Hong Kong

Taiwan

Hong Kong – Taiwan EPC / RFID Academia Awards
香港–台灣大專學界 EPC / RFID 大獎 2013

Winning Case Sharing
得獎案例分享

Table of Contents

目錄

About GS1 Hong Kong

Founded in 1989 by the Hong Kong General Chamber of Commerce, GS1 Hong Kong is a not-for-profit industry support organization. It is committed to enhancing Hong Kong enterprises' competitiveness through the provision of global supply chain standards, best practices and enabling technologies. As GS1's local chapter, GS1 Hong Kong is authorized to issue and administer GS1 identification numbers in Hong Kong. Standards and solutions offered include bar coding services, B2B e-commerce services, Global Data Synchronization (GDS) and Electronic Product CodeTM / Radio Frequency Identification (EPC/RFID). The organization also hosts a wide range of training courses to facilitate knowledge transfer for SCM principles, e-business strategies, global standards and the implementation of enabling technologies. The GS1 community has over one million corporate members spanning over 150 countries and economies and more than 20 industries around the world. For more information about GS1 Hong Kong, please visit: http://www.gs1hk.org.

香港貨品編碼協會簡介

香港貨品編碼協會由香港總商會於 1989 年成立，是一個非牟利的工商業支援機構，致力透過發展全球供應鏈標準、應用技術及提供最佳實務守則，為香港企業提高市場競爭力。香港貨品編碼協會為 GS1 國際組織的本地分會，是獲認可簽發及管理 GS1 國際貨品編碼的機構。協會所提供的標準和解決方案包括貨品編碼及條碼服務、企業對企業電子商貿服務、全球數據同步 (GDS) ，以及產品電子代碼 / 無線射頻識別 (Electronic Product CodeTM / Radio Frequency Identification)。協會亦舉辦一系列促進知識轉移的培訓課程，包括供應鏈管理原理、電子商貿策略、全球標準及如何實施應用技術。GS1 在全世界各地擁有逾一百萬企業會員，遍布全球超過一百五十個國家和經濟體及二十多個行業。如欲獲得更多有關香港貨品編碼協會的資料，請瀏覽：www.gs1hk.org。

About GS1 Taiwan

GS1 Taiwanis established in 1986 and it is a non-governmental organization that forms a bridge between the government and industry sectors. The major job is introducing GS1 Standards to domestic industries. Currently, the organization has over 19,000 barcode members. The major mission of GS1 Taiwan is to enable a harmony to be reached on solutions that meet both the demands of business and the broader needs of society.

Since 1986, GS1 Taiwan has supported many governmental projects to adopt traceability and remain safety in deferent industry segments. In recent years, the organization has nurtured over 4,000 talents via training courses, examinations and activities to fulfill barcodes and EPC/RFID territories.

GS1 Taiwan 簡介

GS1 Taiwan 於 1985 年正式成立並申請加入 EAN International，並於 1986 年通過 EAN 國際組織入會申請核給商品條碼國家代號 471。GS1 Taiwan 為非營利組織，執行長為林暉先生，在商業夥伴中保持中立，結合產、官、學、研等各界資源，使 GS1 Taiwan 真正成為企業夥伴間協同合作的平台。

自 1988 年至今，多次承接經濟部及標準檢驗局之條碼及產業自動化相關專案；近兩年，分別承接“低壓儲氫罐流通履歷認驗證制度研究”，及“台灣用藥安全及藥品控管效率提升之條碼系統應用計畫”等政府專案，推動條碼及 EPC/RFID 技術在工業及醫療產業的發展應用。

GS1 Taiwan 於 2009 年起，於台灣校園及業界推動條碼及 EPC/RFID 人才培育認證教育訓練及考試制度，至今約 4 ,000 人取得 EPC/RFID 基礎認證、數百人取得 GS1 條碼管理師認證，並藉由舉辦多項活動，以培育更多條碼及 EPC/RFID 的人才。

The Hong Kong U-21 RFID Awards

The Hong Kong U-21 RFID Awards was first established in 2009 by GS1 Hong Kong to bring recognition to creative young talents who were committed to developing new EPC/RFID applications or technological products to address business issues and problems of daily lives. The purpose of the Awards is to promote wider adoption of EPC/RFID technology in business and daily lives, and encourage further original EPC/RFID application and technology development in the local academic institutions.

Technology advancement and sustainability requires inputs from both industry and academia. Today's young generations are the industry talents in the future who will undertake the important role of sustaining Hong Kong's competitiveness in the global marketplace. Against this backdrop, the Hong Kong U-21 RFID Awards 2011 was established to:

- Foster collaboration between industry and academia to develop new EPC/RFID applications and technological products with market potential
- Nurture a new generation of technical professionals with creativity and business acumen
- Stimulate market demand for innovative EPC/RFID applications and products
- Inspire new insights in the industry with the innovativeness and enthusiasm of tertiary students

Categories

Best EPC/RFID Concept

The winner of this award will demonstrate a high level of originality and creativity in adopting EPC/RFID technologies attempting to address a well-defined business issue or daily lives' problem, which has foreseeable market potentials.

Most Innovative EPC/RFID Application

The winner of this award will be an EPC/RFID application, integration or product, which is innovative, possesses distinctive features, complies with global RFID standards, and may also address market needs. Heavy weights will be allocated for projects developed through partnership between an enterprise and an academic institution.

香港 U-21 RFID 大獎

香港 U -21 RFID 大獎於 2009 年由香港貨品編碼協會設立，旨在獎勵創意青年人才投入發掘 EPC/ RFID 應用或研發產品，以解決商業以及日常生活的問題。獎項目的是推廣 EPC / RFID 技術更廣泛地在商業和日常生活上採用，並進一步鼓勵本地學術機構發展原創的 EPC/ RFID 應用和技術的。

技術的進步和可持續的發展需要業界和學術界的投入。今天的年輕一代是未來行業的人才，他們將擔任維持香港在全球市場上的競爭力的重要角色。有見及此，香港的 U -21 無線射頻識別大獎成立包含以下目的：

- 促進業界和學術界的合作，開發具有市場潛力的新的 EPC/ RFID 應用和技術產品
- 培養具有創造力和商業頭腦的新一代專業人才
- 激發 EPC / RFID 應用系統和產品的市場創意需求
- 啟發大專學生的創新精神及熱誠

獎項類別

最佳 EPC / RFID 概念

此獎項得主需展示高度的原創性和創造性，以採用 EPC / RFID 技術，解決明確的商業或日常生活中的問題，並能洞察市場潛力。

最具創意 EPC / RFID 應用

此獎項得主需以 EPC / RFID 技術的應用、整合或產品為其參賽項目，得獎項目需具創新意、有鮮明的特點、符合全球 RFID 標準、並滿足市場需求。評通過企業和學術機構之間的合作開發項目可獲更重評分。

The Taiwan EPC Architecture Award

The Taiwan EPC Architecture Award along with college contest of the EPCglobal Standards and the Internet of Things (IOT) was established by EPCglobal Taiwan in 2010. This award and contest are focus on undergraduate students of domestic institutes and universities.

The main purpose of this contest is to introduce EPCglobal Standards to most college students and cultivate experts. Via this activity, students have chances to learn experiences from industrial professions, and exchange ideas with other students.

The contestants should showcase their projects which follows the standard(s) of EPCglobal Architecture Framework.

The contest has two stages:

The First Stage: Referees will judge the students' paper assignments.

The Second Stage: Nominees will present the live demo of their projects in front of referees. In last ten minutes, referees will have the Q&A session with nominees.

After the contest, EPCglobal Taiwan will provide awards and prizes to winners for encouraging their motivation.

EPC 暨物聯網標準專題競賽

EPCglobal Taiwan 為提升 EPCglobal 標準之應用解決方案及專題研究，舉辦大專院校 EPC 暨物聯網標準專題競賽，活動以大專院校大學部學生為主。EPCglobal Taiwan 舉辦此活動，目的在於與業界經驗交流機會，共同營造 EPCglobal 標準之研究、發展、應用，達到培育優質人才落實於產業的效益，因此將頒發獎金及獎狀，以茲鼓勵。

競賽主題將以 EPCglobal Architecture Framework 為主，參賽學生得依其 EPCglobal Architecture Framework 任一標準製作相關專題，發表相關領域成果。

本競賽將分為初賽及決賽兩階段；初賽為書面審查，由 EPCglobal Taiwan 聘請各會內外之專家擔任評審委員，依創新性、實用性及特色展現等相關項目，進行分類及審查，並依成績高低遴選出決賽作品。決賽則邀請入圍學生或團隊至 EPCglobal Taiwan 總會報告其成果，接受各領域之專家評審委員提問 10 分鐘進行審查，並依展示、簡報內容、台風及問答進行決賽評審。

本競賽依照評審委員決議，決選出首獎、特優獎、優等獎各 1 名，佳作若干名，以鼓勵參加競賽的學生。

Most Innovative Award
最具創意大獎

Project title 項目名稱: SmartBeauty

Students 學生: Kwong Wing Yi, Lee Hoi Lam, Leung Hiu Kwan, Leung Hiu Kwan
鄺穎怡，李凱霖，梁曉筠，楊寶玲

Supervisors 指導: Mr. William Leung Kwok Way 梁國偉先生

Institution 院校: Associate in Business , Hong Kong Community College
香港專上學院 商業副學士

Table of Contact

2. Table of Content

1. Project Abstract

Radio-Frequency identification (RFID) is commonly applied to the world in different aspects. The application of RFID techniqueenhances the efficiency and effectiveness of human-beings in completing different tasks. Our project - SmartBeauty is specialized in providing integrated servicesto cosmetic users. This is a one stop solution to fulfill customer satisfaction and provide them with convenient and "All-Day" available shopping experience as well as easy information access. Users can simply enjoy all the functions by using their personal mobile device. RFID embedded smartphones increase SmartBeauty flexibility and enabled customer to shop everywhere at every time.

SmartBeauty is combining RFID system with magic mirror and social network.RFID tags installed inside the cosmetic products and readers will be embedded in smartphones and designated points inside the stores. This placement let customers can serve themselves inside everywhere. They can read the products' information, watch "How-to-Use" video, or even have a virtual make-up. These make-up photos can be shared to BeautyBook, a social network, users can share their beauty experience, comment on the others or take those photos as a reference.

To let all customers enjoy the benefit brought by RFID technology, virtual vanities will be installed in retail shops. Customers can try the cosmetic products on their face but do not need to actually put it on the face.

2. Project Objectives

In this modern era, time is money.People have different tasks and have a tight schedule every day. So they walk fast, eat fast, live fast and speak fast. But everything cannot be done withinlimited time, entertainment time may be thus decreased. For this reason, many people especially women tend to shop online.

As there are a wide range of cosmetic brands and products in the market, we need to try the products before we decide to buy it. However, many cosmetic shops do not provide useful testers or even do not allow customers to try their products. Therefore, customers buy unsuitable cosmetic products easily and a waste of money and product is resulted.

In order to fulfill and satisfy the need of customers from preventing buying unsuitable cosmetic products and reduce the valuable time cost of shoppers. We decide to apply RFID application system integrates into cosmetic shops.

3. Project Challenge

Recently, makeup become a hot topic around women and even men as well. When they are shopping at the store, testing the product always is a significant step. However, useful testers are not provided all the time since they were dirty, used or damaged.This leads us easily purchase unsuitable cosmetic products and waste money. Moreover, customers can only test the cosmetic products on hand or listen to the recommendation of staff. However, this is a time consuming way and not an accurate method to test those products. Sometimes, promotion from salesperson may even discourage customers enter retail stores.

Although cosmetic brands do develop their own webpage or application for customers read products catalog or even shop online, SmartBeauty do provide a distinct value to cosmetic market and solves the shopping issues existed. The following is the shopping issues existed in the market:

To begin with a purchase process, products information is fundamental to decide whether to buy the product. Even products information is overwhelmed in the internet, the information is not organized. Products information and “How-to-Use” Video are not always available in a same platform. Customers are hard to read, compare cosmetic products in a messy information pool. After reading the products information, customer would like to test the products texture and color. Without our SmartBeauty, customer can only test it on their hand. Even they can feel the productstexture; the color cannot be tested accurately as the color on hand in different from the one on face. Also, customer will make their hand dirt in testing the product. Once the product is being tested, customer may want to compare to the other product before they buy the tested one. However, customer probably cannot remember the products they want to buy or tested before. This will cause a loss in customers themselves because they forgot to buy necessary products. On the company side, forgetting to buy is obviously a loss of their sales revenue and brand awareness.

When customers have bought their product, they may found there are numerous cosmetic products on their vanity. However, it is not easy to remember when they have bought the product, what is the purchase date or expiry date, this will cause them buying redundant things, wasting money and not environmentally friendly.

On the other side, though people especially teenagers want to buy cosmetic products; they do not familiar with it. Even they want to search others make up as their reference in the internet, there is no platform including photos tagged with used products, products information, users feedback and last but not least the photos are separated by circumstances.

4. Application Development Design

- Smartphone Reader – Every smartphones are equipped with a NFC reader and specific tag. These NFC smartphones can help us transmit and adopt information via RFID technology in a faster and convenient way.
- Fixed NFC Reader – Installed a fixed NFC Reader in a designated point.
- Tablet with NFC Reader – Equipped with smartphones and salesperson' tablet
- Host Computer and Smartphone – Information display

This project mixes Near Field Communication (NFC) with social network and applies it in different circumstances. NFC reader will be installed in smartphones, a designated point inside the retail shop and tablets along with salesperson. While the RFID enabled tag will be embedded in cosmetic products and NFC smartphones. The following are examples of how the project efficient the cosmetic industry.

As a Display Broad

✓ Displays products' information like characteristic, usage and users' feedback
✓ Shows user's image that he or she has used the cosmetic products (like a magic mirror).
✓ Play as a product sample

As a Communication Tool

✓ Transmit "To-Buy-List" to the shop or cashier
✓ Communicate with salesperson
✓ Share photos, usage feedback to others

As a "My Beauty Product" Checklist

✓ Keep record of "My Beauty Product"
✓ Show Purchase Date
✓ Show Expiry Date

As a promotion tools

✓ Get Loyalty Point, Discount or Prizes

As a Demand Forecasting

✓ Count the number of times that customers check the samples details

5. Work of Procedures Taken to Conduct the Project

SmartBeauty is mainly carried by an application installed in Near Field Communication (NFC) Smartphones. The application acts as a catalog, mirror, social network and shopping cart. To conduct the project, smartphone will play a significant role and play as a reader and a tag to read and transmit data.

The users need only installed the application in a NFC Smartphone, they can enjoy a variety of benefits and conveniences. To introduce the application in detail it will be introduced by pages as follow.

i. Table of Content

This part summarize all key functions including

- Products Information
- Magic Mirror
-BeautyBook
-My-Shopping-List
-My-Beauty-Product
-RewardCash e-Shop

ii. Products Information

Products Information

Cosmetic Products are embedded with a passive Radio-Frequency Identification (RFID) tag including identification information such as unique serial number and product information.

Users can simply hold their NFC smartphone in close proximity of the products, the reader will be activated and the related information will be shown. This can increase store revenue as customer can serve themselves in the shop if the salesperson were being occupied.

If users cannot physically touch the products, they can solely search products information via the application and add favorite items into “My-Shopping-List”

iii. Magic Mirror

Magic Mirror

After reviewing products information, customers can try it virtually on their face.

A Magic Mirror will be included in the application and placed in the store as a virtual vanity. So that customer can test the cosmetic products through a virtual make up everywhere or in front of the magic vanity if they do not have NFC smartphone. If customers use magic mirror via the application, it is advanced to take a photo under efficient lighting so that our application can accurately reflect the "make-up" effect on the smartphone.

Once user finish a virtual make up, they can capture a photo by clicking a button on the mirror. The photo can be saved as reference or shared to the "BeautyBook".

iv. BeautyBook

BeautyBook

"BeautyBook" is a tailored social network. A platform let users share their photos and products feedback.

Those photos can be taken by magic mirror or users own camera. For the former one, all product used on the make-up will be automatically saved in the photo by the RFID reader; however we need to input what products we have used for the latest one. To input this data, we can type for it or simply add it by clicking the product on "My-Beauty-Product" or "History".

When users hang around the "BeautyBook", they can not only review the make-up photos but also knowing what kind of products do the model used. They can give a heart torepresent like the photo, and leave a comment for it. If they want further information about the product used by the model, users can click the product name and the related information will be shown.

Also, those photos will be categorized by occasions such as graduation dinner, wedding party, interview or outdoor activities. This categorization let users efficiently prepare their make-up refer to the models in relevant scenarios.

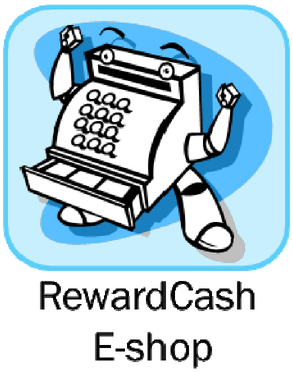
v. My-Shopping-List

When users shop in the store or the application, they may not decide to buy it immediately. “My-Shopping-List” allow users to record what they intend to buy for further comparison. Once “My-Shopping-List” have been confirmed, user need only visit the shop and transmit the List to the salesperson or cashier by holding the NFC smartphone near the salespersons tablet or the fixed reader at the designated point.

vi. My-Beauty-Products

“My-Beauty-Products” is a list showing what do user owned. Once users have brought the product, they can record it by NFC. After it “My-Beauty-Products” will list the Products Name, Purchase Date and Expiry Date. Users can also share their lists to the “BeautyBook” so that others can ask for products feedback and create brand awareness.

vii. RewardCash E-shop



To attract people download the application and register as a member, RewardCash will be promoted in different occasion with different rules. For example, a NFC tag may be embedded in a poster. Users can get RewardCash if they use their smartphone read the tag. Also RewardCash may be gotten by sharing photos to the “BeautyBook”.

RewardsCash can exchange for gifts or discounts depending on the promotion on that period.

6. Open RFID Technology Standards Adopted

In view of smartphone become part of our daily necessities, a smartphone embedded with RFID technique is an ongoing trend. This, a particular RFID readercan read and write on each smartphone of yours to smooth your buying process in cosmetic shops. RFID readers are installed in every Magic Mirror.

NFC- Near Field Communication

It is a set of short distance wireless technologies, usually requiring a distance of 4cm or less to start a connection. It allows you to simplify transactions and data exchange between an NFC tag and other devices like Android-powered device. Not surprisingly, this technology is used in a wide range of ways. Whether waving your smartphone at the checkout lane in the supermarket, swiping it over an exhibit at a local gallery or museum, or bumping phones with a friend to share the latest games, music or photos. NFC lets people learn, play and pay more easily.

NFC- It is an open stage technology standardized in ECMA-340 and ISO/IEC 18092. These standards itemize the coding, speed transfer and frame format of the RF interface of NFC devices, and initialization schemes as well as conditions required for data collision-control during initialization for both active NFC modes and passive modes. Besides, they also define the transport protocol, including data exchange ways and protocol activation. The air interface for NFC is standardized in:

ISO/IEC 18092 / ECMA-340
Near Field Communication Interface and Protocol-1 (NFCIP-1)
ISO/IEC 21481 / ECMA-352
Near Field Communication Interface and Protocol-2 (NFCIP-2)
NFC combines a wide range of existing standards including ISO/IEC 14443 both Type A and B, and FeliCa. NFC authorized smartphones work. Particularly in "card emulation mode" a NFC device should transfer, at a minimum, a unique ID number to an existing reader.

List of NFC phones today: (http://www.nfcworld.com/nfc-phones-list/#available)

- Google Nexus 4
- Google Nexus S
- HTC Desire C
- HTC One
- LG Optimus Elite
- Samsung Galaxy Note II.... etc

7. Partnership Between Industry and Academia

It is essential to develop a wholesome RFID industry- academia relationship to support the development of the industry and enrich the contribution of academia. The industry-academia partnership helps students to gain valuable practical business experiences. It is also important for them to understand the most recent trends in different industries.

Related companies can support the student team to finish a new RFID project, if the idea is valuable and workable. They can provide opportunity for company visit and part of area for student to do labs or research about RFID. This can be seen as a mentoring or internship program. Through these activities, all the required skills for doing well in a role of RFID application developer would have been trained in the candidate already. Also, students can surpass in any other inclination in a real firm.

Benefits from partnering are as follow:

- Companies:
  - Lower labor cost: Since the salary of a internship is lower than hiring a full time staff
  - Better resources coordination: According to the need of company, manager can change the students' job assignment when necessary.
  - Build a working relationship with the students: They may become the future employees of the company

- Students:
  - Gain valuable practical business experiences
  - Apply what they have learnt in class
  - Understand the most recent trends in different industries

- Internship:
  - Companies will be provided with bright, educated, and motivated student interns.
  - Companies can test students' quality before hiring.
  - Students may contribute by bringing in new innovative ideas to the company.
  - Students can get the working certificate when the program is completed.

8. Project Extensibility and Scalability

It is a trend for Cosmetic industry to use RFID application system which can release data in the newer format. Nowadays, RFID is an exceptional application in the world. Cheap in production cost effective and wireless capability are the advantages of RFID application. Not only are organizations keep investigating possible enhancement of RFID, but professionals also keep improving hardware, software design and the media used for transmitting information. The RFID application system is with good flexibility. For instance: Long term maintenance of system will be provided. The precise security service will protect customers' personal information and commercial information from stealing. We keep doing research and developing the whole system which can suggest users to upgrade the system when necessary. Besides, cosmetic business is part of the service industry. In order to meet the needs of different customers, sales people may need to change the service nature all the time. The system can be customized for system users who are potential customers and existing customers for any personal purposes.

If you are asking how much the average woman consumes on beauty products, you may be shocked with the statistics. In her lifetime, a woman will use about HKD$104,000 on different beauty products. For many women makeup is important. Cooperating with different cosmetic brands is our first step. No matter on clothing, shoes, skin care, hair or face, pursuing beauty is the nature of women. Therefore, we plan to cooperate with different clothing brand such as H&M, I.T and UNIQLO in the future. Under the cooperation, we will release a wide range of series on clothing and beauty products at the same time. Both of them will be labeled RFID tags and Magic Mirror will also install in the clothing shop. For example: If the customer wants to buy a sexy dress and have make up for going party, she can wave the tag of the dress by smartphone. After that, not only is she getting the dress's information, but she is also getting recommendation of what make up products should be used to match the beautiful dress. Furthermore, if the customers have any problems or questions about clothing or beauty products, the staff are willing to answer. Some customers may want to buy the dress only because they may think buying a new series of beauty products is wasteful for going one party. In order to solve this problem, the cosmetic shops will also provide make up service. Therefore, the customers can book the make up by connecting their phone with NFC reader in Magic Mirror. Customers' information and make up service time will be sent to their phone when it confirm.

Besides, customers may buy the counterfeiting cosmetic products if they are not buying in specialty shop. Because customers are not experts, they may not identify the fail products. However, if they use the counterfeiting products, serious consequences for instance allergy or dead can be happened. Therefore, after applying RFID system in cosmetic products, all the products will have new package with RFID tag. Customers can wave the product on their smartphone to check it fake or not.

9. Potential Commercial Values

The RFID system can smooth and simplify the purchase process of customers and the workflow of shop assistants. Besides, the collected data is costly for executive in operating a cosmetic business. Furthermore, the better quality services can be provided to valuable customers.

Consumer Behavior Database

The cosmetic shops are keeping information of all customers; existing and potential customers keep his or herown reviewing and consuming record in smartphone through using the App. The reviewed cosmetic products' information, make up methods and To-Buy List are stored and can be regained from phone anytime. If the customer has planned to buy a list of cosmetic products, data can be shared with the shop assistant in the new buying process via Tablet. The staff gets the information from To-Buy List, they can prepare the needed products immediately. When the shop understands more about one customer, staff can provide a more personalized and suitable service to one customer in order to enhance the shop's service quality. With this, customers can enjoy better service, more discounts or special gifts from all cosmetic shops which joined our platform.

Near Field Communication

- As a Checklist

RFID make the steps easier in purchasing by getting the information automatically from customers' phones. Customers and staff and executives are benefit from using RFID system.

To customers in buying the cosmetic products, the RFID system application simplifies the process in choosing and buying the products at the shops. It can reduce time and manual mistakes of the saleslady.

To all staff, the main benefit is receiving To-Buy List from customers immediately as saleslady knows what the customers want to buy. This will be done quickly by them which bring convenient. The saleslady can get the checklist from reader or Tablet. Then, they can communicate with the customers directly as they know the concern of their guests. Also, for dealing with high traffic flow problem, the saleslady can call the customers when the products are ready which can save customers' waiting time.

To the executives in managing budgets of advertising, the system records the customers' To-Buy List. Then the executives can decide which products need more promotion.

- As a Magic Mirror

It is obvious that almost all people have bought the wrong color or unsuitable cosmetic products. Yet, some people may choose to test the products on the bottom of their arms or hands. However, it takes time.

In order to prevent buying wrong products, the cosmetic shops install a Magic Mirror which includes a webcam, Mirror display and NFC reader. The customers stand in front of the Mirror and the customers' face is taken. Then, they wave the tagged testers over the NFC reader. It enables them to see on the Mirror how particular products such as lipsticks, blushers, eye shadow or even foundations would look on their faces. Besides, customers may need to wait for the help of saleslady if there is a high traffic flow. At this time, they can wave the tagged products over the reader to view detailed product information on a Magic Mirror. Then, they may know more about their needs and wants of cosmetic products.

To all staff, they can increase customers' satisfaction level, promote sales and purchase of related products by providing more detailed product information to customers. They can also improve the efficiency of stock control and enhance productivity by using retail area effectively.

Executives can also reinforce product line and product function through deeper analysis of products and recorded data form Magic Mirror. As RFID system is not popular in cosmetic industries, it can also raise the customer awareness of RFID tags and skills.

- As a Demand Forecasting

In tradition, a wide range of cosmetic testers and products stand on the shop counters. However, the shops cannot predict the demand of the products accurately if they only depend on how much testers were used. After using RFID system application, all the cosmetic products affix with RFID tags. The number of times that customers try each labeled testers can be counted by the tag readers.

Staff are benefit from the whole design of RFID system. Since the stored data about transaction and testers may be transmitted by network in time. It can reduce the workload of salesladies to insert or record data and update inventory information immediately. Besides, RFID system can foster the service provide. For cosmetic products buying procedure, the record will be made automatically by using Tablet. This brings convenience to salesladies in checking the customers' own usage history or from To-Buy List.

It is no exaggeration to say that executives can benefit from collecting informative and useful data like showing which products are the most popular and which products customers are the most interest in. Then, marketing department will depend on the collected data to take some actions for stimulating the sales.

- As a Promotion Tool

Marketing managers use bonus point redemption program to get the attention of customers. Billboards with RFID tags will be put in each shop. Besides, posters with RFID labels will also put in different places especially in MTR stations and Shopping Malls. When the customers or potential customers across the billboards or posters, they can wave the tag over their own smartphone to get the bonus point like 10 points at each time.

Benefits for customers are that RFID application can increase their interest. As they need to wave the tag which is more interesting than tradition method to get the bonus points. Besides, they can get the gift or special discount at the appointed points so they may need to look out the posters and billboards for getting the points.

Staff are benefits from the RFID system as well. Firstly, some potential customers may wave the billboards' tag at the shop. And the saleslady can grab the chance to interact with them. Through face-to-face communication, salesladies understand more about the customers and they can comment or make suggestion to them directly. It is possible to explore business opportunities and earn more commission.

Benefits to executives are that it is useful to enhance the brand awareness through RFID promotion tools. In addition, the cost of using this promotion tool is lower than other promotion methods especially television advertising. Then, executives can spend a part of advertising budget on other areas like staff training, technology development or marketing research.

10. Originalities, Uniqueness and Innovativeness Demonstrated

The cosmetic app mainly focuses on the serving a convenient platform for those people who like cosmetic. The magic mirror can prevent people buying wrong product because they can try the products on their face first by using the app before they buy. They can know the products ‘details from the apps instead of standing in front of the counter and listening to the staff’s description with buying pressure. Also, people can simply save a shopping list and let the staff know what they want though the NFC reader. Moreover, we follow the trend that people can share their beauty outlook with make-up though social network.

The new and considerate mobile app can take care of the needs of those cosmetic products’ users. You don’t need search different products with different brand website by website. Our app groups all the cosmetic brands together. The users can find all the information they want from the app. Not only providing information, you can try different product on your face to see whether that is suitable or not though the app. Also, an e-shopping function is provided; customers can save an e-shopping list by using her mobile phone. She can directly use her phone touch the NFC reader at the shop. Then, the staff knows what she wants and takes out the products immediately to her. The customers can buy the products directly because they have understood all the functions and information of the products they have chosen by using the mobile app. After purchasing the cosmetic products, the users can use the mobile to read the barcode on the product and save the record. Therefore, users can manage their cosmetic products well. This is a unique shopping method. The users can simply use the mobile to finish the buying process of cosmetic products from searching, choosing, trying, comparing, making decision and finally purchasing and storing.

Moreover, the app provides unique beauty exchange platform. Not only share photos and status, you can also tag the links for the cosmetic products that you used. That is you can share and recommend your confident cosmetic products to your friends and show your different make-up styles at different occasions.

11. Practicality, User-Friendliness, Extensibilities & Scalabilities Demonstrated

Smartphone is so easy to carry and is now an everyday item for people, users can update their beauty sense anytime anywhere.

Since the software design is created by our team, users only need to learn how to use the app. Also, the users can customize their own page and they are familiarized with their own page. Therefore, the app usage is always friendly, and indeed practically provides desires information to the users that they do not need to search the suitable product one by one. Also, only need the permission notice of the users, the app can be upgraded anytime.

The users can simply put the phone in proximity to the NFC reader at the shop; let the staff know their shopping list. They can complete the purchase transaction immediately instead of wasting time standing in front of the counter for a whole day but still buying the wrong product. For the shop, they can reduce the wastage of the sample so as to cut cost.

Beside the purchase process, users can make a checklist for their beauty products. In the checklist, product names, purchase date and expiry date will be shown. When the cosmetic products approach to the expiry date, notification will pop up to remind users. This function prevents them from using expired products, which will result from side effect like allergy.

12. **Social responsibility**

In the view of customers becoming more care of the social and environmental impacts behind the beauty and cosmetic products they purchase, it is becoming more and more vital for personal care manufactures to put social responsibility in the decision making.

The use of our RFID system acts the basic level of social aware of environmental. The use of RFID system in cosmetic business reduces usage and wastage of cosmetic testers. Besides, recycling boxes will be put in each retail shops so customers can help by recycling the product packaging. After disinfecting and handling, the bottles can reuse finally. It can reduce resources usage and lower the pollution level when produce the new package.

The retail shops minimize the amount of packaging and increase the amount of recirculate in product and transport packaging. In order to smooth the recycling process, all the cosmetic products are also label with packaging symbols. The symbols are a guide to how widely different packaging items are recycled. The information of packing symbols will be stored in the RFID tag, so the recycler can simply read the RFID tag and automatically recycle the packing by the category which the tag store.

The Green Dot

Plastics

Glass

Tidy-man

13. Ways of the Project Results Meet the Objectives

Business benefits:

- Reduce work for staff
- Reduce manual errors effectively
- Improve customer service
- Reduce conflict with customers
- Save money
- Increase brand awareness
- Increase sales revenue

Consumer benefits:

- Access information in a quick and convenient way
- Compare cosmetic products
- Prevent buying wrong products
- Have an easy purchase process
- Save time

14. Reasons of Our Project Deserves an Award

RFID is well-known in logistics, or supply chain management, but not practical in daily life. We try to apply RFID in our daily life. Make up is always a hot topic around women and even men as well. Therefore, we want to create a new method which is more convenient in buying cosmetic products. Our SmartBeauty concept consists of RFID technique which is an innovative, creative and unprecedented idea. The idea is not invisible. It can practice in different real situations. Moreover, our concept is not only focusing on cosmetic business, it can also extend to different industries like clothing, accessories and even hair style.

Besides, everyone own at least one smartphone. They can simply download the mobile app and they can enjoy all the functions in it. It is no exaggeration to say that our system is user-friendliness. It is simple to use and suitable for different ages such as teenagers, office ladies and housewives. On the other hand, each cosmetic shop will put a Magic Mirror so customers can have fun and enjoyment during their buying process.

Since people are more concerning about our planet, fulfills social responsibility is one of our mission. Our idea can also help to maintain a good relationship between business and students for providing mentoring program and internship program. Both the users and providers can gain benefit. It is a win-win situation.

15. Appendixes

References

1. Wikipedia, the Free Encyclopedia (2011). Near field communication. Retrieved July 18, 2013 from http://en.wikipedia.org/wiki/Near_field_communication#Standards

2. NFC phones: The definitive list (2013). Retrieved July 18, 2013 from http://www.nfcworld.com/nfc-phones-list/#available

3. PROTECT THE PLANET, Retrieved July 18, 2013 from http://www.thebodyshop.com.hk/en/vc_text-protecttheplanet.aspx

4. Recycle now, Retrieved July 18, 2013 from http://www.recyclenow.com/why_recycling_matters/recycling_symbols.html

5. How Much Does the Average Woman Spend on Makeup?, Retrieved July 18, 2013 from http://www.ask.com/question/how-much-does-the-average-woman-spend-on-makeup

6. The Growing Need for Corporate Social Responsibility in the Cosmetic Industry, Retrieved July 18, 2013 from http://desertwhale.wordpress.com/2010/05/12/the-growing-need-for-corporate-social-responsibility-in-the-cosmetic-industry/

7. NFC (Near Field Communication), Retrieved July 18, 2013 from http://www.gsmarena.com/glossary.php3?term=nfc

8. Hood, Christopher P. (2006). Shinkansen – From Bullet Train to Symbol of Modern Japan.Routledge.ISBN 0-415-32052-6.

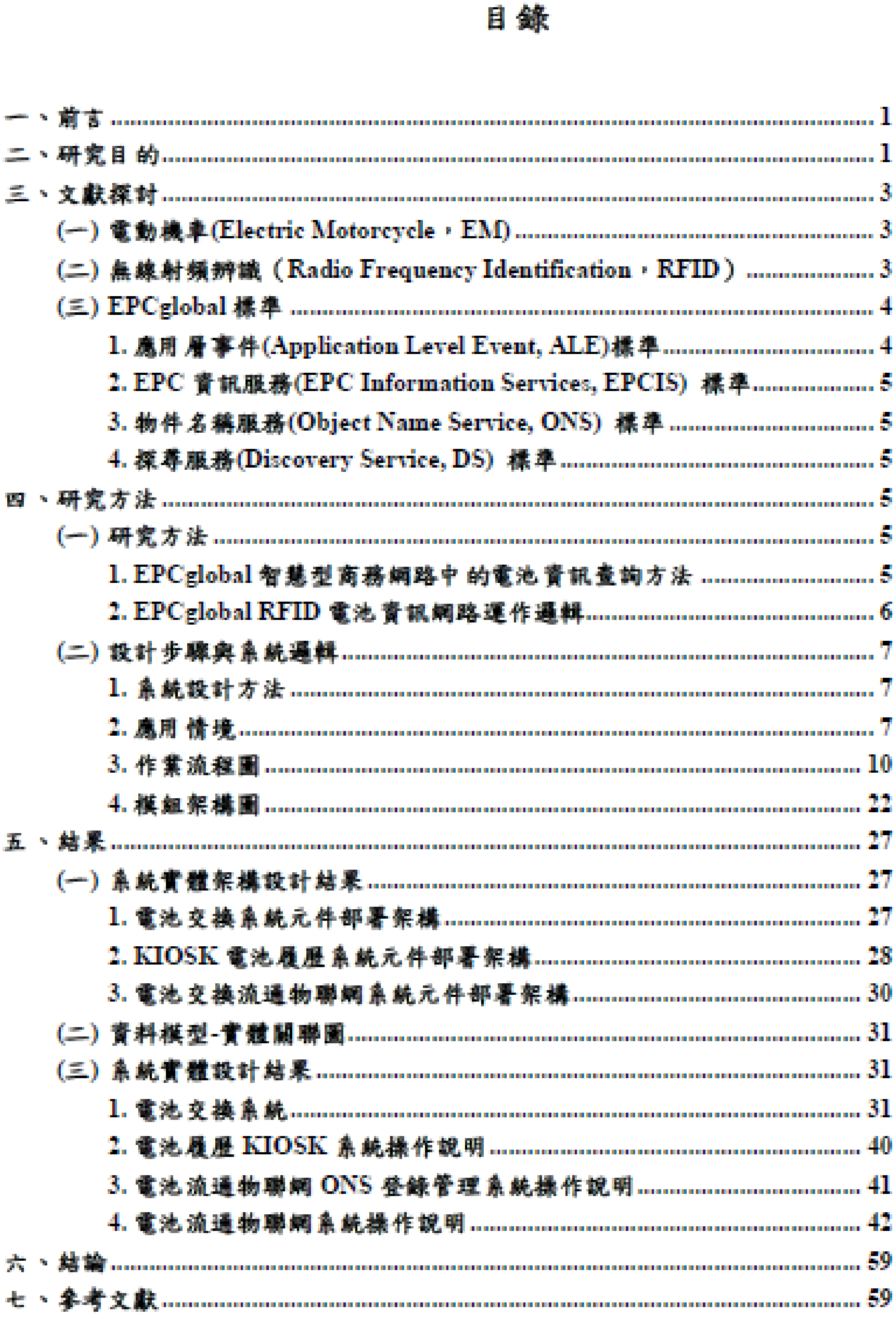
Most Potential Application Award
最具潛質應用大獎

Project title 項目名稱: RFID 電動機車電池流通物聯網

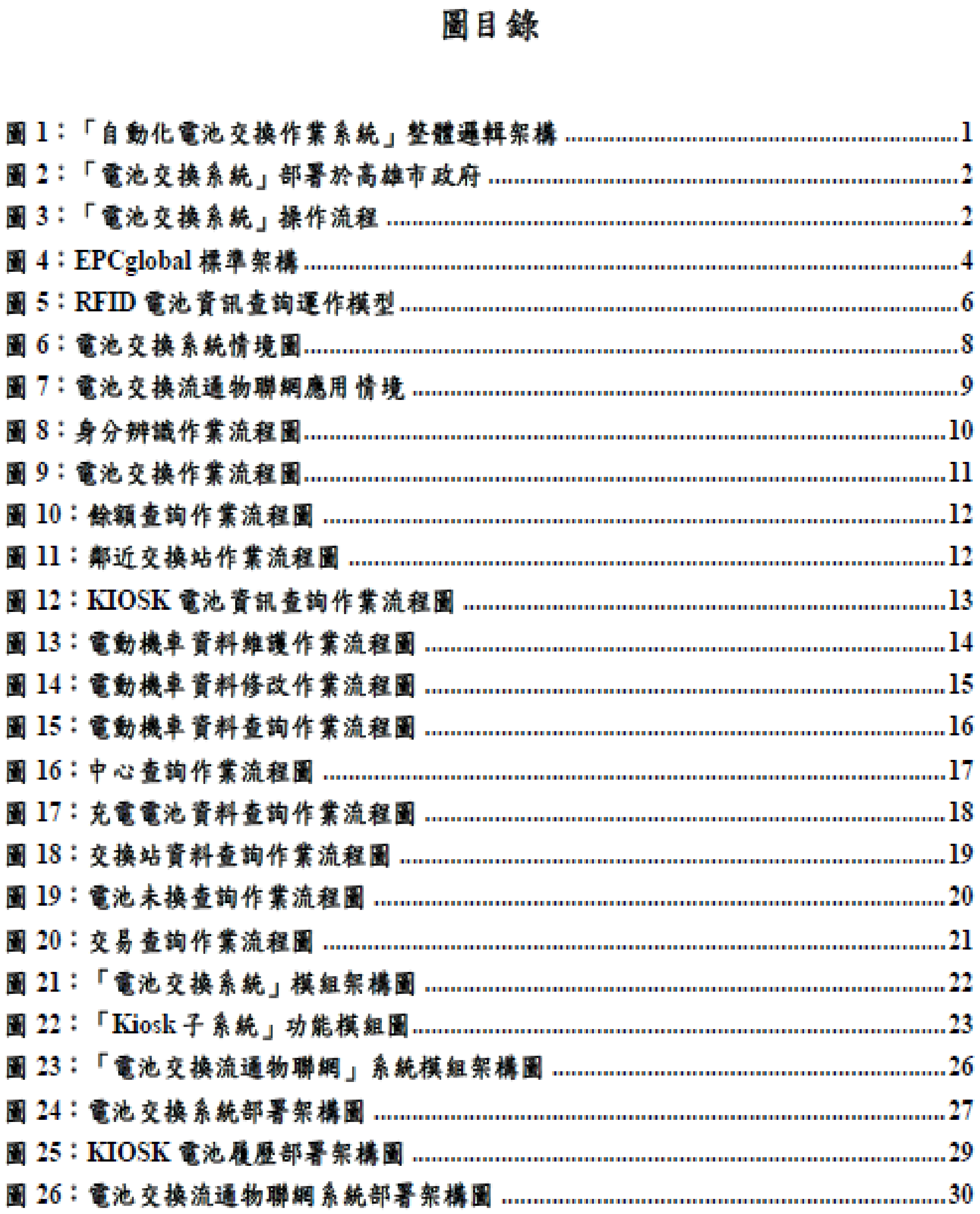
Students 學生: 許維哲、黃信璋、孫羽柔、陳家昌、翁三峯

Supervisors 指導: 高志中老師

Institution 院校: 和春技術學院 資訊管理系



目錄



圖目錄

RFID 電動機車電池流通物聯網

一、前言

高雄市二行程機車數量高達58萬輛，二行程機車每年排放 9千多噸之揮發性有機物，大約是一座煉鋼廠一整年的排放量；另外，一輛機車一年排放的溫室氣體約為 50 棵樹一年吸收的量[8]。為了達成政府節能減碳政策目標，高雄市政府委託「見發先進科技公司」研究開發一套「自動化電池交換作業系統」，希望能建立一套自動化的電動機車電池交換系統，並能有效管理電池流通動態資訊。

本研究為和春技術學院與見發先進科技公司產學合作案所開發之「自動化電池交換作業系統」資訊流作業及管理軟體，由資訊管理系指導老師高志中助理教授帶領本研究團隊成員，許維哲等六員學生所完成。透過此系統，高雄市政府能夠提供民眾方便的電池交換服務，營運中心也能有效率的追蹤電池流通狀態，掌握電池交易資訊，有效營運電池交換業務(如圖 1)。

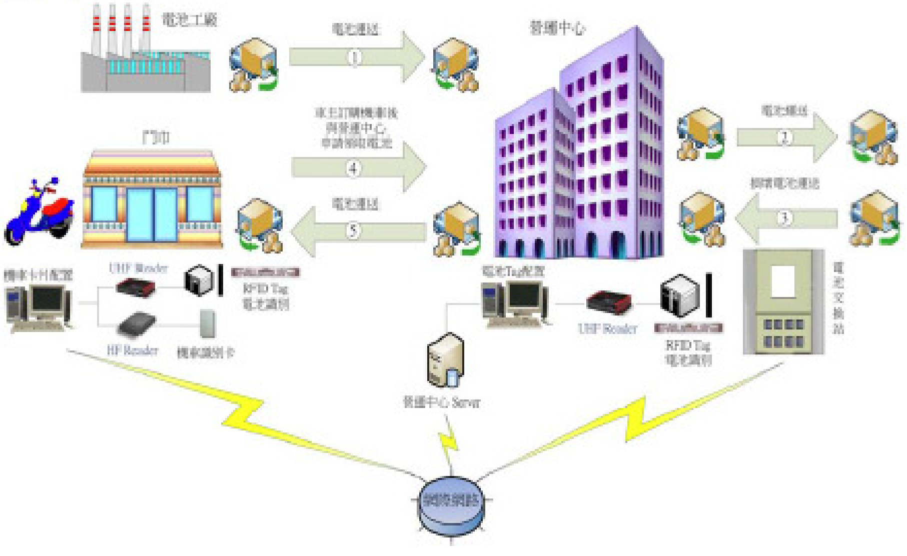


圖 1：「自動化電池交換作業系統」整體邏輯架構

二、研究目的

本研究案目的在建立一套「電動機車電池交換及流通物聯網系統」，此系統包含，「電池交換系統」、「電池履歷 Kiosk」及「電池交換流通物聯網」等三個子系統。「電池交換系統」負責管理電池進站充電、檢測及出站等自動控制作業流程，並具有計費程式(如圖 2)。系統利用悠遊卡驗證車主身分並進行充電扣款。扣款成功後才會在電池出口處送出滿電狀態之電池(如圖 3)。「電池履歷 Kiosk」提供車主或營運中心追蹤電池從出廠之後的流通狀態 。「電池交換流通物聯網」提供電池物流管理功能，包含電池資料查詢、交易資訊、履歷查詢、報表列印管理等功能。

圖 2：「電池交換系統」部署於高雄市政府的外觀，本系統將於高雄市內部署 32 套供高雄市民利用

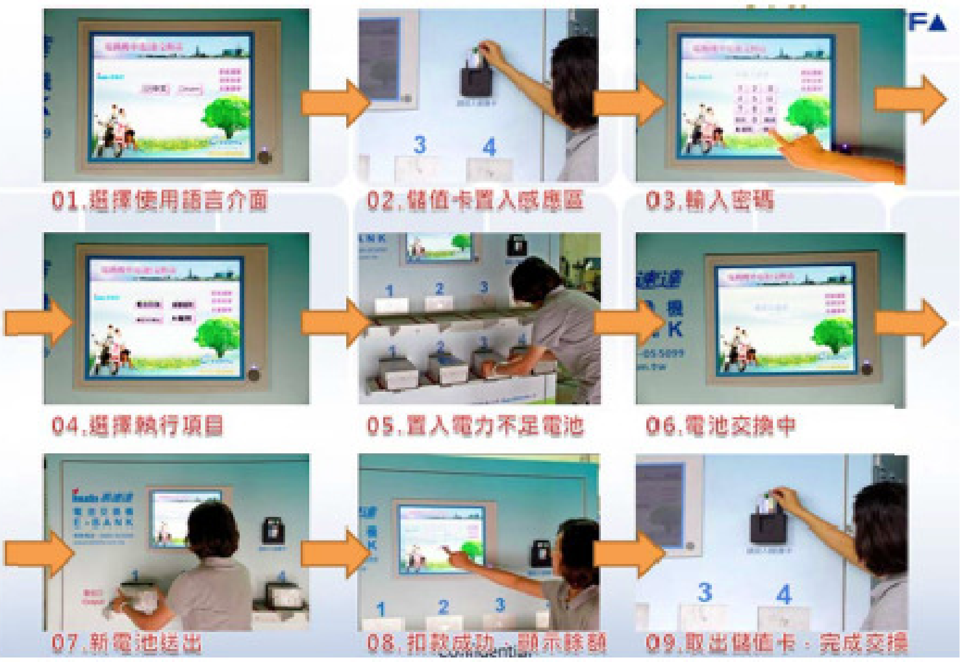
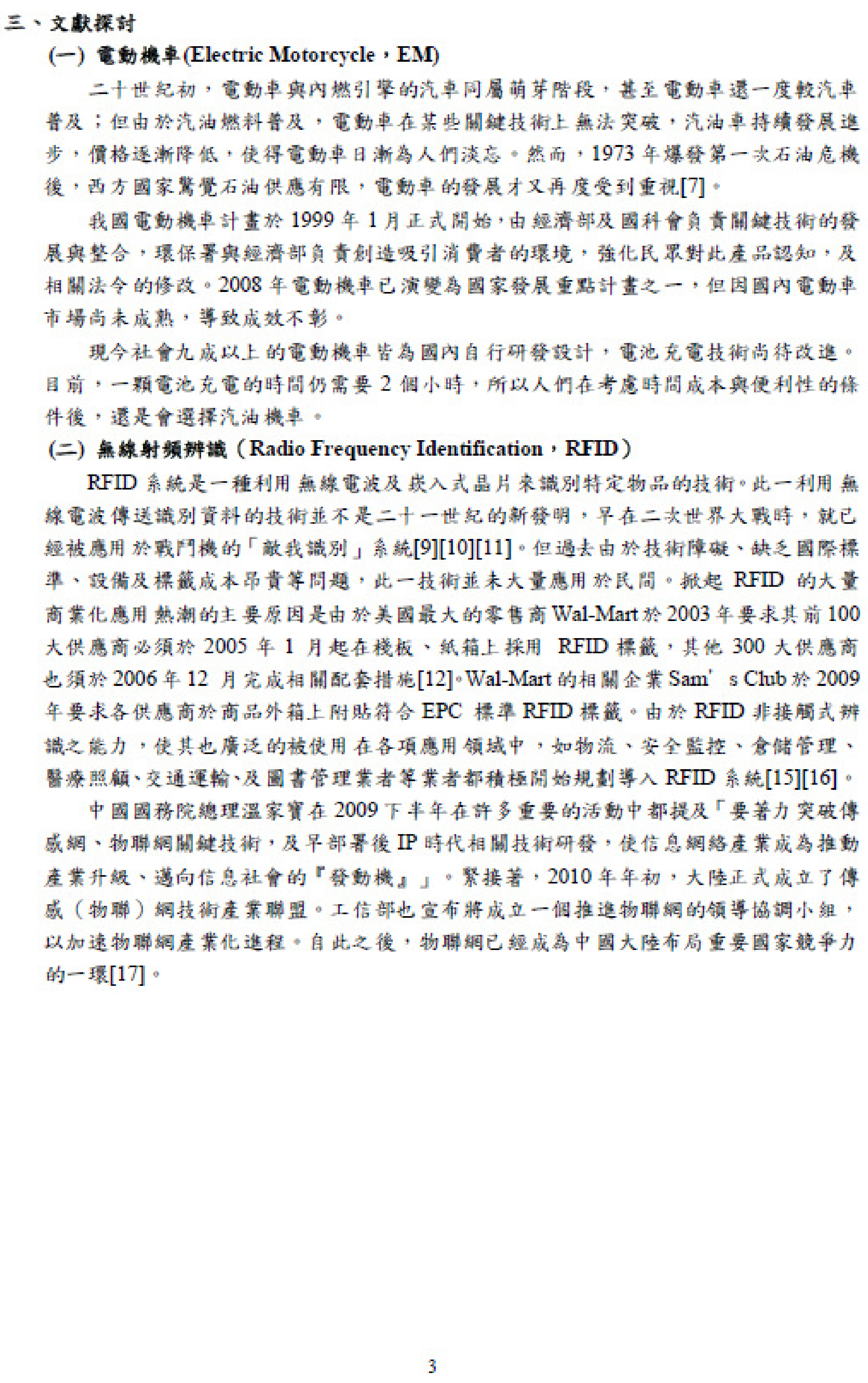


圖 3：「電池交換系統」操作流程



三、文獻探討

(一) 電動機車(Electric Motorcycle，EM)

二十世紀初，電動車與內燃引擎的汽車同屬萌芽階段，甚至電動車還一度較汽車普及；但由於汽油燃料普及，電動車在某些關鍵技術上無法突破，汽油車持續發展進步，價格逐漸降低，使得電動車日漸為人們淡忘。然而，1973 年爆發第一次石油危機後，西方國家驚覺石油供應有限，電動車的發展才又再度受到重視[7]。

我國電動機車計畫於 1999 年 1 月正式開始，由經濟部及國科會負責關鍵技術的發展與整合，環保署與經濟部負責創造吸引消費者的環境，強化民眾對此產品認知，及相關法令的修改。2008 年電動機車已演變為國家發展重點計畫之一，但因國內電動車市場尚未成熟，導致成效不彰。

現今社會九成以上的電動機車皆為國內自行研發設計，電池充電技術尚待改進。目前，一顆電池充電的時間仍需要 2 個小時，所以人們在考慮時間成本與便利性的條件後，還是會選擇汽油機車。

(二) 無線射頻辨識（Radio Frequency Identification，RFID）

RFID 系統是一種利用無線電波及嵌入式晶片來識別特定物品的技術。此一利用無線電波傳送識別資料的技術並不是二十一世紀的新發明，早在二次世界大戰時，就已經被應用於戰鬥機的「敵我識別」系統[9][10][11]。但過去由於技術障礙、缺乏國際標準、設備及標籤成本昂貴等問題，此一技術並未大量應用於民間。掀起 RFID 的大量商業化應用熱潮的主要原因是由於美國最大的零售商 Wal-Mart 於 2003 年要求其前 100 大供應商必須於 2005 年 1 月起在棧板、紙箱上採用 RFID 標籤，其他 300 大供應商也須於 2006 年 12 月完成相關配套措施[12]。Wal-Mart 的相關企業 Sam’ s Club 於 2009 年要求各供應商於商品外箱上附貼符合 EPC 標準 RFID 標籤。由於 RFID 非接觸式辨識之能力，使其也廣泛的被使用在各項應用領域中，如物流、安全監控、倉儲管理、醫療照顧、交通運輸、及圖書管理業者等業者都積極開始規劃導入 RFID 系統[15][16]。

中國國務院總理溫家寶在 2009 下半年在許多重要的活動中都提及「要著力突破傳感網、物聯網關鍵技術，及早部署後 IP 時代相關技術研發，使信息網絡產業成為推動產業升級、邁向信息社會的『發動機』」。緊接著，2010 年年初，大陸正式成立了傳感（物聯）網技術產業聯盟。工信部也宣布將成立一個推進物聯網的領導協調小組，以加速物聯網產業化進程。自此之後，物聯網已經成為中國大陸布局重要國家競爭力的一環[17]。

(三) EPCglobal 標準

為了讓RFID的應用能夠國際化，業界需要一套全球統一的軟硬體標準EPCglobal。EPCglobal的標準不僅只是針對RFID技術的「無線介面協定」 (Air Interface protocol)制定標準而已，其標準所涵蓋的範圍是著眼於供應鏈物流管理所需的標籤識別(Identity)、資料擷取(capture)以及資訊交換(exchange)等全方位標準(如圖 4)。目前，在這個標準架構之下規劃有 15 項標準，現階段已公佈的有 13 項[1]。其中，應用層事件(ALE)、EPC 資訊服務(EPCIS)、物端運算化之優勢，分述如下：

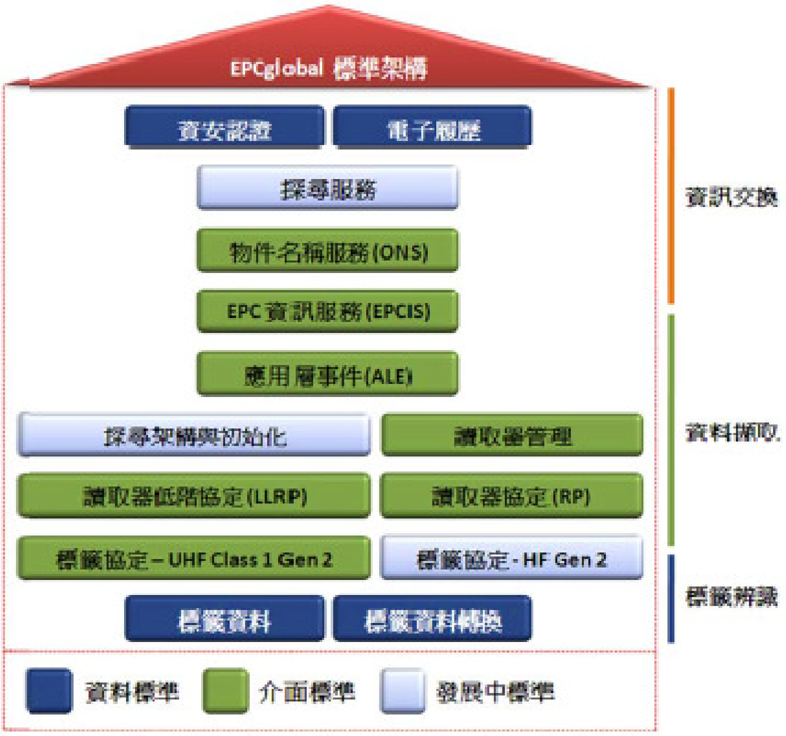


圖 4：EPCglobal 標準架構[1]

1. 應用層事件(Application Level Event, ALE)標準

ALE是一個EPCglobal中介軟體標準的名稱。此標準規範了客戶端應用系統與不同標籤資訊來源之間的中介處理程式標準，包括標籤資料過濾、篩選、轉換、整合等標準。換句話說，符合ALE標準的軟體能夠將原始的標籤資訊進行彙整處理後，提供客戶端另一種高階的標籤資訊，讓客戶端應用系統可以專注於商業邏輯處理，而不需要耗費系統資源在低階的標籤讀取事件及資料過濾整合計算。

2. EPC 資訊服務(EPC Information Services, EPCIS) 標準

EPCIS 的目地是讓不同的應用系統，可以在企業內部和跨企業之間分享 EPC 碼的相關資訊，包括產品的生產履歷、物流過程以及運輸載具等資訊。因此，EPCIS 標準定義了一套階層化的 EPC 資料模型標準，這個格式是以 XML 標記語言為基礎的資料模型，可以提供不同使用者所需的供應鏈管理資訊。EPCIS 標準的目的是讓企業供應鏈的成員在 EPCglobal 網絡中，可以取得共通格式的 EPC 供應鏈管理資訊。

3. 物件名稱服務(Object Name Service, ONS) 標準

ONS 標準規範了一套透過網際網路分散式架構，用以搜尋 EPCIS 服務的作業流程與資料格式。ONS 建立在既有的網際網路 DNS (Domain Name System) 服務架構中，利用 NAPTR 記錄 EPCIS 的網域位置與 Web Service 描述文件的檔案名稱，讓客戶端可以經由 RFID 標籤的 EPC 碼查詢到 EPCIS 所提供的資訊，此服務類似網際網路以領域名稱(Domain Name)對應到 IP 位置的 DNS 服務。

4. 探尋服務(Discovery Service, DS) 標準

探尋服務(Discovery Service, DS) 標準是用來規範 EPC 動態資料追蹤與查詢服務的協定。動態資料追蹤是針對物流過程中，紀錄貼有 RFID 標籤之商品進出各物流站的相關資訊，包括：地點、進出時間、狀態等動態資訊。其目的是讓供應鏈的每一個企業成員，可以有效地追蹤每一批貨的物流狀態。

四、研究方法

(一)研究方法

電動機車節能且低汙染的優勢是政府環保政策的目標。採用 RFID 技術可以記錄電池的物流動態過程，有助於營運中心控管電動機車之電池品質，縮短電池識別的作業時間，降低人力成本及提高效率等綜合競爭力。RFID 物聯網係透過 EPCglobal 的網路技術，追蹤電池的物流動態過程，以確保電池流通履歷資訊的透明度。以下是相關研究模型及方法：

1. EPCglobal 智慧型商務網路中的電池資訊查詢方法

EPC(Electronic Product Code)為「電子商品碼」之簡稱，適合以 RFID 標籤儲存電池辨識碼，用於標示電池物件，並結合網際網路與資訊科技，連接電池物件與網際網路構成一個電池追蹤網絡，使電池的物流動態資訊可以達到透明化及標準化的國際市場要求目的。

EPCglobal 智慧型商務網路利用 ONS 服務將 EPC 碼所表示的 URN 解析為該項商品的資訊服務主機(EPCIS)的 IP 位置及 Web Service 描述文件檔名。在網際網路中任何電腦均能夠依據 URN 資訊，向 ONS 主機詢問該 URN 相對的 EPCIS 主機位址(鄭同伯，2004)；亦即，EPC 網路架構能夠根據 EPC 碼而搜尋到相關的資訊服務主機與其資料庫存取元件，進而讀取相關商品的履歷資訊；就如同在瀏覽網頁時，可以使用 DNS 將 URL 網址對應到網頁主機的 IP 位置一樣。

2. EPCglobal RFID 電池資訊網路運作邏輯

本研究所規劃的 EPCglobal 智慧型商務網路運作的步驟(如圖 5)如下所示：

Step1：RFID reader 讀取到一個 RFID 電池標籤的 EPC 碼。

Step2：RFID reader 將此 EPC 碼傳送到本地客戶端主機(ALE 主機)。

Step3：本地客戶端主機將 EPC 碼轉換成 URN，並將 URN 傳送到本地 ONS 解析器。

Step4：本地 ONS 解析器先檢查本機是否已有該 URN 的記錄，如果有快取記錄則直接向 EPCIS 查詢電池資料。如果沒有快取記錄，則將此 URN 發送到指定的 ONS 伺服器基礎架構，查詢該電池的 EPCIS 主機位址及 Web Service 描述文件檔名。

Step5：ONS 基礎架構回應 ONS 解析器該 URN 所對應的 EPCIS 主機的 URL 網址與 Web Service 描述文件檔。

Step6：ONS 解析器再將 EPCIS 主機位址與 Web Service 描述文件檔名回應給伺服器。

Step7：本地客戶端主機再根據 EPCIS 主機位址聯繫正確的 EPC-IS 伺服器，並利用 Web Service 取得所需的電池資訊。

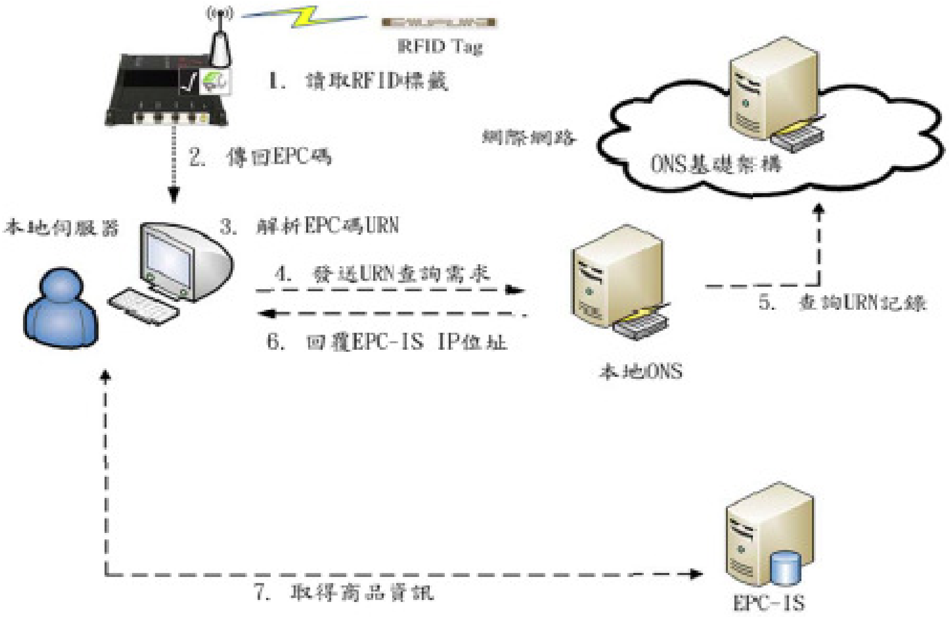
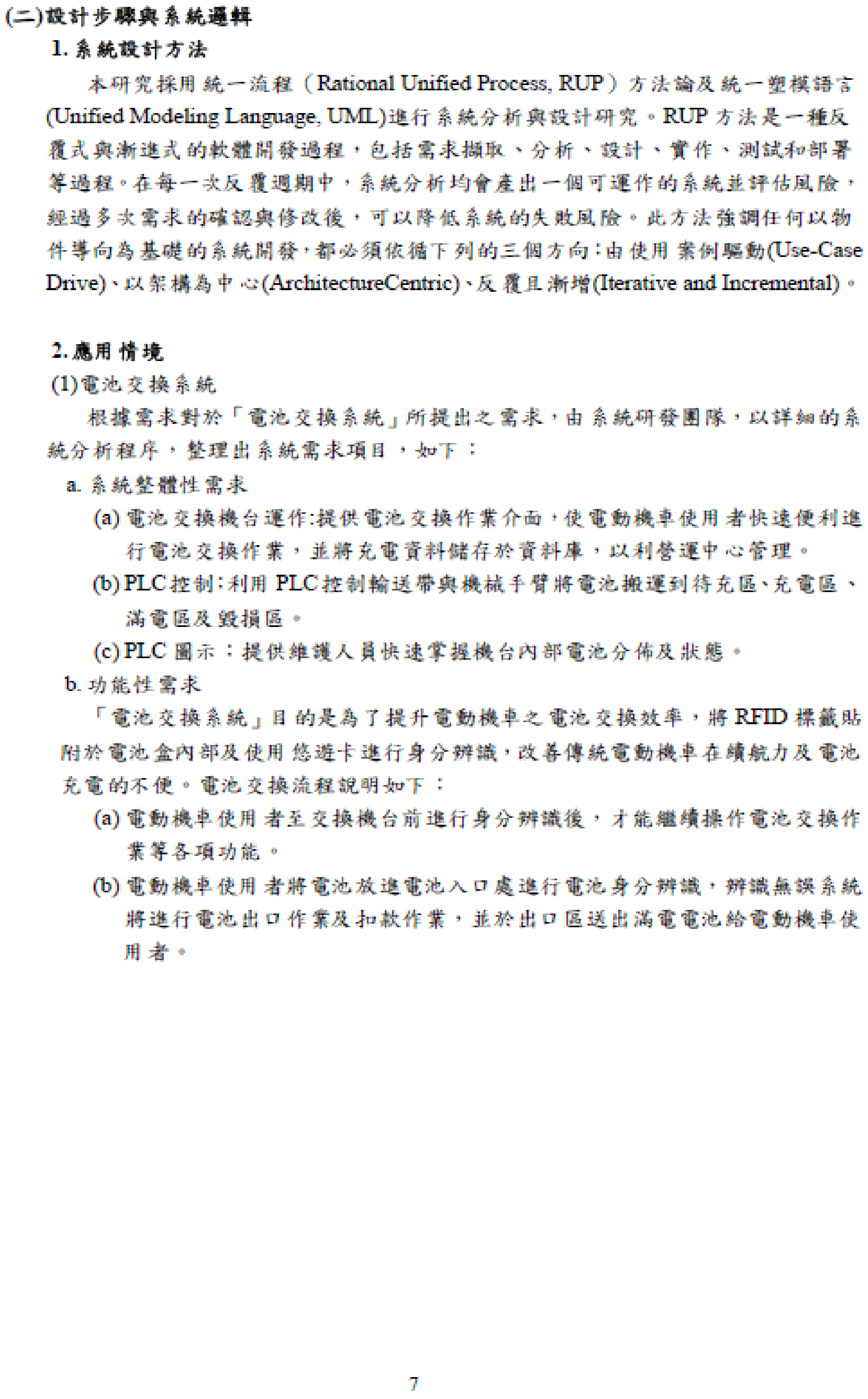


