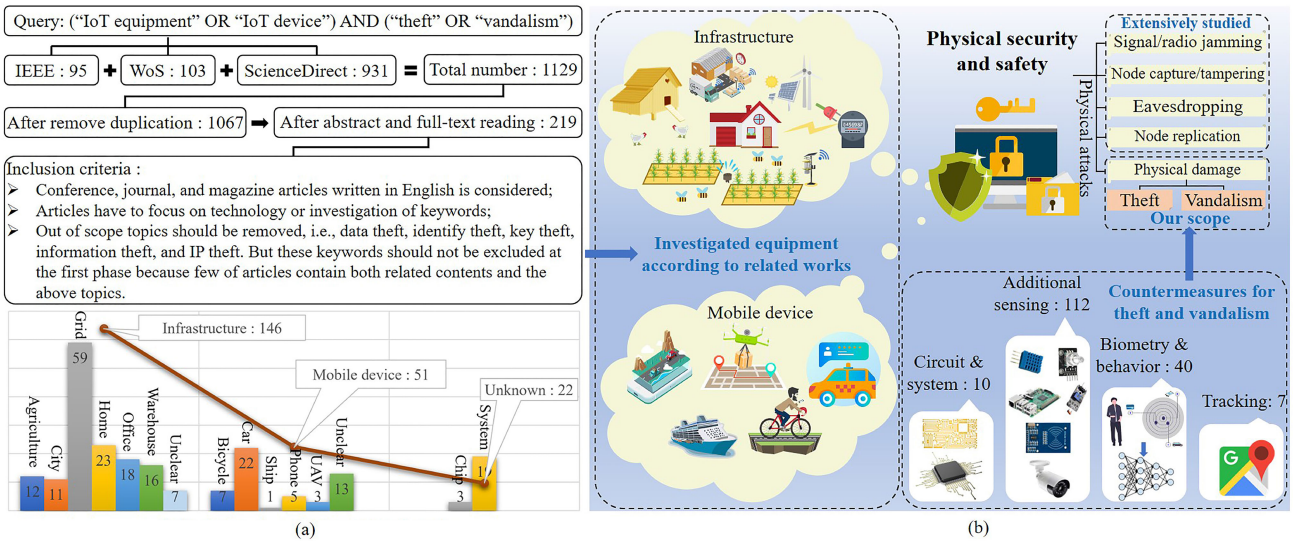


Fig. 1. Methodology and main topics in this survey article. (a) Selection of researches, search query, and inclusion criteria, in which 23 papers only studied antitheft or antivandalism technology rather than specific scenarios; thus, we classified them into "unknown." "Unclear" denotes papers only discuss related technologies in vague backgrounds. (b) Description of equipment and countermeasures, where the number followed each countermeasure is counted from selected works.

Motivation: Most researches focus on technology-oriented security issues to prevent cyber-attacks. However, cyber-attacks are not the only way to steal sensitive information and affect the stable operation of industrial systems. All firewalls, cryptography, and other cyber-security measures cannot work if attacks gain physical access and take what they want [11]. Second, we searched the security or safety issue of IoT equipment or device and found 27 504 papers. Although the duplicates are not removed, the result suggests that only a few works (about 4%) take theft or vandalism of IoT equipment into consideration. Such neglect can result in the instability of an IoT system. Third, to the best of our knowledge, most current studies merely concern specific scenarios and countermeasures without a horizontal comparison.

Last but not least, a survey [12] investigated the camera traps theft and vandalism, and the result demonstrates that most scientists (90%) deliberately avoided some places to prevent lost data and equipment rather than optimizing the scientific rigor. Due to the above reasons, we attempt to fill this gap by reviewing state of the art, existing countermeasures, and future research opportunities of IoT equipment theft and vandalism. Moreover, we present this survey to share the background, state of the art, countermeasures, AI solutions, and future trends with scholars, technicians, and any individual interested in this topic.

Related Work: To investigate related works that addressed theft and vandalism of IoT equipment, we searched three digital databases: 1) IEEE Xplore, 2) Web of Science, and 3) ScienceDirect for a broad view of existing researches in a wide but relevant range. From the technology aspect, the above databases sufficiently cover the theft and vandalism of IoT equipment. The query text and results are shown in Fig. 1(a), where the search range is from 2011 to 2021. IoT equipment or device is the research object, and, meanwhile, theft or vandalism is the research issue. Therefore, we search related works based on both of them.

In the first phase, we searched for research using the query in three databases and exported the result into reference management software (EndNote). The research result indicates that there are 1131 papers. In the second phase, we removed 64 duplicates. In the last phase, the 1067 papers are carefully reviewed based on the principle: antitheft and antivandalism technologies or scenarios must be discussed in detail. Thus, 219 high related papers (including 59 survey papers) are selected. According to the search result, we classified the investigated equipment into two aspects.

1) *Infrastructure:* Fixed/static where they are unlikely to be entirely stolen but can be partly stolen, e.g., power lines, substation facilities, smart street lights, and irrigation equipment.
2) *Mobile device:* Not fixed, e.g., smartphones, unmanned aerial vehicles (UAVs), cars, ship, and bike-sharing (designed as part of the public transport system).

Besides, antitheft and antivandalism schemes are divided into four aspects according to 219 papers.

1) *Circuit and system:* Detecting theft by system-level device identification and analyzing abnormal parts, e.g., physical unclonable function (PUF) and power frequency signal injection.
2) *Additional sensing:* Monitoring theft and vandalism by additional devices, e.g., radio frequency identification (RFID), video surveillance, and infrared sensor.
3) *Biometry and behavior:* Recognizing theft and vandalism by biometric features and well-defined behaviors without additional sensing devices.
4) *Tracking:* Tracking stolen equipment by GPS or other location technologies.

Authorized licensed use limited to: Account Rajalakshmi Institute of Technology - Chennai. Downloaded on February 22,2023 at 07:25:32 UTC from IEEE Xplore. Restrictions apply.

TABLE I
COMPARISON OF RELATED SURVEYS[1] ON PHYSICAL SECURITY AND SAFETY OF IOT EQUIPMENT

Year	Reference	Equipment		Countermeasure			
		Infrastructure	Mobile Device	Circuit & system	Additional sensing	Biometry & behavior	Tracking
2014	Luvisi *et al.* [13]	√			√		
2018	Salvini [14]	√		√			
2018	Aalsalem *et al.* [15]	√			√		
2019	Avancini *et al.* [16]	√				√	
2019	Lozoya-Santos *et al.* [18]		√			√	
2020	Breitinger *et al.* [8]		√				
2021	Stylios *et al.* [19]		√			√	
2021	Himeur *et al.* [17]	√				√	
2021	Elharrouss *et al.* [21]				√		
2021	Lee and Atkison [20]		√	√			√
2021	Our	√	√	√	√	√	√

[1]We select ten representative survey papers from 59 survey papers based on our final result.

As shown in Table I, 10 representative survey papers from 59 survey papers are summarized. Several authors [13]–[17] presented comprehensive literature reviews on protecting specific infrastructures from theft and vandalism, in which RFID, system design, sensor network, and machine learning methods are adopted. Interestingly, Avancini *et al.* [16] highlight the privacy-preserving issue which users pay more attention to rather than the antitheft or antivandalism scheme. In addition, physical security and safety of mobile devices were introduced in [8], [18]–[20], where system design, biometry and behavior analysis, and tracking methods are discussed. In particular, Breitinger *et al.* [8] discussed smartphone theft and the victims' response. The results indicate that only 12.1% of Android users and 6.2% of iOS users have high security knowledge. And nearly half of users even do not know the encryption function of devices.

Contribution: The outline of the contributions of this survey relative to the recent literature in the field can be summarized as follows.

1) Compared with other surveys in the field, this survey provides a deeper summary of the universal and specific features of the typical equipment to enable researchers to have a comprehensive and quick understanding of equipment with a strong research foundation.
2) We provide an overview of antitheft and antivandalism schemes. Moreover, we explore and discuss how to adopt AI solutions.
3) We present future research opportunities which contribute to locating, modeling, evaluating, and managing IoT equipment.

Organization: The rest of the article is organized as follows. The infrastructures and mobile devices are introduced in Section II. Section III investigates the existing theft and vandalism schemes for IoT equipment. AI solutions are discussed and summarized in Section IV. Section V discusses the future research opportunities of IoT equipment security and safety. Finally, Section VI concludes this article.

II. IOT EQUIPMENT

In this section, IoT equipment cases, universal features, and specific features are introduced. The IoT equipment cases are chosen with wide attention based on the searching result, which indicates that these cases have a high physical damage risk. These infrastructures are composed of traditional equipment and IoT modules with well-defined functions. Furthermore, researchers can easily and quickly investigate related works by analyzing the features of studied equipment and the way they are damaged.

