基於比特幣加密演算法之跨平台物聯網系統裝置身份辨識服務

劉祐安　　賴槿峰
宜蘭大學資訊工程研究所
{ tn00414393, cinfon }@gmail.com

摘要

近年來物聯網(Internet of Things, IoT)技術在異質領域受到相當廣泛的應用，且隨著終端行動裝置的普及，使終端行動裝置不僅具備聯絡功能，其連網與應用程式所提供的服務項目漸漸成為現代人的生活核心，終端行動裝置與物聯網相輔相成的關係將成為未來產業的趨勢。未來使用者透過終端行動裝置在物聯網架構下使用服務時，對於人對人、人對物、物對物之間的身份辨識與資訊傳遞安全性是物聯網首當其衝的問題，為了防止個人資訊被竊取，需要一套安全性高的安全機制，比特幣(BitCoin)的加密機制非常適合運用在此。因為比特幣本來就是一種對等、安全與匿名的電子貨幣系統，其幣值穩定程度不下黃金，這得歸功於比特幣完善的貨幣體制。本研究則率先提出於物聯網資訊安全部分結合比特幣之加密機制且運用於 Web 服務、物聯網與感測裝置等技術，提供一套跨平台且具高安全性的物聯網裝置身份辨識與資訊傳輸機制。

關鍵詞：比特幣、物聯網、裝置身份辨識

Abstract

In recent years, IoT technology in the field by a wide range of applications, and the popularity of mobile devices with the terminal, the terminal mobile devices not only have the liaison function, their networking and application services provided gradually become the core of modern life, things end mobile devices and complementary relationship will become future industry trends. Future users of the mobile device via terminal architectures used in networking services for people to people, people to things, thing to things, However the identity between objects in device of identification and pass information security is a problem bear the brunt of things, in order to prevent personal information from being theft, need a safe security mechanisms, Bitcoin encryption mechanism is very suitable for use in this. Because Bitcoin is an inherently peer, secure and anonymous electronic money system, no less than the degree of its currency stable gold, thanks to a sound monetary system Bitcoin. This study is the first to put forward in information security a part of the Bitcoin encryption mechanism used in IoT, with networking and sensing devices and other technologies using Web Service to provide a cross-platform to achieve highly secure networking device Identification & Information transport mechanism

KeyWord：BitCoin, IoT, Device of identification

1. 前言

物聯網(The Internet of Things, IoT)是近年來熱門的研究主題與技術運用，其對於運輸物流、智能環境（家庭、辦公、工廠）與溫室環境等環境上建樹良多，當使用者透過網際網路使用裝置與各種智能物件時，如果某些使用者的個資具備特殊的價值，會吸引駭客利用，如黑洞攻擊(black hole attacks)或者 灰洞攻擊(gray hole attacks)等攻擊手法進行資料竊取，因此如何提高資料傳遞的安全性與隱私性是首當其衝的議題，則裝置身份辨識的資訊安全機制是必要的元素。傳統物聯網會將資料集中儲存在中介層伺服器中進行管理，雖然集中式管理上所需花費的成本相對較低，但攻擊目標明確，若發生駭客攻擊等事件時，資料則完整的曝露出來，因此資料安全性上頗為堪慮。

本研究參考比特幣為基礎之加密演算法，在P2P 的傳輸環境下，針對資料與關鍵值(Key)進行加密，產生加密資料與關鍵值，並透過中介系統伺服(WebService)傳輸加密後的加密資料、關鍵值與公開金鑰(Public Key)，中介系統伺服器本身只提供跨平台資料轉換與傳輸資料之服務並不儲存任何資訊，最後透過公開金鑰與私密金鑰(Private Key)間的加解密運算進行身份確認並取得原始資料。

2. 相關背景

2.1 物聯網系統架構

物聯網透過物件與物件之間資訊交流達到裝置即時監控運用，目前物聯網架構分為三部分如圖1，最上層為應用層，即使用者與物聯網的橋接口，它連接各種物聯網環境所需之應用功能，具備著友善的操作介面與遠端擷取和操控感知控制裝置之系統功能並在此層實現與影響。此外應用層之關鍵問題在於使用者與各種感知控制裝置的資訊傳遞上的安全性與個人身份辨識。其次是中介層內包含中介系統與其服務，在物聯網架構下，中介層之伺服器會儲存許多使用者資訊並集中管理，因此一旦出現資安漏洞損失將難以估計。本研究中介層利用有線和無線網路傳遞應用層與感知控制層之間彼此所需的即時加密資訊，並經由跨平台整合服務來完成不同作業系統間的資料傳遞工作。最底層為感知控制層，其透過感知裝置(Sensor)蒐集資訊與控制裝置(Controller)控制裝置[1][2]。以下三點為物聯網技術之特徵：

