AnyCharge: An IoT-Based Wireless Charging Service for the Public

Kuan-Ting Lai, *Member, IEEE*, Fu-Chiung Cheng, Seng-Cho T. Chou, Yi-Chun Chang, Guo-Wei Wu, and Jung-Cheng Tsai

***Abstract*—Mobile phones have become a necessity of modern life and are used for various tasks, including audio calls, text messaging, Web surfing, video streaming, gaming, and payments. Most of these tasks consume significant battery power, which makes public charging services increasingly important. Therefore, there are many public places and private stores have started to provide free charging services. However, there are several issues that restrict the popularity of public charging service. First, people cannot easily find charging spots. Second, there is no effective way to monitor charging status and manage the chargers. Third, a free charging service increases business expenses. To address these issues, we developed a Internet of Things (IoT)-based wireless charging service system, which is called AnyCharge. There are five major components of AnyCharge: 1) a Wi-Fi enabled wireless charger; 2) an IoT gateway; 3) a cloud-based management platform; 4) a secure Wi-Fi auto-connection algorithm; and 5) a mobile app. The charger is connected to an IoT gateway through Wi-Fi using our secure auto-connection algorithm, and the gateways are linked to the cloud server using message queue telemetry transport. The administrators can monitor and control chargers using the management platform. In addition, Android and iOS apps have been created to allow users to locate free chargers and find the shortest route to the nearest charging spot. We initiated a large-scale experimental deployment in Taiwan, Thailand, Singapore, and Japan. More than 200 chargers have been installed in different places, including restaurants, hospitals, telecom stores, and hotels. Statistics shows that there is a strong demand for public charging services.**

***Index Terms*—Constrained application protocol (CoAP), Internet of Things (IoT), IoT security, message queue telemetry transport (MQTT), Wi-Fi automatic connection, wireless charging.**

I. Introduction

MOBILE devices are ubiquitous nowadays. In addition to making phone calls, people use cell phones to browse Web pages, buy products, pay bills, play video games, and even for live broadcast. Most of the mobile applications are heavy consumers of battery power. As a result, phones still run low on battery power over the course of a day despite advances in battery and power-saving technology. Because mobile phone functions have become so important to our daily activities, people are more willing to visit places with charging services. Some public places and private stores have noticed the need for charging, and have started to provide free charging. However, there are several issues that limit the widespread adoption of public charging services. First, there is no search engine to look up charging spots, so people cannot find the nearest place to charge in an emergency. Second, there is no effective way to monitor and control the chargers. Thus, it is hard to replace broken chargers or limit the usage of certain users. Third, a free charging service increases operation costs, which reduces the motivation of business owners to provide such services.

To solve these issues, we leveraged the latest Internet of Things (IoT) technology and developed an IoT-based wireless charging system to manage chargers. This novel service is called AnyCharge. We designed a Wi-Fi enabled wireless charger, which can automatically connect to an IoT gateway using our automatic and secure Wi-Fi connection algorithm. After the connection is established, the constrained application protocol (CoAP) [1] is used to communicate between the gateway and chargers. The IoT gateway is in charge of managing local chargers and connecting to the cloud server using the message queue telemetry transport (MQTT) protocol [2]. By connecting all the chargers to the cloud, we can monitor the charging status and control the chargers in real time. Therefore, AnyCharge knows where and when chargers are available, and can find the nearest charging spots for users. Android and iOS apps were developed to make it easier for users to search for charging spots. Furthermore, we are able to calculate and control the charging time of each user. Stores can leverage the information and combine promotions with the charging service, such as "30 minutes of free charging with a cup of coffee." The revenue generated from advertisements can compensate for the operation cost, and increase the incentive of business owners to provide the charging service. By utilizing the IoT technology, we built a very flexible service platform and created a win–win solution for the users and business owners.

Among the many charging methods, we selected the Qi wireless power standard [3] as our charging approach. The main reason is that the novelty of wireless charging can attract more users to try our service. The other benefits of wireless

Manuscript received January 3, 2019; revised August 30, 2019 and September 14, 2019; accepted September 17, 2019. Date of publication September 23, 2019; date of current version December 11, 2019. *(Corresponding author: Kuan-Ting Lai.)*

K.-T. Lai, G.-W. Wu, and J.-C. Tsai are with the Department of Electronic Engineering, National Taipei University of Technology, Taipei 10608, Taiwan (e-mail: ktlai@ntut.edu.tw; t107368004@ntut.edu.tw; t107368009@ntut.edu.tw).

F.-C. Cheng is with the Department of Computer Science and Engineering, Tatung University, Taipei 10452, Taiwan (e-mail: fccheng@ttu.edu.tw).

S.-C. T. Chou and Y.-C. Chang are with the Department of Information Management, National Taiwan University, Taipei 10617, Taiwan (e-mail: chou@ntu.edu.tw; d03725001@ntu.edu.tw).

Digital Object Identifier 10.1109/JIOT.2019.2943030

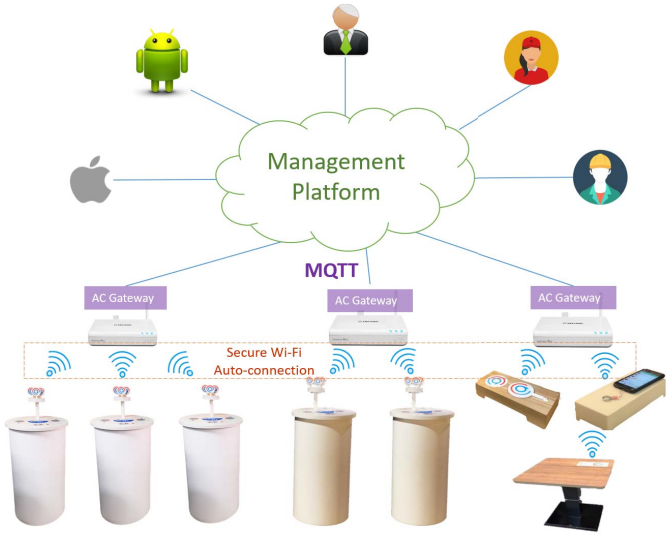
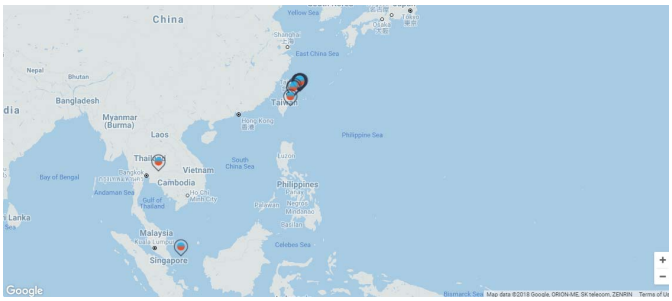
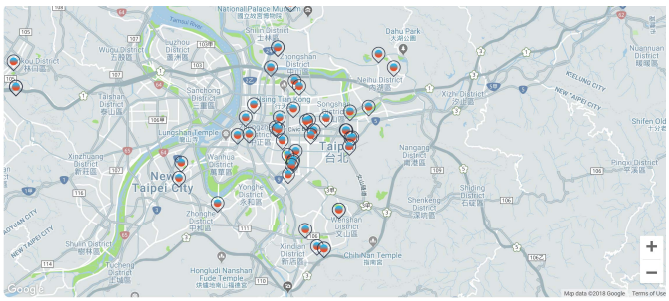


Fig. 1. Overview of AnyCharge's architecture. The system consists of five major components: 1) Wi-Fi enabled wireless charger; 2) IoT gateway; 3) cloud-based management platform; 4) secure Wi-Fi auto-connection algorithm; and 5) mobile app.



(a)



(b)

Fig. 2. Public charging spots shown on AnyCharge's map. (a) Charging spots in Southeast Asia. (b) Charging spots in Taipei.

charging include a unified charging interface for Android and iOS phones, and the ability to embed and hide chargers in furniture.

The system architecture of AnyCharge is shown in Fig. 1. AnyCharge consists of five major components: 1) a Wi-Fi enabled wireless charger; 2) an IoT gateway; 3) a cloud-based management platform; 4) a secure Wi-Fi auto-connection algorithm; and 5) a mobile app. The functions of each component are briefly described below.

1) *Wi-Fi Based Wireless Charger:* Our charger uses the Qi standard and supports high-power charging up to 15 W. This enables us to charge as fast as wired charging. A charger can automatically connect to a gateway through Wi-Fi and is controllable by the cloud management platform.
2) *IoT Gateway:* The gateway is in control of local chargers using the CoAP protocol. An encrypted SSID is generated for the chargers to connect automatically. Besides being a broker between the chargers and the cloud, the gateway needs to guarantee that the chargers work normally when the Internet connection is unstable.
3) *Management Platform:* We developed a Web-based platform on the cloud to manage all the chargers and gateways. This platform supports three main roles: a) administrator; b) engineer; and c) store manager. The administrator has the highest authority and can edit other roles. The engineer role is used to maintain and fix broken chargers. The store manager can control the behaviors of the chargers in his own stores, such as the charging mode or time limits.
4) *Secure Wi-Fi Auto-Connection Algorithm:* The Wi-Fi enabled charger requires no user interface to setup the Wi-Fi connection. Therefore, we developed several secure and automatic Wi-Fi connection algorithms, which automatically establish the connections between the chargers and gateways.
5) *Mobile App:* Android and iOS apps were developed for users to search for the nearest charging spots. In addition, a user can scan a QR code to enter extreme charging mode if he/she meets the criteria set by the store.

