國立暨南國際大學資訊管理學系

碩士論文

有限信任讀卡機下安全服務機制

Secure Service Mechanism for Semi-Trusted Card Readers

指導教授：俞旭昇 博士

研究生：楊佑寧

中 華 民 國 九 十 五 年 六 月

國立暨南國際大學碩士論文考試審定書

資訊管理　　學系（研究所）

研究生　　楊佑寧　　所提之論文

有限信任讀卡機下安全服務機制

Secure Service Mechanism for Semi-Trusted Card Readers.

經本委員會審查，符合碩士學位論文標準。

學位考試委員會

簡宏宇 _____ 委員兼召集人

_____ 委員

陳彥錚 _____ 委員

蔡孟峰 _____ 委員

俞旭昇 _____ 委員

中華民國　95　年　6　月　9　日

博碩士論文電子檔案上網授權書

（提供授權人裝訂於紙本論文書名頁之次頁用）

本授權書所授權之論文為授權人在 暨南國際大學 資訊管理學系 _____組 94 學年度第 二 學期取得 碩士 學位之論文。

論文題目： 有限信任讀卡機下安全服務機制
指導教授： 俞旭昇

茲同意將授權人擁有著作權之上列論文全文（含摘要），非專屬、無償授權國家圖書館及本人畢業學校圖書館，不限地域、時間與次數，以微縮、光碟或其他各種數位化方式將上列論文重製，並得將數位化之上列論文及論文電子檔以上載網路方式，提供讀者基於個人非營利性質之線上檢索、閱覽、下載或列印。

- 讀者基非營利性質之線上檢索、閱覽、下載或列印上列論文，應依著作權法相關規定辦理。

授權人： 楊佑寧
簽　名： 楊佑寧 楊佑寧　　中華民國 95 年 06 月 16 日

誌謝

感謝在我的研究所生涯中所有周遭曾經幫助我和支持我的朋友，由於你們的鼓勵與幫助，我才能順利的面對壓力與克服困難進而完成學業。也感謝我的家人，他們的支持讓我無後顧之憂，可全心全意地進行研究。

在兩年的學術生涯中，特別要感謝的是我的指導教授俞旭昇老師，由於您的殷殷教誨與指導，不僅使學生在專業技能上有長足地進步，在思考問題時也學習從不同的角度觀察與體會。另外我也要感謝與我同窗兩年的夥伴們：哲嘉、宗憲、玉雯、恭達、淑娟、嘉訓、欣緯，因為你們陪伴，不僅讓生活增色不少，也使枯燥單調的研究生活增添許多樂趣。也感謝學弟泰宏與智泉的鼎力相助。

在此論文完成之際，我要將本論文獻給我的親人，尤其是在天國的父親，因為你們的支持與鼓勵，才使我得以完成學業、取得學位。沒有你們默默的付出與全力的支持，我將沒有今天如此的成就，在此對於所有一起陪我走過這段歲月的家人、師長、朋友致上最深的謝意。

楊佑寧 謹誌

國立暨南國際大學科三 203 實驗室

中華民國九十五年六月

論文名稱：有限信任讀卡機下安全服務機制
校院系：國立暨南國際大學資訊管理研究所　　頁數：52
畢業時間：民國 95 年 6 月　　學位別：碩士
研究生：楊佑寧　　指導教授：俞旭昇

論文摘要

隨著智慧卡問世，各種應用智慧卡的遠端認證方法不斷地被提出與修改。智慧卡本身無顯示螢幕且無法自行供給電源，需仰賴讀卡機與終端設備的支援，若讀卡機與終端設備為不安全的，則持卡人的資訊安全將不復存在。

本論文在有限信任讀卡機的前提下，以智慧卡與遠端伺服器認證後的服務與資訊傳遞為研究主軸，提出安全的服務與訊息傳遞架構，以確保資訊能夠安全與正確的傳輸。本論文所提出的方法，在智慧卡抽離讀卡機後，即使讀卡機與終端設備被植入惡意程式，仍能有效保護資訊安全。我們以 JAVA 實作這個架構的原型，以驗證此法在現存硬體環境下的可行性，並提出適用的商業模式，以推廣此架構的應用範圍。

關鍵字：智慧卡、身份認證、資訊安全

Title of Thesis: Secure Service Mechanism for Semi-Trusted Card Readers.
Name of Institute: National Chi-Nan University, Pages: 52
Institute of Information Management
Graduation Time: 06/2006 Degree Conferred: Master
Student Name: Yo-Ning Yang Advisor Name: Shiuh-Sheng Yu

Abstract

After the smart card was presented to the public, various kinds of remote authentication schemes based smart cards are proposed and revised constantly. The smart card does not have a display monitor and is unable to supply its power by itself. It needs the support of a card reader or a terminal device. If we use an unsafe card reader or an insecure terminal device, the cardholder's information will be leak out and insecure.

Based on the hypothesis that card readers are semi-trusted, we studied issues about the service and information transmission after the authentication between a smart card and a remote server is completed. We proposed a secure service and information transmission scheme to ensure the information security and correct transmission. After taking out a smart card from a card reader, we can still resist the illegal programs effectively, even if a card reader or a terminal device is planted by a hostile program. We used JAVA to make a prototype and confirmed the feasibility in the existing hardware environment. We also proposed a suitable business model to promote this application.

Keywords: smart card, authentication, information security

目　錄

圖目錄

表目錄

第一章 緒論

身份認證是網路上互信的基礎，其意義在於防範不法行為，並允許合法使用者者可以存取適當的服務與資訊。由於智慧卡具有計算能力、方便攜帶、保密性佳、資料儲存量大與不易偽造等優點，結合智慧卡作為身份認證的方式將是未來的主流。

本章在以下小節中將依序敘述本篇論文之研究背景與動機、研究目的，最後則描述本論文之章節架構。

1.1 研究背景與動機

由於資訊科技的快速發展與網際網路的普及，各式應用於網路上的商業行為與服務應運而生，而頻繁的網路商業活動也使得使用者與遠端伺服器之間的溝通愈顯重要。早期以身份識別碼與通行碼所形成的溝通認證模式對於目前的網路環境已不符所需。

隨著智慧卡的誕生，許多應用智慧卡的服務也逐漸出現。近年來磁條金融卡與信用卡側錄盜刷事件頻傳，主要是磁卡的認證資訊易被盜取與複製，所以銀行工會已決議在 2006 年底將全面停用磁條金融卡並換發晶片金融卡。線上遊戲業者也開始提供使用智慧卡的認證登入以解決帳號盜用問題。IC 健保卡、結合 IC 卡的病歷交換[27]、預計 2006 年換發完成的國民身份證、捷運悠遊卡與連鎖商店的認同卡等皆為智慧卡相關應用。在學術上，各種應用智慧卡的遠端認證機制也不斷的被提出與改進，但認證後的服務與訊息傳遞則較少提及。

智慧卡本身無顯示螢幕也無法自行供給電源，需仰賴讀卡機與終端設備的配合。倘若終端設備被植入惡意的程式，在使用者認證通過且執行完各項服務並將智慧卡抽離讀卡機後，仍有可能被惡意程式保持與遠端伺服器的連線，進而竊取使用者的資訊或執行相關服務，造成使用者的資訊洩漏與損失。

1.2 研究目的

基於以上的研究動機，在有限信任讀卡機的前提下，本論文提出應用智慧卡與遠端伺服器進行雙向認證後的服務與訊息安全傳遞機制，只要將智慧卡抽離讀卡機，終端設備的惡意程式即無法對遠端伺服器進行溝通與執行服務。讀卡機設定為非專屬設備，可與多個不同的遠端伺服器進行服務存取，而這些遠端伺服器並無相同的後端平台。

1.3 論文架構

本論文共分為六個章節，第一章說明本研究的背景與動機與研究目的，第二章探討相關的文獻，包括智慧卡硬體架構、ISO7816 規範、單向雜湊函數、加解密機制，以及遠端認證的攻擊方式。第三章說明與本論文相關的遠端認證機制。第四章則描述我們的遠端認證機制與認證後的訊息與服務傳遞方法。第五章則是系統環境、系統架構、系統展示與適用的商業模式。第六章則為結論與未來發展，說明本系統的實作成果及未來可供改進及發展的地方。

第二章 文獻探討

2.1 智慧卡

智慧卡（Smart Card）為一外型大小(85.6L*54W*0.76H mm，圖 2.1.3)等同於信用卡（Credit Card）的塑膠卡片，符合 ID-1 信用卡規格，並在卡片中嵌入晶片(25L*15W mm，圖 2.1.3)。舉凡捷運悠遊卡、健保卡、各大銀行的晶片提款卡、網路 ATM、手機 SIM(Subscriber Identity Module)卡，以及預計將在今年全部換發完成的國民身份證皆為智慧卡的應用。

2.1.1 智慧卡之架構

智慧卡晶片通常是單一晶片(Single Chip)而其內部架構(如圖 2.1.1)包含微處理器（Microprocessor）、作業系統（Operating System）與記憶體（Memory）。有些智慧卡甚至包含輔助處理器（Coprocessor）來進行更複雜之計算。一般智慧卡記憶體容量的大小有 8KB、16KB 與 32KB，並遵從國際標準組織 ISO(International Standard Organization)於 1998 年所制訂的 ISO-7816 標準，此標準將分述於 2.1.2-2.1.4 節：

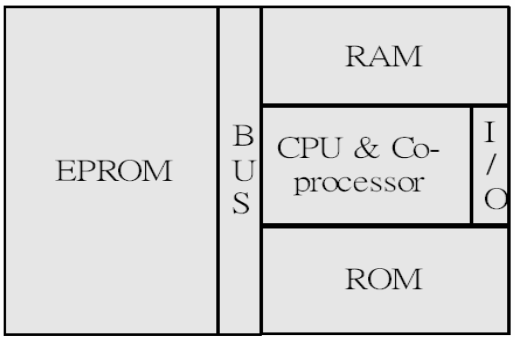

圖 2.1.1 智慧卡晶片架構圖

資料來源：智慧卡標準與實務應用研討會[26]

2.1.2 ISO-7816 Part 1

Part 1 主要規定接觸式(Contact Card)卡片實體規格與耐受需求，如防電磁波干擾、防靜電、抗紫外線或 X 光等輻射，並能承受外力所造成的彎曲、拗曲，使金屬接點與內部晶片不會脫落或翻起。

2.1.3 ISO-7816 Part 2

Part 2 規範晶片的金屬接點之接腳用途、位置和尺寸。如圖 2.1.3 與表 2.1.3 所示：

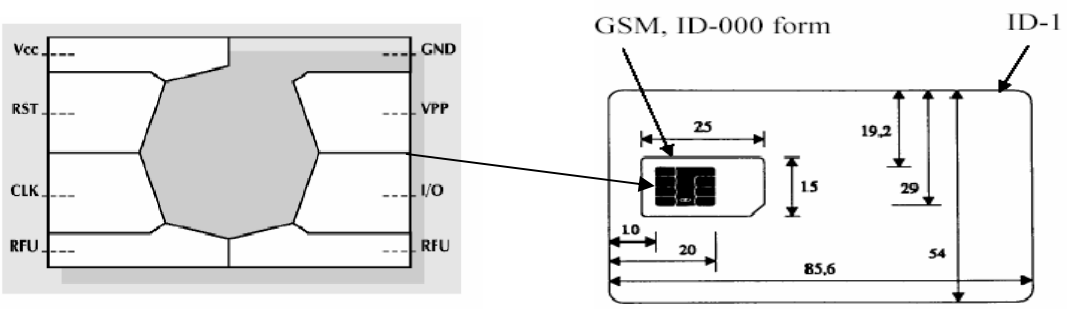

圖 2.1.3 智慧卡晶片接點腳位與智慧卡大小圖

資料來源：智慧卡標準與實務應用研討會[26]