- 使用者在任何具備有線、無線網路環境下皆可使用。
- 終端裝置連上中介系統進行身份辨識。
- 物聯網架構具高擴展性可應用於不同環境。

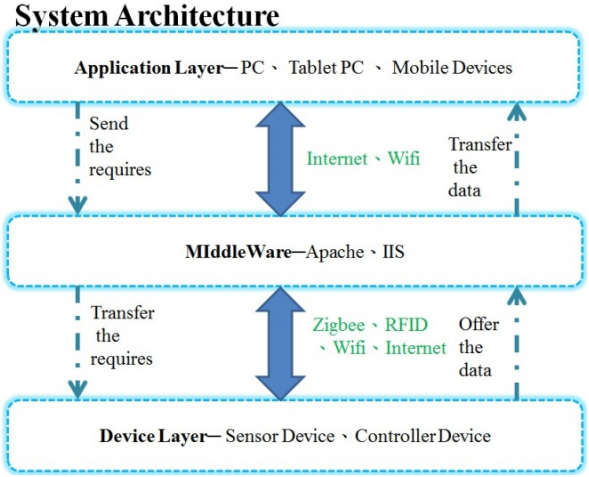

圖 1 物聯網架構圖

2.2 比特幣加密演算法

物聯網技術的蓬勃發展所面臨的考驗將層出不窮，其中身份辨識的重要性與日俱增，傳統裝置身份辨識的作法是使用全域唯一識別碼(Globally Unique Identifier，GUID)產生裝置之唯一值，GUID(public key + hash(s))，其中 s 是一種由連接對象的所有者所提供可選擇數值，它可以是一個唯一的值，例如一個序列號、MAC 地址或內容 URI 等。該 GUID 可以是固定的，只要公開金鑰(public key)是獨一無二的。所有者可以使用公開金鑰連接多個網路對象，差別則是 hash 處理的值[3]。

本研究中將GUID內hash(s)替換成比特幣之演算法來進行終端裝置存取雲端資源，以個人身份辨識各物件，比特幣是由日本數學家中本聰所提出的一套電子貨幣，其完整的安全機制有效防止駭客藉由竄改資料而影響貨幣之市場機制。

比特幣演算加密方式有提到兩種，主要是使用安全雜湊演算法(Secure Hash Algorithm)中的SHA-256 雜湊法，SHA-256 雜湊法是當作固定大小的唯一直來使用，代表資料警在與其對應的資料相符時，兩組資料的雜湊才會相符，資料的些微變更會造成雜湊中無法預期的巨大變更。SHA-256 演算法的雜湊大小事 256 位元，比特幣在加密過程中非為兩個階段：資料加密與關鍵值加密[4]。

2.2.1 第一階段：資料(data)加密

主要是透過 SHA-256 將資料加密之後再將加密後的雜湊值用 SHA-256 進行再次加密，如圖 2 所示，函數如下：

SHA-256(SHA-256(data))

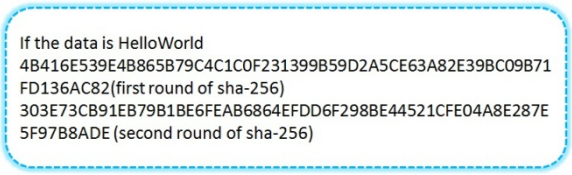

圖 2 資料(data)加密以 HelloWorld 為例

2.2.2 第二階段：關鍵值(key)加密

主要是透過 SHA-256 將關鍵值加密，再將加密後的雜湊值用 RIPEMD-160 再次加密，RIPEMD-160 是一種 160 位元的密碼編譯湊函式。它是用來取代 128 位元的雜湊函式 MD4、MD5 和 RIPEMD。RIPEMD 是依 EU 專案 RIPE(RACE Integrity Primitives Evaluation, 1988-1992)的架構所開發。關鍵值(key)加密如圖 3，函數為：

RIPEMD-160(SHA-256(key))

If the key value is HelloWorld
4B416E539E4B865B79C4C1C0F231399B59D2A5CE63A82E39BC09B71
FD136AC82 (first round is sha-256)
29E7D928F43AFFA082B395135D1B3C713BD876AB(with ripemd-160)