To evaluate our system, we initiated a large-scale deployment with funding from the Taiwanese government. More than 70 charging stations were installed at various places in different countries. The charging spots are listed in our apps and on our website. Fig. 2 shows screenshots of the charge map. The charging stations were installed in Taiwan, Thailand, and Singapore, as shown in Fig. 2(a). Most of the chargers were installed in Taipei, as shown in Fig. 2(b). The formal deployment began in January 2018, and a large quantity of charging data has been collected since then. The total charging time at all of the locations is around 68 min per day. In some places like 24-hour convenience stores, the total charging time is as high as 224.8 min per day. A detailed analysis is provided in Section VI.

In summary, we built an IoT-based public charging system, and launched a large-scale multination deployment. Our system is highly integrated and full featured, which can satisfy the needs of both the users and business owners. The experimental deployment was a successful proof-of-concept that indicated the strong demand for public charging.

The rest of this article is organized as follows. In Section II, we review the relevant IoT and wireless charging technology. The system architecture is presented in Section III, and the charging service is introduced in Section V. The automatic and secure Wi-Fi connection algorithm is elaborated in Section IV.

Section VI shows the statistical results of our experimental deployment, and the conclusion is provided in Section VII.

II. Previous Work

Al-Fuqaha *et al.* [4] conducted a thorough survey on IoT architecture, protocols, service integration, and key challenges. The basic IoT architecture is a three-layer model that consists of the perception layer, network layer, and application layer. The perception layer, also known as the sensor layer, is used to collect and process information. The network layer is in control of transmitting sensor data to the IoT hub or application server using different technologies, such as RFID, 3G, GSM, UMT, Wi-Fi, BLE, ZigBee, etc. The final layer is the application layer, which includes high-level applications, such as smart grids and smart cities. Other researchers proposed a five-layer service-orient architecture (SOA), which includes objects, object abstraction, service management, service composition, and application layer. From this perspective, the object (device) layer corresponds to the perception layer. The object abstraction transfers object data to the service management layer, which is analogous to the network layer. The other three layers belong to the application layer of the three-layer model. The service composition layer enables interactions between user requests and various IoT services [5], [6]. The software developed for the service composition is also called middleware, which is reviewed in [7]. Another review in the literature is [8], which provides a good summary of the state-of-the-art IoT architectures and relevant technologies.

A. IoT Protocols

During the last few years, many IoT protocols have been proposed [1], [2], [9]–[13], and some have been standardized [14]. Protocol innovations occurred in every layer of the seven-layer OSI model except the physical layer. In the link layer, IPv6 over low-power wireless personal area networks (6LoWPANs) were proposed to enable IPv6 packets to be carried efficiently on low-power devices with small link layer frames [15], [16].

In terms of the application layer, two of the most popular protocols are the CoAP [1] and MQTT [2]. The CoAP protocol implements HTTP's RESTful [17] operations (GET, POST, PUT, and DELETE), which enables direct mapping between the two protocols. Moreover, CoAP designed specific mechanisms for IoT, such as reliability, observation, group communication, and resource discovery. The abundant IoT features make CoAP prevalent, and the Internet Engineering Task Force (IETF) standardized CoAP as RFC 7252. Raza *et al.* proposed a DTLS algorithm for CoAP on 6LoWPAN [18].

The MQTT protocol is an ISO standard. The architecture of MQTT is based on the publish-subscribe messaging pattern. An MQTT client can be either a publisher or a subscriber. All the clients are connected to a server called a "broker," which is in charge of routing a publisher's messages to its subscribers. MQTT is a lightweight protocol with a small packet size, and the broker-based design provides an efficient way to exchange device information. These two factors make MQTT as one of the most popular IoT protocols. There is also a variant of MQTT for sensor networks, which is called MQTT-SN [19].

B. IoT Gateway

The main function of the IoT gateway is to bridge the local network of devices into the Internet. Gateways have been widely used to connect wireless sensor networks (WSNs) to cloud servers. Moreover, gateways equipped with additional computation resources can perform edge computing and manage devices locally. Zhu *et al.* developed an IoT gateway based on the ZigBee and GPRS protocols, and bridged the ZigBee sensor network to the Internet [20]. Datta *et al.* [21] proposed the use of a wireless gateway to build a real-time machine-to-machine (M2M) communication platform. The proposed platform assigns a unique ID to each device and generates metadata for sensor values. The gateway is used to communicate with old sensors without wireless connection capability. The services are provided in the representational state transfer (REST) paradigm. Recently, Saxena *et al.* [22] created a 5G gateway prototype to further increase the gateway bandwidth.

The most popular open source software for a gateway is Eclipse Kura, which is based on Java/OSGi [23]. The OSGi is known as the Open Services Gateway initiative, and is a dynamic module system for Java. Kura uses MQTT to connect to the cloud server, and provides many important functions, such as gateway I/O control, network configuration, watchdog, Web administration interface, etc. Kura can be installed on any embedded hardware platform with JVM installed. Although Kura is full featured and reliable, it requires more computational resources to run OSGi, and does not have an automatic Wi-Fi connection mechanism. Therefore, we developed our own lightweight gateway program with secure and automatic connection algorithms.

C. Wireless Charging

The fundamental theory of wireless charging is to transfer energy between a charger and a receiver via electromagnetic induction. The charger uses an induction coil to create an alternating electromagnetic field. The receiver uses another induction coil to receive power from the electromagnetic field, and converts it back to current [24]. There are two charging methods: 1) magnetic induction charging and 2) magnetic resonance charging. Magnetic induction charging has a long history, with the first experiment conducted by Nikola Tesla in 19th century. Therefore, the inductive wireless charging technology is mature and efficient. However, there is one drawback: the power drops rapidly with distance, obeying the inverse-square law. This issue limits the maximum charging distance to 4 cm in the latest Qi standard, and coils of transmitter and receiver need to be aligned. A mathematical model for calculating the effects of distance and misalignment in wireless power transfer efficiency can be found in [25]. Gao *et al.* [26] have conducted experiments to measure the efficiency under different vertical and horizontal displacements.

To address this issue, Kurs [27] proposed to transfer power by making the coils of the receiver and charger resonant at the

Fig. 3. Appearance of a Wi-Fi enabled wireless charger and receiver. The receivers are made for phones without built-in wireless charging support.

same frequency. The proposed method is still inductive, but the strong coupling between the resonant coils enables power to be transferred in tens of centimeters. A comprehensive technical comparison between inductive and resonant wireless charging can be found in [28].

There have been three main wireless charging organizations. The Wireless Power Consortium (WPC) was founded in 2008. The Alliance For Wireless Power (A4WP) and the Power Matters Alliance (PMA) were founded in 2012. WPC proposed the Qi standard based on magnetic induction charging in 2010, and added the resonant mode years later. Qi has been widely adopted by many Android phones. The A4WP and PMA merged into the AirFuel Alliance in 2015. In September 2017, Apple announced to support Qi in its new iPhone 8 series and iPhone X. After Apple joined WPC, Qi has become the single unified wireless charging standard for mobile phones.

D. Public Charging Service

There have been many trial deployments of public charging services during the past few years. In 2014, Starbucks started to deploy wireless chargers in some stores in the United States using resonant technology from Powermat [29]. Powermat used the PMA standard in the beginning, but then joined WPC to embrace the Qi standard in early 2018. ChargeItSpot [30] designed the charging kiosk, which has been deployed in clothes stores such as Under Armour. InforCharge [31] has deployed A4WP wireless chargers in Taiwan. Among the many charging service providers, Aircharge [32] provided the Qi wireless charging service for McDonalds in London, which is similar to our service. However, their chargers do not have IoT connections, and cannot be controlled and monitored in real time. Recently, ChargeSPOT in Hong Kong [33] has started a power bank rental service at airports in Hong Kong, Japan, and Malaysia. Compared with other public charging services, AnyCharge is the only one equipped with IoT technology, and can perform real-time control and monitoring. This key difference enables us to provide more flexible service to both users and business owners.

III. System Architecture

In this section, we will elaborate each component of our system. There are five major components: 1) a Wi-Fi enabled wireless charger; 2) an IoT gateway; 3) a cloud-based management platform; 4) a secure Wi-Fi auto-connection algorithm; and 5) a mobile app. The details of each component are present in the following sections.

(a) (b)

Fig. 4. Charging phone (a) with or (b) without built-in Qi support.

Fig. 5. Circuit boards inside our charger. The main round PCB board is the charging module, and the Wi-Fi module is attached at the side.

A. Wi-Fi Enabled Wireless Charger

The first building block of our system is the Wi-Fi enabled charger. Fig. 3 shows the appearance of the charger and receiver. The charger can be embedded under furniture and integrated into the decorations of different environments. The receiver is designed for phones without built-in wireless charging support. We will illustrate and compare the two charging approaches as shown in Fig. 4. The main circuit module and Wi-Fi module of the charger are shown in Fig. 5.

Additionally, our charger supports two charging modes: 1) normal charging and 2) extreme charging. The normal charging provides 5 W (5 V$\times$1 A) while the extreme charging provides 15 W (9 V$\times$1.67 A). The charge conversion rate is around 75%. A user can use the AnyCharge mobile app to unlock the extreme charging mode if he meets some criteria set up by the store. We will further discuss the charging mode in Section V-A.

