

結合雲端服務之實作數位產權隨選即用系統

陳金鈴
朝陽科技大學資工系
教授
clc@mail.cyut.edu.tw

張慶宏
朝陽科技大學資工系
學生
s9927081@cyut.edu.tw

余柏緯
朝陽科技大學資工系
學生
s9927083@cyut.edu.tw

鄭崇瑋
朝陽科技大學資工系
學生
s9927093@cyut.edu.tw

摘要

現今社會中，行動網路技術的發達使得資料取得方便，使用者常在未經授權下自行上傳與下載數位內容與他人分享，殊不知這已經觸犯到智慧財產權及創作權的法律保護。此外，駭客可在無線傳輸過程中竊取各機密資訊及盜取資料庫檔案，導致身分被冒用個人資料及重要資料被散佈等等。

為了保護數位內容，個人隱私及解決資料傳輸間的不安全性，本系統透過自然人憑證的身份認證來驗證身分與PKI的機制確保傳輸資料加密，並結合雲端服務達成節能減碳(減少硬體成本)隨時自助服務等便利性之優點。簡化以往繁複的步驟，使用者可在付費後享受在網路上即時使用數位內容的功能。

關鍵詞：雲端安全、PKI、數位產權管理、自然人憑證

Abstract

In the recent years, with the advancement of mobile technology, the data could be gotten easily. People often shared or downloaded digital content by himself via unauthentication, but it already has violated the laws of the wisdom property rights and copyright. In addition, the hackers can capture secret information in the wireless network. It will lead to the personal identity be camouflaged or the confidential information be spread.

In order to protect the digital content, the privacy and transmission safety in the wireless network should be protected, we authenticate security the identity via MONICA and transmit the data by asymmetric cryptography. It combined the cloud service to achieve the advantage of carbon reduction(reduce the hardware cost) and provide the instant service. By simplify the complicated steps, users can enjoy the digital content in real-time execution after paying the payment.

Keywords: Public-key infrastructure, digital right management, MOICA, cloud security

1. 前言

將雲端結合密碼學、自然人憑證、串流傳輸技術和線上隨選即用技術可以有效提升雲端的安全。此種技術整合除了提升雲端安全性之外還可以減少使用者的硬體成本，以及實現數位產權管理之概念。也可改變傳統人們下載、執行數位內容的繁雜步驟與費時的缺點。

傳統數位內容採用儲存於硬碟中之方式，再使用相關的驅動軟體開啟數位內容，此種方式會占用使用者的硬體空間與浪費傳輸時間。此外若使用者的電腦受到攻擊或是硬碟破損將導致資料遺失。因此，本研究將數位內容儲存於雲端中[1-5]。提供消費者與廠商儲存。

如何保護無線網路傳輸中的數位內容是目前資訊安全中的一大議題[6]，本研究藉由非對稱式加解密之技術保護數位內容之產權。藉由公鑰對傳輸過程中的數位內容加密[7-9]，待接收端收到加密之數位內容後再使用私鑰對其作解密。其次影片為數位內容中最需要大空間，相對傳輸的時間也會增長。

為了減少容量較大之數位內容的傳輸時間以及安裝驅動程式的時間，本研究結合串流傳輸，以及隨選即用之技術[10-13]，將影片分段傳送並在網頁中嵌入相對應之驅動軟體來提供使用者執行數位內容。使用者可以直接在網頁上觀看數位內容。

使用者帳戶遭到有心人士盜用，為電子商務的安全中一直被學者們關注的問題之一。為了解決此問題的產生，本研究採用政府提倡之自然人憑證技術[14-15]。自然人憑證提供身份不可偽造與交易的不可否認之特性[15]，藉由以上兩點特性，本研究結合自然人憑證，作為認證使用者之機制。使用者要登入時必須使用自己申請的自然人憑證，若無此卡是無法登入。所以我們認為此種登入方式能夠有效保護使用者權益且實際解決帳號盜用之問題的認證方式。

2. 相關技術研究

2.1 串流傳輸技術[10]

