



Secure Enhanced User Authentication Protocol for Cloud Computing Environment

Mona Samir Lackousha, Nabil Hamdy Shaker, and Hisham Dahshan

Abstract: Cloud computing provides innumerable benefits to its customers but failing to solve information security concerns. Cloud customers and providers need to guard against data loss and theft. Encryption of personal and enterprise data is strongly recommended. Strong encryption with key management is one of the core mechanisms that Cloud Computing systems should use to protect data, so key management is an important technology that can help secure applications and data in the cloud. In this paper, a formal analysis of a user authentication protocol for cloud computing is presented. Analysis show that the protocol is vulnerable to replay and Man-in-the middle attacks. To overcome these attacks, a modified authentication protocol for the cloud computing environment is proposed.

Keywords—Cloud computing, authentication, encryption, Cryptographic Key Management (CKM), Elliptic Curve Cryptosystem (ECC).

INTRODUCTION

Cloud computing is a type of Internet-based computing, and it is one of the foundations of the next generation of computing. As shown in figure1, a simple definition of cloud may state that “Cloud Computing is a model for enabling ubiquitous, convenient, on-demand network access to shared pool of configurable computing resources (network, server, storage, application and services) that can rapidly provisioned and released with minimum management effort or service provider interaction.” Cloud computing provides several benefits to its consumer such as availability, flexible cost model, on demand self-services, elastic resources, etc. It facilitates their consumers by providing software, platform and infrastructure as service. Consumers can easily use these services any time everywhere through internet [1, 2].

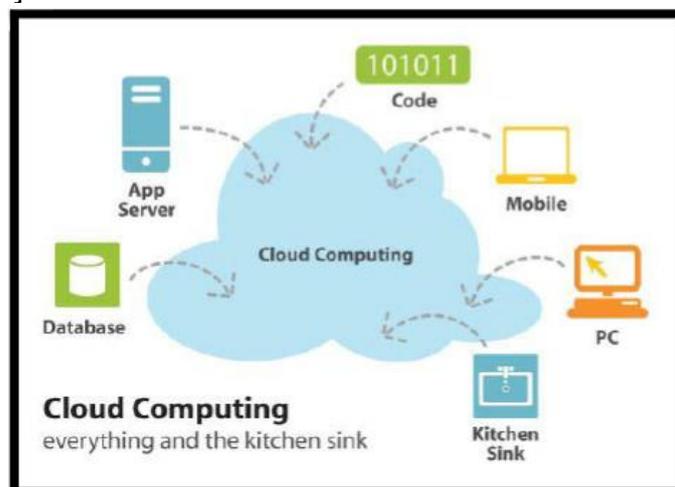


Figure 1: Cloud computing

The cloud computing can either be hosted on-site by the company or off site such as Microsoft's SkyDrive, Google Drive, Samsung's S Cloud service, Apple's iCloud, and Amazon's Cloud Drive. Recent applications, e.g., multimedia streaming, virtual reality, and robotics [3-5], have used cloud computing to provide the services. Also, platforms like Google Apps (e.g., Gmail, Google Groups, Google Calendar ...), YouTube, Vimeo, Flickr, Slideshare and Skype adopt the cloud computing technology.

For providing cloud services, the sensitive data for all clients should be stored in the cloud host. At this time, the data security and the personal privacy should be assured. The cloud provider should guarantee these data and personal information in host database against all accesses of the unauthorized insiders or the malicious outsiders.

Traditional information security mechanism such as cryptography, digital signature, access control mechanism, and trust management are not sufficient to fulfill the need of information security on cloud paradigm. It also provides suggestion on critical area of cloud computing. Cryptographic key management at cloud computing is a challenge and cryptographic keys should be stored on enterprise domain due to their security. However, searching of encrypted data from a large data set is problematic if cryptographic keys are stored at enterprise premises. Furthermore, cryptographic key management is required at cloud when any application process requires working on plain text at cloud platform and data must access cryptographic key. Cryptographic key management includes all operation that can be performed on cryptographic key except encryption/decryption. These operations comprise but are not limited to generation, revocation, sharing and storage of cryptographic keys.

