行動雲端書櫃之應用服務

薛夙珍 副教授
朝陽科技大學資訊管理系
schsueh@cyut.edu.tw

邱亭儒
朝陽科技大學資訊管理系
s10014607@cyut.edu.tw

摘要

因為行動商務的發展成熟，人們的行動裝置不只是用來記事、聽歌，也可以用來看電子書。用戶從數位書城購買電子書之後，常常會需要使用特定的電子書閱讀軟體才可閱讀，對使用者來說，消費者如果在多家數位書城進行挑選或是比價，然後購買電子書，必須搭配各家書店提供的電子書閱讀軟體閱讀。因此，可以將雲端運算的特性，運用在電子書環境裡，整合來自不同數位書城的電子書，並且支持各類型電子書格式，從不同書城所購買的電子書都可以儲存在同一個地方，只要用行動書櫃的雲端閱讀器就可以閱讀電子書，達到整合電子書功能。行動書櫃同時也提供分享以及離線閱讀機制，同時行動書櫃也可以擔任交易認證單位，保護用戶消費資訊的安全。

關鍵詞： 資訊安全、行動商務、雲端應用、電子書

Abstract

Since the full development of mobile commerce, the mobile devices not only used as take notes and listen to music, also read e-books. In general, consumers have to use specific device to read e-books after buying from online bookstores. For users, if they comparing the price, choosing and buying books from online book stores, they have to read e-books with the reading software which bookstore provided. Therefore, the characteristic of cloud computing can be used in the environment of e-books to integrate e-books from different online bookstores and support various types format of e-books, so that the e-books from different bookstores can be stored in same place. As long as consumers use the cloud reader of Mobile-Bookcase to read may achieve the integration of e-books. The Mobile-Bookcase also provide the sharing and offline reading mechanisms, also serve as the role of trading certification to protect the security of consumers' information.

Keywords : Information Security、Mobile Commerce、Application of Cloud Computing、E-book

1. 緒論

行動商務是指商品或服務的交易過程使用行動裝置並透過無線網路來達到一種交易行為[4]。隨著行動設備的發展成熟，以及行動網路的穩定，造就了行動商務近年來受到企業與消費者的重視。當行動商務應用和雲端運算進行結合，透過雲端運算，將資料儲存在網路上，再同步到行動裝置內，讓用戶無論何時、何地、何種裝置都可以存取資料。人們的行動裝置不只可以用來記事、聽歌，也可以用來閱讀電子書。

電子書，顧名思義就是將書本轉成電子化文件，並且使用電子載具閱讀。用戶下載電子書之後常常會需要書城所提供的電子書閱讀軟體才可閱讀，對使用者來說，消費者會在多家電子書店進行挑選或是比價，然後購買電子書，若是從不同書店購買的電子書，就必須搭配各家書店提供的電子書閱讀軟體閱讀，如果每一次都購買了來自不同書城的電子書，就

必須下載一次閱讀軟體，久而久之除了會造成載具的儲存空間消耗，消費者沒辦法很簡單的就可以知道他已經購買過哪一本電子書，無法對自己購買的每一本電子書進行管理，因此也影響了消費者閱讀電子書的效率。

本研究希望利用雲端運算結合行動商務的概念，運用在電子書環境裡，整合來自不同數位書城的電子書，並且支持各類型電子書格式，讓消費者從不同書城所購的電子書都可以儲存在同一個地方，並且只要用行動書櫃的雲端閱讀器就可以閱讀電子書。

1.1 研究動機

由於現在市面上販售電子書的數位書城很多，但不是每一本書都可以在每一間數位書城買到，有些數位書城可能只提供特定種類的電子書，消費者如果在很多數位書城購買電子書，消費者就必須下載數位書城的閱讀軟體，一旦購買來源多了，消費者在閱讀來自不同的數位書城所購買來的電子書的過程，需要對數個閱讀器反覆開啟尋找所需的書籍，多款閱讀軟體也耗減消費者裝置的儲存空間。因此，消費者會需要整合來自不同數位書城所購買到的電子書，也要解決消費者必須安裝數個閱讀軟體的問題。

雖然目前電子書大多在行動裝置上閱讀，但是消費者的裝置未必都處於連線狀態，因此本研究希望能夠讓消費者在離線的狀態下也可以閱讀電子書。因此提出一個電子書離線閱讀功能，讓消費者可以下載電子書到裝置內，無論在何時、何地都可以閱讀電子書。消費者閱讀電子書不該被「是否有連線網路」而限制。但是當電子書被下載到本機裝置，就必須顧及到電子書是否會在下載後被任意散播的可能，同時也要考量下載的電子書會不會占用太多儲存空間，因此需要一個滿足以上需求的離線的電子書閱讀機制。

在實體書市場，書局通常會提供未封裝的實體書讓消費者直接在書局閱讀，消費者可以在閱讀部分內容後決定是否購買。也有消費者在閱讀完整本書內容後仍然購買該本書籍。現代人取得實體書籍的管道很多，可以直接去實體書局、網路書局選購，甚至部分書籍對消費者來說只是臨時需要該本書籍...或其他理由，遇到這種情況時，消費者可以選擇去圖書館借書來看。而當書籍轉化成電子書之後，在電子書市場裡，也應該要提供消費者試讀的服務，以便消費者決定是否購買此本電子書。可以透過分享的概念讓消費者向其他行動書櫃的用戶借電子書來試讀。