B. IoT Gateway

The IoT gateway is in charge of managing local chargers, especially when the Wi-Fi connection is unstable. Fig. 6 shows a photograph of the gateway. The gateway connects to the cloud using the MQTT protocol, and communicates with local chargers using CoAP. We developed the gateway software using Java because of the portability. Regarding the underlying hardware platform, we selected the Universal Developer Kit (UDK-21) developed by Tatung Company

Fig. 6. IoT gateway of our system, which is used to manage local chargers.

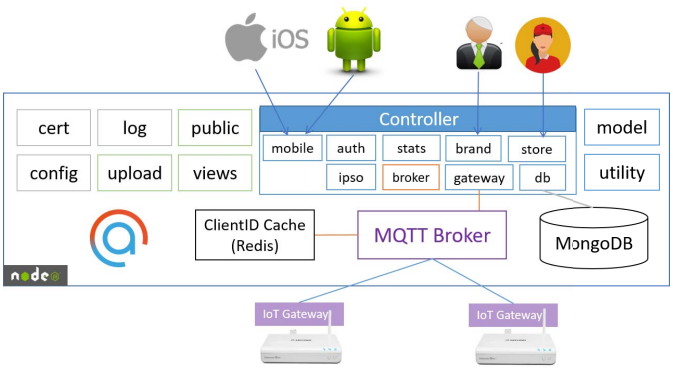


Fig. 7. Architecture of management platform. The platform was developed by node.js and has RESTful APIs for the different roles and mobile app.

and STMicroelectronics [34]. Note that our gateway software can be executed on any embedded platform with JVM since it is written in Java. The gateway has two built-in network interfaces: Ethernet and Wi-Fi. It can also support 4G transmission by attaching a 4G dongle.

C. Management Platform

The cloud-based management platform can be used to manage chargers, gateways, users, and stores. The architecture of the management platform is shown in Fig. 7. We developed the system using node.js, Angular.js, and MongoDB. The lightweight node.js server is combined with the NoSQL database enables us to scale up system easily. The management platform supports four types of roles: 1) administrator; 2) guest; 3) engineer; and 4) store manager. The details of each role are described below.

1) *Administrator:* This role is the super user of the system, and can manage all the devices as well as other roles. An administrator can edit the information of the chargers, gateways, stores, guests, managers, and engineers.
2) *Guest:* This role was created for demonstration purposes. A guest can view the statistics of public charging spots.
3) *Engineer:* An engineer can access the hardware information and perform necessary maintenance.
4) *Store Manager:* A store manager can manage the chargers in his store and set up charging rules for his customers.

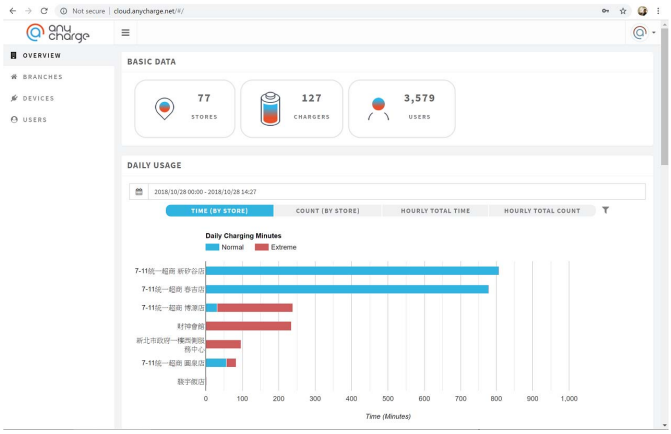


Fig. 8. Main page of management platform for administrator. The first widget summarizes the total stores, chargers, and registered users. The second widget shows the daily usage of each store.

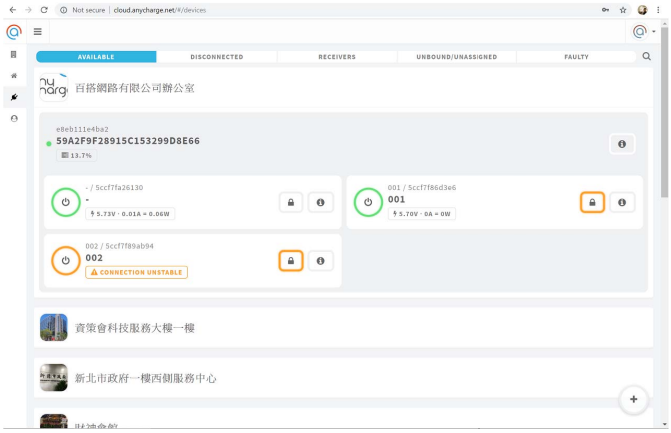


Fig. 9. Hardware monitor page for engineer, which shows the charger status in real time.

We developed RESTful APIs for Android, iOS, and Web Apps. An MQTT broker is employed to communicate with IoT gateways. MongoDB was chosen as the default database. The scalability of the NoSQL database allows us to extend our system easily.

Fig. 8 shows the main page for the administrator. The first widget reveals the total number of the stores, chargers and registered users. The second widget displays today's charging statistics. The hardware monitor page is shown in Fig. 9, which can be used by the engineers to check the status of chargers and gateways. The charging statistics can be viewed in the statistics page of the management platform. Fig. 10 shows the summary statistics page of daily usage. The minimum unit of the charging time is one minute.

D. Secure Wi-Fi Auto-Connection Algorithm

Because the Wi-Fi enabled chargers have no user interface, we need a mechanism that allows chargers to search and connect to gateways automatically. Moreover, the mechanism needs to be safe and secure. We have developed three algorithms: 1) the preshared key (PSK) auto-connection algorithm; 2) one-time password (OTP) auto-connection algorithm; and

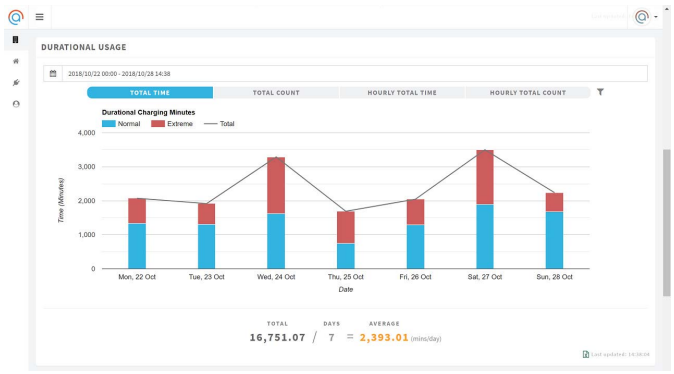


Fig. 10. Statistics widget showing the bar chart of daily charging minutes. The red part represents the extreme charging while the blue part represents the normal charging.

3) device validation algorithm. The details are provided in Section IV.

E. Mobile App

The mobile app allows users to search for the nearest charging spots, register as members, and switch between charging modes. Screenshots of our app are shown in Fig. 11. The login page is shown in Fig. 11(a). A user can choose to login using a Facebook account, register a new account using e-mail, or skip the registration for now. Fig. 11(b) is the QR scan page, which can be used to unlock extreme charging. Fig. 11(c) shows the charging status of the phone and history of the charging records. The charger map is shown in Fig. 11(d), which can display the real-time charging status of selected stores, as well as find the shortest path to the nearest charging spot. The apps can be downloaded from the Google Play Store[1] and Apple App Store.[2]

IV. Automatic and Secure Wi-Fi Connection

Since the chargers have no user interface and are embedded under the furniture, a mechanism is required to enable the client devices to automatically and securely connect to a gateway through Wi-Fi. The first Wi-Fi standard, IEEE 802.11, was released in 1997. It has quickly become the de facto short-range wireless communication standard, and attracted the attention of many hackers. To enhance the security, the Wi-Fi alliance developed the 802.11i standard, Wi-Fi Protected Access (WPA) and WPA2. The latest security standard (WPA3) was announced in June 2018 [35]. Kumar and Gambhir [36] conducted a literature review of Wi-Fi security threats. Alipour *et al.* [37] proposed to extract specific fields from Wi-Fi packets, and applied machine learning algorithms to detect malicious attacks. Waliullah *et al.* [38] demonstrated how to crack the WPA2 passwords of commercial routers using dictionary attack. Kolias *et al.* [39] created a large-scale dataset containing the activities of common Wi-Fi attacks, and evaluated several machine learning algorithms for

[1]https://play.google.com/store/apps/details?id=com.boundlessnet.anycharge
[2]https://itunes.apple.com/us/app/anycharge/id1117457899?mt=8