所謂串流(Streaming)是將聲音、電影以及多媒體，由串流伺服器提供使用者連續或即時傳送分段之影像內容，多媒體檔案在播放前並不需下載整個檔案，通常只需要將開始之影像內容存入記憶體，分段之資料隨時傳送再即時播放[11]。因此使用者不必等到整個檔案全部下載完畢後才能開啟使用，只需要花幾秒到數十秒的時間來下載啟動的部分，即可進行觀看。當多媒體檔案在使用者電腦上播放時，檔案的剩餘部分將從串流伺服器繼續下載[12]。串流內容被分成一連串可以被播放的最小媒介之區塊(Media segment)存放於串流伺服器中，使用者只須向串流伺服器提出影像傳輸之要求，串流伺服器透過非同步的方式，透過網路提供給數個使用者所需要的影像區塊。每個使用者的電腦都具有一個有限大小的資料緩衝區，以存放這些區塊的索引及內容，當使用者確實收到這些媒體區塊後，除了可在使用者電腦中播放之外，亦可將它們傳遞給其他使用者提出需求時產生的節點。這些節點上之資料緩衝區及網路頻寬，便可部份取代串流伺服器原本需付出的硬體資源，並省下了相當的相關成本[13]。

串流技術之優點[10-13]：

1. 即時播放：不需完全下載整個檔案才能使用，檔案一邊下載一邊播放，使用者可以即時的觀賞，但緩衝時間則是與使用的網路頻寬有關。
2. 影片資料不易被複製，可以有效的控制影片的散佈，進而保護影音檔案的智慧財產權。
3. 不占硬碟空間，影片僅暫存而沒有被下載儲存在硬碟裡，節省了設備的儲存空間。
4. 使用者可隨點隨看，檔案置於伺服器，所以使用者可隨時隨地透過網路連上伺服器方可觀看。

串流技術之缺點[10-13]：

1. 傳輸品質不穩，影像失真，須配合所使用的網路頻寬大小及網路壅塞狀況，傳送的資料必須經過壓縮，這樣會影響影片的順暢度及畫面品質。
2. 對網路頻寬要求度高。

2.2 RSA 加解密技術[7-8]

RSA 加密演算法是一種非對稱加密演算法。在公開密鑰加密和電子商業中 RSA 被廣泛使用。而對極大整數做因數分解的難度決定了 RSA 演算法的安全性。換言之，對一極大整數做因數分解其困難度高。到目前為止只有短的 RSA 鑰匙才可能被強力方式破解。只要其鑰匙的長度夠長，則使用 RSA 加密的信息實際上是不能被破解的。

本系統利用 RSA 加密技術之公私鑰的概念與不易被破解性，將儲存於雲端之數位內容的詳細位置透過公鑰加密後儲存於伺服器的資料庫中，以達到安全性。以 RSA 加密原理為例其中 m 為明文， e 為公鑰， n 為兩個大質數 p 和 q 的乘積， C 為密文如下式 1 所示。

$$m^e \equiv c \pmod{n} \quad (1)$$

待消費者要求執行數位內容時，本系統會自動至雲端空間中拿取相對應的私鑰，並向伺服器抓取儲存於資料庫中的數位內容之密文做解密，以 RSA 解密原理為例，其中 m 為明文， e 為公鑰， n 為兩個大質數的乘積， C 為密文，如下式 2 所示。

$$C^d \equiv m \pmod{n} \quad (2)$$

2.3 雲端運算[2-5]

雲端運算 (Cloud Computing)，是一種基於網際網路的運算方式，透過這種方式，共享的軟硬體資源和訊息可以按需求提供給電腦和其他裝置使用。雲端運算概觀如下圖 1 所示：

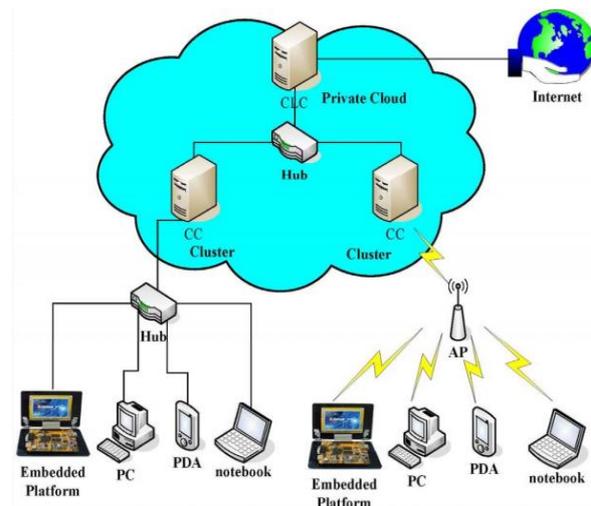


圖 1 雲端運算概觀[16]