1.2 研究目的

為了解決上一節所提到的問題，提出一個整合電子書於行動雲端書櫃的應用服務，以下為本研究之目的：

(1). 整合不同數位書城的電子書：
利用雲端運算可以達到隨處網路存取、資源彙整、高度彈性的特點來運用在行動書櫃裡，整合以及儲存來自不同書城的電子書，並且直接在行動書櫃的雲端閱讀器進行閱讀，不需要再下載各間數位書城所提供的閱讀器。當行動書櫃收到數位書城傳送來的電子書後，會先對電子書進行格式轉換(TXT、DOC、HTML、CHM、PDF)，統一轉換為 EPUB 電子書格式，即便數位書城所販售的電子書格式都不同，都可以在雲端閱讀器上進行閱讀。

(2). 行動書櫃擔任認證交易第三方：
由行動書櫃擔任交易第三方，減少用戶到不同的數位書城購買電子書時，必須將個人資料留在多間數位書城資料庫內的機會，無論用戶從幾間數位書城購買幾本書，用戶都只需要選擇在同一個地方進行付款，減少用戶個人資訊洩漏的機會。透過由行動書櫃擔任交易對象以及認證第三方的作法，數位書城不會知道用戶的交易資訊，例如：信用卡號碼。

用戶可以在行動書櫃告知用戶付款時，再選擇信用卡、線上 ATM 或超商付款。

(3). 在行動書櫃上分享電子書：
在分享的部分會採用帳號認證方式，當用戶將電子書分享給共享者，自己就不能夠閱讀該本電子書。用戶如果要分享電子書給其他用戶，必須先向行動書櫃申請分享帳號，用戶獲得此帳號後將帳號給要分享的用戶-共享者。共享者只要在登入時也輸入分享帳號就可以在連線的狀態下閱讀電子書。

(4). 提供離線閱讀：
為了讓用戶無論是否有網路環境都可以閱讀電子書，因此提供離線閱讀機制。但是離線閱讀必須克服檔案不被轉傳以及不會佔住太多儲存空間的問題。當用戶選擇下載電子書到裝置進行離線閱讀時，行動書櫃會將電子書切割成數個小檔案，更換檔案名稱為隨機命名的流水號，利用位移的作法，儲存到本機端。竊取檔案者無法知道檔案重組的順序，即使被任意移動到別台裝置，也無法輕易重組檔案，因為只有行動書櫃知道檔案重組的排序方式。所以用戶即使進入本機的資料夾複製檔案到別處也無法進行閱讀。用戶可以在雲端閱讀器裡設定，是否要在連到網路後就把已下載的電子書刪除。

2. 文獻探討

在此一章節會探討行動雲端書櫃應用服務所運用的文獻內容。

2.1 雲端運算

雲端運算[6]，就是利用遠端的伺服器使用虛擬化的方式進行管理，再將資源分配給不同的公司或單位。對於公司應用方面，每間公司不需要購買一台伺服器來運作公司資源，而是向資料中心以租用的方式取得遠端伺服器的空間來運算公司資源，公司在擴充資源時不需要購買更大台的伺服器只需要租用更多的伺服器空間；對於個人應用方面，使用者可以不需要購買大容量的硬碟，只要將資料都放在遠端的伺服器空間裡，在權限範圍內可以任意的存取、分享。也不需要在個人電腦裡安裝軟體，只需要連上網路開啟網頁，就可以使用軟體，而軟體的運算效能也是利用遠端伺服器來運作，資源會在網際網路上流通，並且在網際網路上共享運算資源，使用者或公司只要透過網路就可以直接取得資料或資源[2]。資料中心透過虛擬環境的資源分享，因為使用虛擬環境進行控管，使得運算更加彈性，並且提供即時性的服務，而且是以隨收隨付的方式計算價格，以上幾項條件成立即為雲端運算[5]。

美國國家標準暨技術機構 (National Institutes of Standards & Technology，NIST)對雲端運算進行了定義，並且定義為一種概念模式(Peter Mell and Tim Grance, 2009) [7]，在這個定義裡，包括了五個特徵，四個部屬模型，三個服務模式。

在五個特徵的部分，包括隨選自助服務(On-Demand Self-Service)、無所不在的網際網路(Broad Network Access)、共享運算資源(Resource Pooling)、服務屬於快速且彈性化(Rapid Elasticity)以及計量服務(Measured Service)。在雲端運算裏頭，使用者可以根據自己的需求來決定要從雲端供應商獲得多少運算能力以及資源而且不需要隨時與服務供應商互動。使用者可以透過各種設備連結網際網路。雲端供應商提供給使用者服務是採租用的方式，雲端供應商會將一個大型的資源用虛擬化的方式分割與管理給使用者使用，可以依據使用者需求進行動態分配。而且使用雲端運算所提供的服務是快速且有彈性的，對於使用者而言彷彿是在使用一個無限的運算環境。在使用雲端運算的過程，雲端服務會透過服務供應商的掌管以及監控，供應商會監控資源的使