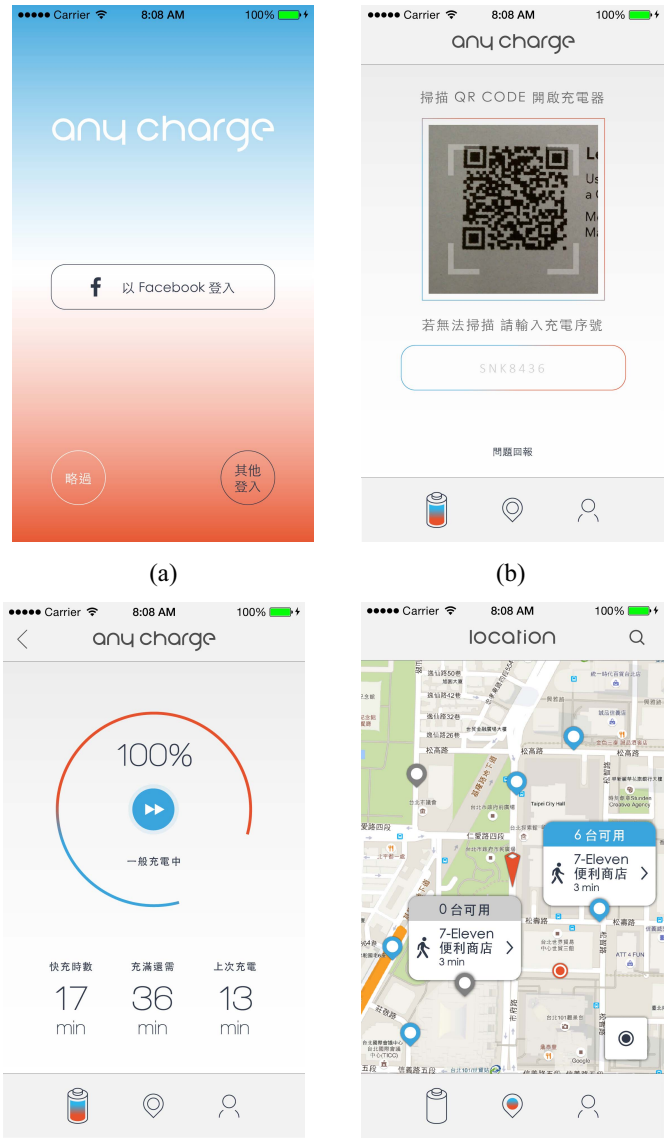


Fig. 11. Screenshots of AnyCharge App. (a) Login. (b) Scan QR code. (c) Charging status. (d) Charge map.

intrusion detection. Recently, Thing *et al.* [40] proposed to detect anomaly events using deep learning algorithms.

In this article, we propose to further enhance the security by adding authorization algorithms. We developed two secure and automatic algorithms and one device validation algorithm [41]. The details of each algorithm are presented in the following.

A. Pre-Shared Key Auto-Connection

A cryptosystem is symmetric if the encrypting and decrypting keys are the same. Given a plaintext message m, a symmetric cryptosystem can be defined as

$$d_k(e_k(m)) = m \tag{1}$$

where k is the key, e_k is the encrypting function, and d_k is the decrypting function. The most common symmetric encrypting function is AES [42].

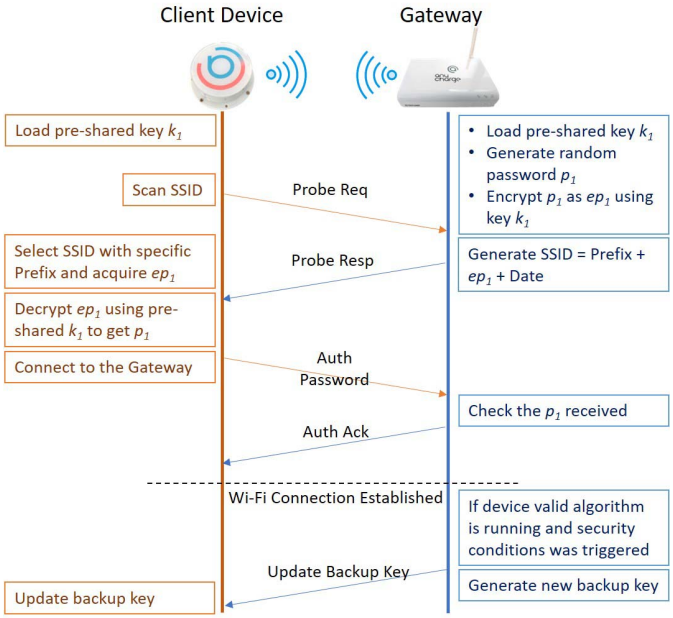


Fig. 12. Protocol of secure and automatic connection with PSK.

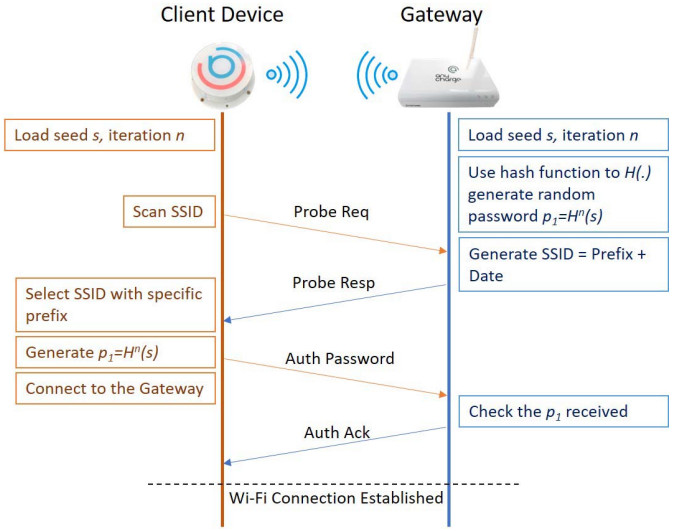


Fig. 13. Protocol of secure and automatic connection using OTP.

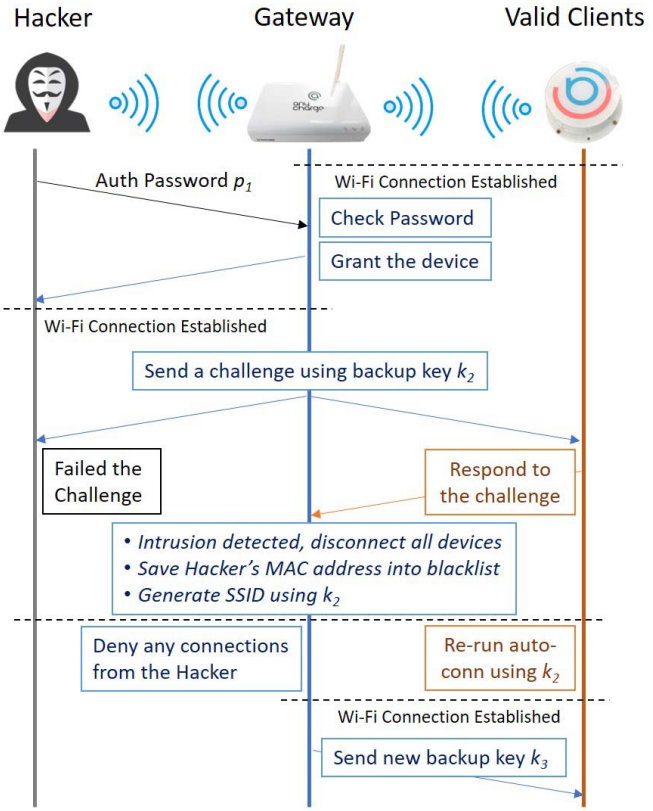


Fig. 14. Valid algorithm for secure Wi-Fi automatic connection.

Fig. 12 illustrates the procedure of the proposed method. Each step of the algorithm is explained below.

1) The gateway loads the PSK k_1 and generates a random password p_1.
2) Encrypt p_1 using PSK k_1 by applying an encrypting function to generate encrypted password ep_1, where $ep_1 = e_{k_1}(p_1)$.
3) Generate an SSID by concatenating an SSID-Prefix, ep_1 and the current date.
4) The client device starts sending probe requests to the surrounding gateways.
5) Once received a probe request, the gateway sends a probe response back.
6) The client device selects the gateway SSID with a specific prefix, and retrieves ep_1 from the SSID.
7) The client device decrypts ep_1 with the preshared k_1 and recovers password p_1.
8) The gateway and client device then perform a 4-way handshake to establish the Wi-Fi connection.
9) Once connected, the gateway can generate a new shared key k_2 and send it to the device.
10) (Optional) If the device validation algorithm is running and any intrusion is detected, the gateway will generate a new backup key and send it to the client.
11) The gateway updates k_1 periodically (e.g., every day at midnight), and disconnects all the clients to rerun the auto-connection process.

B. One Time Password Auto-Connection

In the OTP auto-connection, the gateway, and client devices have no preloaded shared key. Instead, an OTP is generated whenever the Wi-Fi service of the gateway is started. There are two major OTP methods: 1) the time-synchronized method and 2) mathematical algorithms, e.g., hash chain [43]. Both methods usually employ a one-way function, which is easy to compute but hard to invert. That is, the probability of computing a pseudoinverse of a one-way function is negligible. The formal definition of one-way function is defined as below. Given a function $f : \{0, 1\}^* \mapsto \{0, 1\}^*$, whose input and output are binary strings, for all randomized algorithms F and all positive integers c

$$\Pr(f(F(f(x)) = f(x)) < n^{-c} \tag{2}$$

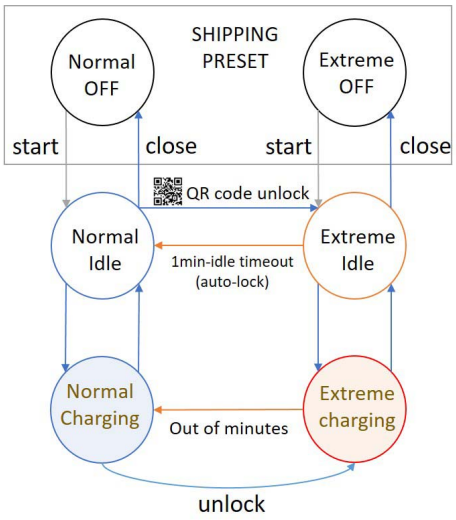


Fig. 15. Finite state machine for switching between normal and extreme charging modes.