圖 3 關鍵值(key)加密以 HelloWorld 為例

3. 系統架構及功能

本研究於資料傳輸上不同於傳統物聯網在中介層之中的資料庫儲存資料，以避免出現資安漏洞後造成無法預期的龐大損失，取而代之的是一套可提供跨平台的系統，其功能是作為應用層與感知控制層之間不同系統的跨平台處理，WebService 技術則在本研究中充分的發揮其跨平台的特性，由於 WebService 所運用 SOAP 通信協議，並以 XML 的標準格式封裝其功能，因此在不同環境下只需取得 WebService 服務來源、SOAPAction 與方法(Method)名稱與其參數即可使用該服務並進行應用[5][6]。

本研究有鑑於比特幣被列為最難被攻破的安全加密機制特性，於物聯網中率先導入比特幣加密演算法強化物聯網資訊安全機制，並在 P2P 的傳輸環境下將所要傳輸內容分類為要求、資料、公開金鑰與關鍵值，其中要求與資訊部分都會額外加上時間用以限定金鑰的有效時限並根據模擬測試的結果針對資料的回應時間加以設定，以下四項為傳輸內容分類詳細說明：[7]

- 要求：應用層欲進行控制與得知裝置訊息所傳輸至感知控制層所執行的行為包含控制指令與感知資訊的索取訊息。
- 資料：感知控制層接受應用層要求後所提供給應用層的資料組合，例如：溫溼度訊息與冷氣啟動與否的狀態等。
- 公開金鑰：用以將加密資料進行解密的密碼組合，例如：應用層公開金鑰須用感知控制層私密金鑰進行解密反之亦然。
- 關鍵值：用以加快設備搜尋的數值，經由設備間的分散式雜湊表(Distributed Hash Table, DHT)來查詢要求尋找的設備所在位置。

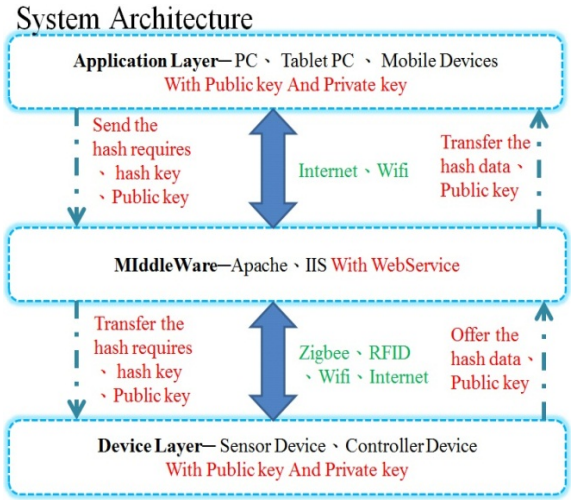

圖 4 導入比特幣加密演算法後的物聯網架構

依據物聯網原有架構區分為三個層級，依序是應用層、中介層與感知控制層，本研究在應用層除了原有的功能外還加入了公開金鑰與私密金鑰的加密與解密運算與根據回應需時的設定來進行金鑰時效判斷等功能，透過上述功能來驗證資訊與其來源是否正確，中介層在本研究中則將其修改成不存在任何資料庫與不儲存任何資訊，並且藉由 WebService 服務的跨平台轉換能力成為應用層與感知控制層之間溝通必備的橋樑，感知控制層除了原有的感知控制功能外也具備金鑰的加解密與金鑰時效判斷等功能，並加入分散式雜湊表，藉此來驗證發送要求對象的身份與加強資料傳遞的安全性。導入比特幣加密演算法之後的物聯網架構如圖 4 所示。

透過導入導入比特幣加密演算法後的物聯網架構與所需資訊的設定本研究將其規劃成一個完善的系統流程如圖 5 所示，此流程主要是從應用層開始透過發送加密要求、關鍵值與公開金鑰至中介層，再藉由中介層 WebService 跨平台功能傳遞給感知控制層，感知控制層透過分散式雜湊表與關鍵值來查詢所要求的裝置，並通過公開金鑰與私密金鑰的解密來還原要求，並將應用層要求的資料加密在與公開金鑰一起回傳至中介層，最後中介層再透過其跨平台功能傳遞資料給應用層，應用層再透過金鑰的解密還原成所需的訊息。其中若資料傳輸的時間超過所需回應的時間則會發生例外錯誤則需重新產生金鑰並且重新發送要求。本研究則透過這些設定來防止入侵竊取資料的情況發生。