Extensive research in cloud security includes several techniques for information security based on two main aspects which are strong algorithms and cryptographic key management. Some issues in cloud computing security are surveyed [6-9] as follows:

Re-Encryption based key management scheme is presented in [6]. This scheme permits access to a common data partition in the cloud among multiple users, ensures confidential data storage even to the cloud provider, and offers greater data access efficiency in a mobile-based cloud system at lower overall communication and processing cost than traditional centralized solutions; all of these features are accomplished through the process of data re-encryption.

In this scheme, single authority of control such as manager can be a bottleneck in the design of the scheme.

Symmetric CKM protocol for cloud based environment scheme is presented in [7]. This protocol manages access control by giving access to authorized data owner. Privacy of data is maintained by distributing key on different drives therefore, un-authorized user cannot retrieve the key completely. The protocol has ability to recover its original cryptographic key in case of misplacing a single component. This technique assumes that cloud services will always be available. Thus, data insertion and fetching will not suffer from the availability of resources but this cannot be always achieved. If consumer's part of the original key is missed, the original cryptographic key cannot be regenerated again.

Yang and Chang's authentication protocol is presented in [8]. Yang and Chang proposed an Elliptic Curve Cryptosystem (ECC) based authentication protocol for remote devices. Yang and Change found that other schemes need a large storage space to keep all user's public keys and certificates, which is inefficient, and proposed an ID-based remote mutual authentication with key agreement scheme for remote devices on ECC. Yang and Chang's scheme performs authentication without password-protection, which results in the risks of insider attack and impersonation attack.

Data Privacy by Authentication and Secret Sharing (PASS) is presented in [9]. This scheme is proposed to protect client's data privacy from cloud employees using authentication and secret sharing.

This scheme is intended to reduce the data privacy risk to a minimum. The PASS adopts public key cryptosystem to encrypt its share, and this increases the transmission cost. PASS chooses not to store the secret key (shared between the client and the cloud server) anywhere in the cloud because of the secret isolation guideline. However, the client needs to store the secret key because the cloud server does not send its share to the client. So, if the client's device is compromised (for example the local computer or the smart card is cracked) then the secret key will leak out.

In this paper, a formal analysis of Amlan et. al. user authentication protocol for cloud computing [15] is presented. Analysis show that the protocol is vulnerable to replay and Man-in-the-middle attacks. To overcome these attacks, a new authentication protocol for the cloud computing environment is proposed. The rest of the paper is organized as follows:

In Section II, a description of Amlan et. al. protocol is presented. In Section III, our proposed authentication protocol is presented. Security and performance analysis of the proposed protocol is presented in Section IV. Finally, Section V concludes the paper.

USER AUTHENTICATION PROTOCOL

In this section, a description of Amnal et. al. Strong User Authentication Framework for Cloud Computing [15] is presented. This protocol has two major advantages as follows:

- 1) The scheme possesses an extra OOB (out of band) factor (other than only two factors) which undoubtedly provides better security over two factor authentication.
- 2) Two separate communication channels, making it very difficult for the adversaries to attack in two different channels. The schematic security architecture of the proposed protocol is shown in Figure 2.

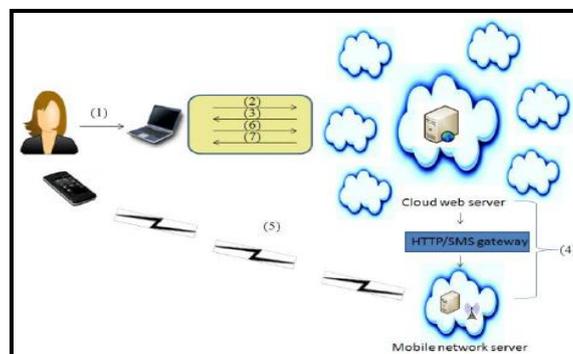


Figure 2: Architecture of the scheme

As shown in the Figure 2, the basic idea of the scheme is as follows.

1. The user inserts the smart card in the terminal and enter user ID and Password (PW). The local system verifies the authenticity of the user based on smart card, ID and PW.
2. Once the local verification is over, the user sends login request to the cloud server.
3. Upon receiving the login request, the cloud server sends some authentication data based on the specific user.
4. The cloud server sends the one time key to the mobile network through HTTP/SMS gateway [13].
5. The mobile network (M) delivers the onetime key to the user via SMS.