A. IoT Equipment Cases

1) Infrastructure—Urban and Rural Facilities: Smart city is promoting the combination of IoT devices and public facilities. Vandalism is a typical phenomenon in the urban environment and usually targets street furniture (e.g., street lamps, monitoring stations, vending machines, and robots) [14]. For instance, with the advantages of small size, wireless communication, message storage, and location, subscriber identity module (SIM) cards are widely applied in public facilities to notify maintainers when public facilities are faulty. However, intruders can steal SIM cards to make harassing calls, which leads to the waste of public resources and the trouble of residents. For instance, 400 high-tech South African traffic lights are vandalized and cannot work due to SIM card theft, which results in $1.3 million costs for repairing, more than 150 SIM card bills, and a hazard in the city's major roads [22]. Decreasing farm population leads to the decline of supervision efficiency, which causes criminal behaviors of agricultural equipment and does damage to farmers [23]. Individual financial losses were up to $76 319 resulting from theft and vandalism of agriculture in which the most common type of theft in the agricultural scenario is the theft of tools and small equipment (33%) in 2000 [24]. Besides, agriculture facilities are usually deployed in the outdoor environment. Thus, it is hard to detect and track theft or vandalism in time, e.g., physical beehive interruption because of vandalism and theft [25].

Authorized licensed use limited to: Account Rajalakshmi Institute of Technology - Chennai. Downloaded on February 22,2023 at 07:25:32 UTC from IEEE Xplore. Restrictions apply.

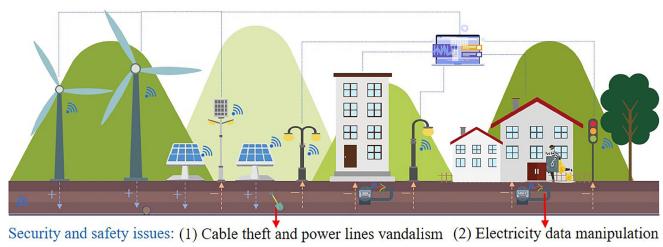


Fig. 2. Physical security and safety issues of smart grid facilities. For illegal activities and their benefits, malicious users destroy public power facilities (cable theft and power lines vandalism), tamper with a smart meter reading, bypass the meter, and hack the meter (electricity data manipulation).

2) Infrastructure—Energy Facilities: Because of electricity theft, more than $89.3 billion are lost annually, and tapping constitutes nearly 80% of total losses [26]. As shown in Fig. 2, electricity theft can be classified into two aspects. 1) *Power facilities:* Theft and vandalism for selling have impacted the operation of urban/rural electrical equipment (e.g., substations, power stations, and base stations). Moreover, vandalism of power facilities monitoring devices (e.g., voltage/current sensors, cameras, and infrared sensors) leads to unprotected smart grid facilities and additional losses. For instance, the US experienced power outages due to severe weather conditions followed by vandalism, equipment failure, etc., which led to about 161 462 h of power outage, affected 157 million customers, and 445-GW demand loss [27]. 2) *Smart meter:* Electricity data manipulation is performed for reducing electricity bills, including tampering with a smart meter (an IoT-based instrument for measuring electricity consumption) reading, bypassing the meter, and hacking the meter. Individuals may tamper with the meter reading for illegal activities (e.g., in-house marijuana growing operations [28]). These malicious behaviors are nontechnical losses, which can lead to a heavy load on electrical systems and dangers to public safety, such as conflagrations [29].

3) Infrastructure—Home, Office, and Warehouse: Home, office, and warehouse facilities are usually placed in the indoor environment; thus, burglary and insider theft are usually performed, leading to physical damage and privacy leakage. For instance, Coca-Cola Inc. announced that several laptops containing about 74 000 employees' personal information were stolen from its headquarters, which greatly impacts personal safety and privacy-preserving. Besides, 137 053 and 46 309 thefts occurred in the home and commercial establishments in 2016, respectively [30].

4) Mobile Device—Smartphone: The smartphone is a small portable device and suffers from theft, which brings economic losses, personal privacy leakage, and illegitimate uses of blackmail. A report [31] indicated that more than ten million smartphones were stolen in the United States in 2013, which constitutes considerable losses for individuals and society.

5) Mobile Device—UAV: Similar to smartphones, UAVs are vulnerable to vandalism due to challenging tasks as well as working characteristics (aerial operation and remote control). For instance, UAVs should be prevented from drifting into a nearby schoolyard [32]. Military UAVs performing reconnaissance missions are easily destroyed by the enemy.

6) Mobile Device—Vehicle: Car and bike-sharing are different transport modes that consist of driven devices, electrical installation, IoT devices, locks, and energy harvesting devices. For the car, physical methods and cyber-attacks are mainly used for allowing unauthorized access. In addition, the parts of cars may also be maliciously damaged or replaced, which are hard to detect [33]. In 2019, a survey [34] investigated the situation of vehicle parts theft in Colombo, and the results indicated that the main stolen parts were lights (28%), airbags (18%), and side mirrors (23%). Unlike cars, bikes have lighter weight, which leads to theft by moving the entire vehicle away, even under a locked state. Many bikes are decomposed into parts and sold separately [35]. In addition, bike-sharing smart locks are composed of various IoT devices that are vulnerable to theft and vandalism (i.e., control chip, GPS location, SIM card or Bluetooth for wireless communication, and charging management module). More than one-third of Belfast Bikes are out of action due to theft or vandalism. The main problem is "simply mindless vandalism," including being dumped in the river and being sawn in half, which leads to about £21 000 economic loss annually [36]. Moreover, Gobee Bike (a bike-sharing manufacturer) pulled out of France in 2018 because more than 3200 bikes were broken and more than 1000 bikes were stolen.

B. Universal and Specific Features

IoT is very heterogeneous; yet, there are commonalities between devices and systems. Hence, it is critical to analyze the universal and specific features of different equipment.

1) Universal Features: They are summarized according to the above cases. The universal features of different equipment are summarized as follows.

1) *Interaction:* IoT equipment is applied to store client data and usually connects with other IoT equipment. Hence, theft or vandalism would lead to a chain reaction. For instance, Apple Watch can control the user's car remotely, which indicates that losing your Apple Watch may result in losing your car and individual's privacy [37].
2) *Unpredictability:* It is hard to predict when and where IoT equipment will suffer from theft and vandalism. Most present works focus on detecting abnormal behavior, making a response, and tracking equipment quickly. Besides, attackers can benefit from destroying or stealing this equipment, thus increasing crime costs and reducing the benefit of theft are conducive to reducing the possibility of theft and vandalism.
3) *False alarm:* Frequent false alarms would lead to the neglect of the physical security and safety of the equipment. Attackers take advantage of the individual's psychology to trigger alarms frequently and steal or destroy equipment without the user's attention. Multiple anomaly detection mechanisms contribute to reducing the possibility of the false alarm rate.

2) Specific Features: They are summarized as reference indexes, which contribute to designing the physical security and

Authorized licensed use limited to: Account Rajalakshmi Institute of Technology - Chennai. Downloaded on February 22,2023 at 07:25:32 UTC from IEEE Xplore. Restrictions apply.

safety scheme for the specific equipment. The specific features can be classified as follows.

1) *Energy capacities:* The energy of the great majority of mobile devices and part of infrastructures are limited. Hence, the physical security and safety scheme will not work if the energy is insufficient.
2) *Sensing and computing ability:* Antitheft and antivandalism schemes mainly rely on the sensing data and detection model. For instance, compared with smart meters, a smartphone usually contains more than ten kinds of sensors and a CPU, which indicates that it supports more complex and accurate detection models. It is inevitable for equipment with low sensing and computing ability to adopt additional detecting devices.
3) *Privacy:* IoT equipment usually contains personal privacy or corporate intellectual property; thus, theft of IoT equipment is not just a loss of property. For instance, smart meters contain users' electricity habits. Therefore, burglary is easy when homeowners are not at home by analyzing this information. Therefore, it is critical to preserve privacy through federal learning and edge computing, which train detection models and execute detection commands at IoT equipment.
4) *Accessibility and risk:* More important IoT equipment indicates more protective measures. For example, compared with a power station, individuals can easily access smart meters and cables. It is almost impossible to protect all IoT equipment from physical damage. Therefore, safety management according to risk level and accessibility becomes a more practical scheme.
5) *Surrounding:* Video surveillance could be adopted to detect theft and vandalism for infrastructures placed in outdoor surroundings (e.g., street lamps, traffic lights, and cables). Nevertheless, it may impact an individual's privacy; thus, sensors and biometry authentication would be better for indoor surroundings, e.g., residential premises.
6) *Mobility:* It is hard to monitor mobile devices by video surveillance because they will not be fixed. However, the motion feature and location can be adopted to detect theft and vandalism.