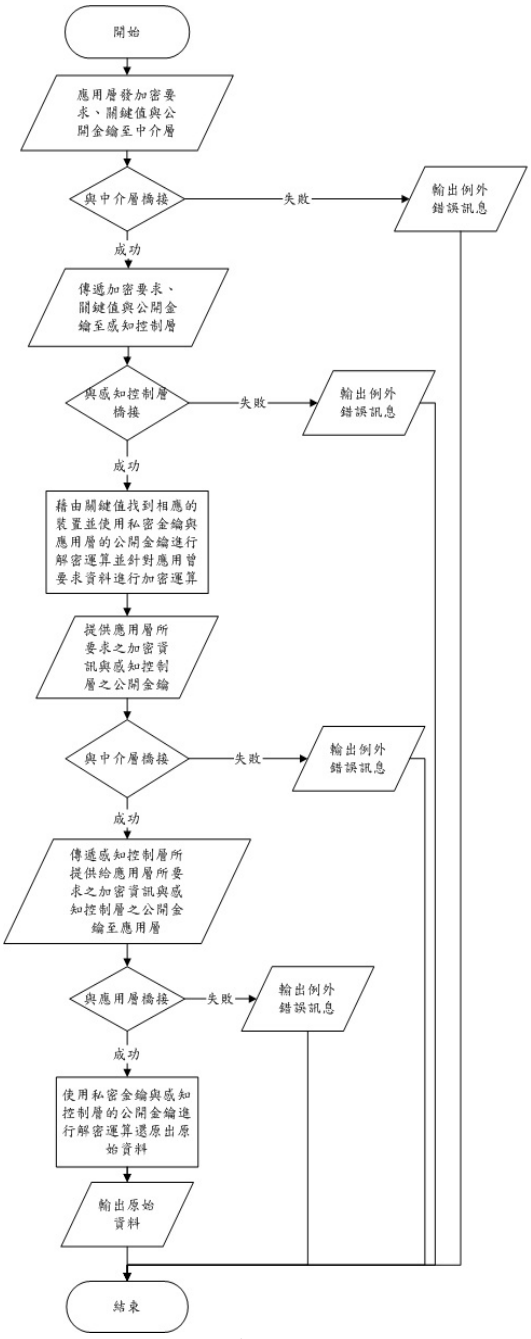

圖 5 系統流程圖

4. 實驗結果與討論

本研究透過 WebService 提供出四種傳輸資訊方法分別為 getdata 與 getdata_MS 用以取得感知裝置的資料、updateSQL 與 updateSQL_MS 用以傳遞控制裝置的控制資料，藉由上述方法提供跨平台服務，服務來源如下圖 6 所示。

透過 Android、Web、表單程式中的 WebService 函式方法來對本研究之 WebService 服務進行運用，

圖 6 WebService 方法

此外將資料的傳輸分為三種不同的形態同時進行，第一種是一般物聯網架構下無加密的型態，第二種是一般物聯網架構下的加密型態，第三種則是本研究導入比特幣加密演算法之型態，並且加入網路攻擊的模擬與應用層取值需時來進行實驗。

常見網路攻擊有擷取資料封包進行資料的竊取，其中黑洞攻擊(black hole attacks)與灰洞攻擊(gray hole attacks)則是擷取資料封包攻擊中最著名的攻擊方式。

- 黑洞攻擊： 是由惡意節點利用假造的 RREP 封包宣稱自己擁有到目的地節點最短的路徑來回覆任何由來源節點所發出的 RREQ 封包，吸引來源節點優先以他為轉送節點，當資料封包傳送到惡意節點後便將所有資料封包丟棄，在網路上形成一個黑洞。
- 灰洞攻擊： 大致上如同黑洞攻擊，差別在於並不會把所有經過它的封包都丟棄，而是選擇性的丟棄封包[8][9]。

駭客攻擊的手法依照不同的行為分類為：主動式攻擊與被動式攻擊，主動式攻擊的模式是企圖改變系統資源，或影響系統運作；被動式攻擊的模式則會企圖竊取或使用來自系統但卻不至於影響系統的資訊，而兩者應對的方式也有所不同。對於主動式的攻擊手法，應該採取偵測方式，在面對攻擊之後要能夠復原其所造成的任何破壞，也因為偵測攻擊可形成嚇阻作用，因此偵測主動式攻擊能較有效預防。而在面對被動式攻擊時偵測上則較為困難，因為攻擊者並不會更改任何的資料，所以面對被動式