雲端運算服務具備以下幾點特性：

1. 隨需自選服務。
2. 隨時隨地用任何網路裝置存取。
3. 多人共享資源。
4. 快速重新部署靈活性。
5. 可被監控與量測的服務。

一般認為雲端運算服務還有如下特徵：

1. 基於虛擬化技術快速部署資源或獲得服務。
2. 減少使用者終端的處理負擔。
3. 降低使用者對於資訊科技專業知識的依賴。

2.4 公開金鑰基礎建設[9]

公開金鑰基礎建設 (Public Key Infrastructure, PKI) 是一種用以強化網路安全的技術，讓使用者透過公眾網路與他人安全且經過驗證地交換資訊，就如同現實世界以簽名、密封文件的方式保全交換的訊息。

密碼學的加密與數位簽章的方式達成所要求的安全目標，PKI 整體而言透過網路所要提供給使用者的是：

1. 保密性 (Confidentiality)：確保僅有預期的接收者會收到訊息。
2. 資料完整性 (Data Integrity)：確保資料在接收前沒有被更改。
3. 驗證性 (Authentication)：確保參與資料交易者的身份無誤。
4. 不可否認性 (Non-repudiation)：交易資訊具有法律效力，參與交易者無法隨意否認。

2.5 自然人憑證[14]

「自然人憑證」是可以在網路上作資料交換時，如同網路身分證藉以辨識使用者之身分。隨著科技進步，我們採用了一種叫「憑證」的工具。「憑證」包含了「數位簽章」跟「公開金鑰」。這個公開金鑰是由憑證中心發行出來的一組金鑰對中的一半，另一半稱為「私密金鑰」，則儲存在 IC 晶片當中。經由憑證使用人和憑證管理中心約定，日後利用這憑證，使用者之身分就可以被辨認，啟用了加解密的功能，不管使用者在網路上傳什麼資料，資料都被加密，即使駭客攔截了資料也無法輕易的

解開。

自然人憑證不僅僅是憑證，它是由內政部憑證管理中心所簽發的。辦理了自然人憑證以後，未來使用者要申請網路部分之業務都不用再臨櫃辦理，只要在家上網就可以經由網際網路享受 E 化服務，提供了便捷的服務。

3. 系統架構與流程

3.1 系統架構

本研究的系統架構主要分為六大部分：

1. 雲端運算系統 (Clouding-Computing System)
2. 非對稱式加解密系統 (Asymmetric cryptography systems)
3. 會員管理系統 (Member Management System)
4. 自然人憑證管理系統 (MOICA Management System)
5. 數位內容上傳系統 (Digital Content Upload System)
6. 資料庫系統 (DataBase System)