III. Countermeasure

In this section, four kinds of countermeasures (circuit and system design, additional sensing device, biometry and behavior analysis, and theft tracking) for these cases are introduced and discussed below. A summary of related papers is listed in Table II.

A. Circuit and System Design

Circuit design: It is a cable or embedded chip theft detection method. The power frequency signal injection technique, which computes the carrier signal's differential change, is mainly used to detect the safety of transmission lines or distribution lines. This technique is efficient and simple for detecting cable theft and power line vandalism, but it cannot accurately locate the place of theft by measuring high-frequency signals. For embedded chips, PUF is a reliable solution to complete device authentication and key storage. The system-level fingerprint will be inconsistent once the chips in embedded chips are stolen or replaced [55]. However, the PUF scheme requires physical or logical tamper resistance. Hence, a two-factor fuzzy commitment scheme was proposed using PUF as the noisy internal source and sensing data as the noisy external source to counter this drawback [10].

System design: It is a framework for discovering any possible physical interactions in the IoT environment. For instance, to detect theft, an energy harvesting device with multiple microcontrollers was designed to measure the harvested power as surroundings' signals [56]. Besides, Ding *et al.* [46] noted that the physical environment will be affected if IoT equipment is broken or stolen. For instance, if there is a high indoor temperature due to vandalism in a heater, the windows will be opened according to the program, which leads to a potential intrusion problem.

B. Additional Sensing Device

Different from circuit and system design, additional sensing devices detect theft and vandalism by estimating whether the measuring data reach any preconditions. Camera, sensors, and RFID are mainly used in distribution networks to detect abnormality. *Camera:* It is widely used for monitoring abnormal conditions of equipment (e.g., car [53], beehive [25], and home [30]) with high human capital costs. To solve human capital costs, real-time image processing based theft detection systems to verify driver's identification were presented in [53] and [57]. The alarm rings and electrical connections are not activated if the driver is unauthenticated. Besides, a video detection model with high response speed can improve theft and vandalism detection accuracy and response time. Therefore, an object detection model was packed in a single Raspberry Pi to detect theft in the edge and prevent middle attacks [30]. In summary, video surveillance has the advantage of criminal identification and evidence preservation; however, the deployment of these monitoring devices requires additional network traffic and calculation resources. *Sensor:* They are embedded into an IoT system, which contains various sensors (e.g., infrared sensors for car [58], vibration sensors for oil and gas pipeline [59], triboelectric nanogenerator based self-powered sensors for wearable equipment [60], etc.) wireless communication devices (e.g., GPRS and ZigBee), and control chip (e.g., Arduino for smart meter [61]) are mainly used in distribution networks to detect outdoor static and unsupervised equipment. *RFID:* It is a passive sensing technology that identifies targets and accesses relevant data by noncontact, two-way communication. Compared with the above sensors, which can be divided into active sensing, RFID consumes less energy and contributes to an environment with a large number of equipment [45]. Besides, RFID saves communication costs compared with GSM and has been widely used in supply chain management [62]. Unfortunately, the tag of RFID may suffer from energy shortage after performing related algorithms and then fails to detect the movement of equipment [63]. Besides, RFID technology cannot detect physically

Authorized licensed use limited to: Account Rajalakshmi Institute of Technology - Chennai. Downloaded on February 22,2023 at 07:25:32 UTC from IEEE Xplore. Restrictions apply.

TABLE II
SUMMARY OF PHYSICAL SECURITY AND SAFETY COUNTERMEASURES FOR INFRASTRUCTURES AND MOBILE DEVICES

Scenario	Year	Scheme	Countermeasure	Theme	Safety analysis	Method	Performance
Power line	2014	Christopher *et al.* [38]	Circuit design	Stealing electricity by destroying the power line	Simulation-based	A Narrow band power line carrier signal injected along with the power frequency signal	+ [38], [39] Electrical signal detection by simple and cheap components for outdoor static and unsupervised equipment + [13] huge number of equipment management by RFID + [25] surveillance video for the outdoor and remote environment
Street lamp	2011	Wang *et al.* [39]	Circuit design	Cable of street lamp theft	Simulation-based	Two methods of tracking resonance frequency	
Tree	2014	Luvisi *et al.* [13]	RFID	vandalism of trees in city	N/A	RFID embedded in trees to manage them	
Beehive	2021	Tashakkori *et al.* [25]	Camera	beehive vandalism	Experiment-based	Monitoring surveillance video for protecting beehive	
Smart meter	2015	Amin *et al.* [40]	Behavior analysis	Rigging the electricity consumption signal	Simulation-based	A game-theoretic framework to simulate the adversarial nature of the electricity theft problem	- [40] Calculating the probability of anomaly behavior only from theoretical perspective − [26], [29], [41] Obtaining more than 90% precision without taking privacy-preserving into consideration + [42] Ensuring high precision and preserving privacy by minimizing the required resources, which would drive future researches in electricity data manipulation
Smart meter	2016	Jindal *et al.* [26]	Behavior analysis	Electricity theft by tampering smart meter	Case data evaluation	A decision tree and support vector machine based top-down scheme	
Smart meter	2016	Jokar *et al.* [42]	Behavior analysis	Predictability property of normal and malicious consumption patterns	5000 customers' data evaluation	A consumption pattern-based energy theft detector	
Smart meter	2018	Zheng *et al.* [29]	Behavior analysis	Abnormal electricity consumption pattern of energy theft	Case data evaluation	A wide and deep CNN based electricity-theft detection method	
Smart meter	2019	Gao *et al.* [41]	Sensor	Electricity theft by tampering smart meter	Case data evaluation	A physically inspired data driven model by electricity usage and voltage magnitude	
Office	2018	Chandrappa *et al.* [43]	Sensor detection	Increasing robbery and intrusion cases	Hardware testing	A ultrasonic sensor and GSM-based theft detection system	- [43], [44] Consuming a lot of energy by surveillance monitoring and active sensing + [45] Immediacy alarm and low consumption by sensing the movement of infrastructures passively, which is suitable for valuable and static equipment + [46] Quickly risk analysis by a entire framework for an environment with a large number of IoT devices
Museum	2019	Liu *et al.* [45]	RFID	More and more criminals have stolen cultural relics	Software and hardware testing	An RFID-based anti-theft method	
Office	2017	Han *et al.* [44]	Sensor	Laboratory property security risks	Experiment-based	An infrared sensor, Bluetooth, GPS and GSM-based anti-theft alarming and mobile tracking	
Home	2018	Ding *et al.* [46]	System design	Attackers leveraging stealthy physical interactions to launch attacks against IoT systems	Simulation-based	A framework for discovering any possible physical interactions in IoT environment	
Smartphone	2011	Gao *et al.* [47]	Hardware design	Reducing the losses caused by the stolen smartphone	Hardware design	Locking SIM card and anti-theft processing module	- [47] Can not prevent devices from stealing − [48]–[50] Based on well-defined motion − [51] Saving energy but requiring additional RFID interface − All references requiring a large number of labelled data + [31] Low energy consumption and can be extended to various motions, which contributes to portable, valuable and energy limited devices
Smartphone	2015	Yang *et al.* [48]	Biometry behavior analysis	Screen locking for smartphone to secure the personal stuff	200 users' handwaving action data	A support vector machine-based authentication pattern	
Smartphone	2015	Ren *et al.* [49]	Biometry behavior analysis	User spoofing by hacking smartphone in healthcare systems	Over 3000 smartphone-based traces data	A user verification system-based on gait patterns derived from acceleration readings	
Smartphone	2017	Hussain *et al.* [51]	RFID and sensor	Anti-theft and anti-lost measure for smartphone	Android system testing	An RFID-based and accelerometer-based twofold probing scheme	
Smartphone	2018	Jin *et al.* [31]	Behavior analysis	Smartphone theft adverse to personal property and privacy	Case data evaluation	A markov-based behavior tracking model named iGuard	
Smartphone	2019	Shen *et al.* [50]	Biometry behavior analysis	Prevalence, monetary value, and mobile nature leading to frequent theft	45 users' data	A walking behavior and matching method	
UAV	2018	Afman *et al.* [32]	Hardware design	The falling of UAV causing serious injury to a human	Hardware testing	An optimal active breaking raking system for UAV	- [52], [53] Additional devices for monitoring − [53] Potential privacy violations + [32] Preset program to reduce risk after theft or vandalism of mobile devices + [54] Monitoring by user's behavior without additional devices, which is suitable for equipment with various sensors
Car	2012	Hu *et al.* [52]	Sensor	Raising automotive vehicle stolen	N/A	A GSM, vibration sensor, and GPS module-based automobile anti-theft system	
Car	2019	Mohanasundaram *et al.* [53]	Camera	Any person trying to break the car	Simulation-based	A face recognition based vehicle theft tracking and detection system	
Car	2021	Kwak *et al.* [54]	Behavior analysis	Performing vehicle-theft detection by driver-identification	Driving dataset of 5 participants	A wavelet transform-based driving-pattern analysis of each driver	

The advantage and drawback of different references are represented by + and −, respectively.