端子名稱	端子功能
Vcc (Supply Voltage)	提供智慧卡所需電源，以 5V 為主。
RST(Reset Signal)	重設信號
CLK(Clock Signal)	脈衝信號
RFU(Reserved for Future Use)	保留未來使用

GND(Ground)	0 電壓
VPP(Programming Voltage)	燒錄電壓
I/O(Data Input / Output)	資料輸出入
RFU(Reserved for Future Use)	保留未來使用

表 2.1.3 智慧卡晶片各端子功能

資料來源：智慧卡標準與實務應用研討會[26]

2.1.4 ISO-7816 Part 3

Part 3 規範晶片電子訊號的處理與通訊傳輸協定，如 APDU(Application Protocol Data Unit)。常用的為 T = 0 字元傳輸協定，詳述如下：

依 ISO7816-4 可將 APDU(如圖 2.1.4.1、2.1.4.2 所示之)區分為 Command APDU 與 Response APDU，各項參數的功能如表 2.1.4 所示：

CLA	INS	P1	P2	Lc field	data field	Le field

圖 2.1.4.1 Command APDU

資料來源：智慧卡標準與實務應用研討會[26]

data field	SW 1	SW 2

圖 2.1.4.2 Response APDU

資料來源：智慧卡標準與實務應用研討會[26]

參數名稱	參數功能
CLA：Instruction Class	命令分類
INS：Instruction Code	命令代碼
P1 & P2：Parameter	自訂參數，不使用為 0
Lc field	指定 Data field 傳送長度
Le field	指定回傳資料長度
Data field	欲傳送至智慧卡的資料
SW1 & SW2：Status Word	執行後狀態回傳碼

表 2.1.4　APDU 參數功能對照表

2.2 單向雜湊函數(One-Way Hash Function)

對任何長度的明文 m，經由單向雜湊函數 h( )可產生固定長度的雜湊函數值 h(m)。雜湊函數可用於明文鑑定(Authentication)或數位簽章(Digital Signature)。雜湊函數值可以說是對明文的一種數位指紋(Digital Fingerprint)或是訊息摘要(Message Digest)。單向雜湊函數具有以下特性：

(1)雜湊函數必需對任意長度的明文，產生固定長度的雜湊函數值。

(2)對任意的明文 m， h(m)可借由軟體或硬體輕易的得到。

(3)對任意的 h(m)，要反推出 m，在計算上是不可行的。

(4)對一個明文 m1，要找到另一個不同的明文 m2，使得 h(m1)=h(m2)，在計算上是不可行的。

條件(1)、(2)及(3)是所謂的單向(One-Way)特性。條件(4)是無碰撞(Collision-Free)性或碰撞阻抗(Collision-Resistant)。常見的雜湊函數有日本電話電報公司(Nippon Telephone and Telegraph(NTT))的 N-Hash(Miyaguchi, Ohta, & Iwata, 1990)、1991 年由 Ronald Rivest 所設計開發的 MD5 (Message Digest Algorithm 5)，MD5 產生 128 位元的訊息摘要值。由國家科技標準局(National Institute of Standards and Technology)與國家安全局(National Security Agency)共同開發的 SHA-1 (Secure Hash Algorithm 1)，則可產生 160 位元的訊息摘要值。

2.3 加解密機制

在資料傳輸過程中，可透過加解密的技術，來防止第三者竊取其資料內容。簡而言之，就是將明文(Plaintext)加密成密文(Ciphertext)再來傳送，接收者再將密文解開為明文即可閱讀，其流程如圖 2.3。常見的加解密系統有對稱式密碼系統(Symmetric Cryptosystem)與非對稱式密碼系統(Asymmetric Cryptosystem)。

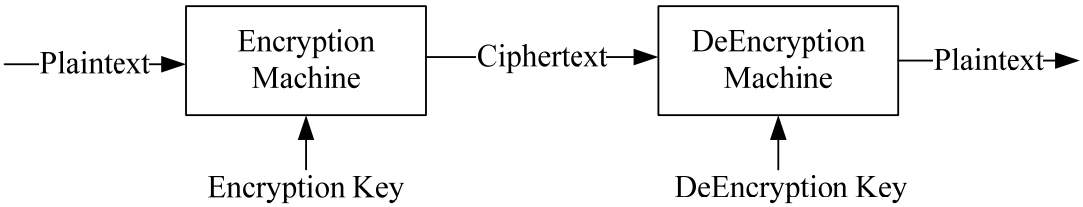

圖 2.3 密碼系統示意圖

2.3.1 對稱式加解密系統(Symmetric Cryptosystem)

對稱式密碼系統，其加解密共用相同的私密金鑰(Private Key)。其最大的特點在於加密速度快，常應用於需要即時或快速加解密的場合。常見的對稱式密碼系統有 DES(Data Encryption Standard)，DES 為區塊加密法，使用 64 位元的金鑰來加密大小為 64 位元的區塊。為了加強安全性而有 Triple DES 出現，Triple DES 採用 192 位元的金鑰來進行區塊加密。新一代的對稱式加密標準 AES(Advanced Encryption Standard)則支援到 256 位元的金鑰。

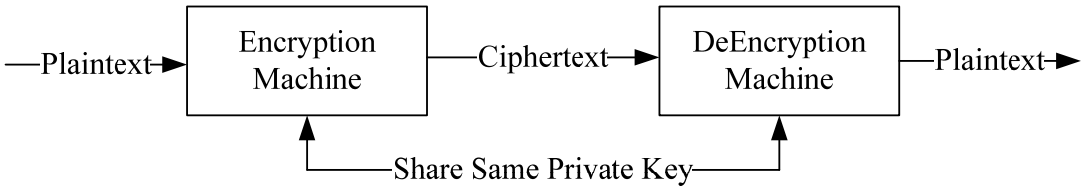

圖 2.3.1 對稱型加解密系統示意圖

2.3.2 非對稱式加解密系統(Asymmetric Cryptosystem)

非對稱式加解密系統，其加解密則是使用不同的金鑰，一把為加密用的的公開金鑰(Public Key)，一把為解密用的私密金鑰(Private Key)。非對稱式加解密優點為安全

性高但相對地速度較慢，適合較短訊息的加解密。常見的有 1978 年由 Rivest、Shamir 與 Adleman 三人提出的 RSA 與 ElGamal。

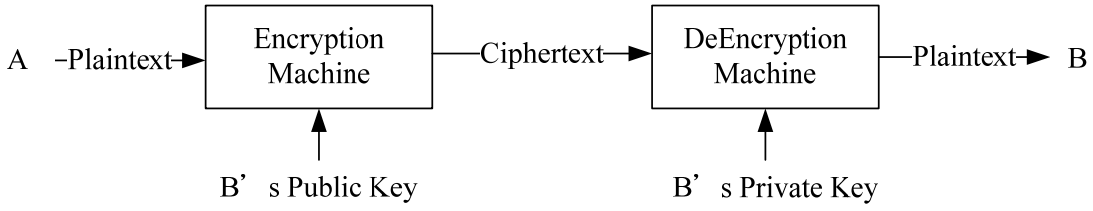

圖 2.3.2 非對稱型加解密系統示意圖

2.4 身份認證攻擊方法

2.4.1 重送攻擊(Replay Attack)

重送攻擊指攻擊者竊取通訊雙方於公開網路傳送的合法訊息，如身份識別碼(ID)與通行碼(Password)，於時間內偽裝成合法使用者將竊取到的訊息重送至系統。為了防止重送攻擊，一般使用時間戳記（Time Stamp）的方式來檢查所傳送訊息的時間是否在一個合理範圍內，以確保訊息不被重送。但在實際網路環境中，由於距離與機器規格的不同，系統的時脈頻率同步有相當程度的困難。另一種解決方法為在溝通過程中採用亂數(Nonce)來防範重送攻擊。

2.4.2 假冒攻擊(Impersonation Attack)

在遠端使用者認證系統中，攻擊者可以利用竊聽、攔截得到前一次通訊雙方之間的傳遞訊息，進而計算偽造出另一個可通過系統驗證的合法登入訊息，達到存取使用者系統中的資料。

2.4.3 中間人攻擊(Man-In-The-Middle Attack)

中間人攻擊是在傳送兩方之間中途截攔資料，並模擬傳送兩方的角色，做資料篡改及模擬兩方公鑰及密鑰，讓傳送兩方溝通時，不知道有第三者在中間側錄及修改彼此傳送的資料。

2.4.4 驗證表被竊取後攻擊(Stolen-Verifier Attack)

此種攻擊方式是從伺服器端竊取驗證表格(Verification Table)中使用者的秘密資訊，如身分識別碼與通行碼。若伺服器端不需儲存驗證表格，則可避免此種攻擊方法。

2.4.5 偽裝伺服器攻擊(Server Spoofing Attack)

此種攻擊方式是偽裝遠端伺服器，而使用者卻不知道此伺服器偽造的，而傳送相關的秘密資料給偽裝的伺服器，以致重要的資料被竊取。

2.4.6 字典攻擊(Dictionary Attack)

由於大多數使用者習慣使用有意義的單詞或數字作為密碼，如生日、電話、身份證字號…等資訊，此類密碼又稱之為懶人密碼。此類攻擊方法的主要技術即利用使用者相關資訊來猜測使用者的密碼。

第三章 相關研究

3.1 通行碼驗證機制

早期的通行碼(Password)認證機制，常利用驗證表格(Verification Table)來儲存個人的身份識別碼(Identity, ID)，系統將使用者輸入的身份識別碼與通行碼與驗證表格內所儲存的進行比對，如圖 3.1 所示，比對成功則表示此使用者為合法登入者，比對失敗則拒絕其登入。此種方法的缺點有二，一是使用者的身份識別碼與通行碼是以明文在公開網路上傳輸，可被輕易竊取，二是驗證表格若以明文方式儲存，易遭受侵入與竄改。此法即使在傳輸過程中將密碼加密仍可能遭受重送攻擊(Replay Attack)。

