多伺服器環境中的使用者身分認證協議之研究

陳德祐、李正吉、王鵬程

摘 要

現今的網路架構有傾向於朝分散式環境發展的趨勢，在這個架構下，系統的資源以及服務分散在多個伺服器上，由這些伺服器共同合作提供使用者需要的資源或服務。因此，多伺服器環境中的使用者身分認證協議成為網際網路應用上一個相當重要的研究議題，近十年來，吸引了相當多的學者致力於此一議題的研究，並且已經有相當豐富的研究成果，然而，這些方法存在相當多的改善空間，例如安全性、效率以及使用者隱私等面向。在這篇文章中，我們將針對目前已提出的多伺服器環境中的使用者身分認證方法進行分析以及比較，指出這些方法的優缺點，並提出在此一環境中的使用者身分認證研究上幾個未來值得繼續深入探討的重要議題。

關鍵詞：使用者身分認證、金鑰協議、多伺服器環境、分散式系統、密碼學、網路安全。

陳德祐：修平技術學院資訊網路技術系助理教授
李正吉：輔仁大學圖書資訊學系助理教授
王鵬程：修平技術學院資訊管理系副教授
投稿日期：990222 接受刊登日期：990322

Research on User Authentication for Multi-server Environment

Te-Yu Chen, Cheng-Chi Lee, Peng-Cheng Wang

Abstract

In the present time, there is a tendency towards the distributed environment in which resources and services are allocated to multiple servers. These servers should cooperate to serve their users. Therefore, user authentication for multi-server environment has become an important issue in the Internet applications. During the recent decades, this issue has attracted much more attention from cryptographic researchers; Though there are some schemes proposed in the literature, a lot of subjects should be improved in these proposed schemes, such as the security, efficiency, and user privacy. In this paper, we will first analyze these schemes in detail. Some important issues deserving to be further researched in the user authentication for multi-server environment are pointed out accordingly.

Keywords: Authentication, key agreement, multi-server architecture, distributed system, cryptography, network security.

Te-Yu Chen, Assistant Professor, Department of Information Networking Technology,Hsiuping Institute of Technology.
Cheng-Chi Lee, Assistant Professor, Department of Library and Information Science,Fu Jen Catholic University.
Peng-Cheng Wang, Associate Professor, Department of Information Management, Hsiuping Institute of Technology.

1. 前言

隨著科技及網路技術的進步及普及，越來越多傳統人們的活動已轉移到網路上進行，現今的生活中，有很多的服務是經由網際網路(Internet)提供給散佈在世界各地的客戶。由於當初網際網路的設計是秉持開放式(openness)的理念，並且欠缺對安全性相關的完整考量，因此，如何能夠為合法的使用者提供服務並且確保資料傳輸過程的安全性，是一個迫切需要認真審視的一個重要議題。使用者身分認證系統(User authentication scheme)是一個由服務供應端(service provider)執行的機制，此機制的功能是讓服務供應端在提供服務前得以用來確認客戶端(client)的身分；相對地，為了確保客戶端避免遭受偽冒伺服器的詐欺，客戶端也必須要確認服務供應端的身分。再者，網際網路上傳遞的資料可以輕易的被讀取，因此，在服務供應端與客戶端互相確認彼此身份的合法性之後，亦須妥善保護服務供應端與客戶端之間傳遞的資料，以避免遭受竊聽。為了保護資料避免被非法竊聽，通常採行對稱式加密(symmetric encryption)的方法，此方法需要一把金鑰，由發送端在資料傳輸前先進行加密，接收端在收到加密過的資料後，再以此金鑰進行解密。是以，為了保護傳輸資料的安全性，使用者身分認證系統需要包含金鑰產生(session key establishment)的程序。基於上述的分析，一個好的使用者身分認證系統，不只要能提供服務供應端與使用者之間彼此身份的雙向認證(mutual authentication)，更要能在完成身分認證時，建立出一把加密後續傳輸資料的金鑰。