圖 5：RFID 電池資訊查詢運作模型



(二)設計步驟與系統邏輯

1. 系統設計方法

本研究採用統一流程（Rational Unified Process, RUP）方法論及統一塑模語言(Unified Modeling Language, UML)進行系統分析與設計研究。RUP方法是一種反覆式與漸進式的軟體開發過程，包括需求擷取、分析、設計、實作、測試和部署等過程。在每一次反覆週期中，系統分析均會產出一個可運作的系統並評估風險，經過多次需求的確認與修改後，可以降低系統的失敗風險。此方法強調任何以物件導向為基礎的系統開發，都必須依循下列的三個方向：由使用案例驅動(Use-Case Drive)、以架構為中心(ArchitectureCentric)、反覆且漸增(Iterative and Incremental)。

2. 應用情境

(1)電池交換系統

根據需求對於「電池交換系統」所提出之需求，由系統研發團隊，以詳細的系統分析程序，整理出系統需求項目，如下：

a. 系統整體性需求

(a) 電池交換機台運作:提供電池交換作業介面，使電動機車使用者快速便利進行電池交換作業，並將充電資料儲存於資料庫，以利營運中心管理。

(b) PLC控制：利用PLC控制輸送帶與機械手臂將電池搬運到待充區、充電區、滿電區及毀損區。

(c) PLC圖示：提供維護人員快速掌握機台內部電池分佈及狀態。

b. 功能性需求

「電池交換系統」目的是為了提升電動機車之電池交換效率，將RFID標籤貼附於電池盒內部及使用悠遊卡進行身分辨識，改善傳統電動機車在續航力及電池充電的不便。電池交換流程說明如下：

(a) 電動機車使用者至交換機台前進行身分辨識後，才能繼續操作電池交換作業等各項功能。

(b) 電動機車使用者將電池放進電池入口處進行電池身分辨識，辨識無誤系統將進行電池出口作業及扣款作業，並於出口區送出滿電電池給電動機車使用者。

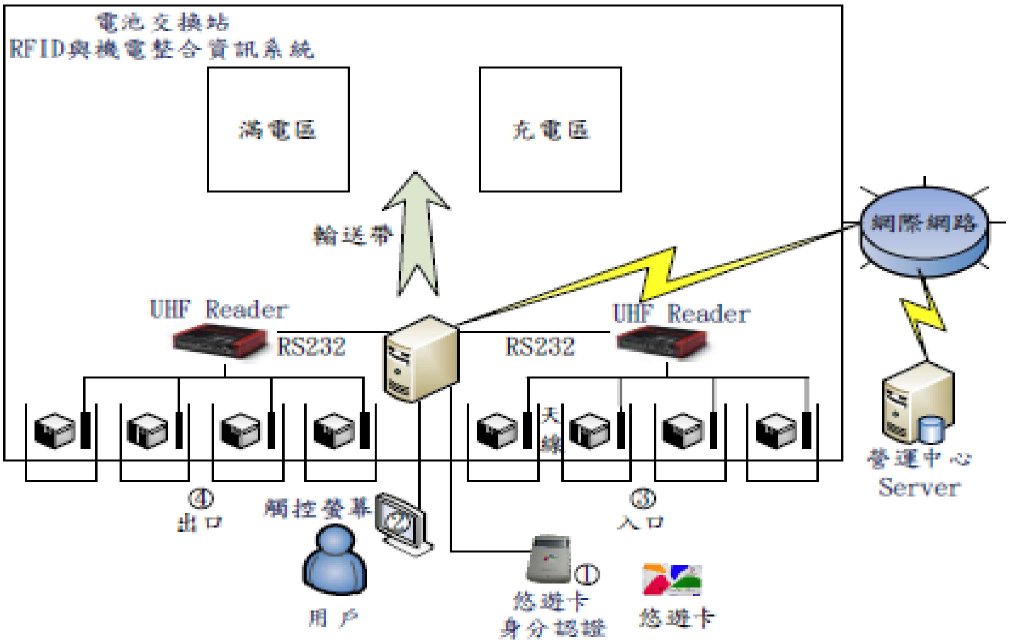


圖 6：電池交換系統情境圖

(2)電池交換流通物聯網

a. 電池從電池供應商出產後，會送往電池交換中心進行分配，並向資訊中心登記電池基本資料。如有損壞會送回電池供應商進行維護。

b. 電動機車從電動車供應商出產後，會配送至交換中心。如有故障會送回電動車供應商進行維修。

c. 電池交換中心則會將電池及電動機車組裝，並送往經銷商販售。

d. 電池交換中會將合格電池配送至電池交換站進行交換。若電池故障則會送回電池交換中心進行檢驗。

e. 使用者可利用電池交換中心網站，查詢電池履歷。

f. 民眾可利用 KIOSK 查詢機，查詢電池履歷。

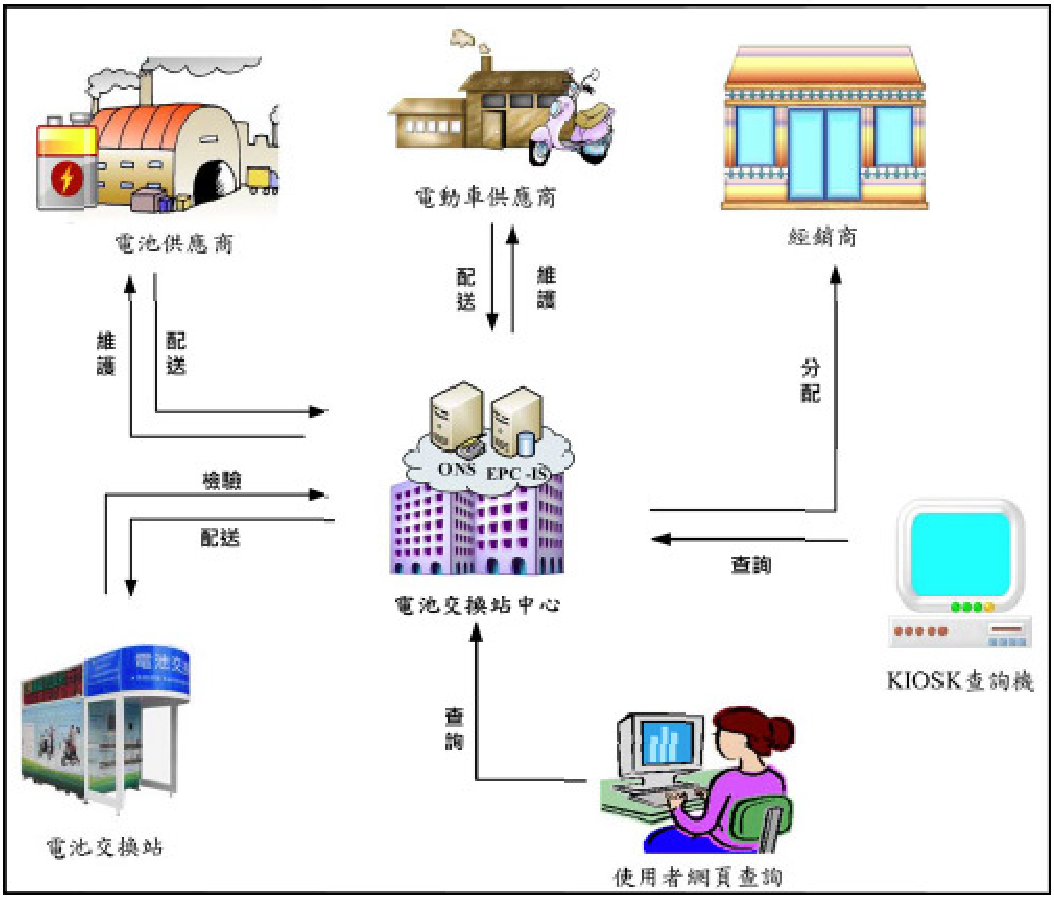


圖 7：電池交換流通物聯網應用情境

9

3. 作業流程圖

(1) 電池交換系統作業程序

a. 身分辨識作業流程

(a) 使用者放置悠遊卡置讀取區。

(b) 輸入使用者自行設定密碼，認證成功進入功能選擇介面，若認證失敗三次將進行鎖卡。

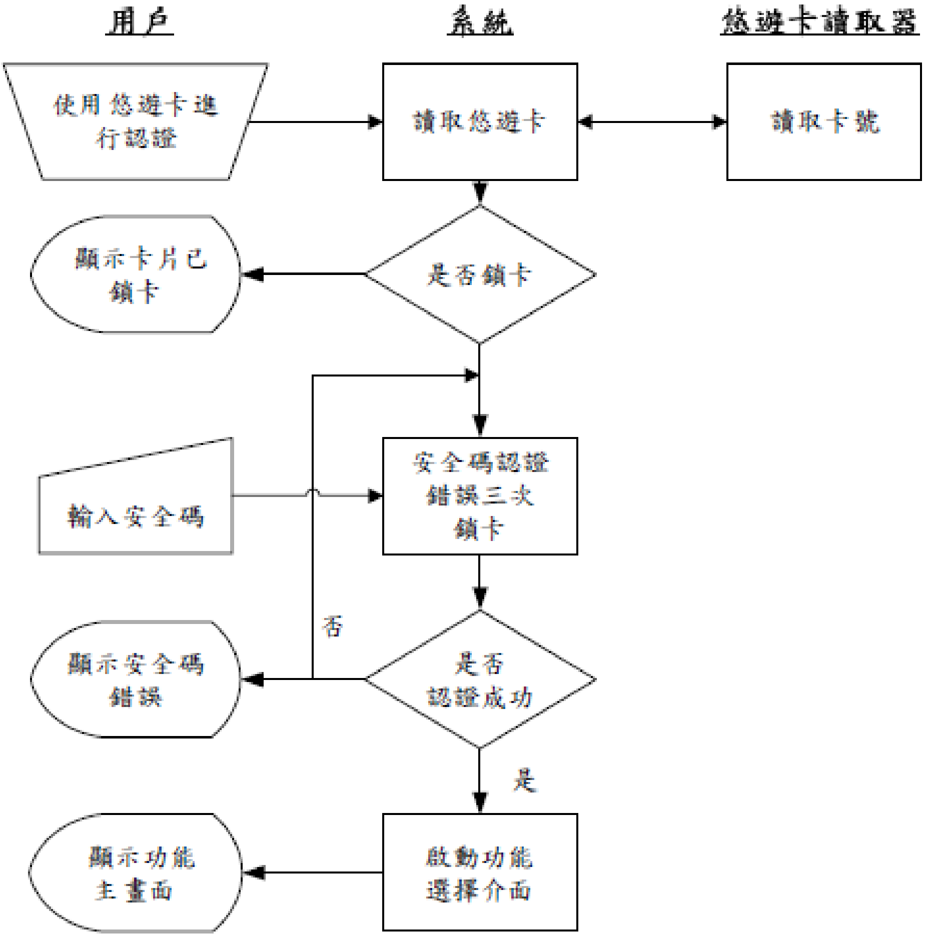


圖 8：身分辨識作業流程圖

b. 電池交換作業流程

(a) 使用者進行身分辨識認證成功，選擇電池交換功能。

(b) 放入無電力需交換電池，系統將會讀取電池 RFID 識別卡進行辨識，若辨識失敗則退回電池並且告知使用者。

(c) 辨識成功則進行電池出口作業流程，並將滿電電池送出給使用者。

(d) 讀取悠遊卡進行扣款動作，並顯示卡片餘額。

(e) 記錄交換電池電量與扣款資訊並顯示於螢幕通知使用者。

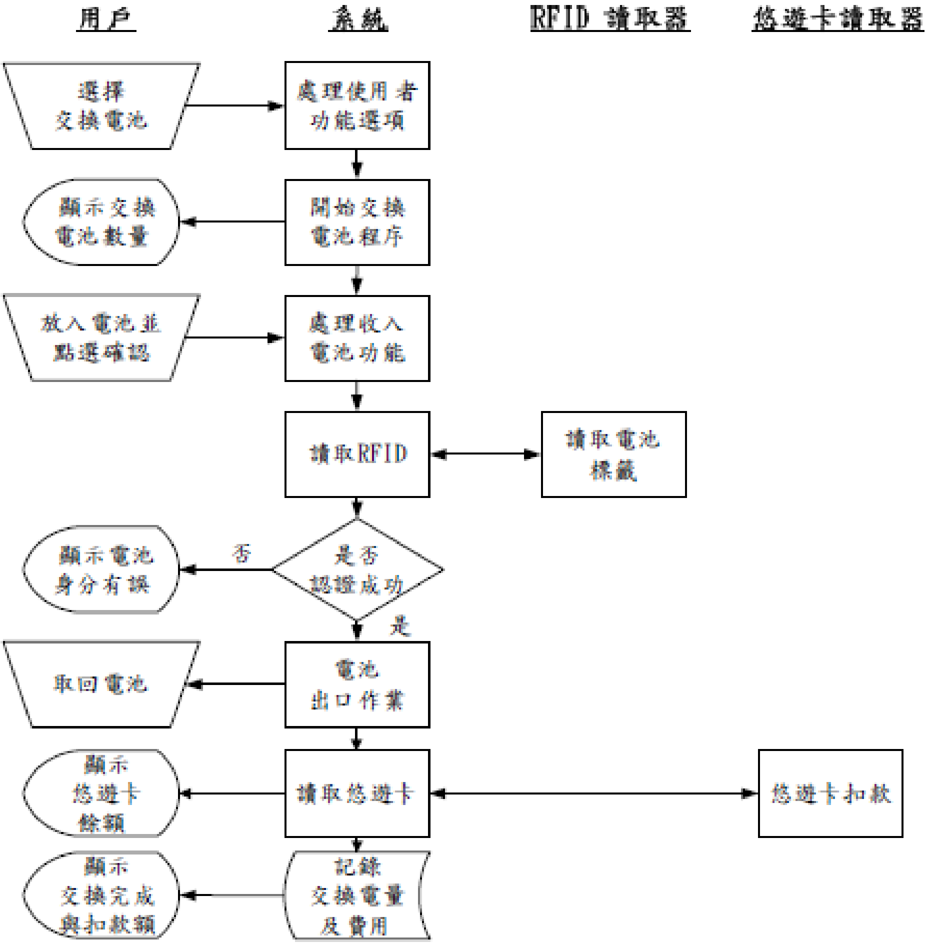


圖 9：電池交換作業流程圖

11

c. 餘額查詢作業流程

(a) 使用者進行身分辨識認證成功，選擇餘額查詢功能。

(b) 系統查詢使用者餘額，並顯示於螢幕上。

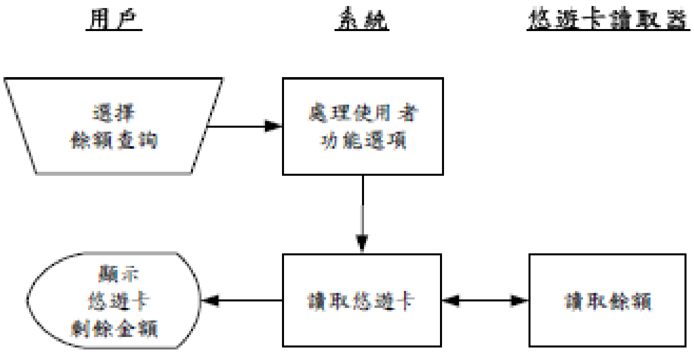


圖 10：餘額查詢作業流程圖

d. 鄰近交換站作業流程

(a) 使用者進行身分辨識認證成功，選擇鄰近交換站功能。

(b) 系統開啟 Google MAP 並顯示鄰近交換站地圖資訊。

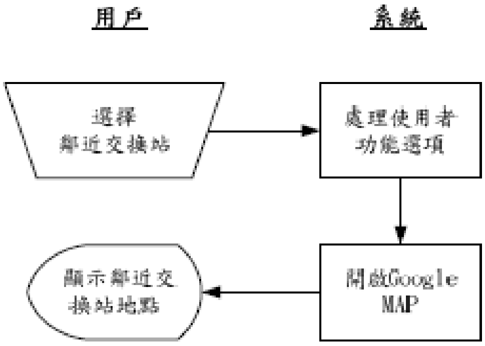


圖 11：鄰近交換站作業流程圖

(2) KIOSK 電池履歷查詢作業程序

a. KIOSK 電池資訊查詢作業流程

(a) 使用者選擇 Kiosk 查詢功能。

(b) 系統開啟 Kiosk 查詢系統。

(c) 系統自動讀取標籤

(d) 沒有讀取到標籤，系統重新自動讀取標籤。

(e) ONS 解析標籤資訊位置

(f) 系統透過 WS 查詢電池資訊，並顯示電池資訊頁

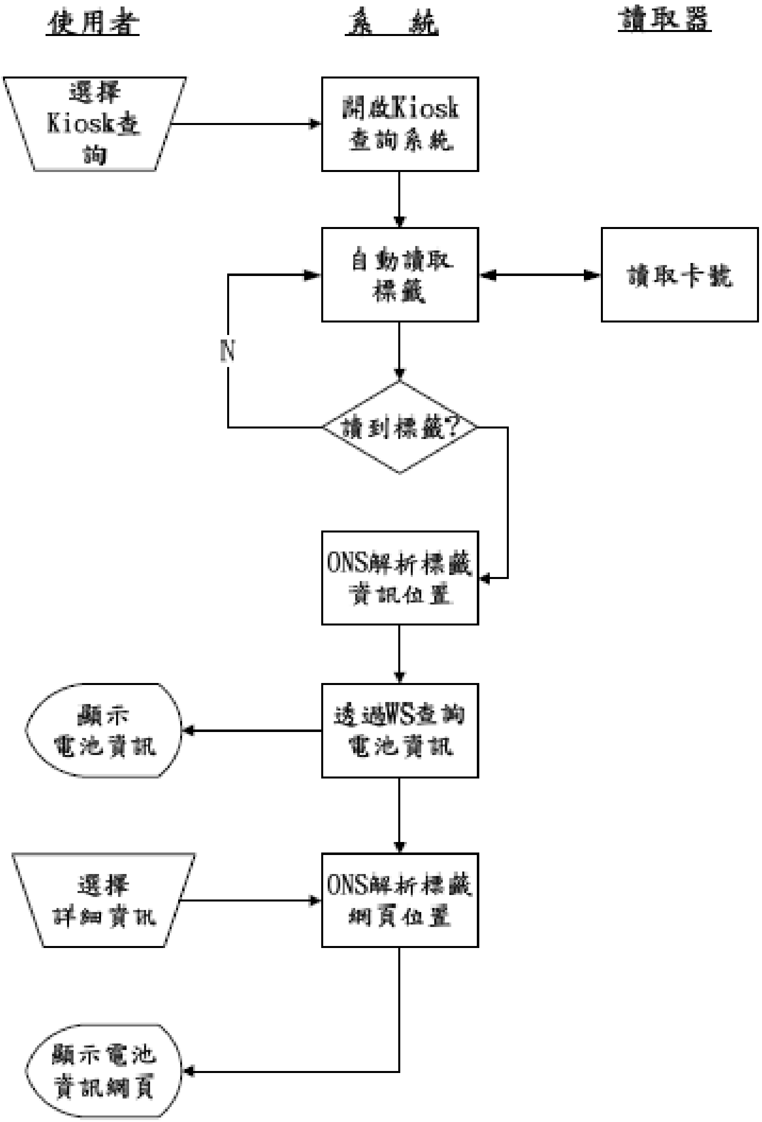
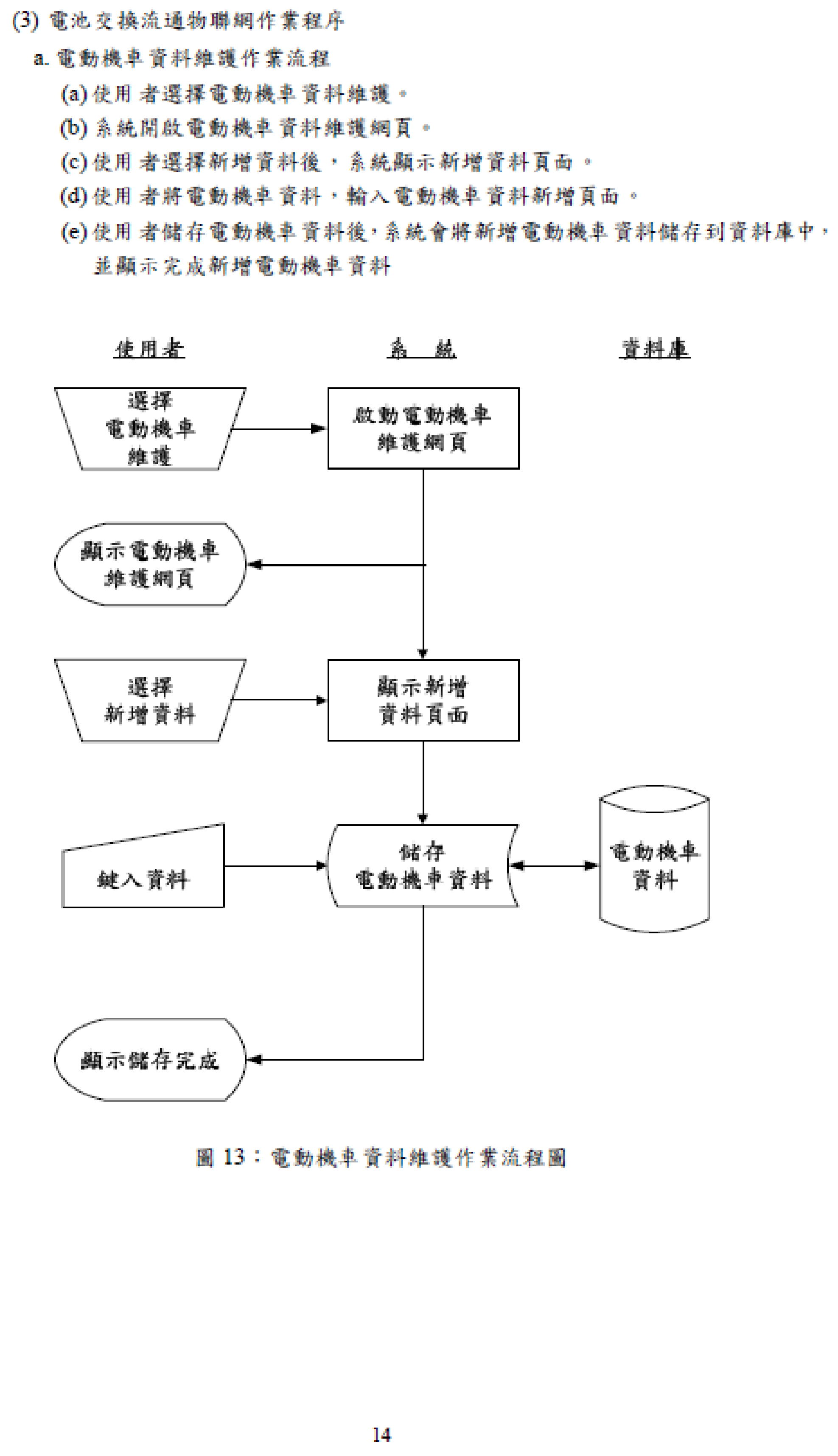


圖 12：KIOSK 電池資訊查詢作業流程圖



(3) 電池交換流通物聯網作業程序

a. 電動機車資料維護作業流程

(a) 使用者選擇電動機車資料維護。

(b) 系統開啟電動機車資料維護網頁。

(c) 使用者選擇新增資料後，系統顯示新增資料頁面。

(d) 使用者將電動機車資料，輸入電動機車資料新增頁面。

(e) 使用者儲存電動機車資料後，系統會將新增電動機車資料儲存到資料庫中，並顯示完成新增電動機車資料

使用者
系 統
資料庫
選擇電動機車維護
啟動電動機車維護網頁
顯示電動機車維護網頁
選擇新增資料
顯示新增資料頁面
鍵入資料
儲存電動機車資料
電動機車資料
顯示儲存完成

圖 13：電動機車資料維護作業流程圖

14

b. 電動機車資料修改作業流程

(a) 使用者選擇電動機車資料維護。

(b) 系統開啟電動機車資料維護網頁。

(c) 使用者選擇欲編輯資料後，系統顯示變更資料頁面。

(d) 使用者填寫修改資料。

(e) 使用者儲存修改資料後，系統會將修改電動機車資料儲存到資料庫中，並顯示完成修改電動機車資料完成。

(f) 如果取消修改：系統則會回復為修改資料前的畫面。

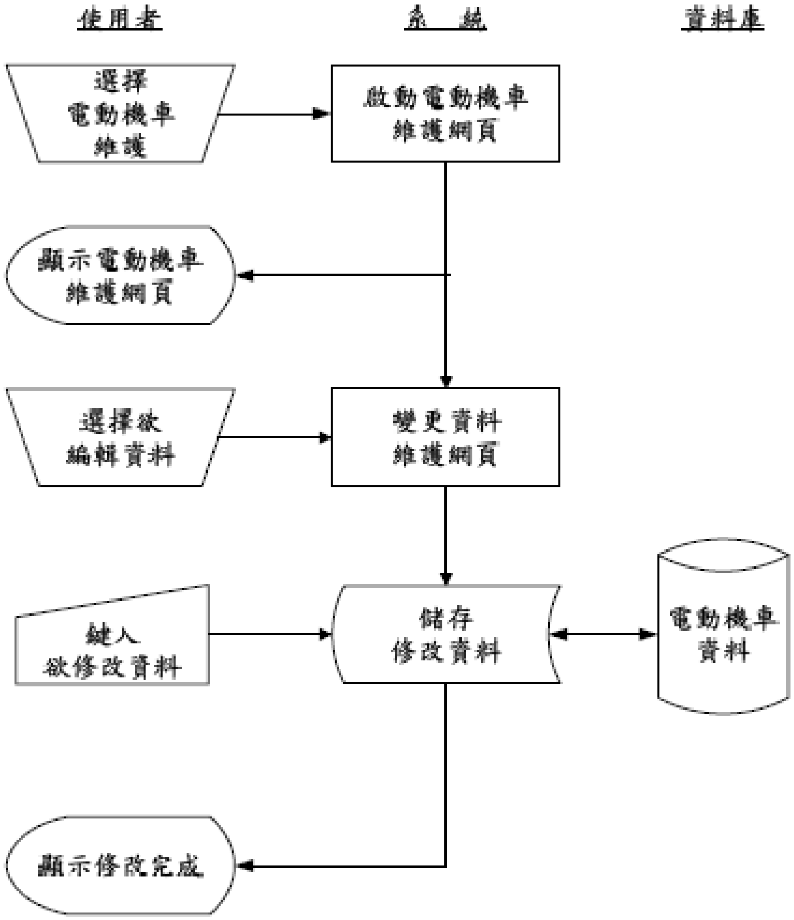


圖 14：電動機車資料修改作業流程圖

c. 電動機車資料查詢作業流程

(a) 使用者選擇電動機車資料維護。

(b) 系統開啟電動機車資料維護網頁。

(c) 使用者輸入查詢條件，系統在使用者點選確認按鈕後， 篩選符合的資料。

(d) 系統會查詢是否有該筆資料，有資料將會顯示紀錄資料，沒有的資料將結束查詢。

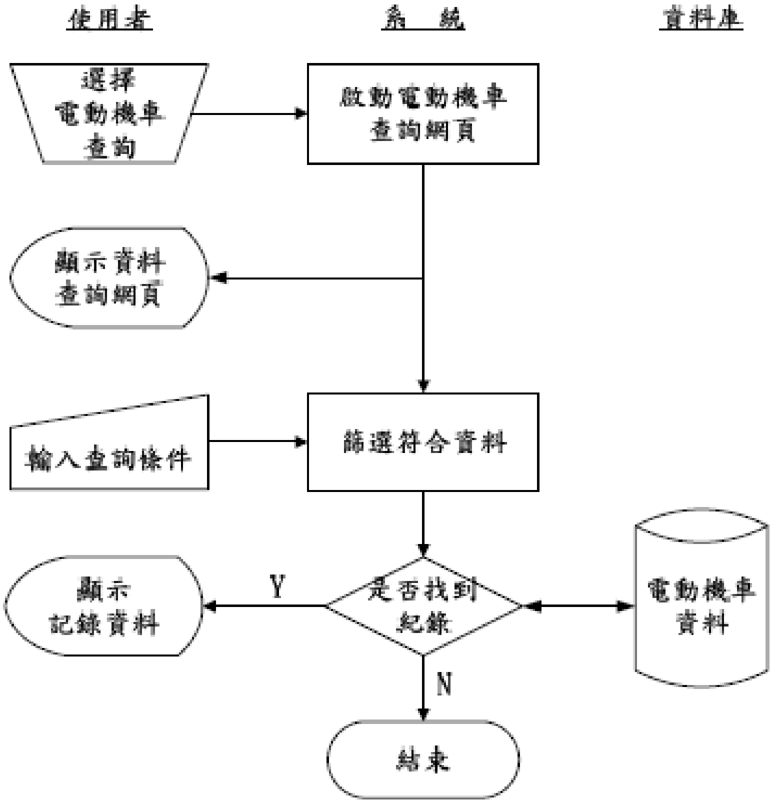


圖 15：電動機車資料查詢作業流程圖

d. 營運中心查詢作業流程

(a) 使用者選擇營運中心查詢。

(b) 系統開啟電營運中心查詢網頁。

(c) 使用者輸入查詢條件，系統在使用者點選確認按鈕後，篩選符合的資料。

(d) 系統會查詢是否有該筆資料，有資料將會顯示紀錄資料，沒有的資料將結束查詢。

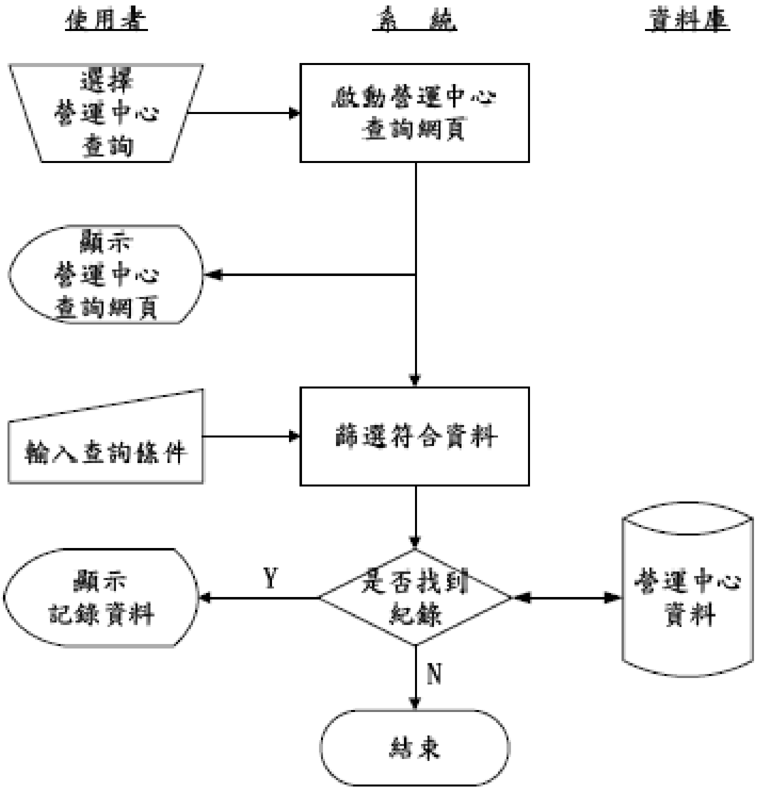


圖 16：中心查詢作業流程圖

17

e. 充電電池資料查詢作業流程

(a) 使用者選擇充電電池資料查詢。

(b) 系統開啟電充電電池資料查詢網頁。

(c) 使用者輸入查詢條件，系統在使用者點選確認按鈕後，篩選符合的資料。

(d) 系統會查詢是否有該筆資料，有資料將會顯示紀錄資料，沒有的資料將結束查詢。

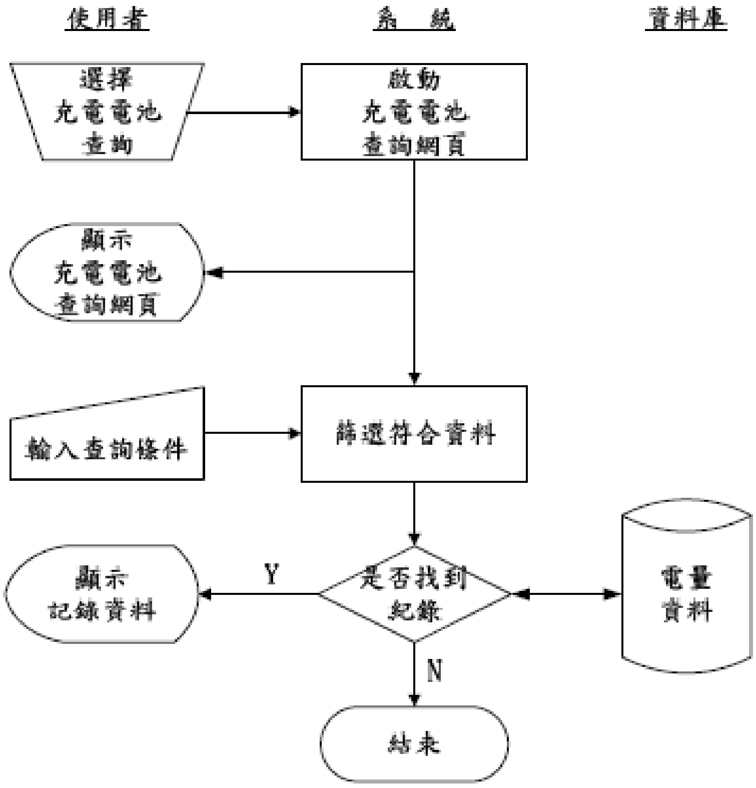


圖 17：充電電池資料查詢作業流程圖

f. 交換站資料查詢作業流程

(a) 使用者選擇交換站資料查詢。

(b) 系統開啟交換站資料查詢網頁。

(c) 使用者輸入查詢條件，系統在使用者點選確認按鈕後，篩選符合的資料。

(d) 系統會查詢是否有該筆資料，有資料將會顯示紀錄資料，沒有的資料將結束查詢。

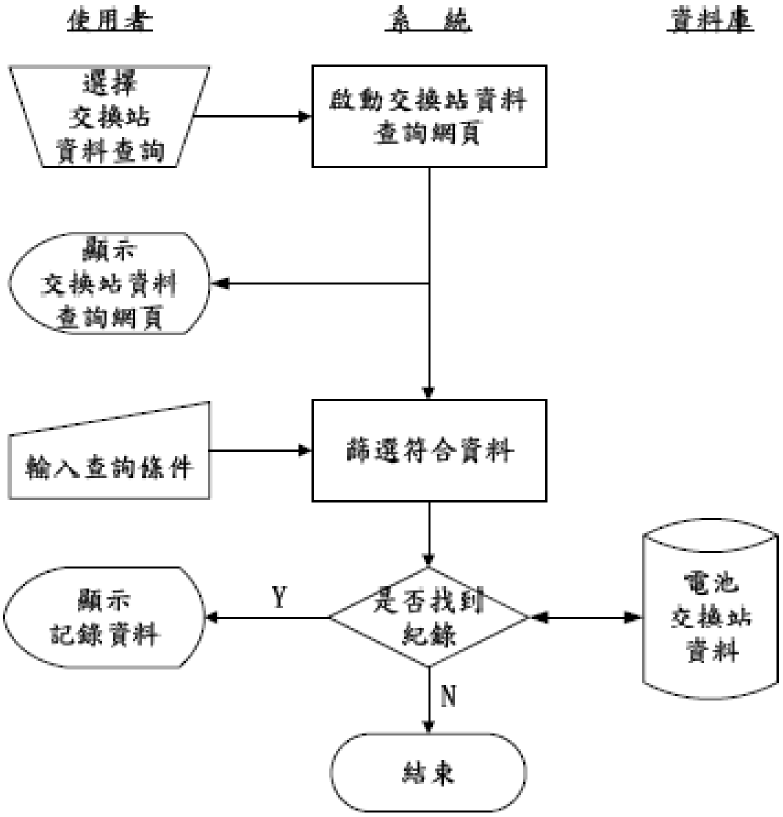


圖 18：交換站資料查詢作業流程圖

g. 逾期電池未換查詢作業流程

(a) 使用者選擇逾期電池未換查詢。

(b) 系統開啟逾期電池未換查詢網頁。

(c) 使用者輸入逾期天數，系統在使用者點選確認按鈕後，篩選符合的資料。

(d) 系統會查詢是否有該筆資料，有資料將會顯示紀錄資料，沒有的資料將結束查詢。

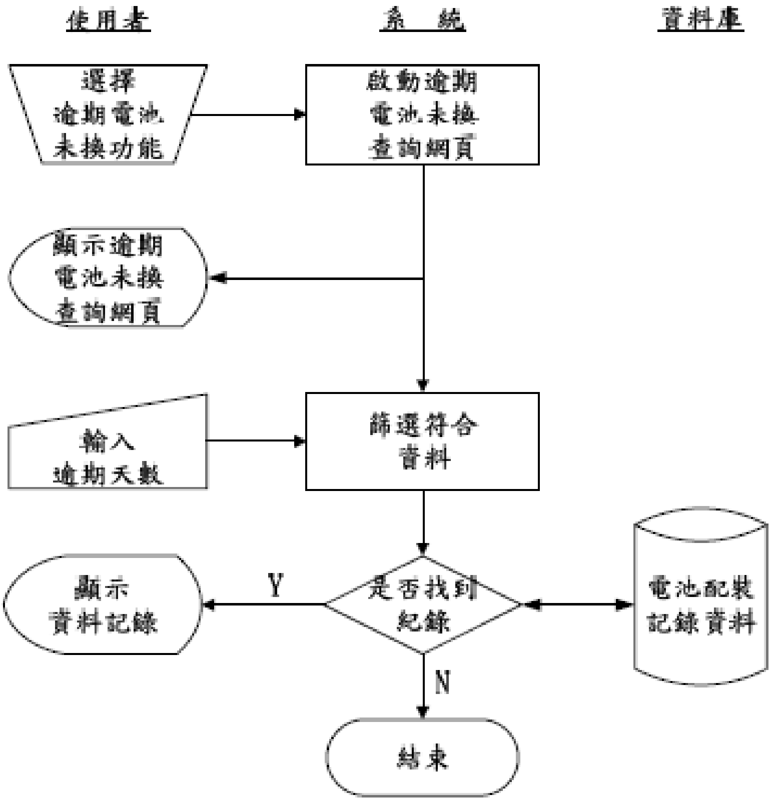


圖 19：電池未換查詢作業流程圖

h. 電池交易查詢作業流程

(a) 使用者選擇電池交易查詢。

(b) 系統開啟電池交易查詢網頁。

(c) 使用者輸入查詢條件，系統在使用者點選確認按鈕後，篩選符合的資料。

(d) 系統會查詢是否有該筆資料，有資料將會顯示紀錄資料，沒有的資料將結束查詢。

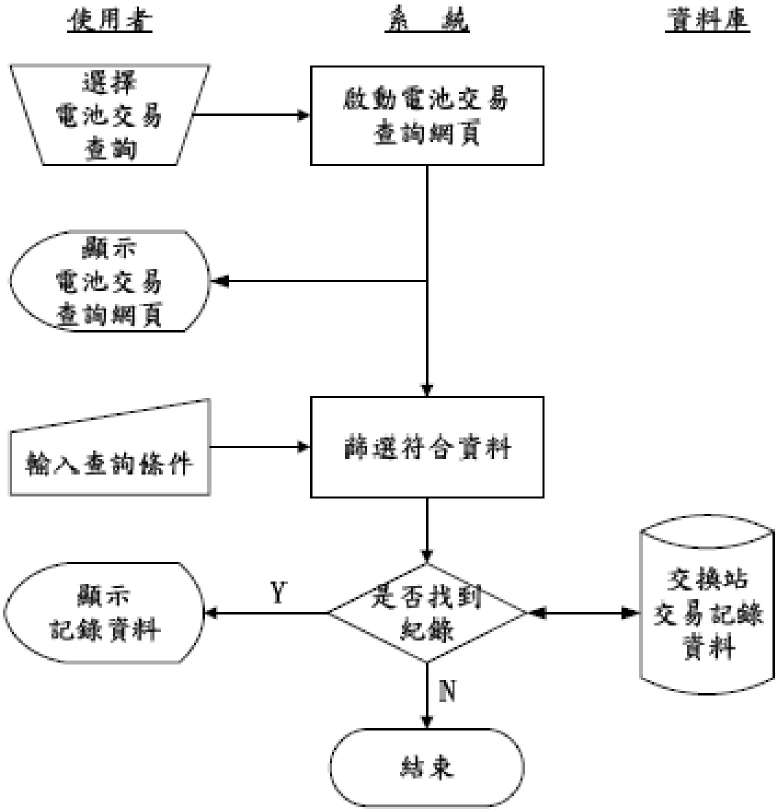


圖 20：交易查詢作業流程圖

i. 電池交換費用統計表流程（略，限於合作廠商保密協定）

j. 交換費用統計表作業流程（略，限於合作廠商保密協定）

k. 營業日報表作業流程（略，限於合作廠商保密協定）

4.模組架構圖

(1) 電池交換系統模組架構

本系統架構包含六個主要功能的模組，分別為連線參數設定模組，車主身分辨識模組、電池交換及扣款、餘額查詢、鄰近交換站、PLC 圖示、悠遊卡帳務處裡。以下為各模組的說明：

a. 連線參數設定功能模組：

(a) 入口讀取器設定功能：提供使用者設定入口 RFID 讀取器參數功能。

(b) 出口讀取器設定功能：提供使用者設定出口 RFID 讀取器參數功能。

(c) HF 通訊設定功能：提供使用者設定 HF 讀取器參數功能。

(d) PLC 通訊設定功能：提供使用者設定 RS232 通訊連線參數功能。

b. 悠遊卡車主身分辨識功能模組：

(a) 車主悠遊卡認證功能：提供車主進行悠遊卡讀取認證功能。

(b) 車主密碼認證功能：提供車主進行密碼認證功能。

(c) 悠遊卡扣款處理功能：提供進行悠遊卡扣款作業功能。

(d) 餘額查詢功能：提供車主進行餘額查詢功能。

c. 電池交換及扣款功能：提供車主進行電池交換作業及扣款作業功能。

d. PLC 圖示功能：顯示交換機台內部電池運作狀態圖示。

e. 鄰近交換站功能：提供使用者查詢鄰近交換站功能。

f. 悠遊卡帳務處理：提供使用者上傳當日交易資料功能。

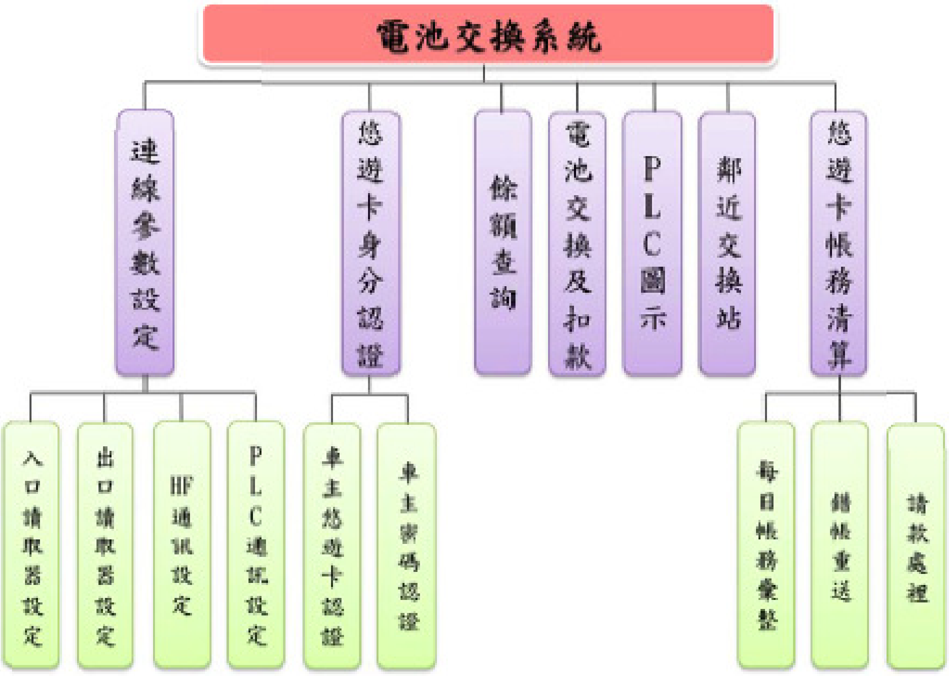


圖 21：「電池交換系統」模組架構圖

(2) KIOSK 電池履歷系統模組架構

本系統架構包含三個模組，分別為 RFID 讀取器設定、查詢簡易資料、查詢詳細資料。以下為各模組功能的說明：

a. RFID 讀取器設定模組：設定 Reader 的標籤讀取模式、連線埠、傳輸率及等待時間等參數。與 Reader 進行連線，並儲存連線資訊。

b. 查詢簡易資料：提供使用者查訊簡易的電池資料。

c. 查詢詳細資料：提供使用者查詢詳細的電池資料。

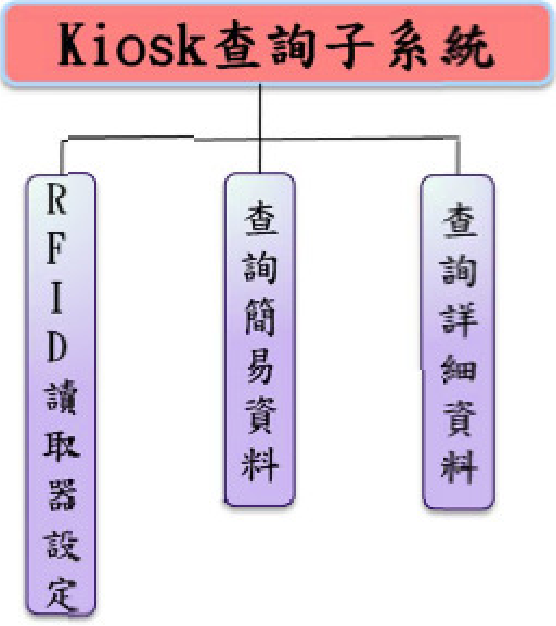
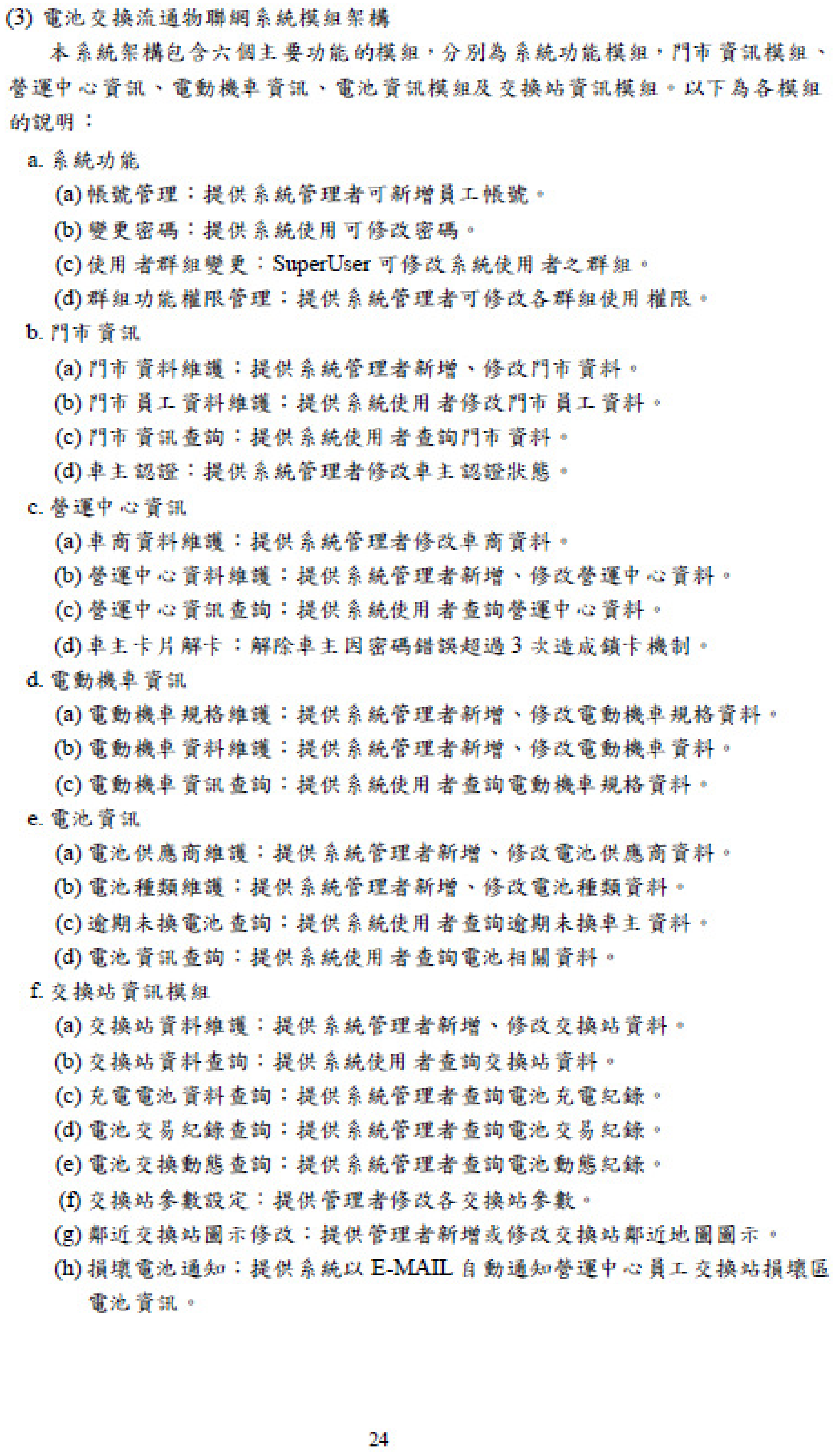


圖 22：「Kiosk 子系統」功能模組圖



(3) 電池交換流通物聯網系統模組架構

本系統架構包含六個主要功能的模組，分別為系統功能模組，門市資訊模組、營運中心資訊、電動機車資訊、電池資訊模組及交換站資訊模組。以下為各模組的說明：

a. 系統功能

(a) 帳號管理：提供系統管理者可新增員工帳號。

(b) 變更密碼：提供系統使用可修改密碼。

(c) 使用者群組變更：SuperUser 可修改系統使用者之群組。

(d) 群組功能權限管理：提供系統管理者可修改各群組使用權限。

b. 門市資訊

(a) 門市資料維護：提供系統管理者新增、修改門市資料。

(b) 門市員工資料維護：提供系統使用者修改門市員工資料。

(c) 門市資訊查詢：提供系統使用者查詢門市資料。

(d) 車主認證：提供系統管理者修改車主認證狀態。

c. 營運中心資訊

(a) 車商資料維護：提供系統管理者修改車商資料。

(b) 營運中心資料維護：提供系統管理者新增、修改營運中心資料。

(c) 營運中心資訊查詢：提供系統使用者查詢營運中心資料。

(d) 車主卡片解卡 ：解除車主因密碼錯誤超過 3 次造成鎖卡機制。

d. 電動機車資訊

(a) 電動機車規格維護：提供系統管理者新增、修改電動機車規格資料。

(b) 電動機車資料維護：提供系統管理者新增、修改電動機車資料。

(c) 電動機車資訊查詢：提供系統使用者查詢電動機車規格資料。

e. 電池資訊

(a) 電池供應商維護：提供系統管理者新增、修改電池供應商資料。

(b) 電池種類維護：提供系統管理者新增、修改電池種類資料。

(c) 逾期未換電池查詢：提供系統使用者查詢逾期未換車主資料。

(d) 電池資訊查詢：提供系統使用者查詢電池相關資料。

f. 交換站資訊模組

(a) 交換站資料維護：提供系統管理者新增、修改交換站資料。

(b) 交換站資料查詢：提供系統使用者查詢交換站資料。

(c) 充電電池資料查詢：提供系統管理者查詢電池充電紀錄。

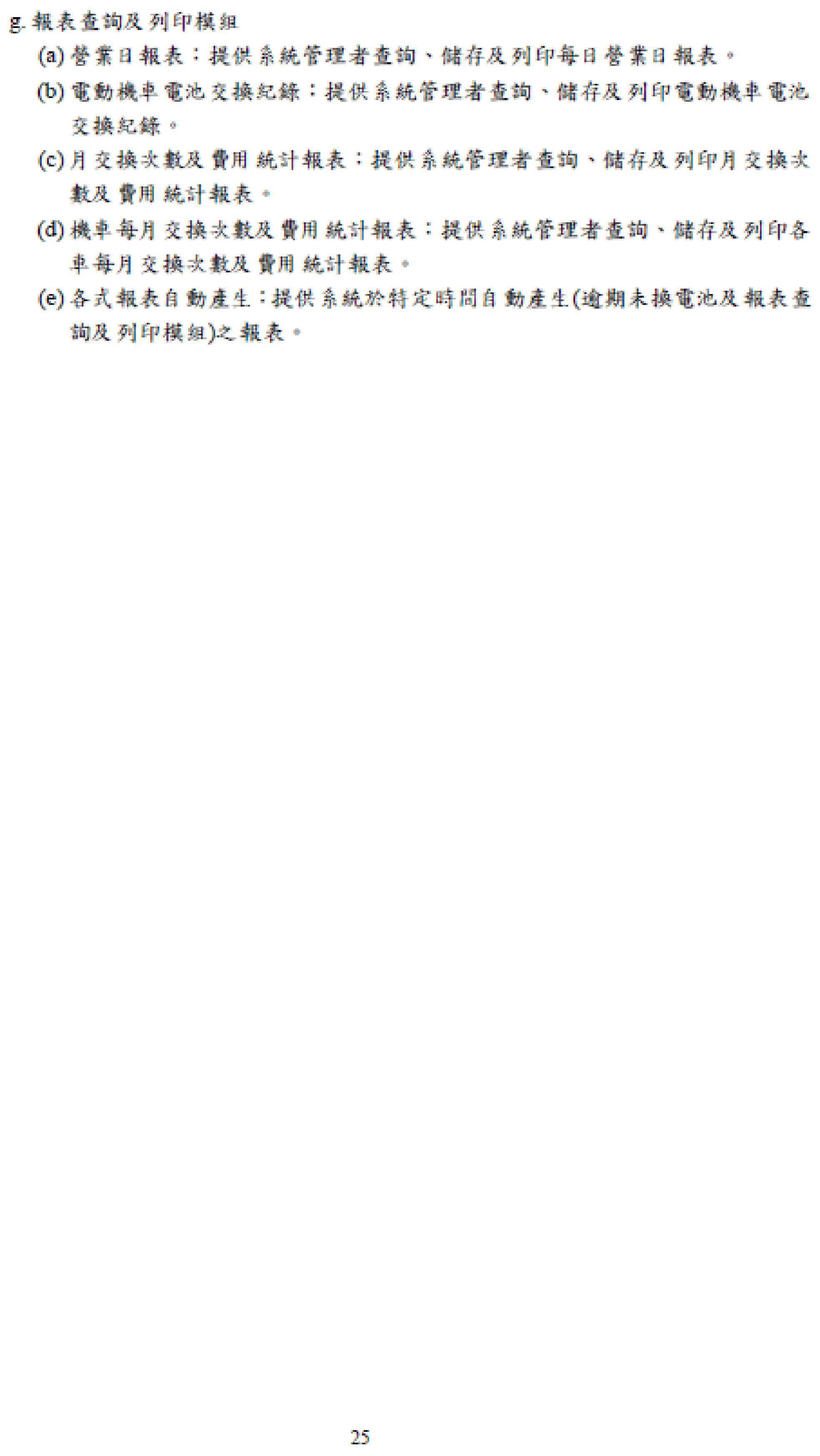
(d) 電池交易紀錄查詢：提供系統管理者查詢電池交易紀錄。

(e) 電池交換動態查詢：提供系統管理者查詢電池動態紀錄。

(f) 交換站參數設定：提供管理者修改各交換站參數。

(g) 鄰近交換站圖示修改：提供管理者新增或修改交換站鄰近地圖圖示。

(h) 損壞電池通知：提供系統以 E-MAIL 自動通知營運中心員工交換站損壞區電池資訊。



g. 報表查詢及列印模組

(a) 營業日報表：提供系統管理者查詢、儲存及列印每日營業日報表。

(b) 電動機車電池交換紀錄：提供系統管理者查詢、儲存及列印電動機車電池交換紀錄。

(c) 月交換次數及費用統計報表：提供系統管理者查詢、儲存及列印月交換次數及費用統計報表。

(d) 機車每月交換次數及費用統計報表：提供系統管理者查詢、儲存及列印各車每月交換次數及費用統計報表。

(e) 各式報表自動產生：提供系統於特定時間自動產生(逾期未換電池及報表查詢及列印模組)之報表。

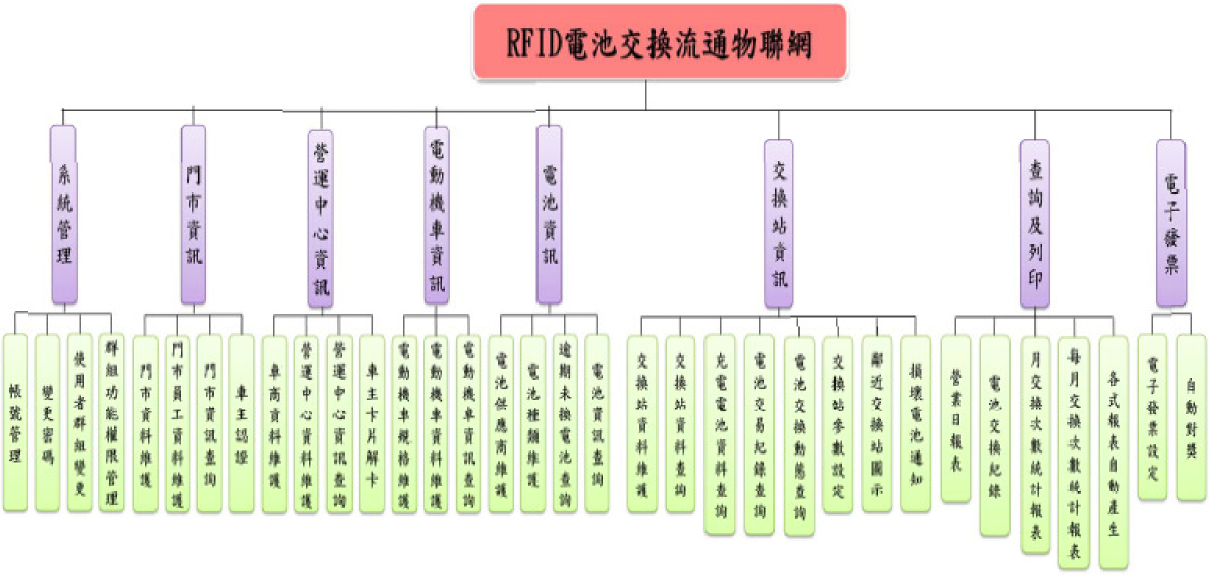


圖 23：「電池交換流通物聯網」系統模組架構圖

五、結果

(一) 系統實體架構設計結果

1. 電池交換系統元件部署架構為包括 2 個執行環境(如下圖)：

(1) 電池交換伺服器：

a. Internet Information Service 7.0：提供網路服務所需的執行環境內含 Web Service 的主要元件 Web Service 的介面資料庫連線字串 DatabaseConnectString。

b. SQL Server 2008：內含本系統的資料庫 DB.mdf，可提供電池交換顧客管理系統相關資料操作服務。

(2) 電池交換系統：提供使用者進行電池交換、餘額查詢、鄰近交換站、PLC 圖示等各項相關操作。

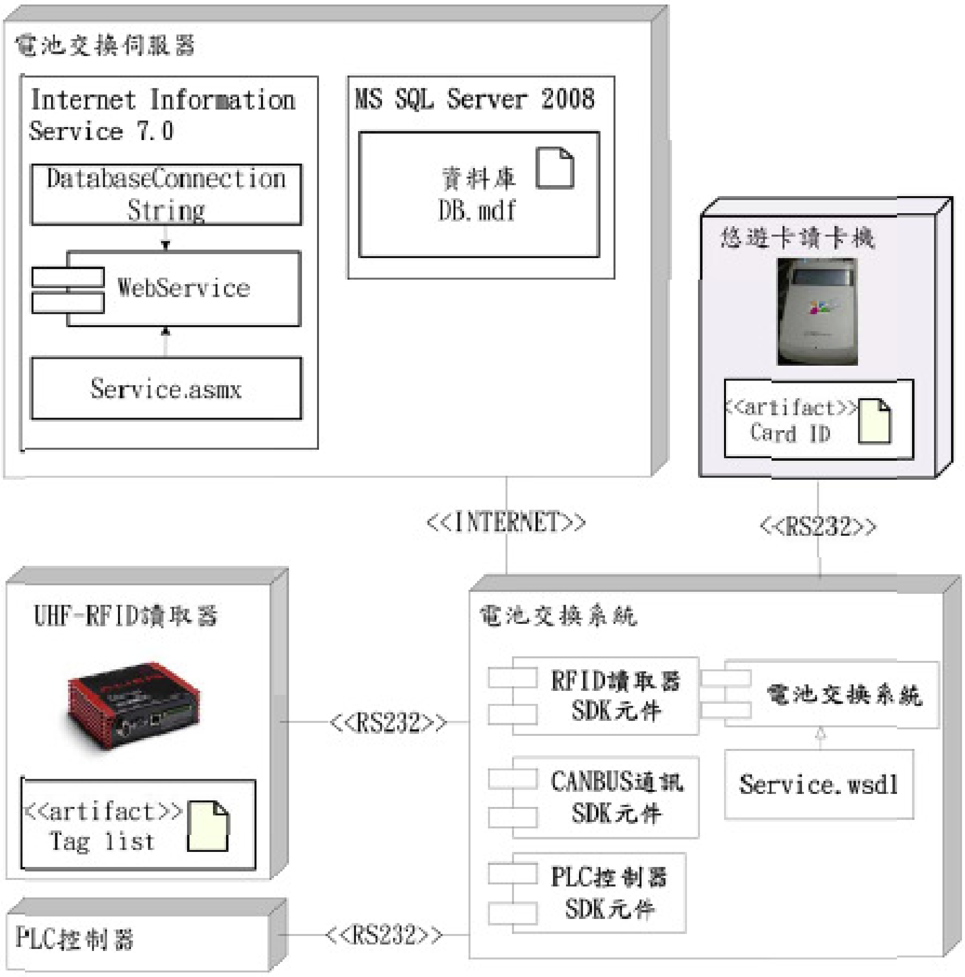
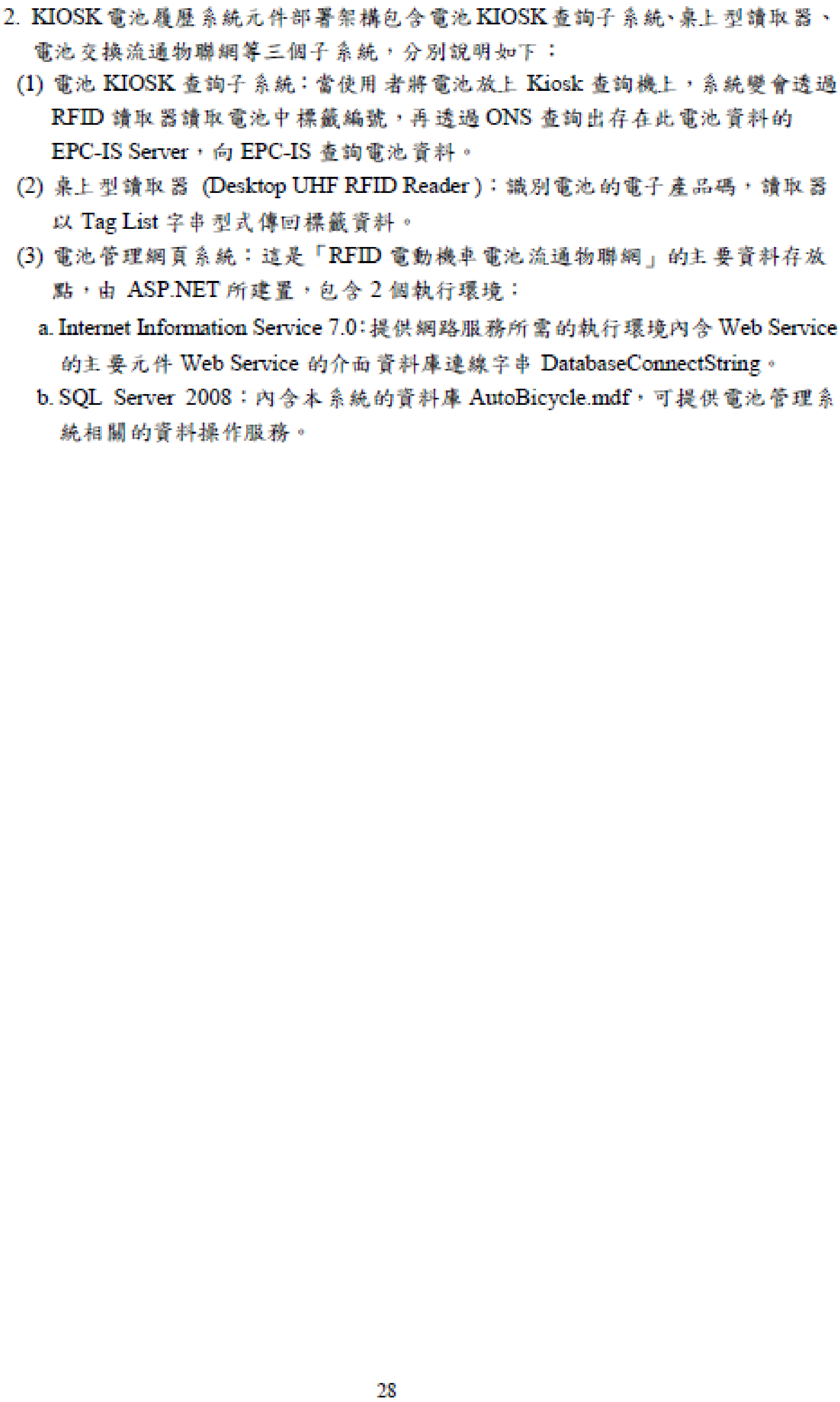