The scheme consists of three phases; registration phase, login phase, and authentication phase and one activity, which is called password change.

Registration phase

In the registration phase, user needs to register at the server by providing appropriate identification details. The server process user's data and issue a smartcard to the user.

Login Phase

This phase is invoked when user wants to login into the cloud. Users are verified before access to the cloud. The procedure is described as follows:

1. User (A) inserts the smartcard and enters user identity and user's password.
2. User (A) sends login request message, M_1 to the server (S) over the public channel. Here, $A \rightarrow S: M_1$, is login request message.
3. Server (S) sends M_2 to user (A) using public channel, $S \rightarrow A: M_2$. Also, server (S) sends user (A), onetime key (K) using secure OOB channel to user's mobile phone, $S \Rightarrow A: K$.
4. When user (A) receives message M_2 , he computes and checks some conditions. If all conditions are true, then proceeds to the next step, otherwise terminates the login session. In this step user authenticates the server.
5. User (A) sends message M_3 to the server (S) over the public channel, $A \rightarrow S: M_3$.

C. Authentication Phase

Authentication phase is processed in the server where, the server decides whether user (A) should be allowed to login or not. The authentication phase process is as follows:

1. Server (S) computes and checks some conditions. If all conditions are true, then proceeds to the next step. Otherwise, terminates the login session. In this step server authenticates user.
2. The server generates session key S_K .
3. The message M_4 is sent to the user over public channel. The message contains the hash of a session key, $S \rightarrow A: M_4$. The session key S_K is needed for final authentication for the user which is valid for some constant definite time.

D. Password Change

Password change is a user friendly facility, which is a very important requirement in user authentication schemes. It allows users to change their password anytime whenever user wishes to change their password.

Amlan et.al. protocol [15] is vulnerable to replay, DOS, and Man-in-the-Middle attacks. For example, a fake mobile network server may pretend as a legitimate mobile network server which is not possible for cloud server to recognize and a fake cloud server may pretend as a legitimate cloud server which is not possible for mobile network server to recognize. Every time a message is sent, it is effectively given to the attack. In this case, the attack will redirect the sent messages from cloud server to mobile network server and also redirect the sent messages from mobile network server to cloud server. Therefore cloud server must authenticate itself.

The proposed authentication protocol

In this section, a description of security and privacy enhancements in Amlan et.al. user authentication protocol for cloud computing [15] is presented. It consists of 5 steps as shown in Figure 3 as follows:

1. Problem Formalization and Analysis
2. Protocol Design
3. Protocol Verification
4. Implementation
5. Evaluation

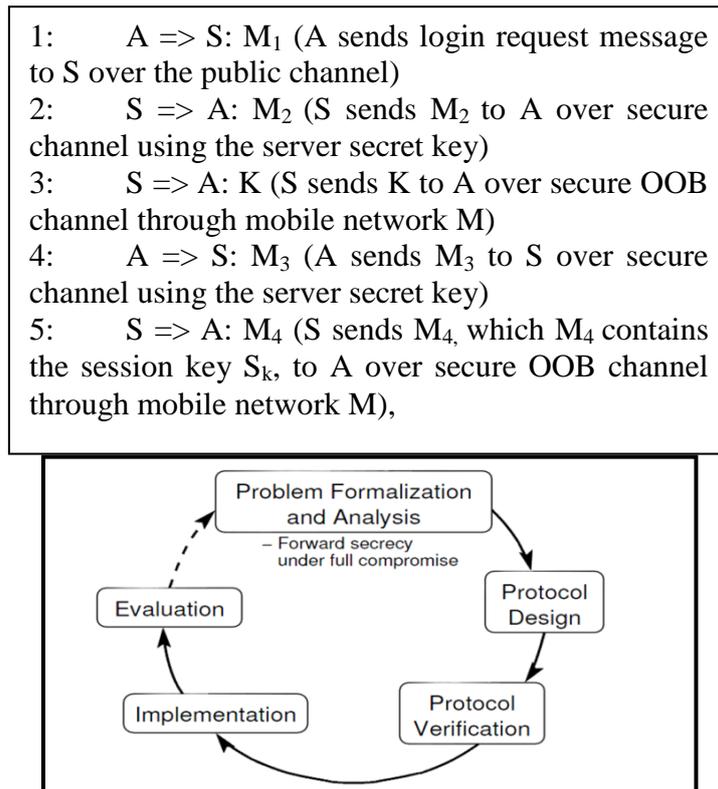


Figure 3: Steps for protocol analysis, Verification, Implementation and Evaluation