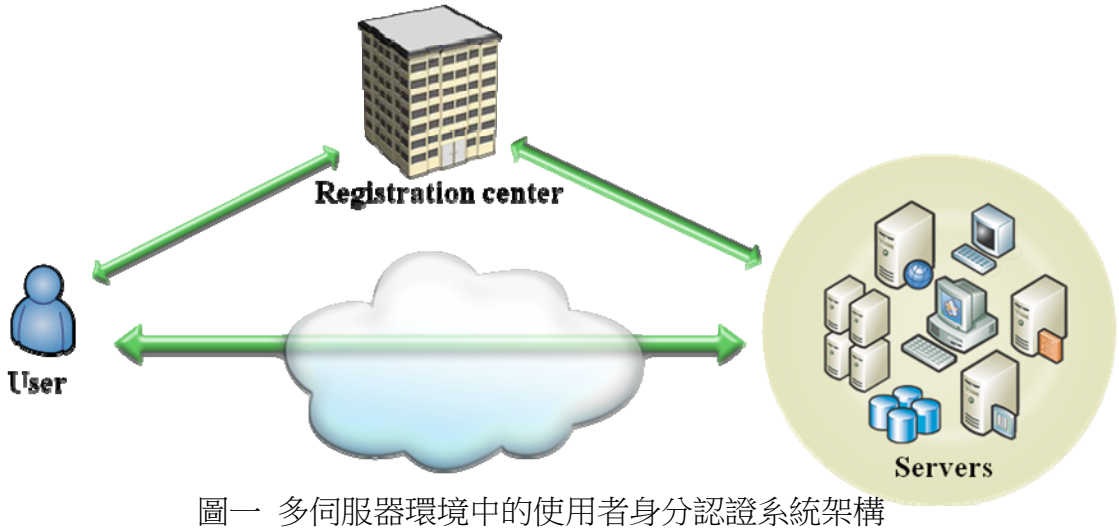
使用者身分認證(user authentication)以及金鑰協議(key agreement)是在網際網路上一個相當重要的研究議題，因此吸引了相當多的學者致力於此一議題的研究，並且已有相當豐富的研究成果，如[2, 4, 7, 12, 13, 14, 18, 21, 22, 23, 30]。這些傳統的使用者身分認證方法都是為單一的服務供應端所設計，然而，現今的網路架構已有傾向於朝分散式環境(distributed environment)發展的趨勢。在分散式環境中，各項資源以及服務散布在多個伺服器上，這些伺服器合作提供服務給它們的使用者。如果將傳統的使用者身分認證方法直接使用在分散式的環境中，每一個伺服器必須各自獨立管理其採行的認證機制，而且使用者必須一一向各個伺服器註冊以取得使用權，並且使用者必須費心於管理這些不同的登入(login)資訊(帳號及密碼等)。因此將傳統的使用者身分認證方法直接使用在多伺服器(multi-server)的環境中，顯得相當沒有效率，且窒礙難行。隨著多伺服器系統的不斷增加，近十

年來也吸引了一些學者對此一議題進行研究，如[1, 5, 6, 16, 17, 19, 20, 24, 26, 28]。由於多伺服器環境中的使用者身分認證越來越受到重視，因此，在這篇文章中，我們將針對目前已提出適用於此環境中的諸多使用者身分認證方法進行分析以及比較，指出這些方法的優缺點，並提出在此一環境中的使用者身分認證研究上幾個未來值得繼續深入探討的重要議題。

一個合格的多伺服器環境中的使用者身分認證系統必須滿足下列幾個基本條件[6, 17, 29]：

(一) 單次註冊：使用者僅需向註冊中心註冊一次，完成註冊後，他可以登入系統中的任一伺服器。

(二) 無須紀錄驗證表單：註冊中心以及任何伺服器皆不需要儲存或維護認證、密碼等表單。



圖一 多伺服器環境中的使用者身分認證系統架構

一般而言，在多伺服器環境中的使用者身分認證系統，如圖一所示，包含三個角色：使用者、註冊中心、以及伺服器。如果使用者想要使用屬於此一系統中的伺服器所提供的資源或服務，他僅需向註冊中心註冊，而不是單獨向各個伺服器註冊，完成註冊後，使用者得以登入此系統中的任何伺服器。

(三) 使用者的便利性：認證系統提供一個便利及友善的使用方式。

(四) 有效率：不論是計算或通訊成本應該越低廉越好。

(五) 達成雙向認證：不僅是伺服器能確認使用者的身分，使用者也要能確認伺服器的身分。

(六) 建立加密金鑰：在完成身分認證後，使用者和伺服器之間要能協議出一把金鑰。

除了上述幾個基本條件外，一個合格的多伺服器環境中的使用者身分認證系統尚須滿足下列幾個安全性的要求[5, 6, 24, 29]：

(一) 金鑰的安全性：僅有使用者和伺服器得知協議出來的金鑰，無其他第三方(包含認證中心)得以知曉金鑰。另外，協議出來的金鑰亦須具有 forward secrecy, key secrecy 等安全性要求。

(二) 認證系統的強韌性：認證系統必須要有充分的安全性，足以抵擋各類型的攻擊，例如偽冒攻擊(impersonation attack)、重送攻擊(replay attack)、密碼猜測攻擊(password guessing attack)、內部攻擊(insider attack)、伺服器/註冊中心愚弄攻擊(server/registration center spoofing attack)等。