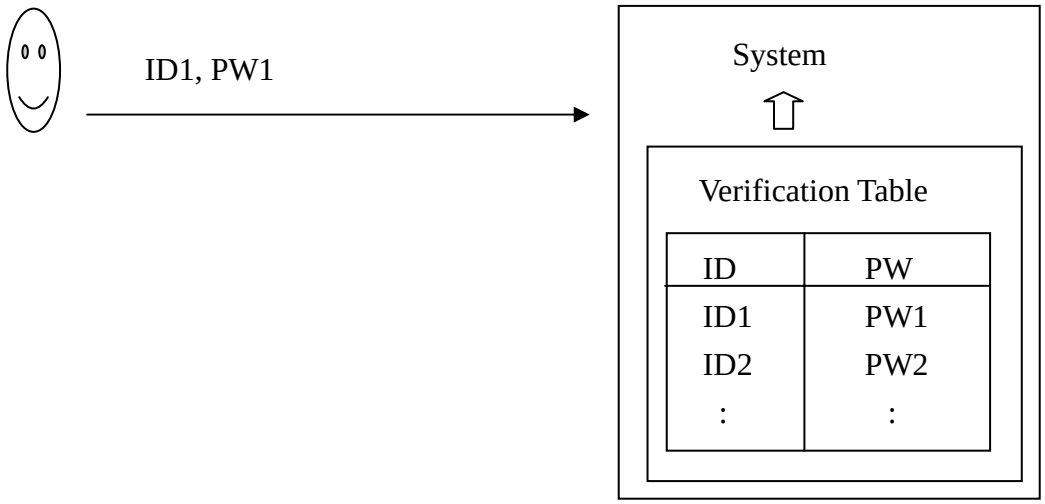

圖 3.1 通行碼驗證圖

3.2 使用智慧卡的通行碼遠端認證機制

Lamport (1981) [1]首先提出密碼認證機制來解決重送攻擊的問題，但仍須儲存驗證表格以致伺服器中的驗證表格存有被攻擊的危險[2][3][4][5][6][7]，所以至今不斷有學者提出新的方法來改進遠端認證機制的安全性與效能[8] [9] [10] [11] [12] [16] [17] [18][19] [20][21]。Chien et al.(2002)[8]提出了使用智慧卡進行遠端雙向認證機制，可讓使用者與系統相互認證，並有以下優點：1.可自由選擇通行碼 2.系統不需儲存驗證表格 3.低的溝通與計算成本。

Juang(2004)[10]提出了以亂數為基礎的遠端相互認證機制，並保留了 Chien et al.(2002)機制的所有優點，此外更可產生出新的溝通金鑰(Session Key)與無時間同步問題(Time-Synchronization problem)以利後續的訊息溝通。

Shieh 與 Wang(2006)[11]和 Lee et al.(2005)[12]則分別提出了以時間戳記(Time Stamp)與單向雜湊函數(One-Way Hash Function)和以亂數(Nonce)與雜湊函數為基礎的遠端認證機制。

由於 MD5 與 SHA-1 分別於 2004 年 9 月與 2005 年 3 月被中國山東大學的王小雲教授先後找出破解方法，MD5 被證實碰撞[13]，即兩組不同的演算結果指向同一組原始值。因此，MD5 變的不安全，使用 P4-1.6G 的電腦瞬間破解 MD4，MD5 完全破解只需 45 分鐘[14]，SHA-1 的碰撞也已被證實[15]。所以完全以單向雜湊函數為基礎的遠端認證機制已不是那麼的安全。所以本文提出的方法主要結合 Juang 與 Lee et al. 的遠端認證機制，並作部分修改。以下分別敘述 Juang 與 Lee et al.的方法：

3.3 Juang 的方法

Juang 提出的遠端認證機制分成二個階段，註冊階段(Registration phase)與登入和溝通金鑰協議階段(Login and session key agreement phase)，茲先說明本論文使用符號如下表：

符號	表達意義
U_i	使用者 i
S	欲登入的遠端伺服器
R	讀卡機
C	智慧卡
ID_i	使用者 i 的唯一身份識別碼
PW_i	使用者 i 的通行碼
X	伺服器 S 所保存的秘密金鑰(Secret Key)
h( )	單向雜湊函數(One-way hashing function)
X→Y：Z	送方 X 送出訊息 Z 至收方 Y
Eg(m)	明文 m 使用金鑰 g 進行對稱式加密
Dq(c)	明文 c 使用金鑰 q 進行對稱式解密
⊕	互斥或運算
||	連結符號
N_1, N_2	亂數(Nonce Number)值
ru_j, rs_j	亂數值，用以計算 Session Key
sk_j	溝通金鑰 Session Key
CMD	使用者欲登入伺服器執行的服務
Res	命令結果傳回值
j	表第 j 次登入

表 3.3 使用符號意義對照表

註冊階段(Registration phase)：

使用者 U_i 於安全環境中傳送他的身份識別碼 ID_i 與通行碼 PW_i 來向系統進行註冊，系統則進行下列步驟：

1. 計算使用者 U_i 的秘密資訊：

   $V_i = h(ID_i, X)$

   $W_i = V_i \oplus PW_i$

2. 儲存 ID_i 與 W_i 至使用者的智慧卡中並將智慧卡給予使用者 U_i。

登入和溝通金鑰協調階段(Login and session key agreement phase)：

使用者拿到智慧卡後，可將智慧卡插入讀卡機然後輸入使用者 U_i 的 ID_i 與 PW_i，若 ID_i 與 PW_i 輸入正確則進行以下步驟：

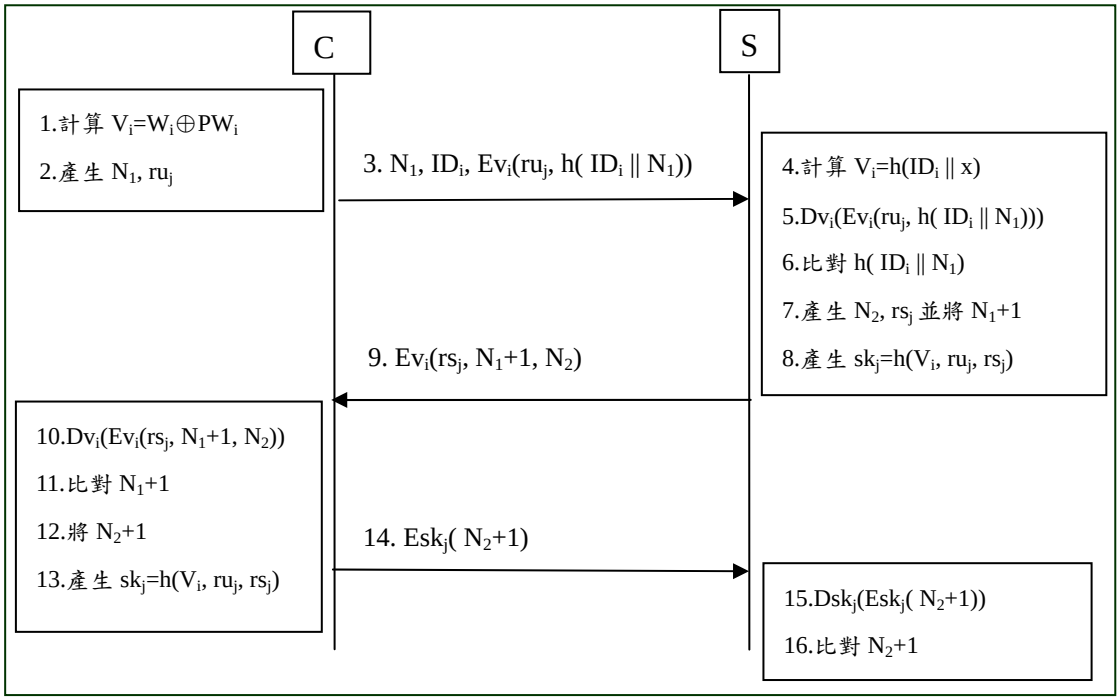

圖 3.3 Juang 的遠端認證圖示

步驟說明：

1. 智慧卡利用使用者輸入的 PW_i 與存於卡片內部的 W_i 進行計算 V_i：

   $V_i = W_i \oplus PW_i$

2. 智慧卡內部以亂數產生器產生亂數 N_1 與 ru_j。

3. 卡片端傳送 N_1、ID_i 與用 V_i 進行對稱式加密過的 ru_j 與 $h(ID_i \| N_1)$至伺服器：

   $C \rightarrow S$：$N_1, ID_i, Ev_i(ru_j, h(ID_i \| N_1))$

4. 伺服器利用步驟 3 所傳入的 ID_i 與儲存於伺服器的 X 計算 V_i：

   $V_i = h(ID_i \| X)$

5. 伺服器使用 V_i 對 $Ev_i(ru_j, h(ID_i \| N_1))$進行對稱式解密：

   $Dv_i(Ev_i(ru_j, h(ID_i \| N_1)))$

6. 伺服器利用單向雜湊函數計算步驟 3 所明文傳入的 ID_i 與 N_1 並比對解碼過的 $h(ID_i \| N_1)$是否相同。

7. 比對無誤則亂數產生 N_2、rs_j 並將 N_1+1。

8. 伺服器利用 V_i、ru_j 和 rs_j 產生 Session Key：

   $sk_j = h(V_i, ru_j, rs_j)$

9. 伺服器傳送用 V_i 進行對稱式加密過的 rs_j、N_1+1 與 N_2 至卡片：

   $S \rightarrow C$：$Ev_i(rs_j, N_1+1, N_2)$

10. 卡端對步驟 9 所收到的訊息 $Ev_i(rs_j, N_1+1, N_2)$ 使用 V_i 進行對稱式解密：

    $Dv_i(Ev_i(rs_j, N_1+1, N_2))$

11. 卡端比對 N_1+1 是否相同。

12. 比對無誤則將 N_2+1。

13. 卡片利用 V_i、ru_j 和 rs_j 產生 Session Key：

    $sk_j = h(V_i, ru_j, rs_j)$

14. 卡端利用 sk_j 加密傳送 N_2+1 至伺服器：

    $C \rightarrow S$：$Esk_j(N_2+1)$

15. 伺服器使用 sk_j 解碼步驟 14 所收到的 $Esk_j(N_2+1)$：

$Dsk_j(Esk_j(N_2+1))$

16. 伺服器比對 N_2+1。

Juang 的遠端認證機制優點如下：

1. 伺服器不需儲存驗證表格。
2. 使用者可自由選擇自己的通行碼。
3. 低的溝通與計算成本。
4. 使用者與伺服器可相互認證。
5. 可由使用者與伺服器協議產生新的溝通金鑰(Session Key)。
6. 使用亂數為基礎，無時間同步問題。
7. 可防禦重送攻擊。

缺點為若 V_i 被破解則亂數值不受保護導致整個機制瓦解。

3.4 Lee et al.的方法

Lee et al.的方法分成三階段，註冊階段(Registration phase)、登入階段(Login phase)與驗證階段(Verification phase)：