本研究之系統架構圖如下圖 2 所示。後續我們將對所有子系統的流程與架構做詳細介紹及說明。

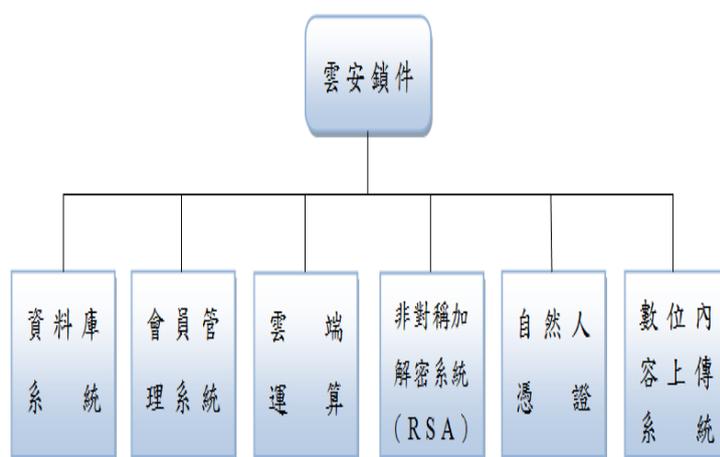


圖 2 雲安鎖件系統架構圖

3.2 系統流程

本研究主要的架構可分為網頁與數位內容上

傳系統，在網頁的部分主要提供使用者選擇數位內容。並透過相對應之執行軟體執行數位內容，主要的系統流程如下圖 3 所示為系統流程圖，主要包含以下幾步驟：

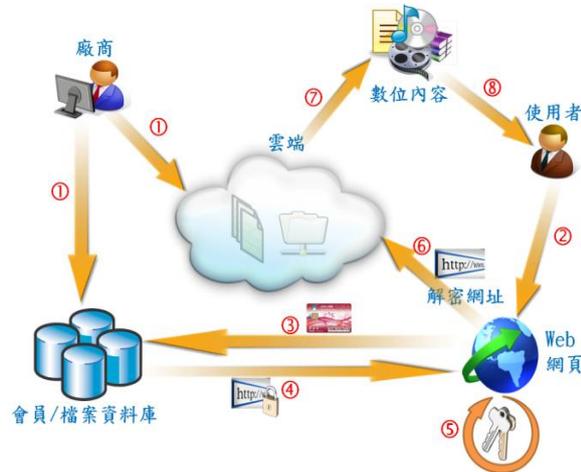


圖 3 系統流程圖

1. 廠商將數位內容存放至雲端並在資料庫建檔。
2. 使用者在網頁上登入自然人憑證卡，進行身分認證，並選取欲執行的數位內容。
3. 網頁將憑證認證的資料以及選取的數位內容名稱傳至資料庫。
4. 資料庫核對認證資料以及扣除該使用者所選取之數位內容的金額，並回傳密文。
5. Web 網頁將密文作解密，以取得數位內容位置。
6. 透過解密完成的連結至雲端抓取數位內容。
7. 雲端開啟選取之數位內容。
8. 傳送至使用者網頁執行。

3.3 雲端整合 RSA 非對稱式技術

本系統開發雲端服務之概念結合 RSA 非對稱式技術來保護傳輸中的數位產權內容，再結合自然人憑證當作身份認證的方式。藉由 RSA 的不易破解性與自然人憑證的不可偽造性與交易的不可否認性，能有效的保護數位產權與消費者權益也提高了雲端服務的安全性。如下圖 4 所示為雲端結合 RSA 加密之技術，主要包含以下幾部分：

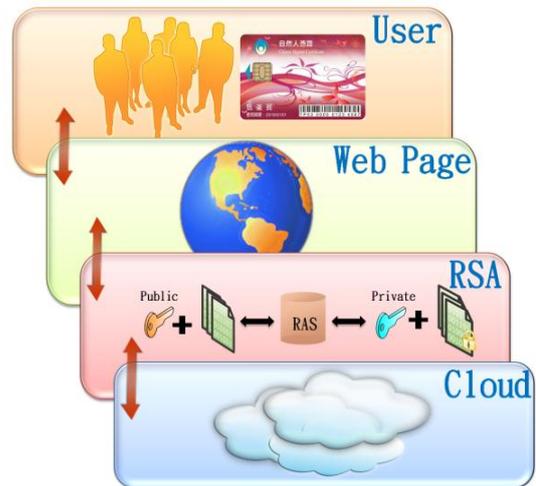


圖 4 雲端結合 RSA 加密之技術

1. 合法授權的使用者在網頁上欲透過雲端來存取資料，在封包傳輸的過程中使用了 RSA 加密的技術來保護數位內容，改善雲端傳輸的不安全性。
2. RSA 即是產生一組公私鑰對數位內容作保護，公鑰對其內容作加密，私鑰則是在確認使用者為合法授權者時才會進行解密的動作。
3. 雲端技術本為複雜的整合再加上 RSA 技術，使得各層之防禦環環相扣。

3.4 系統開發工具

1. 硬體

(1) 個人電腦：

處理器：Intel(R) Core(TM)2 Duo
CPU @2 GHz

記憶體(RAM)：2.00 GB

顯示卡：內建顯示卡

硬碟：80 GB

網路：2 M/128 K (下載/上傳)