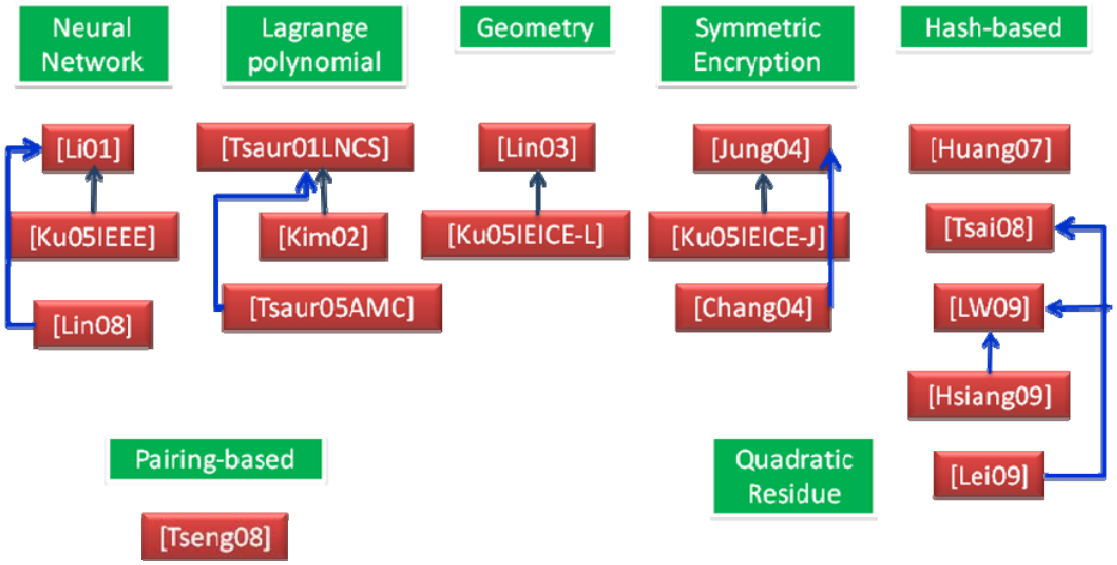
這篇文章剩餘的其它章節安排如下：第二章將介紹目前在多伺服器環境中的使用者身分認證機制的研究現況。經過分析比較這些方法後，我們在第三章提出在多伺服器環境中的使用者身分認證機制上幾個未來值得繼續深入探討的重要議題。最後，第四章是這篇文章的結論。

2. 相關文獻探討

根據我們的探討，從西元 2000 年開始即陸陸續續有一些多伺服器環境中的使用者身分認證方法被提出來，這些方法為了達成他們宣稱的功能，以及保有安全性，通常植基於一些密碼系統常用的數學模型，例如類神經網路(Neural Network)、拉格朗日多項式(Lagrange polynomials)、幾何(Geometry)、對稱式加密(Symmetric Encryption)、雜湊/互斥或運算(Hash-exclusive or based)、二次剩餘(Quadratic Residue)、以及雙線性配對(Bilinear Pairing)等。這些方法的分類整理如圖二所示。

在文獻中，最早的一個多伺服器環境中的使用者身分認證系統是由 Lee and Chang[15]在 2000 年所提出。隨後，Tsaur[25] 和 Li 等人[16] 相繼於 2001 年分別各自提出他們的方法。不幸地，這些方法都存有一些可能遭受攻擊的弱點，Kim 等人[8]於 2002 年指出 Tsaur[25]所提出的方法無法抵擋密碼猜測攻擊。因此，2005 年，Tsaur 等人[27]針對這個問題提出了他們的改進方法，為了解決這個被質疑的問題，他們使用了 RSA 密碼系統以及拉格朗日多項式。

然而， RSA 密碼系統以及拉格朗日多項式的運算為系統帶來了相當高的計



圖二 多伺服器環境中的使用者認證系統

算複雜度，並且為了使用拉格朗日內差法推算出秘密多項式，需要傳輸為數不少的資料量，這個改良的方法在計算上以及資料傳輸上的效率因此較不如人意。另一方面，Ku 等人[9] 於 2005 年亦指出 Li 等人[16]的方法無法有效抵擋密碼猜測攻擊以及內部攻擊。Lin[19]因此於 2008 年提出他們的改量方法，他們的這二個方法都使用了類神經網路系統，類神經網路系統需要龐大的運算以完成類神經網路的建構和訓練，因此導致這二個方法在計算上的效率亦不甚良好。

在 2003 年，Lin 等人[20]基於歐幾里得空間(Euclidean space)中的幾何特性提出了一個多伺服器環境中的使用者身分認證方法，Ku 等人[10] 隨即指出這個方法存在偽造攻擊和密碼猜測攻擊，並且此一方法在遭遇若干系統參數洩漏的情況時，系統修復的代價相當高昂。