Authorized licensed use limited to: Account Rajalakshmi Institute of Technology - Chennai. Downloaded on February 22,2023 at 07:25:32 UTC from IEEE Xplore. Restrictions apply.

damaged equipment [64]. Notably, the above methods cannot work if the sensors, cameras, or RFID are broken. Therefore, multiple verification could be used to ensure that the antitheft system is still useful when a sensor is broken, e.g., an anti-vandalism scheme formed by the combination of surveillance monitoring, voice detection, and RFID detection.

C. Biometry and Behavior Analysis

The biometry and behavior analysis scheme applies data acquired from embedded sensors rather than additional measuring instruments to authenticate users and evaluate equipment operation state. Moreover, the additional sensing scheme will not work if the thief removes or shuts down the sensors and surveillance monitoring devices. Therefore, biometry and behavior analysis has recently attracted more attention.

According to [19], behavior biometrics for mobile devices can be divided into walking gait, touch gestures, keystroke dynamics, behavioral profile, hand waving, and power consumption. All biometrics must be acquired for continuous authentication and cannot achieve high detection accuracy once unexpected behavior occurs. For smartphones, several authors [50], [65] discussed real-time anomaly detection methods; however, these methods rely on the short-term behavior characteristics of users and can only identify biometrics and well-defined motion [49]. Hence, Jin *et al.* [31] designed a theft detection system by exploiting only the built-in inertial sensors on a smartphone. Through a user's key behaviors (e.g., taking out the smartphone and walking), the accuracy rate reached 95%, and the false detection rate was only 4%. Users can quickly find a stolen smartphone with a 4.7-s detection delay, which is conducive to tracking smartphones. For cars, Kwak *et al.* [54] proposed a car theft detection model based on driving habits (e.g., door opening and closing, starting ignition, and seat-belt fastening), which reached an accuracy of 96.18% in binary classification and 91.6% in multiclassification. The usage habits of nodes can also be used to train detection models for infrastructures. For instance, in 2015, Amin *et al.* [40] presented a game-theoretic framework for modeling the genuine and fraudulent behavior of electricity theft. This model can calculate the probability of anomalous behavior from a theoretical perspective. After that, researchers have extensively explored different AI-based detection methods, e.g., a decision tree (DT) and support vector machine (SVM) based top-down scheme to detect electricity theft by gathered electricity consumption data [26], and a wide and convolutional neural networks (CNN) based model for detecting abnormal electricity consumption [29]. The above methods detect electricity theft by collecting users' real-time energy consumption data (i.e., user load profiles) without preserving privacy. Therefore, some studies analyzed the usage pattern of users without invading user privacy. For instance, Jokar *et al.* [42] presented a consumption pattern based theft detector using classification and clustering techniques, which provided high performance with a low sampling rate. Salinas *et al.* [66] proposed a centralized electricity theft detection method based on a Kalman filter and two loosely coupled filters, which can preserve users' privacy by hiding the meter reading from the system operator. In summary, the biometry and behavior analysis scheme requires remarkable characteristics and is continuously running in the IoT equipment. The drawbacks of this scheme are additional energy consumption, continuous occupation of chip memory, and privacy leakage of users.

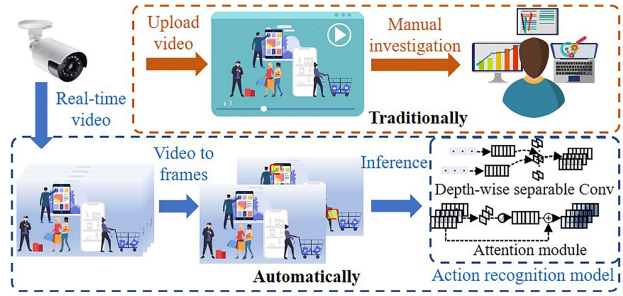


Fig. 3. Two different ways of processing surveillance. The action recognition model can detect theft and vandalism automatically and in real time.

D. Tracking

Equipment location plays a vital role in tracking after a theft, but few studies have focused on applying suitable location technologies according to the features of scenarios. The success rate of tracking highly depends on the accuracy and speed of location. *Outdoor environment location:* GPS, location-based service, and GPS satellite locations are mainly used, in which GPS is the most widely used technology in tracking after a theft. Although GPS has high accuracy and wide coverage, it is not suitable for all users because of its high cost and high energy consumption [67]. *Indoor environment location:* Bluetooth, ZigBee, RFID, WiFi, infrared location, received signal strength, ultrasonic location, and ultra wide band location technologies are mainly used (the distance is usually no longer than 10 m). For instance, Luo *et al.* [68] presented an automated database updating and fingerprinting-based wireless indoor localization system, which provides precise locations in both static and dynamic environments.

IV. AI Solutions

In this section, we explain how AI technology improves theft and vandalism detection countermeasures. Most of the countermeasures discussed in the above section are active detection schemes, which indicates that expert knowledge and high human capital costs are required to evaluate theft and vandalism [30]. A detection model can be trained by AI approaches, including machine learning and deep learning algorithms, to recognize the theft and vandalism of IoT equipment accurately and automatically.

A. Video Action Recognition

As shown in Fig. 3, deep learning based object detection of videos contributes to unmanned and real-time surveillance, where temporal modeling is critical for action recognition. In 2020, Li *et al.* [69] proposed a motion excitation module and multiple temporal aggregation modules to model the long-range

Authorized licensed use limited to: Account Rajalakshmi Institute of Technology - Chennai. Downloaded on February 22,2023 at 07:25:32 UTC from IEEE Xplore. Restrictions apply.

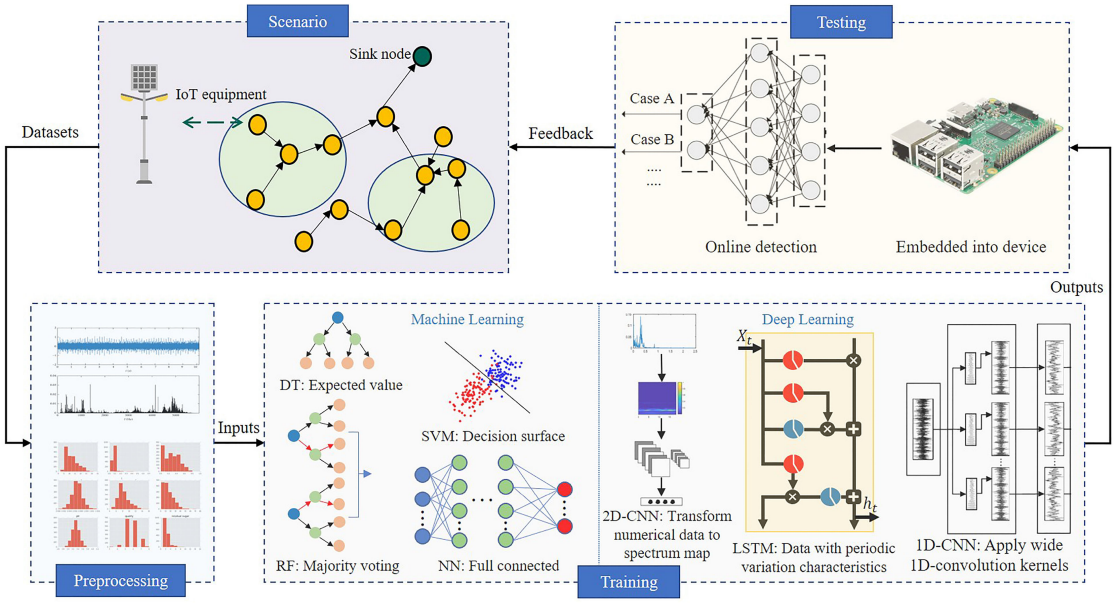


Fig. 4. Flowchart of behavior analysis scheme based model which is embedded in IoT devices. Considering the characteristics of different IoT equipment, the appropriate behavior features and well-defined motions are selected as the inputs. To accelerate the convergence, data preprocessing technology is applied to obtain important features. Then an appropriate machine learning or deep learning model is selected and trained. Finally, after fine-tuning, the model is embedded in IoT devices to form an online antitheft and antivandalism model.

temporal relationship over distant frames. The proposed module achieves the highest top-1 accuracy (48.9%) and top-5 accuracy (78.1%) on the Something-Something dataset. For gradually expanding different dimensions, a coordinate descent and greedy strategy based search strategy were designed to build the optimal video recognition model [70]. One of $X - Fast$, $X - Temporal$, $X - Spatial$, $X - Depth$, $X - Width$, and $X - Bottleneck$ are adopted in each extension to control model complexity. The results reveal that depthwise separable convolution and attention module are critical for the lightweight video recognition model.