(2) 讀卡機：中華電信多功能讀卡機 MS 100

2. 作業系統

(1) Microsoft Windows 7/8 (32/64 bits)。

3. 軟體

(1) Microsoft Visual Studio 2008

ASP.NET：撰寫主網頁各個分頁功能、會員登入系統。

- (2) Microsoft Visual Studio 2008：撰寫 API 程式、自動辨識消費系統。
- (3) Microsoft Windows Media Player：播放解密完成的影像。
- (4) Mysql 資料庫：管理會員的資料、消費。
- (5) 網際網路服務伺服器 (Internet Information Server)：架設自然人登入網頁。
- (6) Apache HTTP Server (簡稱 Apache)：架設伺服器網頁。
- (7) 威力導演 V7：製作串流影音。

3.5 數位內容上傳系統

本研究的數位內容上傳系統提供廠商與使用者上傳數位內容，並自動將數位內容以 RSA 加密保護，主要功能由 RSA 加密、數位內容上傳、數位內容詳細資料所組成如下圖 5 為實際的數位內容上傳系統。



圖 5 數位內容上傳系統實際畫面

使用者必須選擇檔案類型與種類，並選擇欲上傳之數位內容，如下圖 6 所示。

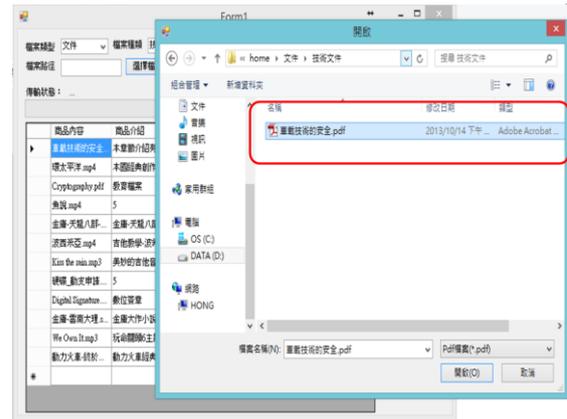


圖 6 上傳數位內容畫面

選擇了數位內容後，程式會自動提示使用者需要輸入產品的價格與介紹，如下圖 7 所示。



圖 7 提示輸入產品介紹與價格

輸入完價格與介紹，若上傳成功，程式會自動秀出成功的提示訊息視窗告知使用者數位內容已成功加密且上傳完畢，如下圖 8 所示。

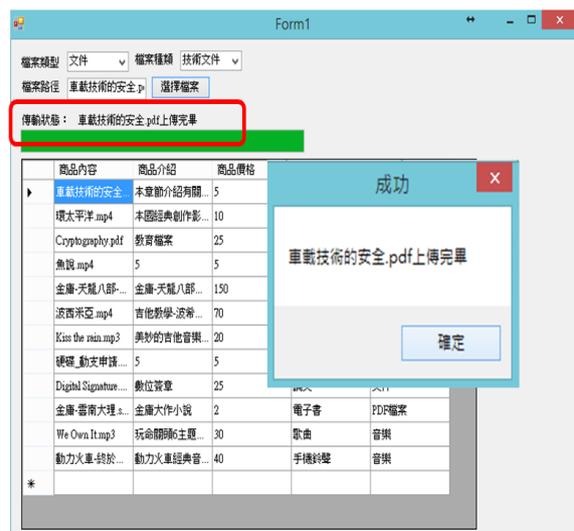


圖 8 數位內容上傳成功提示訊息

3.6 登入流程

系統登入流程分為兩種：(1)一般會員登入(2)自然人憑證登入，如下圖 9 所示：



圖 9 登入種類

1. 一般會員登入

如還未加入會員，系統將提供使用者註冊會員，如下圖 10 所示：

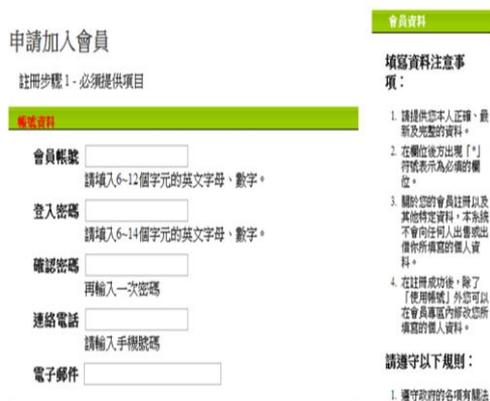


圖 10 會員註冊

登入成功後，網頁上方將會顯示使用者的名稱與下載清單的選項，如下圖 11 所示：



圖 11 一般會員登入成功頁面

2. 自然人憑證登入

點選自然人憑證登入口系統，並將自然人憑證插入讀卡機後，將會要求使用者輸入卡號的密碼，如下圖 12 所示：



圖 12 自然人憑證輸入卡號密碼

系統自動判斷身分登入成功後，系統會顯示自然人憑證的卡號以及使用者的相關資訊，如下圖 13 所示：

您的憑證序號為	7EBFCEA9BD0541F084730B059F9663AC
您的憑證主旨為	C=TW,O=測試機關1
憑證發行者為	C=TW,O=行政院.OU=(測試用) 政府測試憑證管理
您的Email為	test@cht.com.tw
您的卡別為	primary
您的憑證類別為	2.16.886.1.100.3.2.1.1
您的憑證持有人ID為	2.16.886.1.101.20001
您的憑證卡號為	TTA0000000002213

恭喜您成功登入!!!

[回首頁](#)

圖 13 憑證內容

使用者點擊回首頁後，本系統會自動顯示自然人憑證之卡號與下載清單的選項在網頁右上方，如下圖 14 所示：



圖 14 自然人憑證登入之畫面

3.7 資料庫管理

我們的資料庫系統提供完善的會員管理、自然人憑證管理、儲值卡紀錄、會員消費紀錄、數位內容管理與動態新聞等。