用狀況，再根據狀況進行自動控制以及優化，讓使用者得到有效率的雲端服務。

關於雲端運算的四個部屬模型，所闡述的是雲端運算的應用對象及範圍。四個部屬模型包括公有雲(Public Cloud)、私有雲(Private Cloud)、社區雲(Community Cloud)、混和雲(Hybrid Cloud)。根據這四個部屬模型所提供的應用範圍，公有雲顧名思義就是一個公開且被共享的一個運算環境，大多提供給一般民眾或大型團體，在公有雲的環境裡適合存放機密性及影響性較低的資料。私有雲則為專門提供企業進行租用或建置的運算環境。私有雲的環境裡，僅僅提供企業內部服務專門使用，機密性較高。而社區雲則是屬於由多個組織或特定團體共同使用的資源環境。最後混合雲的部分，混和雲混合了兩個或兩個以上的雲端型態，舉例來說，在混和雲的環境裡共存了公有雲及私有雲。雖然兩個雲端環境共處於一個環境，但是必須要透過訂定標準或新技術來確保資料以及應用程式在兩個平台的移植性。

雲端運算的三個服務模式，也就是根據雲端供應商所提供的服務進行區隔，以下三種服務模式分別為軟體即服務(Software as a Service，SaaS)、平台即服務(Platform as a Service，PaaS)、基礎架構即服務(Infrastructure as a Service，IaaS)。SaaS 的服務為公司會將軟體置於雲端環境，讓用戶連結網路就可以使用軟體，用戶可以依據自己的需求，決定要付多少費用取得多少應用。SaaS 的代表例如 Google 應用程式、Dropbox、Salesforce…等等。PaaS 則是在公司在雲端環境上建置平台，用戶可以在平台上進行應用程式開發、軟體部屬等，使用整個平台環境，但是系統、硬體和網路基礎架構仍然由雲端供應商掌控。用戶者不能自行更改。屬於 PaaS 服務的有 Google App Engine、Windows Azure…等等。在 IaaS 的服務模式內，公司會整合如：IT 系統、資料庫、伺服器..等的基礎架構，再讓用戶根據自己所需的運算、儲存以及網路資源向公司租用。用戶可以掌控整個作業系統、硬體、和應用程式。但不能掌控雲端基礎架構。提供 IaaS 服務的公司有 IBM 的 TSAM (Tivoli Service Automation Manager)、Amazon Web Service 的 EC2。

2.2 電子書

電子書 (E-book)，就是透過電子載具，以電子文件的型式提供使用者閱讀，電子載具可以是一般電腦、筆電、平板電腦、電子書閱讀器、手機…等等。2004 年 SONY 在日本推出電子書閱讀器 Librie，但是因為藏書量不多，所以並未受到消費者對電子書的青睞。直到 2007 年，由 Amazon 亞馬遜網路書店推出了 Kindle 電子書閱讀器，由於購買平台直接由 Amazon 提供，能夠提供消費者多元的書籍選擇，而且當時網路技術已經穩定與成熟許多，因此開啟了電子書的激烈競爭市場[3][10]。

根據 2012 台灣數位出版聯盟所做的「2012 年台灣數位閱讀行為調查研究」，調查結果顯示「在閱讀載具的調查方面，受測者最常在平板電腦上閱讀電子書籍，其次是智慧型手機；而閱讀環境方面，消費者最常在 iOS 系統上面閱讀，第二是 Windows 系統，第三是 Android 系統。受測者每個月花在電子書籍上的金額，花費 1-100 元的用戶，有 26.4%；有 25.6%是免費取得電子書，；最後是 101-200 元，占了 22%[1]。」由此調查報告中可了解，行動裝置的發展有效的帶動了電子書市場，且由於電子書不像實體書能夠進行保存，而且製造過程省去花費大量印刷費用，故消費者會希望電子書價格能夠比實體書價格低。

2.3 國際標準電子書格式- EPUB

EPUB 是一種電子書標準規格，由國際數位出版論壇(IDPF, International Digital Publishing Forum)所提出，在 2011 年推出第三

版電子圖書標準 EPUB 3.0，為最終的版本。EPUB 使用 XHTML, CSS 來呈現內容。在 3.0 版本，可以加入影音，以及 Javascirpt。EPUB 支援「自動重新編排」功能，可以根據閱讀器的裝置特性，來決定最適合使用者閱讀的顯示方式。EPUB 是目前電子書常見的檔案格式(*.epub)，目前有許多大廠的閱讀器或軟體都接受 EPUB 檔案，例如：Apple 公司的 ibooks 軟體、Amazon 的 Kindle Fire、Barnes & Noble 的 NOOK…等[8][9]。

3. 行動雲端書櫃之應用服務

行動雲端書櫃的概念在於，利用雲端概念的特性，提供電子書的整合服務，並且提出分享電子書以及離線閱讀的方法，增加消費者在電子書使用上的便利性。並且由行動雲端書櫃擔任交易第三方，認證使用者及數位書城之間的金流交易，保障雙方的交易安全。在本章節將介紹行動雲端書櫃應用服務的角色內容、傳輸流程，應用服務架構圖如圖 3.1 所示。