Juang[6] 使用對稱式密碼系統於 2004 年提出了一個多伺服器環境中的認證金鑰協議方法，這個方法能同時達到相互身分認證以及金鑰協議。然而，Ku 等人[11]指出這個方法無法抵擋內部攻擊，並且這個方法協議出來的金鑰無法具有前向安全性(forward secrecy)。Chang 和 Kuo[1]使用中國餘數定理也提出了一個他們的多伺服器環境中的認證金鑰協議方法，Hwang 和 Shiau[5]於 2007 年指出[6]和[1]這二個方法都欠缺金鑰協議的明確性以及通訊成本過高等問題，同時他們也提出了一個基於平面幾何的方法以改進這些缺點。然而，Hwang 和 Shiau

的方法須要維護使用者資料表，並且他們的方法依然欠缺金鑰的前向安全性。

2009 年，Liao 和 Wang[17]提出了一個基於動態身分識別碼並適用於多伺服器環境中的使用者身分認證系統，為了讓這個方法達到使用者身分的匿名性以適用於一些需要保護使用者身分的特殊應用上，他們巧妙地以動態身分識別碼取代原先固定的身分識別碼而達到匿名性的特性。但是，很遺憾地，他們的方法遭受到相當多不同類型的攻擊，例如偽冒攻擊、愚弄攻擊、以及猜測密碼攻擊等[3, 29]。因此，Hsiang 和 Shih[3]提出了一個改進 Liao 和 Wa 的方法，不過這個改良過的方法依然可能會遭受到偽冒攻擊，而且這個改良過的方法未能提供雙向身分認證，以及一旦使用者執行過密碼修改的程序後，這個使用者將無法再成功地登入任何伺服器。

Tsai[24]也於 2008 年提出了一個多伺服器環境中的使用者身分認證方法，他們的方法因為只使用到相當輕量的運算，例如雜湊函數及互斥或等運算，因此在計算量上相當有效率。然而，這個方法卻不夠安全。Wang 等人[29]於 2009 年指出這個方法會遭受到伺服器愚弄攻擊以及偽冒攻擊，因此他們提出了一個基於二次剩餘的方法以消弭這些弱點。不幸地，這兩個方法都還具有二個缺陷。第一，使用者和伺服器之間協議出來了金鑰未能具有前向安全性，一旦，主金鑰若是遭到破解，則所有先前使用過的金鑰亦會隨之被破解，這也意味先前受到這些金鑰保護的機密訊息將因此而曝光，進而影響到使用者的隱私。第二，註冊中心可以知曉所有伺服器和使用者之間協議出來的金鑰。雖然註冊中心普遍被視為是公正的第三者，但是如果他可以得知使用者跟伺服器之間通訊的內容，然免會引起使用者對其自身隱私權的疑慮。因此，為了要提供一個完全令人信賴的通訊環境，這兩個問題需要特別留意並加以仔細考量。

上述文獻探討中，幾個較具代表性的方法我們對其功能性、安全性以及效率作了詳細的分析以及比較，彙整結果如表一及表二所示。

表一 多伺服器環境中的使用者身分認證方法的功能性/安全性比較

	[24]	[17]	[3]	[29]
Single registration	Yes	Yes	Yes	Yes
Mutual authentication	Yes	No	No	Yes
No verification table	Yes	Yes	Yes	Yes
Securely chosen password	Yes	Yes	No	Yes
Session key agreement	Yes	Yes	Yes	Yes
User's anonymity	No	Yes	Yes	Yes
Necessity of time synchronization	No	No	No	No
Session key secrecy	No	No	No	No
Forward secrecy	No	No	No	No
Resistance to replay attack	Yes	Yes	Yes	Yes
Resistance to stolen-verifier attack	Yes	Yes	Yes	Yes
Resistance to Server Spoofing	No	No	Yes	Yes
Resistance to RC spoofing	Yes	No	Yes	Yes
Resistance to Masquerading attack	No	No	No	Yes

表二 多伺服器環境中的使用者身分認證方法的效率比較

Phase		[24]	[17]	[3]	[29]
A		$2T_{hash}+1T_{xor}$	$5\ T_{hash}+2\ T_{xor}$	$8\ T_{hash}+4\ T_{xor}$	$2T_{hash}+1T_{xor}$
B		$1T_{hash}$	$1T_{hash}$	$1T_{hash}$	$1T_{hash}$
C		$1T_{hash}+2T_{xor}$	$6\ T_{hash}+3\ T_{xor}$	$7\ T_{hash}+7\ T_{xor}$	$1T_{qre}$
D	User	$4T_{hash}+3T_{xor}$	$3\ T_{hash}$	$2\ T_{hash}$	$4T_{hash}$
	Server	$6T_{hash}+7T_{xor}$ /$4T_{hash}+4T_{xor}$	$6\ T_{hash}+3\ T_{xor}$	$8\ T_{hash}+6\ T_{xor}$	$6T_{hash}+4T_{xor}$
	RC	$6T_{hash}+5T_{xor}$ /$4T_{hash}+2T_{xor}$	0	$5\ T_{hash}+7\ T_{xor}$	$8T_{hash}+3T_{xor}+1T_{qrd}$
	Total	$16T_{hash}+15T_{xor}$ / $12T_{hash}+9T_{xor}$	$9\ T_{hash}+3\ T_{xor}$	$15\ T_{hash}+13\ T_{xor}$	$18T_{hash}+7T_{xor}+T_{qre}+T_{qrd}$
E		$2T_{hash}+2T_{xor}$	$4\ T_{hash}+5T_{xor}$	$4\ T_{hash}+4T_{xor}$	$2T_{hash}+2T_{xor}$
F		7rounds	3rounds	5 rounds	5rounds