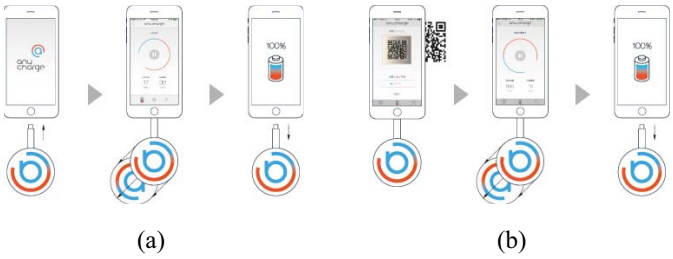


Fig. 16. Visual instructions for using AnyCharge receiver and how to activate extreme charging. (a) Normal charging. (b) Extreme charging.

Fig. 17. Dimensions of our charging station. The total height is 130 cm and the diameter of the table is 60 cm.

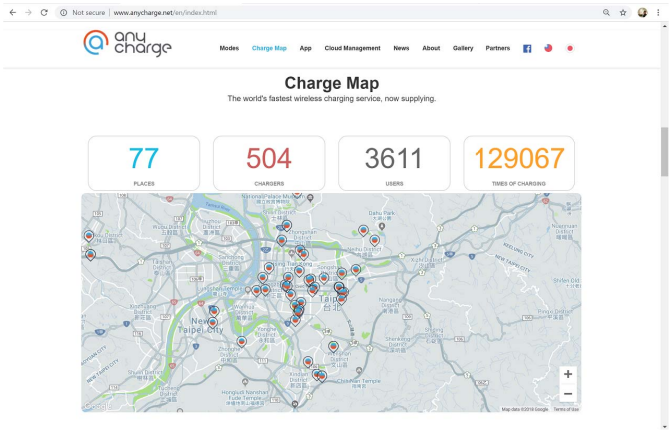


Fig. 18. Real-time summary statistics shown on our Web page on November 11, 2018.

Fig. 19. Store page lists information for stores owned by the manager.

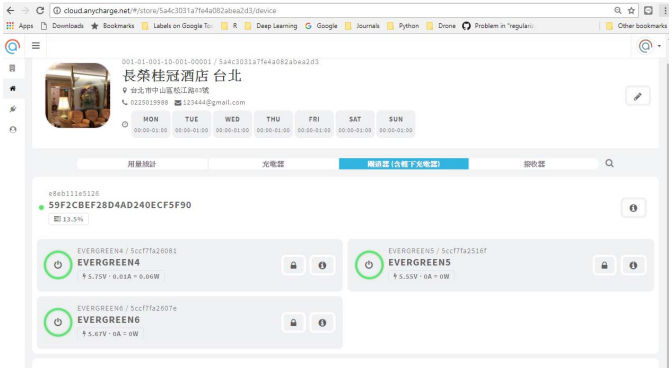


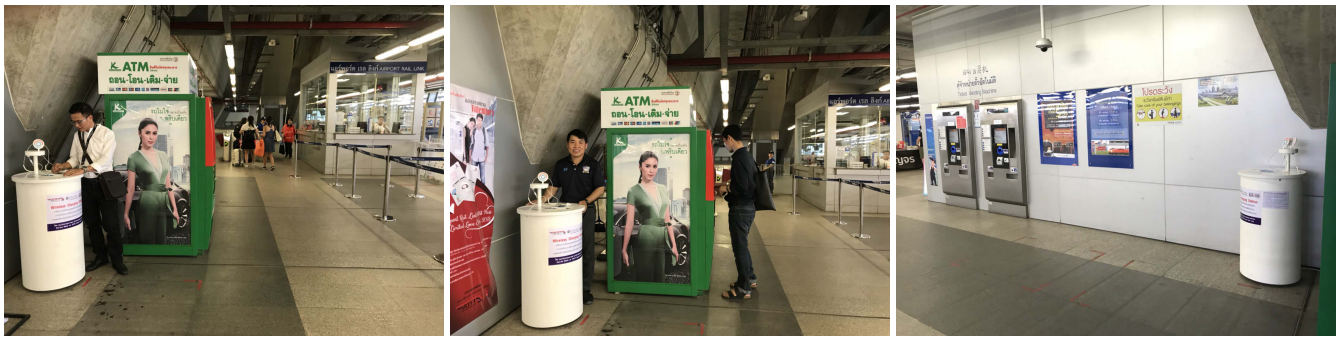
Fig. 20. Hardware monitoring page of store, which shows real-time status of chargers under each gateway.

where $n = \text{length}(x)$. The inversion probability is over the choice of x and randomness of F [44]. In cryptography, the one-way function is usually called hash function [45]. The most common algorithms are the Secure Hash Algorithms (SHA) published by NIST. The latest hash function in the SHA family is SHA-3 [46], which was released in 2015.

In practice, it is difficult to keep the times of all the IoT devices accurately synchronized before connecting to the Internet. Therefore, we selected the hash chain as our OTP generator, and developed an auto-connection algorithm without a PSK. The hash chain is defined as

$$h\big(h^i(s)\big) = h^{(i+1)}(s) \tag{3}$$

where s is a seed and i is the iteration of hashing.



(a) (b) (c)

Fig. 21. Charging stations installed in subway stations in Thailand. (a) and (b) are installed in Makkasan station. (c) is installed in Suwannabhumi station.

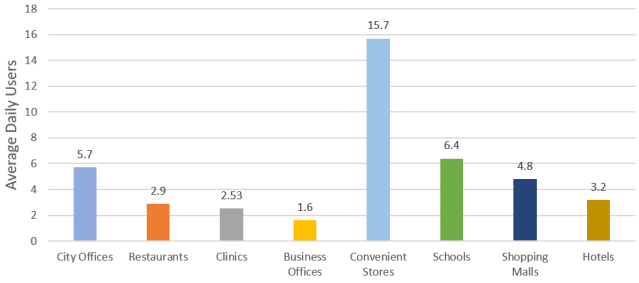


Fig. 22. Average daily users for different location types.

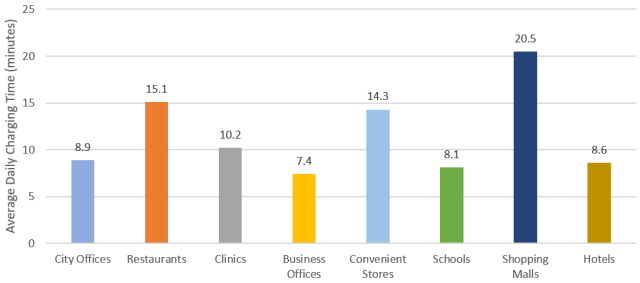


Fig. 23. Average daily charging minutes for different location types.

Based on the hash chain, the proposed OTP auto-connection algorithm is illustrated in Fig. 13. Each step of the algorithm is explained below.

1) The gateway loads a preshared seed s and iteration number n, and generates the password p_1 by repeatedly applying hash function $h(.)$ to the seed s by n times, where $p_1 = h^n(s)$.
2) The gateway generates an SSID by concatenating the SSID-Prefix and date.
3) The client device starts sending probe requests to the surrounding gateways.
4) Once received a probe request, the gateway sends back a probe response.
5) The client generates password p_1 with preloaded seed s, repeat times n, and hash function $h(.)$
6) The client device selects the correct gateway with the target SSID and logs in with password p_1.
7) The gateway and client device then perform a 4-way handshake to establish the Wi-Fi connection.
8) The gateway updates the password periodically (e.g., every midnight) by decreasing the iteration number n, and generating password $p_2 = h^{n-1}(s)$. A new random iteration number will be generated if the hash chain is exhausted ($n = 0$).

C. Device Validation Algorithm

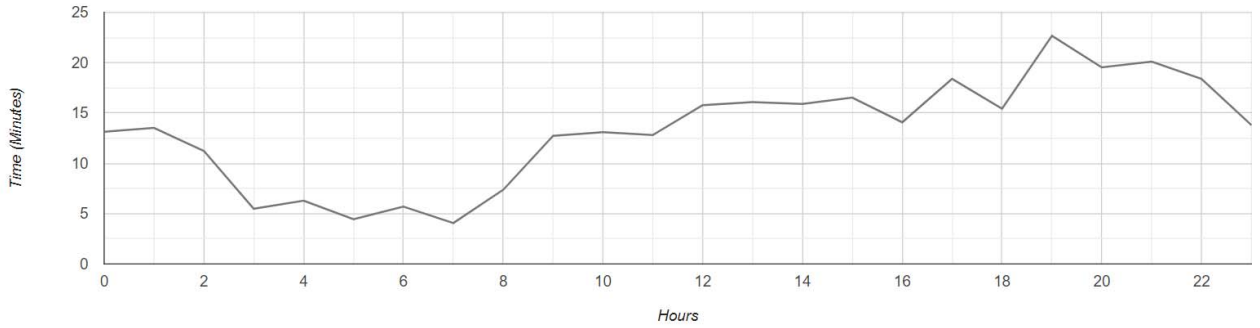
The auto-connection algorithms presented in the previous sections can be further secured by applying the device validation algorithm. The basic idea is saving a backup key k_2 or hash function $h_2(.)$ in client devices, and the gateway send a challenge request to the client devices after the Wi-Fi connection is established. The details of our device validation algorithm are listed below.

1) A hacker device cracks password p_1 and successfully logs in the Wi-Fi network of the gateway.
2) The gateway sends a challenge message encrypted with key k_2. Without key k_2, the hacker device will fail the challenge.
3) Once the challenge failure is detected, the gateway will add the hacker's MAC address into the blacklist to prevent further connections, and notify all the clients of the intrusion.
4) The gateway will disconnect all the clients and rerun the auto connection algorithm using backup key k_2.
5) All the clients reconnect to the gateway using k_2.
6) The gateway generates a new backup key k_3 and sends it to all the clients.