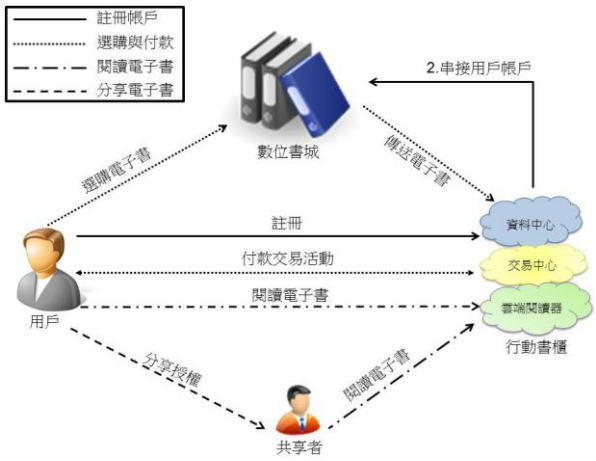

圖 3.1 行動雲端書櫃之應用服務架構圖

3.1 角色介紹

行動雲端書櫃應用服務內有五個主要角色，分別為：用戶、數位書城、行動書櫃、共享者。各角色詳細作用如下：

1. **用戶:**用戶是數位書櫃的消費者，也是行動書櫃的用戶，只需要在行動書櫃進行註冊，行動書櫃就會將用戶的註冊資訊傳送給數位書城，到數位書城選書時只需要登入行動書櫃的帳號密碼即可選購書籍。用戶如果要分享電子書給其他用戶(共享者)，必須向行動書櫃提出申請「分享帳號」的請求，獲得分享帳號後提供給共享者，讓共享者可以閱讀分享的電子書。一旦用戶分享某一本電子書給共享者，則該本電子書用戶在分享期間就無法閱讀電子書。
2. **數位書城:**販售電子書的數位書城，用戶在數位書城只進行選擇電子書並放入購物車，當用戶點選結帳時，數位書城會將購買資訊傳送給行動書櫃。當用戶付款成功後，行動書櫃會通知數位書城傳送電子書到行動書櫃，同時傳送一張同意傳送電子書的憑證給數位書城。數位書城收到訊息後會將用戶購買的電子書壓縮成封包形式連同憑證傳送給行動書櫃。
3. **行動書櫃:**行動書櫃是一個建置在雲端運算環境下的應用程式，數位書城的消費者可以利用行動書櫃來認證與數位書城之間的交易，用戶可以在行動書櫃內管理電子書以及閱讀電子書。它的主要功用分為三部分，第一部分為資料中心、第二部分為交易中心，第三部分為雲端閱讀器，將行動書櫃的功能分為三個單位的原因在於，考量到行動書櫃的負荷量，因此將用戶資訊和交易資料以及用戶的電子書分開儲存，可以防範當行動書櫃被入侵時，無法一次取得用戶的所有資料以及電子書檔案。行動書櫃的架構如圖 3.2 所示。

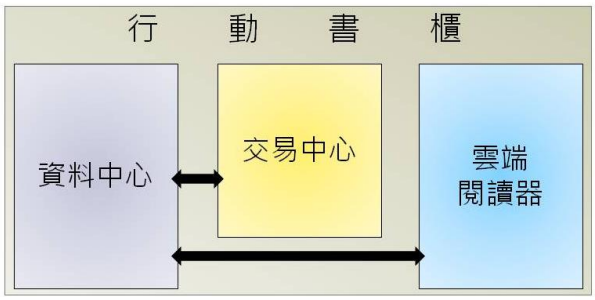

圖 3.2 行動書櫃架構圖

(A). **資料中心：**資料中心負責管理用戶的資料，資料中心會將用戶的註冊資料傳送給數位書城，讓用戶直接以行動書櫃的帳號密碼登入數位書城。無論是註冊用戶或者是用戶申請分享帳號，都由資料中心擔位負責此作業。資料中心會和交易中心和雲端閱讀器雙向傳輸資料。所有行動書櫃和數位書城的互動都由資料中心負責，數位書城無法和交易中心或者是雲端閱讀器直接連結。當數位書城要傳送電子書封包到行動書櫃時，會由資料中心檢查傳來的封包是否安全，且電子書格式是否屬於雲端閱讀器可閱讀的 EPUB 格式，如果傳來的電子書非 EPUB 格式，會在收到時就先進行格式轉換，轉換完成才會傳送到雲端閱讀器。

(B). **交易中心：**交易中心和資料中心是屬於雙向傳輸，交易中心不會和雲端閱讀器直接傳輸資料。交易中心內會儲存用戶的購買資訊，並且負責通知用戶付款並且確認用戶是否付款成功，所有的金流交易都交由交易中心負責。當用戶付款成功後，交易中心會傳送付款成功訊息給資料中心，再由資料中心通知數位書城可以傳送電子書。

(C). **雲端閱讀器：**雲端閱讀器除了提供用戶線上閱讀的功能外，還儲存了用戶所有購買的電子書，用戶可以自訂分類進行排序。當用戶要離線下載時，雲端閱讀器負責將電子書進行分割成數個小檔案，再下載到用戶的本機端。雲端閱讀器與資料中心的資料傳輸屬於雙向傳輸，它不會和交易中心有傳輸通道。

4. **共享者:**共享者是本研究裡獲得用戶分享電子書的角色，共享者要閱讀分享的電子書必須輸入用戶給予的分享帳號才可以閱讀。共享者可以在行動書櫃內搜尋想要看的電子書，再傳送請求給用戶，詢問是否可以分享某一本電子書，用戶同意後，進行申請分享帳號流程，並獲得分享帳號，再將分享帳號給共享者。

3.2 階段流程

本研究主要分為六個階段，第一階段：註冊帳戶，第二階段：選購電子書；第三階段：結帳付款，第四階段：傳送電子書，第五階段：分享電子書，第六階段：離線閱讀電子書。服務流程所使用的符號如表 3 所示，以下分別詳細介紹階段流程：