1. 會員管理：記錄各個會員的詳細資料提供廠商方便管理，如下圖 15 為實際會員資料記錄前半段，圖 16 為實際會員資料紀錄後半段。

m_ID 會員帳號	m_PW 會員密碼	m_level 會員等級	m_money 會員金額	m_name 會員真實姓名	m_sex 會員性別	m_birthday 會員生日
admin	admin	admin	4688			0000-00-00
user01	1234		0			0000-00-00
user02	1234		0			0000-00-00
user03	1234		0			0000-00-00
user04	1234		0			0000-00-00
w123473	q12345	member	0	王曉	女	2013-09-13

圖 15 會員資料記錄前半段

m_zipno 會員郵遞區號	m_city 會員居住縣市	m_canton 會員居住地區	m_address 會員住址	m_jointime 加入會員時間	Buy_Fg
				0000-00-00 00:00:00	4
				0000-00-00 00:00:00	0
				0000-00-00 00:00:00	1
				0000-00-00 00:00:00	2
				0000-00-00 00:00:00	3
822	高雄市	阿蓮區	33333333	2013-09-26 04:49:32	0

圖 16 會員資料紀錄後半段

2. 自然人憑證管理：紀錄消費者所使用的自然人憑證卡號與其相關的資訊，如儲值金額、卡號等等...。如下圖 17 所示。

Pki_CN	L_flog	pki_money
TTA0000000002213	1	4715
TTA0000000001694	1	0
TTA0000000002212	1	0

圖 17 自然人憑證之實際資料畫面

3. 儲值卡紀錄：紀錄各個儲值卡的儲值對象與時間
 自然人憑證管理：此部分為另一種會員的詳細料。如下圖 18 所示。

NO.	c_user	c_pass	c_money	c_mID	c_costime
1	BO61762N6K7613FZVWMB	MVOIVUYOUN	150	admin	2013-10-07 19:08:04
3	FFG16QQBRJY44OCN7S7W	FW1SFRBNRR	150	user2	2013-09-17 15:51:39
4	IF2613WIWMWONSJ5AMB4	6YGR2OEKIQ	150		0000-00-00 00:00:00

圖 18 實際的儲值卡資料紀錄

4. 會員消費紀錄：提供會員自行查詢消費的紀錄，以確保帳戶安全，如圖 19 為實際消費紀錄資料。

t_mld 消費者	t_file 消費的檔案	t_cost 消費額	t_time 消費時間
TTA000000002213	環太平洋.mp4	15	2013-10-15 02:12:32
TTA000000002213	Digital Signature.pdf	20	2013-10-15 02:12:14
TTA000000002213	車載技術的安全.pdf	10	2013-10-15 02:11:42
admin	Digital Signature.pdf	20	2013-10-15 02:04:16
admin	環太平洋.mp4	15	2013-10-15 02:03:43
admin	車載技術的安全.pdf	10	2013-10-15 02:03:14
admin	環太平洋.mp4	2	2013-10-15 01:49:21