圖 24：電池交換系統部署架構圖



2. KIOSK 電池履歷系統元件部署架構包含電池 KIOSK 查詢子系統、桌上型讀取器、電池交換流通物聯網等三個子系統，分別說明如下：

(1) 電池 KIOSK 查詢子系統：當使用者將電池放上 Kiosk 查詢機上，系統變會透過 RFID 讀取器讀取電池中標籤編號，再透過 ONS 查詢出存在此電池資料的 EPC-IS Server，向 EPC-IS 查詢電池資料。

(2) 桌上型讀取器 (Desktop UHF RFID Reader)：識別電池的電子產品碼，讀取器以 Tag List 字串型式傳回標籤資料。

(3) 電池管理網頁系統：這是「RFID 電動機車電池流通物聯網」的主要資料存放點，由 ASP.NET 所建置，包含 2 個執行環境：

a. Internet Information Service 7.0：提供網路服務所需的執行環境內含 Web Service 的主要元件 Web Service 的介面資料庫連線字串 DatabaseConnectString。

b. SQL Server 2008：內含本系統的資料庫 AutoBicycle.mdf，可提供電池管理系統相關的資料操作服務。

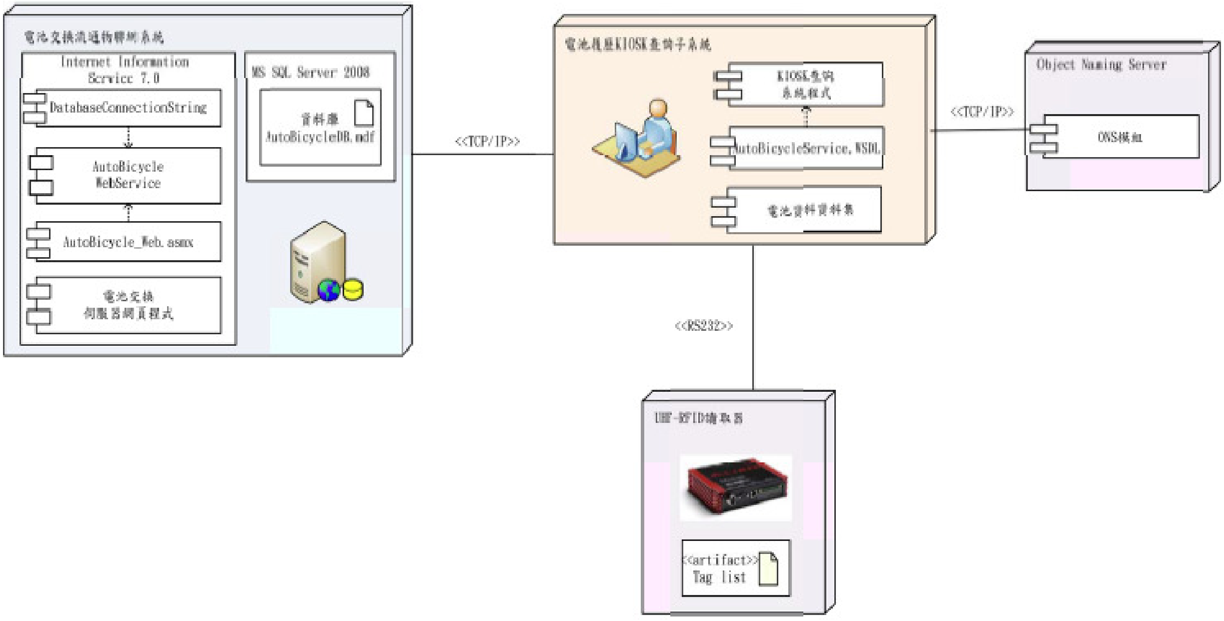


圖 25：KIOSK 電池履歷部署架構圖

3. 電池交換流通物聯網系統元件部署架構包括下列 2 個執行環境：

(1) Internet Information Service 7.0：提供網路服務所需的執行環境內含 Web Service 的主要元件 Web Service 的介面資料庫連線字串 DatabaseConnectString。電池交換伺服器網頁程式提供管理者及使用者查詢相關資訊

(2) SQL Server 2008：內含本系統的資料庫 AutoBicycleDB.mdf，可提供電池交換顧客管理系統相關資料操作服務。

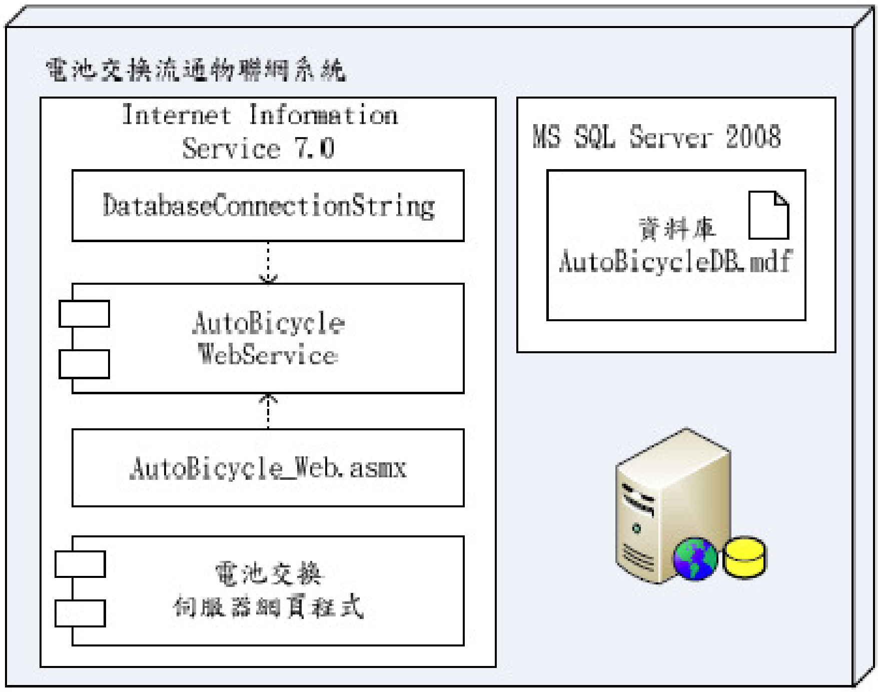


圖 26：電池交換流通物聯網系統部署架構圖

(二) 資料模型-實體關聯圖（略，限於合作廠商保密協定）

(三) 系統實體設計結果

1. 電池交換系統

(1) 電池交換站連線參數設定模組（略，限於合作廠商保密協定）

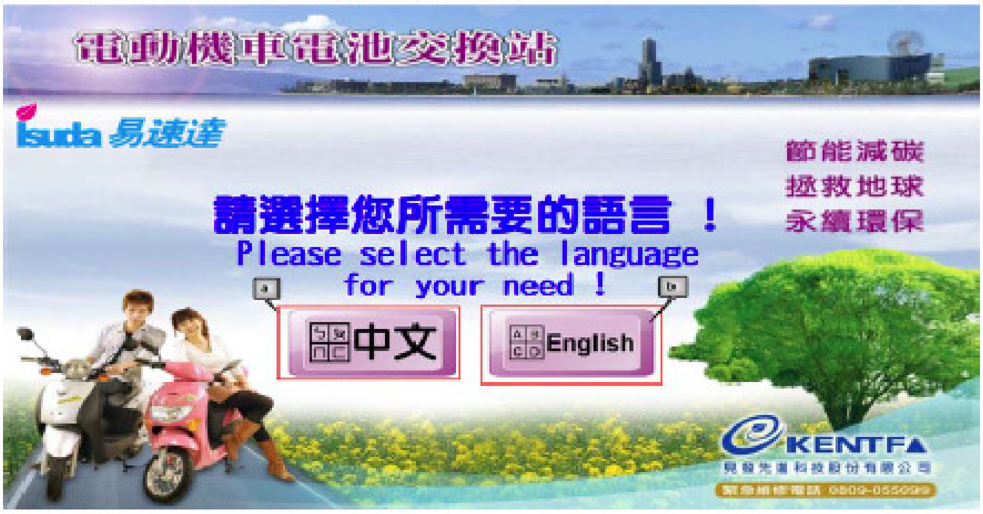
(2) 通訊控制（略，限於合作廠商保密協定）

(3) 顧客電池交換及扣款

a. 主畫面：提供中英文語系選擇功能

(a) 點選中文，以中文介面進行後續操作。

(b) 點選 English，以英文介面進行後續操作。

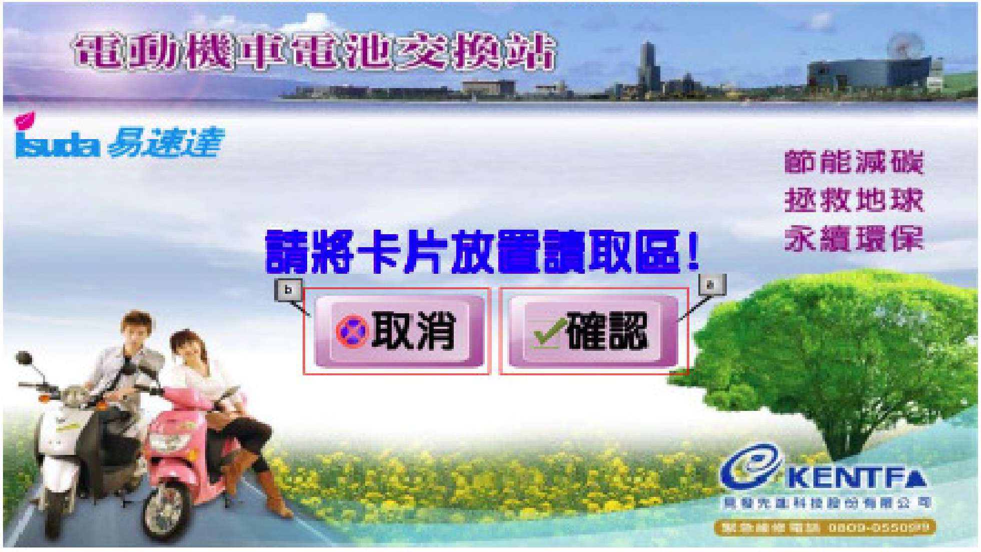


請選擇您所需要的語言！
Please select the language for your need!

b. 悠遊卡讀取畫面：提供悠遊卡讀取功能，系統會等待顧客將卡片放置於悠遊卡卡槽後，進行下列動作。

(a) 確認：執行讀取卡片功能，若讀取成功，則進入密碼輸入介面；若讀取失敗，則顯示查無此卡片資訊。

(b) 取消：取消讀取卡片功能，並返回系統主畫面。



請將卡片放置讀取區!

c. 密碼輸入畫面：提供密碼輸入功能

(a) 輸入密碼資料欄位。

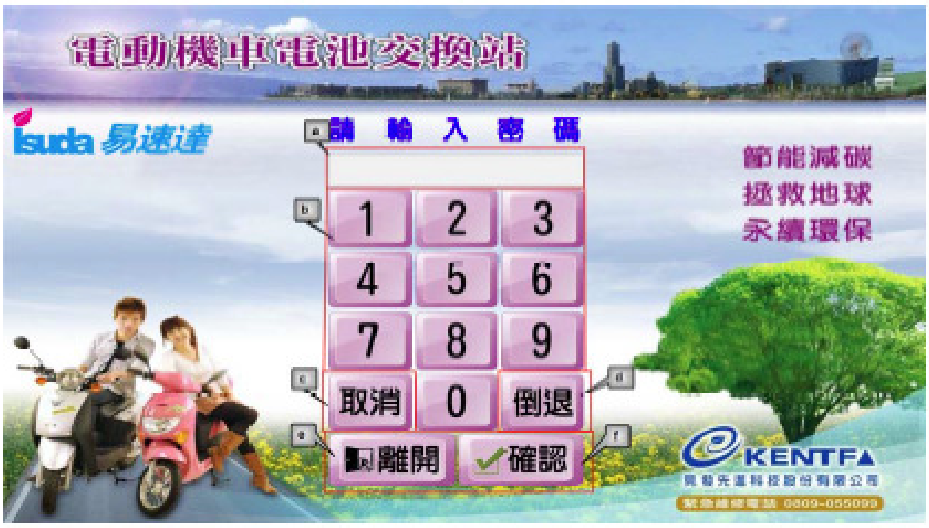
(b) 密碼輸入按鍵。

(c) 取消 ：清空密碼資料，以便重新輸入。

(d) 倒退 ：清除末位數密碼資料，以便重新輸入。

(e) 離開 ：返回系統主畫面。

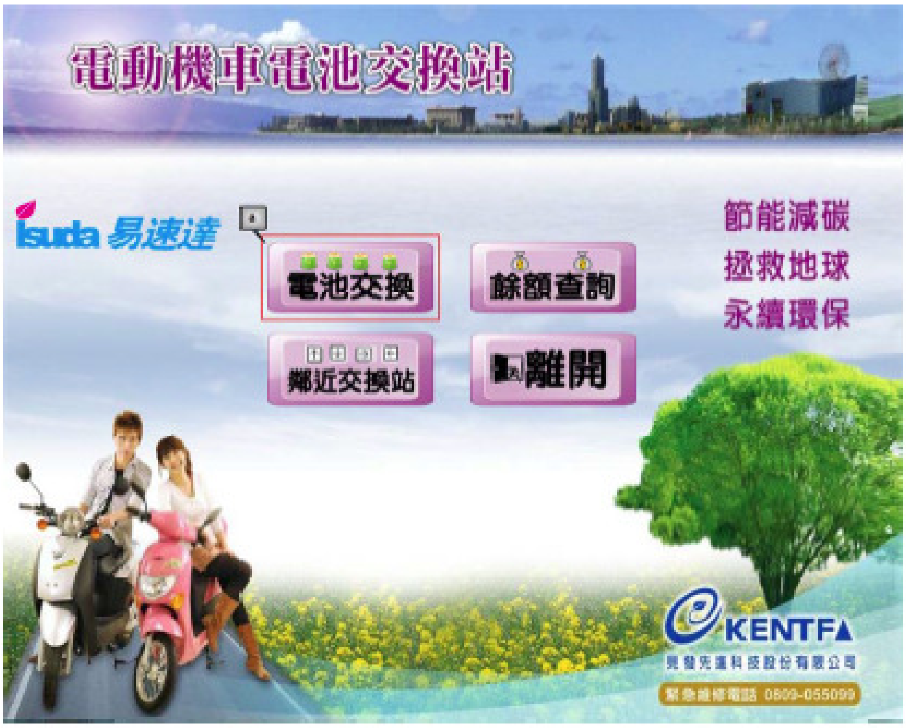
(f) 確認：確認已輸入之密碼，若為正確，則進入系統功能選單，若密碼輸入錯誤，則顯示密碼輸入錯誤，請重新輸入。



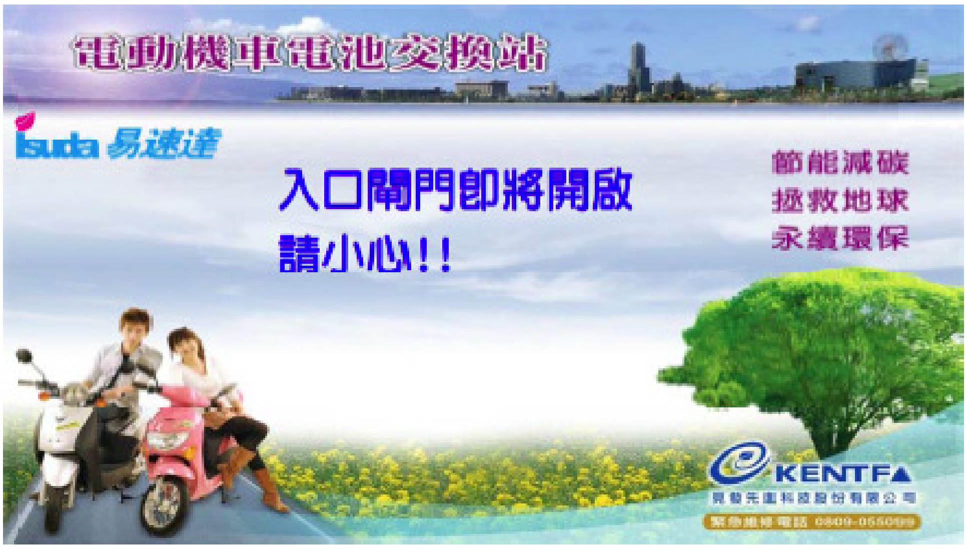
d. 電池交換模組功能選單

(a) 電池交換：提供顧客送入殘餘電量之電池，進行交換程序，並取回滿電量之電池，交換程序如下：

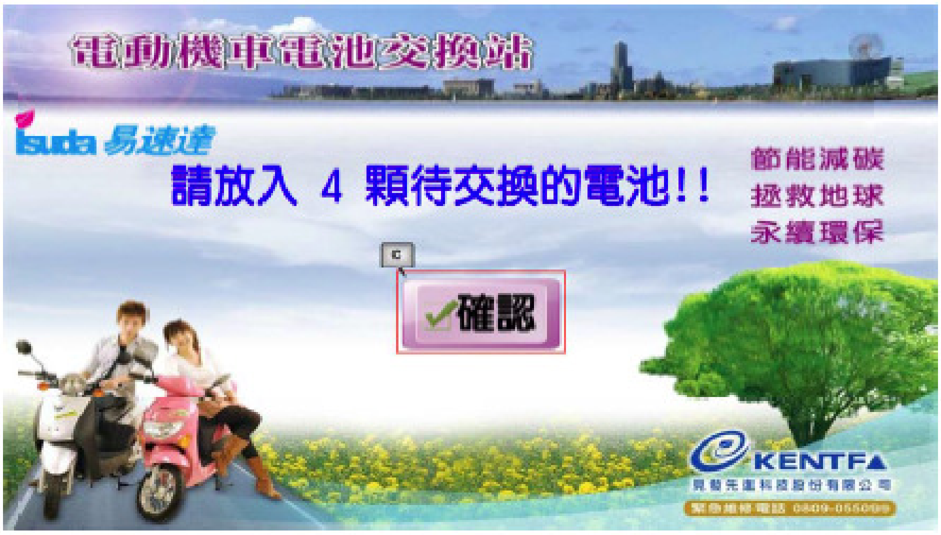
i. 點選【電池交換】按鈕



ii. 顯示入口閘門即將開啟! 請小心!!

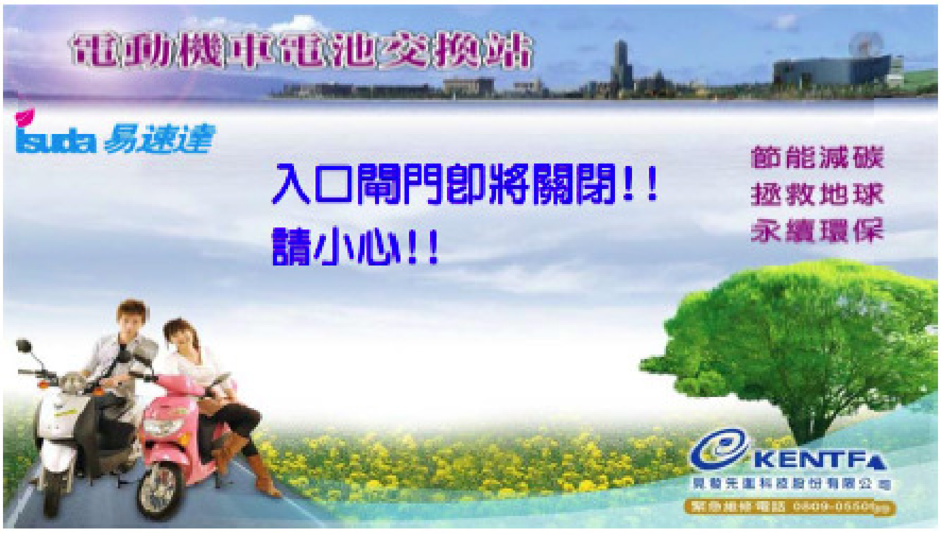

入口閘門即將開啟
請小心!!

iii. 放入四顆待交換電池，並點選【確認】進入下一道程序



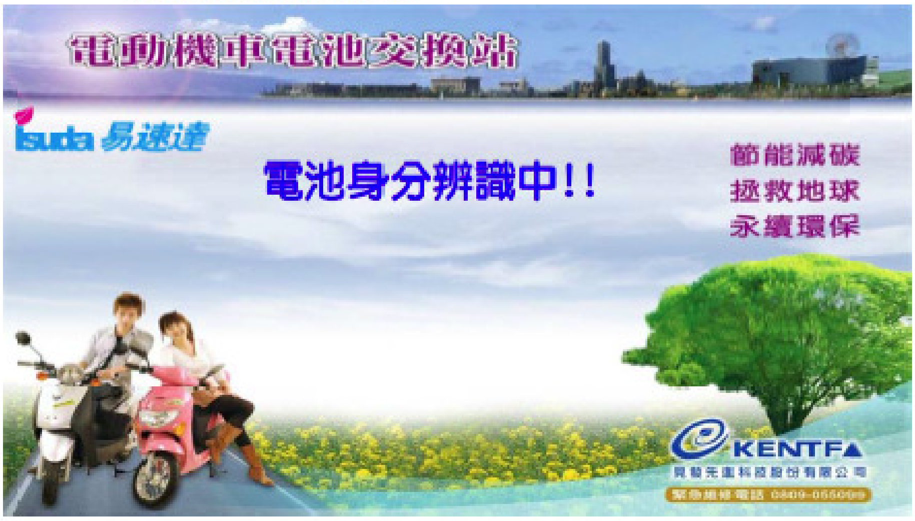
請放入 4 顆待交換的電池!!

iv. 顯示入口閘門即將關閉!! 請小心!!



入口閘門即將關閉!!
請小心!!

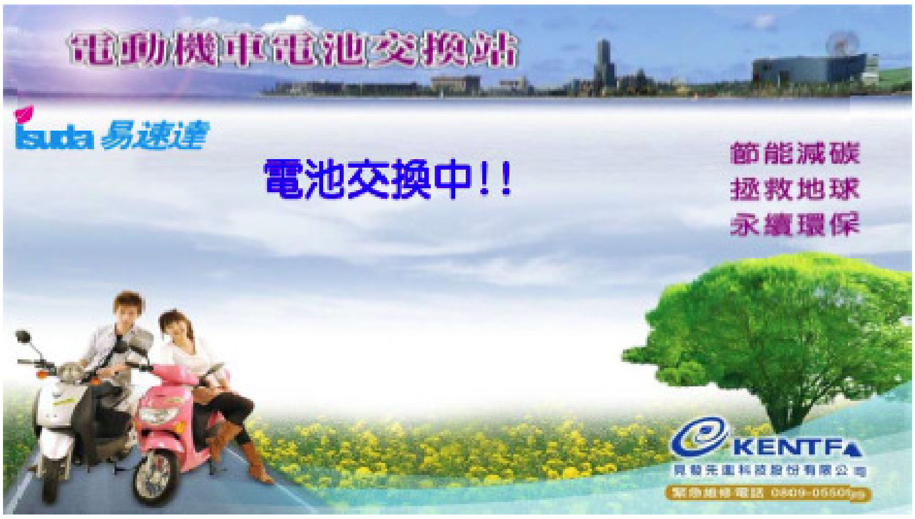
v. 顯示電池身分辨識中!!



電動機車電池交換站

電池身分辨識中!!

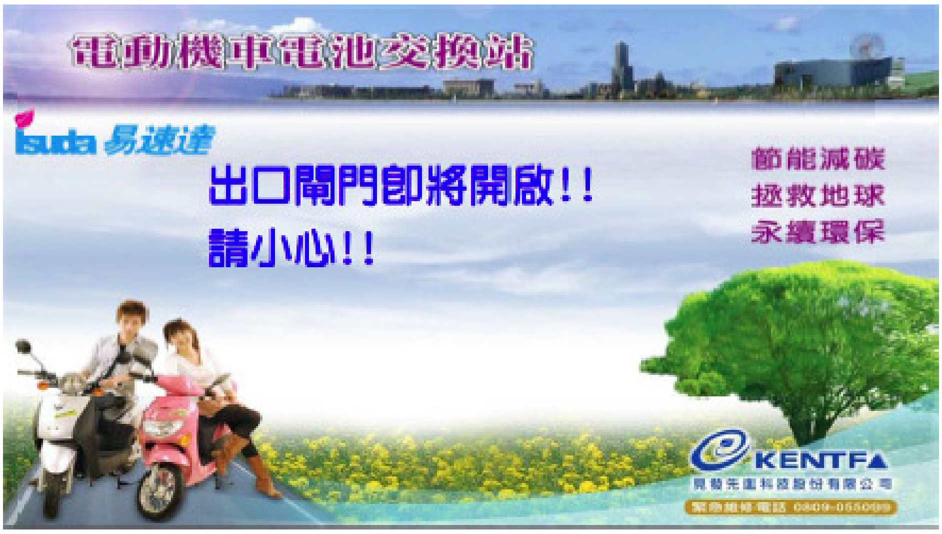
vi. 顯示電池交換中!!



電動機車電池交換站

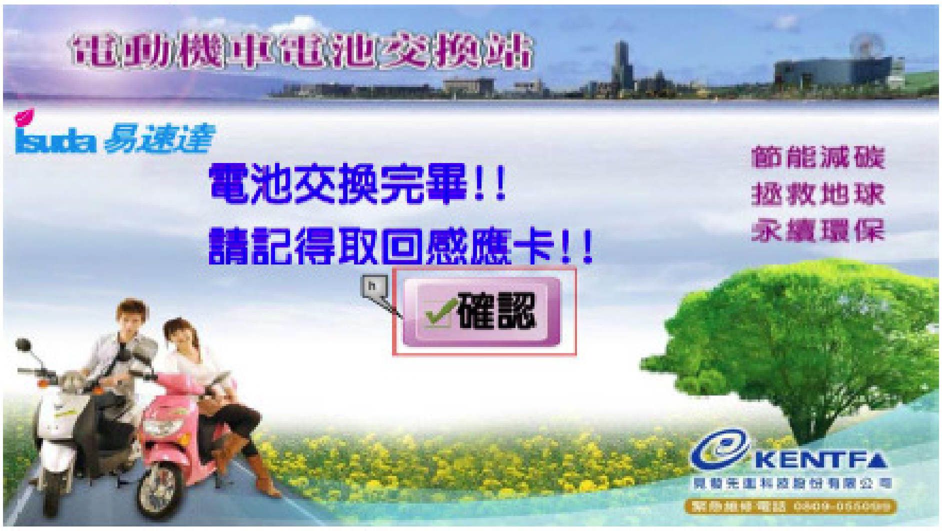
電池交換中!!

vii. 顯示出口閘門即將開啟!!請小心!!



出口閘門即將開啟!!
請小心!!

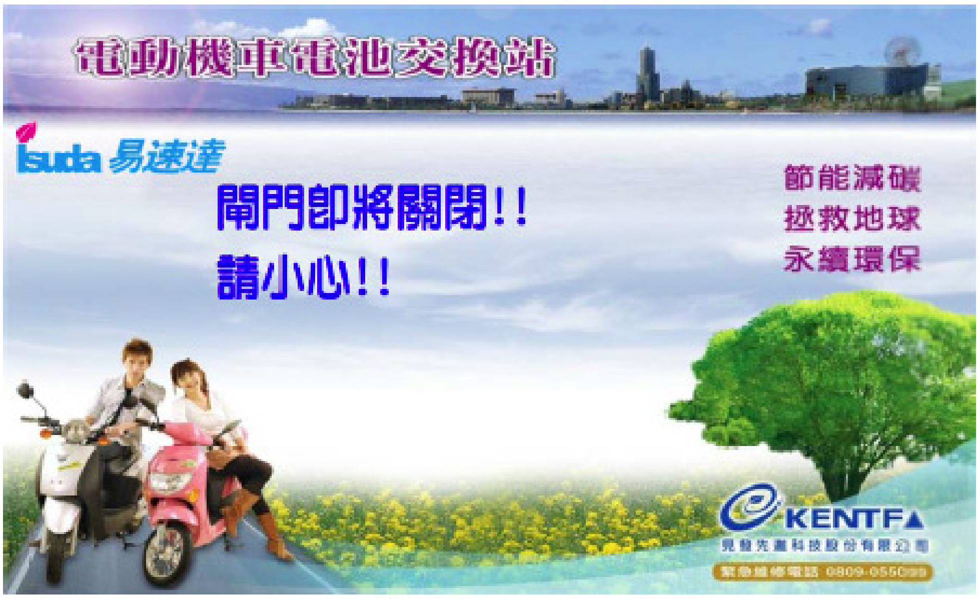
viii. 顯示電池交換完畢!! 請記得取回感應卡!!點選【確認】，進入下一道程序



電池交換完畢!!
請記得取回感應卡!!

36

ix. 顯示閘門即將關閉!!請小心!!

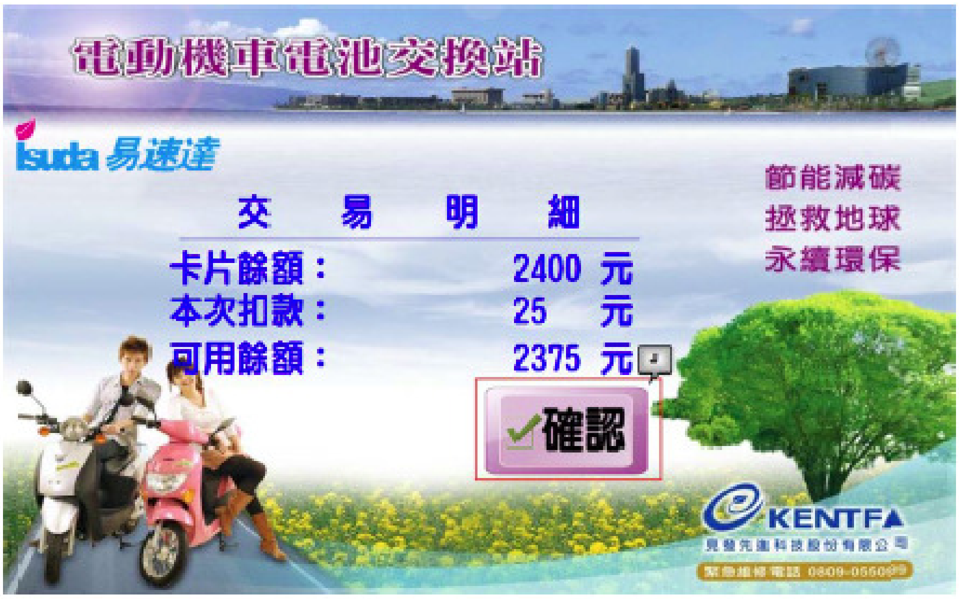


電動機車電池交換站

閘門即將關閉!!

請小心!!

x. 顯示交易明細，並點選確認，進入下一道程序



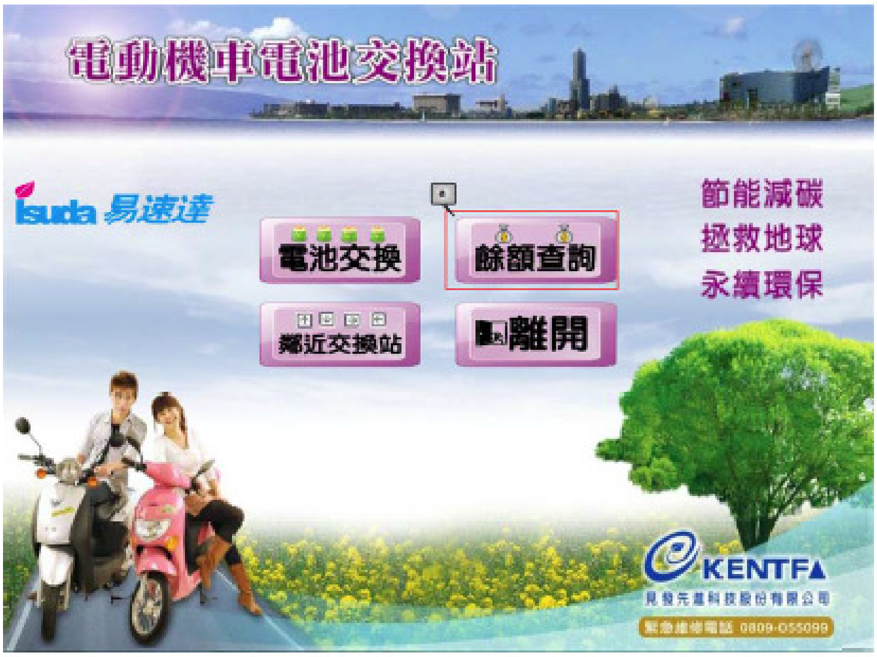
電動機車電池交換站

交易明細

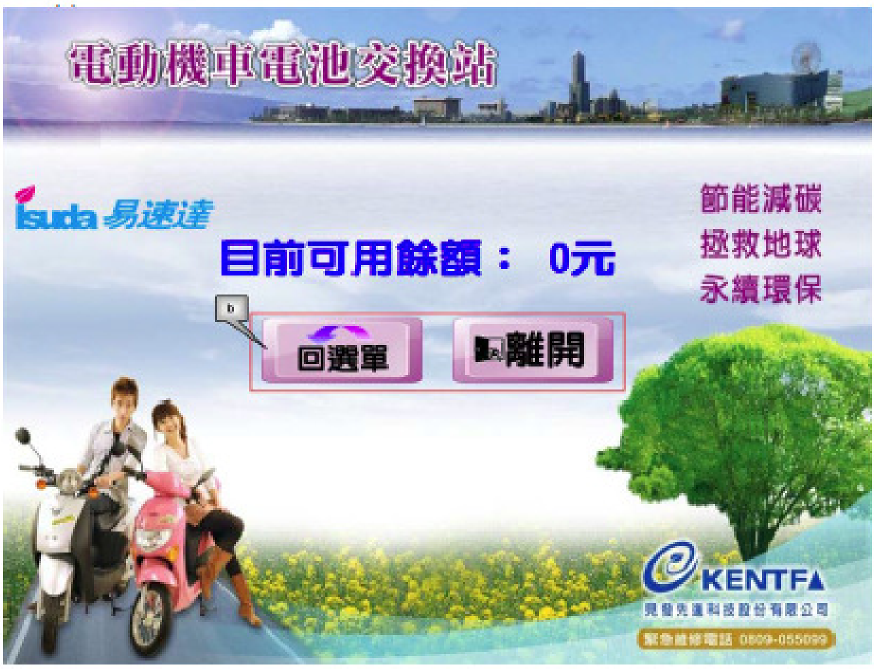
卡片餘額：	2400 元
本次扣款：	25 元
可用餘額：	2375 元

(b) 餘額查詢：提供顧客查詢卡片餘額，查詢程序如下。

i. 點選【餘額查詢】按鈕，進入餘額查詢流程

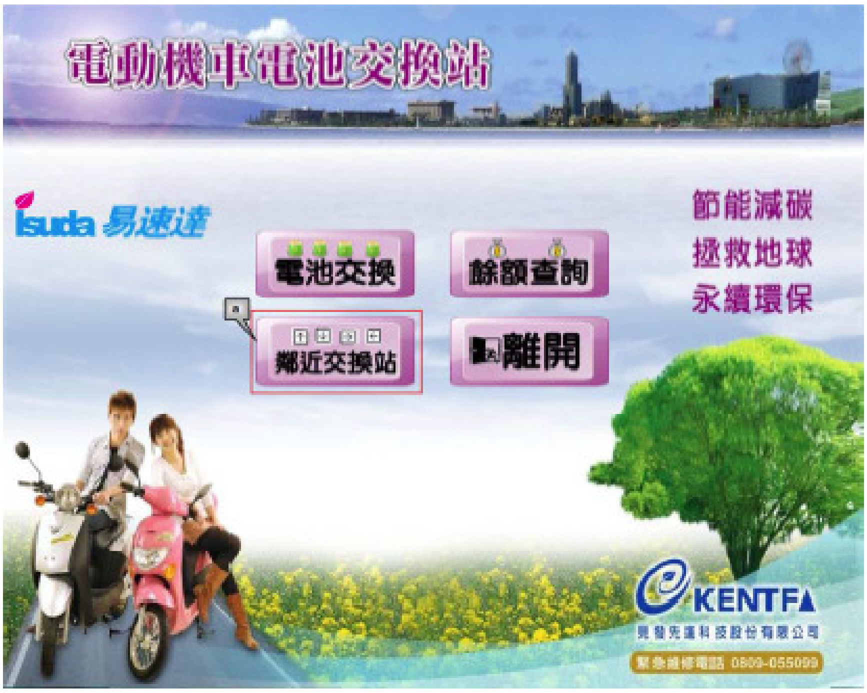


ii. 點選【回選單】回到系統功能選單，或點選【離開】回到主畫面

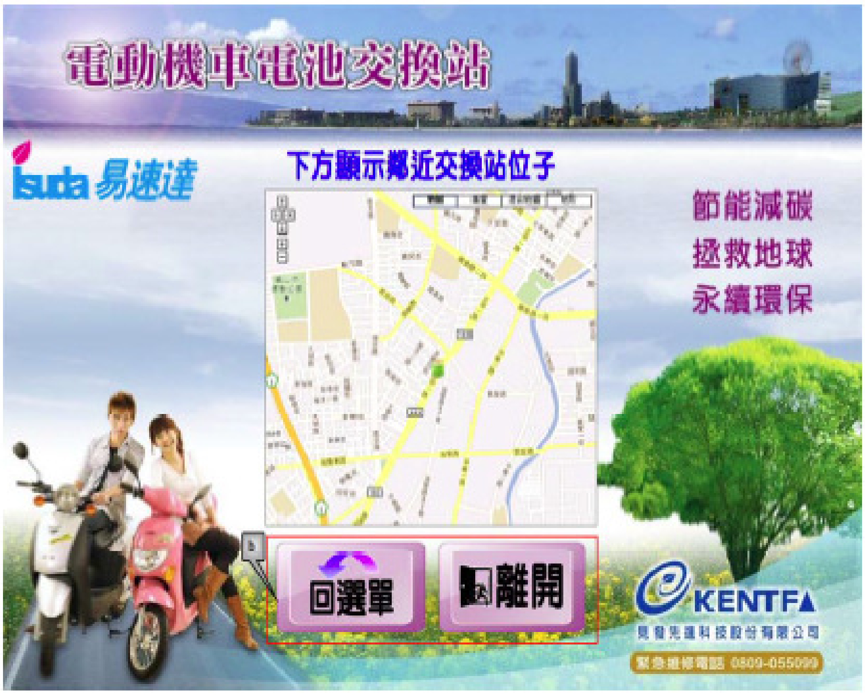

目前可用餘額： 0元

鄰近交換站：提供查詢本機交換站的地點鄰近交換站位置，查詢程序如下

i. 點選【鄰近交換站】按鈕，進入鄰近交換站查詢流程

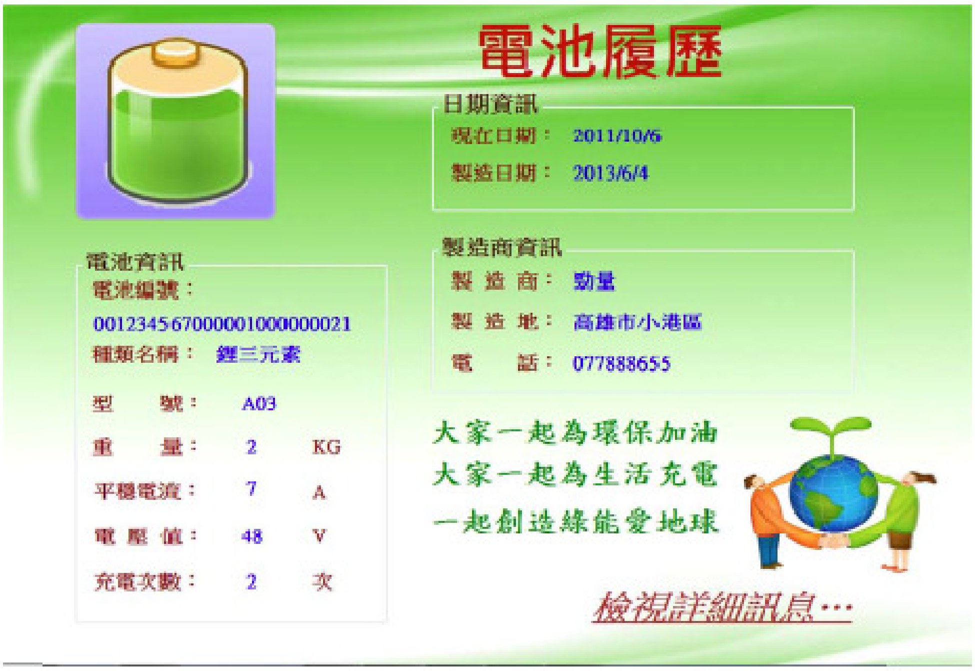


ii. 點選【回選單】回到系統功能選單，或點選【離開】回到主畫面



2. 電池履歷 KIOSK 系統操作說明

(1) 查詢簡易資料：將電池放上感應區後，系統會透過 ONS 向 EPCIS 查詢資料資料。



電池履歷

日期資訊

現在日期： 2011/10/6

製造日期： 2013/6/4

製造商資訊

製 造 商： 勁量

製 造 地： 高雄市小港區

電 話： 077888655

電池資訊

電池編號：

0012345670000001000000021

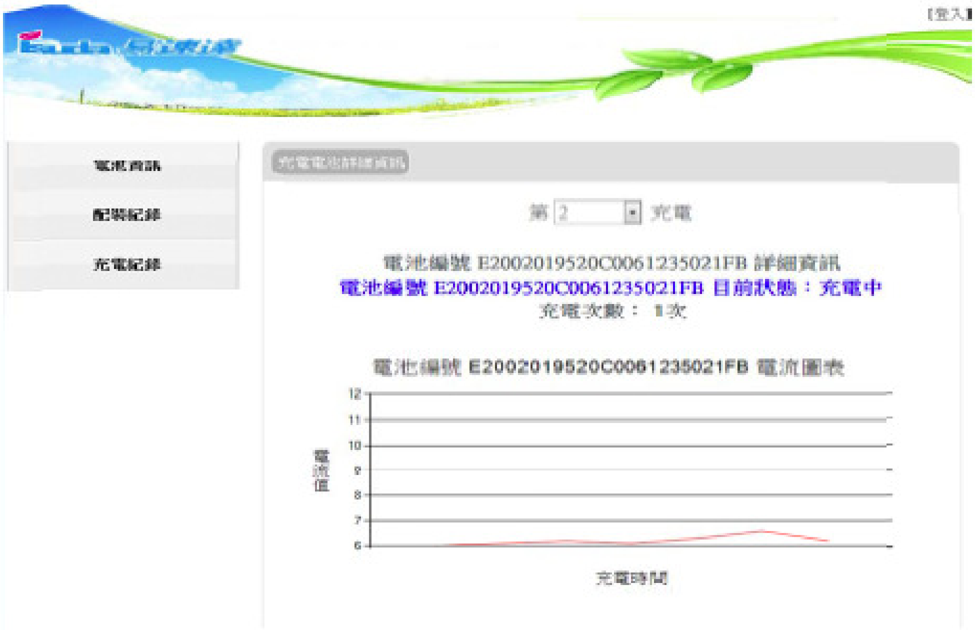
種類名稱： 鋰三元素

型 號：	A03	
重 量：	2	KG
平穩電流：	7	A
電 壓 值：	48	V
充電次數：	2	次

大家一起為環保加油
大家一起為生活充電
一起創造綠能愛地球

檢視詳細訊息…

(2) 查詢詳細資料：點選檢視詳細資訊後，系統會顯示該電池的專屬流通履歷網。



第 2 充電

電池編號 E2002019520C0061235021FB 詳細資訊

電池編號 E2002019520C0061235021FB 目前狀態：充電中

充電次數： 1次

電池編號 E2002019520C0061235021FB 電流圖表

3. 電池流通物聯網 ONS 登錄管理系統操作說明

(1) 公司碼管理

a. 填寫 EPC 編號、公司名稱。

b. 點選【新增 EPC 編碼】即可。

(2) EPC 電池紀錄管理

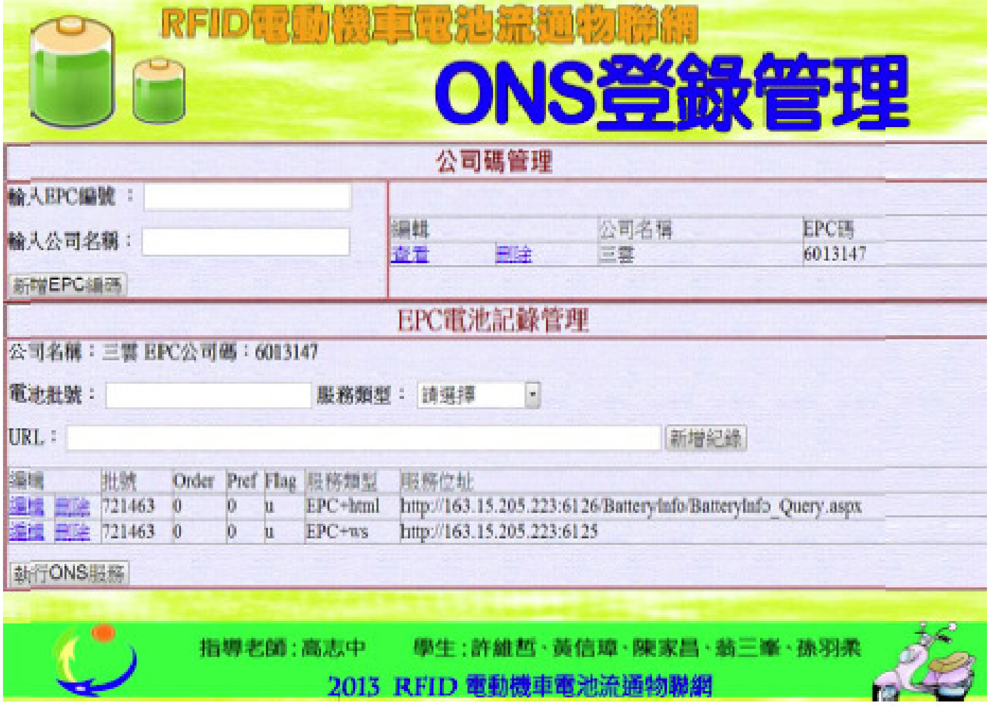
a. 填寫電池批號。

b. 選擇服務類型。

c. 填寫 URL 網址。

d. 點選【新增紀錄】即可。

e. 點選【執行 ONS 服務】即可。



公司碼管理

輸入EPC編號 ：

輸入公司名稱：

編輯		公司名稱	EPC碼
查看	刪除	三雲	6013147

EPC電池記錄管理

公司名稱：三雲 EPC公司碼：6013147

電池批號： 服務類型： 請選擇

URL：

編輯		批號	Order	Pref	Flag	服務類型	服務位址
編輯	刪除	721463	0	0	u	EPC+html	http://163.15.205.223:6126/BatteryInfo/BatteryInfo_Query.aspx
編輯	刪除	721463	0	0	u	EPC+ws	http://163.15.205.223:6125

指導老師：高志中　　學生：許維哲．黃信瑋．陳家昌．翁三峯．孫羽柔

2013 RFID 電動機車電池流通物聯網

4. 電池流通物聯網系統操作說明

(1) 系統管理（略，限於合作廠商保密協定）

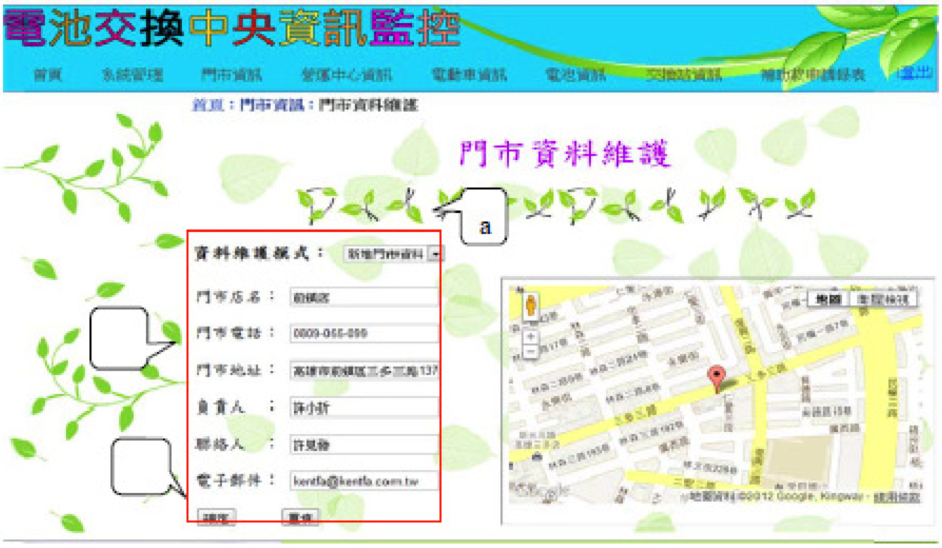
(2) 門市資訊

f. 門市資料維護操作步驟：

(a) 選擇資料維護模式。

(b) 填寫門市店名、門市電話、門市地址、負責人、連絡人、電子郵件。

(c) 點選【確定】即可。



首頁：門市資訊：門市資料維護

門市資料維護

資料維護模式：新增門市資料

門市店名：前鎮店

門市電話：0909-066-099

門市地址：高雄市前鎮區三多三路137

負責人　：許小祈

聯絡人　：許晃翰

電子郵件：kentfa@kentfa.com.tw

確定　重填

42

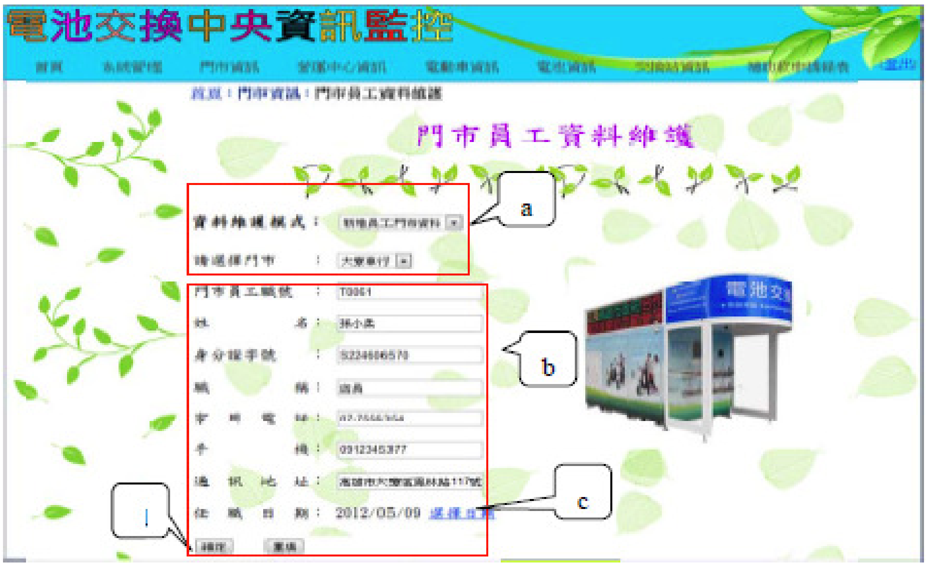
g. 門市員工資料維護操作步驟：

(a) 選擇資料維護模式、選擇門市。

(b) 填寫員工編號、姓名、身分證字號、職稱、家用電話、手機、通訊地址。

(c) 選擇任職日期: 按下【選擇日期】。

(d) 點選【確定】即可。



首頁：門市資訊：門市員工資料維護

門市員工資料維護

資料維護模式：新增員工門市資料

請選擇門市：大寮車行

門市員工職號：T0061

姓名：孫小柔

身分證字號：S224606570

職稱：店員

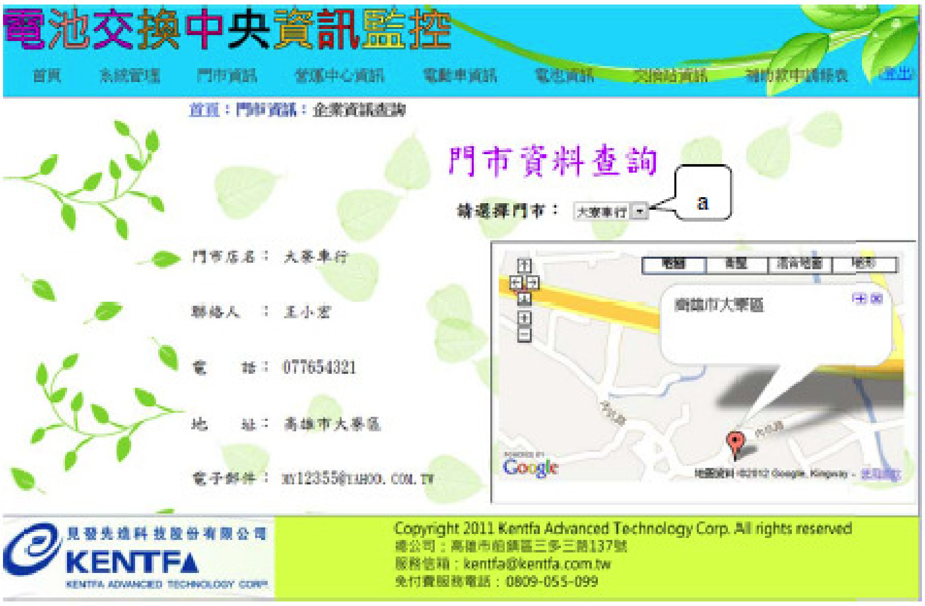
家用電話：07-7555554

手機：0912345377

通訊地址：高雄市大寮區鳳林路117號

任職日期：2012/05/09 選擇日期

h. 門市資料查詢操作步驟：選擇想查詢的門市即可。



首頁：門市資訊：企業資訊查詢

門市資料查詢

請選擇門市：大寮車行

門市店名：大寮車行

聯絡人：王小宏

電話：077654321

地址：高雄市大寮區

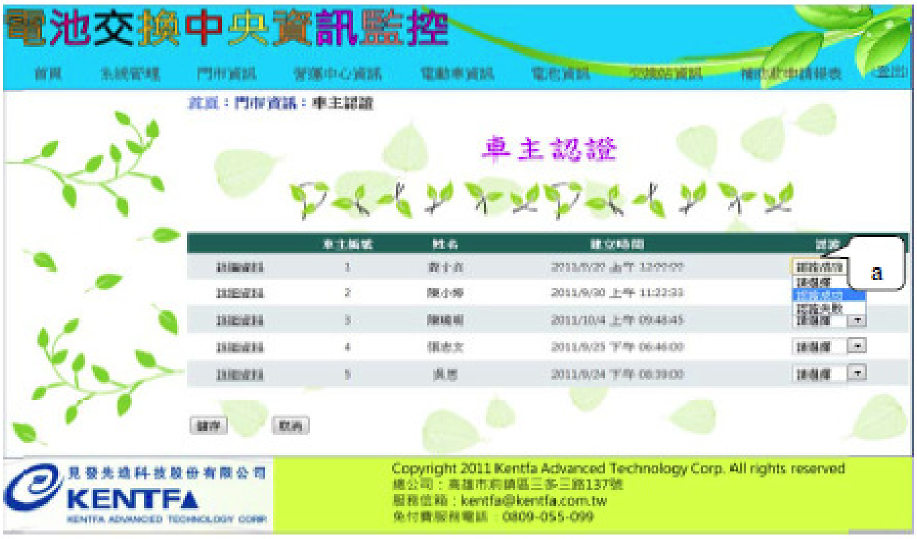
電子郵件：MY12355@YAHOO.COM.TW

Copyright 2011 Kentfa Advanced Technology Corp. All rights reserved
總公司：高雄市前鎮區三多三路137號
服務信箱：kentfa@kentfa.com.tw
免付費服務電話：0809-055-099

i. 車主認證操作步驟：

(a) 選擇車主認證成功或失敗。

(b) 按儲存及修改完成。



電池交換中央資訊監控

首頁：門市資訊：車主認證

車主認證

	車主編號	姓名	建立時間	認證
詳細資料	1	[illegible]	[illegible]	認證成功
詳細資料	2	陳小卿	2011/9/30 上午 11:22:33	請選擇 認證成功 認證失敗
詳細資料	3	陳曉明	2011/10/4 上午 09:48:45	請選擇
詳細資料	4	張志文	2011/9/25 下午 06:46:00	請選擇
詳細資料	5	吳思	2011/9/24 下午 08:39:00	請選擇

見發先進科技股份有限公司
KENTFA
KENTFA ADVANCED TECHNOLOGY CORP.

Copyright 2011 Kentfa Advanced Technology Corp. All rights reserved
總公司：高雄市前鎮區三多三路137號
服務信箱：kentfa@kentfa.com.tw
免付費服務電話：0809-055-099

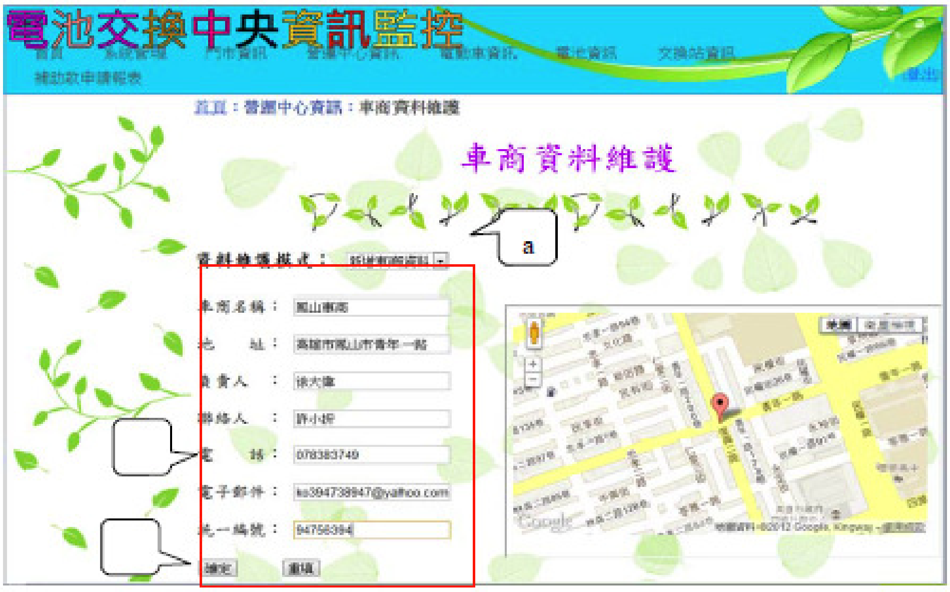
(3) 營運中心資訊

a. 車商資料維護操作步驟：

(a) 選擇資料維護模式。

(b) 填寫車商名稱、地址、負責人、聯絡人、電話、電子郵件、統一編號。

(c) 點選【確定】即可。



資料維護模式： 新增車商資料

車商名稱： 鳳山車商

地　　址： 高雄市鳳山市青年一路

負責人　： 徐大偉

聯絡人　： 許小昕

電　　話： 078383749

電子郵件： ks394738947@yahoo.com

統一編號： 94756394

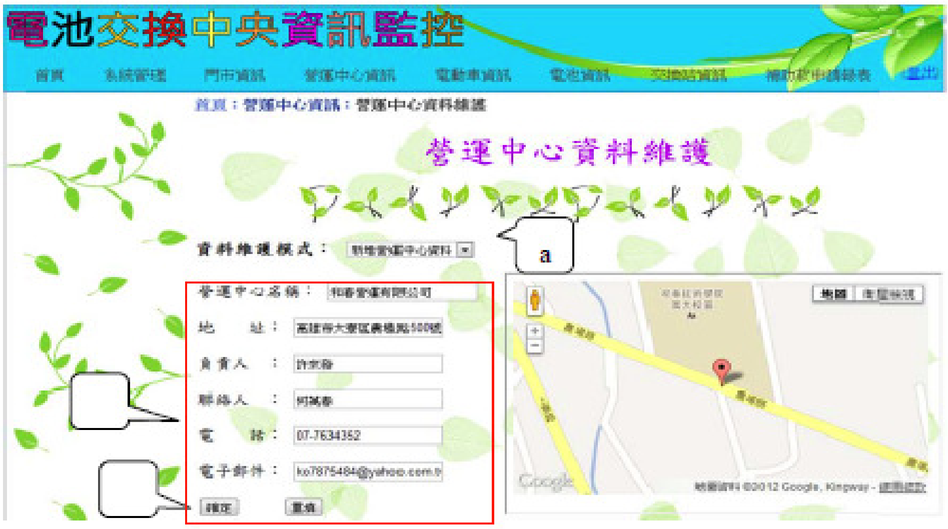
確定　重填

b. 營運中心資料維護操作步驟：

(a) 選擇資料維護模式。

(b) 填寫營運中心名稱、地址、負責人、聯絡人、電話、電子郵件。

(c) 點選【確定】即可。



資料維護模式： 新增營運中心資料

營運中心名稱： 和春營運有限公司

地　　址： 高雄市大寮區鳳林路500號

負責人　： 許家豪

聯絡人　： 柯某泰

電　　話： 07-7634352

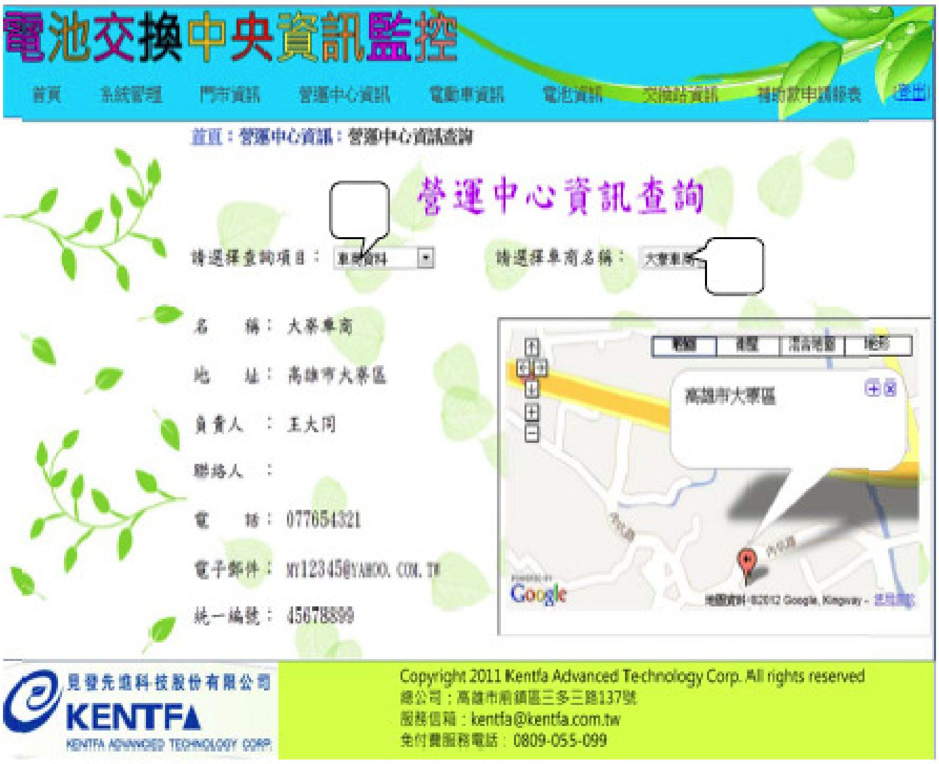
電子郵件： ko7875484@yahoo.com.tw

確定　重填

c. 營運中心資訊查詢操作步驟：

(a) 選擇想查詢的查詢項目。

(b) 再選擇車商名稱即可。



首頁：營運中心資訊：營運中心資訊查詢

營運中心資訊查詢

請選擇查詢項目：車商資料 請選擇車商名稱：大寮車商

名　　稱：大寮車商

地　　址：高雄市大寮區

負責人　：王大同

聯絡人　：

電　　話：077654321

電子郵件：MY12345@YAHOO.COM.TW

統一編號：45678899

晃發先進科技股份有限公司
KENTFA
KENTFA ADVANCED TECHNOLOGY CORP.