表 3 符號表

名稱	符號
用戶	U (User)
行動書櫃	BC_x (BookCase) ; x 可為 dc(資料中心); tc(交易中心); br(雲端閱讀器)
數位書城	EB(E-Book)
共享者	$SHARE_U$; “$SHARE_U$(ID,PW)”為共享者的帳號密碼
帳號	ID_X
密碼	PW_X
用戶個人資料	PI (Personal Information); 包含:電子信箱、手機號碼
購買清單的票證	$TICKET_{PList}$; Plist 為購買清單。未付款時付款狀態為”N”，已付款後付款狀態會為”Y”並加上付款時間戳。
購買金額	Price

國際標準書號	$ISBN^n$; n=數量
電子書	$BOOK^n$; n=數量
ISBN 第四碼到 ISBN 的倒數第二碼	NO4
電子書分割檔	Tmp_n; n=數量
一次性密碼	OTP (One Time Password)
付款收據條碼	NUM_{PP}
加密訊息	E( )
通訊金鑰	K_x
公開金鑰	PK_x
私密金鑰	SK_x
數位簽章	Sign
赫序函數	h
連結	||

3.2.1 註冊帳戶

用戶必須先在行動書櫃註冊用戶，才能在數位書城購買電子書，使用行動書櫃的功能。

步驟一：用戶必須在行動書櫃註冊帳戶，並且選擇要授權的數位書城有哪幾間。

用戶傳送註冊訊息到行動書櫃： $Register(ID_U, PW_U, PI, EB^n)$。

步驟二：行動書櫃收到註冊訊息之後會寄一封確認信到用戶的電子信箱，用戶必須登入電子信箱點選啟動網址，登入帳號以便啟動帳號。

用戶點選啟動網址後，進入行動書櫃進行登入： $Login(ID_U, PW_U)$。

步驟三：行動書櫃按照用戶同意授權的數位書城進行資料庫串接，如果用戶要新增可授權的數位書城，可在進入個人帳戶裡面進行設定。當用戶要到數位書城購書時，直接登入在行動書櫃註冊的帳號密碼

進行行動書櫃和數位書城的用戶資料庫串接： $BC(Database(USER(ID_U)))$ *LINK TO* $EB(Database(USER(ID_U)))$ 。

3.2.2 選購電子書

用戶到數位書城選購電子書，用戶可以選擇一次購買一本或多本，選完後點選加入購物車，確認購買即點選結帳。

步驟一：用戶到數位書城選購電子書，挑選要購買的電子書。

將欲購買的電子書加入購物車選項： $ShoppingCart(Choose(P_{List}(ISBN^n, Price, Date, ID_U)))$。

步驟二：用戶確認購物車內容正確後，點選結帳，系統會根據購物車的內容，自動產生票證形式的購買清單，票證內容包含：電子書的 ISBN、購買金額、購買日期、用戶帳號、付款狀態為"N"。

票證形式的購買清單： $TICKET_{PList}(ISBN^n, Price, Date, ID_U, Payment\ status(N))$。

步驟三：數位書城收到結帳通知，會傳送以數位簽章加密的結帳通知訊息給行動書櫃，結帳通知訊息內包含，數位書城和行動書櫃要共用的公開金鑰、用戶帳號、購買清單票證。

數位書城傳送結帳通知訊息給行動書櫃： $Sign(PK_{EB\text{-}BCdc}(h(ID_U)||(ID_U, TICKET_{PList}))$。

3.2.3：結帳付款

行動書櫃收到結帳通知後，通知用戶進行付款。

步驟一：行動書櫃收到數位書城傳送的結帳通

知，利用數位簽章檢查傳送過程中是否遭到竄改，確認訊息安全後，通知用戶付款，同時會傳送付款通知訊息到用戶手機。

行動書櫃通知用戶付款： $Notify(ID_U, P_{List})||h(ID_U))$。

步驟二；用戶確認交易是由用戶本身所產生，且清單以及金額無誤後，可以選擇線上信用卡付款、ATM 轉帳、超商付款方式進行付款。行動書櫃的交易中心單位收到款項後，會根據用戶的付款方式有不同的付款確認請求。如果用戶是使用信用卡付款、線上 ATM 轉帳進行付款，行動書櫃會傳送一組 OTP(One Time Password，一次性密碼)給用戶，用戶必須在收到 OTP 的十分鐘內，將收到的 OTP 傳回給行動書櫃。如果用戶是使用超商付款則必須傳送付款收據的條碼號碼給行動書櫃。

信用卡付款或線上 ATM 轉帳用戶的付款確認方式：

行動書櫃傳送 OTP 給用戶： $EK_{BCtc\text{-}U}(IDU, OTP)$。

用戶傳回 OTP 給行動書櫃： $Send(OTP)$。

超商付款付費確認方式：

用戶傳送付款收據的條碼號碼給行動書櫃： $Send(NUM_{PP})$。

步驟三:行動書櫃的交易中心單位會檢查 OTP 或是 NUM_{PP} 正確後，會傳送付款成功通知到用戶的電子信箱和手機，此時行動書櫃會對購買清單票證內容的付款狀態從"N"改為"Y"並且加上時間戳。

行動書櫃修改購買清單的票證內容： $TICKET_{PList}(ISBN^n, Price, Date, IDU, Payment\ status(YES, time))$。