符號說明：

- A: 使用者註冊階段。
- B: 伺服器註冊階段。
- C: 使用者登入階段。
- D: 身分確認階段 (包含 session key 的建立)。
- E: 密碼變更階段。
- F: 通訊回合數。
- T_{hash}：執行一次雜湊函數所需的時間。
- T_{xor}：執行一次互斥或運算所需的時間。
- T_{exp}：執行一次模指數運算所需的時間。
- T_{sym}：執行一次對稱式加密或解密所需的時間。
- T_{qre}：執行一次二次剩餘加密所需的時間。
- T_{qrd}：執行一次二次剩餘解密所需的時間。

3. 值得繼續深入研究之議題

由前一章的文獻探討中，我們發現，目前已被提出來的多伺服器環境中的使用者身分認證方法，或多或少都存在一些安全性上面的缺陷。在現今充斥了各類危機的網路環境中，一個方法若有安全性方面的瑕疵，即使它擁有相當強大的功能亦或具有相當低成本的計算量及通訊成本，這個方法依然不具有任何的實用價值，因此，安全性方面的考量，是任何一個方法最基本也是最重要的考量。所以我們認為考量所有可能的安全性威脅，並儘可能地降低計算成本及通訊成本的前提下，設計一個多伺服器環境中的使用者身分認證方法，是一個未來相當值得持續研究的重點。

另外，使用者的隱私權保護是一個越來越受到重視的一個議題，尤其在多伺服器環境中，使用者的隱私將暴露在較高的危險威脅中，因此，能兼顧安全、效率以及使用者隱私權保護的多伺服器環境中的使用者身分認證方法，是另外一個值得進一步探討的研究方向。

目前的多伺服器環境中的使用者身分認證方法之所以存在安全性弱點，最主要的原因為，這些方法大都未提供正式的安全性證明，因此，可證明安全性的多伺服器環境中的使用者身分認證方法，亦是一個值得深入探討的研究方向。

在這一章節中，我們將就這幾個重要的研究方向，逐一進行介紹。

3.1. 同時兼具效率與滿足各項安全要求的多伺服器環境中的使用者身分認證方法

在分散式環境中，各項資源以及服務散佈在不同的伺服器上，用以降低單一伺服器的負擔，並可提供較高的容錯性，避免單一伺服器故障所造成的全面性影響，因為這些優勢，現今有越來越多的網路環境朝向分散式型態發展演進，然而，傳統適用於集中式環境的使用者身分認證機制因此並不全然適用於分散式的多伺服器環境中。經過分析探討集中式環境與分散式環境上使用者身分認證系統的異同，我們歸納出一個合格的多伺服器環境中的使用者身分認證系統必須滿足第 1 章中所列出來的六個多伺服器環境的基本要求條件以及二個安全性的要求條件。

如前一章中的文獻探討所示，近十年來，多伺服器環境中的使用者身分認證問題已引起廣泛的注意，也有一些方法被提出來，在我們進一步針對最近提出的幾個較傑出的方法進行功能性及安全性的分析比較後，彙整如表一所示，有如下之

發現，2008 年 Tsai[24]所提出的多伺服器環境中的使用者身分認證方法，雖然在計算量上相當有效率，但是，這個方法卻不夠安全，不僅無法抵擋愚弄攻擊和偽冒攻擊，而且協議出來的金鑰不具有金鑰前向安全性以及金鑰私密性。2009 年 Liao 和 Wang[17]提出的基於動態身分識別碼並適用於多伺服器環境中的使用者身分認證系統，雖然可以達到使用者身分的匿名性，但是，他們的方法亦遭受到相當多不同類型的攻擊，例如偽冒攻擊、愚弄攻擊、以及猜測密碼攻擊等，而且，這個方法協議出來的金鑰亦不具有金鑰前向安全性及及金鑰私密性。Hsiang 和 Shih[3]於 2009 年提出來改進 Liao 和 Wang 的方法，依然可能會遭受到偽冒攻擊，並且這個改良過的方法未能提供雙向身分認證，以及一旦使用者執行過密碼修改的程序後，這個使用者將無法再成功地登入任何伺服器，在金鑰的安全性方面亦欠缺金鑰的前向安全性以及金鑰的私密性。Wang 等人[29]於 2009 年提出來的多伺服器環境中的使用者身分認證方法，雖然可以抵擋大部分的攻擊，但是這個方法協議出來的金鑰依然未能具有金鑰的前向安全性以及金鑰的私密性等安全要求。