註冊階段(Registration phase)：

使用者 U_i 於安全環境中傳送他的身份識別碼 ID_i 與通行碼 PW_i 來向系統進行註冊，系統則進行下列步驟：

1. 計算使用者 U_i 的秘密資訊：

   $R_i = h (ID_i \oplus X) \oplus PW_i$

2. 儲存 R_i 至使用者的智慧卡中並將智慧卡給予使用者 U_i。

登入與驗證階段(Login phase＆Verification phase)：

使用者拿到智慧卡後，將智慧卡插入讀卡機然後輸入使用者 U_i 的 ID_i 與 PW_i，若 ID_i 與 PW_i 輸入正確則進行以下步驟：

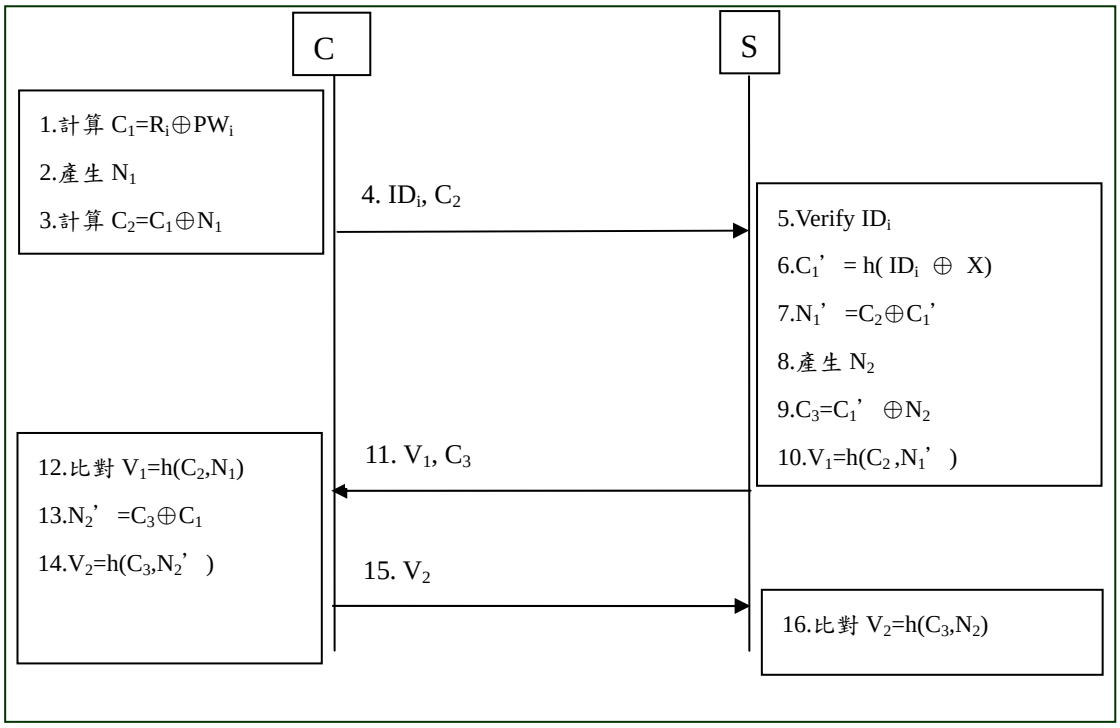

圖 3.4 Lee et al.的遠端認證圖示

步驟說明：

1. 智慧卡利用使用者輸入的 PW_i 與存於卡片內部的 R_i 進行計算 C_1：

   $C_1 = R_i \oplus PW_i$

2. 智慧卡內部以亂數產生器產生亂數 N_1。

3. 卡片端計算 $C_2 = C_1 \oplus N_1$。

4. 卡片端傳送 ID_i 與 C_2 至伺服器：

   $C \rightarrow S$：ID_i, C_2

5. 伺服器驗證 ID_i。

6. 伺服器使用單向雜湊函數將步驟 4 所明文傳入的 ID_i 與伺服器內部儲存的 X 進行

計算 C_1' ：

$C_1' = h(ID_i \oplus X)$

7. 伺服器利用 C_2 與 C_1' 計算：

$N_1' = C_2 \oplus C_1'$

8. 亂數產生 N_2。

9. 伺服器利用 C_1' 與 N_2 計算 C_3：

$C_3 = C_1' \oplus N_2$

10. 伺服器使用單向雜湊函數計算 V_1：

$V_1 = h(C_2, N_1')$

11. 伺服器端傳送 V_1 與 C_3 至卡片端：

$S \rightarrow C$：V_1, C_3

12. 卡片端比對 $V_1 = h(C_2, N_1)$。

13. 比對無誤卡端則計算 N_2' ：

$N_2' = C_3 \oplus C_1$

14. 卡片端計算 V_2 ：

$V_2 = h(C_3, N_2')$

15. 卡片端傳送 V_2 至伺服器端：

$C \rightarrow S$：V_2

16. 伺服器比對 $V_2 = h(C_3, N_2)$。

Lee et al.的遠端認證機制優點如下：

1. 伺服器不需儲存驗證表格。
2. 使用者可自由選擇自己的通行碼。
3. 更低的溝通與計算成本。
4. 使用者與伺服器可相互認證。

5. 使用亂數為基礎，無時間同步問題。

6. 可防禦重送攻擊。

缺點為完全依賴單向雜湊函數使得安全性大幅下降。

第四章 本文的方法

一般的遠端認證機制是以信賴讀卡機為前提[23][24]，我們提出卡片與讀卡機分離的架構並以 Juang 的方法為主體，結合 Lee et al.的變換亂數值機制觀念，保有所有 Juang 機制的所有優點並且比 Juang 機制的安全性更高，此外更深入探討雙向認證之後的服務傳輸方法。

4.1 基本假設

1. 伺服器 S 與其所保存的秘密金鑰(Secret Key) X 是受到良好保護的。
2. 卡片 C 也受到良好保護，無法以非法手段取得卡片內資訊。
3. 讀卡機 R 被視為不可信賴的設備。

4.2 我們的遠端登入機制

我們的方法分成二階段，註冊階段(Registration phase)與登入和溝通金鑰協議階段(Login and session key agreement phase)：