3.2.4 傳送電子書

行動書櫃確認交易成功，便會傳送交易成功通知給數位書城。同時會傳送一張憑證給數位書城，數位書城必須在傳送電子書到行動書櫃時一併附上此張憑證。

步驟一：行動書櫃確認交易成功，在通知數位書城前，先產生一張傳送憑證。憑證內容包 ISBN_R、購買用戶、購買清單、購買金額，通知傳送電子書日期。ISBN_R 是一組亂碼，亂碼的組成是使用購買的電子書中的其中一本的 ISBN 和 ISBN 的第四碼到倒數第二碼相加所運算出來。運算方式以 ISBN: 9789862721247 為例：NO4 為 ISBN 的第四碼到倒數第二碼，也就是 986272724。再將此筆數列和 9789862421247 進行十進制相加，會獲得「9790848993371」，此筆數列也就是 ISBN_R。數位書城不會知道 ISBN_R 的組成來源，所以行動書櫃可以利用此筆數列與收到的電子書的 ISBN 進行比較確認是否相同。

行動書櫃產生 *ISBN_R*： $ISBN\_R=ISBN+NO4$。

行動書櫃產生傳送憑證： $CA(ISBN\_R, TICKET_{PList}, Price, ID_U, Date)$。

步驟二：行動書櫃通知數位書城傳送電子書，會傳送交易成功通知以及傳送憑證。

行動書櫃傳送通知及憑證給數位書城： $Notify(Received\ payment, TICKET_{PList}), Sign(PK_{BCdc\text{-}EB}(CA, ID_U||h(ID_U))$。

步驟三：數位書城收到通知，先檢查購買清單是否為用戶所訂的訂單相同，以及購買清單票證的付款狀態已改為"Y"。再根據清單內容選擇要傳送的電子書有哪些。最後將電子書檔案集合成封包，連同行動書櫃所傳來的憑證傳回行動書櫃。

數位書城傳送電子書給行動書櫃： $Sign(PK_{EB\text{-}BCdc}(CA||Packge(BOOk^n)||h(ID_U))))$。

步驟四：行動書櫃收到數位書城傳來的電子書封包後，會先檢查封包是否安全，再依照憑證上的 ISBN_R，解開原本的 ISBN 數列，將此 ISBN 與收到的封包內的電子書的 ISBN 進行比對，確認該本電子書是否存在，確認存在再依序檢查其他本電子書是否與購買清單內容相同。如果檢查 ISBN_R 不正確或是封包有問題，就會將取消接收檔案，通知數位書城重新傳送電子書。如果檢查正確就會解開封包，確認電子書格式是否為雲端閱讀器可閱讀的格 EPUB，如果電子書不是 EPUB 格式，行動書櫃會先轉為 EPUB 格式在傳送到行動書櫃的雲端閱讀器中。電子書儲存到雲端閱讀器後，用戶就可以利用雲端閱讀器閱讀電子書。

行動書櫃的資料中心傳送電子書到雲端閱讀器： $EK_{BCdc\text{-}BCrb}(ID_U, BOOK^n)$。

3.2.5 分享電子書

用戶可以將購買的電子書分享給其他用戶，但是再分享前必須先向行動書櫃提出申請。用戶如果分享電子書給共享者，則用戶本身在分享期間將無法閱讀被分享的電子書。

步驟一：用戶要分享電子書給其他用戶，先向行動書櫃提出申請。用戶必須提供以下資訊給行動書櫃，包括共享者的帳號、分享哪幾本電子書、分享期限。

用戶向行動書櫃提出申請： $EK_{U\text{-}BCdc}(ID_U, SHARE_U, BOOK^n, EXDATE||h(ID_U))$。

步驟二：行動書櫃收到申請後會根據申請資料產生分享帳號，再將分享帳號傳回給用戶。

行動書櫃傳送分享帳號給用戶： $Send(ID_U(ID_{SHARE}))$。

步驟三：用戶會將分享帳號給共享者，共享者在登入帳戶時，除了登入自己的帳號密碼，同時必須輸入分享帳號。

共享者登入行動書櫃同時輸入分享帳號： $Login(SHARE_U(ID,PW), ID_{SHARE})$。

步驟四：行動書櫃收到共享者已經將分享帳號登入的訊息，會檢查分享帳號裡頭，申請的共享者和登入分享帳號的共享者的帳號是否相同，檢查相同才會傳送要分享的電子書到共享者的雲端書櫃。

行動書櫃檢查分享帳號的登入身分是否正確： $Check(SHARE_U(ID) = ID_{SHARE}(SHARE_U(ID)))$。

行動書櫃傳送要分享的電子書到共享者的雲端閱讀器： $EK_{BCdc\text{-}BCrb}(SHARE_U(ID), IDSHARE, BOOK^n)$。

3.2.6 離線閱讀電子書

用戶可以選擇離線閱讀電子書，當用戶裝置沒有連上網路時，行動書櫃的雲端閱讀器可以當作一般的電子書閱讀器使用。

步驟一：要進行離線閱讀，必須先從行動書櫃下載電子書到本機。為了保護電子書的版權，防止被有心人是複製下載的電子書到別台裝置，所以會將電子書的檔案進行分割，分割成 10 到 20 個小檔案，分割數量是隨機決定的，且檔案命名會產生新的流水號，附檔名為.tmp，流水號和原本電子書書名以及分割順序無關。分割後的檔案只有雲端閱讀器知道如何重組。