綜而言之，這些方法都普遍具有二個共通的缺陷。第一，使用者和伺服器之間協議出來了金鑰未能具有前向安全性，一旦，主金鑰若是遭到破解，則所有先前使用過的金鑰亦會隨之被破解，這也意味先前受到這些金鑰保護的機密訊息將因此而曝光，進而影響到使用者的隱私。第二，註冊中心可以知曉所有伺服器和使用者之間協議出來的金鑰。雖然註冊中心普遍被視為是公正的第三者，但是如果他可以得知使用者跟伺服器之間通訊的內容，然免會引起使用者對其自身隱私權的疑慮。因此，為了要提供一個完全令人信賴的通訊環境，這兩個問題需要特別留意並加以仔細考量。

此外，Tsai[24]、Liao 和 Wang[17]以及 Hsiang 和 Shih[3]等方法亦遭受不同型態的安全威脅，在開放式的網路環境中，各式各樣的攻擊無奇不有，若一個方法禁不起攻擊，則毫無存在的價值。因此，如何仔細審視這些多樣的攻擊類型，進而謹慎的設計能防堵各類型的攻擊，也是一個需要詳加考量的要點。

另外，效率也是另一個重要的考量點，針對這幾個較具代表性的方法我們亦針對其計算上以及通訊上的效率進行比較分析，彙整結果如表二所示。

在計算量的分析比較上，在這些方法中，除了 Wang 等人的方法[29]需要進行稍微複雜的二次剩餘加解密運算外，其他的方法如 Tsai[24]、Liao 和 Wang[17]以及 Hsiang 和 Shih[3]等方法，都只需要

進行一些輕量的運算，如雜湊函數及/或互斥或等運算。雖然這些輕量的運算不會耗費太多系統資源，但是就伺服器端而言，若同時擁進大量的使用者，則累加起來的資源消耗不可謂不大；另一方面，就使用者端而言，若能降低計算量，則可進一步降低使用者端的硬體成本，且可讓使用者更順暢的使用此系統。

在通訊量的分析比較上，在這些方法中，Liao 和 Wang 的方法[17]僅需三回合的資料傳輸，Wang 等人[29]以及 Hsiang 和 Shih[3]的方法各需五回合的資料傳輸，而 Tsai 的方法[24]更需高達七回合的資料傳輸。資料傳輸的回合數越多，意味著使用者需等候的時間也會越多，因此，如何能有效的降低傳輸的回合數以及傳輸的資料量，亦是一個重要的議題。

基於上述的分析、探討，我們認為一個適用於多伺服器環境中，同時兼具安全與效率，並且滿足下列幾點要求的使用者身分認證方法，是第一個重要的研究方向。

1. 適用於多伺服器環境中，亦即使用者僅需向註冊中心註冊一次，完成註冊後，他可以登入系統中的任一伺服器。
2. 無須紀錄驗證表單，註冊中心以及任何伺服器皆不需要儲存、維護認證、密碼等表單。
3. 提高使用者的便利性，從註冊、登入以及密碼的修改，系統都能提供一個便利、友善的使用方式。
4. 達成雙向身分認證，不僅是伺服器能確認使用者的身分，使用者也要能確認伺服器的身分。
5. 協議出一把安全的金鑰，這把金鑰僅有使用者和伺服器得知，無其他第三方(包含認證中心)得以知曉金鑰。另外，協議出來的金鑰必須各項安全性的要求。
6. 此認證系統必須夠強韌，足以抵擋各類型的攻擊。
7. 盡可能的降低計算成本以及通訊成本。

3.2. 具有使用者隱私權保護的多伺服器環境中的使用者身分認證方法

近年來，隨著資訊科技與網路技術的持續發展與普及，使得運用這些技術的各類型應用模式快速的蓬勃發展，在一些應用環境上，例如電子商務，雖然提供了消費者一個極為便利的消費方式，但是也引發了其他的挑戰，尤其是消費者的隱私權保護，這是一個備受矚目的重要議題。因此，我們認為第二個重要的研究方向為，探討使用者匿名性(anonymity)的問題，研發出一個具有使用者隱私權保護的多伺服器環境中的使用者身分認證方法。