Copyright 2011 Kentfa Advanced Technology Corp. All rights reserved
總公司：高雄市前鎮區三多三路137號
服務信箱：kentfa@kentfa.com.tw
免付費服務電話：0809-055-099

(4) 電動車資訊

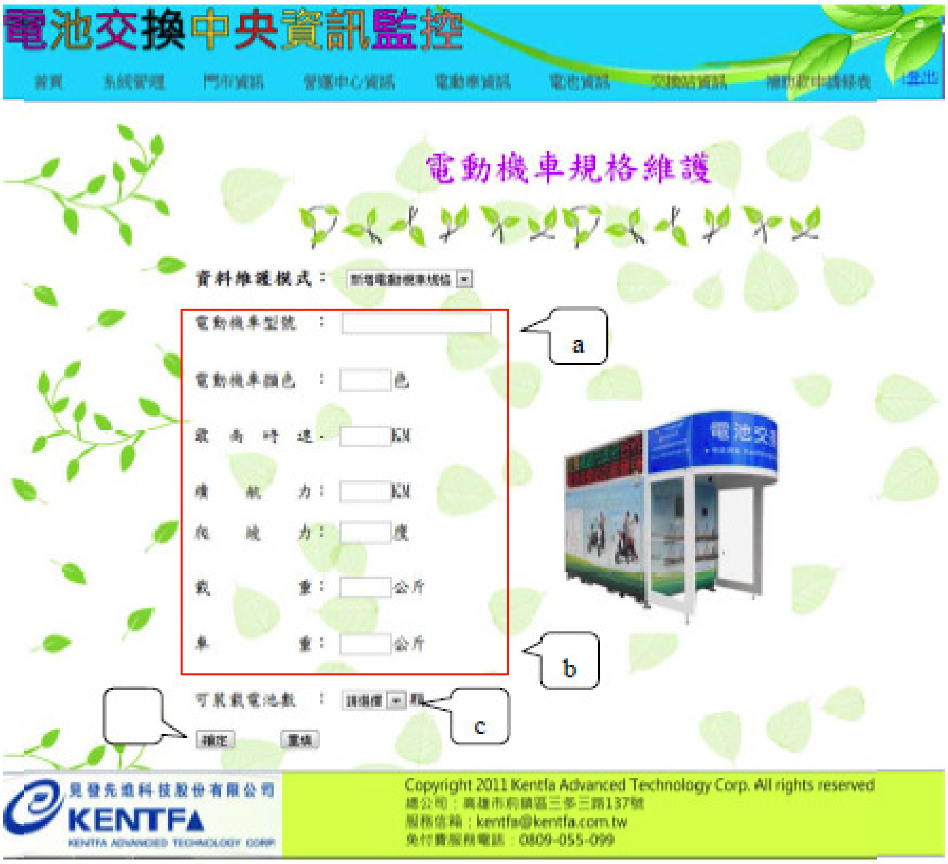
a. 電動機車規格維護操作步驟：

(a) 選擇資料維護模式。

(b) 填寫電動機車型號、電動機車顏色、最高時速、續航力、爬坡力、載重、車重。

(c) 選擇可裝載電池數: 選擇幾顆電池。

(d) 點選【確定】即可。



資料維護模式：新增電動機車規格

電動機車型號 ：

電動機車顏色 ： 色

最高時速： KM

續航力： KM

爬坡力： 度

載重： 公斤

車重： 公斤

可裝載電池數 ： 請選擇 顆

確定 重填

Copyright 2011 Kentfa Advanced Technology Corp. All rights reserved
總公司：高雄市前鎮區三多三路137號
服務信箱：kentfa@kentfa.com.tw
免付費服務電話：0809-055-099

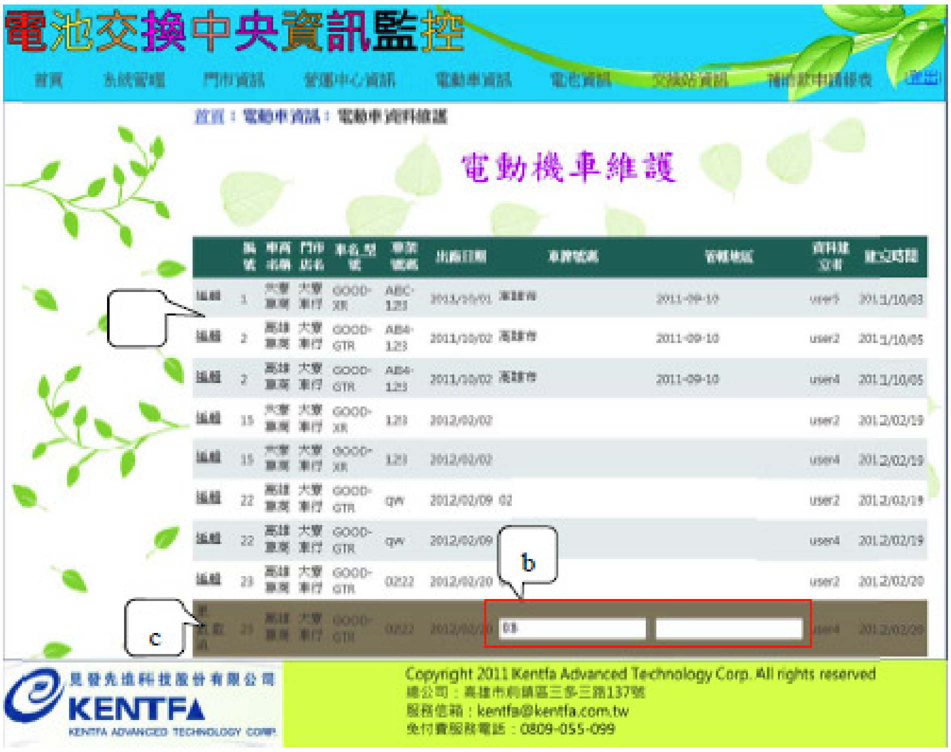
b. 電動車資料維護操作步驟：

(a) 可點選【編輯】。

(b) 填寫車牌號碼、管轄地區。

(c) 點選【更新】。

(d) 再點選【確定】即可。



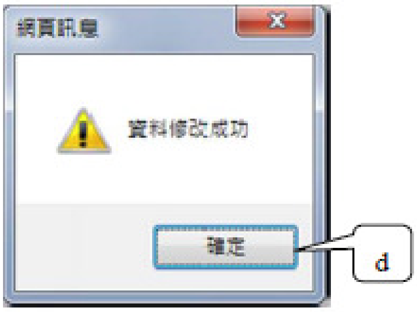
首頁：電動車資訊：電動車資料維護

電動機車維護

	編號	車商名稱	門市店名	車名型號	車架號碼	出廠日期	車牌號碼	管轄地區	資料建立者	建立時間
編輯	1	大豐車商	大豐車行	GOOD-XR	ABC-123	2011/10/01	高雄市	2011-09-10	user5	2011/10/03
編輯	2	高雄車商	大豐車行	GOOD-GTR	AB4-123	2011/10/02	高雄市	2011-09-10	user2	2011/10/05
編輯	2	高雄車商	大豐車行	GOOD-GTR	AB4-123	2011/10/02	高雄市	2011-09-10	user4	2011/10/05
編輯	15	大豐車商	大豐車行	GOOD-XR	123	2012/02/02			user2	2012/02/19
編輯	15	大豐車商	大豐車行	GOOD-XR	123	2012/02/02			user4	2012/02/19
編輯	22	高雄車商	大豐車行	GOOD-GTR	qw	2012/02/09	02		user2	2012/02/19
編輯	22	高雄車商	大豐車行	GOOD-GTR	qw	2012/02/09			user4	2012/02/19
編輯	23	高雄車商	大豐車行	GOOD-GTR	0222	2012/02/20			user2	2012/02/20
更新 取消	23	高雄車商	大豐車行	GOOD-GTR	0222	2012/02/20	03		user4	2012/02/20

見發先進科技股份有限公司
KENTFA
KENTFA ADVANCED TECHNOLOGY CORP.

Copyright 2011 Kentfa Advanced Technology Corp. All rights reserved
總公司：高雄市前鎮區三多三路137號
服務信箱：kentfa@kentfa.com.tw
免付費服務電話：0809-055-099

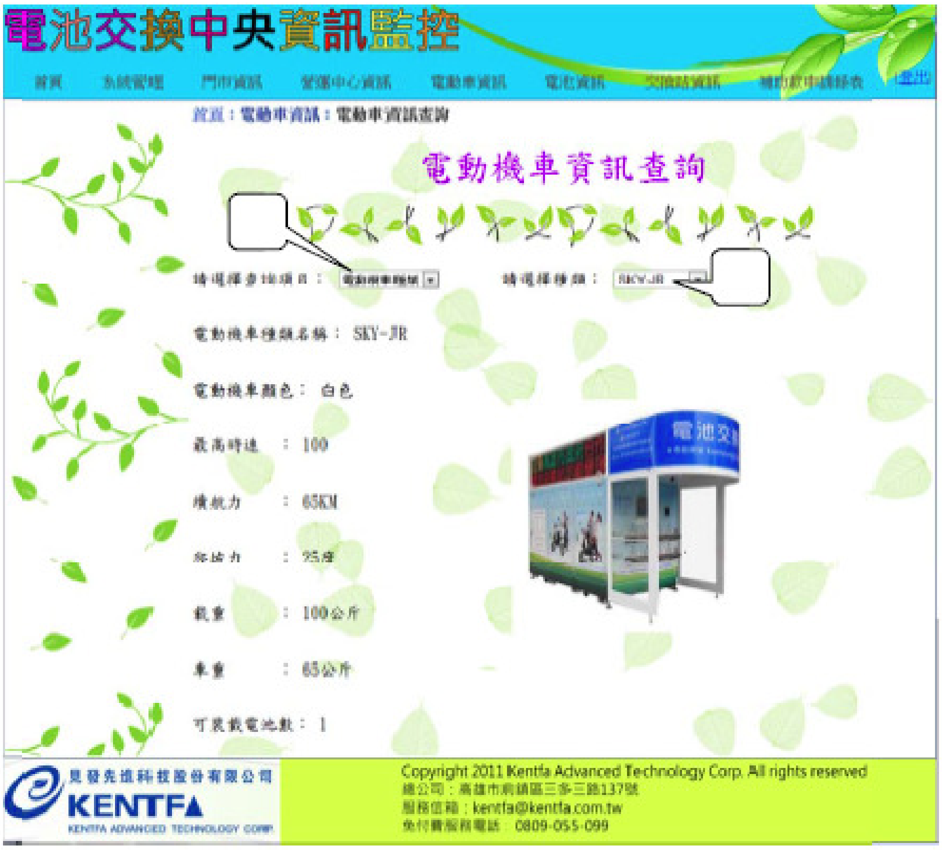


資料修改成功

c. 電動車資訊查詢操作步驟：

(a) 選擇想查詢的查詢項目。

(b) 再選擇種類即可。



首頁：電動車資訊：電動車資訊查詢

電動機車資訊查詢

請選擇查詢項目： 電動機車種類 ▾　　請選擇種類： SKY-JR ▾

電動機車種類名稱： SKY-JR

電動機車顏色： 白色

最高時速　： 100

續航力　： 65KM

爬坡力　： 25度

載重　： 100公斤

車重　： 65公斤

可裝載電池數： 1

崑發先進科技股份有限公司
KENTFA
KENTFA ADVANCED TECHNOLOGY CORP.

Copyright 2011 Kentfa Advanced Technology Corp. All rights reserved
總公司：高雄市前鎮區三多三路137號
服務信箱：kentfa@kentfa.com.tw
免付費服務電話：0809-055-099

49

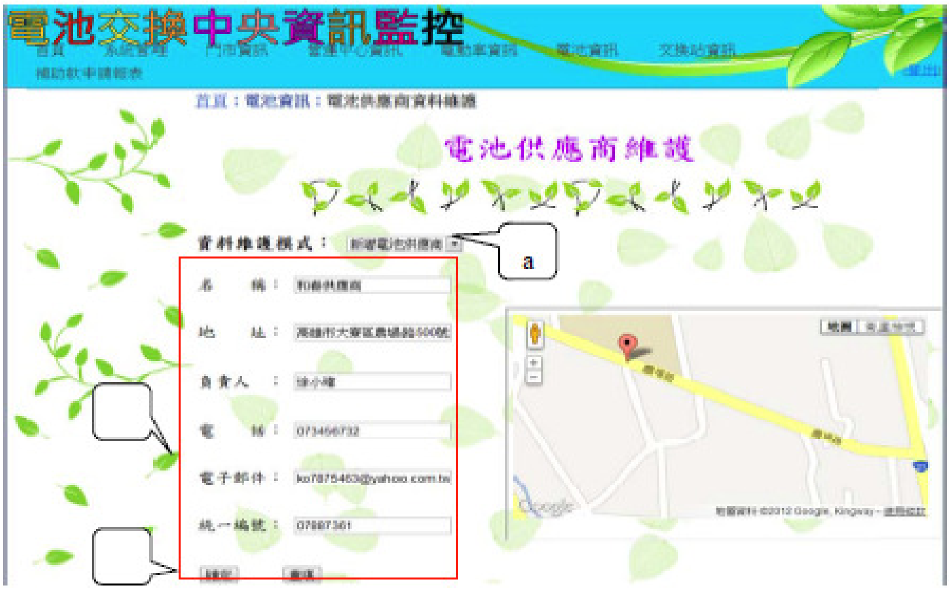
(5) 電池資訊

a. 電池供應商資料維護操作步驟：

(a) 選擇資料維護模式。

(b) 填寫名稱、地址、負責人、電話、電子郵件、統一編號。

(c) 點選【確定】即可。



電池交換中央資訊監控

首頁：電池資訊：電池供應商資料維護

電池供應商維護

資料維護模式： 新增電池供應商

名稱： 和春供應商

地址： 高雄市大寮區農場路500號

負責人： 徐小瑋

電話： 073456732

電子郵件： ko7875463@yahoo.com.tw

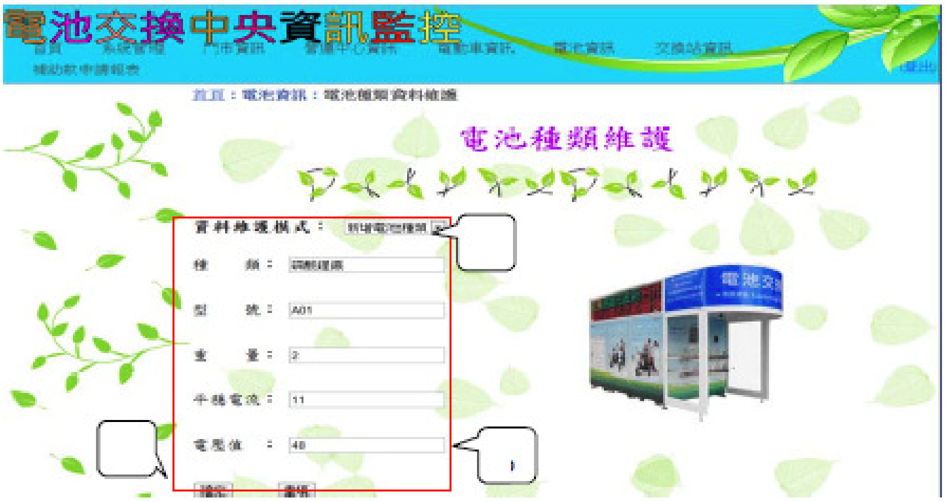
統一編號： 07887361

b. 電池種類維護操作步驟：

(a) 選擇資料維護模式。

(b) 填寫種類、型號、重量、平穩電流、電壓值。

(c) 點選【確定】即可。



電池交換中央資訊監控

首頁：電池資訊：電池種類資料維護

電池種類維護

資料維護模式： 新增電池種類

種類： 磷酸鋰鐵

型號： A01

重量： 2

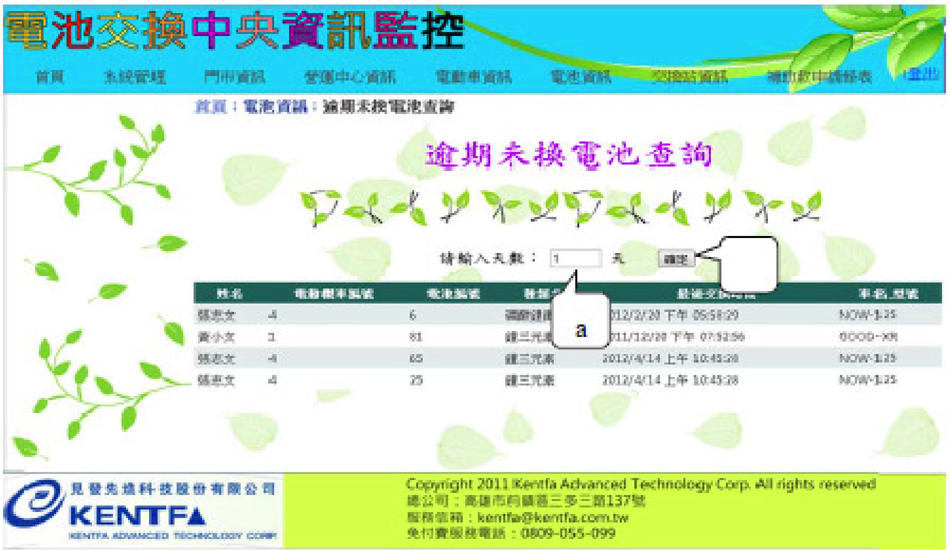
平穩電流： 11

電壓值 ： 48

c. 逾期未換電池查詢操作步驟：

(a) 輸入欲查詢【逾期未換電池】的天數。

(b) 點選【確定】即可。



首頁：電池資訊：逾期未換電池查詢

逾期未換電池查詢

請輸入天數： 1 天 確定

姓名	電動機車編號	電池編號	廠牌	最後交換時間	車名 型號
張志文	4	6	[illegible]	2012/2/20 下午 05:58:29	NOW-125
黃小文	3	81	鐘三元素	2011/12/20 下午 07:52:56	GOOD-XR
張志文	4	65	鐘三元素	2012/4/14 上午 10:45:20	NOW-125
張志文	4	25	鐘三元素	2012/4/14 上午 10:45:28	NOW-125

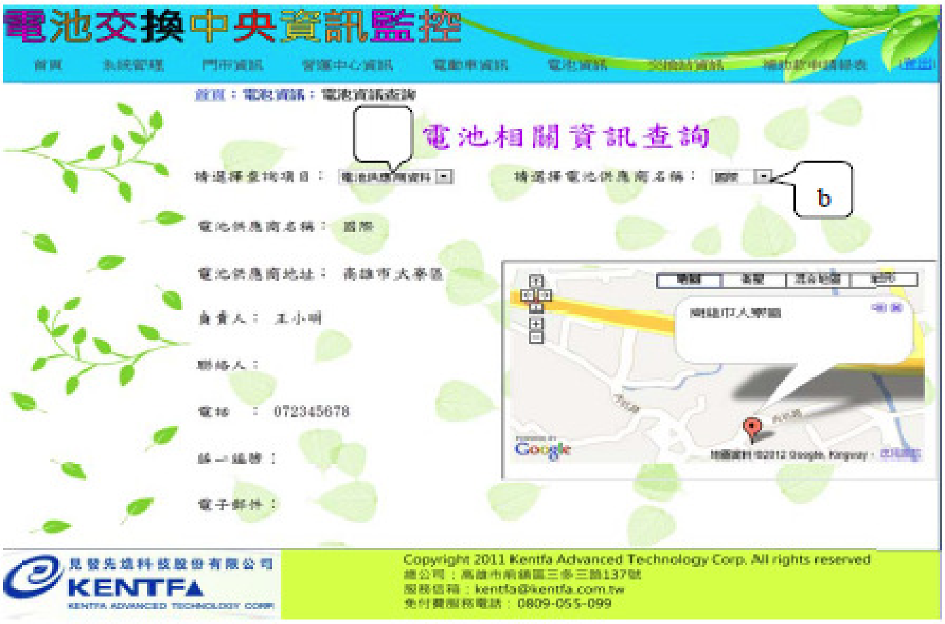
見發先進科技股份有限公司
KENTFA
KENTFA ADVANCED TECHNOLOGY CORP.

Copyright 2011 Kentfa Advanced Technology Corp. All rights reserved
總公司：高雄市前鎮區三多三路137號
服務信箱：kentfa@kentfa.com.tw
免付費服務電話：0809-055-099

d. 電池資訊查詢操作步驟：

(a) 選擇想查詢的查詢項目。

(b) 再選擇電池供應商名稱即可。



首頁：電池資訊：電池資訊查詢

電池相關資訊查詢

請選擇查詢項目： 電池供應商資料

請選擇電池供應商名稱： 國際

電池供應商名稱： 國際

電池供應商地址： 高雄市大寮區

負責人： 王小明

聯絡人：

電話 ： 072345678

統一編號：

電子郵件：

見發先進科技股份有限公司
KENTFA
KENTFA ADVANCED TECHNOLOGY CORP.

Copyright 2011 Kentfa Advanced Technology Corp. All rights reserved
總公司：高雄市前鎮區三多三路137號
服務信箱：kentfa@kentfa.com.tw
免付費服務電話：0809-055-099

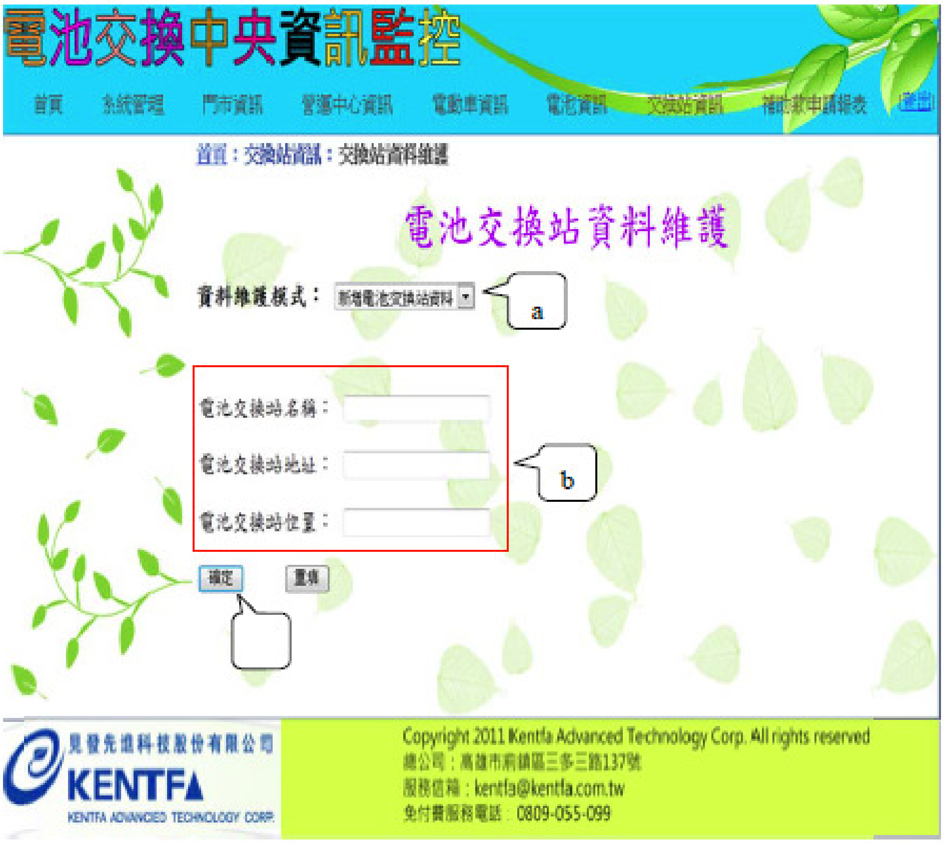
(6) 交換站資訊

a. 交換站資料維護操作步驟：

(a) 選擇資料維護模式。

(b) 填寫電池交換站名稱、電池交換站地址、電池交換站位置。

(c) 點選【確定】即可。



首頁：交換站資訊：交換站資料維護

電池交換站資料維護

資料維護模式： 新增電池交換站資料

電池交換站名稱：

電池交換站地址：

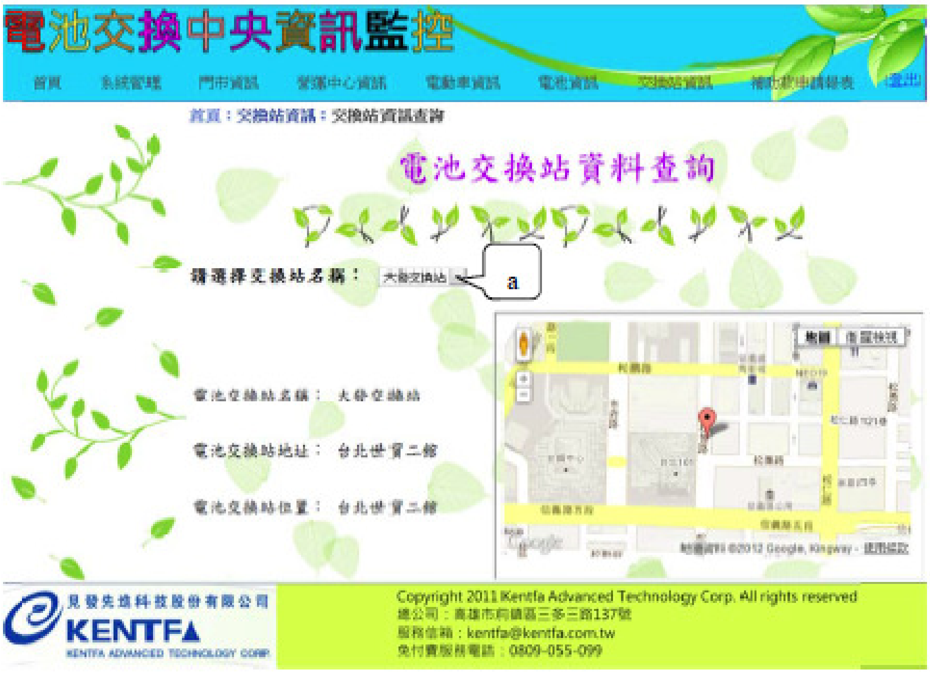
電池交換站位置：

見發先進科技股份有限公司
KENTFA
KENTFA ADVANCED TECHNOLOGY CORP.

Copyright 2011 Kentfa Advanced Technology Corp. All rights reserved
總公司：高雄市前鎮區三多三路137號
服務信箱：kentfa@kentfa.com.tw
免付費服務電話：0809-055-099

52

b. 交換站資料維護操作步驟：選擇想查詢的交換站名稱即可。



電池交換站資料查詢

請選擇交換站名稱： 大發交換站

電池交換站名稱： 大發交換站

電池交換站地址： 台北世貿二館

電池交換站位置： 台北世貿二館

Copyright 2011 Kentfa Advanced Technology Corp. All rights reserved
總公司：高雄市前鎮區三多三路137號
服務信箱：kentfa@kentfa.com.tw
免付費服務電話：0809-055-099

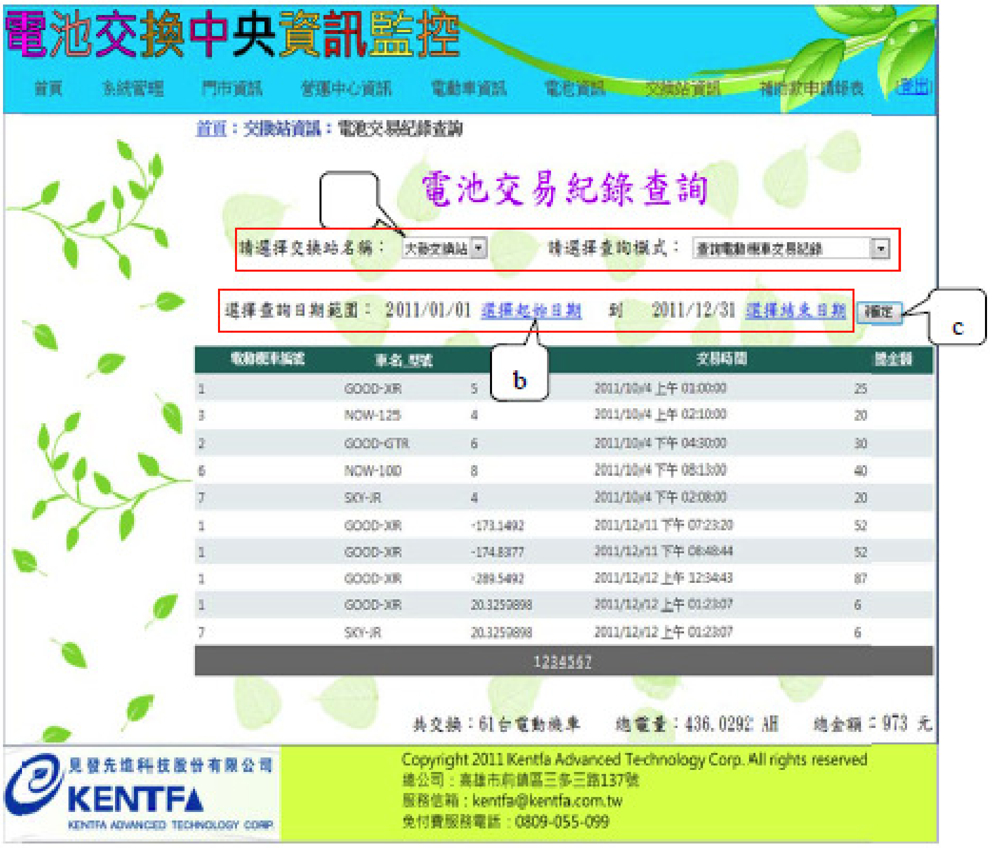
c. 充電電池資料查詢操作步驟（略，限於合作廠商保密協定）

d. 電池交易紀錄查詢操作步驟：

(a) 選擇交換站名稱、查詢模式。

(b) 選擇有效期限: 按下【選擇起始日期】和【選擇結束日期】。

(c) 點選【確定】即可。



首頁：交換站資訊：電池交易紀錄查詢

電池交易紀錄查詢

請選擇交換站名稱： 大發交換站　　請選擇查詢模式： 查詢電動機車交易紀錄

選擇查詢日期範圍： 2011/01/01 選擇起始日期　到　2011/12/31 選擇結束日期　確定

電動機車編號	車名_型號		交易時間	總金額
1	GOOD-XR	5	2011/10/4 上午 01:00:00	25
3	NOW-125	4	2011/10/4 上午 02:10:00	20
2	GOOD-GTR	6	2011/10/4 下午 04:30:00	30
6	NOW-100	8	2011/10/4 下午 08:13:00	40
7	SKY-JR	4	2011/10/4 下午 02:08:00	20
1	GOOD-XR	-173.1492	2011/12/11 下午 07:23:20	52
1	GOOD-XR	-174.8377	2011/12/11 下午 08:48:44	52
1	GOOD-XR	-289.5492	2011/12/12 上午 12:34:43	87
1	GOOD-XR	20.3250898	2011/12/12 上午 01:23:07	6
7	SKY-JR	20.3250898	2011/12/12 上午 01:23:07	6

1234567

共交換：61台電動機車　總電量：436.0292 AH　總金額：973 元

見發先進科技股份有限公司
KENTFA
KENTFA ADVANCED TECHNOLOGY CORP.

Copyright 2011 Kentfa Advanced Technology Corp. All rights reserved
總公司：高雄市前鎮區三多三路137號
服務信箱：kentfa@kentfa.com.tw
免付費服務電話：0809-055-099

54

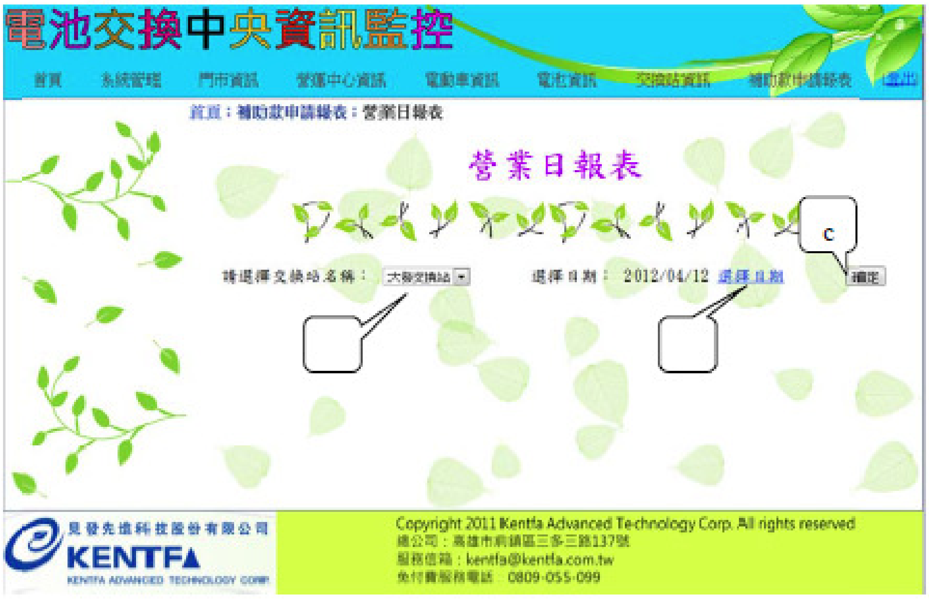
(7) 報表查詢及列印（略，限於合作廠商保密協定）

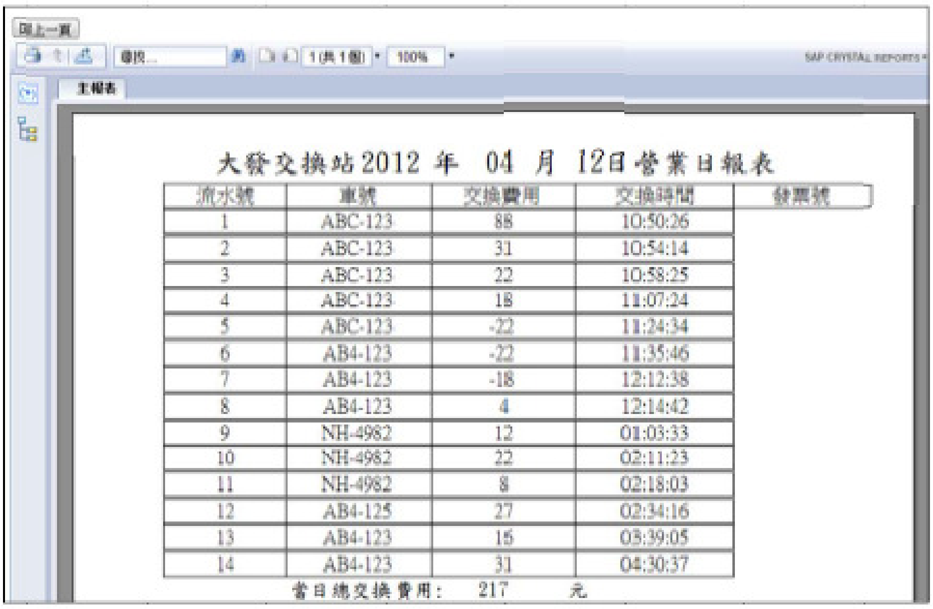
a. 營業日報表操作步驟：

(a) 選擇交換站名稱。

(b) 選擇日期: 按下【選擇日期】。

(c) 點選【確定】即可。


電池交換中央資訊監控
首頁
系統管理
門市資訊
營運中心資訊
電動車資訊
電池資訊
交換站資訊
補助款申請報表
登出
首頁：補助款申請報表：營業日報表
營業日報表
c
請選擇交換站名稱：
大發交換站
選擇日期：
2012/04/12
選擇日期
確定
見發先進科技股份有限公司
KENTFA
KENTFA ADVANCED TECHNOLOGY CORP.
Copyright 2011 Kentfa Advanced Technology Corp. All rights reserved
總公司：高雄市前鎮區三多三路137號
服務信箱：kentfa@kentfa.com.tw
免付費服務電話：0809-055-099



大發交換站2012 年 04 月 12日營業日報表

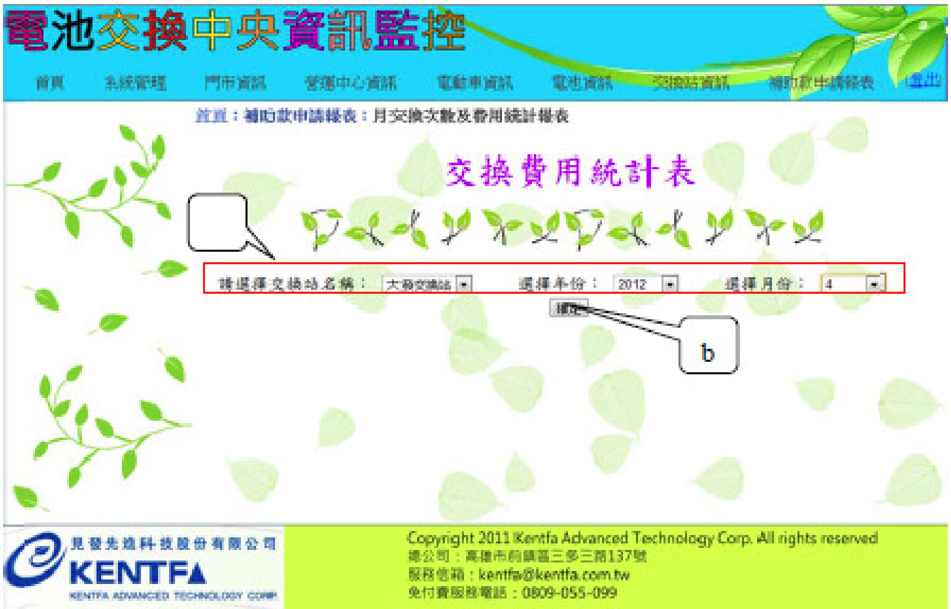
流水號	車號	交換費用	交換時間	發票號
1	ABC-123	88	10:50:26	
2	ABC-123	31	10:54:14	
3	ABC-123	22	10:58:25	
4	ABC-123	18	11:07:24	
5	ABC-123	-22	11:24:34	
6	AB4-123	-22	11:35:46	
7	AB4-123	-18	12:12:38	
8	AB4-123	4	12:14:42	
9	NH-4982	12	01:03:33	
10	NH-4982	22	02:11:23	
11	NH-4982	8	02:18:03	
12	AB4-125	27	02:34:16	
13	AB4-123	16	03:39:05	
14	AB4-123	31	04:30:37	

當日總交換費用: 217 元

b. 月交換次數及費用統計報表操作步驟：

(a) 選擇交換站名稱、年份、月份即可。

(b) 點選【確定】即可。

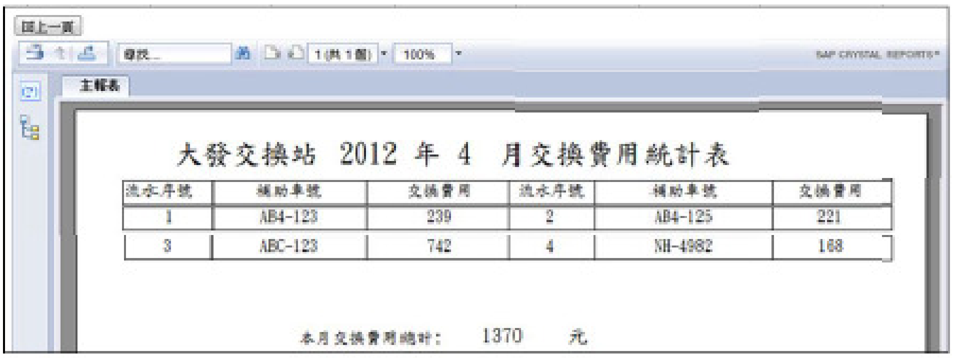


首頁：補助款申請報表：月交換次數及費用統計報表

交換費用統計表

請選擇交換站名稱： 大發交換站 選擇年份： 2012 選擇月份： 4

Copyright 2011 Kentfa Advanced Technology Corp. All rights reserved
總公司：高雄市前鎮區三多三路137號
服務信箱：kentfa@kentfa.com.tw
免付費服務電話：0809-055-099



大發交換站 2012 年 4 月交換費用統計表

流水序號	補助車號	交換費用	流水序號	補助車號	交換費用
1	AB4-123	239	2	AB4-125	221
3	ABC-123	742	4	NH-4982	168

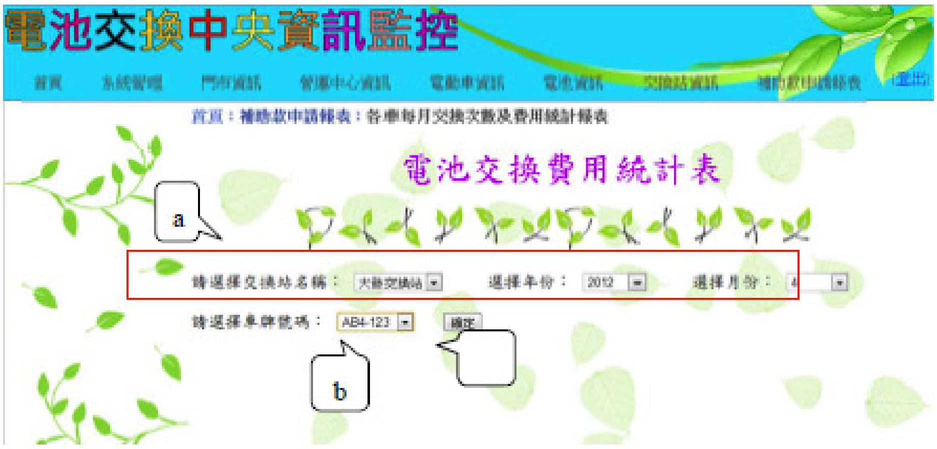
本月交換費用總計： 1370 元

c. 各車每月交換次數及費用統計報表操作步驟：

(a) 選擇交換站名稱、年份、月份即可。

(b) 再選擇車牌號碼。

(c) 點選【確定】即可。

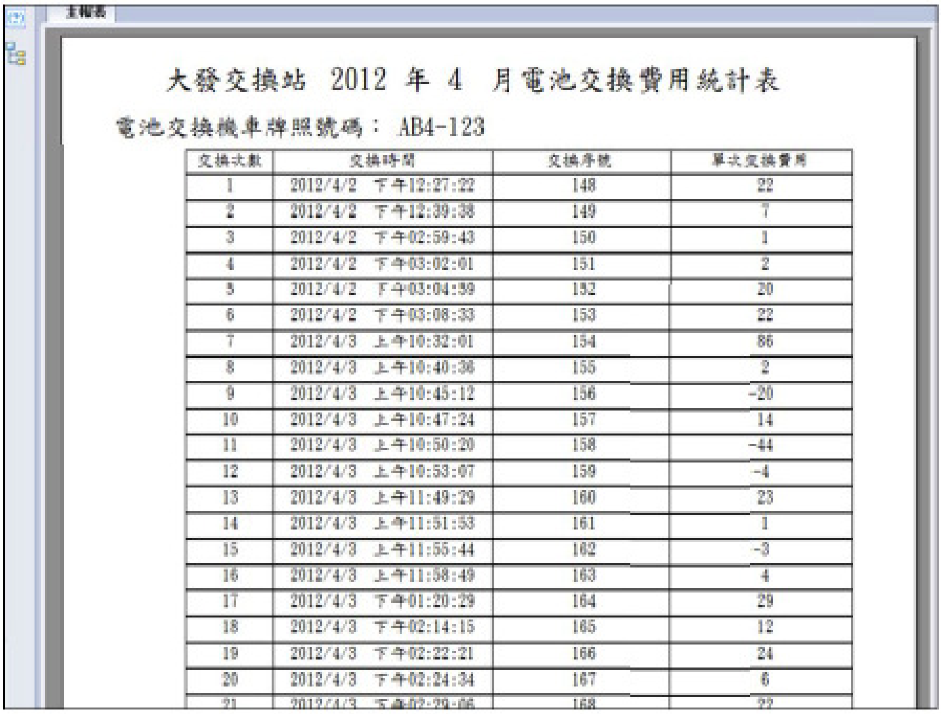


首頁：補助款申請報表：各車每月交換次數及費用統計報表

電池交換費用統計表

請選擇交換站名稱： 大發交換站　選擇年份： 2012　選擇月份： 4

請選擇車牌號碼： AB4-123



大發交換站 2012 年 4 月電池交換費用統計表

電池交換機車牌照號碼： AB4-123

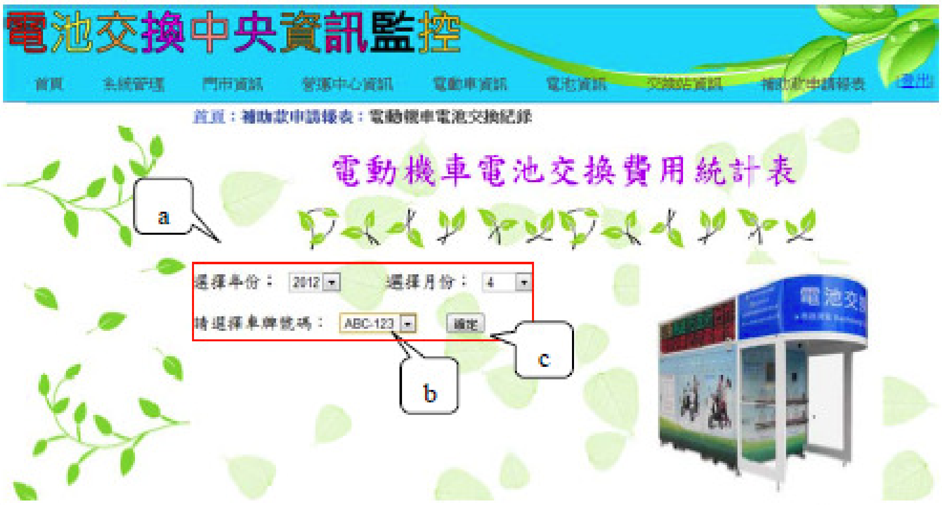
交換次數	交換時間	交換序號	單次交換費用
1	2012/4/2　下午12:27:22	148	22
2	2012/4/2　下午12:39:38	149	7
3	2012/4/2　下午02:59:43	150	1
4	2012/4/2　下午03:02:01	151	2
5	2012/4/2　下午03:04:59	152	20
6	2012/4/2　下午03:08:33	153	22
7	2012/4/3　上午10:32:01	154	86
8	2012/4/3　上午10:40:38	155	2
9	2012/4/3　上午10:45:12	156	-20
10	2012/4/3　上午10:47:24	157	14
11	2012/4/3　上午10:50:20	158	-44
12	2012/4/3　上午10:53:07	159	-4
13	2012/4/3　上午11:49:29	160	23
14	2012/4/3　上午11:51:53	161	1
15	2012/4/3　上午11:55:44	162	-3
16	2012/4/3　上午11:58:49	163	4
17	2012/4/3　下午01:20:29	164	29
18	2012/4/3　下午02:14:15	165	12
19	2012/4/3　下午02:22:21	166	24
20	2012/4/3　下午02:24:34	167	6
21	2012/4/3　下午02:29:06	168	22

d. 電動機車電池交換紀錄操作步驟：

(a) 選擇年份、月份。

(b) 再選擇車牌號碼。

(c) 點選【確定】即可。



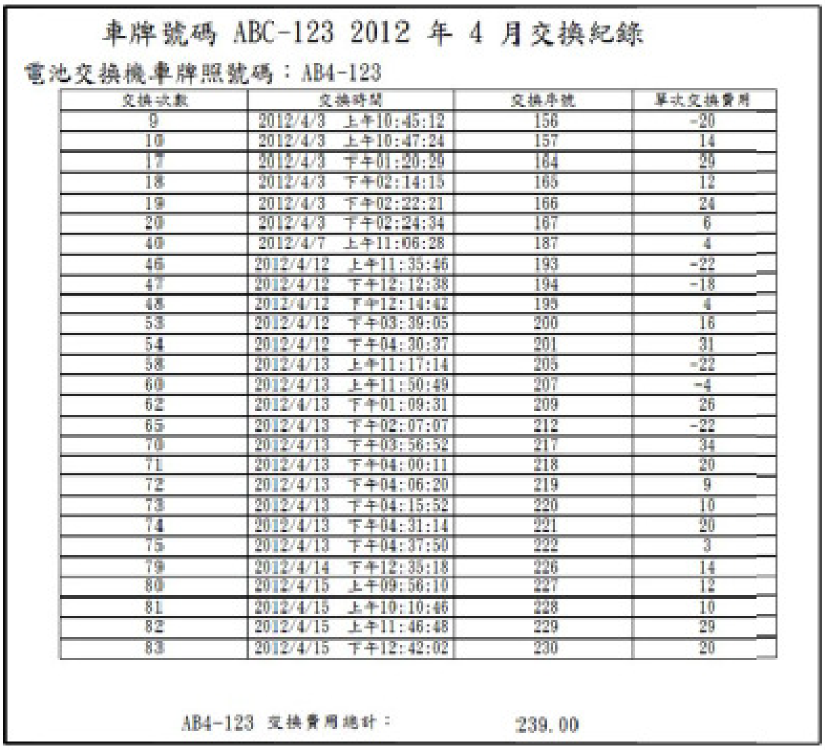
首頁：補助款申請報表：電動機車電池交換紀錄

電動機車電池交換費用統計表

選擇年份： 2012

選擇月份： 4

請選擇車牌號碼： ABC-123



車牌號碼 ABC-123 2012 年 4 月交換紀錄

電池交換機車牌照號碼：AB4-123

交換次數	交換時間	交換序號	單次交換費用
9	2012/4/3 上午10:45:12	156	-20
10	2012/4/3 上午10:47:24	157	14
17	2012/4/3 下午01:20:29	164	29
18	2012/4/3 下午02:14:15	165	12
19	2012/4/3 下午02:22:21	166	24
20	2012/4/3 下午02:24:34	167	6
40	2012/4/7 上午11:06:28	187	4
46	2012/4/12 上午11:35:46	193	-22
47	2012/4/12 下午12:12:38	194	-18
48	2012/4/12 下午12:14:42	195	4
53	2012/4/12 下午03:39:05	200	16
54	2012/4/12 下午04:30:37	201	31
58	2012/4/13 上午11:17:14	205	-22
60	2012/4/13 上午11:50:49	207	-4
62	2012/4/13 下午01:09:31	209	26
65	2012/4/13 下午02:07:07	212	-22
70	2012/4/13 下午03:56:52	217	34
71	2012/4/13 下午04:00:11	218	20
72	2012/4/13 下午04:06:20	219	9
73	2012/4/13 下午04:15:52	220	10
74	2012/4/13 下午04:31:14	221	20
75	2012/4/13 下午04:37:50	222	3
79	2012/4/14 下午12:35:18	226	14
80	2012/4/15 上午09:56:10	227	12
81	2012/4/15 上午10:10:46	228	10
82	2012/4/15 上午11:46:48	229	29
83	2012/4/15 下午12:42:02	230	20

AB4-123 交換費用總計： 239.00

六、結論

本專題所建立的「電動機車電池交換及流通物聯網系統」，可以讓民眾繳回沒有電的機車電池，並在一分鐘內送出飽充的電池。這套系統採用 RFID 標籤來辨識電池身分，以防止錯誤電池被放入充電基座上。另外，本系統使用悠遊卡儲值後，用於車主身分辨識與交換電池費的付費扣款。在電池流通管理方面，本系統採用了 EPCglobal 智慧型商務網路標準架構，利用 ONS 服務將電池 EPC 碼所表示的URN 解析為電池的資訊服務主機(EPCIS)的 IP 位置及 Web Service 描述文件檔名。使得在網際網路中任何電腦均能夠依據 URN 資訊，向 ONS 主機詢問該 URN 相對的 EPCIS 主機位址；進而讀取電池流通的履歷資訊。因此，「電池履歷 Kiosk」可以提供車主或營運中心追蹤電池從出廠之後的所有流通狀態。最後，「電池交換流通物聯網」則是提供了更完整的電池物流資運管理功能，包含電池資料查詢、交易資訊、履歷查詢、報表列印管理等功能。

「電動機車電池交換站」為我國行政院環保署大力推廣的節能減碳政策之一，目前環保署已經同意在高雄市設置 32 座交換站，提供民眾交換電池。未來見發科技將成立「電動機車電池交換營運中心」，服務民眾交換電池。因此，未來的就業市場上將需要大量 RFID 相關人力。其次，台南市、屏東縣、台北市、金門縣等政府單位也紛紛洽談設置「電動機車電池交換站」，未來將會釋放出更多的 RFID 相關就業機會。

七、參考文獻

[1]GS1, 2009. EPCglobal Standards Overview, http://www.epcglobalinc.org/standards.

[2]Martin Roche MD, Cindy Waters RN, Eileen Walsh RN, “Visibility Systems in Delivery of Orthopedic Care Enable Unprecedented Savings and Efficiencies,” U.S. Orthopedic Product News, May/June 2007.

[3]Bernard, P.A., 1985. "Cycle Counting:The Missing Link, " Production and Inven-tory Management, Fourth Quarter, Vol. 26. Iss, 4. pp. 27-42。

[4]Bonney, M., 1994. "Trends in Inventory Management, " International Journal of Pro-duction Economics, Jun., pp. 107-114。

[5]Boss, Richard W., 2003. "RFID Technology for Libraries, "Library Technology Re-ports Nov/Dec. pp.6-64。

[6]Ernst, R., Guerrero, J. and Roshwalb, A., 1992. "Maintaining Inventory SystemAccuracy, "International Journal of Purchasing and Management, Summer, pp. 33-37。

[7]陳欣得、陳君杰(1999)電動機車研發與推廣之社會經濟效益分析與評估。八十八年度國科會/環保署科技合作研究計畫結報/靜宜大學企業管理系。

[8]中華民國環境保護學會學刊，第二十九卷第一期，民國九十五年六月

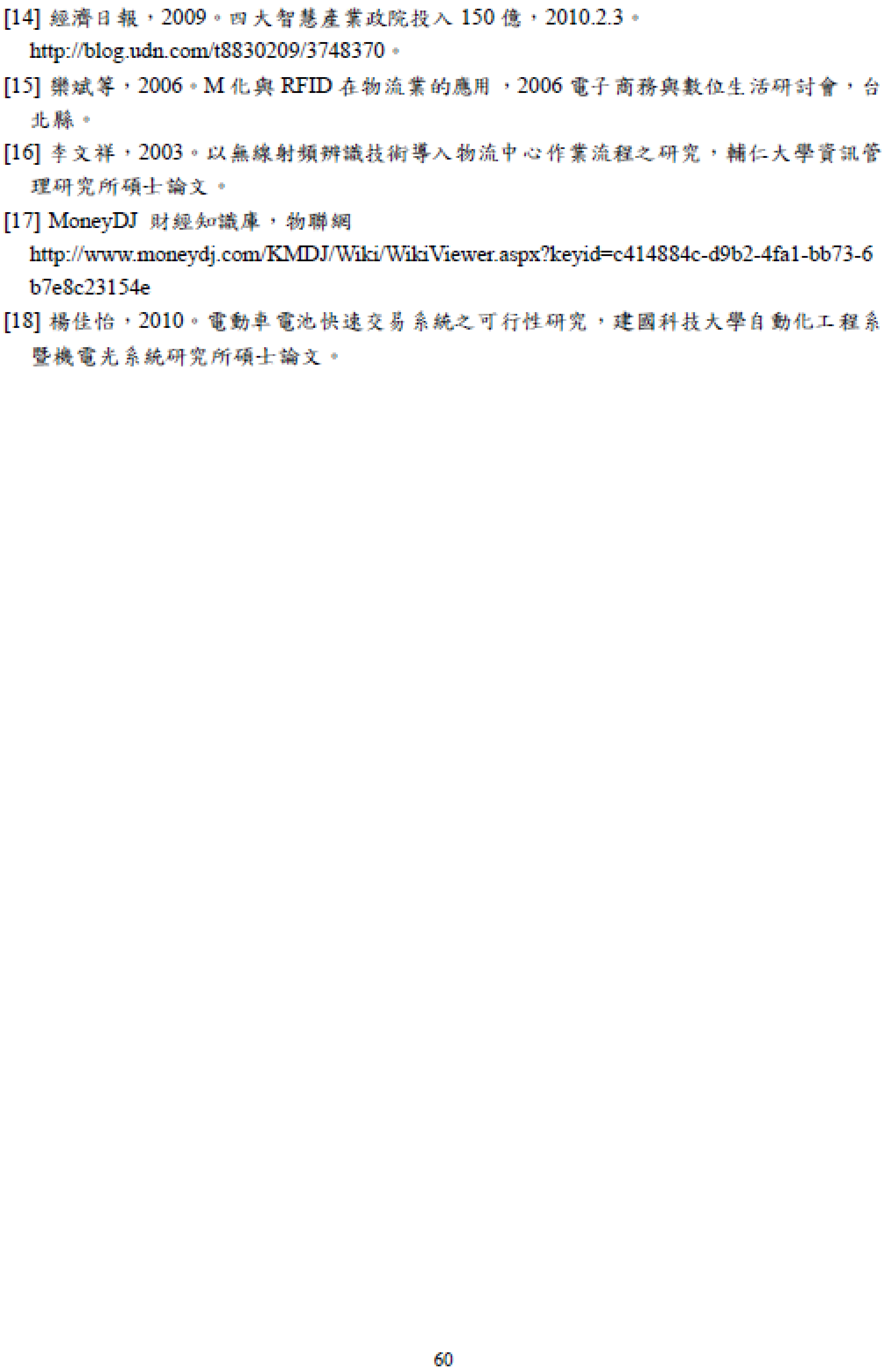
[9]陳宏宇，RFID 系統入門－無線射頻辨識系統，文魁資訊股份有限公司，2004。

[10] 日經 BP RFID 技術編輯部，RFID 技術與應用 ，旗標出版股份有限公司，2004。

[11] 鄭同伯，RFID EPC 無線射頻辨識完全剖析，博碩文化股份有限公司，2006。

[12] 高志中 ，2009。RFID 資訊應用系統之設計實務，博碩文化股份有限公司。

[13] 中華民國消費者文教基金會，http://www.consumers.org.tw/。



[14] 經濟日報，2009。四大智慧產業政院投入 150 億，2010.2.3。
http://blog.udn.com/t8830209/3748370。

[15] 樂斌等，2006。M 化與 RFID 在物流業的應用 ，2006 電子商務與數位生活研討會，台北縣。

[16] 李文祥，2003。以無線射頻辨識技術導入物流中心作業流程之研究，輔仁大學資訊管理研究所碩士論文。

[17] MoneyDJ 財經知識庫，物聯網
http://www.moneydj.com/KMDJ/Wiki/WikiViewer.aspx?keyid=c414884c-d9b2-4fa1-bb73-6b7e8c23154e

[18] 楊佳怡，2010。電動車電池快速交易系統之可行性研究，建國科技大學自動化工程系暨機電光系統研究所碩士論文。

Best Research Award
最佳研究大獎

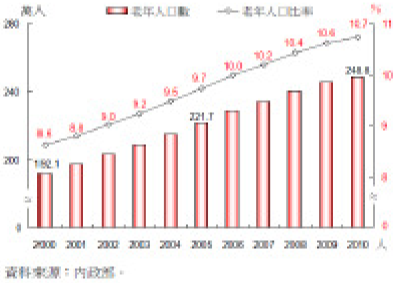
Project title項目名稱: 智慧型老人生理狀態與身體姿態回報系統
Students學生: 洪健峰、郭峰誌、林輝龍
Institution 院校: 樹德科技大學 電腦與通訊系
Supervisors指導: 施順鵬教授

一、 前言

在本作品中，將建置一個智慧老人照護之手機通報系統。利用ZigBee短距離無線通訊的特性，建立一個無線感測網路，在終端節點(End Devices)上結合三軸加速度感測器(ADXL345)，將此節點安裝在使用者身上適當位置，並利用CC2530晶片取得之三軸動作資料，傳回協調器(Coordinator)後，透過UART串列傳輸介面輸入電腦做運算。其中以類神經網路做為人體姿態辨識系統的核心演算法，利用姿態辨別方式，躺、坐、行走以及跌倒，將具有三軸加速度的感應器穿戴到該老人身上，如發生跌倒時會立即將資料回傳給子女或照護人。系統中並加入包含具人體溫度感測的主動式RFID標籤，與血壓、脈搏感測模組，可由系統得知照護中的老人生理狀況，如有溫度升高的現象，也可利用主動式RFID標籤回傳之RSSI做有發燒老人的區域管控，即時掌握老人的健康，以達成智慧型老人生理狀態與身體姿態回報系統之目的。

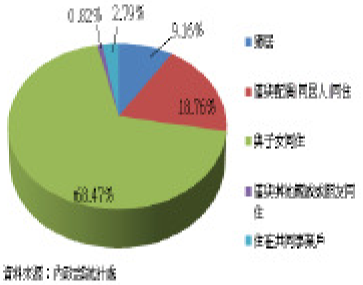
二、 研究目的

隨著科技與醫療的發達，讓多數人都享受到科技與醫療的資源，因高齡化及少子化的影響，獨居老人、安養院…問題已日漸嚴重，而且年輕人多半需至外地工作，導致年齡較高的長輩獨自在家中或需送至安養院照顧，所以無法時常陪在身邊照顧他們，生活起居未受關注，所以我們構想需要受到照顧的老人可佩戴此感測器。本作品同時應用溫度、血壓、脈搏量測的功能，結合主動式 RFID 標籤回傳之 RSSI，管控有發燒的老人在固定區域，老人可於每日定時量測，系統自動將數值傳送至電腦判斷，一旦系統感測到異常數值，將判斷結果透過簡訊功能傳送至子女或照護人的手機，讓監護人可以立即得知，另外，老人外出時，會自動開啟 GPS 定位的功能，盡可能在第一時間做出應變措施。



資料來源：內政部。

圖2-1、老年人口比率(單位:萬人)



資料來源：內政部統計處

圖2-2、2010老人居住分配圖

1

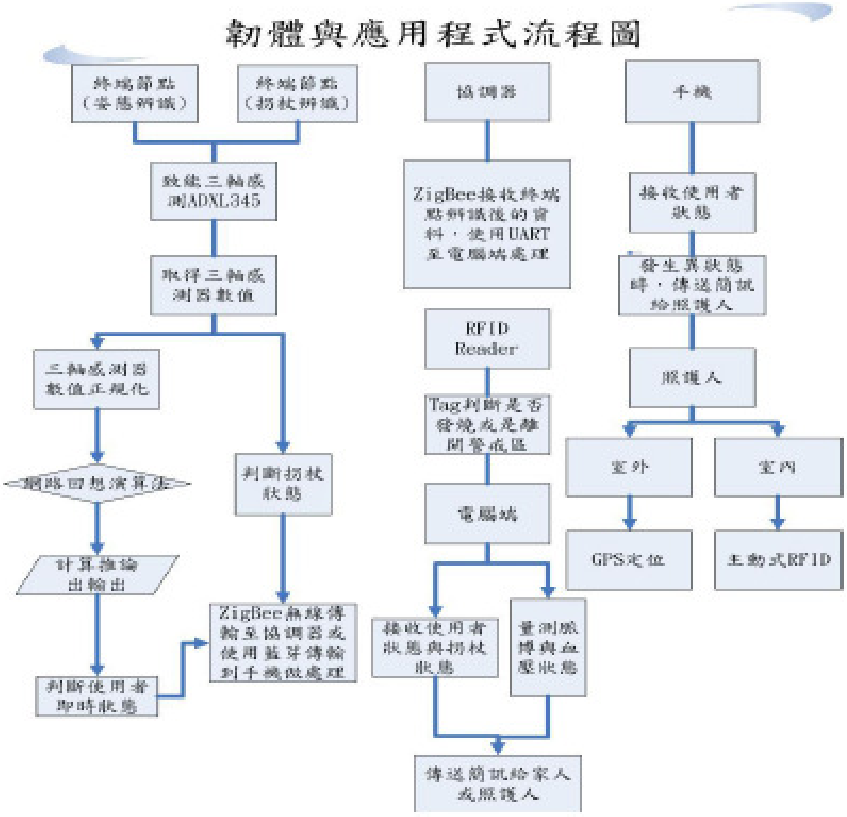


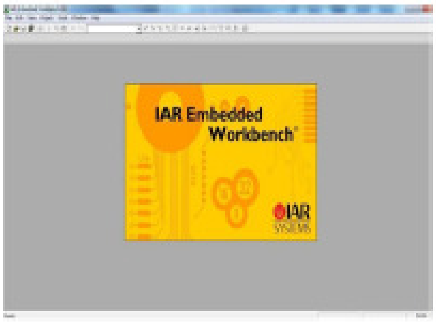
圖2-3、韌體與應用程式流程圖

本系統所使用技術主體架構為ZigBee和主動式RFID，上述技術應用越來越廣泛，已有許多關於ZigBee和主動式RFID的應用，例如：電子收費ETC、無人圖書館管理、商業大樓自動控制、家庭自動化控制這方面的應用，代表所用技術發展成熟且價格漸漸被接受，故為本系統創意應用之技術。