用戶從行動書櫃下載電子書到本機： $Download(Tmp_1,...,Tmp_n)$。

步驟二：用戶在離線的狀態下要閱讀電子書，可以直接打開行動書櫃應用程式，利用雲端閱讀器進行閱讀，此時雲端閱讀器會直接讀取儲存在本機端的電子書，並且將檔案重組。

行動書櫃讀取本機端的電子書： $Read(Tmp_n+...+Tmp_n)$。

4. 分析與討論

根據本篇所提出的行動書櫃應用服務，進行了安全特性分析以及攻擊分析，分析結果如下：

4.1 安全特性分析

本研究所設計的服務流程可以滿足下列安全特性：

1. 身分認證機制：用戶需要在行動書櫃申請帳號，但是不需要在各個數位書城註冊帳號。本研究設計讓行動書櫃和各個數位書城進行帳號的串接，當用戶需要從數個數位書城購買電子書時，不需要每一次都註冊新的帳號，只需要授權數位書城能夠取得行動書櫃的用戶帳戶即可，增加用戶的便利性。行動書櫃因為分成三個單位各自成立一個資料庫儲存資料，只有資料中心的資料庫內的用戶帳號資料庫會和數位書城進行串接，所以不必擔心在資料庫串接的情況下會造成用戶資料外洩，串接資料庫概念圖如下圖 4.1。

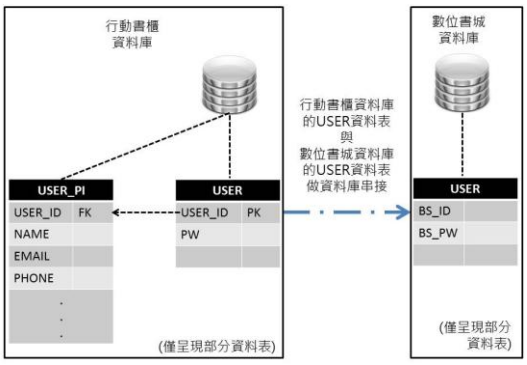

圖 4.1 串接資料庫概念圖

2. 不可否認性：行動書櫃通知用戶付款時，同時也會發送付款通知到用戶手機，可以讓用戶免於在不知情情況下被盜用付款，如果用戶發現，自己根本沒有購買書籍，可以馬上連絡行動書櫃，阻止交易行為。在用戶信用卡或 ATM 轉帳後，用戶必須輸入付款成功時畫面所提供的 OTP(One Time Password)，OTP 有時效限制，每一次付款後所產生的 OTP 都不同，用戶必須在十分鐘內輸入完畢，整個交易才算完成，才會確定扣款。而使用超商結帳的用戶則必須利用結帳收據上的條碼，提供條碼給行動書櫃的交易中心，交易中心可以利用此條碼查詢付款是否正確。為了確認是用戶本身要付費的款項且已完成付款，而交易中心也的確有收到款項，因此利用 OTP 和傳送收據條碼的方式，來保障整個交易過程的安全。利用數位簽章的特性來滿足不可否認性，保障行動書櫃和數位書城之間的結帳和傳送電子書過程中，雙方都有收到訊息。數位書城通知行動書櫃有一筆交易必須通知用戶結帳，行動書櫃不能否認已經接收到通知付款的訊息，以此避免行動書櫃和數位書城雙方有機會被有心人士利用通知重複付款的動作。再傳送電子書的步驟加入數位簽章，避免傳送電子書的過程中，出現重複發出請求的問題發生，行動書櫃和數位書城雙方在傳送訊息時利用數位簽章來確認雙方的不可否認性，降低某一方有抵賴的可能性發生。
3. 保密性：整個傳輸流程中，主要加密方式使用對稱式金鑰加密。利用通訊金鑰來保護數位書城、用戶、行動書櫃三方的傳輸安全。在傳送電子書的部分，為了確保數位書城傳送來的封包是安全的電子書檔案，所以在行動書櫃發送傳送電子書請求時一併發送了一組憑證，此組憑證是數位書城可以傳送檔案到行動書櫃的許可證，數位書城為了電子書的安全，會將電子書包裝成一個封包再連同憑證一併傳送給行動書櫃，除此之外行動書櫃會透過憑證上的資料檢查封包

內的檔案是否正確。而在分享電子書的部分，使用分享帳號來確保電子書不被任意分享給某一方，當共享者使用分享帳號登入時，行動書櫃會記錄共享者在行動書櫃的動作。為了提供用戶便利性，用戶可以選擇離線閱讀，離線閱讀必須下載電子書到本機端，可是因為有被竊取電子書檔案到別台機器的可能性，為了避免這樣的情況發生，會將電子書的檔案在下載前先分割成數個小檔案，且使用流水號命名，但是組成排序方式和檔案名稱無關，只有行動書櫃的閱讀器知道組成順序。利用分割的方式來達到電子書的保密性，不被有心人士任意轉傳。

4. 資料完整性：利用赫序函數的不可逆推性以及數位簽章加密的方式來檢查檔案或訊息在傳送過程中是否有遭受到攔截、竄改。因為是憑購買清單來取得電子書檔案，所以每一個傳送購買清單的過程都會加入赫序函數的運算來確認傳送過程沒有訊息沒有遭受到竄改，可以避免被有心人士更改購買清單而讓有心人士從中獲得電子書。在申請分享帳號的過程中使用赫序函數運算讓接收者可以檢驗過程是否遭到竄改，避免分享出被修改過的分享清單。