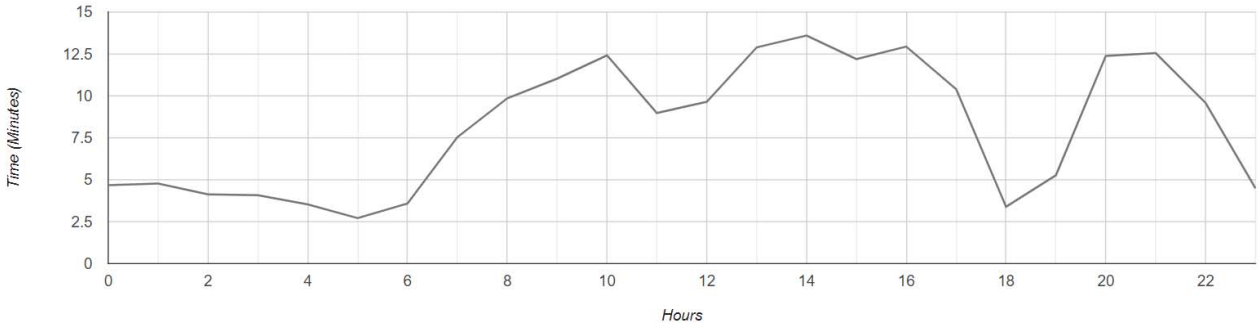
V. Charging Service

A. Normal Charging and Extreme Charging

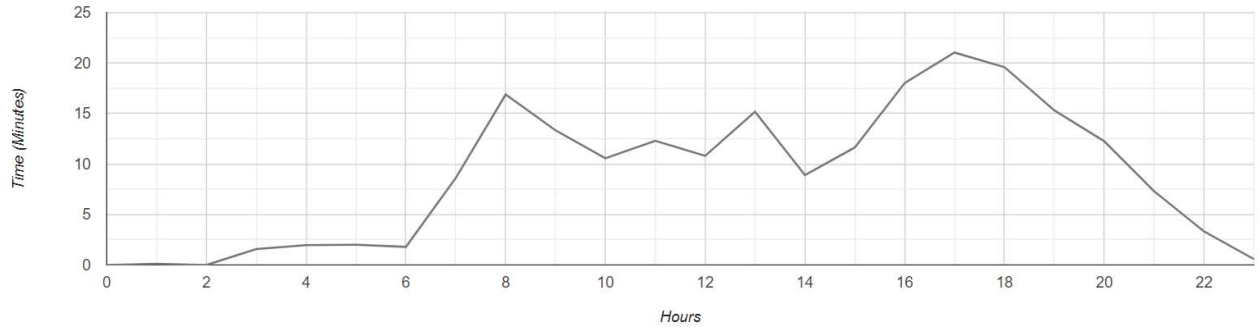
As previously mentioned, we designed two charging modes: 1) normal charging and 2) extreme charging. The charging speed differentiation strategy plays an important role in our service model. By default, the charger provides only the normal charging speed at 5 W. If a user wants to unlock the extreme charging mode, he/she can register as a member of AnyCharge, and receive 30 min of free extreme charging. The user can obtain more extreme-charging minutes by fulfilling some requirements, such as buying a cup of coffee, or using



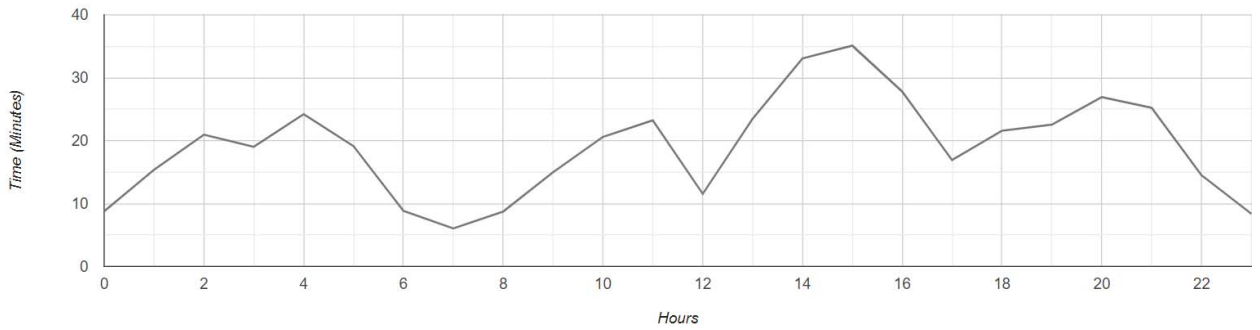
(a)



(b)



(c)



(d)

Fig. 24. Average hourly charging time at convenience stores in 2018. There are four stores in different types of districts: commercial and residential mixed-use district, industrial district, business district, and university district. (a) Average hourly charging time of store A in the commercial and residential mixed-use district. (b) Average hourly charging time of store B in the industrial district. (c) Average hourly charging time of store C in the business district. (d) Average hourly charging time of store D in the university district.

a credit card from a certain bank. In other words, we have turned charging service into a promotion tool, which increases the willingness of business owners to install chargers.

The control flow of the charging mode is illustrated in Fig. 15. As shown in the figure, a charger can be preconfigured to use the normal or extreme mode before shipping,

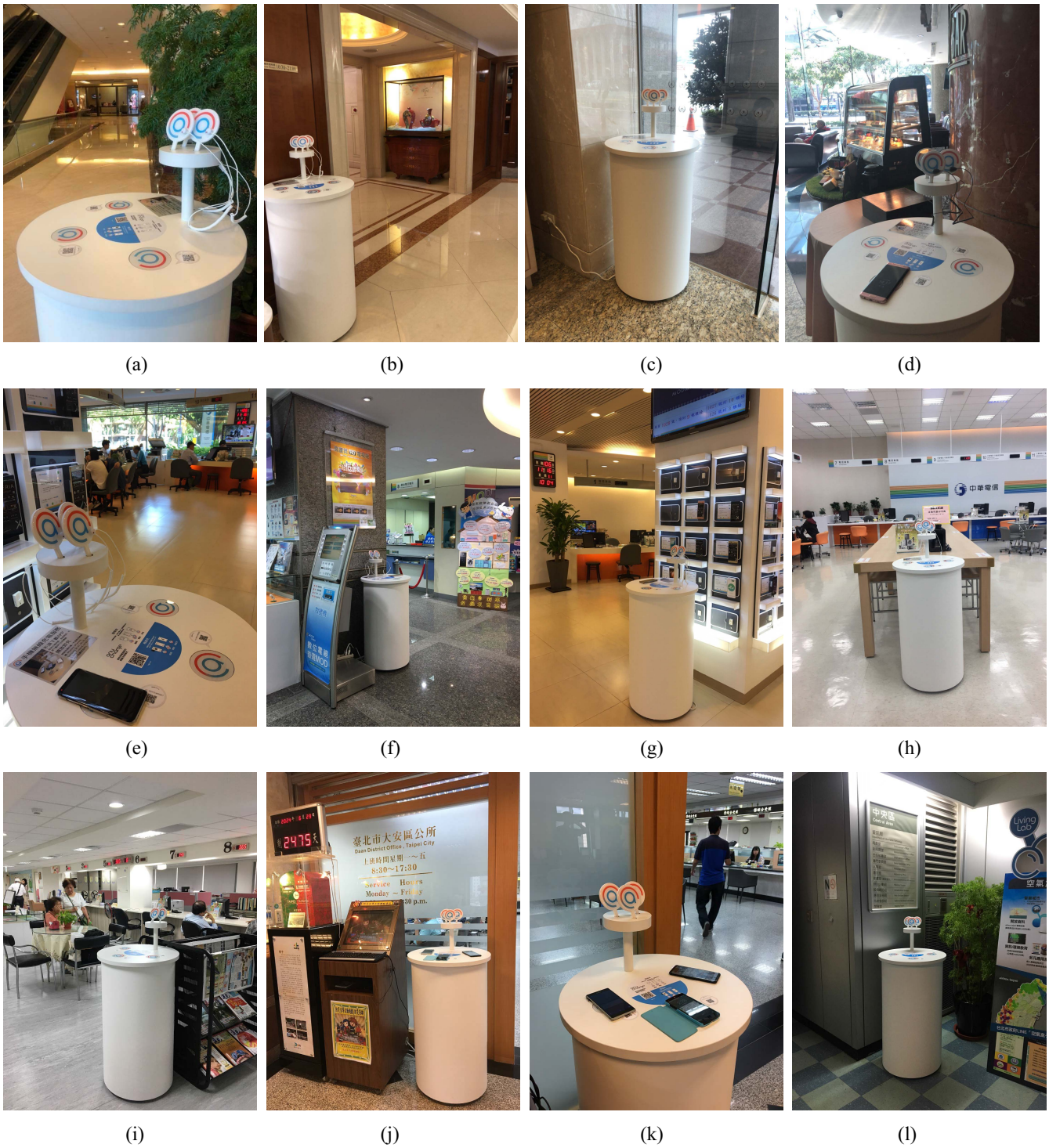


Fig. 25. Photographs of charging stations installed in different places. The stations in the first row ((a), (b), (c), (d)) are installed in hotels, the stations in the second row ((e), (f), (g), (h)) are installed in telecom stores, and the stations in the third row ((i), (j), (k), (l)) are installed in city offices.

and will enter the normal or extreme idle mode after the power is on. To unlock the extreme charging mode, a user needs to scan the QR code of the charger before charging. The charger will change from the normal/extreme idle state to the normal/extreme charging state when a user begins to charge his/her phone. After the charging is done, the charger will return to the idle state and wait for the next user. The state automatically switches from extreme idle to normal idle after idling for a period of time. The default timeout length is 1 min. The visual instructions used to explain how to change charging modes are shown in Fig. 16.