在文獻探討中，我們發現 Liao 和

Wang[17]、Hsiang 和 Shih[3]以及 Wang 等人[29] 所提出來的方法有將匿名性的問題考慮進去。Liao 和 Wang[17]以及 Hsiang 和 Shih[3]是使用動態的身分識別碼取代掉固定的身分識別碼，來達到匿名性；而 Wang 等人[29]的方法則是使用二次剩餘將身分識別碼先加密後再傳輸，以達成匿名性。基於這二種方式的這三個方法雖然都宣稱可以達到匿名性以及隱私權的保護，但，所提供的保護層次及效果是不一樣的。以二次剩餘將身分識別碼先加密後再傳輸的方式，可以確保資料傳輸過程的使用者匿名性，但是無法對伺服器端隱匿使用者的真實身分。而以動態的身分識別碼取代掉固定的身分識別碼的方式，不僅可以確保資料傳輸過程的使用者匿名性，也可以對伺服器端隱匿使用者的真實身分。這兩種方式並無絕對的孰優孰劣，僅是適用於不同之應用環境的差異。

匿名性(Anonymity)，意指隱藏個人的真實身分不讓外界得知。進一步以匿名的程度可將匿名性分成二類：一、訊息傳送者和接收者的匿名性，二：訊息與傳遞者關係的匿名性。雖然，使用者的隱私權需要受到保護，但也不可無限擴張，在某些應用環境下，使用者亦須承擔一定程度的責任，因此，是否可以提供可事後追蹤的匿名性，亦是一個值得探討的問題。

綜觀上述的分析、探討，我們歸納出一個具有使用者隱私權保護的多伺服器環境中的使用者身分認證方法必須滿足 3.1 節所指出的幾點要求外，並須針對使用者隱私權加以適當的保護。

3.3. 可證明安全性的多伺服器環境中的使用者身分認證方法

在前面章節的分析中，我們可以發現，目前的多伺服器環境中的使用者身分認證方法或多或少存在一些安全性方面的弱點，這些方法之所以存在安全性弱點，最主要的原因為，這些方法大都以傳統的安全性分析的方式來探討其安全性，這種分析方式顯然無法令人信服。因此，一些較正規的安全性證明方式，例如 the random oracle model 或 the standard model，是必須導入到多伺服器環境中的使用者身分認證協議。然而，由於多伺服器環境較為複雜，如何將這些正規的安全性證明方式適當地套用於此一環境中，需要再進一步的加以研究。所以，我們認為可證明安全性的多伺服器環境中的使用者身分認證方法，亦是一個未來值得探討的重要議題。

4. 結論

在這篇文章中，我們探討了多伺服器環境中的使用者身分認證協議直至目前的研究成果，並針對這些已經被提出來的

方法就效率、安全性以及功能性等各面向進行深入的分析比較，經由這些分析比較，我們指出各個方法的優缺點，並進而擘劃出幾個未來值得進一步探討、研究的方向：安全性、效率以及使用者隱私權保護。藉由這幾個研究方向的實踐，將帶來如下優點：

- 對現行分散式多伺服器網路環境的安全性做一相當程度的改善。
- 安全的完成使用者身分認證，防堵所有可能的安全性威脅，保障合法使用者的權益。
- 有效率的完成使用者身分認證，降低系統硬體需求門檻以及等候時間。
- 適度的保護使用者隱私權，充分保障使用者與伺服器彼此之間的權利與義務。
- 在多伺服器環境中提供一個安全且令人安心的使用者身分認證機制，促進電子商務交易安全以及消費者隱私，提高電子商務服務之品質。

如此，將可以提升系統的可信賴度，降低使用者及服務供應端的疑慮，提供一個安全且令人安心的使用者身分認證的機制，也勢必可以將多伺服器環境中的使用者身分認證研究領域提昇至一個更臻成熟、符合實際應用需求的境界，並進而促進數位產業的永續蓬勃發展。

References

[1] C. C. Chang and J. Y. Kuo. An efficient multi-server password authenticated key agreement scheme using smart cards with access control. In *19th IEEE Int. Conf. Advanced Information Networking and Applications (AINA2005)*, volume 2, pages 257-260, Taipei, Taiwan, March 2005. IEEE Computer Society.

[2] H. Y. Chien, J. K. Jan, and Y. M. Tseng. An efficient and practical solution to remote authentication: Smart card. Computers and Security, 21(4):372-375, 2002.

[3] H. C. Hsiang and W. K. Shih. Improvement of the secure dynamic ID based remote user authentication scheme for multi-server environment. Computer Standards and Interfaces, 31(6):1118-1123, 2009.

[4] M. S. Hwang and L. H. Li. A new remote user authentication scheme using smart cards. IEEE Transactions on Consumer Electronics, 46(1): 28-30, 2000.