Problem Formalization and Analysis

As discussed in Section II, Amlan et.al. protocol [15] is vulnerable to replay, DOS, and Man-in-the-Middle attacks when analyzed using Scyther tool [16, 17, 18]. Some solutions are introduced to solve those attacks in our design. To prevent both Man-in-the-Middle attack and replay attack, all sent messages in the network are encrypted using the server secret key where the session key (S_k) is sent to the mobile network then the mobile network will send it to the user

B. Protocol Design

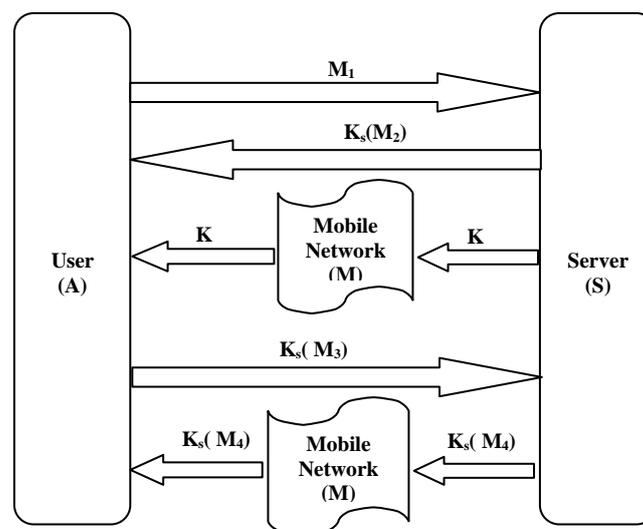


Figure 4: Diagram Of the proposed protocol

Our proposed authentication protocol improves authentication framework for Cloud Computing by increasing the authentication strength between server (S) and user (A) using

server secret key (K_s) during the exchange of the messages between S ,and A. The authentication mobile network (M) appears as a trusted third party to enhance the security and efficiency of the network. A simplified block diagram of our proposed protocol is shown in Figure 4. Messages exchanged between server S and user A of the proposed protocol can be summarized as follows:

c. Protocol Verification

In this section, a formal verification of Amlan et.al. protocol [15] is presented. The formal verification has been made using the scyther tool [16, 17]. Scyther tool was developed by Cas Cremers in 2007 [18]. Scyther, is a formal protocol analysis tool, for the symbolic automatic analysis of the security properties of cryptographic protocols (typically confidentiality or variants of authenticity). It assumes perfect cryptography, which means that an attacker gains no information from an encrypted message unless he knows the decryption key. Scyther takes as input a role-based description of a protocol in which the intended security properties are specified using claims. Claims are of the form claim (Principal, Claim, Parameter), where Principal is the user's name, Claim is a security property (such as 'secret'), and Parameter is the term for which the security property is checked. The description of a protocol is written in SPDL (Security Protocol Description Language) language. For the protocol verification, Scyther can be used in three ways:

- *Verification claim*: Scyther verifies or falsifiers security properties.
- *Automatic claims*: if user does not specify security properties as claim event, Scyther automatically generates claims and verifies them.
- *Characterization*: each protocol role can be characterized. Scyther analyzes the protocol and provides a finite representation of all traces that contain an execution of the protocol role. Scyther generates attack graph. This graph presents a way or another where an attack can intrude the system.