三、 文獻探討

✧ IAR 介紹

如圖 3-1 韌體程式以「IAR for MCS-51」撰寫而成，使用的語言為 C 語言。程式分成二個部分，第一部分是 ZigBee 終端節點的部分，如圖 3-2 所示，此部分的程式為讀取 ADXL345 的三軸資料為主，透過 CC2530 的輸出腳，輸出時脈與控制訊號給 ADXL345 的輸入腳，而 ADXL345 的輸出腳則負責送出三軸資料給 CC2530 的輸入腳，再由 CC2530 負責將收到的資料以 RF 的方式傳送出，在 ZigBee 終端節點裡必須設置所要傳送之目標位置的網路位址參數，這樣才能將資料正確的傳送出去。



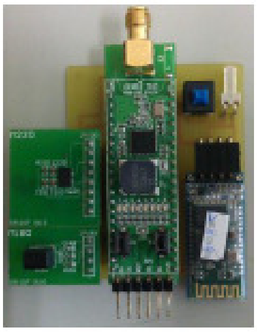


圖 3-1 開發韌體之 IAR 軟體介面　　圖 3-2、ZigBee 之三軸加速度感測器節點

✧ Zigbee 無線通訊部分：

隨著無線通訊、電池技術及嵌入式微處理技術的迅速進步，微小的電子裝置可以內嵌精密感測、計算及通訊等多樣化的功能，帶動了無線感測網路(Wireless Sensor Networks，WSN)的發展，如圖 3-3 所示，無線感測網路是由許多的感測節點(Sensor Node)所組成，負責監控並蒐集生活環境相關的資料。只要是使用無線通訊，包刮兩個以上的節點(Node)，每個節點配合一至多個感測器，都可以廣義的被歸納在屬於「無線感測網路」的範圍內。

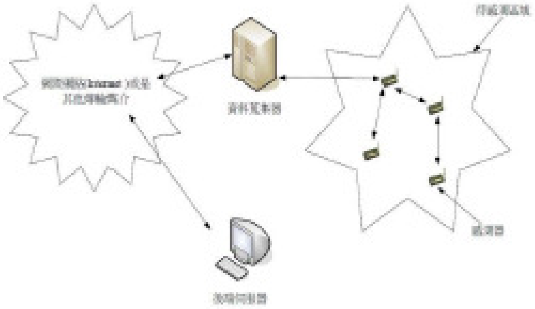


圖3-3、無線感測網路

✧ 主動式 RFID:

RFID 是「Radio Frequency Identification」的縮寫，中文可以稱為「無線射頻識別系統」。由感應器(Reader)和 RFID 標籤(Tag)組成，主動式的標籤內有電池，可以主動傳送訊號供感應器讀取、訊號傳送範圍也會比被動式廣，原理是利用感應器發射無線電波，觸動感應範圍內的 RFID 標籤，藉由電磁感應產生電流，供 RFID 標籤上的晶片運作並發出電磁波回應感應器。參考如圖 3-4。

3

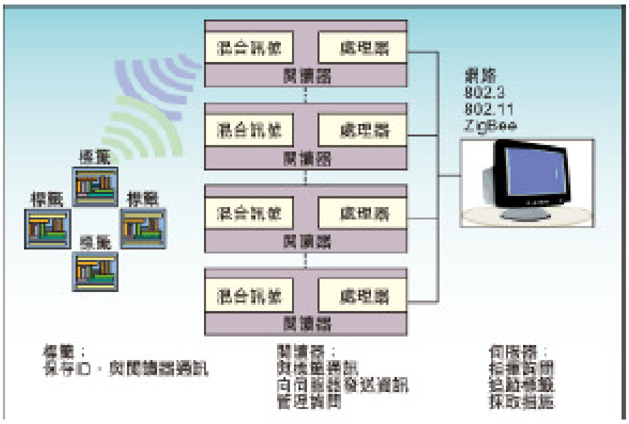


圖 3-4 主動式 RFID 架構

✧ 藍芽傳輸技術

圖 3-5、藍牙標誌

➢ 藍芽應用

1. 行動電話和免提裝置之間的無線通訊，這也是最初流行的應用 。
2. 特定距離內電腦間的無線網路。
3. 電腦與外設的無線連線，如：滑鼠、耳麥、印表機等。
4. 藍牙裝置之間的檔案傳輸。
5. 傳統有線裝置的無線化，如：醫用器材、GPS、條形碼掃描器、交管裝置。
6. 數個乙太網之間的無線橋架 。
7. 7 代家用遊戲機的手柄，PS3、PSP Go、Nitendo Wii
8. 依靠藍牙支援，使 PC 或PDA能透過手機的數據機實作撥號上網。
9. 即時定位系統(RTLS)，應用"節點"或"標籤"嵌入被跟蹤物品中讀卡器從標籤接收並處理無線訊號以確定物品位置。

✧ **App Inventor**

App Inventor 原是 Google 實驗室（Google Lab）的一個子計畫， Google App Inventor 是一個完全線上開發的 Android 程式環境，拋棄複雜的程式碼而使用樂高積木式的堆疊法來完成您的 Android 程式。除此它也支援樂高 NXT 機器人，對於 Android 初學者或是機器人開發者來說是一大福音。對於手機控制機器

4

人的使用者而言，不需要太華麗的介面，只要使用基本元件例如按鈕、文字輸入輸出即可。

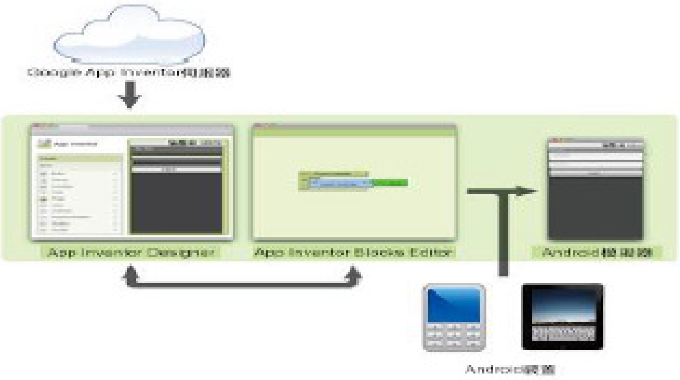
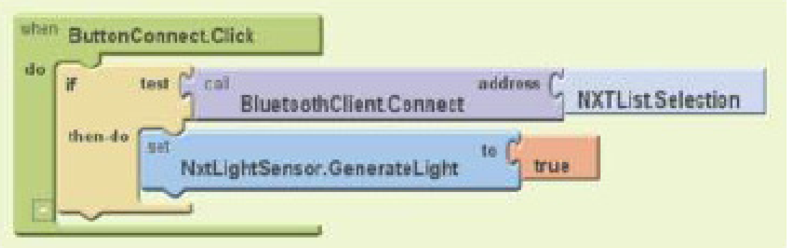


圖 3-6、App Inventor 工作架構圖

開發一個 App Inventor 程式就從您的網路瀏覽器開始，首先要設計程式的外觀。接著是設定程式的行為。最後只要將手機與電腦連線，程式就會顯示在手機上。



```
when ButtonConnect.Click
do
  if test call BluetoothClient.Connect address NXTList.Selection
  then-do set NxtLightSensor.GenerateLight to true
```

圖 3-7、App Inventor 程式編輯圖

App Inventor 讓您可在網路瀏覽器上來開發 Android 手機應用程式，App Inventor 仍持續開發與更新，並不定期推出新的元件，完成的程式可下載到實體手機或在模擬器上執行。App Inventor 伺服器會儲存您的工作進度還會協助您管理專案進度。

四、研究方法

圖 4-1 為本作品系統架構圖，用來作資料擷取與傳送的 ZigBee 是採用 Texas Instruments 公司所提供的 CC2530 的系統晶片，擁有低成本及低功耗之特性。主動式 RFID 模組為頻率 2.45G 的無線射頻設備，用於人員管制與溫度感測；作品軟體之 API 以 VB.NET 撰寫完成，晶片以 IAR 開發軟體編譯 C 語言並線上燒錄。

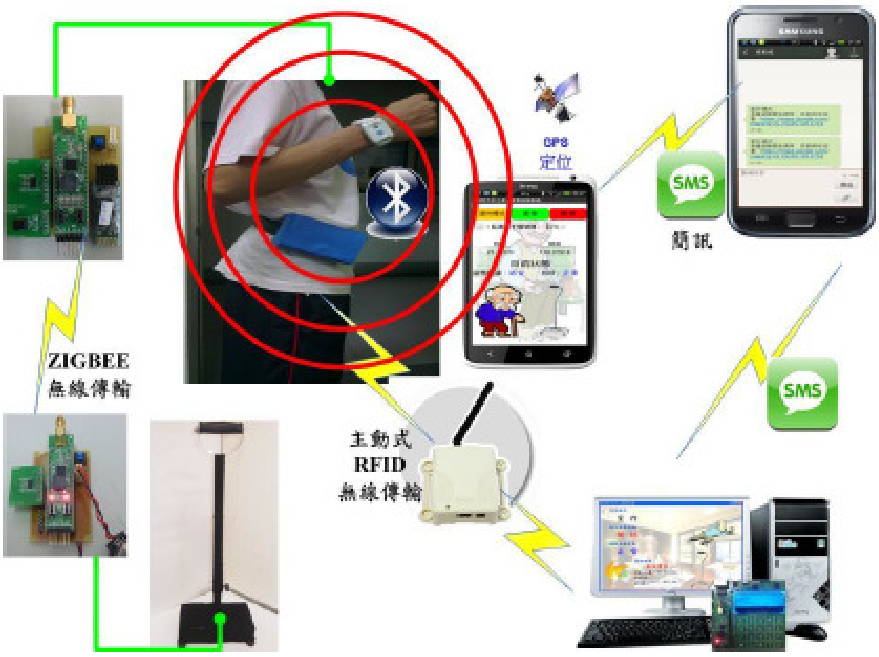
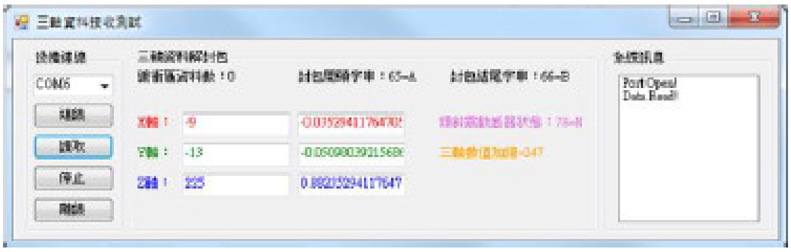


圖 4-1 系統架構圖

本作品的應用程式為以「Visual Studio .Net 2008」的 Visual Basic 撰寫設計而成，並分為五個部分，第一部分是測試接收三軸資料的程式，如圖 4-2 所示，此程式在設計時必須配合韌體部分撰寫，必須知道 ZigBee 終端節點與協調器回傳資料時封包的開頭與結尾，才能將資料完整接收；資料接收之後，經由數值正規化的動作，將動作記錄起來，供網路訓練所使用 ，或者是將資料即時輸入訓練後的網路，供網路回想時辨認動作，而網路訓練後之可用參數也完整的紀錄起來(紀錄之參數如圖 4-3 所示)。



三軸資料解封包
緩衝區資料數：0
封包開頭字串：65=A
封包結尾字串：66=B

X軸：-9　-0.0352941176470
Y軸：-13　-0.0509803921568
Z軸：225　0.88235294117647
資料接收緩衝器狀態：1.78=8
三軸數值加總=347

接收訊息
Port Open!
Data Read!

圖 4-2、三軸資料接收測試程式

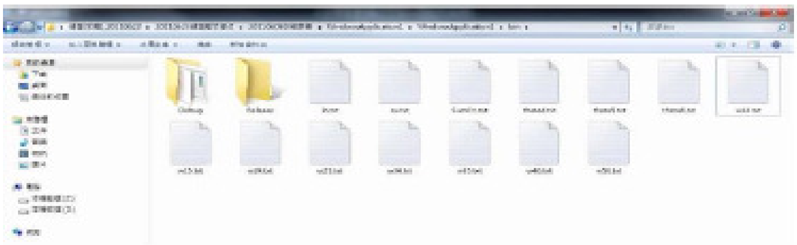


圖 4-3、網路訓練後之參數紀錄

第二部分是倒傳遞類神經網路訓練程式，如圖 4-4 與圖 4-5 所示，將網路的訓練程式獨立撰寫，讀入由三軸正規化後的資料，自行設計動作編碼，再進行網路訓練，再將網路誤差、可用 網路參數做儲存的動作，以供判斷網路是否收斂與網路回想時可使用 的網路參數。圖 4-4 是學習演算法撰寫階段的程式，將演算法每個計算步驟做成單部執行的功能，一步一步除錯；圖 4-5 是學習演算法程式完成後，簡化過的程式，因學習後就不再使用 ，所以操作介面以簡單為主。

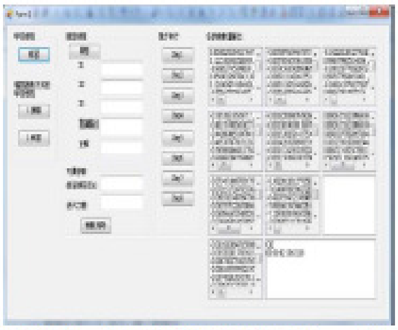
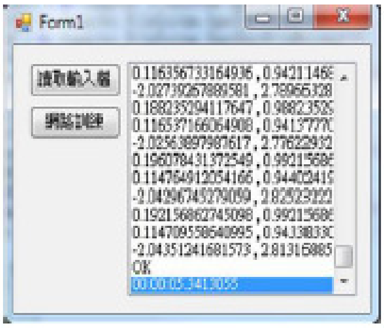


圖 4-4、學習演算法撰寫階段之程式介面



```
0.116356733164936,0.9421146
-2.027392657889581,2.7896632
0.188235294117647,0.9882352
0.116537166064908,0.9413777
-2.02563897987617,2.7762293
0.196078431372549,0.9921568
0.114764912054166,0.9440241
-2.04296745279059,2.8252392
0.192156862745098,0.9921568
0.114709558640995,0.9433833
-2.04351241681573,2.8131688
OK
00:00:05.3413055
```

圖 4-5、學習演算法程式介面

第三部分是網路回想與動作判斷的程式，如圖 4-6 所示，程式內包含了三軸讀值的程式，即時接收三軸的資料並正規化，再將正規化後的數值，當作網路回想的輸入，計算其推論輸出，即可完成即時動作辨識。為了在實驗上方便觀察動作改變時的三軸特徵，利用 VB 的繪圖功能，畫出 X、Y、Z 的數值/時間曲線圖與三軸數值加總/時間曲線圖。X、Y、Z 曲線圖，可以在動作產生變化時，看出三個軸的變化特徵；三軸數值加總曲線圖，可以在跌倒發生時，看出三軸受重力加速度所影響時的劇烈變化特徵。

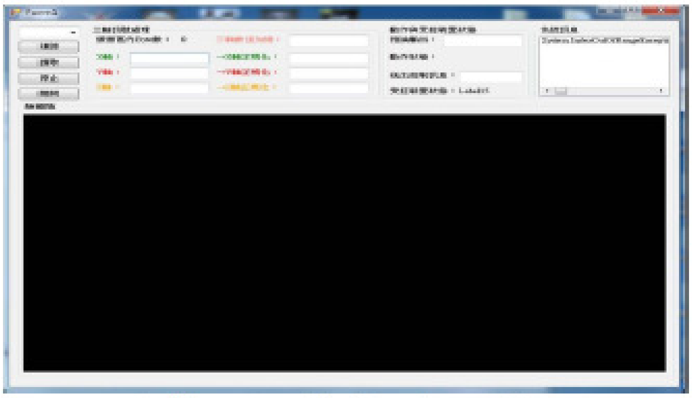
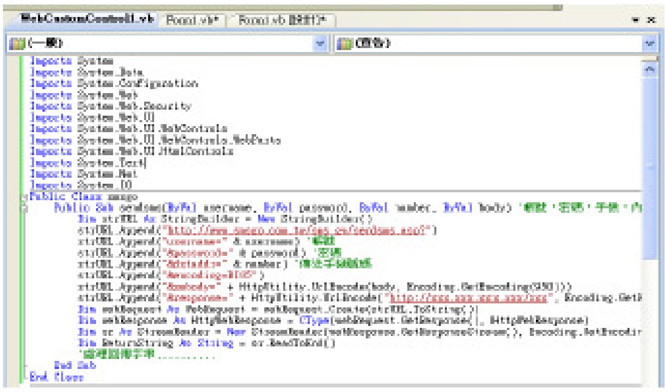


圖 4-6、網路回想與動作判斷之程式介面

第四部分是手機簡訊的程式，如圖 4-7 所示，這個程式在老人發生跌倒時，將利用網路經過手機伺服器，傳送簡訊內照護人的手機，照護人能立即知道老人情況，給予幫助。



```
Imports System
Imports System.Data
Imports System.Configuration
Imports System.Web
Imports System.Web.Security
Imports System.Web.UI
Imports System.Web.UI.WebControls
Imports System.Web.UI.WebControls.WebParts
Imports System.Web.UI.HtmlControls
Imports System.Text
Imports System.Net
Imports System.IO
Public Class smsgo
    Public Sub sendsms(ByVal username, ByVal password, ByVal number, ByVal body) '帳號，密碼，手機，內
        Dim strURL As StringBuilder = New StringBuilder()
        strURL.Append("http://www.smsgo.com.tw/sms_gw/sendsms.asp?")
        strURL.Append("username=" & username) '帳號
        strURL.Append("&password=" & password) '密碼
        strURL.Append("&dstaddr=" & number) '傳送手機號碼
        strURL.Append("&encoding=BIG5")
        strURL.Append("&smbody=" + HttpUtility.UrlEncode(body, Encoding.GetEncoding(950)))
        strURL.Append("&response=" + HttpUtility.UrlEncode("http://xxx.xxx.xxx.xxx/xxx", Encoding.GetE
        Dim webRequest As WebRequest = webRequest.Create(strURL.ToString())
        Dim webResponse As HttpWebResponse = CType(webRequest.GetResponse(), HttpWebResponse)
        Dim sr As StreamReader = New StreamReader(webResponse.GetResponseStream(), Encoding.GetEncodin
        Dim ReturnString As String = sr.ReadToEnd()
        '處理回傳字串..........
    End Sub
End Class
```

圖 4-7、手機簡訊傳送程式

第五個部分是由主動式 RFID Reader 可以掌握住範圍內老人的體溫以防止老人身體不適，同時也可以進行 Reader 範圍內的判斷，可以監控一些特別需要照顧的老人，也能達到防止老人走失的效果。

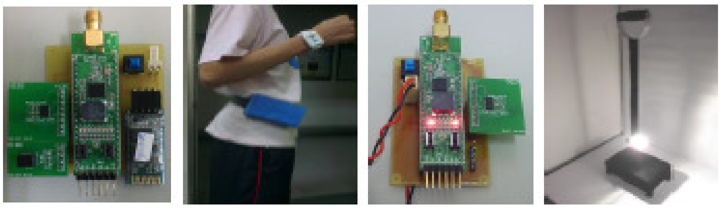


圖 4-8、姿態辨識感測器，配戴在使用者之腰部，拐杖辨識感測器安裝在柺杖上，也設置了一個 LED 燈方便夜間照明

8

- ➢ VB.NET 程式介面：

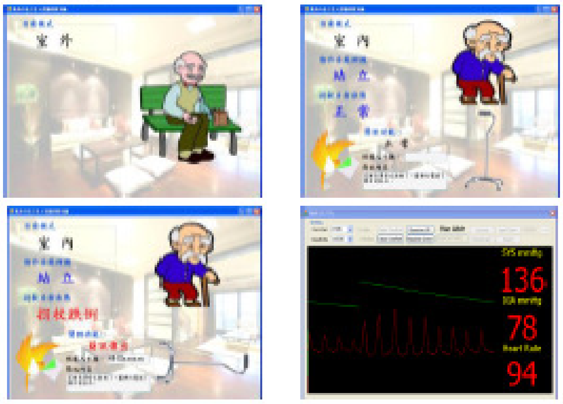


圖 4-9、外出時及正常狀態下、跌倒發生時及血壓及脈搏量測的程式介面圖

- ➢ APP 手機程式介面：

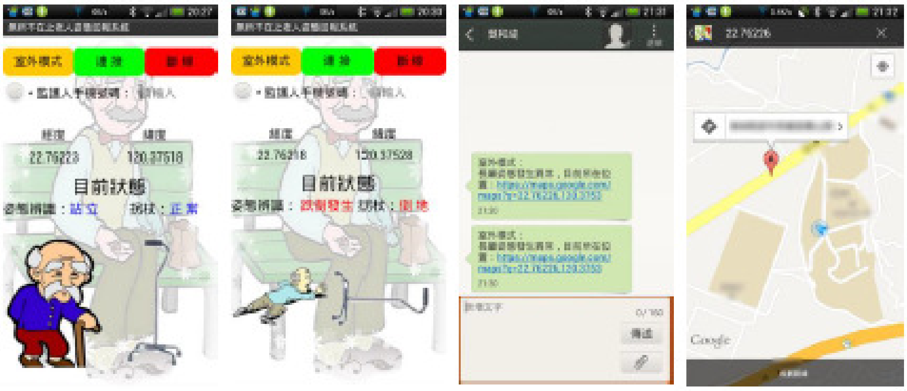


圖 4-10、正常狀態下及發生跌倒時手機接收到簡訊，並透過手機 GPS 定位

✧ 類神經演算法部分：

類神經網路(articial neural network)或稱為人工神經網路，所指的是生物神經網路的資訊處理系統。類神經網路較正確的定義為：「類神經網路是一種計算系統，使用大量簡單相連的人工神經元來模仿生物神經網路的能力。人工神經元是生物神經元的簡單模擬，它從外界環境或者其他人工神經元取得資訊，並加以簡單的運算，並輸出其結果到外界環境或者其他人工神經元」。

類神經網路是由許多的人工神經細胞所組成，人工神經細胞又稱類神經元、人工神經元、處理單元。每一個處理單元的輸出以扇狀送出，成為其他許多處理單元的輸入。

處理單元其輸出值與輸入值的關係式：

$$Y_j = f(\sum_i W_{ij} X_i - \theta_j)$$

Yj＝模仿生物神經元的模型的輸出訊號。

f()=模仿生物神經元的模型的轉換函數，是一個用以將從其他處理單元輸入的輸入值乘積和轉換成處理單元輸出值的數學公式。

Wij=模仿生物神經元的模型的神經節強度，又稱連結加權值。

Xi=模仿生物神經元的模型的輸入訊號。

θj=模仿生物神經元的模型的閥值。

如圖 4-11 所示，介於處理單元間的訊號傳遞路徑稱為連結。每一個連結上有一個數值的加權值Wij，用以表示第 i 個處理單元對第 j 個處理單元之影響強度。一個類神經網路是由許多個人工神經元與其連結所組成，並且可以組成各種網路模式。一個 BPN 包含許多層，輸入層處理單元用以輸入外在環境的訊息，輸出層處理單元用以輸出訊息給外在環境。此外，一個層狀類神經網路經常包含若干層隱藏層，隱藏層的存在提供類神經網路表現處理單元間的交互作用，與問題的內在結構的能力，通常每一層處裡單元均有連結與相鄰層的處理單元連接。

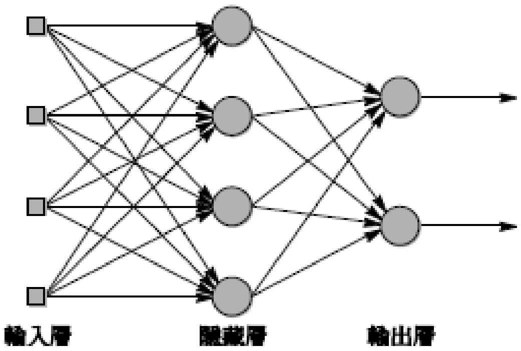


圖 4-11、類神經網路模型：以倒傳遞網路為例

✧ 倒傳遞類神經網路部分：

➢ 數值正規化

如圖 4-12 所示，由於我們的類神經網路轉換函數選擇的是雙彎曲函數

f(x)=1/1+e-x，所以我們在做類神經網路運算之前先把三軸數值正規化到-1~+1之間，讓神經網路比較好收斂。

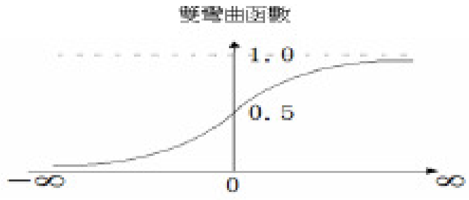


圖 4-12、本研究所使用的轉換函數，雙彎曲函數只會趨近 0 到 1，並不等於 0 跟 1。

極值正規化公式：把 X 正規化到 Ymax 與 Ymin 之間：

$$\frac{X - X_{\min}}{X_{\max} - X_{\min}}(Y_{\max} - Y_{\min}) + Y_{\min}$$

例如現有一組三軸資料(X,Y,Z)=(200,130,15)，將此數值經由正規化公式輸出後：

X 軸為：0.784313725490196

Y 軸為：0.509803921568627

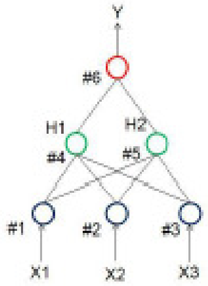
Z 軸為：0.0588235294117647

並將此組正規化後的數值當作是類神經網路的輸入。

- 倒傳遞類神經網路演算法

網路架構：

隱藏層神經元的數目=(輸入神經元數目+輸出神經元數目)/2，所以決定網路架構與網路參數加權值 W、閥值 θ 與學習速率 η(如圖 4-13)：



$W_{14}=1$

$W_{15}=-1$

$W_{24}=-1$

$W_{25}=1$

$W_{34}=1$

$W_{35}=-1$

$W_{46}=-1$

$W_{56}=1$

$\theta_4=1$

$\theta_5=1$

$\theta_6=1$

$\eta=0.18$

圖 4-13、本研究之倒傳遞網路模型與初始加權值、閥值與學習速率之設定。

網路演算法：網路演算法分為學習過程與回想過程。

學習過程：

1.設定網路參數。

2.以+1~-1 之間的隨機亂數決定 W、θ 的初始值。

3.輸入一個訓練範例的輸入向量 X 與目標輸出向量 T。

4.計算推論輸出向量 Y。

a.計算隱藏層輸出值

$$net_4 = W_{14} \cdot X_1 + W_{24} \cdot X_2 + W_{34} \cdot X_3 - \theta_4$$

$$H_1 = \frac{1}{1+\exp(-net_4)}$$

$$net_5 = W_{15} \cdot X_1 + W_{25} \cdot X_2 + W_{35} \cdot X_3 - \theta_5$$

$$H_2 = \frac{1}{1+\exp(-net_5)}$$

b.計算輸出層輸出值

$$net_6 = W_{46} \cdot H_1 + W_{56} \cdot H_2 - \theta_6$$

$$Y = \frac{1}{1+\exp(-net_6)}$$

5.計算差距量δ。

a.計算輸出層差距量δ

$$\delta_6 = Y(1-Y)(T-Y)$$

b.計算輸出層差距量δ

$$\delta_4 = H_1(1-H_1) \cdot W_{46} \cdot \delta_6$$

$$\delta_5 = H_2(1-H_2) \cdot W_{56} \cdot \delta_6$$

6.計算 W 修正量ΔW、θ 修正量Δθ。

a.計算輸出層 W 修正量ΔW、θ 修正量Δθ

$$\Delta W_{46} = \eta \cdot \delta_6 \cdot H_1$$

$$\Delta W_{56} = \eta \cdot \delta_6 \cdot H_2$$

$$\Delta \theta_6 = -\eta \cdot \delta_6$$

b.計算隱藏層 W 修正量ΔW、θ 修正量Δθ

$$
\begin{array}{ll}
\Delta W_{15} = \eta \cdot \delta_5 \cdot X_1 & \Delta W_{1\,4} = \eta \cdot \delta\ _4 X \\
\Delta W_{25} = \eta \cdot \delta_5 \cdot X_2 & \Delta W_{2\,4} = \eta \cdot \delta\ _4 X \\
\Delta W_{35} = \eta \cdot \delta_5 \cdot X_3 & \Delta W_{3\,4} = \eta \cdot \delta\ _4 X \\
\Delta \theta_5 = -\eta \cdot \delta_5 & \Delta \theta_4 = -\eta \cdot \delta_4
\end{array}
$$

7.更新 W、θ

a.採批次學習法採批次學習，所以將所有範例的ΔW、Δθ 加總後再進行更新。

b.計算輸出層與隱藏層 W、θ

$$
\begin{array}{lll}
W_{14} = W_{14} + \Delta W_{14} & W_{1\,5} = W_{1\,5} + \Delta W_{1} & W_{4\,6} = W_{4\,6} + \Delta W \\
W_{24} = W_{24} + \Delta W_{24} & W_{2\,5} = W_{2\,5} + \Delta W & W_{5\,6} = W_{5\,6} + \Delta W \\
W_{34} = W_{34} + \Delta W_{34} & W_{3\,5} = W_{3\,5} + \Delta W & \\
\theta_4 = \theta_4 + \Delta \theta_4 & \theta_5 = \theta_5 + \Delta \theta_5 & \theta_6 = \theta_6 + \Delta \theta_6
\end{array}
$$

8.重複步驟 3 到步驟 7，直到收斂(誤差不再有明顯變化) 。

9.誤差計算公式：

$$E = \sum \sqrt{(T - Y)^2}$$

回想過程：

1.設定網路參數。

2.讀入更新過後的 W、θ。

3.輸入一個測試範例的輸入向量 X。

4.計算推論輸出向量 Y。

訓練範例輸入後，經由學習演算法運算之後，必須經由誤差公式計算其誤差，來判斷網路是否學習成功，若網路學習成功則收斂(如圖 4-14)。

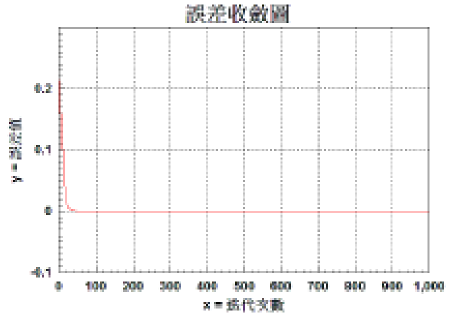
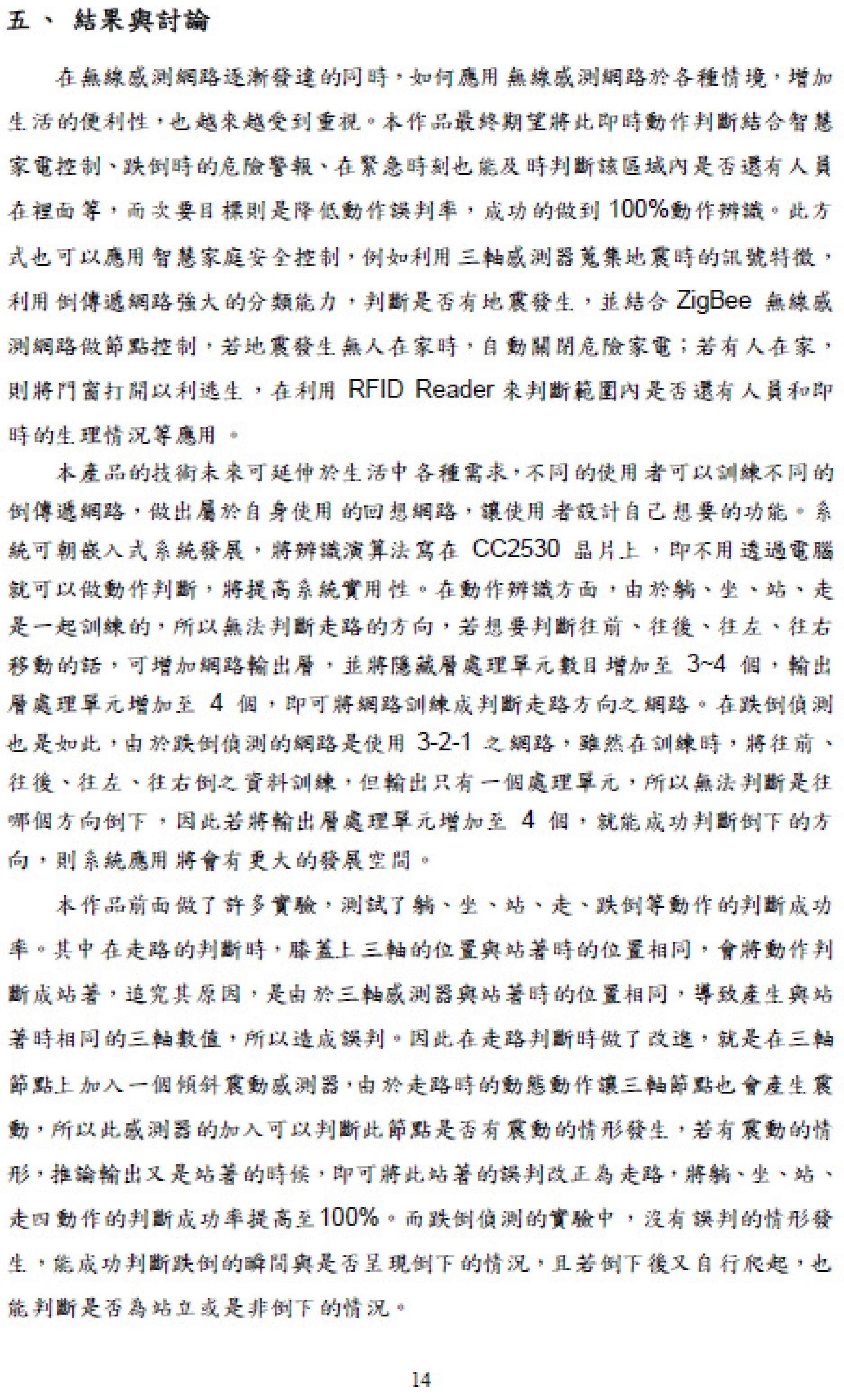


圖 4-14、誤差收斂圖

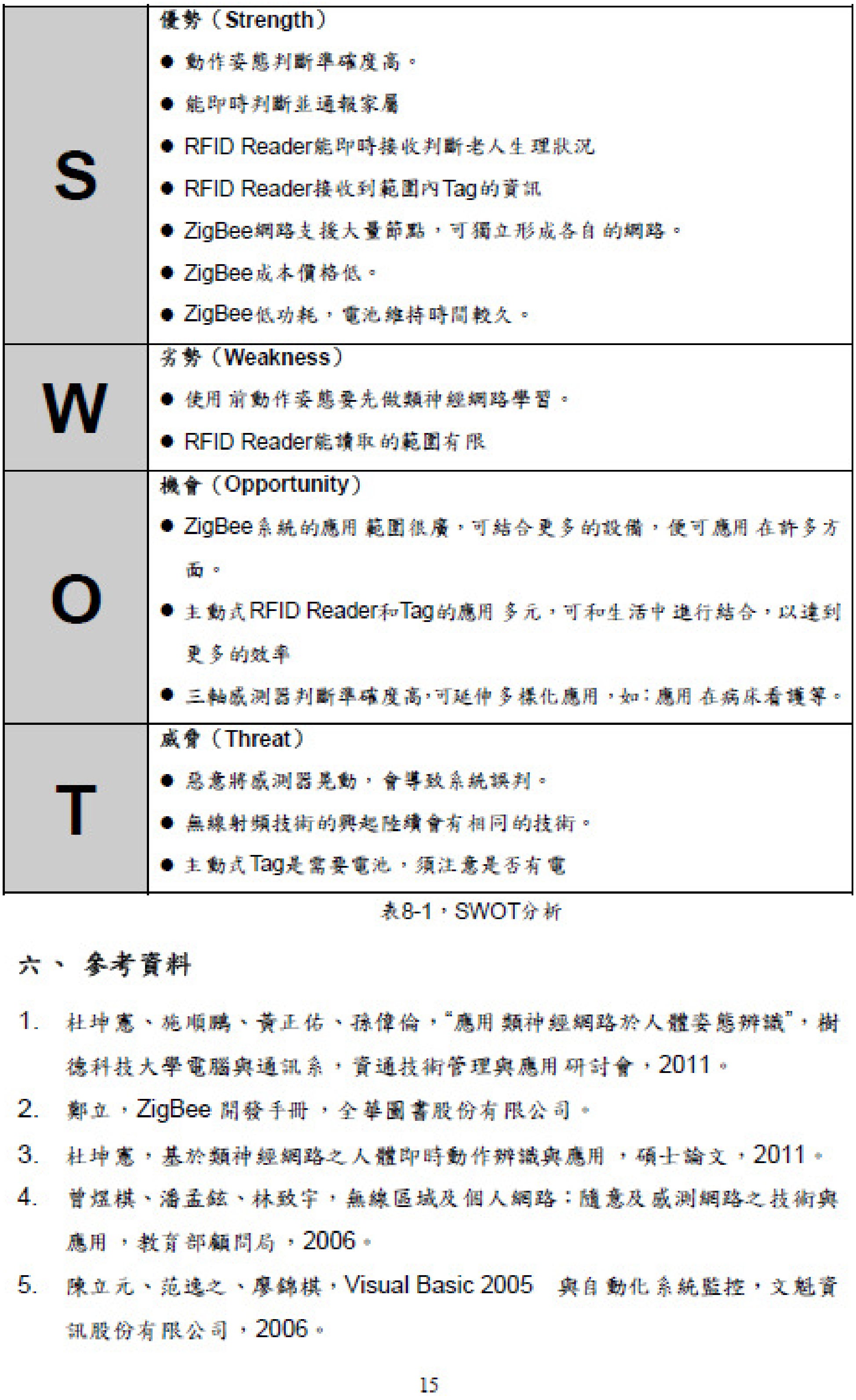


五、 結果與討論

在無線感測網路逐漸發達的同時，如何應用無線感測網路於各種情境，增加生活的便利性，也越來越受到重視。本作品最終期望將此即時動作判斷結合智慧家電控制、跌倒時的危險警報、在緊急時刻也能及時判斷該區域內是否還有人員在裡面等，而次要目標則是降低動作誤判率，成功的做到100%動作辨識。此方式也可以應用智慧家庭安全控制，例如利用三軸感測器蒐集地震時的訊號特徵，利用倒傳遞網路強大的分類能力，判斷是否有地震發生，並結合ZigBee無線感測網路做節點控制，若地震發生無人在家時，自動關閉危險家電；若有人在家，則將門窗打開以利逃生，在利用RFID Reader来判斷範圍內是否還有人員和即時的生理情況等應用。

本產品的技術未來可延伸於生活中各種需求，不同的使用者可以訓練不同的倒傳遞網路，做出屬於自身使用的回想網路，讓使用者設計自己想要的功能。系統可朝嵌入式系統發展，將辨識演算法寫在CC2530晶片上，即不用透過電腦就可以做動作判斷，將提高系統實用性。在動作辨識方面，由於躺、坐、站、走是一起訓練的，所以無法判斷走路的方向，若想要判斷往前、往後、往左、往右移動的話，可增加網路輸出層，並將隱藏層處理單元數目增加至3~4個，輸出層處理單元增加至4個，即可將網路訓練成判斷走路方向之網路。在跌倒偵測也是如此，由於跌倒偵測的網路是使用3-2-1之網路，雖然在訓練時，將往前、往後、往左、往右倒之資料訓練，但輸出只有一個處理單元，所以無法判斷是往哪個方向倒下，因此若將輸出層處理單元增加至4個，就能成功判斷倒下的方向，則系統應用將會有更大的發展空間。

本作品前面做了許多實驗，測試了躺、坐、站、走、跌倒等動作的判斷成功率。其中在走路的判斷時，膝蓋上三軸的位置與站著時的位置相同，會將動作判斷成站著，追究其原因，是由於三軸感測器與站著時的位置相同，導致產生與站著時相同的三軸數值，所以造成誤判。因此在走路判斷時做了改進，就是在三軸節點上加入一個傾斜震動感測器，由於走路時的動態動作讓三軸節點也會產生震動，所以此感測器的加入可以判斷此節點是否有震動的情形發生，若有震動的情形，推論輸出又是站著的時候，即可將此站著的誤判改正為走路，將躺、坐、站、走四動作的判斷成功率提高至100%。而跌倒偵測的實驗中，沒有誤判的情形發生，能成功判斷跌倒的瞬間與是否呈現倒下的情況，且若倒下後又自行爬起，也能判斷是否為站立或是非倒下的情況。



S	優勢（Strength） ● 動作姿態判斷準確度高。 ● 能即時判斷並通報家屬 ● RFID Reader能即時接收判斷老人生理狀況 ● RFID Reader接收到範圍內Tag的資訊 ● ZigBee網路支援大量節點，可獨立形成各自的網路。 ● ZigBee成本價格低。 ● ZigBee低功耗，電池維持時間較久。
W	劣勢（Weakness） ● 使用前動作姿態要先做類神經網路學習。 ● RFID Reader能讀取的範圍有限
O	機會（Opportunity） ● ZigBee系統的應用範圍很廣，可結合更多的設備，便可應用在許多方面。 ● 主動式RFID Reader和Tag的應用多元，可和生活中進行結合，以達到更多的效率 ● 三軸感測器判斷準確度高,可延伸多樣化應用，如:應用在病床看護等。
T	威脅（Threat） ● 惡意將感測器晃動，會導致系統誤判。 ● 無線射頻技術的興起陸續會有相同的技術。 ● 主動式Tag是需要電池，須注意是否有電

表8-1，SWOT分析

六、 參考資料

1. 杜坤憲、施順鵬、黃正佑、孫偉倫，“應用類神經網路於人體姿態辨識”，樹德科技大學電腦與通訊系，資通技術管理與應用研討會，2011。

2. 鄭立，ZigBee 開發手冊，全華圖書股份有限公司。

3. 杜坤憲，基於類神經網路之人體即時動作辨識與應用，碩士論文，2011。

4. 曾煜棋、潘孟鉉、林致宇，無線區域及個人網路：隨意及感測網路之技術與應用，教育部顧問局，2006。

5. 陳立元、范逸之、廖錦棋，Visual Basic 2005 與自動化系統監控，文魁資訊股份有限公司，2006。

6. 曾吉弘、 蔡宜坦、黃凱群、賴偉民、盧玟攸、施力維，Android手機程式超簡單 App Inventor 入門卷，旗林文化 ，2012

7. 曾吉弘、賴偉民、謝宗翰、林毓祥、薛皓云 ，Android手機程式超簡單 App Inventor 機器人卷，旗林文化 ，2012

8. 廖國良、林家禎、許永和、李金鳳，RFID無線射頻辨識實驗系統，台灣優奎士有限公司。2010

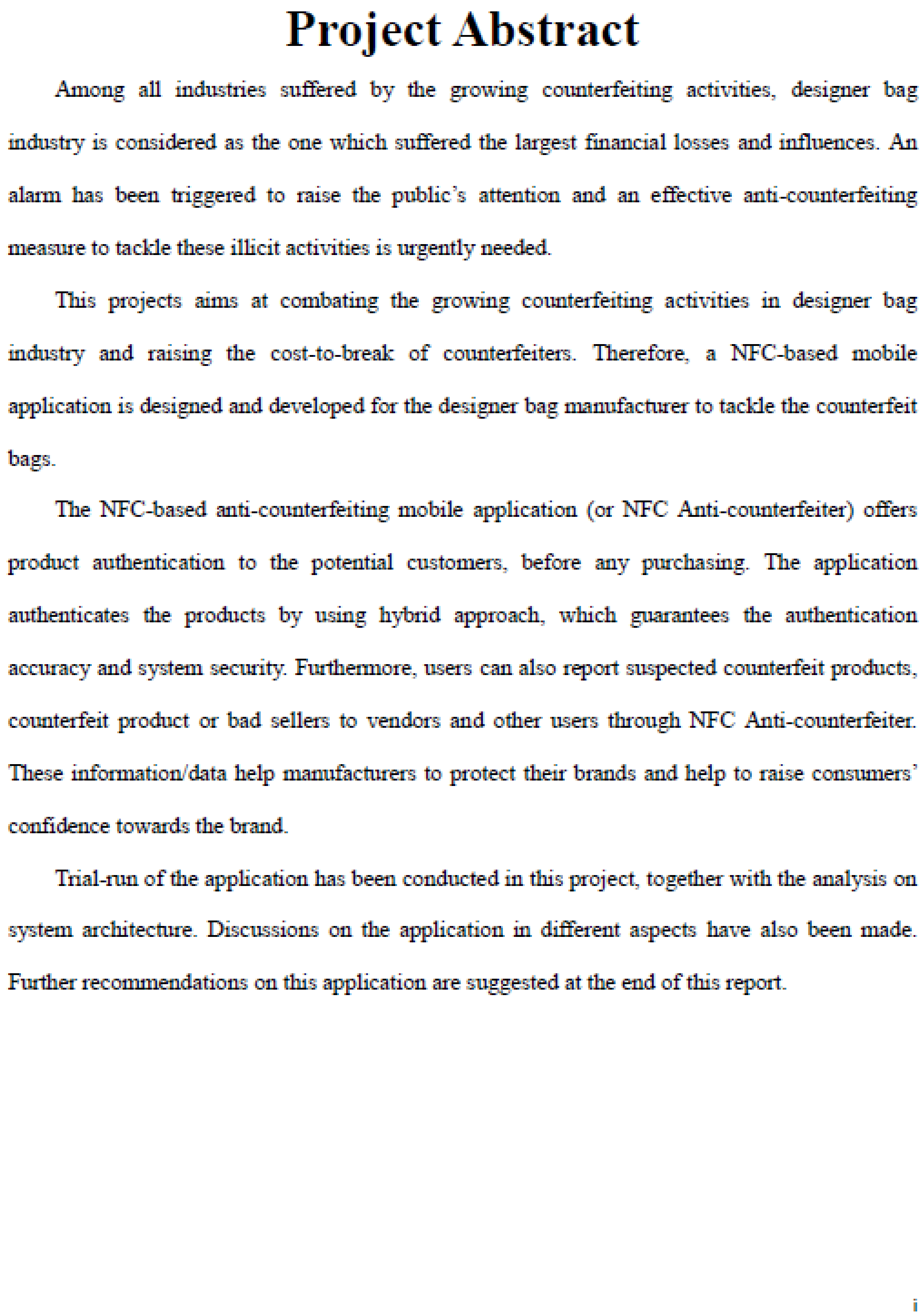
Best Research Award
最佳研究大獎

Project title項目名稱: Design and Development of NFC-based Mobile Application for Anti-counterfeiting in Designer Bag Manufacturer

Students學生: Chung Chun Lan, Kwong Kuk Hung, Wu Wing Sum, Lau Wing Yu
鍾春蘭，鄺鵠鴻，胡詠芯，劉詠如

Institution 院校: Department of Industrial and Systems Engineering , The Hong Kong Polytechnic University 香港理工大學 工業及系統工程學系

Supervisors指導: Dr. Ip Wai Hung Andrew, Dr. Lee K.M. Carman, Dr. Ho T.S. George
葉偉雄博士，李嘉敏助理教授，何道森專任導師



Project Abstract

Among all industries suffered by the growing counterfeiting activities, designer bag industry is considered as the one which suffered the largest financial losses and influences. An alarm has been triggered to raise the public's attention and an effective anti-counterfeiting measure to tackle these illicit activities is urgently needed.

This projects aims at combating the growing counterfeiting activities in designer bag industry and raising the cost-to-break of counterfeiters. Therefore, a NFC-based mobile application is designed and developed for the designer bag manufacturer to tackle the counterfeit bags.

The NFC-based anti-counterfeiting mobile application (or NFC Anti-counterfeiter) offers product authentication to the potential customers, before any purchasing. The application authenticates the products by using hybrid approach, which guarantees the authentication accuracy and system security. Furthermore, users can also report suspected counterfeit products, counterfeit product or bad sellers to vendors and other users through NFC Anti-counterfeiter. These information/data help manufacturers to protect their brands and help to raise consumers' confidence towards the brand.

Trial-run of the application has been conducted in this project, together with the analysis on system architecture. Discussions on the application in different aspects have also been made. Further recommendations on this application are suggested at the end of this report.

i

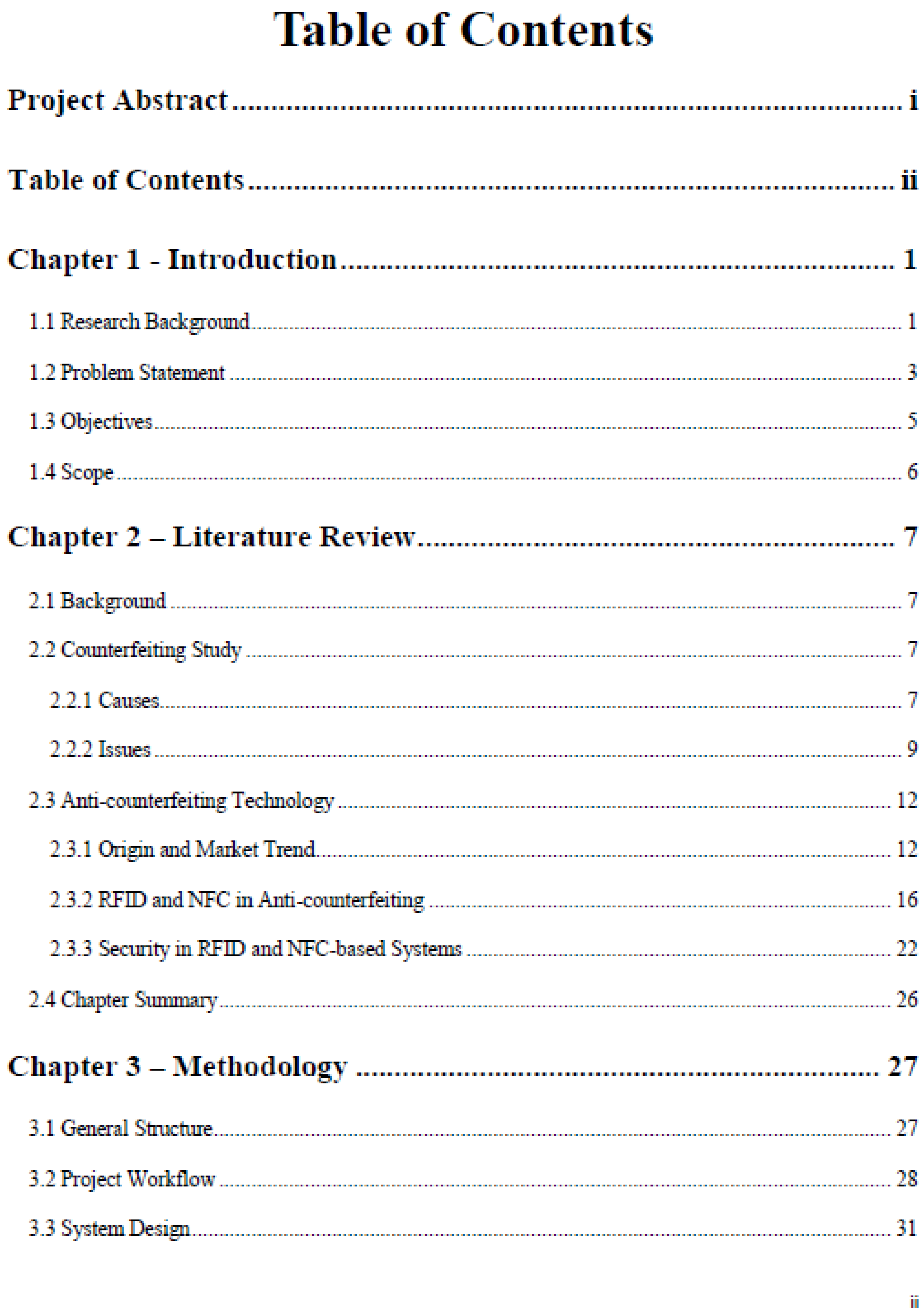
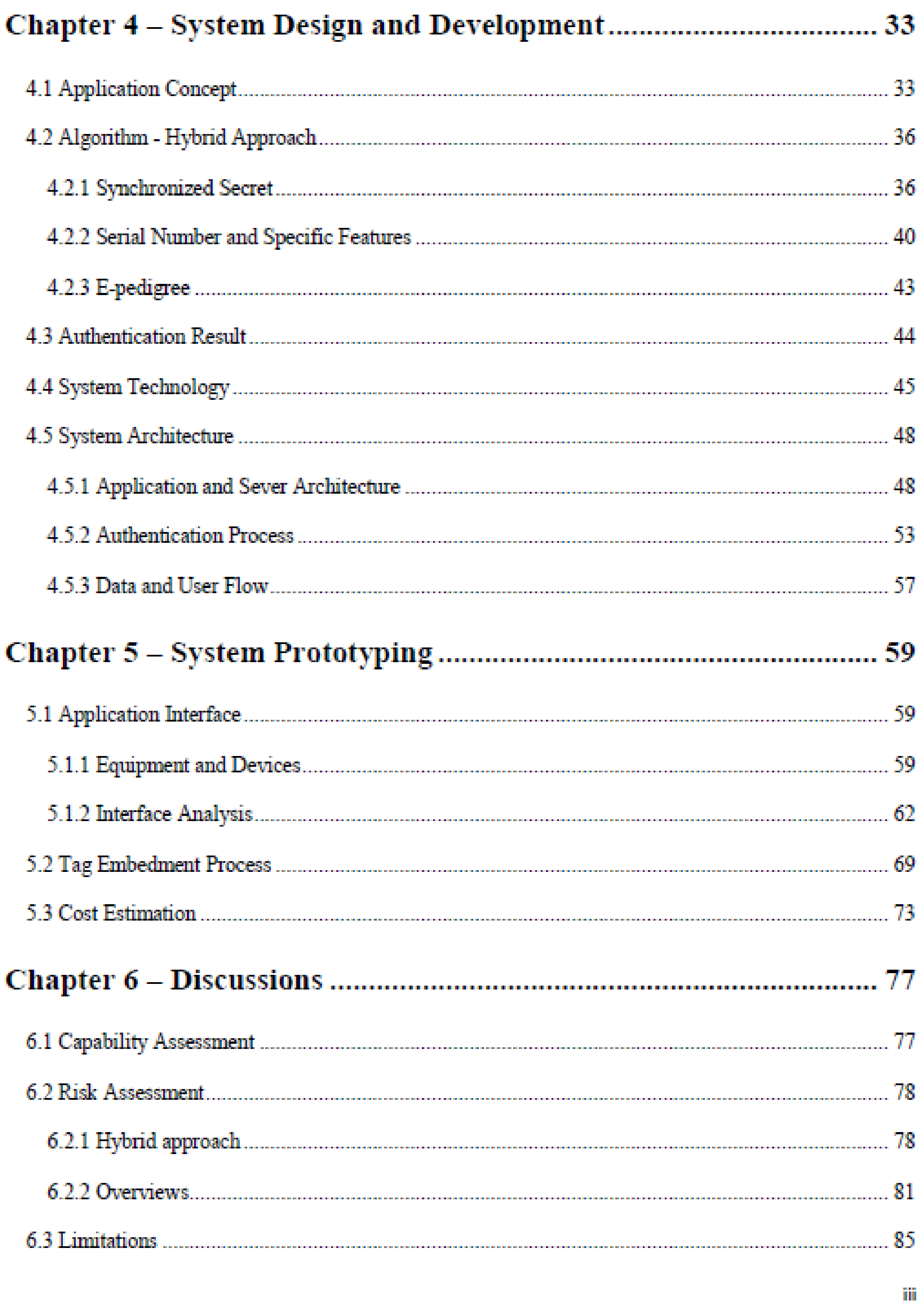
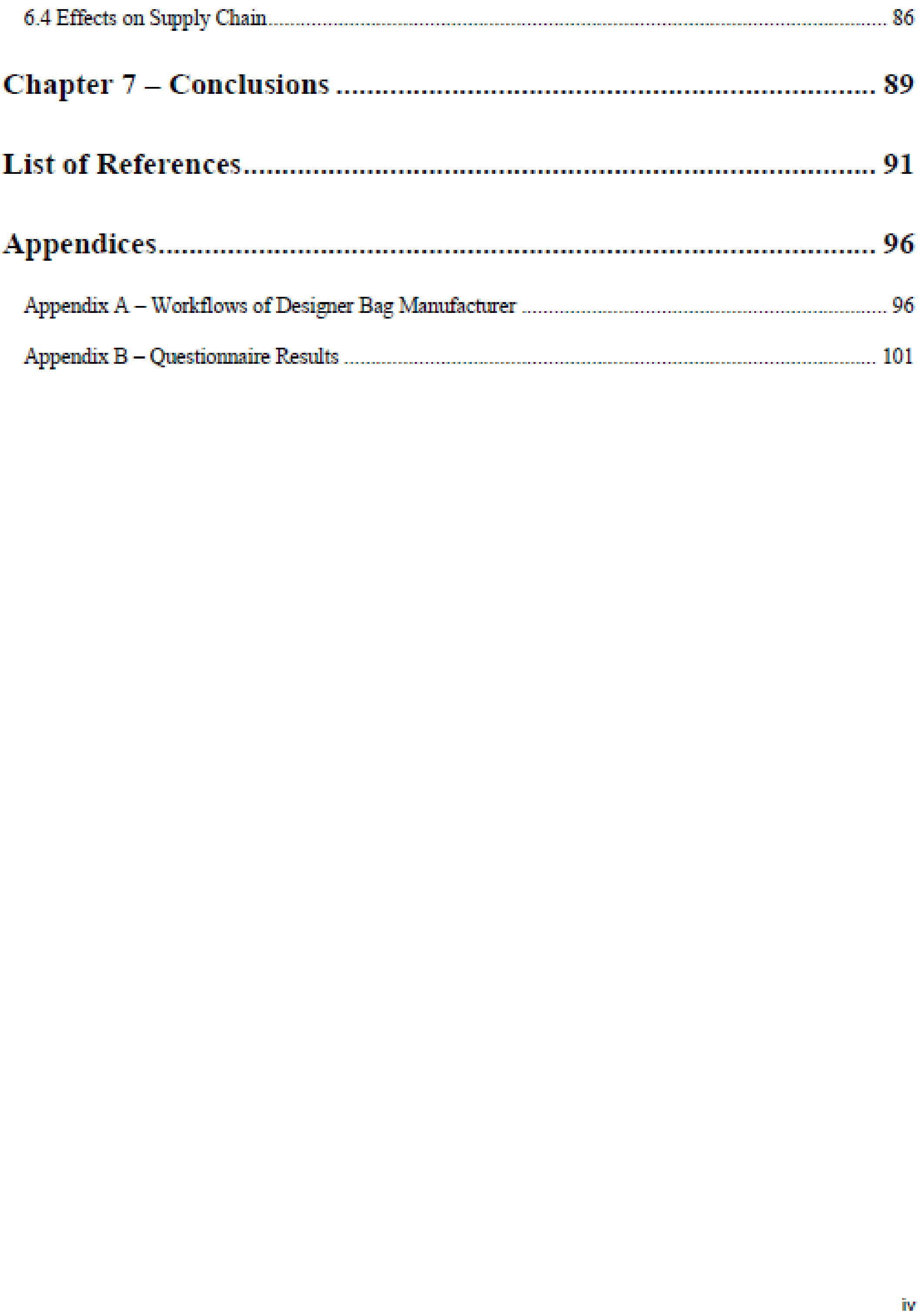


Table of Contents





Chapter 1 - Introduction

1.1 Research Background

Nowadays, counterfeit prevention has rung a bell in the society. According to Mallor (2007), counterfeit goods are non-genuine goods "that copy or otherwise purport to be those of the trademark owner whose mark has been unlawfully used". It is different from copyright violation. Copyright violation involves unauthorized transfer of licensed material like sharing of music and movies electronically; it does not involve any form of consumer fraud.

Almost every product can be counterfeited. The imitations of arts, toys, clothing, pharmaceuticals, watches, electronics, handbags and shoes are all around in the market and spread through the globe. These kinds of counterfeit have resulted in serious patent and trademark infringement. There are sharply increase of ranges of different goods to infringement too.

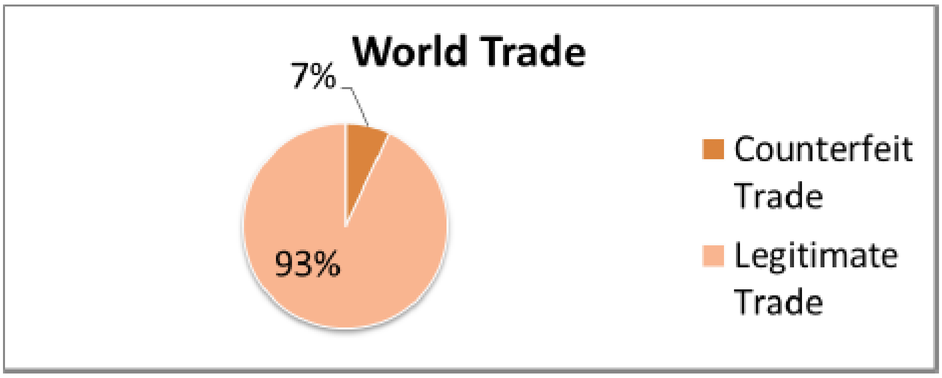


Figure 1.1- Counterfeit Trade Ratio (US Chamber of Commerce, 2012)

According to the White Horse Laboratories (White Horse Laboratories, 2012), there is 142% increase in reported counterfeit components from 2011 to 2012, which has skyrocketed in the past 12 months. Also, Counterfeiting Intelligence Bureau (CIB) of the International Chamber of Commerce (ICC) (Counterfeiting Intelligence Bureau, 2012) has been estimated that counterfeit goods have made up 5 to 7% of World Trade which amounts to US$600 Billion per year. Counterfeiting is responsible for the loss of over 750,000 American jobs (US Chamber of Commerce, 2012).

A research of Organization for Economic Cooperation and Development mentioned in Terseko (2008) and Lewis (2012), companies "spent over half their R&D investment on anti-privacy technologies and product differentiation."

China, Russia, India, Brazil, Indonesia, Vietnam are famous of rampant exuberant intellectual property violations. Brand names, trademarks and copyrights are infringed by local counterfeiters. The local governments do not have strict legislation on these kinds of activities. On the contrary, this situation indirectly encourages the counterfeit activities.

China is the worst offenders by far. According to Blanchard (2007), over 80% of all counterfeit goods in 2006 are made in China. As China joined World Trade Organization in 2001, it removes trade barriers. At that time, China already has substantial amount of counterfeits within its border, thus, large number of counterfeit goods flow across the borders and spread through the globe. Although there is legislation against the counterfeit activities, it is extremely strict on paper and hard to enforce. Moreover, pressure to eliminate counterfeiting often conflicts with the government's obligation to increase the employment level (Lewis, 2012). Li Guorong of the China United Intellectual Property Protection Center (2012) once explained "Sometimes the factory that produces counterfeits is the largest single employer in the province, so if there is a raid the local mayor might call the police and tell them not to proceed" (Phillips, 2005). Therefore, it is extremely hard to solve the issue.

1.2 Problem Statement

Because of the emergence of massive counterfeits, different problems and issues have seriously disrupted the society's operation. It is necessary to tackle those issues immediately.