註冊階段(Registration phase)：

使用者 U_i 於安全環境中傳送他的通行碼 PW_i 來向系統進行註冊，系統則賦予使用者唯一的身份識別碼 ID_i 與進行下列步驟：

1. 計算使用者 U_i 的秘密資訊，X 為伺服器保存的秘密金鑰(Secret Key)：

   $V_i = h (ID_i \| X)$

   $W_i = V_i \oplus PW_i$

   $Q_i = h (ID_i \oplus X)$

   $R_i = Q_i \oplus PW_i$

2. 系統於安全環境儲存 ID_i、W_i 與 R_i 至使用者的智慧卡中並將智慧卡給予使用者 U_i。

登入和溝通金鑰協議階段(Login and session key agreement phase)：

使用者拿到智慧卡後，將智慧卡插入讀卡機然後輸入使用者 U_i 的 PW_i，智慧卡比對通行碼無誤則進行以下步驟：

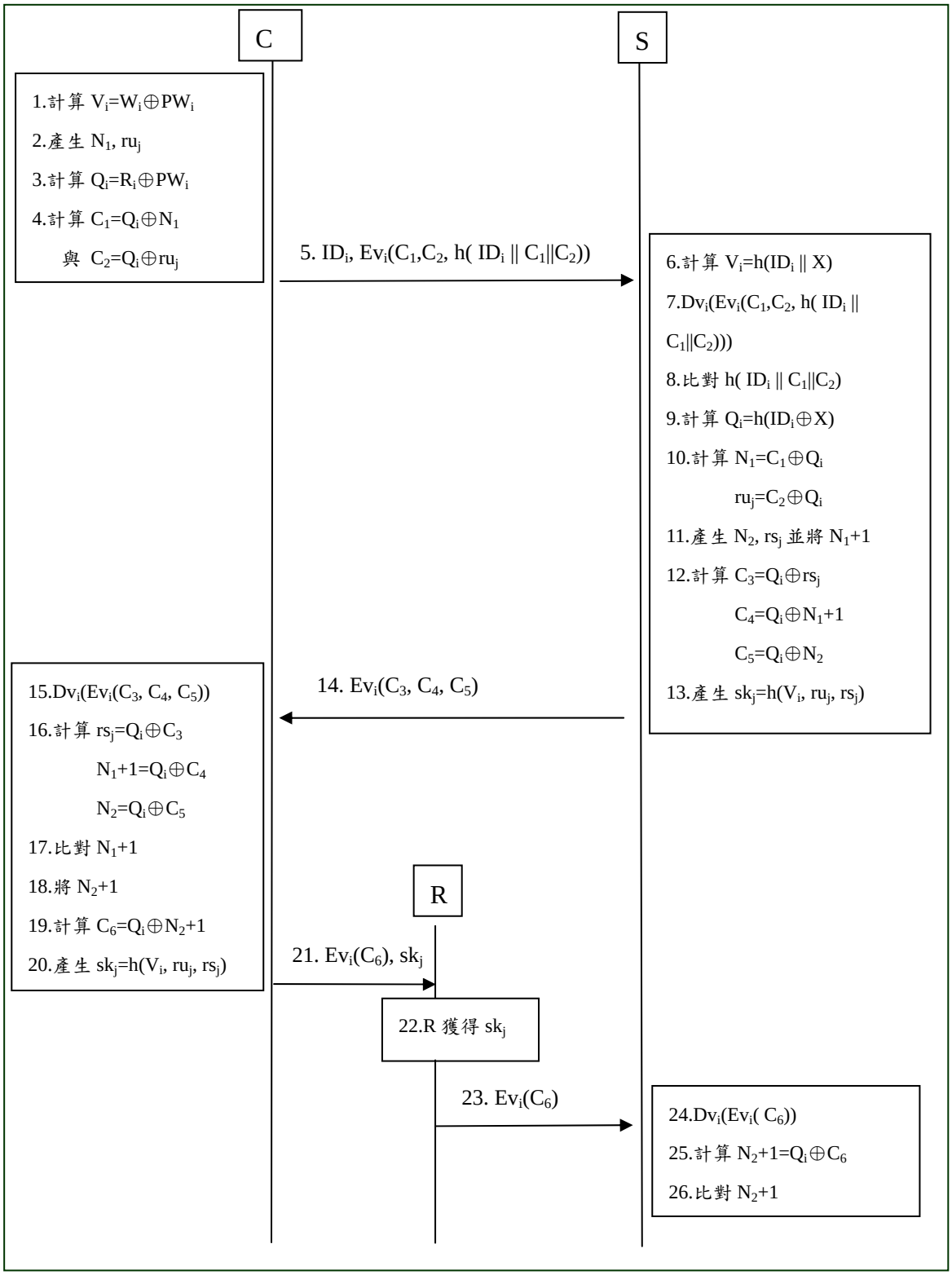

圖 4.2 本論文登入和溝通金鑰協議階段

步驟說明：

1. 智慧卡利用使用者輸入的 PW_i 與存於卡片內部的 W_i 進行計算 V_i：

   $V_i = W_i \oplus PW_i$

2. 智慧卡內部以亂數產生器產生亂數 N_1 與 ru_j。

3. 智慧卡利用使用者輸入的 PW_i 與存於卡片內部的 R_i 進行計算 Q_i：

   $Q_i = R_i \oplus PW_i$

4. 將 N_1 與 ru_j 分別與 Q_i 進行互斥或(XOR)運算：

   $C_1 = Q_i \oplus N_1$

   $C_2 = Q_i \oplus ru_j$

5. 卡片端傳送 ID_i 與用 V_i 進行對稱式加密過的 C_1、C_2 與 $h(ID_i \| C_1 \| C_2)$至伺服器：

   $C \rightarrow S$：$ID_i, Ev_i(C_1, C_2, h(ID_i \| C_1 \| C_2))$

6. 伺服器利用步驟 5 所傳入的 ID_i 與儲存於伺服器的 X 計算 V_i：

   $V_i = h(ID_i \| X)$

7. 伺服器使用 V_i 對 $Ev_i(C_1, C_2, h(ID_i \| C_1 \| C_2))$進行對稱式解密：

   $Dv_i(Ev_i(C_1, C_2, h(ID_i \| C_1 \| C_2)))$

8. 伺服器利用單向雜湊函數比對 $h(ID_i \| C_1 \| C_2)$是否相同。

9. 伺服器利用步驟 5 所傳入的 ID_i 與儲存於伺服器的 X 計算 Q_i：

   $Q_i = h(ID_i \oplus X)$

10. 使用 Q_i 分別算出 N_1 與 ru_j：

    $N_1 = C_1 \oplus Q_i$

    $ru_j = C_2 \oplus Q_i$

11. 亂數產生 N_2、rs_j 並將 N_1+1。

12. 使用 Q_i 分別算出 C_3、C_4 與 C_5：

    $C_3 = rs_j \oplus Q_i$

    $C_4 = N_1+1 \oplus Q_i$

$C_5 = N_2 \oplus Q_i$

13. 伺服器利用 V_i、ru_j 和 rs_j 產生 Session Key：

$sk_j = h(V_i, ru_j, rs_j)$

14. 伺服器傳送用 V_i 進行對稱式加密過的 C_3、C_4 與 C_5 至卡片：

$S \rightarrow C$：$Ev_i(C_3, C_4, C_5)$

15. 卡端對步驟 14 所收到的訊息 $Ev_i(C_3, C_4, C_5)$ 使用 V_i 進行對稱式解密：

$Dv_i(Ev_i(C_3, C_4, C_5))$

16. 使用 Q_i 分別還原 rs_j、N_1+1 與 N_2：

$rs_j = C_3 \oplus Q_i$

$N_1+1 = C_4 \oplus Q_i$

$N_2 = C_5 \oplus Q_i$

17. 卡端比對 N_1+1 是否相同。

18. 比對無誤則將 N_2+1。

19. 使用 Q_i 算出 C_6：

$C_6 = N_2+1 \oplus Q_i$

20. 產生 Session Key，$sk_j = h(V_i, ru_j, rs_j)$。

21. 卡端利用 V_i 加密傳送 C_6 與 sk_j 至讀卡機:

$C \rightarrow R$：$Ev_i(C_6), sk_j$

22. 讀卡機取得 sk_j。

23. 讀卡機續傳 V_i 加密過的 C_6 至伺服器：

$R \rightarrow S$：$Ev_i(C_6)$

24. 伺服器使用 V_i 解碼步驟 21 所收到的 $Ev_i(C_6)$：

$Dv_i(Ev_i(C_6))$

25. 使用 Q_i 算出 N_2+1：

$N_2+1 = C_6 \oplus Q_i$

26. 伺服器比對 N_2+1。

我們的遠端認證機制優點如下：

1. 伺服器不需儲存驗證表格。
2. 使用者可自由選擇自己的通行碼。
3. 低的溝通與計算成本，整個雙向認證階段包含 Session Key 的產生，共使用六次對稱式加解密與六次的單向雜湊函數。
4. 使用者與伺服器可相互認證。
5. 可由使用者與伺服器協議產生新的溝通金鑰(Session Key)。
6. 使用亂數為基礎，無時間同步問題。
7. 可防禦重送攻擊。
8. 與 Juang(2004)[10]方法不同處在於即使 V_i 被破解，由於 Q_i 的保護所以無法立即計算出各項亂數值與溝通金鑰，形成雙重保護。

4.3 服務傳輸階段

使用者在卡片與伺服器雙向認證後會進行各項伺服器所提供的服務，如察看卡片內資訊或進行金融操作，本階段主要是預防在使用者將卡片抽離讀卡機後，不法的木馬程式若偵測得到使用者的相關資訊，偽裝成卡片繼續與伺服器溝通與進行相關服務的操作。

服務傳輸階段：

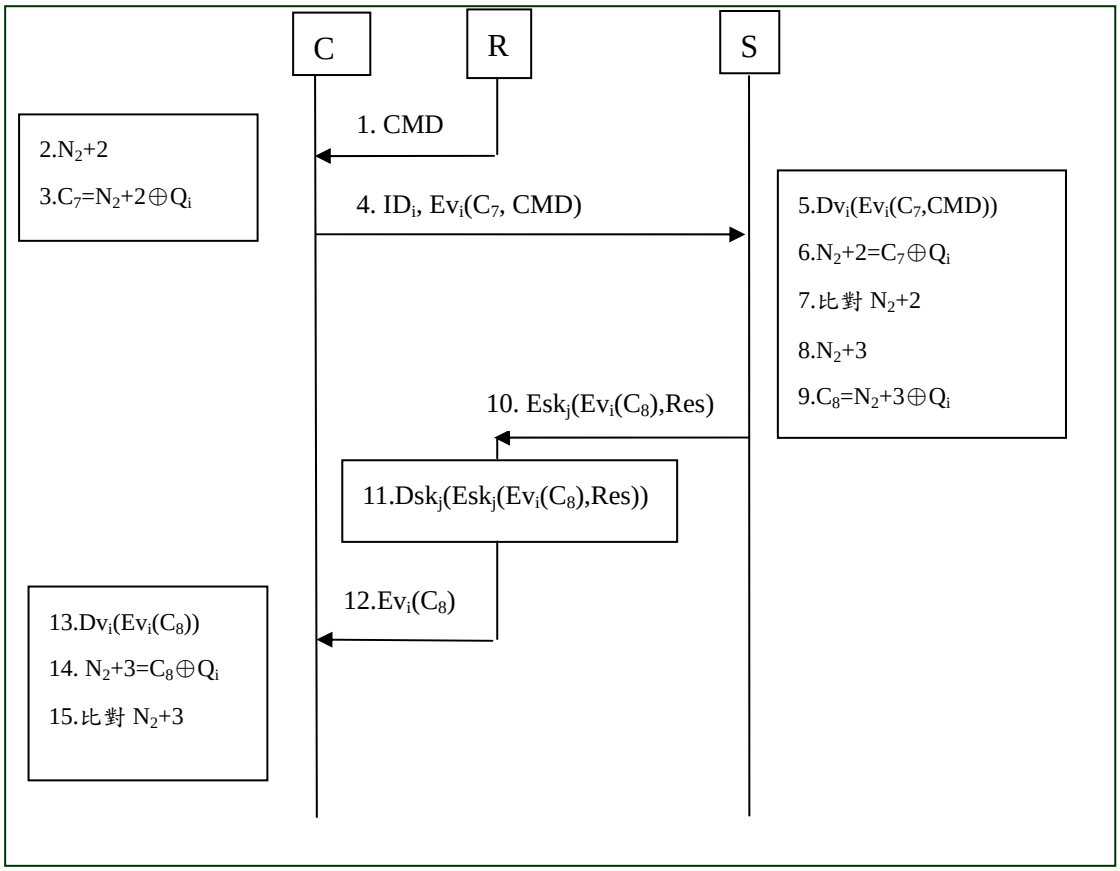

圖 4.3 本論文服務傳輸階段

步驟說明：

1. 使用者選擇所欲執行的命令 CMD 由讀卡機傳至卡片：

   R→C：CMD

2. 智慧卡內部將(N_2+1)+1 成為 N_2+2。

3. 使用 Q_i 計算 C_7：

   $C_7 = N_2+2 \oplus Q_i$

4. 卡片明碼傳 ID_i 與用 V_i 對稱式加密過的 C_7 與 CMD：

   C→S：ID_i, Ev_i(C_7, CMD)

5. 伺服器使用 V_i 對 Ev_i(C_7, CMD)解密：

   Dv_i(Ev_i(C_7, CMD))

6. 使用 Q_i 計算 N_2+2：

$N_2+2 = C_7 \oplus Q_i$

7. 比對 N_2+2。

8. 將$(N_2+2)+1$ 成為 N_2+3。

9. 使用 Q_i 計算 N_2+3：

   $C_8 = N_2+3 \oplus Q_i$

10. 伺服器將 C_8 以 V_i 加密再將 $Ev_i(C_8)$與 Res 以 sk_j 加密傳至讀卡機：

    $S \rightarrow R$：$Esk_j(Ev_i(C_8), Res)$

11. 讀卡機使用 sk_j 解碼 $Esk_j(Ev_i(C_8), Res)$並將 Res 呈現給使用者：

    $Dsk_j(Esk_j(Ev_i(C_8)) ,Res)$

12. 讀卡機將 $Ev_i(C_8)$傳至卡端：

    $R \rightarrow C$：$Ev_i(C_8)$

13. 卡片使用 V_i 對 $Ev_i(C_8)$解密：

    $Dv_i(Ev_i(C_8))$

14. 使用 Q_i 計算 N_2+3：

    $N_2+3 = C_8 \oplus Q_i$

15. 比對 N_2+3。

在服務傳輸階段的資訊傳輸共使用六次對稱式加解密。

4.4 安全性分析

針對第二章文獻探討 2.4 節的各種身份認證攻擊法，從安全性角度來分析本論文所提出的安全服務機制。

4.4.1 重送攻擊(Replay Attack)

在本研究機制是透過 Q_i 轉換過的亂數 N_1 及 N_2 來進行認證的通過，且 N_1 與 N_2

經由 V_i 加密。若攻擊者收集 N_1 及 N_2 來進行重送攻擊，也因為每次傳輸的 N_1 及 N_2 值都會改變，所以攻擊者無法通過卡片端或遠端伺服器的認證。

4.4.2 假冒攻擊(Impersonation Attack)

由於每一次傳遞的訊息都經過 V_i 加密保護，且 V_i 的組成是以使用者 ID 與遠端伺服器的秘密金鑰(Secret Key)經過單向雜湊函數所產生。而遠端伺服器的的秘密金鑰並不在網路上傳送，因此攻擊者無法得知秘密金鑰，也就無法進行假冒攻擊。

4.4.3 中間人攻擊(Man-In-The-Middle Attack)

由於攻擊者必須知道 N_1 與 N_2 值，才可進行中間人攻擊，然而在每個傳送步驟中，N_1 及 N_2 值都是處於 V_i 與 Q_i 的保護下，並不是以明碼方式傳送。因此，中間人攻擊並無法成功達到其目的。

4.4.4 驗證表被竊取後攻擊(Stolen-Verifier Attack)

本機制在伺服器端並無儲存驗證表格(Verification Table)。因此，驗證表被竊取後攻擊對於本機制並無威脅。

4.4.5 偽裝伺服器攻擊(Server Spoofing Attack)

攻擊者想要偽裝成遠端伺服器，必須先知道秘密金鑰(Secret Key)來計算 V_i 與 Q_i，但秘密金鑰只有遠端伺服器知道，且每次傳遞的訊息都經由 V_i 加密與 Q_i 轉換。所以偽裝伺服器攻擊對於本研究機制並不可行。

4.4.6 字典攻擊(Dictionary Attack)