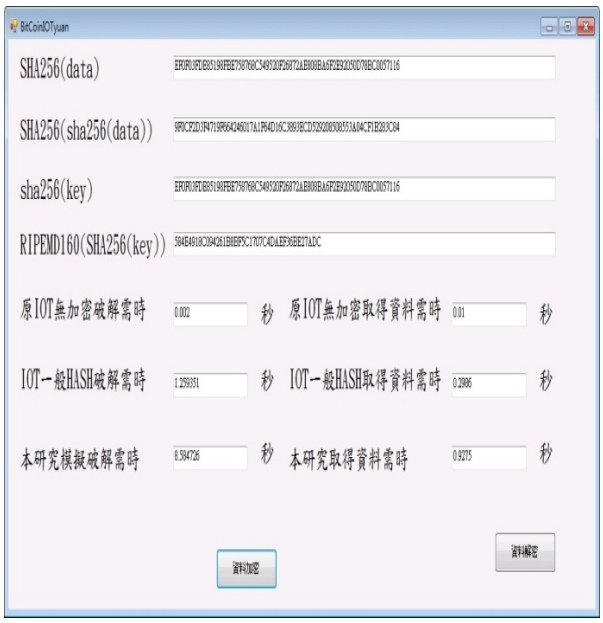

圖 7 本研究加解密與應用層取值需時模擬程式

攻擊時，處理的重點是預防攻擊而非偵測攻擊。而加密演算法在處理上是屬於預防攻擊的類型，且被動式攻擊手法中的灰洞攻擊在攻擊上較可以保持封包完整性而不作丟棄，故本研究在攻擊種類選擇灰洞攻擊作為比較傳統物聯網架構與導入比特幣加密演算法後的物聯網架構下，遭受攻擊後的差異性。針對灰洞攻擊模擬之實驗程式為圖 7 所示。

為了方便研究的實驗展示，本研究於實驗程式加入資料加密按鈕用以取得現在加密的資料並將其顯示，資料解密按鈕則可針對三種型態進行模擬灰洞攻擊模擬與應用層取值需時實驗。由於密碼強度決定加密資料破解時間的長短，而應用層取得資料的時間若比資料被破解時間還要迅速則可使被竊取的資料有效程度降低甚至無效化，若破解時間小於等於應用層取得資料的時間，則被竊取的可能性比破解資料的時間需大於應用層取得資料的時間的可能性還要高出許多，故本研究的目的在於提高破解資料的需要用時或提升破解時間與應用層取得資料時間的比率。

由圖 8 可以得知本研究的破解需時較另兩種型態高，因為無加密狀態下被竊取則駭客即可得知資料內容，一般加密的加密強度則比本研究的加密強度還要遜色一些，故此圖則呈現出本研究加密機制破解所花費的時間較高，說明了駭客竊取上的難度也較高。