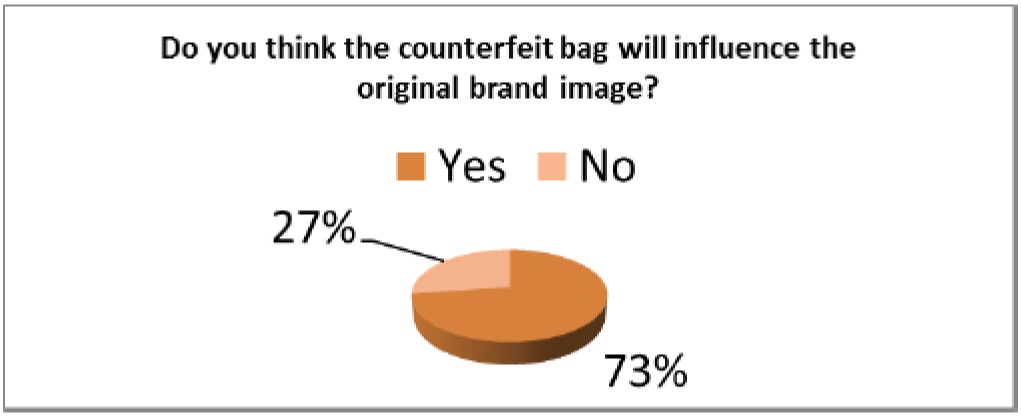


Figure 1.2- Interview Result I for the anti-counterfeit study

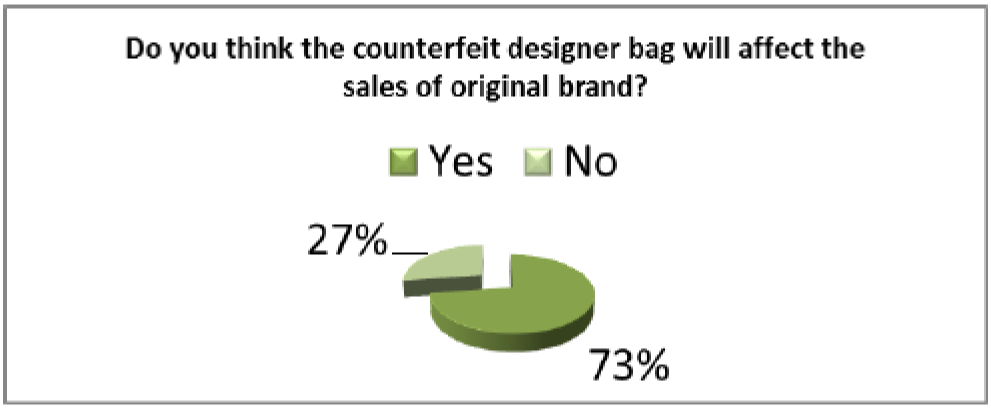


Figure 1.3-Interview Result II for the anti-counterfeit study

An interview has been conducted on the counterfeit situation. The details of the interview will be put in the Appendix section. From the two diagrams shown above, over 70% of interviewees are agreed that the counterfeit bags will influence the original brand image and affect the sales of that brand.

For the company, especially those companies with high amount of intellectual property and patents are facing severe counterfeit problems which are now creating greater and greater financial losses of the company. The huge financial loss will force the company to impose higher selling price to the customers. This situation will form a vicious cycle. The customers will be thereby forced to buy counterfeits because they cannot afford to buy the genuine goods. The increased sales in counterfeits will lead the counterfeit manufacturer to expand their production and product range.

For the customers, they are now frustrated by different counterfeit products and facing potential harm that those counterfeits may cause to them. For example, fake medicine, electronic appliances and devices do not follow any quality standard. These counterfeits impose potential dangers to the users and threaten their life. Also, with the improving counterfeiting technology, the customer might fall into the trap of consumer fraud which they buy counterfeits which they consider it as genuine. Hence, they suffer financial losses.

The society and the business still have not figured out an effective mean to tackle the counterfeiting activities. Although there are different methods or means developed to deal with this situation, the results are varied and unsatisfactory. Researchers are still working on building a stronger anti-counterfeiting tool.

Although there are current researches focused on developing a valid and effective means to prevent counterfeiting, such as RFID, NFC, QR code, Barcode, Laser marking, which are all the current methods suggested by different researches, the public are overwhelmed by the massive choices of anti-counterfeiting tools.

Among all anti-counterfeit technologies, NFC is the latest technology introduced these years, and it is still not widely implemented. NFC is seen as an applicable and effective method combating counterfeiting among most researches. Therefore, this project will investigate NFC in anti-counterfeiting.

1.3 Objectives

The basic idea of this project is to develop an effective and efficient model for anti-counterfeiting purpose. There are four objectives needed to be fulfilled to accomplish the project.

1. To analyze the current counterfeit situation and its issue

   It is necessary to have an in-depth knowledge on the current counterfeiting issues before developing the anti-counterfeit application. The application will only be effective if it targets at the right problems. Also, the study may raise the readers' attention to the seriousness of the current situation.

2. To design and develop a NFC-based anti-counterfeit mobile application

   The main core of this project is to develop an effective anti-counterfeit model which is applicable on the mobile phone. The model will be developed based on the latest NFC technology which allows tag identification by phone devices. There will be a demo shown in the later chapter. The system architecture will be analyzed in this report too.

3. To compare the anti-counterfeit approach developed with other existing anti-counterfeit approaches in the market. A comparison of the approached developed in this project with other approaches using similar technologies will be done in the project. By similar technology, it refers to the technologies which focus on contactless identification such as RFID and NFC. The comparison will help the readers to have clearer understanding on how they are different from and why this approach works.

4. To evaluate the effectiveness of NFC anti-counterfeit mobile application developed

   A risk assessment on the application developed will be done at the evaluation chapter. The risk assessment will focus on the capability to deal with different potential security threats. Rating will be given at the end of the risk assessment and will be compared with those of other anti-counterfeiting approaches.

1.4 Scope

In this project, a NFC-anti-counterfeit mobile application will be developed. The application and approach is designated in designer bag industry. It is not applicable in other industries such as drugs manufacturers, food manufacturing.

However, it does not mean that the whole concept of the NFC anti-counterfeit application cannot be fit in different industries except designer bag manufacturer. It is because the information selected and data shown in application are specified and designed to designer bag manufacturers. The counterfeit designer bags will be our primary target in the war of anti-counterfeiting.

The anti-counterfeiting technology used in the application is NFC. There will be no other anti-counterfeit technologies else used such as watermark, laser printing and barcode in this application. Consideration on NFC tag used in the application will also be included. However, no packaging will be designed in this project.

Although there are suggestions on tag embedment during the manufacturing process, there is no suggestion on improving the business process and workflow of the designer bag manufacturer. Also, there will be measures suggested on the authentication of second-hand bags. However, the main focus is in first hand genuine bags.

The concept of the application designed is on individual basis which means that one application developed is for one brand only. The application is not able to authenticate the bags from other brands although they are using the same NFC technology

Chapter 2 – Literature Review

2.1 Background

Counterfeiting of product is widely spread through the world. World Customs Organization (2012) has estimated that counterfeit products have been destined for more than 140 countries. The counterfeiting activities have covered more than 70% of the countries in the world. The situation is very serious.

The International Chamber of Commerce (2012) has also found out that "counterfeiting accounts for between 5-7% of world trade, worth an estimated US$600 billion a year" The counterfeit activities has resulted in great financial losses of the brand owners.

There are two main sections in this chapter. One will discuss the current counterfeiting situation and its issues, the other one will focus on the current anti-counterfeiting technologies.

2.2 Counterfeiting Study

2.2.1 Causes

One of the reasons why counterfeit is so prevalent is that is extremely lucrative for those unscrupulous merchants. The use of poor materials and low quality standards for those counterfeit goods enables the merchants to gain higher profit margin.

The advent of low-cost technology has also contributed to the increased prevalence of counterfeiting (Hopkins, 2003). Counterfeiters can access to tools like photographic-quality computer scanners and digital printers easily to replicate logos and create very similar packaging.

The risks of counterfeiting are generally small. According to Hopkins (2003), Legal penalties for counterfeiting are low in most countries, and do not exist at some other nations. For example, in US, Many who are caught and accused of trafficking in counterfeited goods mostly receive probation for their crime only (K.Lewis, 2012).

The existing demand for certain goods vastly exceeds the supply also encourages counterfeiting. The counterfeiters can fulfill this demand by selling those fake and cheap products. Taking Hermes handbag as an example, Hermes handbags are so expensive but there are many customers still willing to wait for years and cannot receive their bags yet. Hence, if the counterfeiters can offer a reasonable price of that counterfeit which offers very high facsimiles, and the customers do not have to wait it anymore, the counterfeiters can receive both praise and profits from those happy customers.

Increased globalization is another reason that has led to a greater number of counterfeit goods in the marketplace. Globalization has been so advantageous to the global economy; it has also greatly expedited legitimate international trade and encourages every development of humankinds. Yet, we cannot deny that globalization has great influence and help on the distribution of counterfeit goods, as well as the incentive to counterfeit. Counterfeits are easier to be flown between countries..

Moreover, the resources of customs are strained too due to rapid grow of globalization. When there are more goods across the boarders, the harder to do counterfeit preventions from investigating supply chain by customs officials. Also, it is hard to inspect large quantity of goods in short period, thus, it further increases the infiltration of counterfeit products.

Why globalization has further worsened the counterfeit problems due to increasing outsource manufacturing. Company licensed their intellectual property to foreign companies, which they have right to produce genuine brand-name goods. However, Tim Philips (2005) points out an example that from the factory's point of view, it is tempting to make 150,000 quantities by using extra materials instead of producing licensed amount 100,000. Since there is no inspector to inspect the extra products, no standard are needed to be followed during the production and thereby the factory can earn higher profits without paying extra license fee by selling all of them. This phenomenon called "Ghost Shift".

2.2.2 Issues

Since trade in counterfeits usually involves illegal black market transactions along the distribution chain, the burgeoning counterfeit industry has thereby resulted in huge loss in tax revenue, an absence of regulatory control, and an environment where terrorists and members of organized crime syndicates can fund illicit and deadly activities through counterfeit operations (Lewis, 2012).

As counterfeit provides no quality control procedures, the users or the buyers may face several potential crisis and suffer different consequences. The damage is more than just economic, the shoddy quality of counterfeit goods has led to deaths, illnesses, and injuries (Lewis, 2012).

First, fake goods are not safe; it can lead to injuries, deaths, and illnesses, especially for electronic device and medicine. For example, medicine manufactured without proper hygiene standard is poison to the patient. Patient may thereby die after taking the medicine. Electronic device without quality control procedure may lead to electricity leakage and explosion.

Second, some fake goods cause no physical harm and injury; however, customers are finically harmed when they are forced to spend their money on those poor quality, unsafe counterfeit products.

Since businesses are forced to raise their price in order to cover their losses from counterfeiting, the consumers are forced to pay higher price in order to buy for the genuine goods.

It is true that counterfeit operations often come with and involve the groups who joined criminal activities. Funding of criminal and terrorist groups mostly comes from intellectual property crime which is counterfeit operations. This funding method is very popular in Russia and Asia.

Counterfeiting can be used as an attack method by terrorists. They can flood the market with counterfeit products such as medicine to endanger and harm the consumers. This could create panic among consumers and destabilize the economy (Lewis, 2012).

According to Philips (2005), intellectual property represents around 45% to 75% of the assets of most of the fortune 500 companies; the loss of brand equity is particularly painful for genuine businesses. Furthermore, if customers are stop buying the genuine products and they are turned to buy counterfeit goods, the company not only loses its brand equity but all its future revenue that their consumers would provide.

Counterfeiting not only brings huge losses to the brands, but also cause fierce dilemma between the brands and the customers. When there are massive counterfeits appeared in the market and those counterfeits are made of low quality, unknowing customers then complain to the legitimate manufacturers or producers due to low product quality. Although the brands do not make those counterfeits, the customers still think it is the company's responsibility to prevent counterfeits and if the company fails to do this, they should serve the fake products anyway (Hopkins, 2003). Therefore, this presents a dilemma.

The company can refuse to service them or replace their fake goods with a genuine one. If they refuse to service, they may lose their customers and potential customers as the customers may become infuriated and complain to their family and friends. Future profits are lost eventually.

However, if the company is willing to replace the counterfeits by genuine goods, they would face another problem, that is, they have to pay, including money and reputation, for the counterfeiters, this pay-off seems unfair to the company as they are not responsible for compensating the losses for the customers who have bought the counterfeits.

From the point of legal liability, the company suffers seriously from the counterfeits. A customer has bought a fake good which he considered this as genuine products may sue the company for liability damages if he gets injured by this product. According to Arthur Best of the University of Denver Strum College of Law, "tort law would be likely to support a victim's claim against a producer of legitimate goods if harm from a counterfeit product was unforeseeable, the enterprise had a role in creating the risk of crime, and it failed to take reasonable steps to reduce the risk."(Lewis, 2012).

Government has also suffered great losses from tax revenue. They cannot collect the tax from the counterfeiters. Therefore, social welfare and funding for different programs will be affected

Not only financial losses would be occurred under fierce counterfeiting, but also innovation would be affected. Counterfeiting discourage innovation as it just copies from the existing innovation and design. According to Hopkin (2003), counterfeiters only need 2 percent of the time and 1/1000 of the cost of the genuine to make the counterfeit one and then enter the market.

2.3 Anti-counterfeiting Technology

2.3.1 Origin and Market Trend

Summarized from the above section of the reviews of counterfeiting, counterfeits and fake goods not only have caused billions of economic losses to the countries and companies, but also have threaten the safety and health of the consumers seriously. Illicit activities have also been enforced from the benefit of operating counterfeit activities too.

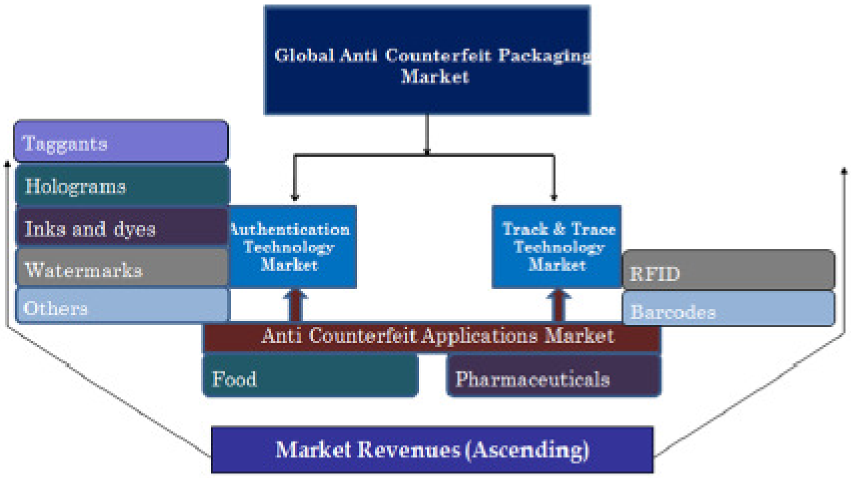

Global Anti Counterfeit Packaging Market
Taggants
Holograms
Inks and dyes
Watermarks
Others
Authentication Technology Market
Track & Trace Technology Market
RFID
Barcodes
Anti Counterfeit Applications Market
Food
Pharmaceuticals
Market Revenues (Ascending)

Figure 2.1-Comprehensive Market Segmentations (Bhardwaj & Shenoy, 2012)

Anti-counterfeit technology has been divided into two main categories which are authentication technology and track and trace technology. Food or daily essentials mostly adopt the authentication technology while pharmaceuticals, which matters life and death, adopts track and trace technology.

Taggants, holograms, inks and dyes, watermarks belong to the authentication technology while RFID and barcodes belong to the track and trace technology market. They are both used in global anti-counterfeiting packaging market.

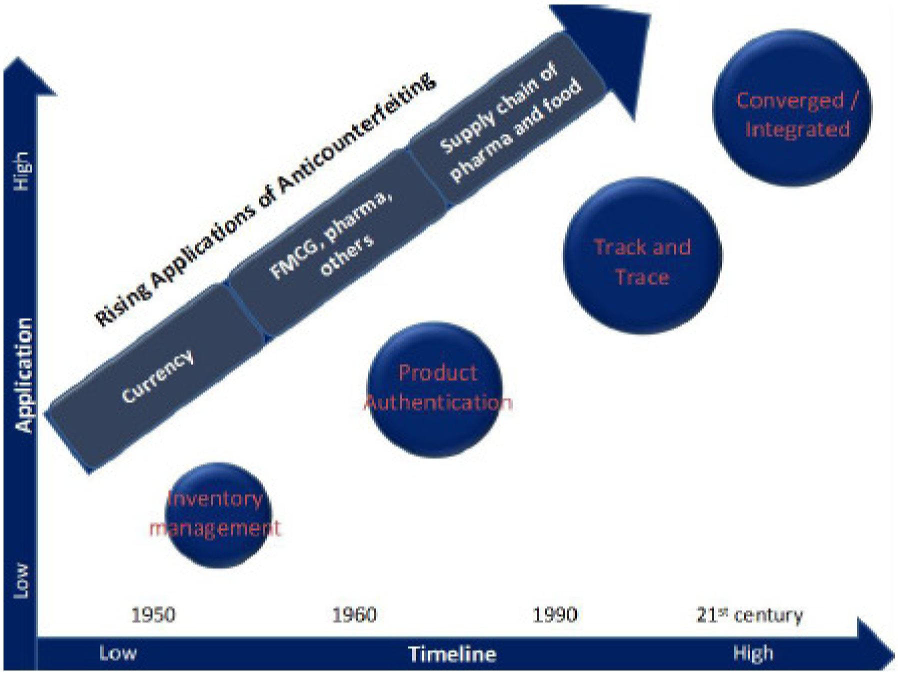


Figure 2.2-Anti-counterfeit packaging evolution (Bhardwaj & Shenoy, 2012)

The demand on the anti-counterfeit of public changes from time to time. In the 1950s, the society was focusing on the development of anti-counterfeit features on the currency, which is money note. The reason why they focused on currency is the blooming of globalization, multi-national trades were promoted at that time. Therefore, counterfeiters tried to fake the money note in exchange of products.

In 1960s, people started to realize that there was a need to authenticate the products, especially for pharmaceutical, before using them as the counterfeiting activities were getting intense. Researches at time focused on authentication technology.

During 1990s to 2000s, track and trace technology was started to be promoted and applied with the supply chain management. The improvement in information system has played an essential role in this major change.

Bhardwsj & Shenoy (2012), Bansal (2009), Malla (2010), Gudala & Pramill (2012), experts in anti-counterfeit technology, predict that converged and integrated technology will be the main trend for anti-counterfeiting in the future time.

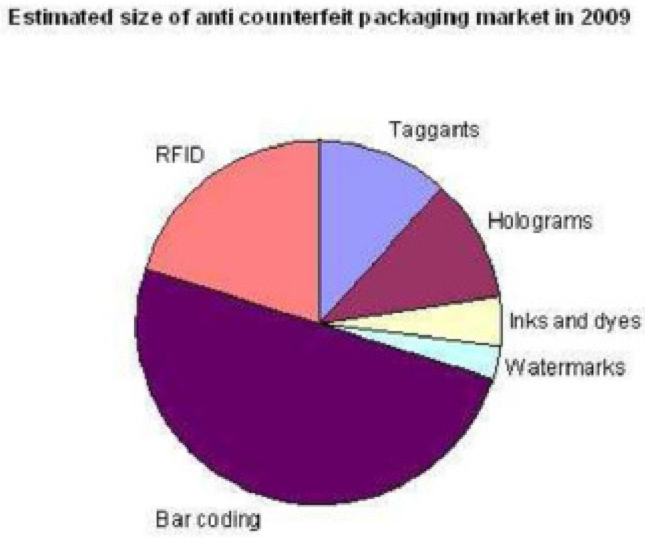


Figure 2.3-Estimated size of anti-counterfeit packaging market in 2009 (SecurPham, 2012)

By far, bar code owned the largest market share among all, which owns over half of the total market share. Followed by the RFID, 46%, it is expected to have the second largest share among all.

Taggants and holograms are expected to obtain similar shares, 29% because they require high investment cost which lead to a higher market entry. That is the major reason why taggants and holograms are having less market share then bar code's.

Iks and dyes and watermark are started to fade out. According to Securing Pharma (2012), USA has 45% of the total patents registered in anti-counterfeit technology followed by Europe with 31%.

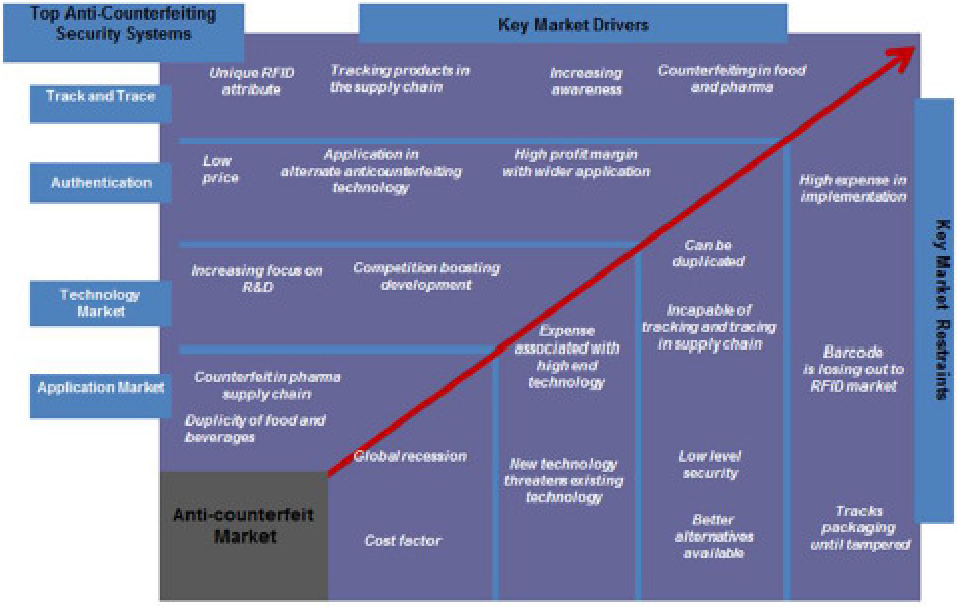

Top Anti-Counterfeiting Security Systems
Key Market Drivers
Track and Trace
Unique RFID attribute
Tracking products in the supply chain
Increasing awareness
Counterfeiting in food and pharma
Authentication
Low price
Application in alternate anticounterfeiting technology
High profit margin with wider application
High expense in implementation
Technology Market
Increasing focus on R&D
Competition boosting development
Can be duplicated
Incapable of tracking and tracing in supply chain
Expense associated with high end technology
Barcode is losing out to RFID market
Application Market
Counterfeit in pharma supply chain
Duplicity of food and beverages
Global recession
New technology threatens existing technology
Low level security
Anti-counterfeit Market
Cost factor
Better alternatives available
Tracks packaging until tampered
Key Market Restraints

Figure 2.4-Market Trend (Bhardwaj & Shenoy, 2012)

The diagram has investigated the key market drivers and key market restraints in different aspects. The diagram has well-explained the current market trend in anti-counterfeit issues.

In the application market, the counterfeit activities in pharmaceutical and food and beverages have provided market opportunities for anti-counterfeit application. However, the development of the application market has been restricted by the global economic downturn and the cost factor,

For the technology market, R&D starts to receive more focus from the researchers under competitive business environment. Companies are more willing to put resources in R&D, and this has facilitated the development of anti-counterfeiting technology. Moreover, the situation has resulted in high R&D expenses associated with high end technology of the company and the development of new technology might replace the existing, old and traditional technologies.

For authentication technology, the competitive pricing has won it a place in the market. It is easier to be applied in other alternate anti-counterfeiting technologies. Because of the low price, the companies are able to use them with high profit margin. However, the authentication technology fails to track and trace the product in supply chain. The security is very low under this technology. There will be better alternatives available in the market; the companies do not necessarily use this technology for anti-counterfeiting.

The track and trace technology is welcomed by the market out of the following reasons. First, the unique RFID attribute allows product authentication in individual level and product tracking in the supply chain. Researchers and the market are started to pay more awareness to this newly developed technology. It is proved to combat the counterfeiting in food and pharmaceutical significantly (Power, 2012).

However, there are few market restraints on the promotion of track and trace technology. First, it is very expensive. The implementation cost is very high, some SMEs cannot even afford it. Second, barcode, a type of track and trace technology, is gradually losing its market share. Third, the product cannot be traced when the package is tampered. Therefore, it is important to protect the chips.

2.3.2 RFID and NFC in Anti-counterfeiting

In this section, an overview of anti-counterfeiting approaches suggested by different scholars will be presented. An evaluation and categorization will also be provided in the followings.

The purpose of product authentication is to answer whether a given product is genuine or not. It helps defining the products are original or counterfeits. To do product authentication, it is necessary to insert a security feature, which can be a key factor to help authenticating the product, into a product and at the same time, this security feature have to be authenticated too to prevent any cloning. Therefore, RFID tag is fit for this purpose and fulfills the requirement of authenticating the security feature.

One concept has to be defined and explained first before the discussion of anti-counterfeiting approaches. The differences between RFID and NFC have already mentioned in the last section. However, it cannot be denied that RFID and NFC are very similar technologies, or even developed on the same concept.

The applications of RFID are mostly applicable on NFC with some configuration changes. Therefore, in this section, some RFID anti-counterfeiting approaches will be studied for the development of NFC anti-counterfeiting application.

Although RFID is not the only technology that can fulfill the requirement and be used as product authentication, it is the most cost-efficient way among all of them. Halogram, water mark, laser marking, barcode are traditional ways of production authentication, however, they do not have the competitive advantages that RFID has including non-line of sight reading, item-level identification, non-static nature of security features and resistance against cloning (Filimon, 2012). For instance, highly visible QR codes -which are also used in multiple anti-counterfeiting applications-, can be easily generated as they can be printed by any printers whereas RFID/NFC tags require specific machines to write data on them (Vazquez-Briseno, M. et al., 2012). As a result, QR codes are easier to copy than RFID/NFC tags.

Furthermore, the adoption of RFID/NFC tags can add high business value to whole supply chain and logistics activities of companies. Therefore, balancing the cost and the effectiveness, RFID is the most desire solution among all choices. Nevertheless, with the development and popularization of NFC technology, the end-users, or consumers, can participate in product authentication by using their cell phones. Actually, although NFC readers are not yet mainstream, analysts anticipate that NFC-enabled mobile phones will likely reach 863 million units by the end of 2015 (Frost & Sullivan, 2011)

Anti-counterfeiting approaches have been categorized into several types. They are specific features-based authentication, tag authentication, location-based authentication and weak authentication respectively (Filimon et al, 2012).

Specific features-based authentication is based on what the product is while tag authentication is based on what the product has and what the product know. Location-based authentication is based on the location – where the product is and where it has been to. Weak authentication is an approach which can be used for some cases which do not consider security as the first priority and an important issue because this type of authentication does not provide a comparable level of security with other three approaches.

Specific Features-based Authentication

The principle of this approach is to write a digital signature on the tag. The digital signature is made up of combination of the transponder ID number and product specific features of the item which is to be authenticated (Filimon, 2012). The feature can be physical or chemical, as long as it can identify and verify the product. For example, a very precise weight (Filimon, 2012). This approach is suitable for products which are hard to be cloned.

Measuring and verifying the chosen feature is part of the authentication process. The users, mostly customs, will first measure the actual special feature of the product needed to be verified and then he will compared the feature measured with the one stored in the digital signature from the tag. If it does not match with the digital signature, then the product is fake.

According to Lehtonen (2012), foure steps have to be taken in the process of product authentication by using Specific feature-based approach:

1. Obtain the product ID number by reading the tag tagged in the product.
2. Find the network address of the authorized server for the original product class.
3. Establish a secure connection with that authorized server.
4. Download the information for further manual authentication, that is, the information of the specific feature of the original.

With four steps taken, the user can physically measure the inspected product to determine whether the product is authentic or not. If the measure result mismatches the information downloaded, the inspected product will be considered as counterfeit.

The advantage of this approach is to have the tag cost low. It is because the focus is on the data, digital signature in this case, written in the tag, not the tag itself. The selection of tag is not important for the whole product authentication.

However, there are disadvantages too. Under this approach, the user has to physically verify the suspected product every time in the process of product authentication. This is very time-consuming.

The key success factor of this approach relies on the views of right-holders to share the authentication data on online servers with the customs of the customers for the verification (Lehtonen, 2012). If the right-holders are willing to share their authentication data, it means that the customs, or the customers, could rely on the timeline of the data and causes no delay. Moreover, if the customs and customers are allowed to share information of counterfeits detected to the authorized share, it will help the right-holders to protect their right.

Tag Authentication

This approach is suitable for the security feature, which is the tag itself, hard to be cloned. By the read-write encryption, the tag can be protected from cloning. This approach is totally relied on the encryption method for the tag. The current methods are cryptographic primitive protocol, symmetric and asymmetric encryption-based protocol and physical unclonable function-enabled protocol (Filimon, 2012). Since the cost and the computing resources of the tags are limited, the user has to strike a balance between security, cost and the authentication performance.

Lehtonen (2012) has pointed out 6 core processes that the tag authentication has to be taken in order to achieve the product authentication and high security at the same time:

1. Read the tag and identify the product

2. Find the network address of the authorized server for the original product class
3. Establish a secure connection with that authorized server.
4. Establish the authentication protocol used by the tags.
5. Automatically authenticate the tag by using the protocol obtained from step 4.
6. Verify the tag-product integrity

It does not need a high requirement on hardware of the interrogator as the authentication protocols can be made transparent for the interrogator during step 4 and 5. The authentication can be processed on the authenticated server which has been connected in step 3 so the reader is only responsible of showing the result sent from the back-end server.

One conceptual issue has to be clarified here: what the user does in previous 5 steps is to verify the tag itself, not the product itself. Therefore, step 6 is necessary in order to authenticate the product itself. Verification is necessary to confirm the authenticated identity (tag in this case) matches the physical product. If step 6 is not taken, any fake product equipped with the authentic tag can easily pass the verification.

However, although tag authentication can authenticate the tag itself, which cannot be achieved by specific feature-based authentication, the latter itself focuses more on the product itself. Tag authentication only provides brief verification on the suspected items by using the brief information given in the server.

Location-based Authentication

The principle behind this approach is, when the location of the original subject is known, it can easily find out the fake product when the location shown in the server does not match with the location that the people found this item. The location could be geographic like Hong Kong, Japan or step of processes such as distributing, assembling. The authentication method has made use of the track and trace capability, which is offered by RFID and NFC technology.

The advantage of this approach is less complexity in RFID tag. The right-holder could just write an identification number such as a unique ID number in the tag and leave the back-end server to record down the track of this number every time it passes through the tag readers.

The disadvantage of this approach is that location-based authentication can only be practical under this situation: "the location of genuine products can be followed with a high enough degree of spatial and temporal granularity" (Filimon, 2012). Therefore, it is hard for the right-holders to collect all tracking information from the complicated supply chain.

If the current location of the product is unknown, the users, customs and consumers in this case, can only rely on the estimation provided by the system to verify and authenticate whether the product is counterfeit or not.

Weak Authentication

This approach is the simplest authentication technique among all four approaches. The process only involves a unique serial numbering and confirmation of the identity.

The security only focuses on keeping the valid unique serial number away from the counterfeiting and not to let them get it. If the counterfeiter gets the list containing valid product ID, they can pass the authentication test.

One way to secure the unique product ID number is to assign the product number randomly from a large ID number database. Therefore, the counterfeiters would be very difficult to find and guess the product ID number to be used for their fake goods.

In this approach, some customer-driven initiatives are proposed (Filimon, 2012). The basic idea behind this approach is to let consumers to discover the counterfeits and share their experience and information with other consumers. Therefore, when other know about the shops (which sell the counterfeit), they will avoid buying in that shop again.

However, one of the difficulties on implementing this approach is that this core algorithm behind has over-relied on the fact that the customers have a certain level of knowledge to verify whether a product is counterfeit or not.

Its technical realization depends on two assumptions (Filimon, 2012):

1. Enable Item-level tagging on products
2. Consumers have a certain level of technical knowledge to use the reader (or NFC-enabled phone) to read the tag, understand the information and interact with the back-end server database.

The benefit of this approach is lower cost compared with other three approaches. If the supply chain is RFID-enabled, it just needs to operate this approach. Besides, this approach has strongest ability to spoil the business of counterfeiters as customers are involved in reporting the shops which are selling counterfeits.

However, it brings little value on the whole supply chain under this approach as the written data is not enough for assisting the whole supply chain operation. It just helps authenticating the inspected products.

2.3.3 Security in RFID and NFC-based Systems

It cannot be denied that it is impossible to cease all counterfeit activities by using RFID. It is impossible to cease all counterfeit activities by all means. We can just reduce it. Therefore, the key goal of RFID/NFC anti-counterfeiting is to change the risk-return profile for the counterfeiters – raising the risk and thereby minimizing the return and then cut down their counterfeit activities themselves.

European Commission (2012) has listed the general requirement of a product authentication system:

1. The system is allowed to be used in multiple locations by multiple parties.
2. The cost and effort to perform a product authentication should be low, or fairly low
3. The optimal solution should let consumers to participate in the product authentication.
4. The product authentication should have an appropriate security level.

As different products require different level of security, cost-to-break (CTB) is one of the measures to quantify the level of security. CTB is the lowest expected cost for anyone to discover and exploit a vulnerability of one particular system (Michahelles et al, 2012). The measurement helps to find out the amount of security needed to stop a criminal to do the illegal activities. This amount of security needed can be depended on the probability of the criminals getting caught while they are doing their criminal activities. Security level of product authentication can be determined by how it fulfills derived with misuse cases functional and non-functional security requirements (Filimon, 2012).

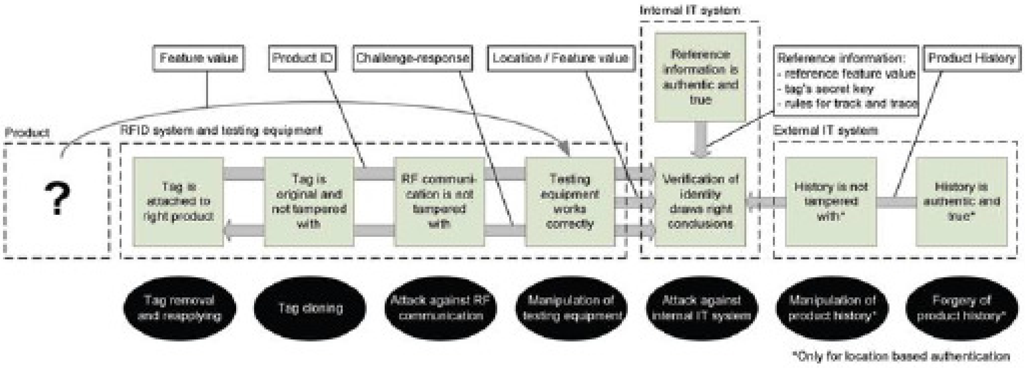

Internal IT system
Feature value
Product ID
Challenge-response
Location / Feature value
Reference information is authentic and true
Reference information:
- reference feature value
- tag's secret key
- rules for track and trace
Product History
Product
RFID system and testing equipment
External IT system
?
Tag is attached to right product
Tag is original and not tampered with
RF communication is not tampered with
Testing equipment works correctly
Verification of identity draws right conclusions
History is not tampered with*
History is authentic and true*
Tag removal and reapplying
Tag cloning
Attack against RF communication
Manipulation of testing equipment
Attack against internal IT system
Manipulation of product history*
Forgery of product history*
*Only for location based authentication

Figure 2.5-Chain of trust (rectangles) and threats against (ovals) RFID-based product authentication system (Filimon, 2012)

The above figure has illustrated the chain of trust of a general RFID-based product authentication system under location-based authentication approach. Every step in this chain of trust could be an attack point against this system. This chain helps to find out general attack point to be secured.

Taking the step of "Tag is attached to right product" as an example, there is a threat that the tag could be removed and reapplied by someone, making the data recorded in the server inaccurate. Tag cloning is possible under the step of "Tag is original and not tampered with", therefore, if the tag cloning is successful, the tag would be misused by counterfeiters.

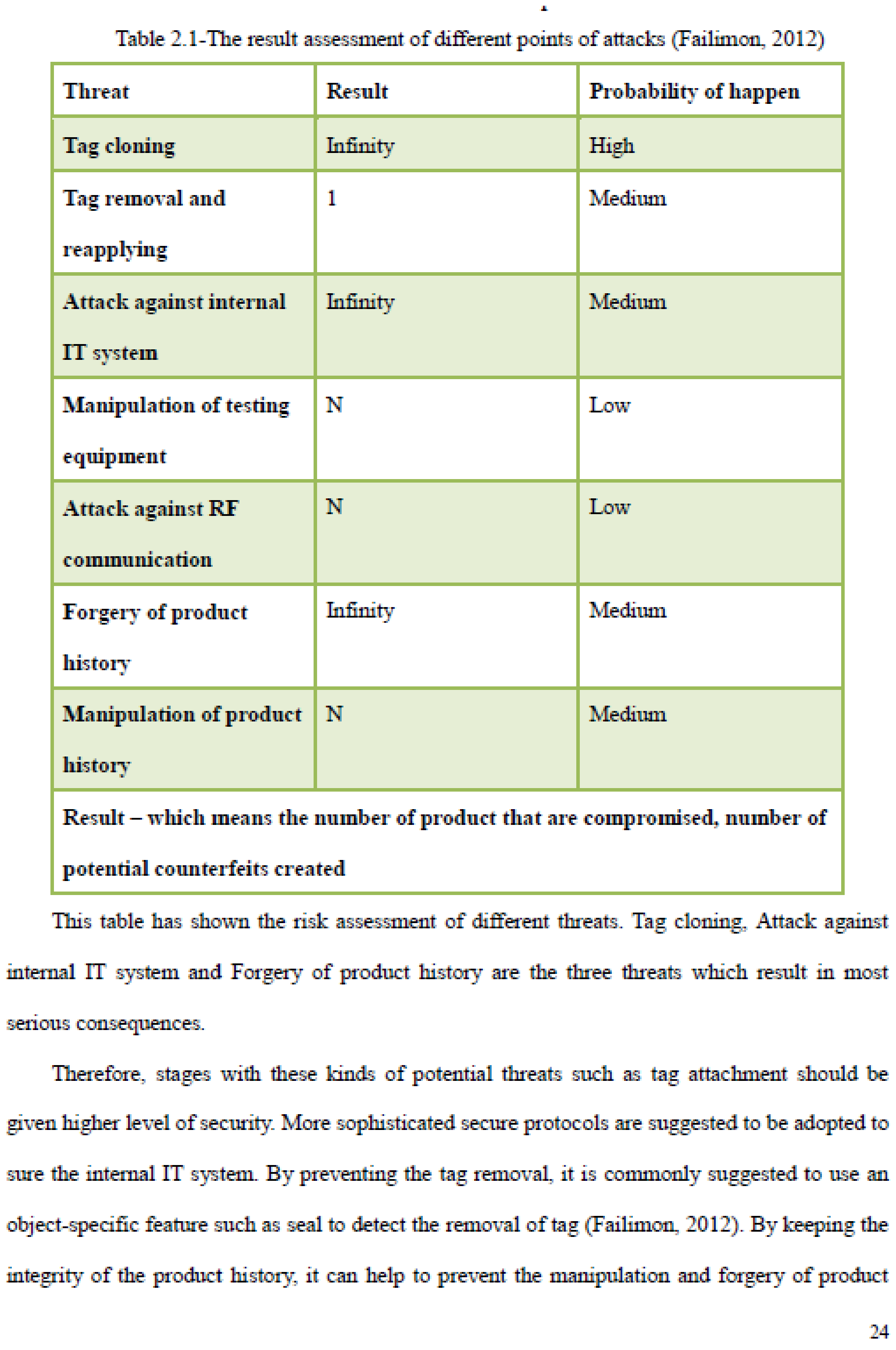


Table 2.1-The result assessment of different points of attacks (Failimon, 2012)

Threat	Result	Probability of happen
Tag cloning	Infinity	High
Tag removal and reapplying	1	Medium
Attack against internal IT system	Infinity	Medium
Manipulation of testing equipment	N	Low
Attack against RF communication	N	Low
Forgery of product history	Infinity	Medium
Manipulation of product history	N	Medium
Result – which means the number of product that are compromised, number of potential counterfeits created		

This table has shown the risk assessment of different threats. Tag cloning, Attack against internal IT system and Forgery of product history are the three threats which result in most serious consequences.

Therefore, stages with these kinds of potential threats such as tag attachment should be given higher level of security. More sophisticated secure protocols are suggested to be adopted to sure the internal IT system. By preventing the tag removal, it is commonly suggested to use an object-specific feature such as seal to detect the removal of tag (Failimon, 2012). By keeping the integrity of the product history, it can help to prevent the manipulation and forgery of product history.

Table 2.2-Comparison of different approaches towards cost, cloning and checking complexity (Filimon, 2012)

Approach	Complexity of check	Cost of tag	Cloning resistance	Clone detection	Tag reapplying resistance
Specific feature-based authentication	High	Low	Yes	No	Yes
Tag authentication	Medium / High	Low / High	Yes	No	No
Location-based authentication	Medium / High	Low	No	Yes	Yes
Weak authentication	Low	Low	No	No	No

For specific feature-based authentication, it is suitable to use at the product itself hard to be clone, therefore, the security can be on the difficulty of the cloning of the specific features. According to the cost to break principle mentioned in the last part, the cost to clone the unique features from genuine products to make another counterfeits carrying those unique features would be a burden for the counterfeiters. However, this approach has one loophole, which is no clone detection. This means that if the counterfeiters overcome with the burden, the cost and the technique, the right-holders cannot be notified their products and tags have been cloned.

For the tag authentication, it has no clone detection too. Also, it does not have any tag reapplying resistance which means that the tag can be re-applied. This causes a security threat for the counterfeiters to use it over and over again. The cost of implementing tag authentication varied on the complexity of checking and the selection of tag.

Location-based authentication does provide clone detection and tag reapplying resistance. As the tracking record of the genuine products is provided by the right-holders, counterfeits can be obviously found when the tracking record mismatch its current location. However, this approach does not have cloning resistance. The counterfeiters can clone the tag very easily. This approach focuses on the data recorded down in the server from the tag, not the tag itself.

Weak authentication is weak among all approaches. No cloning resistance, no clone detection and no tag reapplying resistance. However, the implementation cost is the lowest among all. Weak authentication just provides a unique identity number and a tag containing that ID number. It is the easiest and simplest way for product authentication.

2.4 Chapter Summary

Summarized from the above literature reviews, the root causes and consequences of counterfeiting activities have been studied in the former part, which further stresses the need of an effective anti-counterfeiting measure to tackle this difficult situation.

In the second part, an in-depth study of current anti-counterfeiting technologies has been conducted for the purpose of better addressing the counterfeiting activities. The market trend of the future anti-counterfeiting technology development, competitive advantages of different types of anti-counterfeiting technology have been analyzed, together with the technical analysis of some common technologies.

The literature reviews has specifically focused on RFID and NFC, the former is the origin of NFC while the latter is the focus of the application developed in the project. Different RFID anti-counterfeiting approaches have been studied and evaluation for the study of feasibility of NFC in anti-counterfeiting. The security of RFID and NFC system is also studied for the purpose of maximizing the cost-to-break of counterfeiters by the application.

Chapter 3 – Methodology

The ultimate goal of the project is to develop an effective anti-counterfeit application for the designer bag industry. Before the start of the project, a clear workflow has to be designed for the project organization. The content has to be decided in this chapter too.

3.1 General Structure

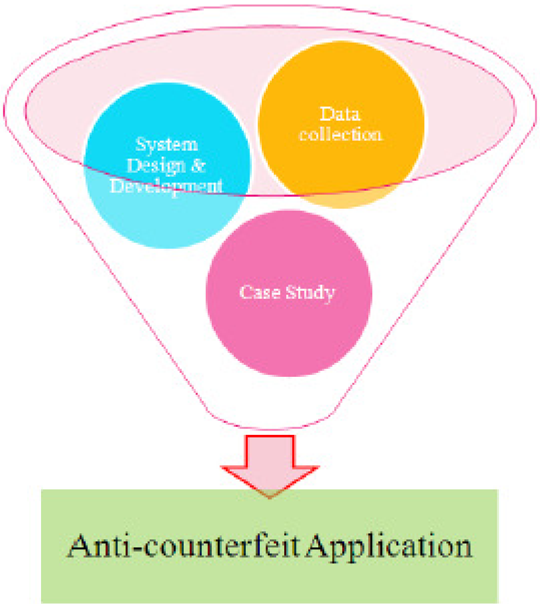


Figure 3.1-General Input and Output for the project

The diagram above has shown the general workflow for the project. It is undoubtedly that the anti-counterfeit application is the core of this project. All the efforts and researches done are for developing an effective application. Therefore, the final output will be the application.

There are three main inputs in this project. Data collection is one of the major tasks. Without collecting data from the journals, researches, theses, reports and even news, the application designed cannot well-target the root problem that causing the counterfeit so prevalent. If the application cannot address the problem well, it is useless and ineffective.

The second major input is system design and development. The anti-counterfeit system has to be designed with proper system architecture, right choice for the equipment and interface design before actual development. The framework has to be decided before constructing any program. When the system framework is decided, construction of the program can be started.

Case study refers to the study of information given by Coach, a reputable designer-brand bag manufacturer which has revenue-sharing contract with that brand. The data given by Coach will be applied in the trial-run of the application. Also, cost estimation of the project will be done based on the information and forecast of the manufacturer.

With only all these three elements together, the application is considered to be completed.

3.2 Project Workflow

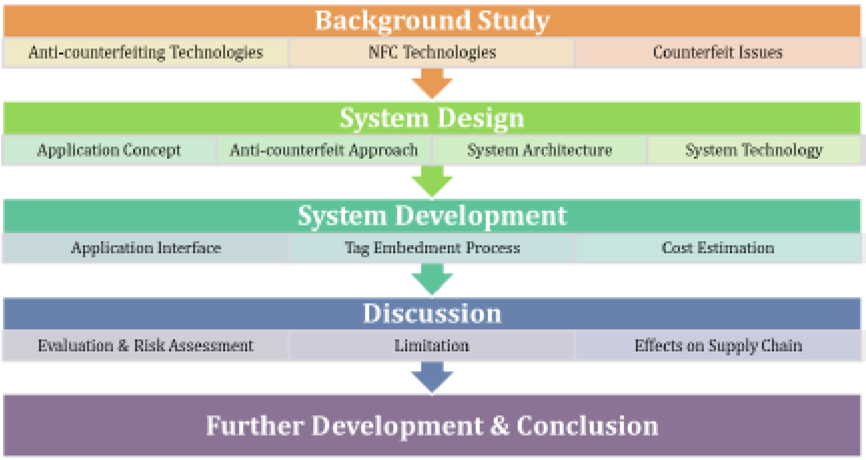


Figure 3.2-Project Workflow

The above diagram has shown a more detailed project workflow compared with the previous diagram. The former is more general. The project will be generally divided into five parts which are data collection, system design, system development, discussion and conclusion with further development.

Data Collection

There are three major elements in the data collection part. The data collected are mostly categorized into three major categories which are anti-counterfeiting technology, NFC technology and counterfeit issues.

The study in other current anti-counterfeiting technology is essential in the application development. It makes the competitive advantages owned by NFC technology clearer. Also, it helps better differentiation between NFC and other anti-counterfeit technologies.

The study of NFC technology is a must in this project as the core of the application is NFC technology. In-depth understanding in NFC allows better utilization of NFC in the application which could make it more effective and accurate.

Information on counterfeit issues gives a clear and better view on the today's world situation which could help greatly in the system design for better addressing the problem. Also, it also raises an alarm that the seriousness of counterfeit activities.

System Design

The application concept has to be stated clearly before the start of system design. It helps better positioning and sharping of the application. The application will be developed according to the concept stated.

The anti-counterfeit approach used in the application will be designed. It is different from the anti-counterfeit application. For figure of speech, the approach is a 'soul' while the application is the 'container'. The approach is used to determine the authenticity of the bag and the application is a set of interface showing the necessary information and instruction to the users. Therefore, it is necessary to design the approach first before developing the application.

System technology refers to the necessary setting for the anti-counterfeit project. The configuration is necessary in the application development while system architecture refers to the structure of the application.

System Development

A real demo will be shown in this part. It will analyze the application from the user's point of view. The application interface will be extracted from the demo and shown in the report. All data used in this part is all provided by the manufacturer.

Tag embedment process will also be designed for the manufacturer. It will suggest how manufacturer can embed the tags into the bags during the manufacturing process. The tag embedment process will be developed according to the manufacturing workflow of that manufacturer.

Cost estimation will also be done in this part. The forecast data is given by the manufacturer too. It will estimate how many resources and how much investments needed to be put in the project. Returns on investment and payback period will also be calculated in this part.

Discussion

Risk assessment of the application will be done to evaluate the effectiveness. Comparison of other approaches with the approach developed in the project will also be shown to compare their capabilities in dealing the potential security threats. This is another type of evaluation.

Limitation of the application will also be discussed. Although the application developed may have competitive advantages over the others, there are some shortcomings at all. The discussion on limitation allows rooms for further improvement.

As the application has placed influences on the supply chain, it is essential to discuss the effects placed on different stakeholders. The stakeholder involves retailer, customer, manufacturer and the brand owner. Different effects placed on the stakeholders may affect the implementation of the application.

Conclusion and Further Development

Further development refers to the further exploration on the potential of the application. The application not only can be used for anti-counterfeiting purposes, but also can be used in other aspects such as marketing. Customer-relationship management is a desirable aspect for the further development. Thus, in this section, different concept other than anti-counterfeiting will be suggested and discussed. Although they have not been implemented in this project, it is possible to investigate in future researches.

3.3 System Design

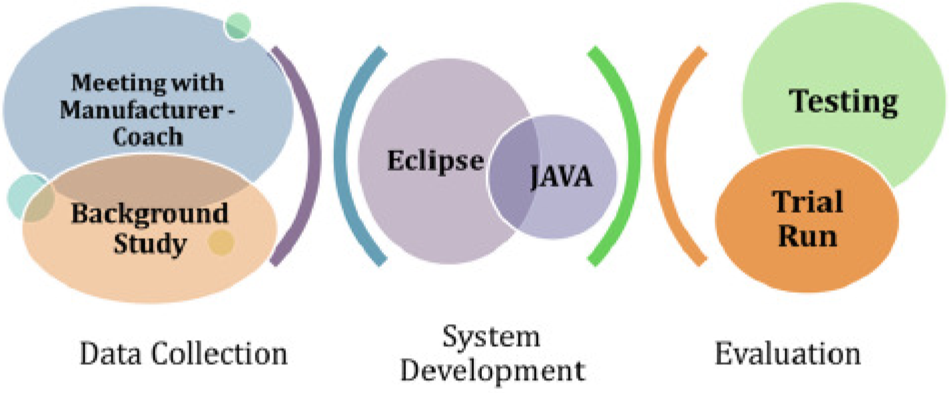


Figure 3.3 Designs and Development

It is necessary to collect data from the designer bag manufacturer for the design of the application. Background study should also be conducted to investigate the root causes of the counterfeiting activities for better addressing the problem. It is also required to study the current anti-counterfeiting technologies, such as bar code and laser printing, for developing an effective anti-counterfeiting application.

The NFC-based mobile application will be written in JAVA language and developed by Eclipse, programming software. Eclipse is the most common software in constructing Android application.

The evaluation will be done by having application testing and trial run. The effectiveness and result will be evaluated by different perspectives, including risk assessment, cost estimation.

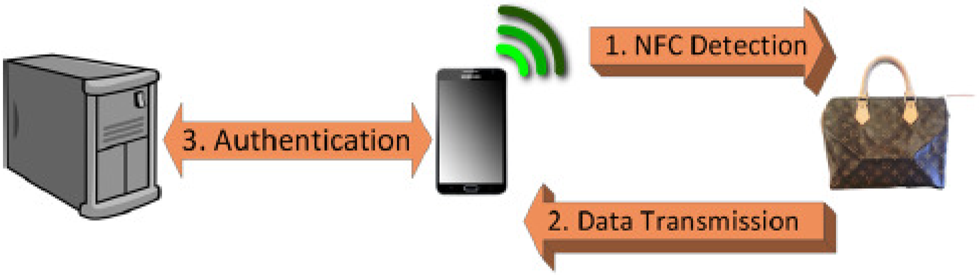


Figure 3.4-General flow of Anti-counterfeit Application

A general flow of the application has been shown by the diagram above. The concept of the application is to allow user to use their smart phone to detect and read the NFC tag embedded inside the bag.

The application will thereby obtain the information and data stored in the tag and then transfer back to the clouding server for authentication. Once the server has received the information and data sent from the application, it then will start to authenticate the product according to the information received.

When the server has finished the authentication, it will soon send the authentication result back to the application. Thus, the application will show the result to the user once it receives the result sent from the server. The authentication process is over.

The whole authentication process is completely relied on the clouding server placed in the I.T department in the company. The application will only act as a bridge for the communication between the server and the tag. Therefore, the core will be the server.

Chapter 4 – System Design and Development

This project aims at developing an effective and reliable NFC-based anti-counterfeit application for designer bag manufacturers. This chapter will be divided into six sections, which are application concept, hybrid approach, system accessories and system architecture.

In the first section, the application concept will be defined, which limits the uses and functions of the application. The application will be developed according to the concept defined.

The second section will introduce the original anti-counterfeit approach designated for the mobile application. Algorithm of the approach will be explained in this section. The security layers of the approach will also be analyzed.

Mobile requirement for the application will be listed out in the third section. This is the basic requirement for the mobile to run the anti-counterfeit application. Hardware requirement for server will also be listed for company to run the authentication program

System design and architecture will be explained in the fifth section. Authentication process and application structure will be presented. It will also include the structure of authentication server and database.

4.1 Application Concept

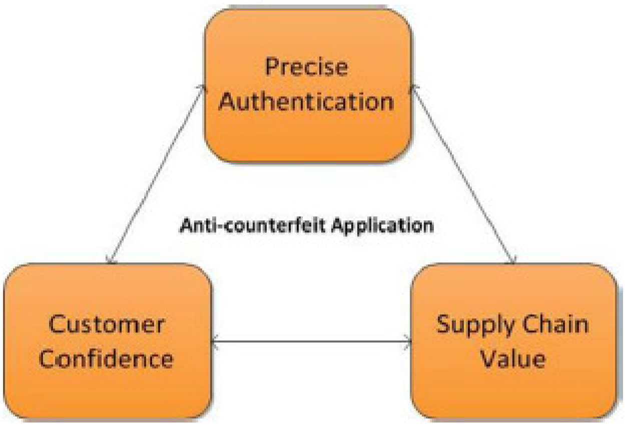


Figure 4.1 Conceptual Framework of the application

33

There are three objectives for the anti-counterfeit application. These objectives have molded the prototype of application. The application has to achieve the following expectations:

1. To provide precise authentication for the potential customers. The application should be able to authenticate both first hand and second hand designer bag. It should also contain resistances to different external threats such as tag cloning and manipulation of tag information.

2. To increase customers' confidence in buying genuine designer bag. The application is designed as company-based. Therefore, the application is designated for one company's products. Other designer brands' products cannot be authenticated by the application. With products' genuineness guaranteed by the application, the customer confidence will be increased.

3. To add value to the company's supply chain. The application brings integration of information system and supply chain management. It helps the company to have better control of the flow of products and make better strategic decisions by assigning tags to each product.

The anti-counterfeit application will be constructed under these three main objectives.

The characteristics of the application determine the system accessories and application configuration. To fulfill the three objectives of the application, the characteristics have been positioned as the following:

1. The application is allowed to be used in multiple locations

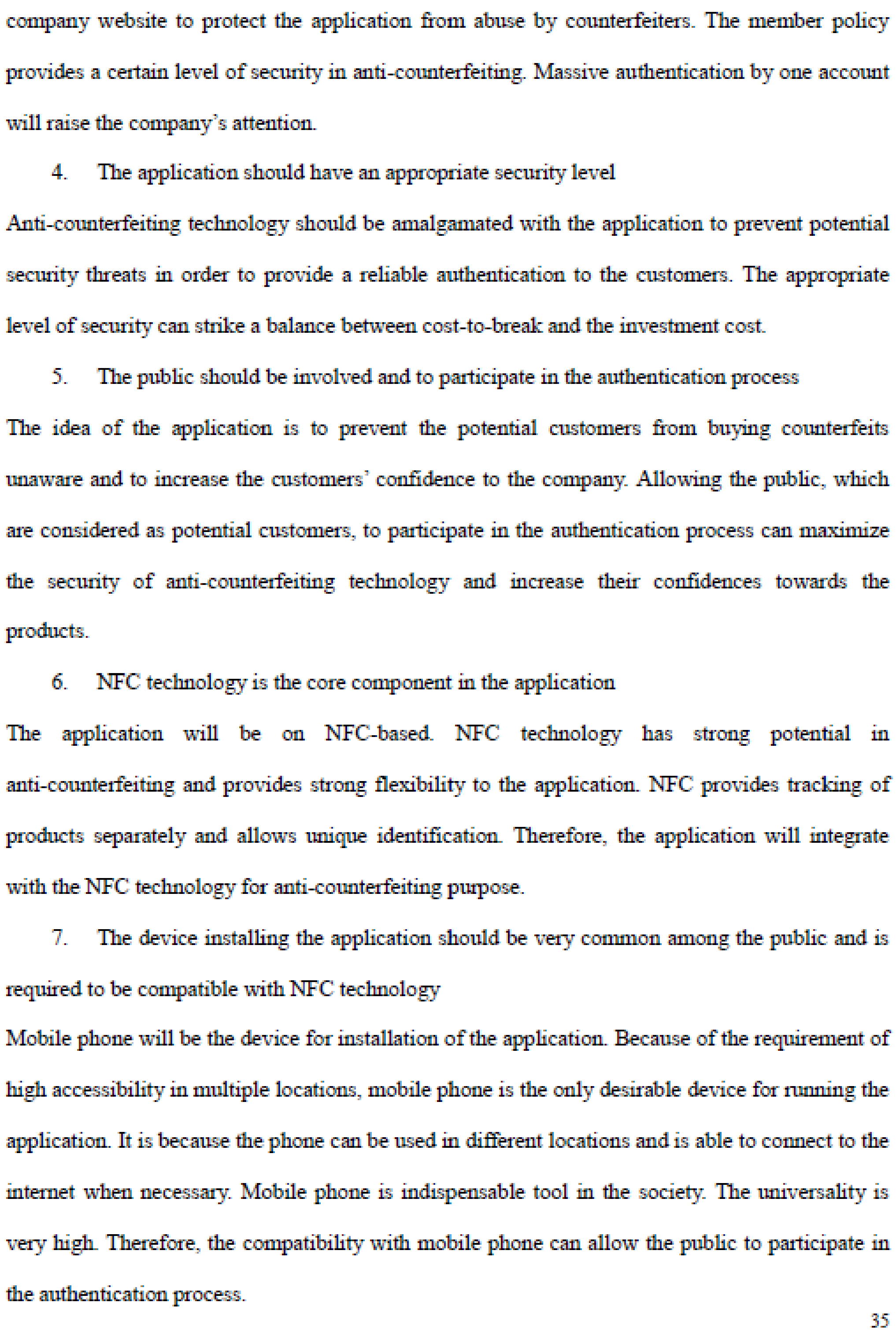
The application is designed to be portable. It can be used when there are products needed for authentication. The common location for using this application will be retail shops, auction sales, booths and boutiques. High accessibility is allowed by the application

2. The application is allowed to be used by multiple parties

The application does not limit the user entry. The entry requirement of the application is very low therefore it can be used by multiple parties. The authorized level is equivalent to all users, they are treated equally in the application.

3. The application adopts membership policy

The application requires users to first register an account from the brand owner through the



company website to protect the application from abuse by counterfeiters. The member policy provides a certain level of security in anti-counterfeiting. Massive authentication by one account will raise the company's attention.

4. The application should have an appropriate security level

Anti-counterfeiting technology should be amalgamated with the application to prevent potential security threats in order to provide a reliable authentication to the customers. The appropriate level of security can strike a balance between cost-to-break and the investment cost.

5. The public should be involved and to participate in the authentication process

The idea of the application is to prevent the potential customers from buying counterfeits unaware and to increase the customers' confidence to the company. Allowing the public, which are considered as potential customers, to participate in the authentication process can maximize the security of anti-counterfeiting technology and increase their confidences towards the products.

6. NFC technology is the core component in the application

The application will be on NFC-based. NFC technology has strong potential in anti-counterfeiting and provides strong flexibility to the application. NFC provides tracking of products separately and allows unique identification. Therefore, the application will integrate with the NFC technology for anti-counterfeiting purpose.

7. The device installing the application should be very common among the public and is required to be compatible with NFC technology

Mobile phone will be the device for installation of the application. Because of the requirement of high accessibility in multiple locations, mobile phone is the only desirable device for running the application. It is because the phone can be used in different locations and is able to connect to the internet when necessary. Mobile phone is indispensable tool in the society. The universality is very high. Therefore, the compatibility with mobile phone can allow the public to participate in the authentication process.

8. Server authentication and manual authentication are both implemented in the authentication process

To provide precise authentication, both types of authentication are adopted to tackle any possible potential threats. Server authentication eliminates the low level technology-enabled counterfeiters from copying the products while the manual authentication can tackle the high-end counterfeiters with irreplaceable material used for the products and unclonable physical anti-counterfeiting features. The implementation of server and manual authentication can maximize the authentication accuracy.

9. Simple, fast and precise are the core values of the application

The application aims at providing a reliable and precise authentication to the users, which are potential customers, by a simple application with clear instruction in a very short processing time. These three core values represent the competitive advantages of application compared with other anti-counterfeiting technology.

4.2 Algorithm - Hybrid Approach

Hybrid approach is the original anti-counterfeiting approach developed in this project. It is designated for the NFC-based anti-counterfeiting application. This approach applies the key concepts of four approaches introduced in the previous section. They are specific features-based approach, tag authentication approach, location-based approach and weak authentication approach.

The hybrid approach amalgamates and integrates them into one. It provides synchronized secret, serial number, manual authentication and e-pedigree. To conclude, this hybrid approach contains four layers of security for the authentication purposes.

4.2.1 Synchronized Secret

Synchronized secret is the well-developed and common method to secure tags from cloning by low cost. This method focuses on the rewritable memory of the tags. The tag will contain a set of dynamic number in the rewritable memory that will be changed every time when it is detected by a genuine reader. That set of dynamic number is called synchronized secret. The synchronized secret stored in the tag can also be considered as one time token that will be updated synchronously in the back-end system. The database will keep track of the synchronized secret that is written on the tag to detect any synchronization errors.

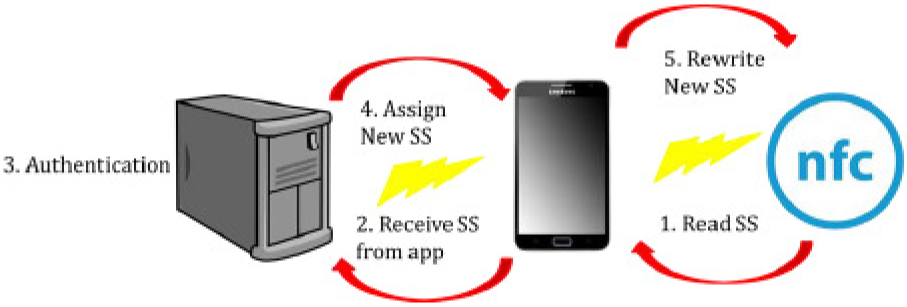


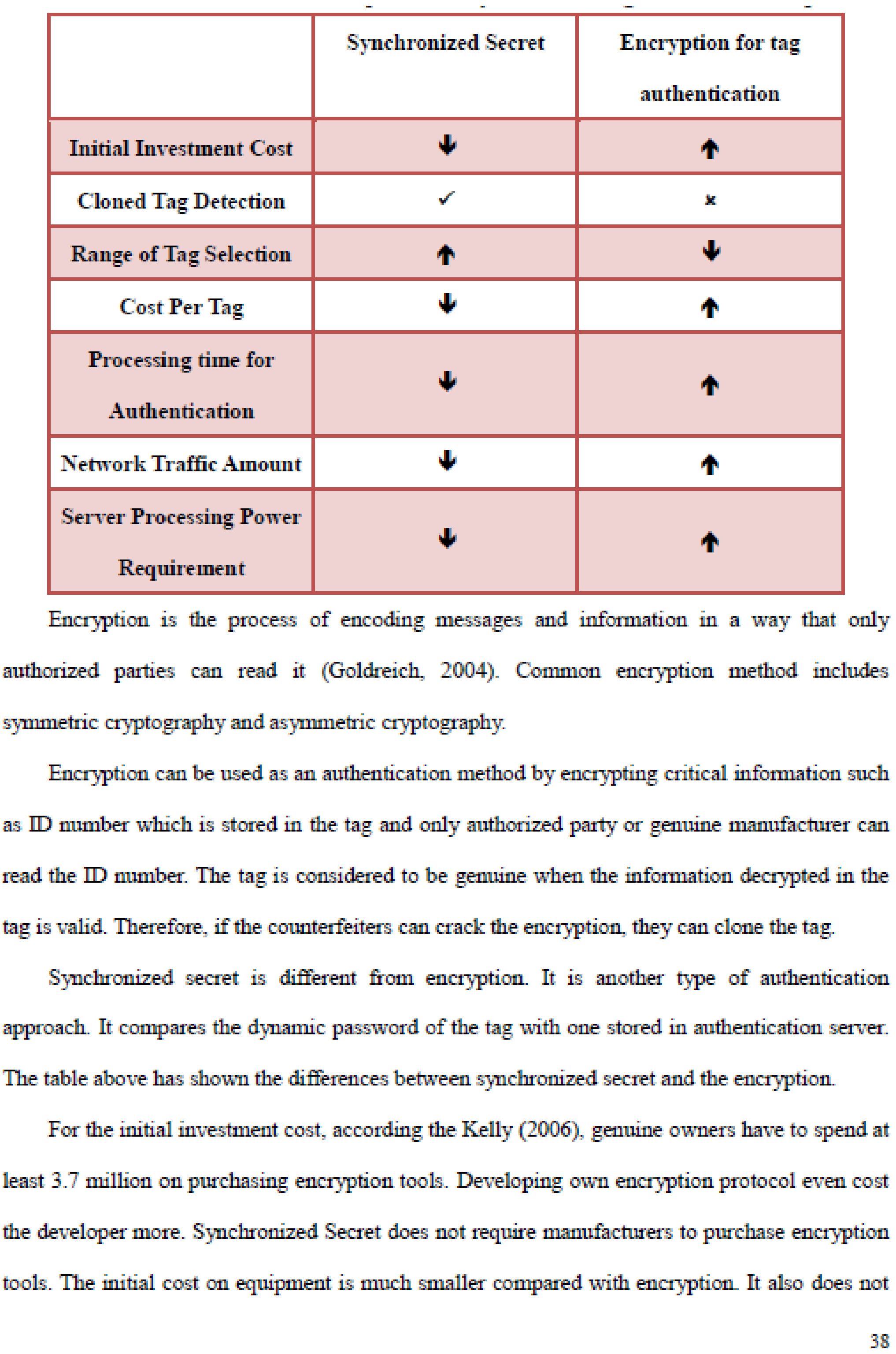
Figure 4.2-Synchronized Secret Procedure

In this application, when the NFC tag reader identifies and reads the NFC tag embedded in the bag, the authentication server will first verify the tag's static identifier, which is the unique ID number of the tag, if the ID is valid, the authentication server will then compare the synchronized secret stored in the tag with the one recorded in the database, if they are matched, the tag is considered to be valid and passes the first check. If they are different, synchronization error is detected and alarm will be triggered, the tag will be considered as cloned tag in the aspect of tag authentication, the alarm will be shown in both application and database server.