B. Behavior Analysis

Most of the behavior data are numerical data. Hence, machine learning algorithms (black-box models good at classifying and regressing numerical data) have been widely used in theft and vandalism of IoT equipment, e.g., SVM (classifying by decision surface), DT (evaluating results by expected value), random forest (RF, classifying by majority voting), and neural network (NN, classifying using full connected layer). Due to the improvement of model accuracy brought by deep learning algorithms, researchers applied deep learning algorithms. Initially, the numerical data are transformed in the frequency domain to form spectrum maps. Then, a two-dimensional CNN (2-D CNN) model based on image data is applied to build the model. Although this method can improve the accuracy of the detection model, it will reduce the execution efficiency of the model and consume more computing resources. Therefore, the parameters of CNN have been modified to make them suitable for numerical data in recent advances. For instance, wider convolution kernels have been applied to ensure the feature extraction of periodic signals [29].

C. Embedding in IoT Equipment

Theft and vandalism detection models are embedded in IoT equipment to ensure the quick response of malicious behaviors and reduce bandwidth occupation, decision latency, and privacy leakage. A flowchart of behavior analysis based physical security and safety model is shown in Fig. 4. However, low efficiency, high energy consumption, and high memory footprint result from large model size and floating-point operations (FLOPs). These disadvantages have an impact on embedding AI models in IoT equipment. Hence, lightweight models are designed from the following aspects.

1) *Compression technologies:* Improving model efficiency by compressing model's layers, e.g., 1) quantization which compresses the weight parameters from 32-b floating-point value to 8-b unsigned integers [71] and 2) pruning which deletes unimportant filters to increase the sparsity of model. Compression technologies contribute to greatly reducing the model parameters (generally, the parameters of a model can be compressed to 20%–50% of that of the original model) with a slight decrease of accuracy.
2) *Learning technologies:* Training a model in a different way, e.g., 1) distillation which learns a small model from a large well-trained model [72] and 2) hyperparameter optimization, which learns parameters automatically. Learning technologies require a large number of computing resources to build a small and high accuracy model.
3) *Architectures designs:* Designing efficient layers instead of baseline layer, e.g., 1) depthwise separable convolution layer which consists of group convolution and pointwise convolution [73] and 2) attention mechanism which reduces network depth by enhancing important filters of each layer and suppressing invalid filters. The

Authorized licensed use limited to: Account Rajalakshmi Institute of Technology - Chennai. Downloaded on February 22,2023 at 07:25:32 UTC from IEEE Xplore. Restrictions apply.

model's parameters with well-designed architectures can be reduced to 10% of that of the baseline model.

4) *Inference platforms:* Selecting suitable software and hardware. TensorFlow Lite and PyTorch Mobile have been widely used to compress trained models through quantization, graph optimization steps, etc. TensorFlow Lite has stronger compatibility and can be deployed in microcontrollers, e.g., Android and iOS systems-based smartphones, STM32, Arduino, and Raspberry Pi.

The above technologies represent different ways to obtain lightweight models. Considering IoT equipment's different storage and computing capacity, a tradeoff between accuracy and efficiency is critical to design and evaluate the appropriate model. FLOPs, latency, energy consumption, and model size are usually adopted to evaluate the model's efficiency. Accuracy, F-score, precision, and recall are usually used to evaluate the performance of the model. By analyzing the above metrics, the physical security and safety model can achieve Pareto-optimality (the desired state of the model with better accuracy and less latency of inference).

D. Privacy Preserving

For preserving personal privacy, users are not willing to share their data which leads to the lack of real-world datasets. Therefore, it is necessary to build the model based on a small number of training samples with the characteristics of fast convergence and high accuracy. Zero-shot learning and transfer learning play an important role in this area [74]. The steps of these two methods include: 1) using the trained model in similar scenarios (with a large number of data) or additional information (semantic spaces) and 2) applying a small number of samples in the target scenario to retrain the model and fine-tune the parameters [75]. The trained model will be suitable for the target scenario after the above steps. For instance, the pretraining motorcycle theft detection model can be used to train a bike theft detection model, as shown in Fig. 5. Unlike offline training methods that train models on the cloud, federated learning contributes to privacy-preserving by training models on IoT equipment without transmitting data from IoT equipment to the cloud.

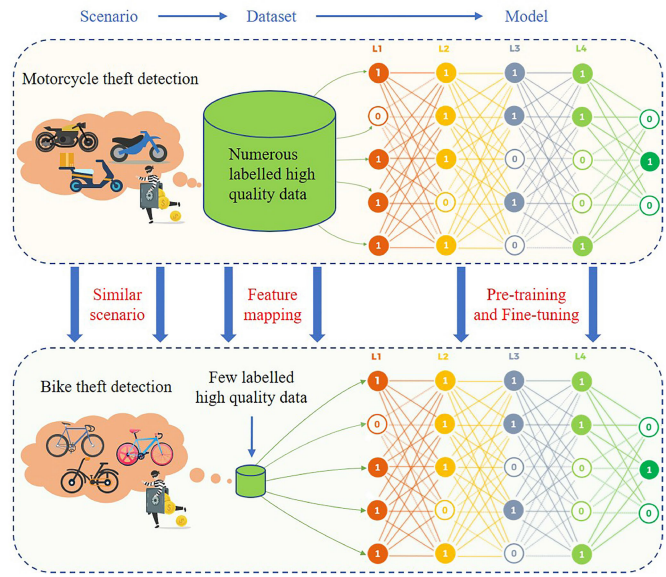


Fig. 5. Example of a transfer learning application. Motorcycle theft shares similar features with bike theft. There are few labeled high-quality data for bike theft detection models. The well-trained motorcycle theft detection can be transferred to the bike theft detection model.

V. Future Research Opportunities

Realizing the vision of physical security and safety of IoT-based equipment is not an easy task due to numerous challenges that need to be addressed. In the following paragraphs, we briefly discuss future research opportunities in the development phases of the security and safety of IoT-based equipment.

A. Tradeoff Between Availability and Safety

To ensure the security and safety of IoT equipment, researchers prefer to use detection models with strong generalization performance and high accuracy. However, there is an inevitable contradiction between reducing the false alarm rate and improving the detection rate for pattern recognition based models, which indicates that the false alarm rate and detection rate trends are consistent. Users will be troubled by false alarms if there is a high false alarm rate (by setting a low threshold value). Besides, the combination of sensor-based and behavior analysis based methods contributes to reducing the false alarm rate, saving energy consumption, and resources by two steps: 1) low sampling frequency and sensor-based methods under a stable situation and 2) high sampling frequency and behavior analysis based methods if an abnormal state is detected in the first step.

B. Blockchain-Based IoT Equipment Integrity Management

Equipment with lost or broken parts may still be able to maintain operation for a short time. Therefore, compared with vandalism or theft of the entire equipment, that of equipment parts is more difficult to detect. Due to the characteristics of decentralization, independence, security, and anonymity, a blockchain-based scheme can be used to achieve the traceability and integrity of the equipment using the interaction among nodes or parts [76]. IoT equipment can verify the authenticity of the management center node through the signature certificate, which is conducive to preventing vandalism from malicious commands (e.g., false location of UAVs) [77]. Furthermore, communication between equipment through datagram transport layer security can prevent malicious IoT equipment from cheating, eavesdropping, and tampering with other devices. For instance, the manager in blockchain will verify the authenticity of the device and publish it to the proxy node once the IoT equipment is registered in the system for the first time, which prevents the error information caused by malicious node registration (smart meters data tampering) [78]. In particular, blockchain and federated learning contribute to privacy preservation and safety of IoT equipment by training theft and vandalism detection models on IoT equipment or edge nodes.

Authorized licensed use limited to: Account Rajalakshmi Institute of Technology - Chennai. Downloaded on February 22,2023 at 07:25:32 UTC from IEEE Xplore. Restrictions apply.

C. Continuous Biometrics Learning

User behavior and habits may be changed. Moreover, attackers will study how to avoid theft and vandalism detection if they find these countermeasures, which suggests that the pretrained model would be invalid. Hence, the continuous learning paradigm can be used to update models [79].