本研究中的卡片設有密碼，只要三次驗證錯誤即鎖住卡片。因此無法透過字典攻擊法來猜測密碼。

4.5 與其他文獻之比較

C1：無驗證表格：

在本研究中並無驗證或密碼表格存在於伺服器上。若存於伺服器上，可能會遭受通行碼驗證資訊遭竊後之攻擊(Stolen-Verifier Attack)。

C2：自由選擇密碼：

使用者可以自由地選擇且變更自己的密碼。本研究的方法並不是以使用者密碼做為產生秘密金鑰(Secret Key)、溝通金鑰(Session Key)或加解密的依據。因此，使用者可以自行設定卡片上的密碼，以防止遺失後被人竊取使用。

C3：低的計算與溝通成本：

由於卡片上電力及記憶體容量的限制下，卡片無法提供強大的運算能力。因此，只能適用於低運算、計算的情況下，才能達到更好的效率。本研究中提出的方法只使用對稱式加解密、單向雜湊函數與互斥或運算(XOR)作為在認證雙方時的計算，而服務的加解密部份，則是透過讀卡設備及伺服器。因此服務的執行與結果回傳，不需透過卡片，因此在運算及計算方面，卡片省去了許多加解密繁重的負擔。

C4：雙向認證：

伺服器與卡片互相彼此認證。本研究透過登入和溝通金鑰協議階段裡的亂數值 N_1 與 N_2 達成雙向認證的目的。

C5：無時間同步問題：

在登入和溝通金鑰協議階段時，需考量彼此認證間的時效性，以防止攻擊者竊取彼此間的封包，進行 Guessing Attack、Impersonation Attack…等攻擊。而在 Tsaur et al.[23] 與 Line et al.[25]皆利用 Timestamp 來解決認證時效性的問題，因此有嚴重的時間同步問題(Time synchronization problem)。相對而言，在本研究的架構、Juang[10]、Shieh and Wang[11]及 Lee et al.[12]是以亂數值(Nonce Number)解決此項問題，所以無時間同步的問題。

C6：新的溝通金鑰：

伺服器與卡片必須產生新的溝通金鑰(Session Key)以保護接下來訊息傳達。透過在雙方每次的認證中，以亂數產生 rs_j 與 ru_j。如果認證無誤，將 V_i、rs_j 及 ru_j 以單向雜湊函數產生出新的 Session Key，$sk_j = h(V_i, rs_j, ru_j)$。

C7：安全的服務與資訊傳輸模式：

一般雙向認證後的資訊傳輸即為使用新的 Session Key 作為加解密，而本文提出以原有 V_i 配合新的 Session Key 加上亂數進行傳輸，能有效防止讀卡機與終端設備被惡意程式植入時產生的威脅。

C8：安全性評量指數：

由於雜湊函數 MD5 與 SHA-1 先後被山東大學的王小雲教授找到碰撞，完全以雜湊函數為基礎所提出的遠端認證機制將面臨嚴重的安全性問題。

本論文的方法則採用對稱式加解密配合單向雜湊函數做運算，即使對稱式加解密被破解，由於傳輸的參數經 Q_i 轉換過，所以仍無法立即計算出溝通金鑰(Session Key)。指數算法為 C1 至 C7 各一顆星(不含 C3)，有達到即加一顆。

SCHEME	C1	C2	C3	C4	C5	C6	C7	C8
Our Scheme	Yes	Yes	6Sym+6H+n*6Sym	Yes	Yes	Yes	Yes	★★★★★★
Juang (2004) [10]	Yes	Yes	6Sym+6H	Yes	Yes	Yes	No	★★★★★
Lee et al. (2005) [12]	Yes	Yes	5H	Yes	Yes	No	No	★★★★
Shieh and Wang (2006) [11]	Yes	Yes	9H	Yes	Yes	Yes	No	★★★★★
Chien et al. (2002) [8]	Yes	Yes	5H	Yes	No	No	No	★★★
Sun (2000) [22]	Yes	No	3H	No	No	No	No	★★
Hwang and Li (2000) [21]	Yes	No	2Exp	No	No	No	No	★
Yang and Shieh (1999) [20]	No	Yes	3Exp	No	Yes	No	No	★★

C1：無驗證表格 C2：自由選擇密碼 C3：低的計算與溝通成本 C4：雙向認證

C5：無時間同步問題 C6：新的溝通金鑰 C7：安全的服務與資訊傳輸模式

C8：安全性評量指數，符合 C1 至 C7(不含 C3)任一項即得一顆星號★

Sym：對稱式加密或解密 H：單向雜湊函數 Exp：指數運算 n：服務執行次數

表 4.5 各遠端認證機制比較表

(資料來源：Wen-Gong Shieh, Jian-Ming Wang, “Efficient remote mutual authentication and key agreement.” Computers and Security, 2006 [11] 與本研究整理)

第五章 系統實作

本章共分為三節，5.1 為系統開發環境之介紹，5.2 則為系統架構，5.3 為系統實作細節與系統畫面之展示，5.4 則為試用之商業模式。

5.1 系統開發環境

本系統的開發環境與使用工具如下：

1. 本系統採用 Java 程式語言，環境為 JDK (Java Developer's Kit) 1.3.1_15 版與 JCE (Java Cryptography Extension) 1.2.1 版。
2. 以 UltraEdit-32 v10.10 為程式開發工具。
3. 智慧卡的開發工具為 Schlumberger 公司的 Cyberflex Access SDK (Software Development Kit) 4.5 版，並符合 Java Card 2.1.1 API specification。
4. 卡片為 Cyberflex Access e-gate 32K card，並符合以下標準 (資料來源：Cyberflex Access SDK 4.5)：
   - ISO7816.
   - Universal Bus Specification(USB) 1.1.
   - Java Card Application Programming Interface 2.1.1.
   - Open Platform Card Specification 2.0.1.
   - 8-bit CPU microcontroller.
   - External clock frequency 1 to 7.5 MHz.
   - Temperature range from -25 to 75 ° C.
   - 30KB EEPROM.
   - EEPROM endurance 700,000 cycles.

- Data retention 10 years.

5. 讀卡機為 Reflex USB v2，支援 USB1.1。
6. 環境運作機器為 FMV LOOX T70K(Pentium-M 753(1.2GHz)，1GB RAM，Hitachi 7k60 HD)。
7. 作業系統為 Microsoft Windows XP Professional SP2。

5.2 系統架構

在本文提出的安全服務機制下，系統呈現三層式的架構(如圖 5.2)，當卡片與遠端伺服器雙向認證後，使用者透過智慧卡經由讀卡機與終端設備向遠端伺服器進行服務的存取，讀卡機與終端設備則被有限度信任。

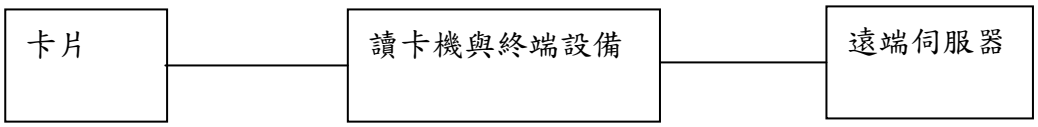

圖 5.2 安全服務機制之三層式架構

5.3 系統實作與展示

針對本文提出的安全服務機制實作出三項常見的服務應用程式，分別為查詢餘額、加值與扣款。卡片內服務相對應的 Command APDU 指令如表 5.3.1：

服務\指令	CLA	INS	P1	P2
查詢餘額(Balance)	0x97	0x30	0x0	0x0

加值(Deposit)	0x97	0x10	0x0	0x0
扣款(Withdraw)	0x97	0x20	0x0	0x0

表 5.3.1 服務與相對應的 Command APDU 指令表

在系統加解密機制方面，第一階段的卡片與遠端伺服器雙向認證採用安全性較高的 Triple-DES 對稱式加解密機制，第二階段的服務傳輸則提供 DES 與 Triple-DES 兩種對稱式加解密，讓使用者依資料量與安全性考量選擇所需的加密方式。

而程式中使用的雜湊函數則為目前安全性較佳的 SHA-1，其訊息摘要為 20Bytes。其餘系統使用的參數格式請參閱表 5.3.2：

名稱	長度(單位：Byte)	說明
以下參數每次雙向認證後保持原狀不更動		
SecretKey	10	伺服器的秘密金鑰
V_i	16	加解密用金鑰
W_i	16	存於卡片內部用於計算 Vi
Q_i	4	保護並轉換各項傳輸過程中的參數
R_i	4	存於卡片內部用於計算 Qi
ID_i	4	使用者唯一代碼
PW_i	4	使用者密碼
以下參數將於每次雙向認證時更新		
SessionKey	16	新的加解密金鑰
ru_j, rs_j	4	用於製作 Session Key
N_1, N_2	4	認證使用

表 5.3.2 系統各項參數長度意義表

以下將展示本系統的實作畫面：

1. 圖 5.3.1 為卡片尚未插入讀卡機時的狀態，使用者可選擇不同的讀卡機進行服務。

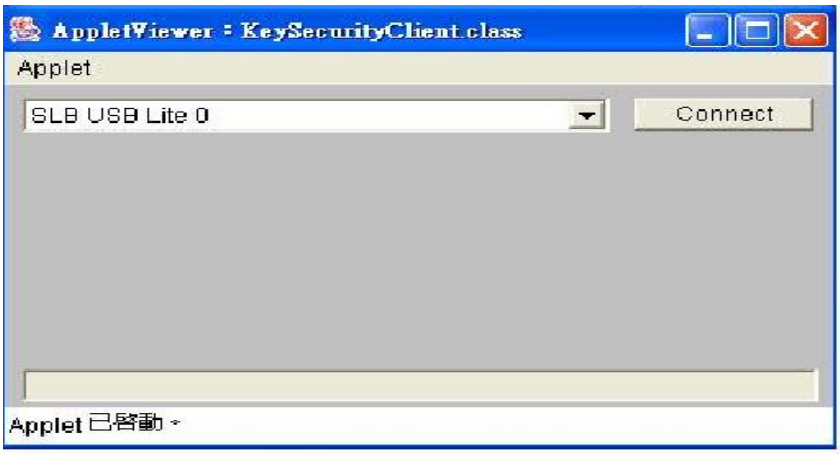

圖 5.3.1 讀卡機介面

2. 使用者選擇適當的讀卡機插卡，輸入使用者密碼經卡片驗證無誤後，顯示查詢餘額、加值與扣款的服務，並可自由選擇 DES 或 Triple-DES 加密機制，如圖 5.3.2。

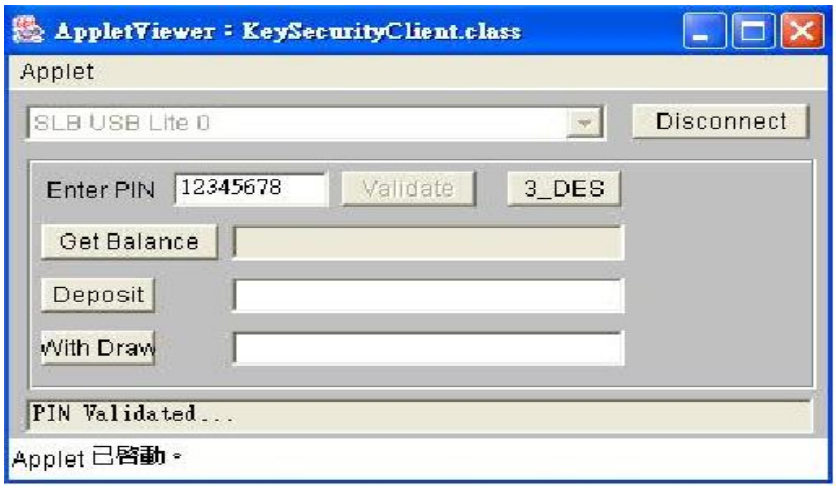

圖 5.3.2 服務選單

3. 使用者選擇適當的讀卡機插卡，輸入使用者密碼經卡片驗證無誤後，進行第一階段雙向認證，第一階段採用 Triple-DES 進行資料加解密，於伺服器端顯示 Session Key 與 N_2(-83, 109, 53, 13)，N_2 並變動至(-82, 110, 54, 14)，第一階段耗時約 4.7 秒，如圖 5.3.3。