[5] R. J. HWANG and S. H. SHIAU. Provably efficient authenticated key agreement protocol for multi-servers. The Computer Journal, 50(5): 602-615, 2007.

[6] W. S. Juang. Efficient multi-server password authenticated key agreement using smart cards. IEEE Transactions

on Consumer Electronics, 50(1): 251-255, November 2004.

[7] H. S. Kim, S. W. Lee, and K. Y. Yoo. ID-based password authentication scheme using smart cards and fingerprints. ACM SIGOPS Operating Systems Review, 37(4):32-41, Oct. 2003.

[8] S. Kim, S. Lim, and D. Won. Cryptanalysis of flexible remote password authentication scheme of ICN01. Electronics Letters, 38(24): 1519-1520, 2002.

[9] W. C. Ku. Weaknesses and drawbacks of a password authentication scheme using neural networks for multi-server architecture. IEEE Transactions on Neural Networks, 16(4):1002-1005, 2005.

[10] W. C. Ku, S. T. Chang, and M. H. Chiang. Weaknesses of a remote user authentication scheme using smart cards for multi-server architecture. IEICE Transactions on Communications, E88-B(8):3451-3454, 2005.

[11] W. C. Ku, H. M. Chuang, and M. H. Chiang. Cryptanalysis of a multi-server password authenticated key agreement scheme using smart cards. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, E88-A(11): 3235-3238, November 2005.

[12] L. Lamport. Password authentication with insecure communication. Communications of ACM, 24:77-772, 1981.

[13] C. C. Lee, M. S. Hwang, and W. P. Yang. A flexible remote user authentication scheme using smart cards. ACM Operating Systems Review, 36(3):46-52, 2002.

[14] J. K. Lee, S. R. Ryu, and K. Y. Yoo. Fingerprint-based remote user authentication scheme using smart cards. Electronic Letters, 38(12):554- 555, 2002.

[15] W. B. Lee and C. C. Chang. User identification and key distribution maintaining anonymity for distributed computer network. Computer Systems Science and Engineering, 15(4): 211-214, November 2000.

[16] L. H. Li, I. C. Lin, and M. S. Hwang. A remote password authentication scheme for multi-server architecture using neural networks. IEEE Transactions on Neural Network, 12(6): 1498-504, November 2001.

[17] Y. P. Liao and S. S. Wang. A secure dynamic ID based remote user authentication scheme for multi-server environment. Computer Standards and Interfaces, 31(1): 24- 29, 2009.

[18] C. H. Lin and Y. Y. Lai. A flexible biometrics remote user authentication scheme. Computer Standards and Interfaces, 27(1):19-23, 2004.

[19] I. C. Lin. A neural network system for

authenticating remote users in multi-server architecture. International Journal of Communication Systems, 21:435-445, 2008.

[20] I. C. Lin, M. S. Hwang, and L. H. Li. A new remote user authentication scheme for multi-server architecture. Future Generation Computer System January, 19:13-22, 2003.

[21] Y. Liu, W. Gao, H. Yao, and X. Yu. Elliptic curve cryptography based wireless authentication protocol. International Journal of Network Security, 5(3):327-337, 2007.

[22] H. M. Sun. An efficient remote user authentication scheme using smart cards. IEEE Transactions on Consumer Electronics, 46(4): 958-961, 2000.

[23] C. S. Tsai, C. C. Lee, and M. S. Hwang. Password authentication schemes: Current status and key issues. International Journal of Network Security, 3(2):101-115, 2006.

[24] J. L. Tsai. Efficient multi-server authentication scheme based on one way hash function without verification table. Computers and security, 27:115-121, 2008.

[25] W. J. Tsaur. A flexible user authentication scheme for multi-server internet services. In Networking-ICN, volume 2093 of LNCS, pages 174-183. Springer-Verlag, 2001.

[26] W. J. Tsaur, C. C.Wu, and W. B. Lee. A smart card-based remote scheme for password authentication in multi-server internet services. Computer Standards and Interfaces, 27: 39-51, 2004.

[27] W. J. Tsaur, C. C. Wu, and W. B. Lee. An enhanced user authentication scheme for multi-server internet services. Applied Mathematics and Computation, 170:258-266, 2005.

[28] Y. M. Tseng, T. Y.Wu, and J. D.Wu. A pairing-based user authentication scheme for wireless clients with smart cards. INFORMATICA, 19(2): 285-302, 2008.

[29] R. C. Wang, W. S. Juang, and C.L. Lei. User authentication scheme with privacy preservation for multi-server environment. IEEE COMMUNICATIONS LETTERS, 13(2): 157-159, 2009.

[30] S. Wang, Z. Cao, and H. Bao. Efficient certificate-less authentication and key agreement (CL-AK) for grid computing. International Journal of Network Security, 7(3): 342-347, 2008.