圖 19 消費紀錄資料

5. 數位內容管理：此部分提供記錄各種數位內容的種類、金額、介紹及私鑰位置等等，如下圖 20 為消費者紀錄資料。

Name	File	Price	introduction	Kind	addr
車載技術的安全.pdf	XzeEAYnKLVAnzYsIUZaZPvVZQCP/CkCaRzGLVNEzpa4d...	5	本章節內容介紹有關於車載系統的安全問題	技術文件	文件
環太平洋.mp4	KQI3ZV2HiZp6BpHnAlWuH+QnK38Yl4qY(+zYoiCspJ7P%U)Y...	20	本國經典創作影片-環太平洋	圖片	電影
Cryptography.pdf	og8lhNsDTEiU74nqP2VizK2GsVAQzA0UhzbtYRvuujjOZG...	15	RSA加密解密介紹	書籍	PDF檔案
魚說.mp4	c3BRqJAGATODpVeRqM3FCk2X8aJIAOwuu7VZmniS2q7PwI6Vd...	5	5	歷史紀錄片	電影

圖 20 消費紀錄資料

6. 動態新聞管理：動態新聞資料主要提供網站自動且隨時更新即時的活動、產品消息等等...如下圖 21 所示。

id_no 新聞公告編號	news_type 新聞公告類型	news_title 新聞公告標題	news_content 新聞公告內容
1	網站資訊	第 18 屆資訊應用服務創新競賽報名	(一) 報名日期：102 年 10 月 8 日(二)~ 102 年 10 月 16 日(三)下午六點截止 (二) ...
2	網站資訊	第 18 屆資訊應用服務創新競賽報名(上傳資料)	上傳專題資料 1.系統概述文件-附件 1-1)或(附件 1-2)或(附件 1-3)或(附件 1-4)或(附...
3	系統公告	網站測試	本網站為新架設之網站 目前處於測試狀態中 有部分功能運轉或無法使用請多多包涵

圖 21 實際動態新聞資料儲存畫面

3.8 系統執行內容

成功登入會員後，點選網頁右上角之下載清單即會顯示歡迎訊息以及目前點數，如下圖 22 所示：

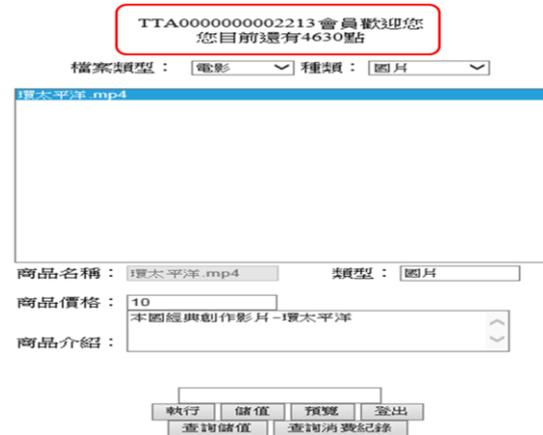


圖 22 下載清單畫面

本系統提供消費者預覽數位內容之功能，點選預覽後如下圖 23 所示：



圖 23 數位內容預覽畫面(以影片為例)

本系統採用計次性扣款的方式進行消費再利用嵌入驅動軟體技術讓使用者可在網頁上直接觀看數位內容，以達到節省空間、成本、時間的效果，執行結果如下圖 24 所示：

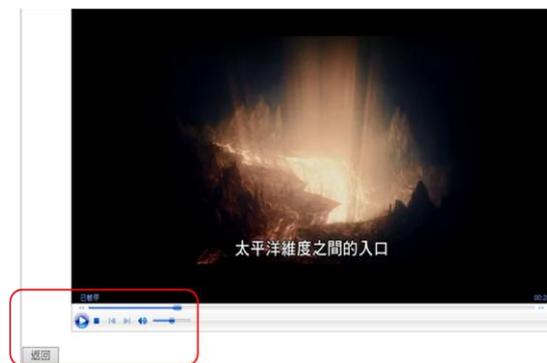


圖 24 網頁上執行數位內容的畫面(以影片為例)

4. 結論

本研究的系統能夠防範非法下載以及防止盜版與分享，並透過雲端服務節省成本及帶來更快捷的便利性。並在檔案傳輸時使用密碼學保護數位內容，已付費的使用者可在網路上登入會員系統，由系統判斷付費金額，藉此取得金鑰解密後即可在網頁上直接使用檔案。