B. Charging Station

The Wi-Fi enabled charger was designed to be embedded into a table and fixed by screws underneath. However, most

TABLE I
STATISTICS FOR DIFFERENT INSTALLATION SITES

Type	City Offices	Restaurants	Clinics	Telecom Stores	Business Offices	Convenient Stores	Subways	Schools	Shopping Malls	Hotels
Installed Base	16	8	11	8	10	5	2	3	4	10
Avg. Daily Users	5.7	2.9	2.53	N/A	1.6	15.7	N/A	6.4	4.8	3.2
Avg. Daily Minutes	50.8	43.8	25.9	N/A	12.4	224.8	N/A	51.84	98.6	27.8
Avg. Charging Time	8.9	15.1	10.2	N/A	7.4	14.3	N/A	8.1	20.5	8.6

stores do not want to modify their decorations. To simplify the installation process, we designed a movable charging station with wheels. The appearance and dimensions of this charging station are shown in Fig. 17. The station consists of two parts: 1) a cylindrical container with a round table on top and 2) a single-rod receiver stand on the table. Three chargers are embedded in the table. The container is 100 cm tall, and the diameter of the top table is 60 cm. The height of the receiver stand on the table is 30 cm tall. With three wheels attached to the bottom, the charging station can easily be moved to and installed at any place with an AC power socket. This feature makes it extremely suitable for public places. We will see in Section VI that most of our installations are charging stations.

VI. EXPERIMENTAL DEPLOYMENT

Since 2018, we have launched a large-scale multination experimental deployment. The summary statistics are updated in real time on our website (www.anycharge.net), as shown in Fig. 18. To date, we have installed chargers at 77 locations in Taiwan, Thailand, the Philippines, and Singapore. Our service has been used more than 130 000 times, and more than 3000 users have registered as AnyCharge users. The details of the installations and statistics will be introduced in the following sections.

A. Installation and Management

To study the usage rate of our service, we tried to deploy the charging stations in various types of places. The installation locations include city offices, restaurants, hospitals, dental clinics, plastic surgery clinics, telecom stores, business offices, 24-hour convenience stores, subways, universities, shopping malls, hotels, etc. More than 90% of the installations are charging stations, some are desktop chargers, and a few are customized embedded chargers. All the store information is saved in our database and can be searched using the management platform. The store management interface is shown in Fig. 19. The small number under the store name shows the presently available chargers. As introduced in Section III-C, the store manager can see the information for his/her own stores, while the administrator can see information for all the stores. Additionally, the store manager has permission to check the status of the chargers and gateways at each store, as shown in Fig. 20.

Some photographs of the installed charging stations are shown in Figs. 21 and 25. The charging stations installed at subways in Thailand are shown in Fig. 21. With regard to the photographs in Fig. 25, the four stations in the first row are installed in hotels. The stations in the second row are installed in telecom stores, and the last four stations in the third row are installed in city offices.

B. Statistics Analysis

Table I lists the charging statistics for each type of installation site. The statistics of the telecom stores and subways cannot be shown due to nondisclosure agreements. The most frequently used type of charging location is the convenience store. An average of 15.7 people use the service every day. The convenience stores are opened 24 h a day in Taiwan, which can explain why the average number of users is more than twice that for the other types of locations. The place with the longest charging time is the shopping mall. The average charging time at the shopping mall is 20.5 min. The shopping mall, restaurants, and convenience stores tend to have longer charging times because the customers prefer to stay at the location longer. Most of the restaurants in our installed base are coffee shops.

We further analyze the hourly usage of our service. The average hourly charging minutes of convenience stores in 2018 are shown in Fig. 24. Among many types of locations, the convenient store was chosen for analysis because it has the highest total charging time. We showed the line charts of hourly charging time of stores A, B, C, and D, which are located in the commercial and residential mixed-use district, industrial district, business district, and university district, respectively. Store A has high charging usage from 6:00 P.M. to 2:00 A.M. because most customers visit the store after work. Store B has high usage rate from 8:00 A.M. to 9:00 P.M., with a drop at 6:00 P.M., which may be caused by that workers get off work around 6:00 P.M. Store C is in business district and has no usage from 11:00 P.M. to 2:00 A.M. It is because that most of the white-collar workers have already returned home after 10:00 P.M. Store D is located in the university neighborhood. One interesting observation is that there is a demand of charging from midnight to 4:00 A.M.

In terms of the other types of locations, the statistics of business offices actually vary largely, because some of the charging stations are placed in lobbies, and some are placed in offices. The charging stations at schools are installed in student activity centers, and have shorter charging times on average. Two of the clinics in the installed base are dentist clinics, one is a plastic surgery clinic, and others are clinic rooms in hospitals. Regarding hotels, all the charging stations are placed in lobbies, as shown in Fig. 25(a)–(d). The overall daily average user is 5.4 people, and the average charging time is 12.5 min.

VII. Conclusion

In this article, we presented an IoT-based wireless charging system called AnyCharge, which provides a free public charging service. By leveraging the latest IoT technology, we are able to turn free charging into a promotion tool, and create a win–win solution for both users and business owners. A large-scale deployment was conducted in Taiwan, Thailand, and Singapore. More than 200 chargers have been installed at 77 different locations, and attracted around 4000 users to register as AnyCharge members. The statistics revealed that there is an average of 5.4 daily users, and each user charges for 12.5 min on average. The experimental deployment showed the great potential of this public charging service. For future work, we will combine AnyCharge with more advertising tools, such as interactive digital signage, to increase the revenue.

Acknowledgment

The authors would like to thank the Department of Industrial Technology (DoIT) of the Ministry of Economic Affairs, Taiwan, for sponsoring the development and deployment of this project.

References

[1] Z. Shelby, K. Hartke, and C. Bormann, "The constrained application protocol (CoAP)," Internet Eng. Task Force, RFC 7252, Jun. 2014. [Online]. Available: https://tools.ietf.org/rfc/rfc7252.txt

[2] A. Banks and R. Gupta, *MQTT Version 3.1.1*, OASIS Standard, 2014.

[3] D. Van Wageningen and T. Staring, "The Qi wireless power standard," in *Proc. IEEE 14th Int. Power Electron. Motion Control Conf. (EPE/PEMC)*, 2010, pp. S15–S25.

[4] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2347–2376, 4th Quart., 2015.

[5] I.-R. Chen, J. Guo, and F. Bao, "Trust management for SOA-based IoT and its application to service composition," *IEEE Trans. Services Comput.*, vol. 9, no. 3, pp. 482–495, May–Jun. 2016.

[6] A. Urbieta, A. González-Beltrán, S. B. Mokhtar, M. A. Hossain, and L. Capra, "Adaptive and context-aware service composition for IoT-based smart cities," *Future Gener. Comput. Syst.*, vol. 76, pp. 262–274, Nov. 2017.

[7] A. H. Ngu, M. Gutierrez, V. Metsis, S. Nepal, and Q. Z. Sheng, "IoT middleware: A survey on issues and enabling technologies," *IEEE Internet Things J.*, vol. 4, no. 1, pp. 1–20, Feb. 2017.

[8] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1125–1142, Oct. 2017.

[9] P. Bellavista and A. Zanni, "Towards better scalability for IoT-cloud interactions via combined exploitation of MQTT and CoAP," in *Proc. IEEE 2nd Int. Forum Res. Technol. Soc. Ind. Leveraging Better Tomorrow (RTSI)*, 2016, pp. 1–6.

[10] T. Song, R. Li, B. Mei, J. Yu, X. Xing, and X. Cheng, "A privacy preserving communication protocol for IoT applications in smart homes," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1844–1852, Dec. 2017.

[11] C.-T. Cheng, N. Ganganath, and K.-Y. Fok, "Concurrent data collection trees for IoT applications," *IEEE Trans. Ind. Informat.*, vol. 13, no. 2, pp. 793–799, Apr. 2017.

[12] V. Arora, F. Nawab, D. Agrawal, and A. El Abbadi, "Multi-representation based data processing architecture for IoT applications," in *Proc. IEEE 37th Int. Conf. Distrib. Comput. Syst. (ICDCS)*, 2017, pp. 2234–2239.

[13] S. Bera, S. Misra, S. K. Roy, and M. S. Obaidat, "Soft-WSN: Software-defined WSN management system for IoT applications," *IEEE Syst. J.*, vol. 12, no. 3, pp. 2074–2081, Sep. 2018.

[14] I. Ishaq *et al.*, "IETF standardization in the field of the Internet of Things (IoT): A survey," *J. Sensor Actuator Netw.*, vol. 2, no. 2, pp. 235–287, 2013.

[15] Z. Shelby and C. Bormann, *6LoWPAN: The Wireless Embedded Internet*, vol. 43. Hoboken, NJ, USA: Wiley, 2011.