Comparison between Synchronized Secret and Encryption

In tag authentication, the common approach is using encryption to authenticate the tag. However, the results are various. Synchronized secret is the recent research development. It is proved that it can authenticate the tag effectively and provide cloned tag detection in different researches. The table below has shown the comparison of synchronized secret and encryption.

Table 4.1-Comparison of Synchronized Secret with Encryption in different aspects



	Synchronized Secret	Encryption for tag authentication
Initial Investment Cost	↓	↑
Cloned Tag Detection	✓	×
Range of Tag Selection	↑	↓
Cost Per Tag	↓	↑
Processing time for Authentication	↓	↑
Network Traffic Amount	↓	↑
Server Processing Power Requirement	↓	↑

Encryption is the process of encoding messages and information in a way that only authorized parties can read it (Goldreich, 2004). Common encryption method includes symmetric cryptography and asymmetric cryptography.

Encryption can be used as an authentication method by encrypting critical information such as ID number which is stored in the tag and only authorized party or genuine manufacturer can read the ID number. The tag is considered to be genuine when the information decrypted in the tag is valid. Therefore, if the counterfeiters can crack the encryption, they can clone the tag.

Synchronized secret is different from encryption. It is another type of authentication approach. It compares the dynamic password of the tag with one stored in authentication server. The table above has shown the differences between synchronized secret and the encryption.

For the initial investment cost, according the Kelly (2006), genuine owners have to spend at least 3.7 million on purchasing encryption tools. Developing own encryption protocol even cost the developer more. Synchronized Secret does not require manufacturers to purchase encryption tools. The initial cost on equipment is much smaller compared with encryption. It also does not require manufacturers to put computational resources on developing encryption protocol. Therefore, synchronized secret is much more suitable for the manufacturers who have limited budget.

For the cloned tag detection, synchronized secret offers detection of cloned tag by triggering alarms when the one time token stored in the tag does not match with the one stored in the database. However, for the encryption, it does not offer any clone detection, it is only responsible of hiding the critical information from the unrelated and unauthorized party. If the counterfeiters clone the tag successfully, the genuine manufacturers will not notice any cloned tag.

There are more types of tag can be chosen in the synchronized secret approach. Low-cost NFC and RFID tag can be used in this approach. Passive tag can also be used under this approach. However, for the encryption, some low cost tags cannot be chosen because of the limited capacity of the tag. Encryption requires more capacity to store the cipher text content. Less range of tags is available for the encryption.

Cost per tag is much higher than that of tags under synchronized secret approach. Encryption requires tag with higher processing power. The cost of tag itself is already higher than those adopting synchronized secret. The manufacturers are also required to encrypt every tag, thus, the variable cost is higher than just that of inputting data into the tag.

The processing time for authentication is shorter under synchronized secret. The authentication server only needs to validate the static identifier of the tag and compare the one time token of the tag with the database's. However, the encryption requires the authentication server to read the cipher text first, and decrypt the cipher text, it may take around 30 seconds to decrypt the message if simple encryption method such as symmetric cryptography is taken (Kelly, 2006). The processing time varies from the sophistication of the encryption method.

During the authentication process, the user needs to connect his mobile phone to the internet. Synchronized secret consumes less network traffic than encryption. It is because during the authentication, the application only needs to transfer the UID of the tag and the one-time token to the authentication server, if the tag is genuine, the authentication server will send back another dynamic password to the application. However, the encryption method requires the application to send back the cypher text to the server, the text file is much larger than the synchronized secret and UID. After decoding the text file, the authentication server is also required to send back the decrypted file to the application. The whole process consumes more network traffic amount.

The processing power requirement of the server varies from different methods. Synchronized secret requires lower processing power than encryption method. It is because the former does not need the server to do decryption work. If there are large amount of cypher text files needed to be decoded at one time, bottleneck problem will be occurred in the server with lower processing power. Therefore, under encryption approach, it is commonly required server with high processing power.

To conclude from the above assessment, synchronized secret is more suitable for the mobile application. The low investment and variable cost allows more small to middle enterprises (SMEs) to join the NFC anti-counterfeit mobile application. The low network traffic amount and processing time attract more users to use this application. The cloned tag detection allows manufacturers to locate the cloned product.

4.2.2 Serial Number and Specific Features

In this hybrid approach, the second and third layers of security are serial number and specific features. In this approach, the synchronized secret and e-pedigree are independent, they work individually. Their results are individually accessed. However, serial number and specific features are inter-related. Their results are not individually accessed. They are a chain.

Serial number is unique ID number for each product. It is different from the unique identifier used in the synchronized secret. The unique identifier is the unique ID number of the tag, not the product itself. The serial number is the unique ID number of the product itself.

In this stage, the application will first read the serial number and the unique identifier stored in the tag and then send them back to the authentication server. If the serial number and the unique identifier are validated and matched with the database record, the authentication server will send the information containing critical information, which is the information about specific features of that product, to the application and show the information to the users for further manual authentication.

The serial number will not be shown during the authentication process to prevent any leak of serial number to the counterfeiters. The application will show validation result of the serial number. Also, if the serial number does not match with the record in database, the user is not able to continue the specific-feature authentication.

Comparison of Serial Number and Digital Signature

It is different from the traditional specific-feature authentication. The traditional specific-feature authentication focuses on the use of digital signature while the hybrid approach will focus on serial number. The reason of choosing serial number to establish the connection to the authentication server is the cost burden of the manufacturers and the low price/performance ratio.

The synchronized secret stored in the tag is already used as tag authentication; therefore, using digital signature to authenticate the tag itself is a replicate act. It cannot be denied that the authentication accuracy will be increased. However, the authentication accuracy will not be significantly improved if digital signature is adopted. It is because the application does have other four layers of security to assure the authentication accuracy. Adding digital signature will slightly increase the accuracy only. Also, this replicate act will result a collision with the principle of cost-to-break.

The cost-to-break principle aims at discovering the lowest expected cost for anyone to discover and exploit a vulnerability of one particular system (Lhtonen et al, 2012). Therefore, during application development, as long as satisfactory authentication accuracy rate is guaranteed, the developer should adopt the lowest developing and operating cost for the application.

Therefore, in this application, manual authentication, tag authentication, e-pedigree and serial number are enough for one authentication, the authentication accuracy is guaranteed. Second, adding digital signature will not improve the application significantly. Third, developing digital signature for each product consumes large amount of resources, including computational and manual resources, the development and operation cost are very high. The price/performance ratio will be very low.

To conclude, digital signature is considered not suitable for this NFC-based anti-counterfeiting application. Serial number and the unique identifier are enough for establishing the connection to the authentication server.

Manual Authentication

The specific features authentication is the third layer of security which will be triggered after the product passes the serial number authentication. It is a type of manual authentication. In this stage, human interference is inserted for the security.

Users are provided with detailed information about the anti-counterfeiting features of the products, in this study, it would be designer bags. There are pictures showing the anti-counterfeiting features of the bags such as the inner bag logo, the sewing style and the leather textures. The users can further authenticate the bags based on the pictures and information provided. A secure connection to the server will be established during the specific features authentication.

The manual authentication further enhances the authentication accuracy by authenticating the physical features of the products. The full reliance of the NFC tag in the authentication may cause a potential risk that the authentication will be inaccurate if there is any vulnerability of the authentication system. With the inspection of physical anti-counterfeiting features included during the authentication process, it can avoid the unnecessary risks brought by the full reliance on the tag. Also, the difficulty in 1:1 forgery of physical anti-counterfeiting features further significantly increases the risk-return profile for the counterfeiters.

Therefore, with the manual authentication included in the authentication application, the cost-to-break for the counterfeiters will be hardly afforded. The risk for selling counterfeit bags will be very high. The counterfeit activities will be effectively combated. Also, the authentication accuracy will be significantly increased with eliminating the potential risk of discovering vulnerability by counterfeiters due to the full reliance on the tag.

4.2.3 E-pedigree

E-pedigree is the final security layer for the authentication. It provides the logistics record of the scanned product to the user. E-pedigree will show where the product is currently located according to the company's information.

The logic behind E-pedigree for authentication is that if the product is not currently located at the place where the company's record states, the product is considered as counterfeit.

Taking a LV Neverland bag as an example, a potential customer finds it discounted in a small boutique in Hong Kong. He doubts its authenticity so he decides to use the NFC anti-counterfeit application to authenticate the bag before making any purchasing decision. After scanning the tag, he first clicks the E-pedigree to check the logistics record of the Neverland bag. The record shows that the bag is currently located at flagship in New York which does not match with the fact. Based on the logistics record provided by the company, the user is alerted that this bag is not genuine.

The authentication server will search the logistics record of the product according to the tag's unique identifier, which is the UID of the tag. The UID of the tag will be obtained by the authentication server from reading the tag at the beginning.

The status of the product will also be shown in the E-pedigree. The user will be notified if the product is sold. The company will not update the logistics record of the product after the product is sold.

The reveal of the product status can eliminate the unnecessary misunderstanding of second-hand bag. The use of the product will not be in the control of the company after the product is sold. Therefore, it is not the company's control of the second hand bag market. However, it is the company's responsibility to guarantee the authenticity of the bag, no matter it is sold or not. For this reason, showing the status of the product can help the buyer to authenticate the second hand bag.

E-pedigree is another type of manual authentication. The user has to verify the place where he meets the product with the location given by the company. The complexity of this manual authentication is far less than the specific features authentication which requires the user to examine the physical anti-counterfeiting features of the bag.

4.3 Authentication Result

The structure of the hybrid approach has been presented in the above section. The hybrid approach has equipped with 4 security layers which are synchronized secret, serial number, specific-features authentication and E-pedigree. These four security layers provide tag authentication, ID authentication, location authentication and physical features authentication for the product.

Table 4.2-The algorithm behind the hybrid approach

Result	Serial No.	SP	Tag	Location
Genuine	Pass	Pass	Pass	Pass
Counterfeit	Fail	Fail	Fail	Fail
2nd bag /Counterfeit	Pass	Pass	Pass	Fail
Counterfeit	Pass	Fail	Pass	Pass
Counterfeit	Fail	Pass	Pass	Pass
Counterfeit	Fail	Fail	Pass	Pass
Counterfeit	Pass	Fail	Fail	Pass
Counterfeit	Pass	Pass	Fail	Fail

The above table shows the algorithm of identifying genuine and counterfeit goods. A product will be considered as genuine only when it passes four inspections. Product failing any one of the three inspections, which are serial number, synchronized secret and specific-features, it will be considered as counterfeit.

The only exception is products which only fails location authentication. Under this circumstance, the user will be provided with the current product status to further authenticate the product. If the product status shows the product has been sold, the fail in location authentication will become reasonable as the company is no longer in possession of the product. Therefore, the product with this authentication result will be considered as second hand bag. If the product status shows that the product is still on shelf, then the product examined will be considered as counterfeit.

Under this algorithm, the application is able to authenticate the product; no matter it is second hand product or brand new genuine product. In the aspect of second handbag market, the algorithm not only protects the authenticity of second hand product, but also put a stop on counterfeiters to invade second-hand bag market.

4.4 System Technology

It is essential and necessary to select system accessories on both hardware of server-side and client-side before developing the application. The system accessories will be divided into two types, which are accessories to run the mobile application in the aspect of the users, and the accessories needed to operate and perform the authentication services by the company.

Powerful computers with high processing power are needed for the company to operate and perform the authentication services to users. They are used as servers to provide high processing speed and large storage capacity to the authentication. Servers are classified into two types, which are database server and authentication server respectively. The former is responsible of storing the basic information and the anti-counterfeiting data, especially synchronized secret and information related to specific features, of each product. The latter is focus on authenticating the authenticity of the products. It includes sending, receiving and processing the data transferred from the database servers to the mobile device.

Network system should be prepared and installed for the internet access from end-users to the servers in order to operation the authentication. Broadband network should be adopted to deal with the large amount of data transferred and maintain short response time from the server to the end-user. Optical Fiber is recommended in this set-up.

For the implementation of the anti-counterfeiting application, there are software packages needed to be installed to provide the services to the end-users. Database server is run based on SQL language and thereby Database Management System is necessary for the operation of database server.

The Authentication server is built upon programming languages which are JAVA and C++ respectively. Language packages should be installed properly before the development and configuration of the authentication server.

There are requirements for the end-users to run the application. Mobile phone with NFC function is a must for running the operation. The application relies on the NFC reading device installed in the mobile phone to read the NFC tag embedded in the product.

The application is only compatible with the Android system which is the only system allowing the NFC read/write function. Mobile phones with IOS, Symbian or Windows Mobile are not able to run the application. The version of Android system is not limited for running the application. It is compatible from Android 2.1 to 4.2 Ice Cream Sandwich.

NFC tags play an essential and critical role in the anti-counterfeiting application. Unique identifier stored in the NFC tags helps authentication server to identify the products and give appropriate response. Because of the special nature of synchronized secret, NFC tag should offer read/write protection and authentication. Access control should also be provided by the NFC tag. MIFARE Classic is the recommended NFC tags for the application.

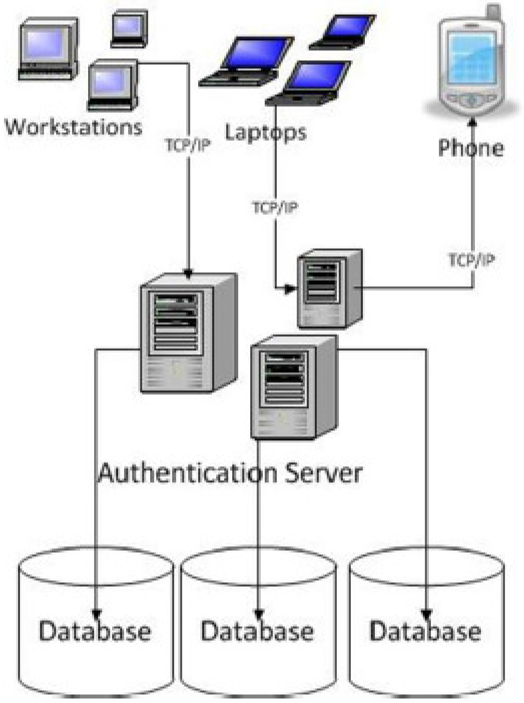


Figure 4.3-Diagram showing the general system set-up

The above diagram shows the general setting of the authentication system. Database server, or called SQL server, will connect to the authentication server by optical fiber, to achieve maximum bandwidth for efficient data transmission.

The authentication server will communicate with the end-users through TCP/IP. TCP/IP is the internet protocol used by the internet. The server will transmit data through internet to the mobile phone, where the anti-counterfeit application is installed in.

The authentication server will have interaction with notebooks and workstations through the portal. The portal also requires internet access for data transfer. All tasks must gone through the authentication server.

4.5 System Architecture

4.5.1 Application and Sever Architecture

A counterfeit application with hybrid approach has been designed to combat fierce counterfeiting activities in designer bag market. In this section, system architecture of the application will be designed and shown. It includes system architecture of the application and thee server. Authentication flow, including client-side and server-side, and dataflow diagram will also be shown in this section.

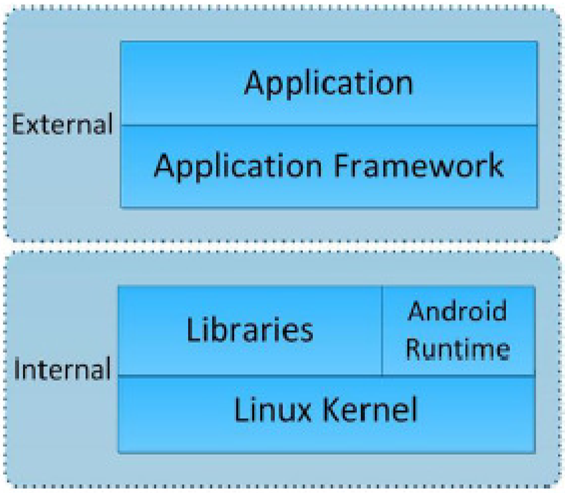


Figure 4.4-System Architecture Of The Application

Linux Kernel is the basic and the lowest layer in the application. The operation system of Android is built based on the model of Linux Kernel. This layer is responsible of interacting with the hardware of the mobile phone and contains all important and essential hardware drivers, including camera and display screen.

This layer is essential for the NFC device installed in the phone. The NFC driver must be installed in this layer in order to run the device. When the driver is properly installed, the application will be able to read the NFC tag embedded in the bag.

Libraries and Android Runtime are both belong to the second layer, but they are separately operated. Runtime is used to run the application under optimize condition. It helps the application to consume less processing power and memory.

Libraries enable the device to execute different forms of data. It consists of C++ language and JAVA which is the programming language used in the application. The media codec stored in libraries provides sound effect to the application. Also, OpenGL provides rendering of 2D and 3D graphics to the application.

Application and Application Framework form the external part of the whole system. Framework provides direct interaction to the users by providing graphical user interface. It helps managing the activity held by the application. It also is responsible of content management.

All these three layers contribute to the operation of application. Without these three layers, the mobile will fail to run the application and provide its functions. The variables of those layers are needed to set very carefully for the development of the project.

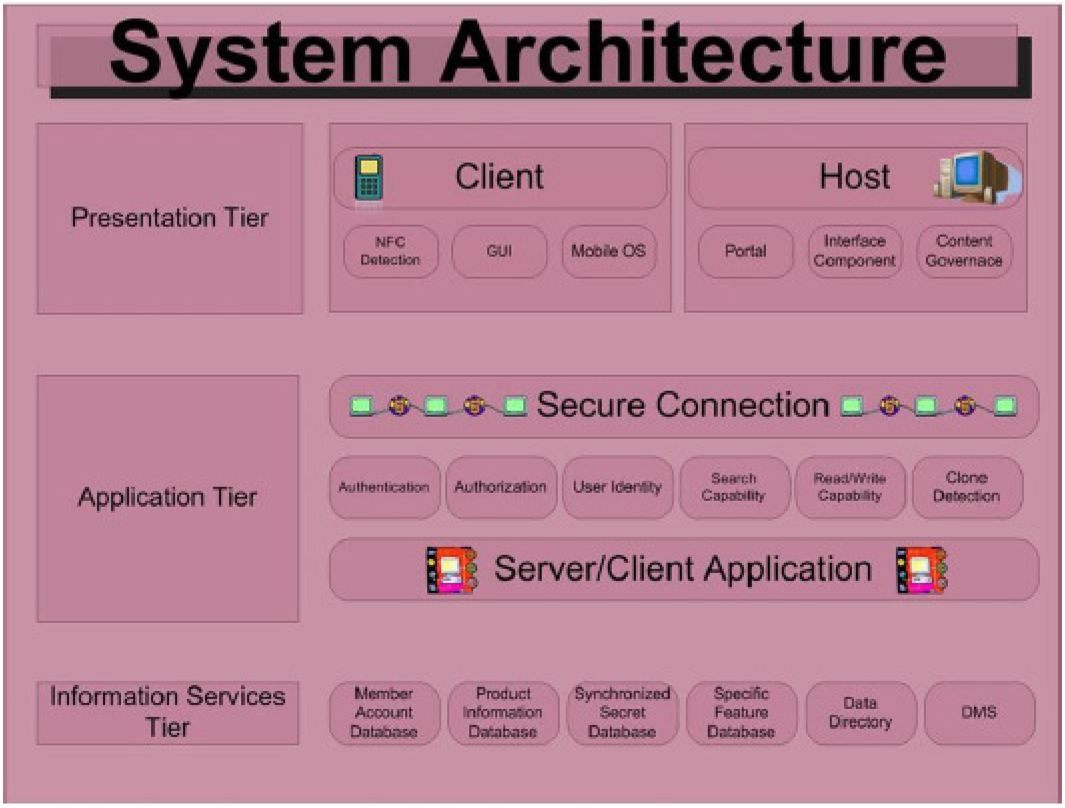


Figure 4.5-Server System Architecture of the anti-counterfeit application

The server system is divided into three tiers which are presentation tier, application tier and information services tiers. The logic of this structure is to breakdown the major activities of the authentication into different minor tasks for the transmission, search and calculation process.

Presentation Tier

This tier has direct interaction with the users, including the end-user and the programmer, or called responsible party. The former will use the application through the graphical user interface provided by the application which is built based on Android, the mobile operating system.

The latter will input the product data, including tag information, tracking record and other product data through the portal into database server. They will also provide content governance to the system. Interface components are used to decorate the portal interface and to allow the user to interact with it. All activities are needed to go through the portal.

At all, there are two systems, which are application and the portal, which is not the focus in this project, provide different services to client. Only officers responsible of product data entry input will be authorized to use the portal to manage the system. The other system is application which is used by the end users to authenticate the product.

Application Tier

The application server tier is the most essential part in the anti-counterfeit application. All authentication operations have to be processed in the application server. The mobile application only acts as the middleman between the user and the authentication server.

The authentication server will be responsible of providing serial number authentication and synchronized secret authentication to the users. Authorization is also part of the server's tasks. For example, the server will check and certify the user's membership validity and authorize them to use the mobile application. It also specifies access rights to different resources and offers information security.

The server also provides assistance to end-users for further manual authentication. It provides information and data required for specific-features authentication and E-pedigree.

Search capability and Read/Write capability are also performed by the authentication server. It will give search command to database server for searching required data and information. Read/Write capability is to give and perform tag writing and reading in remote mode through the mobile application.

Clone detection is designed for protecting tag cloning. When the synchronized secret stored in the tag does not match with the one stored in the database server, the authentication server will trigger an alert immediately. The alert will raise both the end user's and company's attention. The company will thereby take further actions when alarm is raised.

Secure connection offers data protection during the internet transmission of two platforms. It masks sensitive and confidential data from third parties and provides verification of the interested party's identity who involves in the exchange of data. Third party is not able to view and modify the protected data.

Secure Sockets Layer (SSL), a common encryption protocol used by various industries, will be used to encrypt the transfer channel. It will be applied to the Client/Server transmission.

Server/Client application offers system activation. It allows communication between layers, execution and calculation of programs and activities. It is a set of program for authentication system. The core function is no major different from operation system. The application can be considered as a 'heart' to keep the system 'alive', such as doing authorization.

Information Service Tier

The major activity in information service tier is data storage. It provides necessary data for the system during authentication. This data warehouse consists of different minor database servers for various types of data and purposes.

It includes database storing membership information, product information, synchronized secret and specific feature information. All data are well-classified and categorized in this layer in order to achieve effective and efficient data search.

The database will be continuously updated, especially the one storing synchronized secret. Each synchronized secret stored database is synchronized with the corresponding tags. Officers responsible of manual data input can access the data warehouse through portal installed in workstations.

Data Directory acts as a catalog which indicates the location of a particular data. It indicates user a path to find the data. Also, it provides serialization to the database. Thus, effective content governance can be achieved. Data redundancy can be prevented.

DMS, the abbreviation of document management system, is a computer system installed in the database. It is also the core component of this tier. The major function is to track and store different electronic documents, data and information. It provides history tracking to the users. DMS acts as the backbone of database. Storage, versioning, security, integration and indexing are all provided by it. Only authorized staff can modify the database.

4.5.2 Authentication Process

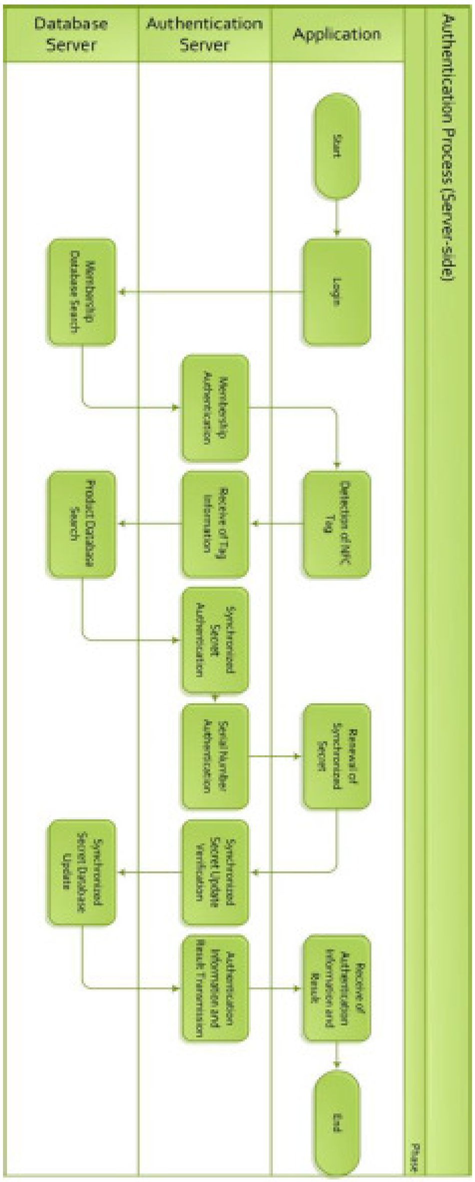

Database Server
Authentication Server
Application
Authentication Process (Server-side)
Start
Login
Membership Database Search
Membership Authentication
Detection of NFC Tag
Receive of Tag Information
Product Database Search
Synchronized Secret Authentication
Serial Number Authentication
Renewal of Synchronized Secret
Synchronized Secret Update Verification
Synchronized Secret Database Update
Authentication Information and Result Transmission
Receive of Authentication Information and Result
End
Phase

Figure 4.6-Cross-functional Workflow of Authentication Process (Server-side)

The above diagram focuses on the server-side of the authentication process. The process has been categorized according to the execution device. There are three major systems involved in the authentication process which are application, authentication server and database server.

The application in this diagram refers to the mobile application installed in the end user's phone. The actions taken in the application will call activities in authentication server and database server. Therefore, it is necessary to include application, which is not belonging to server-side, in this flow diagram. Also, it is noted that internet access is necessary for running the application.

When the user login the application with ID and password, the database server will search the membership database immediately when the data is received successfully. The authentication server will verify the membership according to the information sent from database.

When the ID and password that end user have entered are proved to be matched with the membership database record by the authentication server, the authentication will send command to the application and unlock it. The user can thereby read the tag by application.

The application will soon send back the information of tag read to the authentication server. Once the authentication server receives the data, it will automatically give search command to the data warehouse. The data warehouse will thereby search the product data according to the data read from the tag.

The database will send the search result and the required data to the authentication server. First, the authentication server will start synchronized secret authentication for tag verification. It will compare the secret with the one stored in the tag. If the tag passes the synchronized secret authentication, the server will enter the next stage.

Serial number authentication will be held immediately after the pass of tag authentication. The server will verify the existence of serial number. If the serial number is validated, the server will send tag renewal command to the application, and then the application will write a brand new synchronized secret to the tag, and the database will updated synchronously.

When the synchronized secret renewal is successful, the authentication server will sort out the information needed for manual authentication and result of automatic authentication, and send to the end-user and show them in the application. The server cycle is over at this stage.

The diagram below shows the client-side of the authentication process. The difference between with the above diagram is that the end-user can verify the authenticity of the product according to the result sent from the server and by manual authentication.

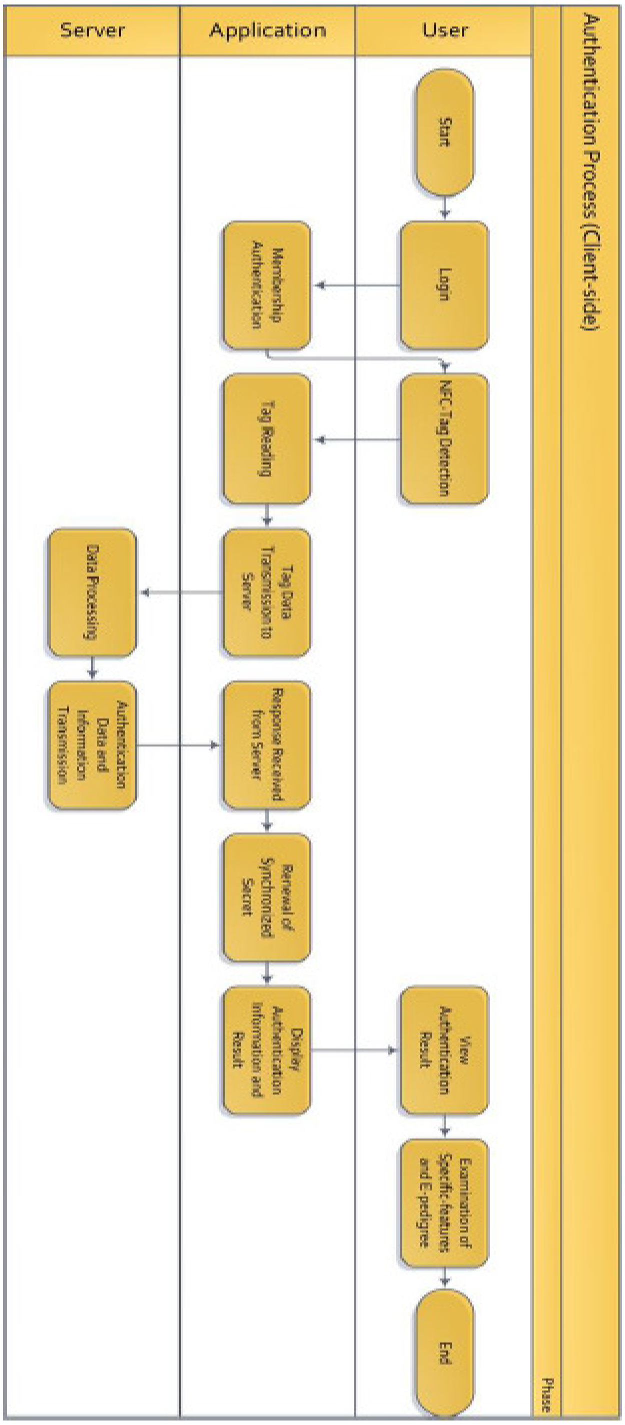

Server
Application
User
Authentication Process (Client-side)
Phase
Start
Login
Membership Authentication
NFC-Tag Detection
Tag Reading
Tag Data Transmission to Server
Data Processing
Authentication Data and Information Transmission
Response Received from Server
Renewal of Synchronized Secret
Display Authentication Information and Result
View Authentication Result
Examination of Specific-features and E-pedigree
End

Figure 4.7-Cross-functional Workflow of Authentication Process (Client-side)

4.5.3 Data and User Flow

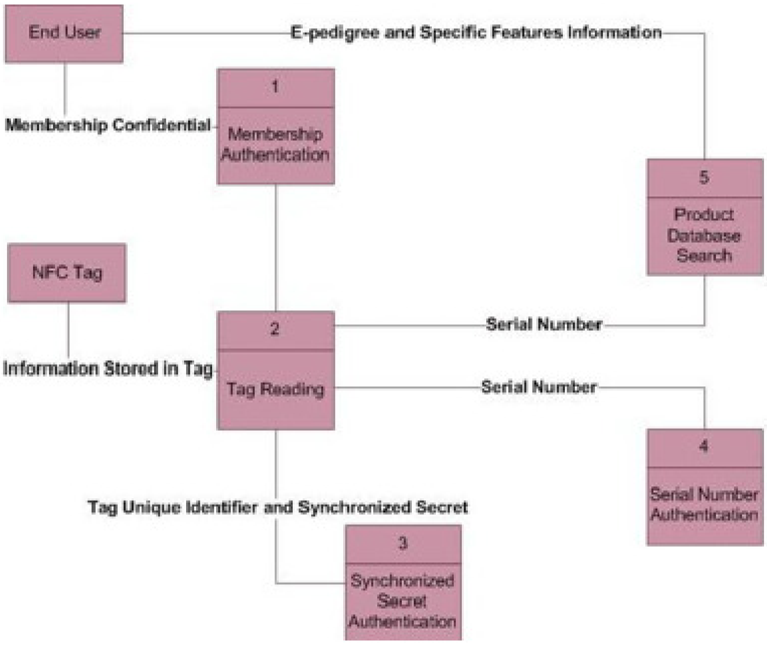

End User
E-pedigree and Specific Features Information
1
Membership Authentication
Membership Confidential
5
Product Database Search
NFC Tag
2
Tag Reading
Information Stored in Tag
Serial Number
Serial Number
4
Serial Number Authentication
Tag Unique Identifier and Synchronized Secret
3
Synchronized Secret Authentication

Figure 4.8-Data Flow Diagram of the Anti-counterfeiting Application

Data flow diagram represents the flow of data through the system. It shows the types of data input and output through the system. The route of data will be clearly shown in this diagram. Data processing time will not be shown in this diagram.

End user in this diagram refers to the user using the application. The first step requiring data and information is membership authentication. It needs the end-user to submit membership confidential for authentication.

Tag reading, the second procedure, will retrieve information and data stored in the tag. Those data is essential for the authentication.

Tag unique identifier and synchronized secret, which is part of the information retrieved from the tag, are used in synchronized secret authentication, the third procedure. Serial number is critical in the fourth and fifth procedures. The former needs to verify the validity of serial number and the latter will be held based on the ID number.

The final data flow will be the search result generated from the fifth procedure. The end user will obtain E-pedigree and specific-features information for their manual authentication together with the result of serial number and synchronized secret authentication.

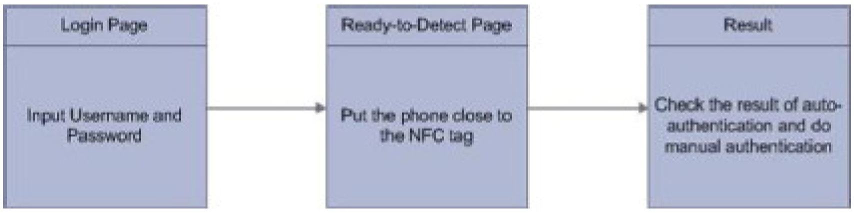

Login Page
Input Username and Password
Ready-to-Detect Page
Put the phone close to the NFC tag
Result
Check the result of auto-authentication and do manual authentication

Figure 4.9-User interface flow diagram

The user interface flow diagram shown above has molded the mock interactions that the users have with the anti-counterfeit application. It has three major interactions during the authentication.

First, the user is required to login with username and password. Second, if the login is successful, user is given the instruction to start the authentication. The user is instructed to use the application for NFC tag detection.

When the NFC tag is read successfully, the application will wait for the server response. When the response is received, the authentication will move to the next stage which the user will be able to check the auto-authentication result. In the following, the user can do manual authentication based on the information shown in the application. This is the last interaction between user and the application.

Chapter 5 – System Prototyping

In last chapter, it mainly focuses on the application concept, the algorithm and the structure of hybrid approach, together with the presentation of system architecture design.

In the following, a beta test will be conducted for the application. The application demo has been developed for the implementation. All Product information and manufacturing work flow used in this beta test have been provided by a reputable designer brand manufacturer.

The application interface will be firstly presented, together with the tag embedment process in the following section and the cost estimation for the anti-counterfeit system also.

5.1 Application Interface

5.1.1 Equipment and Devices

The table below lists the features of the phone used in this beta test. Google Nexus 4 is the first model developed with NFC device. Most current mobiles with NFC function are all developed based this model. Applications developed on Nexus 4 allow great compatibility with other smart phones. Therefore, Nexus 4 is chosen to be the application device.

Table 5.1-Major features of Nexus 4 for application development

Google Nexus 4	
Operation System	Android
Version	4.1 Ice Cream
NFC function	Enabled

5.2-Specifications of Tag used in trial run

Mifare RF	
Version	MF1 IC S50
Operating Distance	Up to 100mm
Operating Frequency	13.56 MHz
Fast Data Transfer	106 kbit/s
High Data Integrity	16 Bit CRC, parity, bit coding, bit counting
Anti-Collision	Enabled
Typical ticketing transaction	<100 ms
EEPROM	
Tag Memory	1 Kbyte, organized in 16 sectors with 4 blocks of 16 bytes
User definable access conditions for each memory block	Enabled
Data Retention	10 years
Write Endurance	100,000 cycle
Security	
Authentication	Enabled with mutual three passes
Data Encryption	Enabled
Replay Attack Protection	Enabled
Multi-application with Key Hierarchy	Enabled
Key Identifier	Enabled
Transport Key Protection	Enabled

The tag used in this demonstration is Mifare RF which provides high price/performance and satisfactory capability for product authentication. It is usually used as contactless smart card with very flexible size. It is very suitable to be embedded in the bag.

The tag is passive contactless. It does not require any battery. Therefore, the cost is very low. Also, the inexistence of the tag avoids unnecessary inconvenience to the buyer. It is very suitable for short range NFC mobile application. It is simple to use and does not require any sophisticated technology which prevents high investment cost of manufacturer. The best benefit brought by the tag is long lifetime. As there is no mechanical wear required, the effective time for data retention can be up to 10 years.

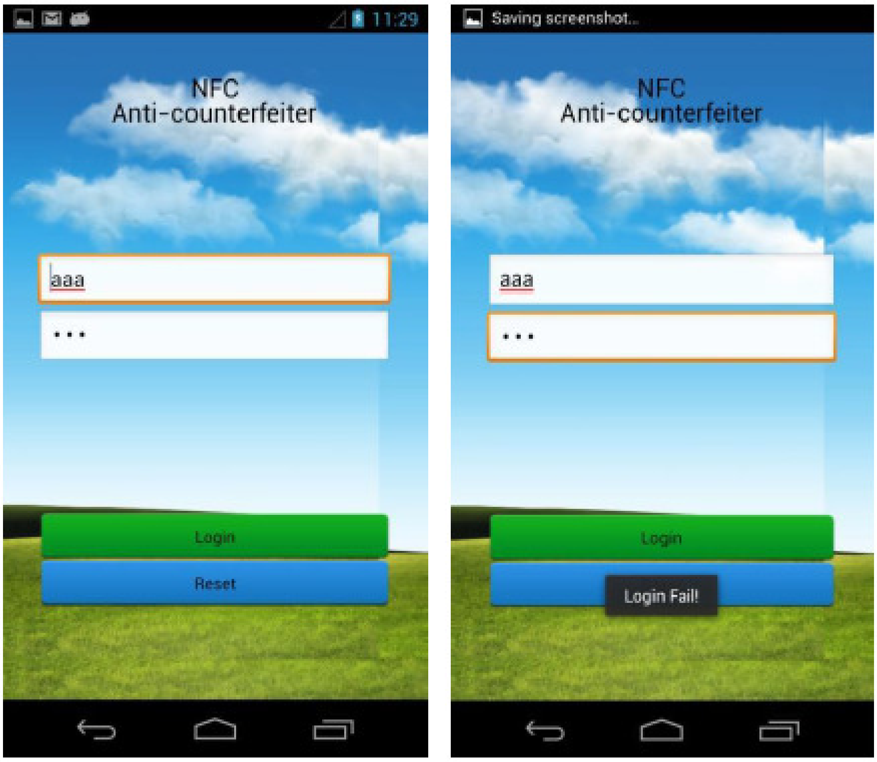
Anti-collision function provides simultaneous operation of the tag. Multiple tags can operate at the same time without data collision. It can ensure the transaction performed by each individual tag can be executed correctly without any data corruption.

The data transfer speed of the tag is 106kbit/s which is average among all classes of NFC tag. It is already enough for product authentication. Taking a typical ticket transaction as an example, the tag can be able to finish the transaction within 100 mile second. The transmission rate is enough for the authentication purpose.

The tag also places high emphasis on security issues. Authentication is provided with three mutual passes by the tag. Data cyphering and response authentication are also equipped by the tag. Tag tampering can be prevented. This has given a competitive advantage to those low cost tags such as Mifare Classic. Two unique tag identifiers are given by the tag for double tag authentication and guarantee the tag uniqueness.

Overall, the low-cost tag selected is able to fulfill the tag requirements of hybrid approach and user expectation.

5.1.2 Interface Analysis



aaa
•••

aaa
•••

Login Fail!

Figure 5.1-Login Page of the Application

This is the login page of the anti-counterfeit application. User ID and password are required for membership authentication. The diagram in the right shows the result of fail membership authentication.

The membership allows the company to track the tag detection record of users. The membership registration requires users to enter their personal information such as Hong Kong Identity Number.

Therefore, the counterfeiters may not able to use the application to massive detect the tag information for counterfeiting purposes. Any suspected detection will raise the company's attention and further action will be taken.

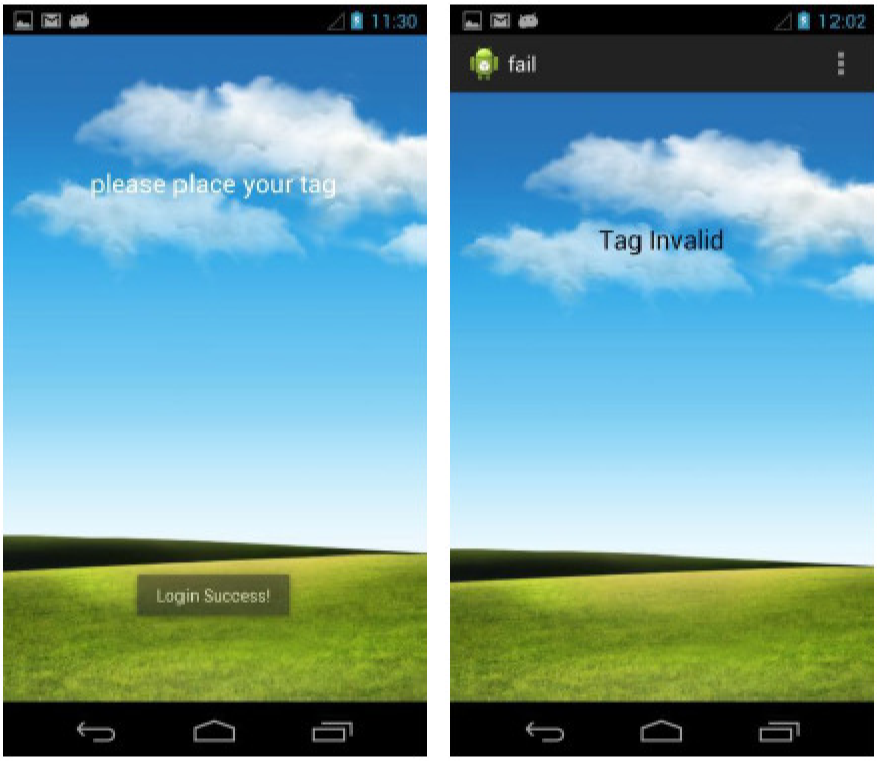


Figure 5.2-Tag Detection Page of the Application

When the user successfully logins, it will turn to the next page where further instruction is shown. The page will first show the login status to the user. "Login Success!" has been displayed on the bottom of the screen which is shown in the left diagram.

Together with the login status, the screen also gives the instruction of "Please Place You Tag" at the top. It is a ready-to-detection signal to the user. The application is under NFC reading mode which will immediately and automatically detect the tag nearby.

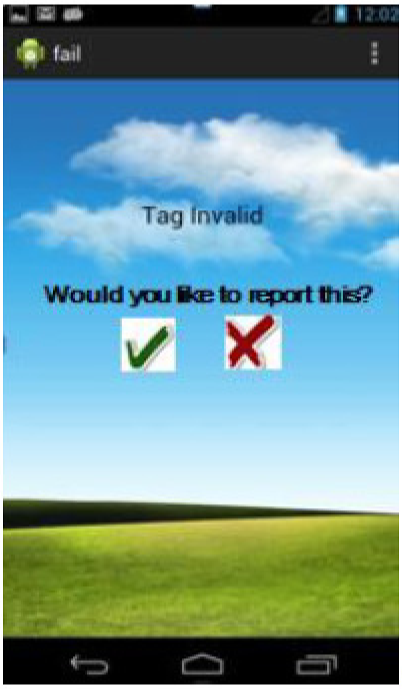
The diagram on the right demonstrates the fail tag detection. A "tag invalid" message has been shown in the screen, together with the fail signal displayed at the top of the screen. There are few reasons of fail tag detection:

1. It is not an authorized tag; therefore, the application is not able to extract the tag information.

2. It is a fake tag. Counterfeit bag is determined due to inexistence of tag information stored in data warehouse. The authentication server even cannot find a matched record in it. Therefore, it shows "the tag is valid" at the page

3. Unsuccessful NFC tag detection. The detection process is interrupted due to the inappropriate place of NFC tag.

4. The tag is damaged and unable to be read by the application. Thus, the application will determine the invalidity of the tag.

. 

Tag Invalid

Would you like to report this?

(2 more images for PPT)

If the tag is invalid, a message will appear, asking whether or not the user would like to report this event. If the user selects YES, he/she will be asked to fill a simple reporting form and post related pictures, as shown in the figure just above

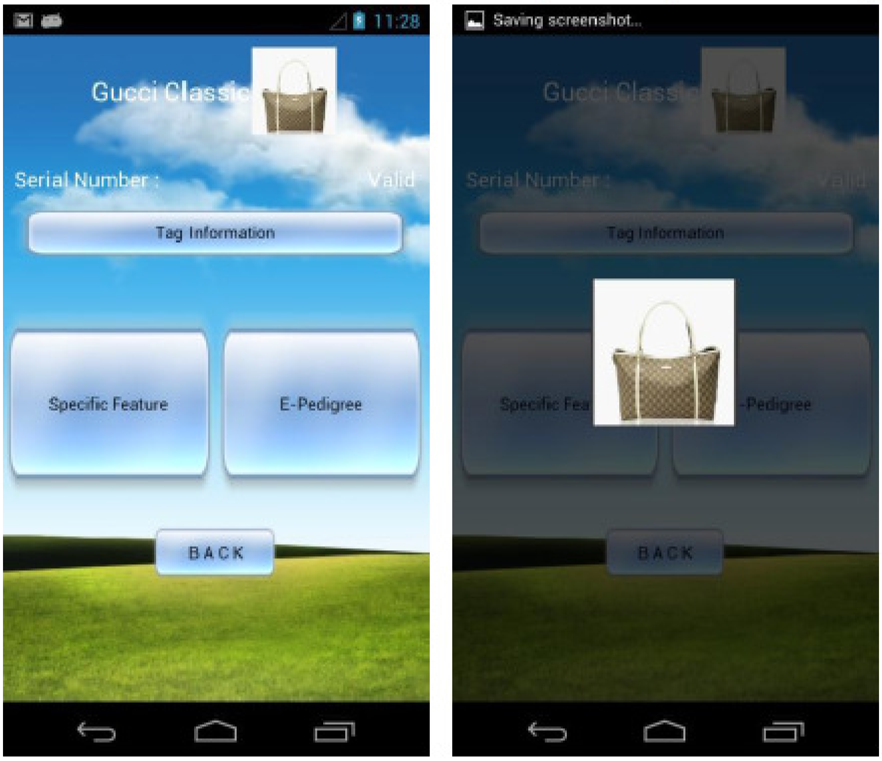


Figure 5.3-The Main page of the Application

After successful NFC tag detection, it may take time for the application to send the data retrieved from the tag back to the authentication server. When the authentication process held by the server finished, the application will receive the information sent from the server, and then those will be displayed in another page.

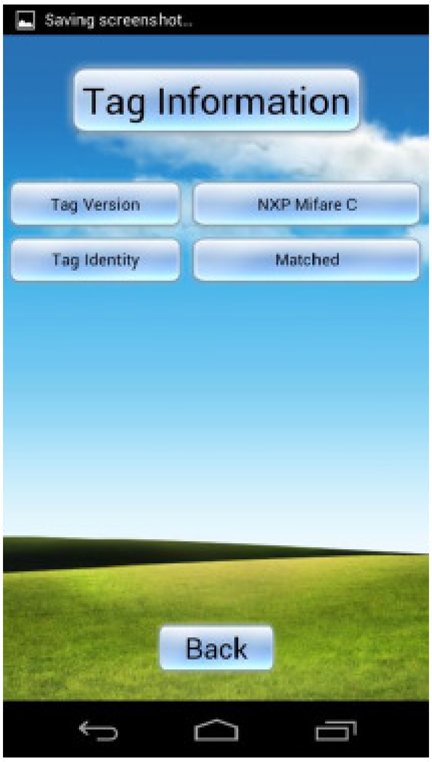
In this page, name and photo of the product will be shown. The product examined in this beta test is Gucci Classic. The picture of the bag can be enlarged by clicking the position of the photo on the screen.

Thus, if the product name and appearance shown in the application are found unmatched with the bag examined, the bag will be considered as counterfeit. This is the very first and simple authentication procedure.

The validity of the serial number will not be shown in the application. It is used to minimize the possibility of cloning. It prevents the counterfeiters from copying the serial number to forge the product information stored in the tag.

The result of the serial number authentication will be shown next to the serial number. In this case, the serial number is valid. Therefore, it unlocks the specific-feature authentication and E-pedigree to the users as these two types of information are given based on the serial number.

User can click the middle section of the page to view the tag authentication result sent from the authentication server. The tag authentication is held independently. Therefore, if the serial number is invalid, the user can still view the tag authentication result.


Saving screenshot...

Tag Information

Tag Version	NXP Mifare C
Tag Identity	Matched

Figure 5.4-Tag Information Page of application

The layout is very simple in tag information page. It only shows tag version and tag identity in this page.

The tag identity refers to the synchronized secret stored in the tag. When the authentication server finished the authentication, the result will be shown in this field. In this case, the Gucci Classic passes the tag authentication.

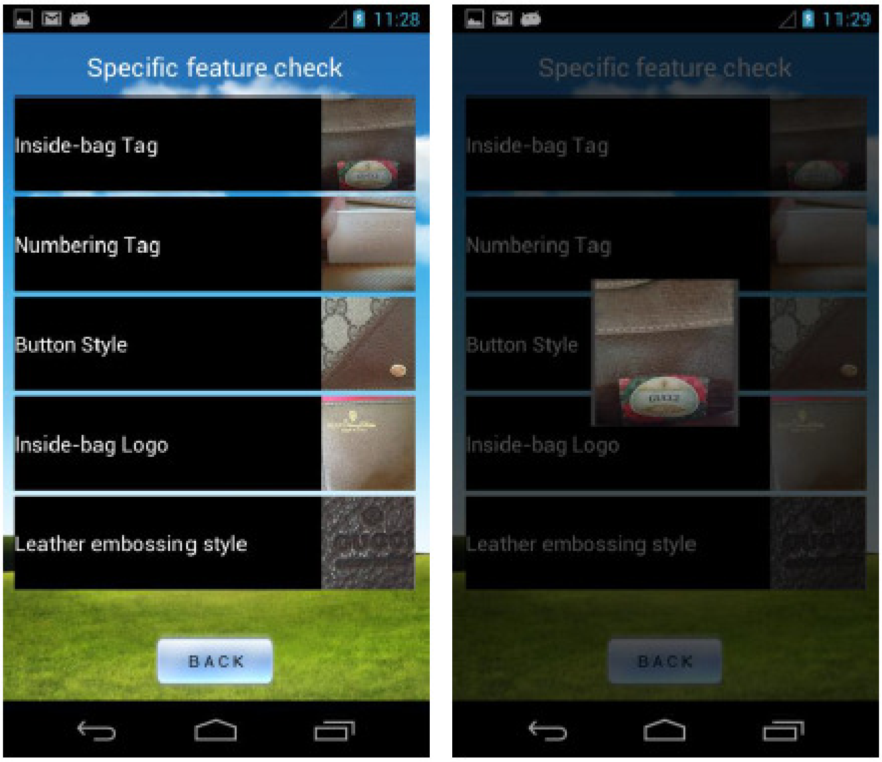


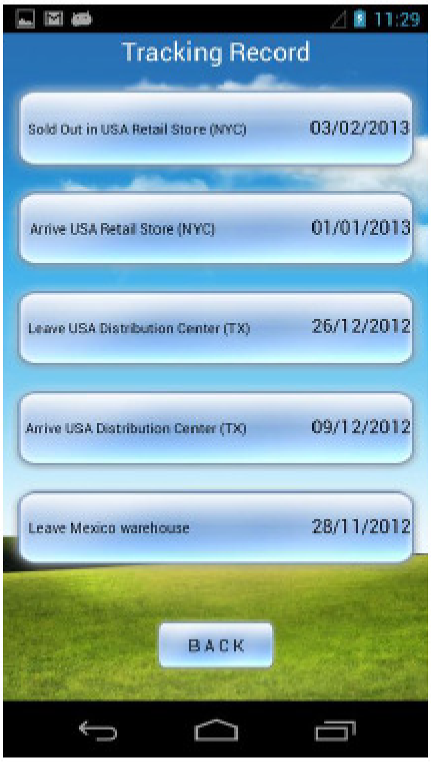
Figure 5.5-Specific-feature page of the application

Photos of physical anti-counterfeiting features or characteristics of the bag are shown in this page. Enlargement of photo can be achieved by clicking the photo. Descriptions of those features and characteristics are placed next to the photos for assisting the user to do manual authentication.

In this case, the Gucci Classic can be examined manually by checking whether there is inside-bag tag with the correct design, or numbering tag with matched number shown in the photo. The button style, which the button is exclusive owned by the brand and designated for the particular bag, can also be part of authentication. Inside-bag logo with the correct printing, and leather embossing style, which makes the brand different from others, are playing essential role during the checking.

Those features and characteristics increase the difficulty in counterfeiting. The counterfeiters may not be able to have access to the suppliers and get the exact manufacturing materials or do not have equivalent technology or special machine to make the exact design and pattern of the bag. Given that the counterfeiters have purchased relevant manufacturing machineries and obtained adequate technology, and have channels to purchase material from their exclusive suppliers, the cost-to-break is too high for the counterfeiters to make profit. The insanity investment cost will discourage the counterfeiters from making the fake bag.

Therefore, the manual authentication has given high reliability for the users in the checking. It raises the authentication accuracy. Although it takes some time, it is almost flawless.



Tracking Record

Sold Out in USA Retail Store (NYC) 03/02/2013

Arrive USA Retail Store (NYC) 01/01/2013

Leave USA Distribution Center (TX) 26/12/2012

Arrive USA Distribution Center (TX) 09/12/2012

Leave Mexico warehouse 28/11/2012

Figure 5.6-E-pedigree Page

The E-pedigree offers product tracking record to the user. The status of the product is shown in this page. The user is able to define whether the product he detected is exactly at the same position as the E-pedigree states.

The display of product status provides a firewall to the company that even if the former three security layers are broke by the counterfeiters, they can never forge their product position. Where the customer tags the bag are their current position. If the tagging position are found unmatched with the E-pedigree, the product is fake.

The only exception is the second hand product. The owner right goes to the buyer when the bag is sold. Therefore, where the bag goes will not be the matter of the brand. In order to protect the right of the buyer, the company is still responsible to prove the authenticity of the product.

Thus, product status will be shown in this page. The diagram above has shown that the Gucci Classic has been sold out in New York City. If the product detected has been stated second-hand, the user can refer to the previous three authentication results to determine the authenticity of the product.

The last security layer has protected the second hand bag market and the right of the buyer. Again, the cost-to-break is too high to afford by the counterfeiters. Therefore, the four authentication locks are enough for anti-counterfeiting and authentication purposes.

5.2 Tag Embedment Process

The design of tag embedment process is based on the information, floor plan and manufacturing workflow provided by a reputable luxurious designer brand manufacturer.

This famous brand manufacturer has large market share in accessory market in Europe and United State. The large sales volume has attracted counterfeiters to manufacture fake bags of the brand. The fierce counterfeiting has created brand image damage and financial loss of the brand. In this section, suggestion will be given on how the tag is embedded in the bag during the manufacturing process.

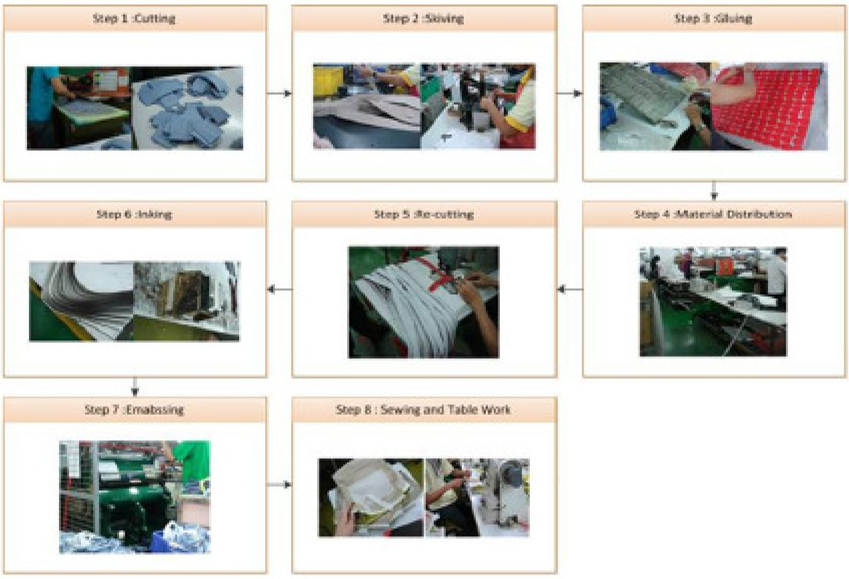


Figure 5.7-The Original Handbag Manufacturing Processes

Figure 5.7 shows the original handbag manufacturing processes that the manufacturer will first cut the fabric into pieces of different sizes according to the instruction of technical packages sent from the design department. The fabrics are purchased from the authorized suppliers.

After finishing the cutting, the next step is to skive those pieces of different size. It is used to control the thickness of the fabrics.

Third, the materials are sent to gluing. Gluing is used when the fabrics are needed to glue with other materials for shaping purpose. Baggage tag is one of the products produced in gluing process.

The fourth step is material distribution to different sector according to the function and part of fabrics. Its purpose is to reform the manufacturing process and divided the workflow into different sectors which the previous three steps are all necessary for all fabrics.

Re-cutting, the fifth step is to re-shape the fabrics into desired shape while the sixth step, inking, is to smoothen the edge of the fabrics. After that, those materials will go through the embossing process which is used to compress carve and mold the design on the surface of the fabrics.

As far as embedding tags into handbags is concerned, there is an additional step needed. The figure below shows the new handbag manufacturing processes.

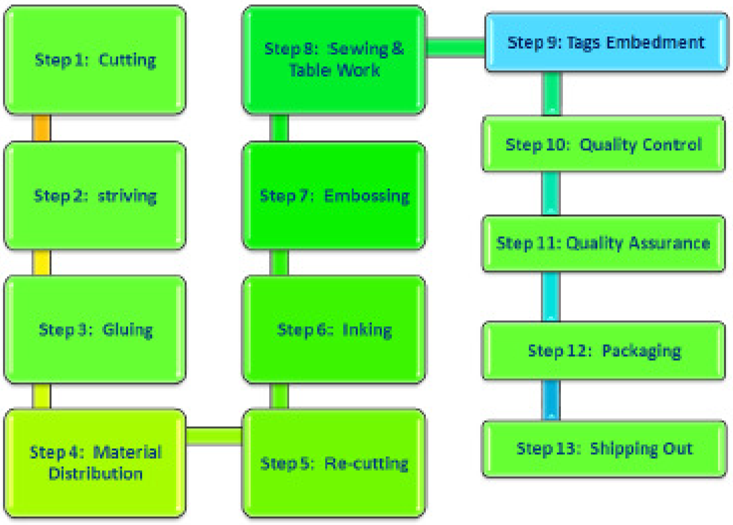


Figure 5.8-The New Handbag Manufacturing Processes

The tags can be added during this stage as all bags will be finished all manufacturing processes in this stage that tags can be embedded in the inner side of the bag by workers. After finishing the tags embedment, in-house quality control can be processed as well as quality assurance in order to make sure the products without any mistakes. Furthermore, packaging of handbags is also needed before shipping out the bags to wholesalers or suppliers.

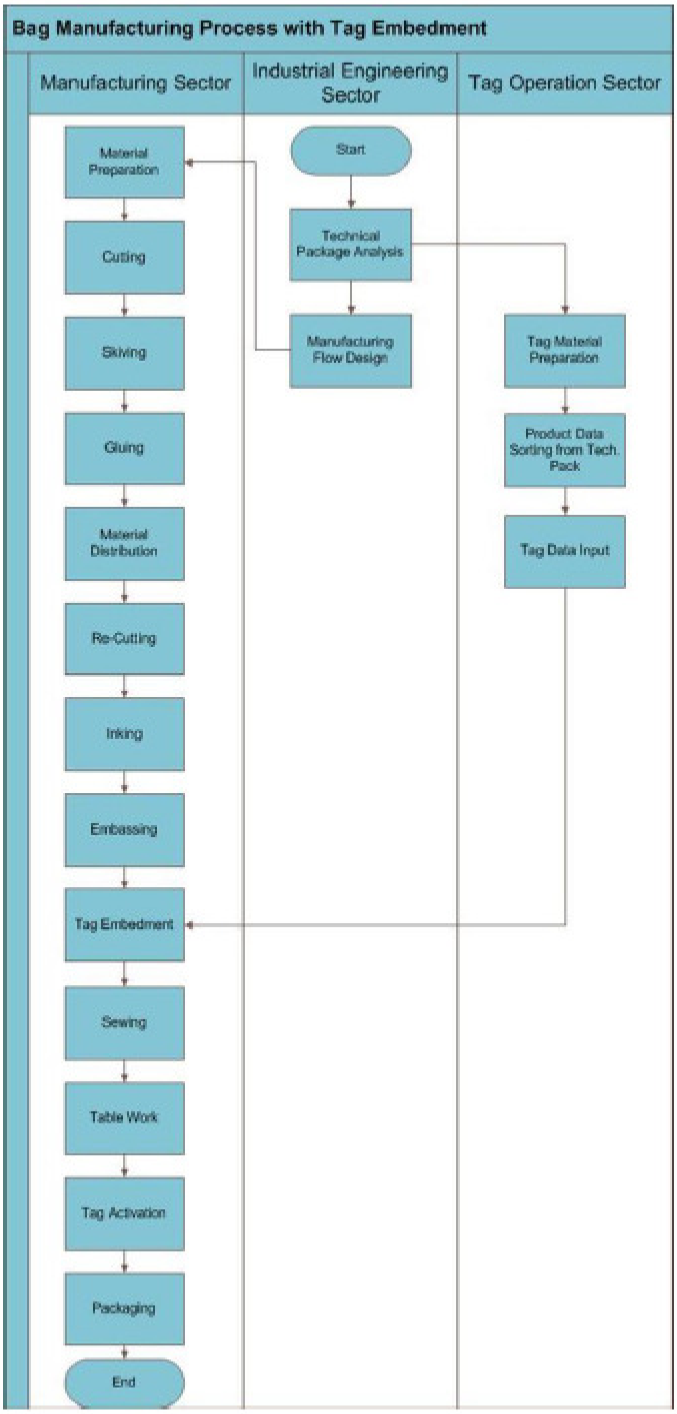


Figure 5.8-Suggested flow for tag embedment process

Before starting manufacturing the bag, the manufacturer will first receive the technical package sent from the designer. The technical package consists of the blueprint of the bag, the material requirement, the anti-counterfeit information such as serial number and other required documents for manufacturing.

Tag material preparation is suggested to be started during the technical package analysis. This step is to prepare the tags for the bags, the manufacturer may need to order the tags from other suppliers, and the tags ordered may be general or tailor-made. It depends on the need of the company. After finishing the tag material preparation, the tag operation sector should extract the anti-counterfeit information of products from the technical package and do the sorting for better categorization.

Tag data input can be started when the sorting is finished. The staff is required to input the data into tag for the embedment. The tag should be ready at this stage. Those will be sent from the tag operation sector to the manufacturing sector for tag embedment.

After the sewing is finished, the tag will be activated before the bag is packaged. It is to ensure all tags are well-embedded in the bag, run smoothly before leaving the factory and to start product tracking.

5.3 Cost Estimation

Financial analysis of the anti-counterfeit project will be done in this part. Project budget estimation will be shown together with the future sales forecast. This is a five-year based project. Therefore, the budget shown below will only consist of five years.