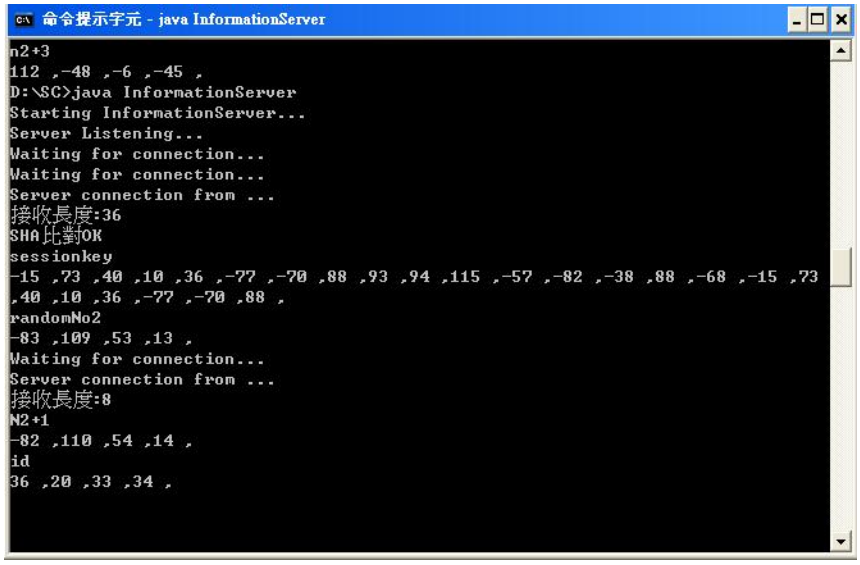

圖 5.3.3 遠端伺服器資訊：第一階段雙向認證完成

4. 執行查詢餘額的服務，N_2 經過兩次動作變動至(-80, 112, 56, 16)，使用 Triple-DES 約 1.7 秒，DES 則約 0.7 秒，如圖 5.3.4。

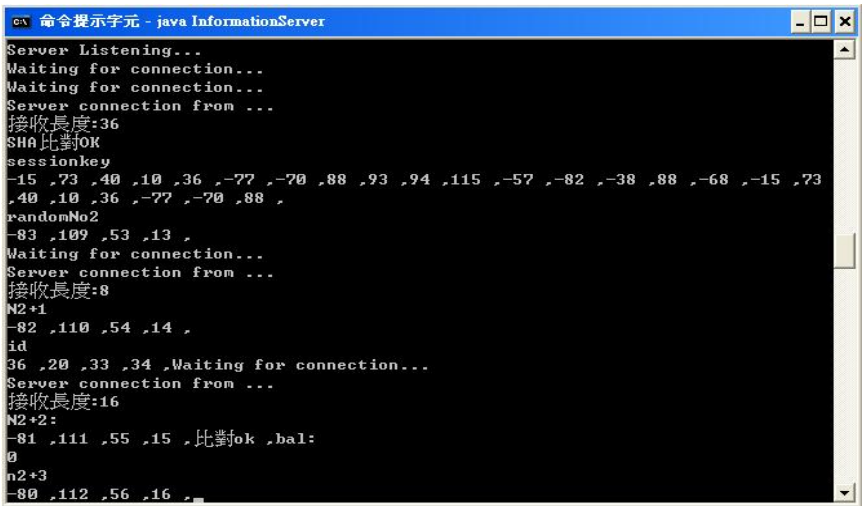

圖 5.3.4 遠端伺服器資訊：執行查詢餘額服務

5. 執行加值 15 元兩次的動作，餘額成為 30 元，N_2 則動作 4 次變動至(-76, 116, 60, 20)，如圖 5.3.5。

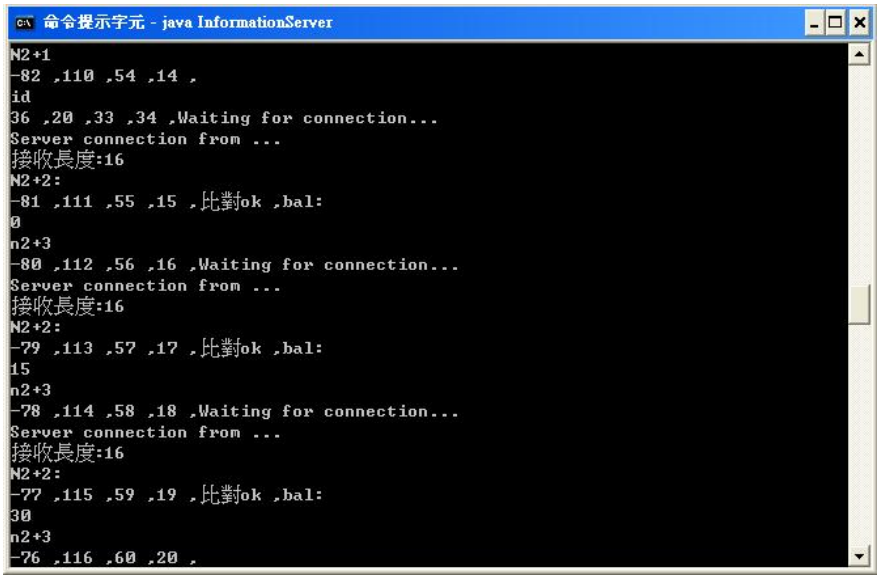

圖 5.3.5 遠端伺服器資訊：執行加值 15 元兩次的服務

5.4 安全服務機制適用的商業模式與應用

本節提出兩種可適用本機制的商業應用模式與相關應用實例，應用行業範圍則包含金融機構、線上遊戲業、醫療院所、連鎖商店、政府便民服務、線上學習與股市投資資訊等，分述於 5.4.1 至 5.4.5 節。

5.4.1 獨立封閉式

各家公司的卡片系統為獨立，使用者需擁有多張卡片，如 7-11 I-cash 卡、星巴克隨行卡、丹堤 e 卡與 IS Coffee VIP 等。

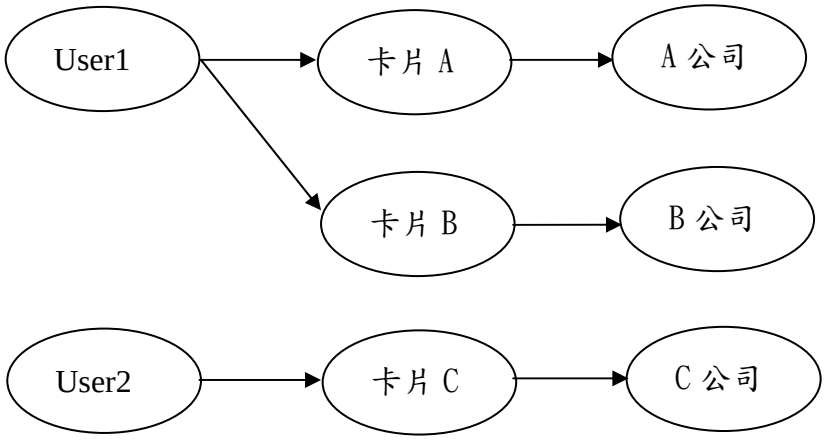

圖 5.4.1 獨立封閉式

5.4.2 異業或同業結盟式

各家結盟公司的卡片系統一致，使用者需只需擁有一張卡片，達到一卡多用的目的，如台北悠遊卡與台中 e 通卡。

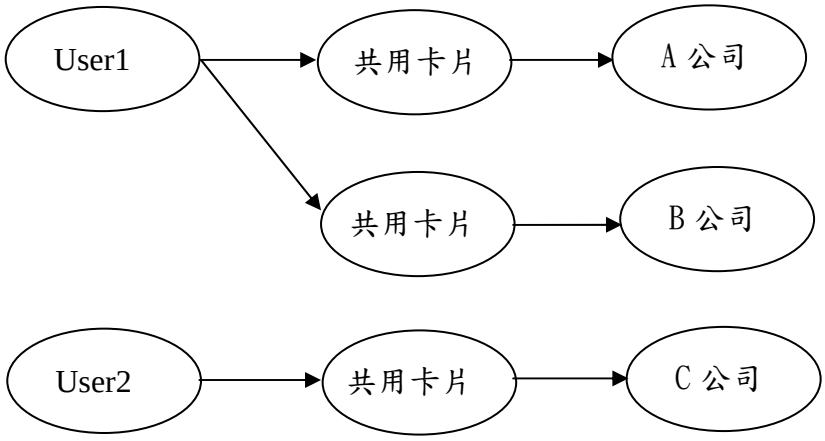

圖 5.4.2 異業或同業結盟式

5.4.3 安全服務機制應用於分散式電子病歷

本文所提出的安全服務機制可完全地配合分散式電子病歷[27]的應用，病患甲可在 A 醫療院所將甲之前於 B 醫療院所的就診資料讀回至 A 醫療院所，以進行完整的醫療診斷。在甲將 IC 健保卡取走後，可有效預防不法程式對病患個人資料資料的存取。

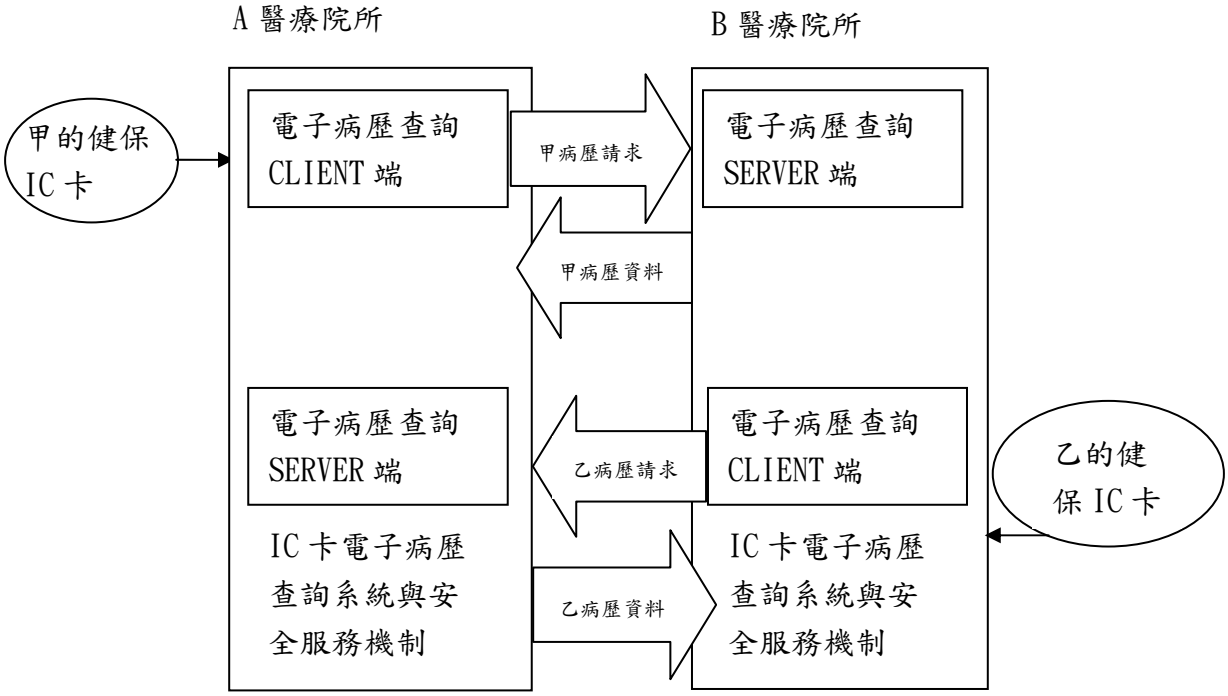

圖 5.4.3 安全服務機制應用於分散式電子病歷

資料來源：[27]