[16] J. Olsson, "6LoWPAN demystified," Texas Instrum., Dallas, TX, USA, Rep. SWRY013, Oct. 2014. [Online]. Available: http://www.ti.com/lit/wp/swry013/swry013.pdf

[17] R. T. Fielding and R. N. Taylor, "Principled design of the modern Web architecture," *ACM Trans. Internet Technol.*, vol. 2, no. 2, pp. 115–150, 2002.

[18] S. Raza, D. Trabalza, and T. Voigt, "6LoWPAN compressed DTLS for CoAP," in *Proc. 8th IEEE Int. Conf. Distrib. Comput. Sensor Syst.*, 2012, pp. 287–289.

[19] A. Stanford-Clark and H. L. Truong, *MQTT for Sensor Networks (MQTT-SN) Protocol Specification*, vol. 1, Int. Bus. Mach. Corporat., Armonk, NY, USA, 2013.

[20] Q. Zhu, R. Wang, Q. Chen, Y. Liu, and W. Qin, "IoT gateway: Bridging wireless sensor networks into Internet of Things," in *Proc. IEEE/IFIP 8th Int. Conf. Embedded Ubiquitous Comput. (EUC)*, 2010, pp. 347–352.

[21] S. K. Datta, C. Bonnet, and N. Nikaein, "An IoT gateway centric architecture to provide novel M2M services," in *Proc. IEEE World Forum Internet Things (WF-IoT)*, 2014, pp. 514–519.

[22] N. Saxena, A. Roy, B. J. R. Sahu, and H. Kim, "Efficient IoT gateway over 5G wireless: A new design with prototype and implementation results," *IEEE Commun. Mag.*, vol. 55, no. 2, pp. 97–105, Feb. 2017.

[23] Eclipse Foundation Inc. (2001). *Eclipse Kura*. [Online]. Available: https://www.eclipse.org/kura/

[24] X. Lu, P. Wang, D. Niyato, D. I. Kim, and Z. Han, "Wireless charging technologies: Fundamentals, standards, and network applications," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 2, pp. 1413–1452, 2nd Quart., 2016.

[25] K. Fotopoulou and B. W. Flynn, "Wireless power transfer in loosely coupled links: Coil misalignment model," *IEEE Trans. Magn.*, vol. 47, no. 2, pp. 416–430, Feb. 2011.

[26] Y. Gao, A. Ginart, K. B. Farley, and Z. T. H. Tse, "Misalignment effect on efficiency of wireless power transfer for electric vehicles," in *Proc. IEEE Appl. Power Electron. Conf. Expo. (APEC)*, 2016, pp. 3526–3528.

[27] A. Kurs, "Power transfer through strongly coupled resonances," Ph.D. dissertation, Dept. Phys., Massachusetts Inst. Technol., Cambridge, MA, USA, 2007.

[28] Digi-Key. (2016). *Inductive Versus Resonant Wireless Charging: A Truce May Be a Designer's Best Choice*. [Online]. Available: https://www.digikey.com/en/articles/techzone/2016/aug/inductive-versus-resonant-wireless-charging

[29] *Powermat*. Accessed: Oct. 5, 2019. [Online]. Available: https://www.powermat.com

[30] *ChargeItSpot*. Accessed: Oct. 5, 2019. [Online]. Available: http://chargeitspot.com

[31] *InforCharge*. Accessed: Oct. 5, 2019. [Online]. Available: https://www.inforcharge.com

[32] *Aircharge*. Accessed: Oct. 5, 2019. [Online]. Available: http://charge-spot.net

[33] *ChargeSPOT HK*. Accessed: Oct. 5, 2019. [Online]. Available: https://www.charge-spot.net

[34] Tatung Company. (2016). *Universal Development Kit for IoT (UDK-21)*. [Online]. Available: http://www.tatung.com/Product/Advanced/23

[35] Wi-Fi Alliance. (2018). *Wi-Fi Alliance® Introduces Wi-Fi Certified WPA3™ Security*. [Online]. Available: https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-wi-fi-certified-wpa3-security

[36] U. Kumar and S. Gambhir, "A literature review of security threats to wireless networks," *Int. J. Future Gener. Commun. Netw.*, vol. 7, no. 4, pp. 25–34, 2014.

[37] H. Alipour, Y. B. Al-Nashif, P. Satam, and S. Hariri, "Wireless anomaly detection based on IEEE 802.11 behavior analysis," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 10, pp. 2158–2170, Oct. 2015.

[38] M. Waliullah, A. B. M. Moniruzzaman, and M. S. Rahman, "An experimental study analysis of security attacks at IEEE 802.11 wireless local area network," *Int. J. Future Gener. Commun. Netw.*, vol. 8, no. 1, pp. 9–18, 2015.

[39] C. Kolias, G. Kambourakis, A. Stavrou, and S. Gritzalis, "Intrusion detection in 802.11 networks: Empirical evaluation of threats and a public dataset," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 184–208, 1st Quart., 2016.

[40] V. L. L. Thing, "IEEE 802.11 network anomaly detection and attack classification: A deep learning approach," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, 2017, pp. 1–6.
[41] F.-C. Cheng, "Automatic and secure Wi-Fi connection mechanisms for IoT end-devices and gateways," in *Proc. Int. Conf. Emerg. Technol. Comput.*, 2018, pp. 98–106.
[42] J. Daemen and V. Rijmen, "Rijndael, the advanced encryption standard," *Dobb's J.*, vol. 26, no. 3, pp. 137–139, 2001.
[43] L. Lamport, "Password authentication with insecure communication," *Commun. ACM*, vol. 24, no. 11, pp. 770–772, 1981.
[44] O. Goldreich, "Foundations of cryptography—A primer," *Found. Trends® Theor. Comput. Sci.*, vol. 1, no. 1, pp. 1–116, 2005. doi: 10.1561/0400000001.
[45] S. Halevi and H. Krawczyk, "Strengthening digital signatures via randomized hashing," in *Proc. Annu. Int. Cryptol. Conf.*, 2006, pp. 41–59.
[46] M. J. Dworkin, "SHA-3 standard: Permutation-based hash and extendable-output functions," NIST, Gaithersburg, MA, USA, Rep. 202, 2015.

Kuan-Ting Lai received the B.Eng. degree in electrical engineering, in 2003, the M.Sc. degree in computer science, in 2005, and the Ph.D. degree from National Taiwan University, Taipei, Taiwan, in 2015.

From 2012 to 2013, he was a Visiting Scholar with DVMM Lab, Columbia University, New York, NY, USA. He is currently an Assistant Professor with the Department of Electronic Engineering, National Taipei University of Technology, Taipei. His current research interests include computer vision, machine learning, data mining, and the Internet of Things.

Fu-Chiung Cheng received the Ph.D. degree in computer science from Columbia University, New York, NY, USA.

He is currently the Director of the Smart Internet of Things Research and Development Center and an Associate Professor with the Computer Science and Engineering Department, Tatung University, Taipei, Taiwan. He is the Founder with the Columbia-Tech Corp, Westborough, MA, USA, focusing on smart Internet of Things (IoT) applications. He has also served as the Director of the Industry-University Cooperation Division, the Director of the Academic Cooperation Division, the Director of the Teaching Technology Division, the Chairperson with the Computer Science and Engineering Department, Tatung University, and the Director of the Multimedia Development Division, Tatung Company, Taipei. He has obtained over 30 invention patents related to IoT, embedded systems, and system chip design in Taiwan, China, the United States, Japan, and the European Union. He has published over 50 papers and won 5 best paper awards in international and domestic conferences. The Smart Home Demo Center supervised by Prof. Cheng hosts over 40 groups of visitors each year from enterprises, domestic, and foreign universities, nonprofit organizations, and governments to showcase the smart IoT core techniques, including automatic and secure Wi-Fi connection, voice and gesture control, expert system for smart M2M communication, IoT development IDE, and IoT fault tolerance gateway. The IoT techniques have been applied to a smart home, a smart data center, a smart wireless charging system, and a smart health enhancement system. His current research interests include IoT software and hardware platform development, IoT application development, IoT education, and IoT business models.

Seng-Cho T. Chou received the B.Sc. degree from the Chinese University of Hong Kong, Hong Kong, the M.S. degree from the University of California, Santa Barbara, CA, USA, and the Ph.D. degree in computer science from the University of Illinois at Urbana-Champaign, Champaign, IL, USA.

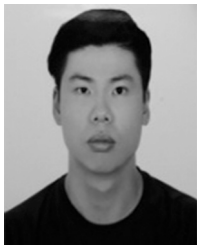
He is a Professor in information management with National Taiwan University, Taipei, Taiwan. His current research interests include business IT, AI, data analytics, Internet, and blockchain technologies.

Yi-Chun Chang is currently pursuing the Ph.D. degree with the Department of Information Management, National Taiwan University, Taipei, Taiwan.

She is also a Section Chief with the Criminal Investigation Bureau, Taipei. Her current research interests include organized crime, crime networks analysis, and knowledge management.

Guo-Wei Wu received the Bachelor of Computer Science degree from National Taiwan Ocean University, Keelung, Taiwan, in 2018. He is currently pursuing the master's degree with the Department of Electronic Engineering, National Taipei University of Technology, Taipei, Taiwan.

His current research interests include deep learning and the Internet of Things.



Jung-Cheng Tsai received the Bachelor of Electrical Engineering degree from Tatung University, Taipei, Taiwan, in 2018. He is currently pursuing the master's degree with the Department of Electronic Engineering, National Taipei University of Technology, Taipei, Taiwan.

His current research interests include wireless charging and the Internet of Things.