Table 5.3-The Initial Cost of the project

Setup Cost	HKD
System Development	1,300,000
System Infrastructure	300,000
Staff Training	200,000
Total	1,800,000

The system development cost covers both application and clouding system development which are outsourced to third-party system provider. Therefore, the cost may be higher than self-development.

The outsourcing has given the company advantages that the system will be more reliable by contracting experts for system development. Less human and time resources will be consumed by avoiding developing the system on their own.

The system infrastructure refers to the equipment needed to implement the anti-counterfeit project. The project not only requires the company to purchase NFC-tag related device for the tag operation, but also computing devices for the system application.

Staff training is necessary for the project implementation. As the company does not have similar applications before, the staffs there are not capable of running the system fluently and effectively without any training.

Table 5.4-Current Sales Volume

	HKD
Annual Average Volume of Good Sold	3,000,000
Average net profit per good	355

It is estimated that, at the end of the project, it will bring 2% increase in volume of good sold. This sales volume estimation is based on the data that the company has provided for the project. Each bag sold approximately brings the company 355HKD dollar. Also, there are 3,000,000 average bags sold in the past three years.

Table 5.5-Estimated Growth on Volume of Good Sold

	Estimated Growth on Volume of Good Sold
Year 1	0%
Year 2	0.5%
Year 3	1.0%
Year 4	1.5%
Year 5	2%

The estimated growth data is provided by the company for their future strategic planning on their anti-counterfeit project. In year 1, there will be no growth on the volume of good sold. However, as the time goes, there will be a slow increase of 0.5% every year.

There are many reasons to explain the growth. First, the buyers will not be lured into buying fake bags by using the application. Second, there are less counterfeits in the market which improves the brand image, therefore, sales volume is increased. Third, the application raised the public's attentions which have done a promotional effect to attract potential customers.

Table 5.6-Investment planning for the project

	Year 0	Year 1	Year 2	Year 3	Year 4	Year 5
Sales Increased	N/A	0	5,325,000	10,650,000	15,975,000	21,300,000
Less:						
Tag Cost	N/A	9,000,000	9,045,000	9,090,000	9,135,000	9,180,000
Maintenance	N/A	30,000	30,000	30,000	30,000	30,000
Administration	N/A	50,000	50,000	50,000	50,000	50,000
Equipment	300,000	-	-	-	-	-
Training	200,000	-	-	-	-	-
System	1,300,000	-	-	-	-	-
Profit	(1,800,000)	(9,080,000)	(3,800,000)	1,480,000	6,760,000	12,040,000

This is the investment planning for this five-year plan. The maintenance refers to the maintenance cost of both the equipment and the system. It is calculated according to the normal market rate, it charges the company 10% of the total equipment cost annually.

The administrative cost covers all the necessary cost generated from administrative works in the project. It is estimated around 50,000HKD per year as the project does not require the company too many resources.

The tag is estimated around 3HKD per each. Started from year 1, all bags will be embedded with tags for anti-counterfeiting purposes. That is the reason why the tag cost is very high in the investment planning table shown above.

There will be deficit for the first two years. The year 0 means the time that initial cost occurred. The company will start to have profit by the third year. The volume of goods sold grows slowly during that period.

Table 5.7-Financial Analysis of the Investment

	HKD	**Formula**
Total Investment	1,800,000	
Total Net Profit	5,600,000	
Returns on Investment	311%	=(Net Profit/Investment)*100 =(5,600,000/1,800,000)*100

Payback Period	2.64 years	=A+B/C
		A=Last Period with Negative Cash Flow
		B=Cash Flow At the End of Period A
		C=Total Cash Flow During the Period After A
		=2+(12,880,000/20,280,000)

The total net profit bought by this project is 5,600,000HKD which is the triple of the total investment. It gives 311% in the returns on investment. Although the payback period may be a bit longer, the investment result is satisfactory.

Chapter 6 – Discussions

6.1 Capability Assessment

Table 6.1-An overview of capability of different approaches

	Specific features-based authentication	Tag authentication	Location-based authentication	Weak authentication	Hybrid Authentication
Product authentication	✓	✗	✗	✓✗	✓
Tag authentication	✓✗	✓	✗	✗	✓
Location authentication	✗	✗	✓	✗	✓

Weak authentication is the weakest authentication method among all. Although a set of unique ID number stored in the tag might be able to help the examiner to track down the product data, or define its identity, it is more suitable for product tracking in supply chain management, but not anti-counterfeiting purpose. It is because the tag will be easily cloned together with the serial number, the authentication accuracy cannot be guaranteed.

Location-based authentication will only be able to authenticate the current location of the product by making use of trace and track capability provided by NFC tag. The trace- and-track will record the location and response to the server when there is a reading device reading the tag. No other information will be provided under this approach. Therefore, it fails to provide product and tag authentication.

Tag authentication aims at authenticating the tag itself, not the product. Therefore, no product or location authentication will be provided under this approach. The examiner will only focus on the tag embedded in the product itself.

Specific features-based authentication provides critical information of the product to the examiners for manual authentication. The examiner will base on that information provided to authenticate the product. It focuses on the product itself, not the tag.

However, as the examiner needs to get the information through a valid digital signature stored in the tag, the digital signature itself is a type of tag authentication. No locational record will be provided under this approach. Among all authentication approaches, hybrid approach is by far able to provide all three types of authentication including tag authentication, product authentication and location authentication.

Synchronized secret is developed for tag authentication by using one-time token. Specific-features provides information on physical anti-counterfeiting features for examiner to do manual product authentication E-pedigree shows the product tracking record which has extracted from the supply chain information system.

To conclude, the hybrid approach has combined all characteristics of different approaches that is by far the most comprehensive anti-counterfeiting approach.

6.2 Risk Assessment

6.2.1 Hybrid approach

The hybrid approach provides multiple authentications to the potential customer regarding to provide comprehensive and accurate. This approach mainly consists of two types of authentication which are intelligence authentication and manual authentication.

Table 6.2-Risk assessment result of hybrid authentication

Hybrid authentication	
Threat	Probability of happen
Tag Cloning	Low
Tag Removal and re-applying	Low
Manipulation of tag information	Low

The hybrid approach has high resistance towards tag cloning. The synchronized secret stored in the tag is designated for the threat. The authentication server will send a one-time token every time when the tag is being read and update it simultaneously with the tag. Therefore, when a tag is read by the application, the authentication sever can authenticate the tag at once.

Moreover, the tag authentication also supports the clone detection. When a tag being read by the application is found unmatched with the synchronized secret record stored in the database, an alarm will be triggered, the company will be able to trace the cloned tag for further follow-up.

For the tag removal and re-applying, this approach can provide a high resistance towards these two threats. The manual authentication eliminates the possibility of tag removal and re-applying. The authentication of physical anti-counterfeiting features, such as in-bag logos and sewing style, requires the users to examine the product very carefully.

If a tag is removed and re-applied to another counterfeit hand bag, the user can find that the characteristics of the bag being examined does not matched with the information and pictures shown in the application during the stage of specific features authentication.

Furthermore, counterfeits with the tag removed from the genuine bag will be found unmatched in the E-pedigree. The tracking record stored in the database server will reveal the cover to the counterfeits. Although the tag is being removed from the genuine bag, the counterfeiters are not able to forge the logistics record which is not stored in the tag. Therefore, the counterfeit bag cannot pass the examination during the stage of location authentication.

Although there is no sophisticated encryption protocol used in this approach, most of the conclusive information is stored in the database server in the company. The manipulation of tag information is not able to make a tag authentic. The tag is only a unique identifier to the authentication server. Any manipulation of tag information will not help in passing the application's authentication.

Also, the synchronized secret stored in tag is only a one-time token, the counterfeiters will not be benefited from copying that token to other tags as the token will be changed every time.

The examination of physical anti-counterfeit features also blocks the counterfeiters' attempts to manipulate the tag information. Manipulating Tag information cannot help passing the authentication so this approach has high resistance towards manipulating tag information.

Compared with the other four anti-counterfeiting approaches, this hybrid approach is obviously more appropriate to be applied in the designer bag industry.

Firstly, the specific features approach is designated for the product which are hard to be cloned. It requires the products with anti-counterfeit markings, such as laser printing. This type of anti-counterfeit marking may damage the aesthetic design of the bag.

However, under hybrid approach, it is only required the bag to have simple physical anti-counterfeit features, such as sewing style. This kind of feature is quite hard to be cloned because the manufacturers have given specific trainings and equipment to the cobblers for manufacturing the bag. Other features like leather striae are hard to be copied. It is because those materials are made-to-order and limited to be purchased.

Secondly, the hybrid approach has raised maximum cost-to-break which is hard to achieve in tag authentication approach since the latter over-replies on the encryption protocol of the tag. Once the encryption has been cracked by the counterfeiters, they can copy the tag easily. The cost on cracking the encryption protocol can be recovered by counterfeiting activities.

The hybrid approach has more diversified anti-counterfeiting measures and hence the counterfeiters are distracted by different measures and have to put more afford to break the anti-counterfeiting approach. The cost to break for the counterfeiters has been maximized. The profit by selling counterfeits may not be able to cover the cost to break the system.

Thirdlyl, the hybrid approach has allowed second-hand bag authentication which locational approach fails to achieve. As the second hand bag market has significant influences in fashion industry, therefore failing in authenticating second hand bag is not tolerant.

Fourth, although serial number authentication has been adopted in the hybrid approach, it is not the only anti-counterfeiting measure adopted. This has made a visible difference with the weak authentication approach which has only adopted one anti-counterfeiting measure.

6.2.2 Overviews

Table 6.3-The risk assessment of five approaches

	Specific features-based authentication	Tag authentication	Location-based authentication	Weak authentication	Hybrid authentication
Tag Cloning	Average	Low	High	Very High	Low
Tag Removal /Re-applying	Low	Very High	Low	Average	Low
Manipulation of Tag Information	Average	Low	Very High	High	Low

Specific Feature-based Authentication

The ideal product for specific features-based authentication is the type of product which is very hard to be cloned. Money note is one of the examples. It is very hard to copy the characteristics, especially those sophisticated anti-counterfeiting printing of the product so the preferred product under this approach is the type of product which has lots of anti-counterfeiting markings and printings for enabling the examiners to authentication according to the critical information given by the server.

Therefore, the probability of tag removal and re-applying is very low. The counterfeiters cannot just take off the tag embedded in the genuine product and apply to their fake product. The critical information given by the digital signature can easily reveal that product with the genuine tag is fake.

However, the approach does not put much emphasis on the resistance of tag cloning and manipulating tag information. It is strongly believed by the supporters that sharing the critical information of the product by the digital signature stored in the tag which is embedded in product to the examiner is already enough for anti-counterfeiting.

Besides, as the tag cost is very low, the tag does not able to provide enough security for product authentication. Counterfeiters can just clone the tag format and manipulate the tag's data and digital signature to the fake tag.

Given that the approach only provides a digital signature for very little tag authentication, it is overlooking the consequence of little resistance of manipulating tag information and tag cloning.

The digital signature written in the tag only is only used as a medium to connect an address where the critical information is contained with the device. It does not help to classify whether this tag is placed by the genuine manufacturer.

A loophole would be resulted due to little resistance of manipulation of tag information. It is possible for the counterfeiters to edit the tag information and replace the real digital signature by the fake one. As a result, the fake digital signature will provide the wrong information to the examiners for authentication.

Tag Authentication

Compared with the risk assessment result of specific features-based approach, the probability of the tag cloning happens under tag authentication approach is very small. It is because this approach put much emphasis on the security features of the tag. It uses sophisticated encryption method to prevent the tag from being copied.

Manipulation of the tag information cannot be altered easily due to the sophisticated encryption system of the tag. It takes many efforts for the counterfeiters to alter any data inside the tag.

Therefore, it takes much effort for the counterfeiters to crack the encryption method, the cost and resources consumed to crack the tag could be higher than the revenue earned from the counterfeiting activities. As a result, the probability of tag cloning and manipulation of tag information are very low under tag authentication approach.

However, for the tag removal and re-applying, the chances are very high under this approach. Although the information of the tag is highly impossible to be manipulated, it does not limit where the tag is placed.

The examiner does not know where the tag is originally from during the authentication process, also, the authentication server does not know where the tag is currently being placed, therefore, it has given a chance for the counterfeiters to re-apply the genuine tag, which is originally belong to another genuine bag, to their counterfeits.

Although there is high possibility of tag re-applying and removal for the tag authentication, it is not easy to get the genuine tag by the counterfeiters secretly. The counterfeiters have to pay large effort in obtaining genuine tag to combat the anti-counterfeit mechanism. They may not be able to cover the cost from doing counterfeiting activities.

However, the tag authentication only depends on its sophisticated encryption system of the tags. It ignores a fact that if the counterfeiters have enough resources, such as money and technology, to find the vulnerability of the encryption system, the tag authentication system will no longer be effective.

Location-based Authentication

For the tag cloning, the probability of happen is high. Normally, tag using location-based authentication approach is not given any cloning resistance, the tag is only responsible of reporting its current location to the authentication server, the examiner will authenticate the product through the tracking record given by the server. Therefore, it is easy to be cloned.

However, this approach has overlooked the consequences of no after-sales location record. Due to the ignorance in second-hand bag authentication, the counterfeiters may thereby clone the tag of sold items to pretend their fake bag is "99% new" genuine item. Therefore, this would make the anti-counterfeit mechanism ineffective.

The key success factor of this approach is 'how well the location of the genuine product is known' (Failimon, 2012). If the company does not know the location of the genuine product after the product is being sold, the counterfeiters can use this loophole to pretend their counterfeits as genuine second hand items. This is the major reason of why there is high tag cloning rate.

For the tag-removal and re-applying, it makes no sense to counterfeiters to re-apply the tags of genuine products to their counterfeits. Instead of getting genuine tags from the genuine products to apply for their counterfeits, they can just clone the tags. As the tags do not have cloning resistance, they can copy the tag easily.

The reason of little cloning resistance is that the tag is designed to report the current location back to the server, therefore, the manufacturers does not pay high effort to the security features of the tag itself. The counterfeiters can manipulate the tag information without consuming too many resources.

Therefore, it gives counterfeiters chances to modify the tags in order to make their counterfeits looks more authentic. The examiners may find difficulties to do the authentication.

Weak Authentication

There is high probability of tag cloning under weak authentication approach. The tag is used to store a set of serial number by simple encryption method. If the counterfeiters manage to get the serial number from the tag, they can use that number for their counterfeits.

Logically, the counterfeiters can remove the tag from the genuine product and re-apply to their counterfeit. However, because of the little tag cloning resistance, the counterfeiters do not need to remove the tag from original product to their counterfeit, they can just clone the tag, the cost is much lower.

Under this approach, the company does not put too many resources on the security features of the tag itself; they usually adopt a simple encryption method to hide the information stored in the tag. Therefore, if the counterfeiters are willing to put resources on cracking the encryption method, it is possible for them to manipulate the information stored in the tags

Conclusion

From the table shown, the hybrid approach is considered to be the most reliable and comprehensive anti-counterfeiting approach for designer bag industry.

It not only prevents the second-hand bag problem mentioned in the locational approach section, but also solves the tag removal and cloning problem brought by the tag authentication. It also enhances the authentication accuracy to a level which specific-features authentication approach cannot achieve.

6.3 Limitations

Although the application designed can provide accurate authentication to the customers and combat the anti-counterfeiting activities, there are few limitations brought it.

1. High initial cost

The whole anti-counterfeiting mechanism requires the company to invest large amount of money for acquisition of equipments needed, development of the application, setting up the clouding system and providing training, which the company may have to invest millions dollars initially that discourages SMEs to develop this application.

2. More complicated tag operation procedure

This hybrid approach has more complicated tag operation involved in the tag embedment and authentication procedure than others that is time-consuming. Also, the authentication procedure involves more tag data transfers, such as synchronized secret, it even involves tag re-write. More trainings are also needed for the staff responsible of tag operation.

3. High visibility in supply chain is required

The application requires high information transparency in supply chain. For example, the E-pedigree has put a strict condition on the product tracking section in supply chain management. It needs clear individual tracking record of the products. If the company did not have a visible supply chain, it might fail to provide data for the application. The application might not be very appropriate for the company without proper supply chain management.

4. Strict conditions for the application device

The application can only run on the Android phone. Although Android phone has obtained almost half of the cell-phone market, the market coverage is still not wide-enough. People using IOS system and Symbian are not able to use the anti-counterfeit application. Besides, the application also requires the cell-phone to be NFC-enabled. If the Android phone does not equipped with the NFC device, it cannot run the application. This has limited the user entry. There is only 1/3 of Android phone equipped with NFC function.

6.4 Effects on Supply Chain

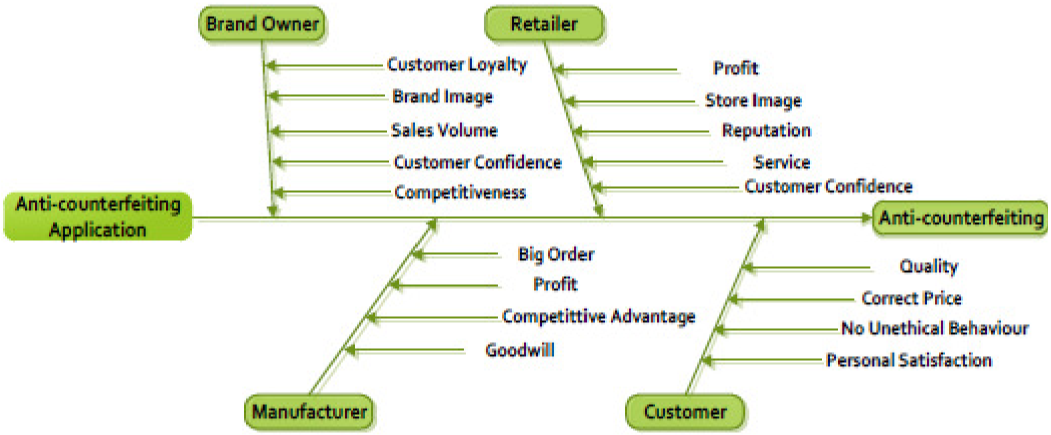


Figure 6.1-Diagram showing the cost and effect relationship of the application

The application has placed different effects on different stakeholders in the value chain. At all, there are generally four types of stakeholders involved in the supply chain which are brand owner, manufacturer, retailer and customer. The ultimate goal of the application is to combat counterfeiting activities.

For the brand owner, the application increases its sales volume by combating the counterfeiting activities. Customers will not be lured to buy fake bag by using the application. The anti-counterfeiting activities will decrease the number of counterfeits which people are harder to buy the counterfeit bags in the market, so they are forced to buy genuine bags. Therefore, the sales volume will be increased by forcing some buyers who tend to buy counterfeits before to buy genuine goods.

This can also achieve higher customer loyalty. The anti-counterfeit application makes people more ‘admire’ to the brand as the bags are hard to be cloned. The buyer will be more satisfied for bring the bags because there are very few counterfeit existed in the market, and people around them will not consider the bags as the counterfeits.

Better brand image can also be achieved by establishing the anti-counterfeit application. The application can protect the brand image by assisting the buyers from buying poor quality counterfeits. This can also enhance the customer satisfaction by providing them excellent authentication service during their shopping.

The application even enhances the brand's competitiveness compared with other designer brand rivals. Other competitors without the comprehensive anti-counterfeiting application will face more serious counterfeiting, bigger loss in sales volume and profit. Their brand image may be affected by those massive poor quality counterfeit bags. This makes the brand with the application more competitive and capable of getting more designer bag market share.

For the manufacturer, the increased sales volume of the bag has encouraged the brand owner to order more from the manufacturers, thus, the bigger and consistent order has won the manufacturers more profit. Also, the increase in sales volume of the brand owners will further increases the sales commission amount earned by the manufacturers. To conclude, there will be more profit for the manufacturer when the application is established.

The tag operation technology owned by the manufacturer has formed the competitive advantages among other factories. It represents that the manufacturer is capable of using latest anti-counterfeit technology for their products, which other rivals not yet control. This will make the manufacturer more competitive among the industry. Goodwill can be obtained from collaboration on application development and operation.

For the retailer, the sales volume of the genuine bags will be increased as there are less counterfeits existed in the market, customers are more willing to buy genuine bags for different reasons. The profit will be eventually increased.

The store image will be improved by being proved to sell genuine products in store, hence, the reputation of the store is increased. The customer confidence towards the store will also be enhanced as the store is authorized seller. Because of enabling the customer to use the application for authentication, better service can be achieved.

By using the application, the customer can buy quality bag by preventing themselves from buying counterfeits. Counterfeit bags are mostly made of poor quality materials or even some polluted materials. They may be harmful to the users such as causing allergy to them.

They can buy the genuine bag at a correct price in authorized stores. Some counterfeits are sold at retail price which cause financial losses to customers as they are cheated. With this application, the customers are able to buy the genuine bags with correct retail price and prevented from being defrauded by the counterfeiters.

By buying no fake bag, they prevent any unethical behavior, and at the same time, their personal desire can be satisfied by buying genuine products. They will have higher satisfaction which counterfeit bags cannot give.

Chapter 7 – Conclusions

In this project, there are two main goals which are combating the growing counterfeiting activities and raising the cost-to-break of counterfeiters. Therefore, an effective NFC-based mobile application has been developed to achieve these two goals. Compared with current applications, already available on the market, our application not only can authenticate the products but also can provide the possibility to report counterfeit products.

The NFC-based mobile application has been developed for designer bag manufacturer. Hybrid approach is the anti-counterfeiting approach developed and designated for the mobile application. It consists of four layers of security which are synchronized secret, specific feature, E-pedigree and serial number to offer an accurate and precise authentication to the potential customers from preventing them from buying the fake products.

System technology and architecture have been explained and analyzed in detail, together with the suggested tag embedment flow for the designer bag manufacturer. Trial run of the application has been implemented for evaluation.

For the discussion, capability and risk assessment have been done for the application and it also compares the results of different approaches with hybrid approaches. Among all five approaches, hybrid authentication has been considered as the most effective anti-counterfeiting measures and proved with highest resistances against different potential threats among all.

Although the application is proved to provide an accurate product authentication to the user, there are some limitations. The limitations are also discussed in the discussion part. The application requires high visibility in supply chain, and places strict conditions on the application devices. It also requires high investment cost, and the authentication procedure is far more complicated than other current anti-counterfeiting technologies such as bar code and laser printing. Despite the limitations, the application is proved to place positive influences on the whole supply chain.

There are still a lot of potentials for improvement. The company can also focus on the customer-relationship management by utilizing the application. In-app promotion would be one of the options. Therefore, the application will not be used as a authentication tool only, but also a tool to enhance and improve the customer-relationship.

At all, the application is able to combat the growing counterfeiting activities and raise the cost to break of the counterfeiters in designer bag industry. Although there are some limitations and disadvantages brought by the application, these obstacles can be overcome by the future technology advancement.

List of References

1. Ahson, S. (2008). RFID Handbook. : CRC Press.
2. Benyo, B., Vilmos, A. & Kovacs, K. (2007, July 7). NFC Applications and Business Model of the Ecosystem. 16th IST Mobile and Wireless Communications Summit, pp.1-5.
3. Bhardwaj, K. & Shenoy, M. (2009). Global anti-counterfeit packaging market for food and pharmaceutical – technologies & global markets.,
4. Biermann, C. J. (1996). Handbook of Pulping and Paper-making. San Diego: USA: Academic Press.
5. Blakeney, M. (2008). International Proposals for the Criminal Enforcement of Intellectual. Property Rights: International Concern with Counterfeiting and Piracy. Queen Mary School of Law Legal Studies Research Paper, 2009 (29).
6. Blanchard, D. (2007, May Date). How to Fix a Leaky Supply Chain. How to Fix a Leaky Supply Chain, p..
7. Boxall, G. (2000). The Use of RFID for Retail Supply Chain Logistics. London: The Commonwealth Conference & Events Centre.
8. Briseno, M. (2012). International Proposals for the Criminal Using RFID/NFC and QR-Code in Mobile Phones to Link the Physical and the Digital World., .
9. Capps, C. (2001). Near field or far field? : EDN.
10. Cointalk (2011). . Retrieved December 3, 2012 from http://www.cointalk.com
11. Counterfeiting Intelligence Bureau (2012). . Retrieved October 5, 2012 from http://www.icc-ccs.org/icc/cib
12. European Commission (2011). . Retrieved November 3, 2012 from http://ec.europa.eu/index_en.htm
13. Filimon, E. (2012). Anti-counterfeiting – Prevention of counterfeit products with

RFID., .

14. Finkenzeller, K. (2000). RFID Handbook. West Sussex: John Wiley & Sons Ltd.
15. Finkenzeller, K. & Muller, D. (2010). RFID handbook. : Wiley-Blackwell.
16. Fressancourt, A., Hérault, C. & Ptak, E. (2008). NFCSocial: Social networking in mobility through IMS and NFC., .
17. Frost & Sullivan (2011). "NFC: When will be the Real Start?"
18. Gentry, J. W., Purtrevu, S. & Shultz, C. (2001). How Now Ralph Lauren? the Separation of Brand and Product in A Counterfeit Culture. Advances in Consumer Research, 28 (258-265).
19. Gould, L. S., Hérault, C. & (2000). What you need to know about RFID. Automotive Manufacturing & Production, 112 (2), 46-49.
20. Grossman, G. M. & Shapiro, C. (1988). Foreign counterfeit of status goods. The Quarterly Journal of Economics C111, (412), 79-100.
21. Harrop, P. (2006, September Date). Contactless cards vs RFID enabled phones. Contactless cards vs RFID enabled phones, p.9.
22. Hartmann, T. (2010, April 3). Applying RFID technology across the factory floor. The Industrial Ethernet Book, pp.20-21.
23. Hologram Solution (2011). . Retrieved December 3, 2012 from http://www.hologramsolution.com/
24. Hopkins, M. P. (2003). Counterfeiting exposed: Protecting Your Brand and Customers. : Hoboken: John Wiley & Sons.
25. Innovision Research & Technology Plc (2013, January). Near Field Communication in the real world - part II: Using the right NFC tag type for the right NFC application. , p..
26. International Association of Conference Centers (2012). . Retrieved October 10, 2012 from http://www.iacconline.org/
27. International Organisation for Standardisation (2004). Near Field Communication -

Interface and Protocol (NFCIP-1). :,

28. Jones, N. (2008). Important Mobile and Wireless Market Directions, 2008 to 2012. Gartner Research, .
29. Kelly, C. J. (2006). The Cost of Encryption. Retrieved November 11, 2012 from http://www.iccwbo.org/
30. Lehtonen, M. & Fleisch, E. (2012). The Potenital of RFID and NFC in Anti-Counterfeiting., .
31. Lehtonen, M., Michahelles, M. & Flesich, E. (2007). Trust and security in RFID-based Product Authentication Systems. IEEE Systems Journal, Special Issue on RFID Technology: Opportunities and Challenges, 1 (2).
32. Lewis, K. (2012). The fake and the fatal: The Consequences of Counterfeits. The Park Place Economists Volume XVII, .
33. Mallor, J. P. (2007). Business Law: The Ethical, Global, and E-commerce Environment. New York: The McGraw-Hill Companies.
34. Merina, M. & Mariño, P. (2011). Supply Chain Management in International Logistics – RFID Applications. :,
35. Microtrace Solution (2011). . Retrieved December 3, 2012 from http://microtracesolutions.com/
36. Miller, B. & Bisdikian, C. (2001). Bluetooth Revealed: The Insider's Guide to an Open Specification for Global Wireless Communications. New Jersey: Prentice-Hall.
37. Mullen, J. (2007). The application of RFID technology in a port. : AIM Global.
38. NFC mobile payment pilot in Holland. (2006, June 5). Card Technology Today,, pp.3-16.
39. NFC technology in six month trial. (2005, December 5). Card Technology Today,, pp.11-12.
40. Oded, G. (2004). Foundations of Cryptography: Volume 2, Basic Applications. :

Cambridge university press.

41. Organization for Economic Co-operation and Development (2007). The Economic Impact of Counterfeiting and Piracy. Paris: OECD Publications.

42. Philips, T. (2005). Knockoff: The Deadly Trade in counterfeit goods. London: Kogan Page Limited.

43. Power, G. (2012). Anti-counterfeit technologies for the protection of Medicines. World Health Organization:,

44. Preradovic, S., Balbin, I., Nemai, C. & Swiegers, G. (2008). A Novel Chipless RFID System Based on Planar Multiresonators for Barcode Replacement. : IEEE International Conference on RFID.

45. Resatsch, F., Sander, U. & Leimeister, J. M. (2008). Do Point of Sale RFID-Based Information Services Make a Difference? Analyzing Consumer Perceptions for Designing Smart Product Information Services in Retail Business. Electronic Markets, 18 216-231.

46. Secure Pharma, C. J. (2006). Anti-counterfeit has immense growth potential in the Asian market. Retrieved November 17, 2012 from http://www.securingindustry.com/

47. The International Chamber of Commerce (2011). . Retrieved November 9, 2012 from http://www.iccwbo.org/

48. United Nations Office On Drugs and Crime (2011). . Retrieved November 11, 2012 from http://www.iccwbo.org/

49. US Chamber of Commerce (2012). . Retrieved October 16, 2012 from www.thetruecosts.org

50. Vazquez-Briseno, M., Hirata, F. I., de Dios Sanchez-Lopez, J., Jimenez-Garcia, E., Navarro-Cota, C., & Nieto-Hipolito, J. I. (2012). Using RFID/NFC and QR-Code in Mobile Phones to Link the Physical and the Digital World. Interactive Multimedia. Dr Ioannis Deliyannis (Ed.). InTech, 219-242.

51. Webb, W. (2007). Wireless Communications: The Future. : John Wiley & Sons.

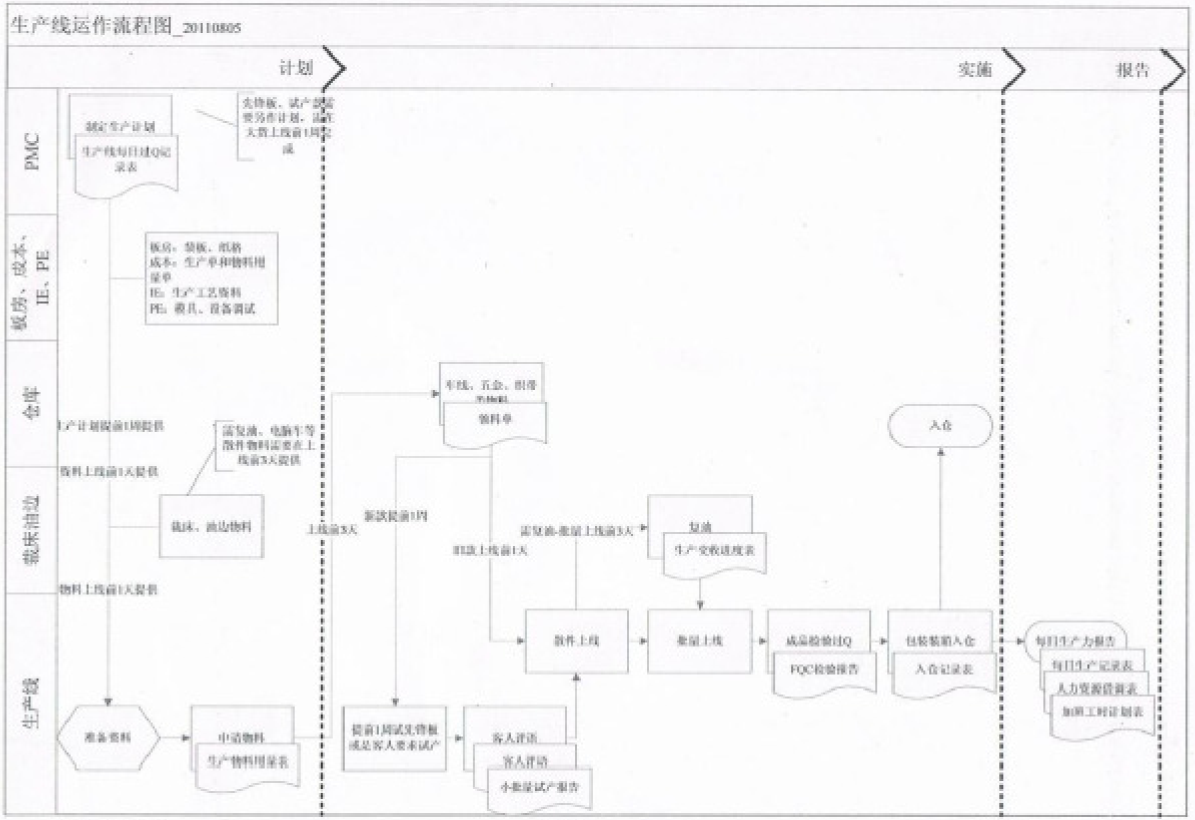
52. White Horse Laboratories (2012). Counterfeit Prevention. Retrieved October 3, 2012 from http://whitehorselabs.com/services/counterfeit-prevention/

53. World Customs Organization (2011). . Retrieved November 9, 2012 from http://www.wcoomd.org/

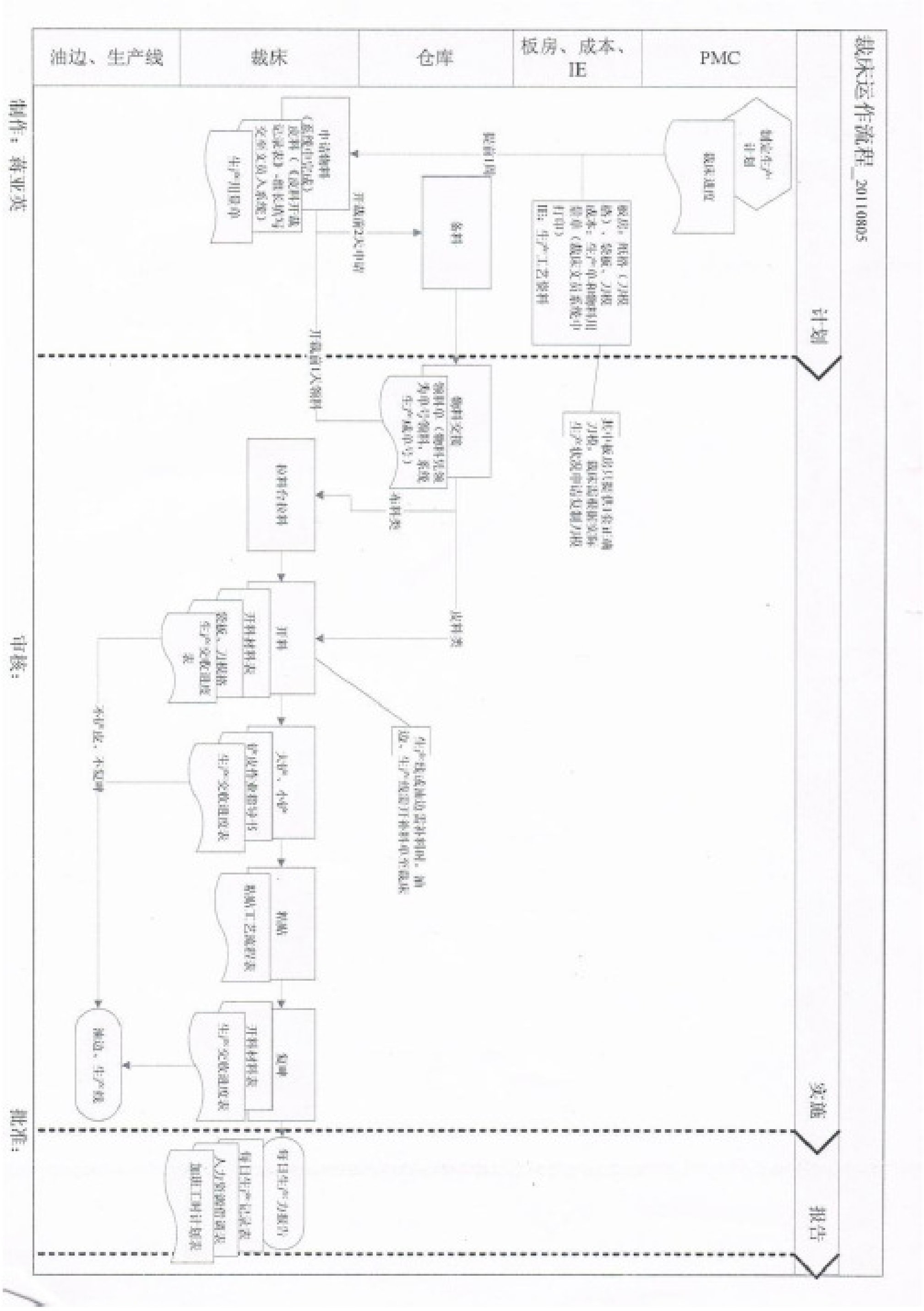
54. Wu, N. C., Nystorm, M. A. & Lin, T. R. (2011). Challenges to global RFID adoption. Science Direct.

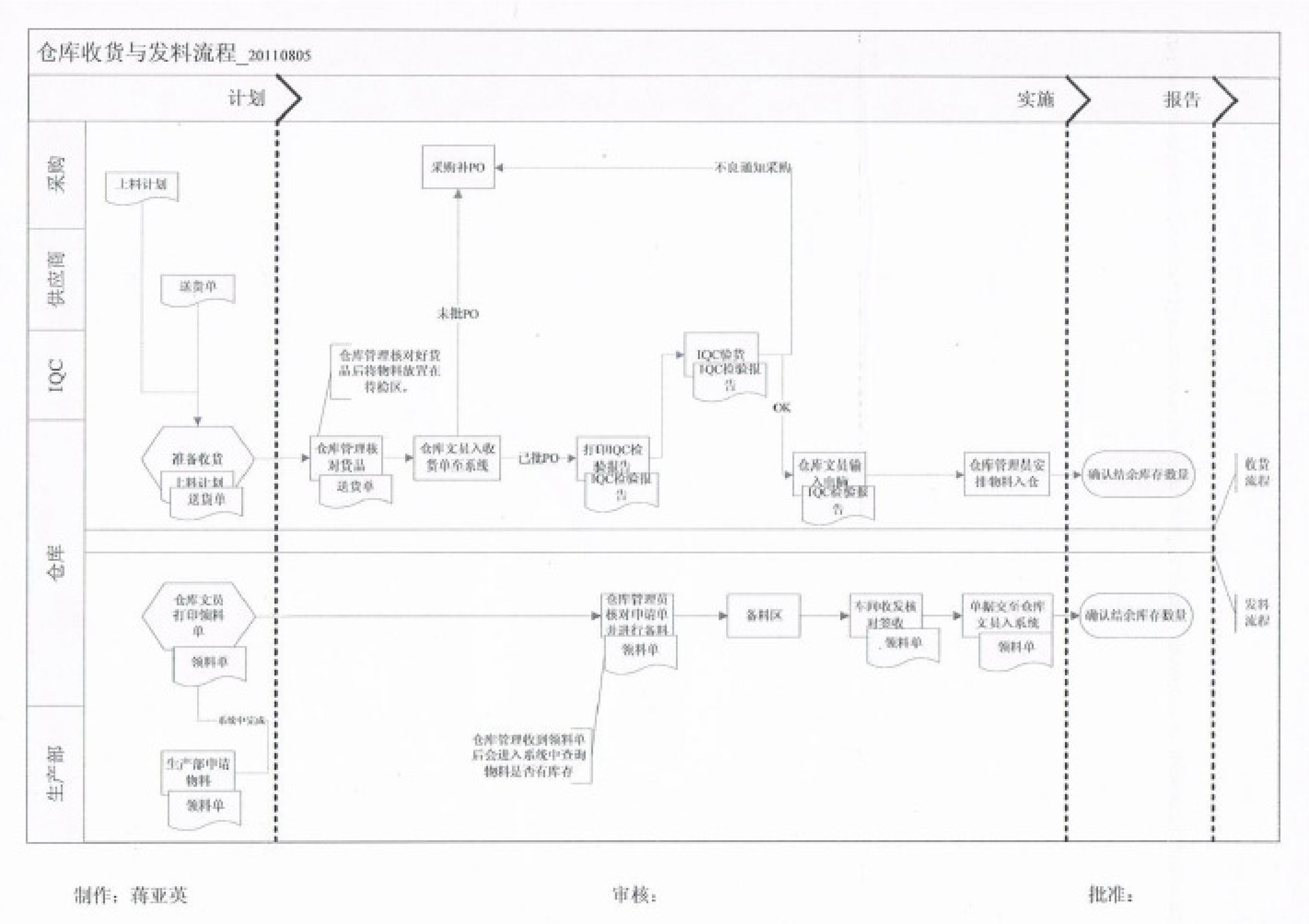
Appendices

Appendix A – Workflows of Designer Bag Manufacturer


生产线运作流程图_20110805
计划
实施
报告
PMC
板房、成本、IE、PE
仓库
裁床油边
生产线
制定生产计划
生产线每日达Q记录表
先修板、试产款需要另作计划，须在大货上线前1周完成
板房：禁板、纸格
成本：生产单和物料用量单
IE：生产工艺资料
PE：模具、设备调试
生产计划提前1周提供
物料上线前1天提供
需复油、电脑车等散件物料需要在上线前3天提供
裁床、油边物料
物料上线前1天提供
准备物料
申请物料
生产物料用量表
上线前3天
车线、五金、担带等物料
领料单
新款提前1周
旧款上线前1天
需复油-批量上线前3天
提前1周试先修板或是客人要求试产
客人评估
客人评估
小批量试产报告
散件上线
复油
生产变化进度表
批量上线
成品检验过Q
FQC检验报告
包装装箱入仓
入仓记录表
入仓
每日生产力报告
每日生产记录表
人力资源借调表
加班工时计划表

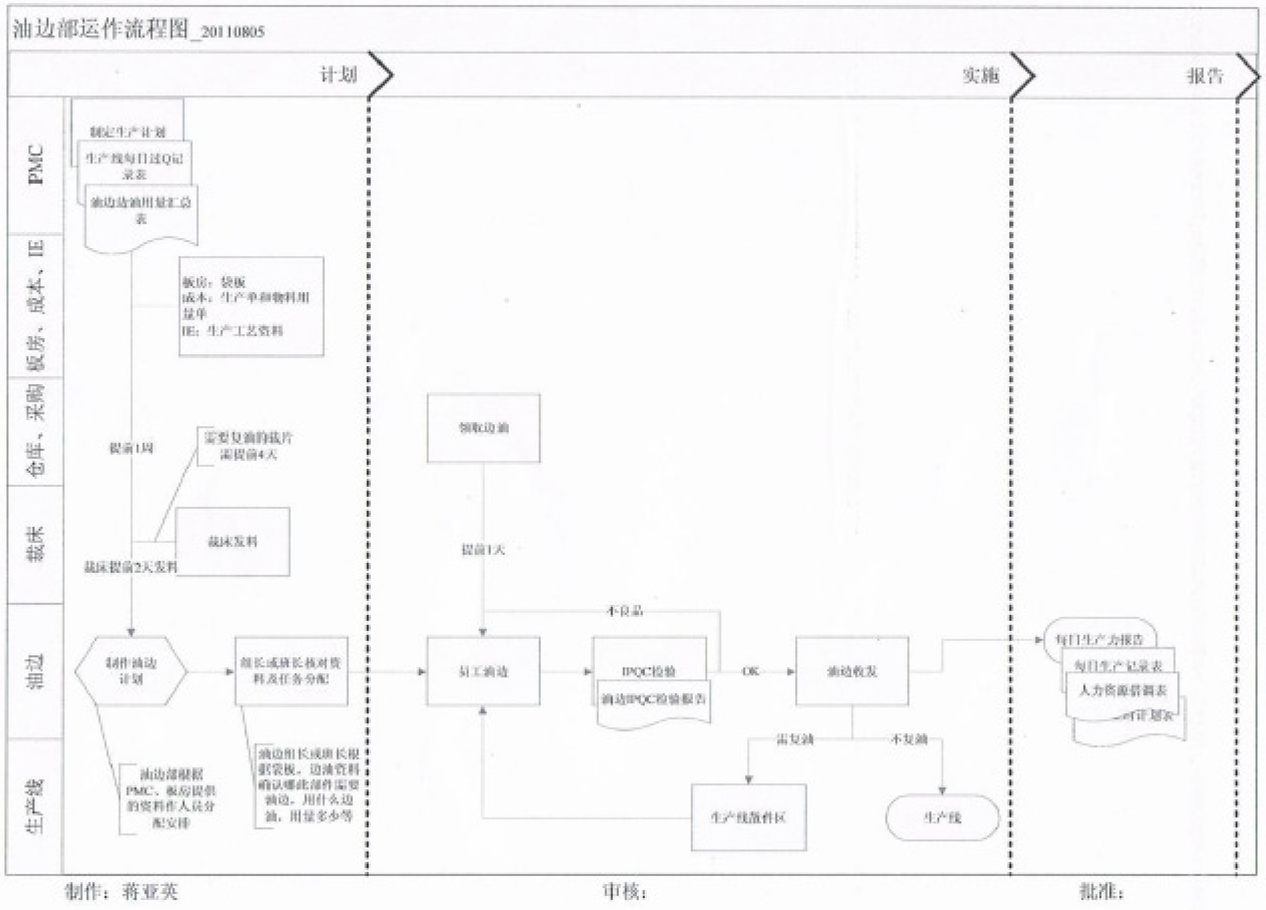
制作：蒋亚英　　审核：　　批准：


裁床运作流程_20110805
计划
实施
报告
PMC
板房、成本、IE
仓库
裁床
油边、生产线
制定生产计划
裁床进度
板房：纸格（刀模格）、袋板、刀模
成本：生产单和物料用量单（裁床文员系统中打印）
IE：生产工艺资料
其中板房只提供1套正确刀模，裁床需根据实际生产状况申请复制刀模
提前1周
备料
开裁前2天申请
申请物料（系统中完成）
皮料（《皮料开裁记录表》-组长填写交至文员入系统）
生产用量单
开裁前1天领料
物料交接
领料单（物料员领为单号领料，系统生产成单号）
布料类
皮料类
拉料台拉料
开料
开料材料表
袋板、刀模格
生产交收进度表
生产线或油边需补料时，油边、生产线需开补料单至裁床
大铲、小铲
铲皮作业指导书
生产交收进度表
粘贴
粘贴工艺流程表
复啤
开料材料表
生产交收进度表
不铲皮、不复啤
油边、生产线
每日生产力报告
每日生产记录表
人力资源借调表
加班工时计划表
制作：蒋亚英
审核：
批准：



仓库收货与发料流程_20110805

制作：蒋亚英　　审核：　　批准：


油边部运作流程图_20110805
计划
实施
报告
PMC
板房、成本、IE
仓库、采购
裁床
油边
生产线
制定生产计划
生产线每日过Q记录表
油边边油用量汇总表
板房：袋版
成本：生产单和物料用量单
IE：生产工艺资料
提前1周
需要复油的裁片需提前4天
裁床发料
裁床提前2天发料
制作油边计划
组长或班长核对资料及任务分配
油边部根据PMC、板房提供的资料作人员分配安排
油边组长或班长根据袋板、边油资料确认哪些部件需要油边，用什么边油，用量多少等
领取边油
提前1天
员工油边
不良品
IPQC检验
油边IPQC检验报告
OK
油边收发
需复油
不复油
生产线散件区
生产线
每日生产力报告
每日生产记录表
人力资源借调表
计划表
制作：蒋亚英
审核：
批准：

Appendix B – Questionnaire Results

Study on anti-counterfeit issues in Designer Bags

Dear Sir/Madam,

We are students from the Department of Industrial and Systems Engineering, The Hong Kong Polytechnic University. We are conducting a project on the anti-counterfeiting technology in designer bag industry.

It would be appreciated if you can take few minutes to complete the questionnaire. Your information is essential and critical in my study on anti-counterfeiting. All information collected is confidential and will be destroyed when project is finished. Thank you for your participation.

Counterfeit Issue

1. Have you ever bought counterfeit designer bag (i.e. bags with brand) before?

□ Yes □ No

2. Do you think the counterfeit bag will influence the original brand image?

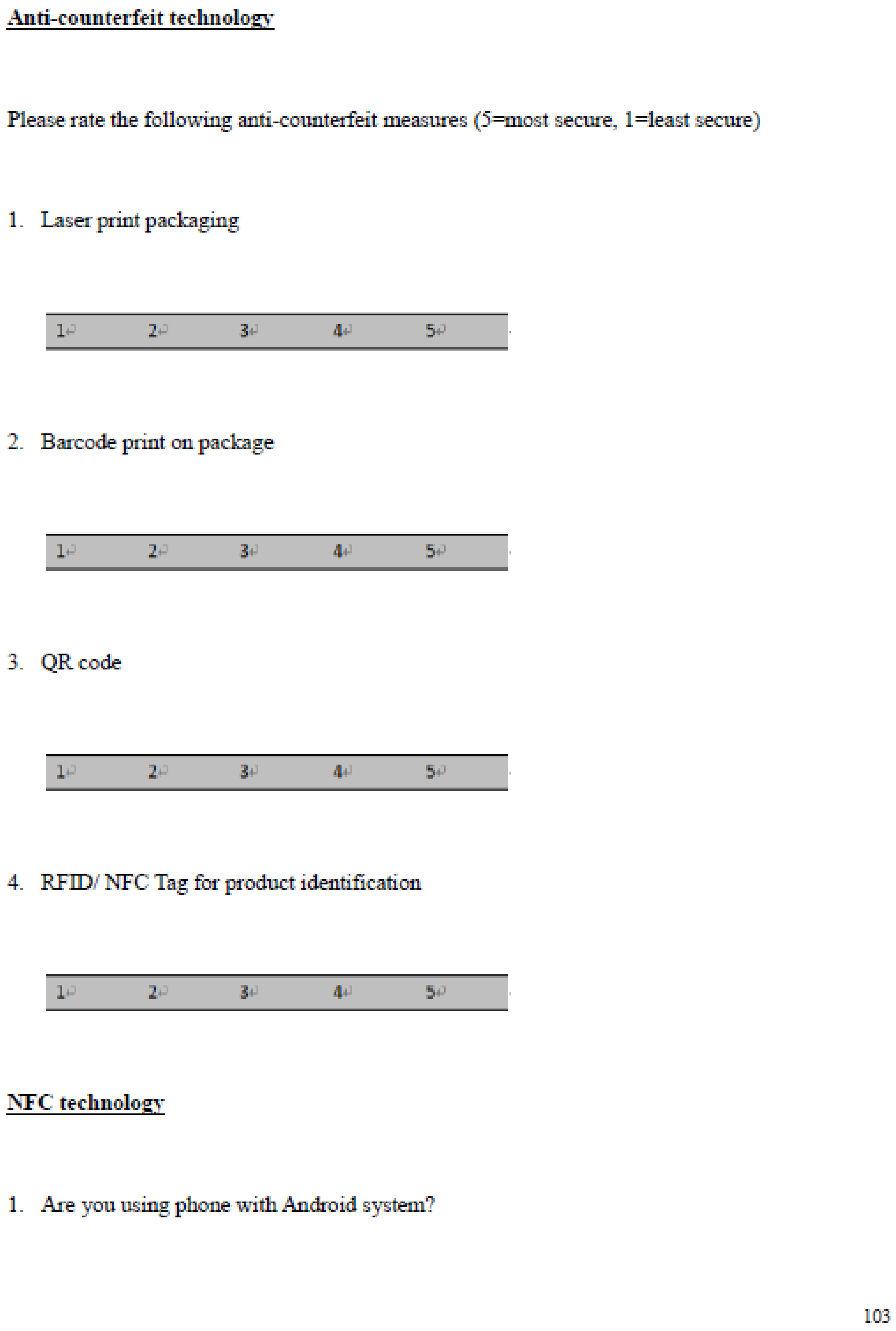
□ Yes □ No

3. Do you think the counterfeit designer bag will affect the sales of original brand?

□ Yes □ No

4. Do you want to buy genuine designer bag in the future?

□ Yes □ No



Anti-counterfeit technology

Please rate the following anti-counterfeit measures (5=most secure, 1=least secure)

1. Laser print packaging

1↵	2↵	3↵	4↵	5↵

2. Barcode print on package

1↵	2↵	3↵	4↵	5↵

3. QR code

1↵	2↵	3↵	4↵	5↵

4. RFID/ NFC Tag for product identification

1↵	2↵	3↵	4↵	5↵

NFC technology

1. Are you using phone with Android system?

□ Yes □ No

2. Have you heard of NFC?

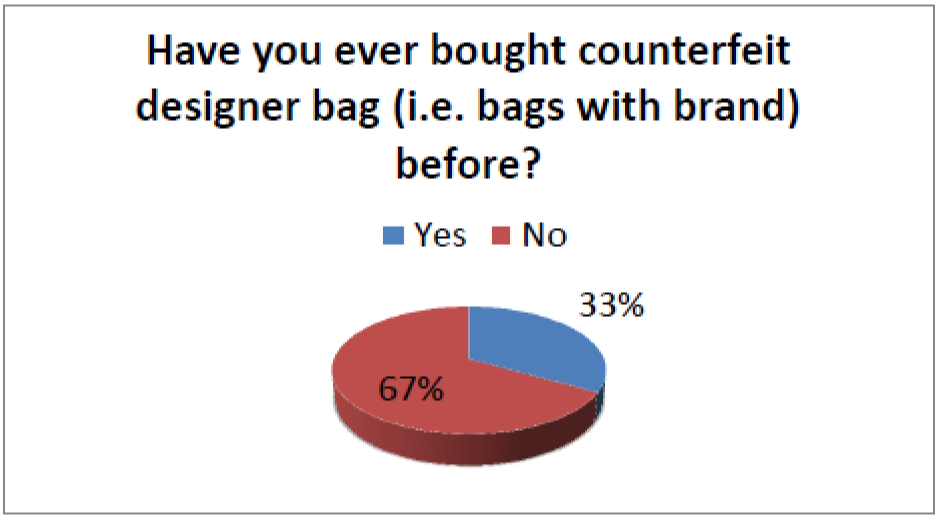
□ Yes □ No

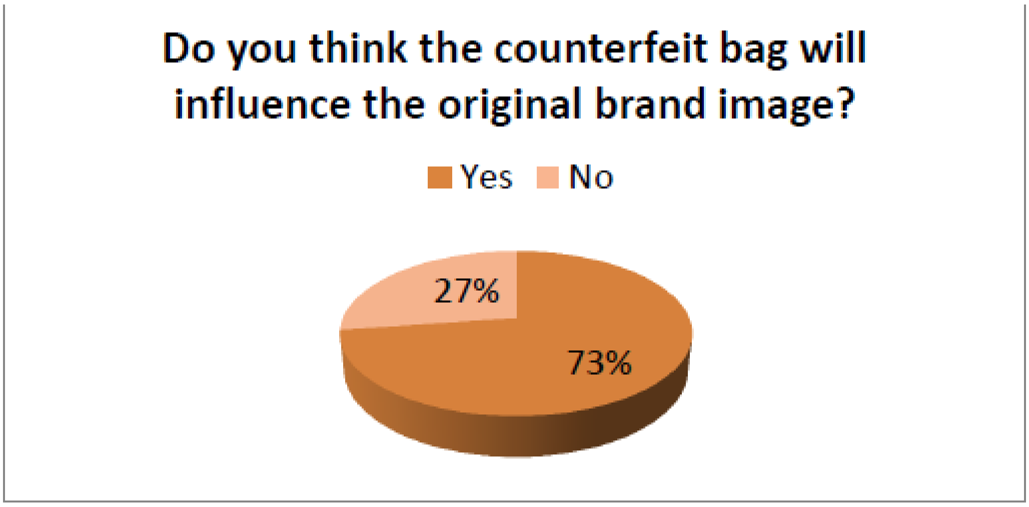
3. Have you used NFC application before?

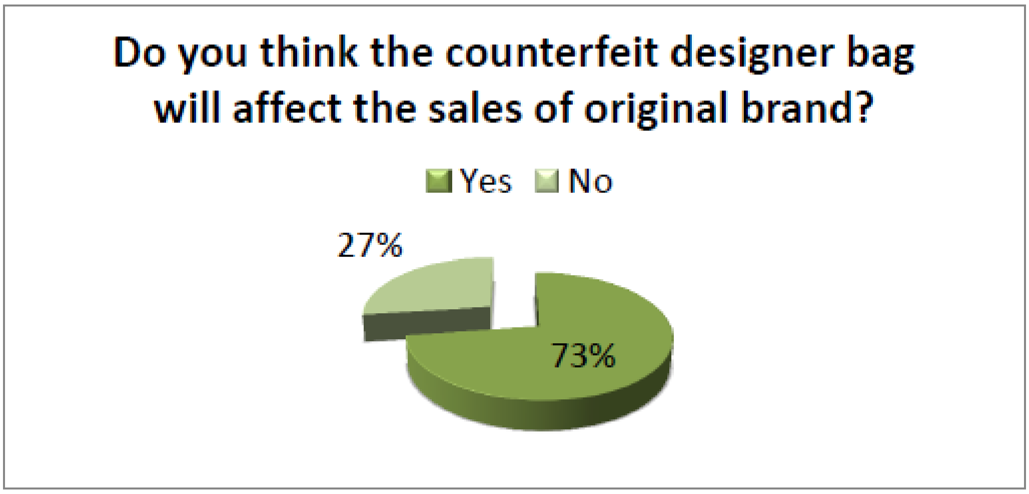
□ Yes □ No

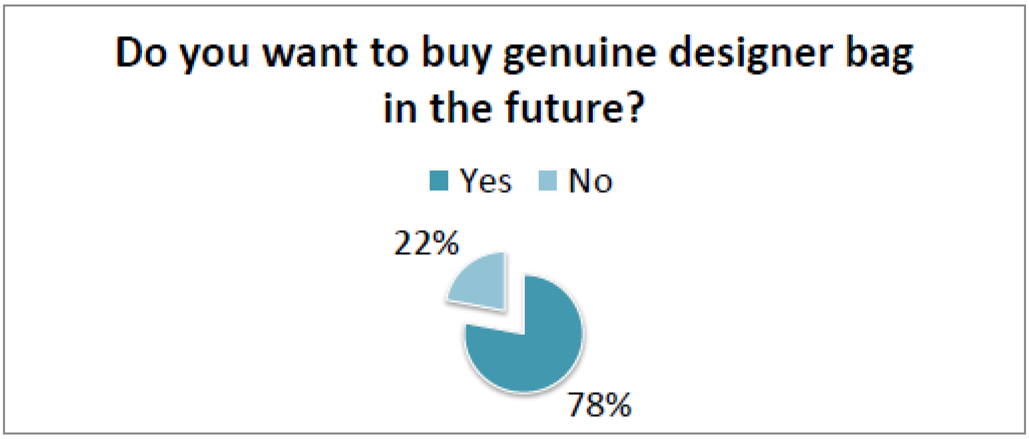
Results

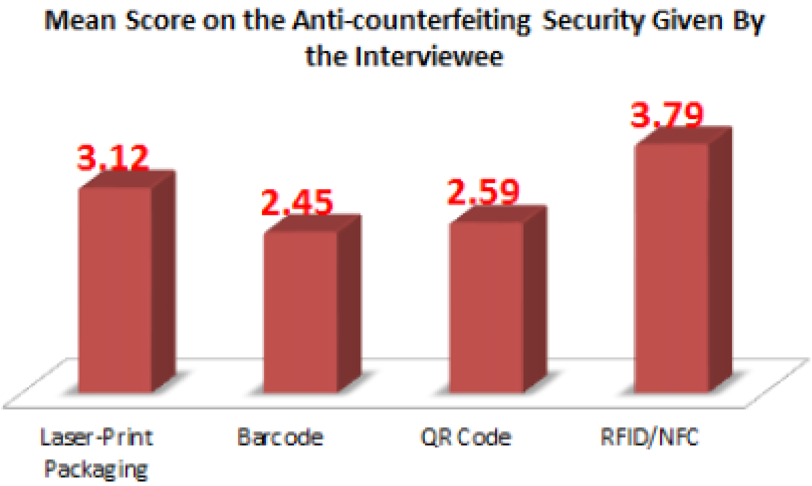
Response Rate		
Questionnaire Distributed	Response Received	
70	66	94.29%

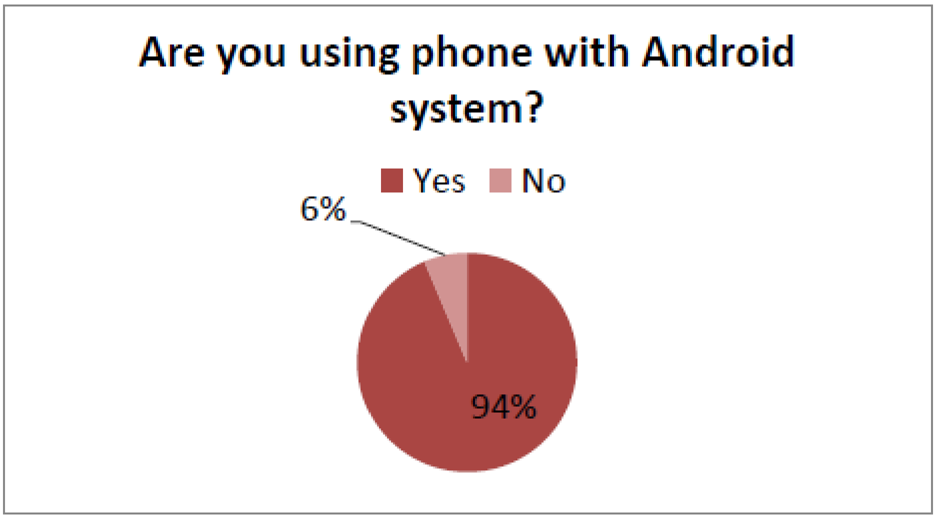



Do you think the counterfeit bag will influence the original brand image?

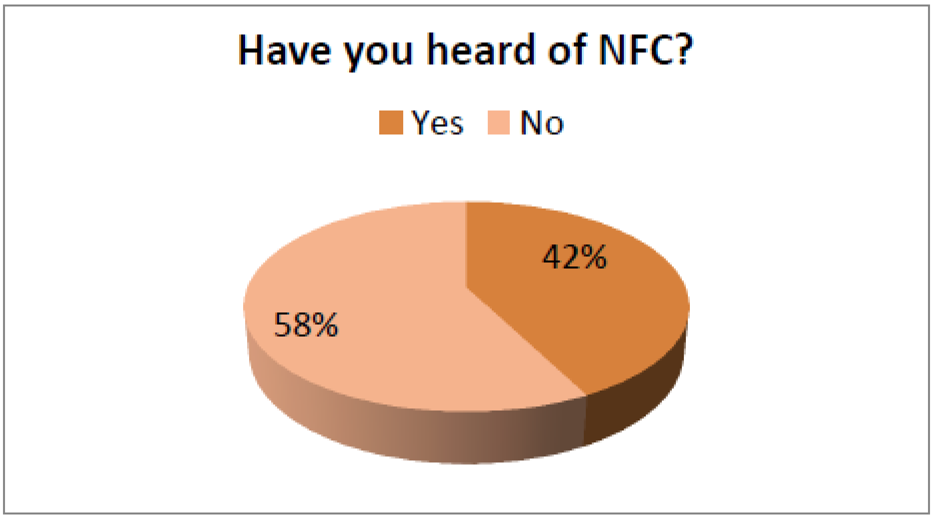

Do you think the counterfeit designer bag will affect the sales of original brand?

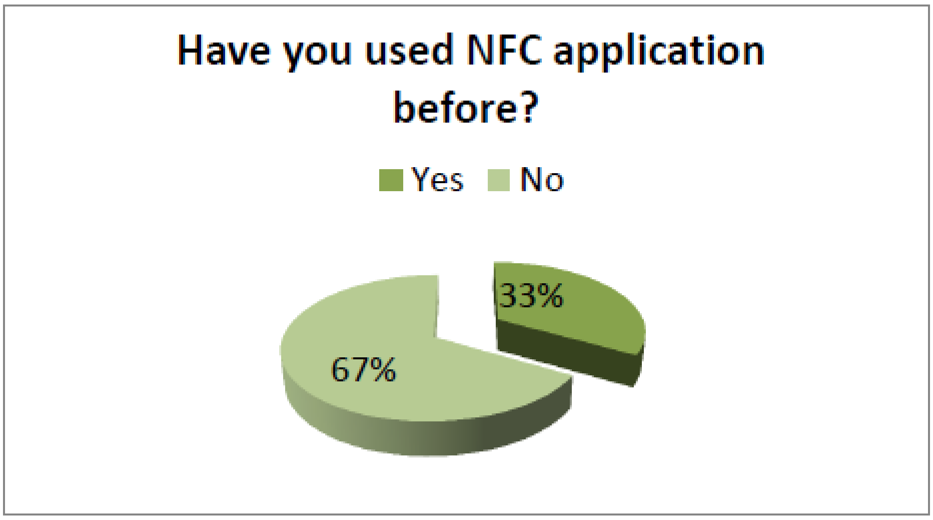

Do you want to buy genuine designer bag in the future?


Mean Score on the Anti-counterfeiting Security Given By the Interviewee
3.12
2.45
2.59
3.79
Laser-Print Packaging
Barcode
QR Code
RFID/NFC


Are you using phone with Android system?
Yes
No
6%
94%

106


Have you heard of NFC?
Yes
No
42%
58%


Have you used NFC application before?
Yes
No
33%
67%