D. 6G-Based Active Detection for IoT Equipment

Based on the historical data of theft and vandalism, targeted inspection through active detection can reduce the probability of theft or vandalism. On the one hand, the daily active detection of the equipment contributes to diagnosing the potential problems of the equipment. On the other hand, active detection plays a deterrent role in physical security and safety issues, thus reducing the safety risk of equipment. As the key technology of 6G communication, intelligent reflecting surfaces (IRSs) show different sensitivities to incident signals from different directions [80]. This implies that IRSs can be employed as sensing devices to passively detect the location and state of the equipment, especially on indoor equipment, e.g., detection of smartphone theft in a crowd. Furthermore, indoor location and wireless power transfer improve the deployment of the pass detection module. Compared with RFID technology, an IRS receives signals from a 6G base station rather than a Reader, which implies that the IRS for active detection has the advantages of a wide detection range, high bandwidth, and accurate positioning.

VI. Conclusion

Aiming to improve the quality of life through perception, communication, and application, IoT-based equipment has been widely used in modern life. Physical security and safety are critical for the integrity and stability of IoT-based equipment. We presented an overview of the physical security and safety in infrastructures and mobile devices. This, in turn, should provide a good foundation for researchers who are interested in IoT equipment security and safety. Furthermore, countermeasures for solving theft and vandalism issues were discussed. Moreover, four types of theft and vandalism schemes and AI solutions were summarized. Finally, the future research opportunities that pertain to theft and vandalism detection and prevention mechanisms were discussed. These topics provide a good starting point for discussion and further research on IoT equipment's physical security and safety.

References

[1] A. K. Sikder, G. Petracca, H. Aksu, T. Jaeger, and A. S. Uluagac, "A survey on sensor-based threats and attacks to smart devices and applications," *IEEE Commun. Surv. Tut.*, vol. 23, no. 2, pp. 1125–1159, Apr.–Jun. 2021.

[2] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, "Network intrusion detection for IoT security based on learning techniques," *IEEE Commun. Surv. Tut.*, vol. 21, no. 3, pp. 2671–2701, Jul.–Sep. 2019.

[3] R. David, G. John, and R. John, "Data age 2025: The evolution of data to life-critical don't focus on big data; focus on the data that's big," IDC, Seagate, Apr. 2017. Accessed: Nov. 29, 2021. [Online]. Available: https://www.import.io/wp-content/uploads/2017/04/Seagate-WP-DataAge2025-March-2017.pdf

[4] M. Qabulio, Y. A. Malkani, and A. Keerio, "A framework for securing mobile wireless sensor networks against physical attacks," in *Proc. Int. Conf. Emerg. Technol.*, 2016, pp. 1–6.

[5] X. Yang *et al.*, "A survey on smart agriculture: Development modes, technologies, and security and privacy challenges," *IEEE/CAA J. Automatica Sinica*, vol. 8, no. 2, pp. 273–302, Feb. 2021.

[6] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, "A survey of machine and deep learning methods for Internet of Things (IoT) security," *IEEE Commun. Surv. Tut.*, vol. 22, no. 3, pp. 1646–1685, Jul.–Sep. 2020.

[7] M. J. Lencwe, S. P. D. Chowdhury, and T. O. Olwal, "Detection of underground power cable theft: Strategies and methods," in *Proc. IEEE PES/IAS PowerAfrica*, 2018, pp. 1–9.

[8] F. Breitinger, R. Tully-Doyle, and C. Hassenfeldt, "A survey on smartphone user's security choices, awareness and education," *Comput. Secur.*, vol. 88, 2020, Art. no. 101647. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404819301919

[9] A. Karkouch, H. Mousannif, H. Al Moatassime, and T. Noel, "Data quality in Internet of Things: A state-of-the-art survey," *J. Netw. Comput. Appl.*, vol. 73, pp. 57–81, 2016. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1084804516301564

[10] D. Choi, S.-H. Seo, Y.-S. Oh, and Y. Kang, "Two-factor fuzzy commitment for unmanned IoT devices security," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 335–348, Feb. 2019.

[11] S. Al-Fedaghi and O. Alsumait, "Towards a conceptual foundation for physical security: Case study of an it department," *Int. J. Saf. Secur. Eng.*, vol. 9, no. 2, pp. 137–156, 2019.

[12] P. D. Meek, G. A. Ballard, J. Sparkes, M. Robinson, B. Nesbitt, and P. J. Fleming, "Camera trap theft and vandalism: Occurrence, cost, prevention and implications for wildlife research and management," *Remote Sens. Ecol. Conservation*, vol. 5, no. 2, pp. 160–168, 2019.

[13] A. Luvisi and G. Lorenzini, "RFID-plants in the smart city: Applications and outlook for urban green management," *Urban Forestry Urban Greening*, vol. 13, no. 4, pp. 630–637, 2014. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1618866714000764

[14] P. Salvini, "Urban robotics: Towards responsible innovations for our cities," *Robot. Auton. Syst.*, vol. 100, pp. 278–286, 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0921889016303505

[15] M. Y. Aalsalem, W. Z. Khan, W. Gharibi, M. K. Khan, and Q. Arshad, "Wireless sensor networks in oil and gas industry: Recent advances, taxonomy, requirements, and open challenges," *J. Netw. Comput. Appl.*, vol. 113, pp. 87–97, 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1084804518301309

[16] D. B. Avancini, J. J. Rodrigues, S. G. Martins, R. A. Rabêlo, J. Al-Muhtadi, and P. Solic, "Energy meters evolution in smart grids: A review," *J. Cleaner Prod.*, vol. 217, pp. 702–715, 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0959652619302501

[17] Y. Himeur, K. Ghanem, A. Alsalemi, F. Bensaali, and A. Amira, "Artificial intelligence based anomaly detection of energy consumption in buildings: A review, current trends and new perspectives," *Appl. Energy*, vol. 287, 2021, Art. no. 116601. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0306261921001409

[18] J. de J. Lozoya-Santos, V. Sepúlveda-Arróniz, J. C. Tudon-Martinez, and R. A. Ramirez-Mendoza, "Survey on biometry for cognitive automotive systems," *Cogn. Syst. Res.*, vol. 55, pp. 175–191, 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1389041717301948

[19] I. Stylios, S. Kokolakis, O. Thanou, and S. Chatzis, "Behavioral biometrics & continuous user authentication on mobile devices: A survey," *Inf. Fusion*, vol. 66, pp. 76–99, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1566253520303493

[20] M. Lee and T. Atkison, "Vanet applications: Past, present, and future," *Veh. Commun.*, vol. 28, 2021, Art. no. 100310. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2214209620300814

[21] O. Elharrouss, N. Almaadeed, and S. Al-Maadeed, "A review of video surveillance systems," *J. Vis. Commun. Image Representation*, vol. 77, 2021, Art. no. 103116. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1047320321000729

[22] "South africa thieves hit traffic lights for SIM cards," Accessed: Mar. 26, 2021. [Online]. Available: https://www.bbc.com/news/world-africa-12135841

[23] J. S. Kim, M.-G. Kim, B. R. Cha, and S. B. Pan, "A study of determining abnormal behaviors by using system for preventing agricultural product theft," in *Proc. Adv. Computer Sci. Ubiquitous Comput.*, Berlin, Germany: Springer, 2016, pp. 937–943.

Authorized licensed use limited to: Account Rajalakshmi Institute of Technology - Chennai. Downloaded on February 22,2023 at 07:25:32 UTC from IEEE Xplore. Restrictions apply.

[24] E. Barclay and J. F. Donnermeyer, "Crime and security on agricultural operations," *Secur. J.*, vol. 24, no. 1, pp. 1–18, 2011.

[25] R. Tashakkori, A. S. Hamza, and M. B. Crawford, "Beemon: An IoT-based beehive monitoring system," *Comput. Electron. Agriculture*, vol. 190, 2021, Art. no. 106427, doi: 10.1016/j.compag.2021.106427.

[26] A. Jindal, A. Dua, K. Kaur, M. Singh, N. Kumar, and S. Mishra, "Decision tree and SVM-based data analytics for theft detection in smart grid," *IEEE Trans. Ind. Informat.*, vol. 12, no. 3, pp. 1005–1016, Jun. 2016.