4.2 攻擊分析

本節假設可能會發生的攻擊問題，並且對其分析，分析結果如下：

1. 數位書城與行動書櫃串謀竊取電子書：每一次數位書城和行動書櫃要傳送電子書時，都必須有購書清單作為傳送證據，雖然數位書城和行動書櫃可以假造一個用戶去書城購書產生購買清單，可是當假用戶要進行付款時，因為沒有OTP 或者是付款收據條碼因而無法在購買票證上加入已付款的標記，因為購買票證沒有已付款標記，所以系統無法同意傳送電子書，因此可以避免數位書城與行動書櫃串謀的機會產生。
2. 行動書櫃遭到入侵：每一個系統都有可能被入侵的可能性，行動書櫃也是有被入侵的可能性。但是即使行動書櫃遭到入侵，入侵者無法一次就全部獲得使用者資訊，因為本研究所設計的行動書櫃，內部又細分為三個單位，當入侵者要全部入侵三個單位就必須耗費比較長的時間，在入侵者破解的這段時間內，資安人員可以進行防護機制的加強，以保護消費者資料以及電子書檔案。
3. 數位書城傳送有毒封包：數位書城不能夠自動傳送封包到行動書櫃，每一次的傳送都必須包含由行動書櫃所發行的憑證，行動書櫃必須收到憑證才會收數位書城的封包，每一次的憑證都是每一次交易才產生，一旦傳送電子書過程完成就會銷毀憑證。即使數位書城傳送封包來時是加上憑證所傳輸的，行動書櫃收到封包後還是會先直接剖析封包內容，掃描是否夾帶病毒，掃描完成確定無病毒才會解開封包，將電子書檔案傳送到雲端閱讀器進行儲存；如果掃描過程發現檔案有異狀或者是包含病毒會直接刪除檔案，並且通報數位書城傳送檔案有異狀，然後重新產生一張新的憑證傳送給數位書城要求重新傳輸。
4. 用戶下載電子書到本機再任意轉傳：用戶無法將下載到的電子書檔案轉傳到別台機器裡面，因為行動書櫃下載的電子書會經過分割成數個檔案，即使這些小檔案被轉移到別台機器裡，因為不知道重組順序，所以無法進行檔案復原，而重組順序每一次都會不相同，只有行動書櫃知道如何重組才可以獲得完整檔案，因此可以避免檔案被任意轉傳。

5. 用戶帳戶遭到盜用任意購買電子書：用戶如果被盜帳號進入數位書城任意購買書籍時，行動書櫃會用手機通知有筆購書交易要付款，此時用戶會發現帳戶被盜用，可以馬上通知行動書櫃取消交易，減少被扣款的問題發生。

5. 結論

透過本研究所設定的行動書櫃，可以達到整合電子書的功能，用戶不再需要擔心，每一次要到新的數位書城購買電子書時就要下載新的電子書閱讀器，而且可以直接在行動書櫃管理用戶所購買的每一本電子書，不必開啟每一個書城的閱讀器去尋找某一本書。而用戶和數位書城之間的金流交易，有行動書櫃擔任第三方交易認證單位，不必擔心某一方不承認已付款或者是已傳送電子書，行動書櫃也不會將用戶的付款資訊傳送給數位書城，所以不用擔心資料必須留給每一間數位書城而造成資料外洩。如果用戶有分享電子書的需求，可以透過向行動書櫃申請分享帳號，再將分享帳號給共享者即可完成分享動作，用戶不用在冒著風險將自己的帳號密碼給其他用戶，讓其他用戶登入自己的行動書櫃，造成個人損失。在離線閱讀的部分，提供下載功能，讓用戶不處於連線狀態也可以閱讀電子書，同時，考慮到電子書出版商及作者的權益，透過分割儲存檔案的做法保護檔案不被任意外流。行動書櫃是建立於雲端環境的一個行動應用，透過行動書櫃可以讓消費者在購買電子書以及閱讀電子書之間的活動更為便利，在第 4.2 節所提到的攻擊分析可以證明在傳送重要資訊的傳輸過程，加入安全技術以及交互比對認證的機制，保障了用戶、數位書城及行動書櫃三方的安全。

參考文獻

[1] 台灣數位閱讀行為調查研究問卷結果報告，台灣數位出版聯盟，2012/6/29。

[2] 陳瀅，「雲端策略：雲端運算與虛擬化技術」，天下文化，2010

[3] 葉錦清，”電子書營運模式(Business Model)分析”，工業技術研究院，2010/12/20。

[4] Asghar Afshar Jahanshahi, Alireza Mirzaie, and Amin Asadollahi, “Mobile Commerce Beyond Electronic Commerce: Issue and Challenges,” Asian Journal of Business and Management Sciences, vol. 1, no.2, pp. 119-129, 2011.

[5] Md. Tanzim Khorshed, A.B.M. Shawkat Ali, and Saleh A. Wasimi, “A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing,” Future Generation Computer Systems, vol. 28, no.6, pp. 833-851, 2012.

[6] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, and Matei Zaharia, “Above the Clouds: A Berkeley View of Cloud Computing,” Technical Report No. UCB/ EECS-2009-28, University of California at Berkley, USA, 2009.

[7] Peter Mell and Tim Grance, The NIST Definition of Cloud Computing, 2009

[8] IDPF- EPUB http://idpf.org/epub

[9] EPUB- 維基百科 http://zh.wikipedia.org/wiki/EPUB

[10] 電子書- 維基百科 http://zh.wikipedia.org/wiki/電子書