而本研究開發的系統有以下幾點功能與優點：

1. 消費紀錄供：提供管理者、消費者可自行管理與查詢自己或消費者的消費紀錄。
2. 自動化的雲端運算服務：替使用者減少下載、安裝軟體所對應之驅動程式、身份認證、數位內容解密的時間。
3. 雲端空間：提供消費者與廠商租借，儲存數位內容並藉由本系統自動保護其內容。
4. 節省硬體資源：使用者可以省去的硬體資源。
5. 即時隨選服務：提供消費者使用數位內容時，可透過本系統在網頁上執行。

首先在未來研究的部分主要可分為三大部分，我們可針對計次性消費模式進行彈性調整，藉由記錄使用者購買日期並提供其數天內可無限使用。防止封包遺漏、執行斷線和網路異常等狀況。

第二我們將本次研究的開發核心移植至 Android 系統上，藉此支援移動設備以及車載網路環境。

第三為了有效的防範封包攔截的問題，我們將把數位內容使用串流傳輸技術來將數位內容分個數個區塊並對其中某幾個封包加密。當使用者取得後網頁將自動將封包解密並直接執行，並且將在傳送封包的 AP 上做保護的功能避免封包在傳送過程中遭到攔截。

5. 誌謝

本論文為國科會編號 NSC102-2815-C-324-003-E 之計畫，由於國科會的支持，使得本計畫得以順利進行，特此致上感謝之意。

6. 參考文獻

- [1] 許文峰，"風神：一個新的雲端儲存系統"，交通大學網路工程系碩士論文，2011。
- [2] 邱亭儒，"基於行動雲端的數位內容管理之

研究"，朝陽科技大學資訊管理系碩士論文，2013。

- [3] 蔡碧展，"基於 Hadoop 平台的雲端基因架構"，國立高雄第一科技大學資訊管理研究所論文，2010。
- [4] 陳旻裕，"雲端資料安全與存取控制之系統設計與實作"，中興大學資訊管理學系碩士論文，pp. 1-60，2013。
- [5] 翁雋傑，"混合雲之帳號與檔案內容權限管理與同步系統之實作-以 Google Docs 及 Hadoop 為例"，政治大學資訊管理研究所學位論文，2011。
- [6] J.-Z. Chang, "Implementation of adaptive streaming over HTTP on iOS platform," 國立台灣科技大學電機工程系碩士論文, 2013.
- [7] 吳崇濂，"運用雲端計算以輔助 RSA 加解密計算之研究"，東海大學資訊工程學系碩士論文，2012。
- [8] Rivest, Ronald L., Adi Shamir and Leonard M. Adleman, "Cryptographic communications system and method.", U.S. Patent, No. 4, 1983.
- [9] 任上鳴，"公開金鑰基礎建設之長期安全性"，成功大學電腦與通信工程研究所學位論文，2012。
- [10] 蘇奕宇、高靖鈞、劉炳傳，多媒體串流播放緩存之輸出控制技術，電腦與通訊，No. 149, pp. 81-86，2013。
- [11] 張裕榮，"串流媒體接續中段時間播放機制"，朝陽科技大學資訊工程系暨網路與通訊研究所論文，2006 年。
- [12] 蕭文娟，"數位視訊科技發展對傳播媒體展現之變革影響"，玄奘大學資訊傳播學院玄奘資訊傳播學報，No. 2, pp.81-101，2004。
- [13] 涂玉真，"多媒體即時串流傳輸協定研究與實作"，國立台北科技大學電機工程系研究所論文，2008。
- [14] 吳志崧，以自然人憑證實作一次性密碼之身份認證機制，義守大學資訊管理學所碩士論文，2012。
- [15] 蘇建興、王威傑，"運用政府機關數位憑證實現雙向驗證之研究"，臺北商業技術學院資訊管理系北商學報，第 20 期，pp.83-98，2011。
- [16] 張寶榮，"雲端應用之現況與未來"，國立高雄應用科技大學，p.25-27，2011。
http://cloud.cc.ncku.edu.tw/ezfiles/256/1256/attach/55/pta_15675_3077916_80036.pdf