[27] H. Masrur, A. Sharifi, M. R. Islam, M. A. Hossain, and T. Senjyu, "Optimal and economic operation of microgrids to leverage resilience benefits during grid outages," *Int. J. Elect. Power Energy Syst.*, vol. 132, 2021, Art. no. 107137. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0142061521003768

[28] Z. A. Baig *et al.*, "Future challenges for smart cities: Cyber-security and digital forensics," *Digit. Investigation*, vol. 22, pp. 3–13, 2017. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1742287617300579

[29] Z. Zheng, Y. Yang, X. Niu, H. Dai, and Y. Zhou, "Wide and deep convolutional neural networks for electricity-theft detection to secure smart grids," *IEEE Trans. Ind. Informat.*, vol. 14, no. 4, pp. 1606–1615, Apr. 2018.

[30] J. A. Mohammed, A. Paul, A. Kumar, and J. Cherukuri, "Implementation of human detection on raspberry pi for smart surveillance," in *Proc. IEEE Int. Conf. Innov. Technol.*, 2020, pp. 1–8.

[31] M. Jin, Y. He, D. Fang, X. Chen, X. Meng, and T. Xing, "iGuard: A real-time anti-theft system for smartphones," *IEEE Trans. Mobile Comput.*, vol. 17, no. 10, pp. 2307–2320, Oct. 2018.

[32] J. P. Afman, L. Ciarletta, E. Feron, J. Franklin, T. Gurriet, and E. N. Johnson, "Towards a new paradigm of UAV safety," 2018, *arXiv:1803.09026*.

[33] K. Lee, H. Yeuk, J. Kim, and K. Yim, "Anti-theft solutions for in-vehicle electronic devices," in *Proc. 8th Int. Conf. Innov. Mobile Internet Serv. Ubiquitous Comput.*, 2014, pp. 549–553.

[34] A. Jayakody, S. Nishshanka, N. Liyanage, N. De Silva, and A. Abhayawardhana, "RFID based theft detection system for automobile parts," in *Proc. Int. Conf. Advancements Comput.*, 2019, pp. 386–391.

[35] P. Jarupunphol, W. Buathong, and T. Chansaeng, "The MTAS for addressing motorcycle theft," in *Proc. 13th Int. Conf. Elect. Eng./Electron., Comput., Telecommun. Inf. Technol.*, 2016, pp. 1–4.

[36] A. Ferguson, "Over one-third of belfast bikes are stolen or vandalised," Irish News, Apr. 2017. Accessed: Mar. 26, 2021. [Online]. Available: https://www.irishtimes.com/news/ireland/irish-news/over-one-third-of-belfast-bikes-are-stolen-or-vandalised-1.3055499

[37] R. Kirk, "Cars of the future: The Internet of Things in the automotive industry," *Netw. Secur.*, vol. 2015, no. 9, pp. 16–18, 2015. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1353485815300817

[38] A. V. Christopher, G. Swaminathan, M. Subramanian, and P. Thangaraj, "Distribution line monitoring system for the detection of power theft using power line communication," in *Proc. IEEE Conf. Energy Convers.*, 2014, pp. 55–60.

[39] W. Yuanyuan, J. Jinbao, Z. Xiangjun, and L. Sidong, "Anti-theft monitoring and location system for cable of street lamp," in *Proc. 4th Int. Conf. Electric Utility Deregulation Restructuring Power Technol.*, 2011, pp. 913–915.

[40] S. Amin, G. A. Schwartz, A. A. Cardenas, and S. S. Sastry, "Game-theoretic models of electricity theft detection in smart utility networks: Providing new capabilities with advanced metering infrastructure," *IEEE Control Syst. Mag.*, vol. 35, no. 1, pp. 66–81, Feb. 2015.

[41] Y. Gao, B. Foggo, and N. Yu, "A physically inspired data-driven model for electricity theft detection with smart meter data," *IEEE Trans. Ind. Informat.*, vol. 15, no. 9, pp. 5076–5088, Sep. 2019.

[42] P. Jokar, N. Arianpoo, and V. C. M. Leung, "Electricity theft detection in AMI using customers' consumption patterns," *IEEE Trans. Smart Grid*, vol. 7, no. 1, pp. 216–226, Jan. 2016.

[43] D. Chandrappa, H. Pavan, M. Sagar, and M. Dakshayini, "IoT security solution to avoid theft," in *Proc. Int. Conf. Wireless Commun., Signal Process. Netw.*, 2018, pp. 1–3.

[44] Y. Han, Z. Chen, and T. Guo, "Design of equipment anti-theft tracker based on wireless sensor network," in *Proc. 1st Int. Conf. Electron. Instrum. Inf. Syst.*, 2017, pp. 1–5.

[45] Z. Liu, M. Wang, S. Qi, and C. Yang, "Study on the anti-theft technology of museum cultural relics based on Internet of Things," *IEEE Access*, vol. 7, pp. 111387–111395, 2019.

[46] W. Ding and H. Hu, "On the safety of IoT device physical interaction control," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2018, pp. 832–846.

[47] Y. Gao, C. Zhou, and D. Shang, "A smart phone anti-theft solution based on locking card of mobile phone," in *Proc. Int. Conf. Comput. Inf. Sci.*, 2011, pp. 971–974.

[48] L. Yang *et al.*, "Unlocking smart phone through handwaving biometrics," *IEEE Trans. Mobile Comput.*, vol. 14, no. 5, pp. 1044–1055, May 2015.

[49] Y. Ren, Y. Chen, M. C. Chuah, and J. Yang, "User verification leveraging gait recognition for smartphone enabled mobile healthcare systems," *IEEE Trans. Mobile Comput.*, vol. 14, no. 9, pp. 1961–1974, Sep. 2015.

[50] W. Gu, L. Shangguan, Z. Yang, and Y. Liu, "Sleep hunter: Towards fine grained sleep stage tracking with smartphones," *IEEE Trans. Mobile Comput.*, vol. 15, no. 6, pp. 1514–1527, Jun. 2016.

[51] M. J. Hussain, L. Lu, and S. Gao, "An RFID based smartphone proximity absence alert system," *IEEE Trans. Mobile Comput.*, vol. 16, no. 5, pp. 1246–1257, May 2017.

[52] J. Hu, J. Li, and G. Li, "Automobile anti-theft system based on GSM and GPS module," in *Proc. 5th Int. Conf. Intell. Netw. Intell. Syst.*, 2012, pp. 199–201.

[53] S. Mohanasundaram, V. Krishnan, and V. Madhubala, "Vehicle theft tracking, detecting and locking system using open CV," in *Proc. 5th Int. Conf. Adv. Comput. Commun. Syst.*, 2019, pp. 1075–1078.

[54] B. I. Kwak, M. L. Han, and H. K. Kim, "Driver identification based on wavelet transform using driving patterns," *IEEE Trans. Ind. Informat.*, vol. 17, no. 4, pp. 2400–2410, Apr. 2021.

[55] Z. Huang and Q. Wang, "A PUF-based unified identity verification framework for secure IoT hardware via device authentication," *Netw. Secur.*, vol. 23, no. 2, pp. 1057–1088, 2020. [Online]. Available: https://doi.org/10.1007/s11280-019-00677-x

[56] T. Tsunoda and K. Nimura, "Information harvesting method by an energy harvesting device with multiple microcontrollers," in *Proc. IEEE 42nd Annu. Comput. Softw. Appl. Conf.*, 2018, pp. 259–265.

[57] A. P. Sreedevi and B. S. S. Nair, "Image processing based real time vehicle theft detection and prevention system," in *Proc. Int. Conf. Process Automat., Control Comput.*, 2011, pp. 1–6.

[58] D. Mukhopadhyay, M. Gupta, T. Attar, P. Chavan, and V. Patel, "An attempt to develop an IoT based vehicle security system," in *Proc. IEEE Int. Symp. Smart Electron. Syst.*, 2018, pp. 195–198.

[59] M. Y. Aalsalem, W. Z. Khan, W. Gharibi, and N. Armi, "An intelligent oil and gas well monitoring system based on Internet of Things," in *Proc. Int. Conf. Radar, Antenna, Microw., Electron., Telecommun.*, 2017, pp. 124–127.