5.4.4 安全服務機制應用於線上遊戲

各式線上遊戲不管是在網路咖啡廳或玩家家中皆可應用本機制，達到預防不法程式的危害，保障玩家的個人資料、虛擬寶物與金錢。

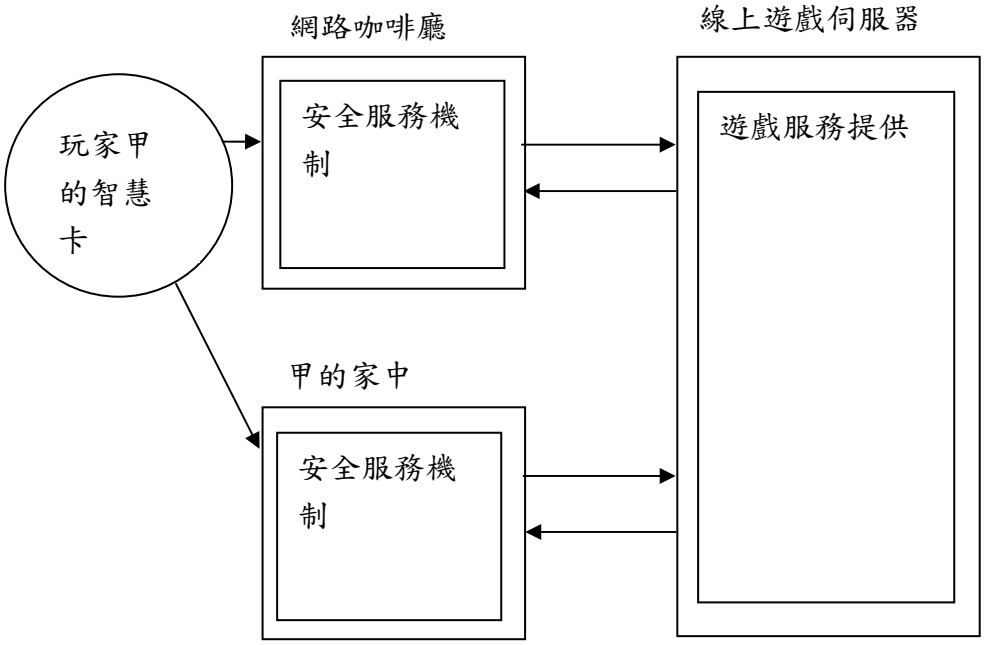

圖 5.4.4 安全服務機制應用於線上遊戲

5.4.5 安全服務機制應用於金融操作

近年興起的網路報稅與線上轉帳或固定地點的 ATM 等金融操作也都適用本機制，達到阻礙歹徒的不法行徑，保障個人的財產與資訊。

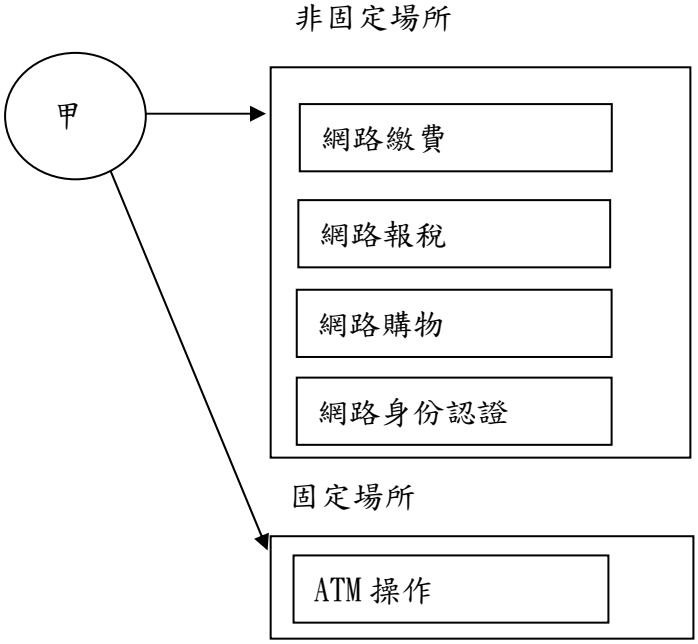

圖 5.4.5 安全服務機制應用於金融操作

第六章 結論與未來研究方向

6.1 結論

網路上的身份認證與資訊傳輸是一項重要的資訊安全議題，由於大部分應用智慧卡的身份認證僅著墨於相互認證，且單向雜湊函數的碰撞陸續被找到，完全以單向雜湊函數為基礎的身份認證機制安全性將大幅下降。本論文所提出的有限信任讀卡機之安全服務機制，利用對稱式加解密配合單向湊函數使用，除提供卡片端與遠端伺服器之相互認證機制，亦能在不完全信任讀卡機之下，提供安全的服務與訊息傳遞架構，防止讀卡機和終端設備之不法程式的危害。

6.2 未來研究方向

1. 本論文提出之安全服務機制，未來在應用上非常廣泛，舉凡金融服務、健保 IC 卡、線上遊戲業、捷運悠遊卡與各式認同卡等皆可配合使用。
2. 本論文對於讀卡機為有限信任，但若能完全不信任讀卡機，則將大幅提昇安全與便利性，也為將來研究之重點。

參考文獻

[1] Leslie Lamport, “Password authentication with insecure communications.” Communication of ACM, vol. 24, pp. 770-772, Nov. 1981.

[2] Lein Harn, D. Huang, C,-S. Laih, “Password authentication using public-key cryptography.” Computer Mathematics with Application, vol. 18, No. 12, pp. 1001-1017, 1989.

[3] Chin-Chen Chang, Ling-Hua Wu, “Sharing a polynomial for password authentication.” Journal of Computers, R.O.C., vol. 1, No.4, pp. 11-17, 1989.

[4] G. Horng, “Password authentication without using password table.” Information Processing Letters, vol. 55, pp.247-250, 1995.

[5] J. K. Jan, Y. Y. Chen, “Paramita wisdom’ password authentication scheme without verification tables.” The Journal of Systems and Software, vol. 42, pp. 45-57, 1998.

[6] H.-Y. Chien, J.-K. Jan, Y.-M. Tseng, “A modified remote log in authentication scheme based on geometric approach.” Journal of System and Software, vol. 55, pp.287-290, 2001.

[7] Cheng-Chi Lee, Li-Hua Li, Min-Shiang Hwang, “A remote user authentication scheme using hash functions.” ACM Operating Systems Review, vol.36, No. 4, pp.23-29, 2002.

[8] Chien H, Jan J, Tseng Y, “An efficient and practical solution to remote authentication：smart card.” Computer and Security, vol. 21, No. 4, pp. 372-375, 2002.

[9] Hsu CL, “Security of Chien et al’s remote user authentication scheme using smart card.” Computer Standards and Interfaces, vol. 26, pp.167-169, 2004

[10] Wen-Shenq Juang, “Efficient password authenticated key agreement using smart cards.” Computer and Security, vol. 23, No. 2, pp. 167-173, 2004.

[11] Wen-Gong Shieh, Jian-Ming Wang, “Efficient remote mutual authentication and key agreement.” Computers and Security, vol 25, No.1, pp.72-77, 2006.

[12] Sung-Woon Lee, Hyun-Sung Kim, Kee-Young Yoo, “Efficient nonce-based remote user authentication scheme using smart cards.” Applied Mathematics and Computation, vol. 167, pp.355-361, 2005.

[13] X. Y. Wang, D. G. Feng, X. J. Lai, and H. B. Yu, ”Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD. ” Rump session of Crypto’04 and IACR Eprint archive, August 2004.

[14] Xiaoyun Wang, Hongbo Yu , “How to Break MD5 and Other Hash Functions.” Advances in Cryptology – EUROCRYPT 2005: 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005.

[15] Xiaoyun Wang, Yiqun Lisa Yin, Hongbo Yu, “Fing collision in the full SHA-1.” Advances in Cryptology – CRYPTO 2005: 25th Annual International Cryptology Conference, Santa Barbara, California, USA, August 14-18, 2005.

[16] C. C. Chang, T. C. Wu, “Remote password authentication with smart cards.” IEEE Proceedings 138, pp.165-168, 1991.

[17] C. C. Chang, W. Y. Liao, “A remote password authentication scheme based upon EI Gamal’s signature scheme.” Computer and Security, vol. 13,pp. 137-144, 1994.

[18] T. C. Wu, “Remote log in authentication scheme based on a geometric approach.” Computer Communications, vol. 18, pp.959-963, 1995.

[19] M.-S. Hwang, “A remote password authentication scheme based on the digital signature method.” International Journal of Computer Mathematics, vol. 70, pp. 657-666, 1999.

[20] W. H. Yang, S. P. Shieh, “Password authentication schemes with smart cards.” Computer and Security, vol. 18, pp.727-733, 1999.

[21] M.-S. Hwang, L. H. Li, “A new remote user authentication scheme using smart cards.” IEEE Transactions on Consumer Electronics, vol. 46, pp.28-30, 2000.

[22] H. Sun, “An efficient remote user authentication scheme using smart cards.” IEEE Transactions on Consumer Electronics, vol. 46, No.4, pp.958-961, 2000.

[23] Wei-Chi Ku, Hao-Chuan Tsai, and Maw-Jinn Tsaur, “Stolen-Verifier Attack on an Efficient Smartcard-Based One-Time Password Authentication Protocol,” to appear in IEICE Transaction on Communications, Vol.E87-B, No.8, Aug. 2004.

[24] 余彥宏，智慧卡離線交易認證機制之研究，碩士論文，民國 93 年。

[25] I. C. Lin, M. S. Hwang and L. H. Li, “A new remote user authentication scheme for multi-server architecture, Future Generation Computer Systems, Vol. 19, pp. 13-22, 2003.

[26] Workshop on Smart Card Standards and Practical Applications, Sep.2005.

[27] 劉建良，“健保 IC 卡與分散式電子病歷系統整合探討”，國立暨南國際大學資訊管理學系碩士學位論文，2001 年。