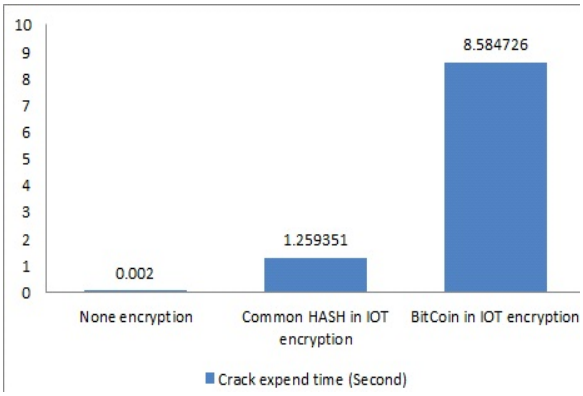

圖 8 破解需時比較

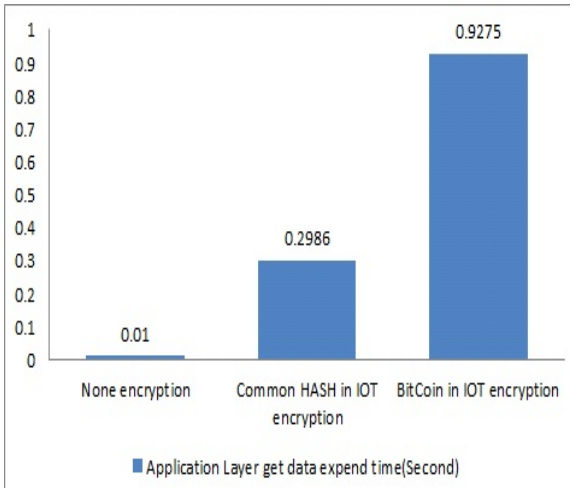

圖 9 應用層取得資料時間比較

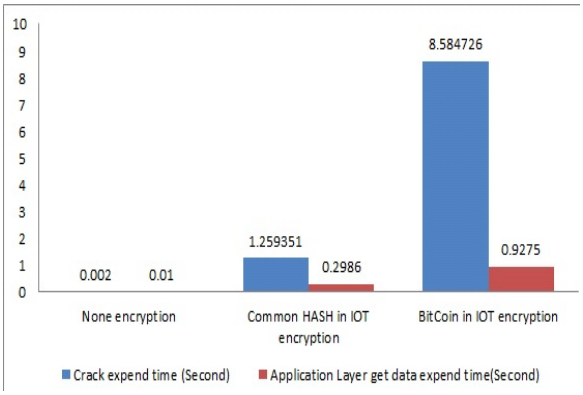

圖 10 破解需時與應用層取得資料時間比較圖

本研究的資料取得時間雖較另兩種型態高，主要是無加密的情況無須經過解密運算而一般加密的情況則因為加密與運算的複雜度較本研究低而導致本研究花費時間較高的結果，如圖 9。

圖 10 顯示出無加密一旦被竊取，則系統無任何反應時間進行處理問題，而一般加密下雖有反應時間，但僅有不到一秒的情況其反應時間相當有限，而本研究導入比特幣加密演算法的物聯網系統，在面對攻擊時可以反應的時間較為寬裕，面對資料已被竊取等特殊狀況則有較高的緩衝時間可以運用，就算駭客真的竊取到資料也只是一堆過期且無效的資料，所以無法進行有效應用。

5. 未來展望

未來當 IOT 的運用不斷擴張，針對回應所需之最佳時間部分將會依照不同的節點長度而有所不同，在此部份則可加入資料探勘分散式分群法中的 k-means 演算法來完成回應需時的自我學習功能，以針對不同的環境使用其最佳化回應需時來判斷重新建立連線時間、資料時效性與公開金鑰與私密金鑰定時變更時間。

另外針對一些記憶體修改工具能針對記憶體位置中的資訊進行變更的竄改，如 CheatEngine[10]，最常見的攻擊模式類似 Facebook 網頁服務或遊戲中，駭客可以輕易地利用此程式來竄改服務或是遊戲寶物等有價值的內容，由於是更改記憶體區塊，任何加密機制能無法有效防範，而這則是另一種未來所需面對的一項重大考驗。

6. 參考文獻

[1] 王威程, 賴槿峰,"智慧聯網之中介系統負載平衡研究" ,*TANET2012*,2012

[2] S.De, F.Carrez, E.Reetz, R.Tönjes, W.Wang, "Test-Enabled Architecture for IoT Service Creation and Provisioning", *The Future Internet Lecture Notes in Computer Science*, Vol.7858, pp233-245, 2013

[3] J. Li, Y. Shvartzshnaider, J.A. Francisco, R.P. Martin, K. Nagaraj and D. Raychaudhuri, "Delivering Internet-of-Things Services in MobilityFirst Future Internet Architecture", *Proceedings of the International Conference Internet of Things (IOT)*, pp31-38, 2012.

[4] I.Miers, C.Garman, M.Green, A.D. Rubin, "Zerocoin：Anonymous Distributed E-Cash from Bitcoin", *IEEE Symposium on Security and Privacy*,pp397-415, 2013

[5] K.Li ,L.Jiang,"The Research of Web Services Composition based on Context in Internet of Things", Computer Science and Automation Engineering (CSAE), *IEEE International Conference on*, pp160-163,2013

[6] S.Li, X.Qiao, X.Li, "Study on the Architecture of Platform for Internet of Things Service Based on EDSOA" , Computer and Information Technology (CIT), *IEEE 12th International Conference on*, pp953 – 959, 2012

[7] F.Reid, M.Harrigan , "An Analysis of Anonymity in the Bitcoin System", *Security and Privacy in Social Networks*, pp197-223, 2013

[8] 鄒博鈞,張建明,林義軒,趙涵捷,陳俊良,"發展一個在 MANET 下基於混合式主被動防禦架構避免黑洞攻擊之 BDSR 策略",*TANET2010*, 2010

[9] G.Usha, Dr.S.Bose, "Impact of Gray Hole Attack on Adhoc networks ", Information Communication and Embedded Systems (ICICES), *International Conference on*,pp404-409, 2013

[10] Cheat Engine Developers. Cheat Engine. http://cheatengine.org