[60] Y. Zhou, M. Shen, X. Cui, Y. Shao, L. Li, and Y. Zhang, "Triboelectric nanogenerator based self-powered sensor for artificial intelligence," *Nano Energy*, vol. 84, 2021, Art. no. 105887. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2211285521001452

[61] H. K. Kondaveeti, N. K. Kumaravelu, S. D. Vanambathina, S. E. Mathe, and S. Vappangi, "A systematic literature review on prototyping with Arduino: Applications, challenges, advantages, and limitations," *Comput. Sci. Rev.*, vol. 40, 2021, Art. no. 100364. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1574013721000046

[62] Y.-J. Tu, W. Zhou, and S. Piramuthu, "A novel means to address RFID tag/item separation in supply chains," *Decis. Support Syst.*, vol. 115, pp. 13–23, 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167923618301544

[63] C. Shao, H. Roh, and W. Lee, "Next-generation RF-powered networks for Internet of Things: Architecture and research perspectives," *J. Netw. Comput. Appl.*, vol. 123, pp. 23–31, 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1084804518302686

[64] T. Fan, F. Tao, S. Deng, and S. Li, "Impact of RFID technology on supply chain decisions with inventory inaccuracies," *Int. J. Prod. Econ.*, vol. 159, pp. 117–125, 2015. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0925527314003181

[65] D. Shen, I. Markwood, D. Shen, and Y. Liu, "Virtual safe: Unauthorized walking behavior detection for mobile devices," *IEEE Trans. Mobile Comput.*, vol. 18, no. 3, pp. 688–701, Mar. 2019.

[66] S. A. Salinas and P. Li, "Privacy-preserving energy theft detection in microgrids: A state estimation approach," *IEEE Trans. Power Syst.*, vol. 31, no. 2, pp. 883–894, Feb. 2016.

[67] V. Primault, A. Boutet, S. B. Mokhtar, and L. Brunie, "The long road to computational location privacy: A survey," *IEEE Commun. Surv. Tut.*, vol. 21, no. 3, pp. 2772–2793, Mar. 2019.

[68] R. C. Luo and T. J. Hsiao, "Dynamic wireless indoor localization incorporating with an autonomous mobile robot based on an adaptive signal model fingerprinting approach," *IEEE Trans. Ind. Electron.*, vol. 66, no. 3, pp. 1940–1951, Mar. 2019.

Authorized licensed use limited to: Account Rajalakshmi Institute of Technology - Chennai. Downloaded on February 22,2023 at 07:25:32 UTC from IEEE Xplore. Restrictions apply.

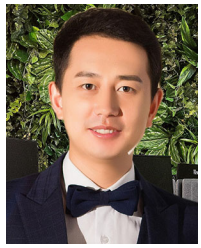
[69] Y. Li, B. Ji, X. Shi, J. Zhang, B. Kang, and L. Wang, "Tea: Temporal excitation and aggregation for action recognition," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit.*, 2020, pp. 909–918.
[70] C. Feichtenhofer, "X3D: Expanding architectures for efficient video recognition," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit.*, 2020, pp. 203–213.
[71] B. Jacob *et al.*, "Quantization and training of neural networks for efficient integer-arithmetic-only inference," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit.*, 2018, pp. 2704–2713.
[72] Z. Chen, L. Zhang, Z. Cao, and J. Guo, "Distilling the knowledge from handcrafted features for human activity recognition," *IEEE Trans. Ind. Informat.*, vol. 14, no. 10, pp. 4334–4342, Oct. 2018.
[73] M. Sandler, A. Howard, M. Zhu, A. Zhmoginov, and L.-C. Chen, "Mobilenetv2: Inverted residuals and linear bottlenecks," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit.*, 2018, pp. 4510–4520.
[74] W. Wang, V. W. Zheng, H. Yu, and C. Miao, "A survey of zero-shot learning: Settings, methods, and applications," *ACM Trans. Intell. Syst. Technol.*, vol. 10, no. 2, pp. 1–37, 2019.
[75] X. Liu, W. Yu, F. Liang, D. Griffith, and N. Golmie, "Towards deep transfer learning in industrial Internet of Things," *IEEE Internet Things J.*, vol. 8, no. 15, pp. 12163–12175, Aug. 2021.
[76] Z. Cui *et al.*, "A hybrid blockchain-based identity authentication scheme for multi-WSN," *IEEE Trans. Serv. Comput.*, vol. 13, no. 2, pp. 241–251, Feb. 2020.
[77] S. Huh, S. Cho, and S. Kim, "Managing IoT devices using blockchain platform," in *Proc. 19th Int. Conf. Adv. Commun. Technol.*, 2017, pp. 464–467.
[78] O. Novo, "Blockchain meets IoT: An architecture for scalable access management in IoT," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 1184–1195, Apr. 2018.
[79] C. V. Nguyen, Y. Li, T. D. Bui, and R. E. Turner, "Variational continual learning," 2018. [Online]. Available: https://openreview.net/forum?id=BkQqq0gRb
[80] S. Gong *et al.*, "Toward smart wireless communications via intelligent reflecting surfaces: A contemporary survey," *IEEE Commun. Surv. Tut.*, vol. 22, no. 4, pp. 2283–2314, Oct./Dec. 2020.

Xing Yang (Student Member, IEEE) received the M.S. degree in control engineering from the Nanjing University of Information Science and Technology, Nanjing, China, in 2018. He is currently working toward the Ph.D. degree in agricultural electrification and automation from College of Engineering, Nanjing Agricultural University, Nanjing.

He has been a Visiting Ph.D. Student with the University of Lincoln, Lincoln, U.K., since 2021. He has authored or coauthored papers in several prestigious journals/conferences, such as IEEE Wireless Communications, *IEEE/CAA Journal of Automatica Sinica*, and IEEE International Conference on Computer Communications. His current research interests include fault diagnosis in wireless sensor networks, agricultural Internet of Things reliability, and machine learning algorithm.

Lei Shu (Senior Member, IEEE) received the B.S. degree in computer science from the South Central University for Nationalities, Wuhan, China, in 2002, the M.S. degree in computer engineering from Kyung Hee University, Seoul, South Korea, in 2005, and the Ph.D. degree in computer engineering from Digital Enterprise Research Institute, National University of Ireland, Galway, Ireland, in 2010.

Until 2012, he was a Specially Assigned Researcher with the Department of Multimedia Engineering, Graduate School of Information Science and Technology, Osaka University, Osaka, Japan. He is currently a Distinguished Professor with Nanjing Agricultural University, Nanjing, China, and a Lincoln Professor with the University of Lincoln, Lincoln, U.K. He is also the Director of the NAU-Lincoln Joint Research Center of Intelligent Engineering, Nanjing, China.



Ye Liu (Member, IEEE) received the M.S. and Ph.D. degrees in electronic science and engineering from Southeast University, Nanjing, China, in 2013 and 2018, respectively.

He was a Visiting Scholar with Montana State University, Bozeman, MT, USA, from 2014 to 2015. He was a Visiting Ph.D. Student from 2017 to 2018 with the Networked Embedded Systems Group, RISE Swedish Institute of Computer Science, Kista, Sweden. He is currently a Researcher with Nanjing Agricultural University, Nanjing. He has authored or coauthored papers in several prestigious journals, such as the IEEE Communications Magazine, *IEEE Internet of Things Journal*, ACM Transactions on Embedded Computing System, and IEEE Network. His current research interests include wireless sensor networks, energy harvesting systems, and mobile crowdsensing.

Gerhard Petrus Hancke (Senior Member, IEEE) received the B.Eng. and M.Eng. degrees in computer engineering from the University of Pretoria, Pretoria, South Africa, in 2002 and 2003, respectively, and the Ph.D. degree in computer science from the Security Group, Computer Laboratory, University of Cambridge, Cambridge, U.K., in 2009.

He is currently an Associate Professor with the Department of Computer Science, City University of Hong Kong, Hong Kong, China. His current research interests include system security, embedded platforms, and distributed sensing applications.

Mohamed Amine Ferrag received the bachelor's, master's, Ph.D., and HDR degrees in computer science from Badji Mokhtar-Annaba University, Annaba, Algeria, in 2008, 2010, 2014, and 2019, respectively.

Since 2014, he has been a Senior Lecturer with the Department of Computer Science, Guelma University, Guelma, Algeria. Since 2019, he has been a Visiting Senior Researcher with the NAU-Lincoln Joint Research Center of Intelligent Engineering, Nanjing Agricultural University, Nanjing, China. Some of his research findings are published in top-cited journals, such as the IEEE Communications Surveys and Tutorials, *IEEE Internet of Things Journal*, IEEE Transactions on Engineering Management, and IEEE Access. His research interests include wireless network security, network coding security, and applied cryptography.

Kai Huang received the Ph.D. degree in agricultural engineering from China Agricultural University, Beijing, China, in 2018.

He is currently a Postdoctoral Researcher with the Department of Electrical Engineering, Nanjing Agricultural University, Nanjing, China. His main research interests include agricultural Internet of Things.

Dr. Huang has guest edited the special issue "Smart Agricultural Applications with Internet of Things" in *Sensors*. He has served as a PC Member in the "IoT Computing Systems" area of 3PGCIC-2019.

Authorized licensed use limited to: Account Rajalakshmi Institute of Technology - Chennai. Downloaded on February 22,2023 at 07:25:32 UTC from IEEE Xplore. Restrictions apply.