Ensuring cloud computing environment protection means that we should satisfy the following four properties to protect cloud computing against different attacks:

Property 1- Confidentiality

This claim is fulfilled if the server (S) has the guarantee that all exchanged user data (A) is secret. The exchanged user data messages between the user A and the server S is called Msg. Each information (α) in Msg should remain secret [16, 17, and 18]. The formalization of information confidentiality is given below

$$\forall \alpha \in \text{Msg} (\text{claim}(S, \text{Secret}, \alpha)) \quad (1)$$

Property 2- Integrity

This claim is fulfilled if the user A, server S, and the mobile server M have the guarantee that all exchanged keys (described as key) are secret and unique. We have included an additional restriction that only claims concerning sessions between trusted agents are evaluated. Its formal definition is shown as follows [16, 17, and 18]:

$$\forall \text{key} (\text{claim}(S/A/M, \text{Secret}, \text{key})) \quad (2)$$

Property 3- Access control

A cloud computing should have a correct mechanism to verify that a given user is authorized to use a particular service. A service should always be bound to an authenticated user. Its formal definition is given as follows [16, 17, and 18]:

$$\forall \alpha \in \text{Msg} (\text{claim}(S, \text{Secret}, \alpha)) \quad (3)$$

Property 4- Freshly of messages

An important part of security protocols is the generation of fresh values which are used for challenge-response mechanisms (often called nonces), or as session keys. This claim is fulfilled if the server S, user A and mobile server M have the guarantee that the session key is fresh [16, 17, and 18]:

$$(\text{claim}(S/A/M, \text{Fresh}, \text{key})) \quad (4)$$

Analysis of the proposed design

This model is going to be challenged with the following requirements using the Scyther tool.

1. Property 1: In the formal analysis it is proven that an intruder cannot obtain the data exchange between the server S and user A.
2. Property 2: In the formal analysis it is proven that the authorization key exchanged in the authentication protocol is secret
3. Property 3: It is proven that unauthenticated user cannot access the services provided, and cannot impersonate another user. Also, it is not possible to modify the data by an unauthorized individual.

d. New Protocol Implementation

The steps to implement the new protocol are as follows:

1. Use scyther tool to discover the attacks to the used protocol and the result as shown in figure 5.

We found that there are attacks on the secrecy of (K,R,BB,B,C) which discovered by the following claims:

- claim_s1(A,Secret,K);
- claim_s2(A,Secret,R);
- claim_s3(A,Secret,BB);
- claim_s4(A,Secret,B);
- claim_s4(A,Secret,C);



Claim	Status	Comments
phdProtocol A phdProtocol,a1 Secret B	Ok	No attacks within bounds.
phdProtocol,a2 Secret C	Ok	No attacks within bounds.
phdProtocol,a3 Secret R	Ok Verified	No attacks.
phdProtocol,a4 Secret K	Ok Verified	No attacks.
phdProtocol,a5 Secret BB	Ok Verified	No attacks.
phdProtocol,a6 Niagree	Ok Verified	No attacks.
phdProtocol,a7 Nisynch	Ok Verified	No attacks.
S phdProtocol,s1 Secret K	Ok Verified	No attacks.
phdProtocol,s2 Secret R	Ok Verified	No attacks.
phdProtocol,s3 Secret BB	Ok Verified	No attacks.
phdProtocol,s4 Secret B	Ok Verified	No attacks.
phdProtocol,s5 Secret C	Ok Verified	No attacks.
phdProtocol,s6 Niagree	Ok Verified	No attacks.
phdProtocol,s7 Nisynch	Ok Verified	No attacks.
M phdProtocol,m1 Secret K	Ok Verified	No attacks.

Done.

Figure 5: Scyther verifies or falsifies security properties for the proposed authentication protocol

We avoided this kind of attack by encrypting all sent messages in the network using the server secret key (y).

Also there are attacks on the secrecy of the session key ($S_k = \text{hash}(R \oplus \text{hash}(BB \oplus K))$). We avoided this kind of attacks by sending the S_k to the mobile network then the mobile network will send it to the user.

2. Use Scyther tool to avoid these attacks by modifying the protocol and the result as shown in figure 6.

Figure 6 shows that all the claims used to verify the security properties for the proposed authentication protocol with a status (OK) for all the claims and there are no attacks within bounds are found.

Claim	Status	Comments	Patterns
A phdProtocol,a1 Secret B	Ok	No attacks within bounds.	
phdProtocol,a2 Secret C	Ok	No attacks within bounds.	
phdProtocol,a3 Secret R	Ok	Verified No attacks.	
phdProtocol,a4 Secret k	Ok	Verified No attacks.	
phdProtocol,a5 Secret BB	Ok	Verified No attacks.	
phdProtocol,a6 Niagree	Ok	Verified No attacks.	
phdProtocol,a7 Nisynch	Ok	Verified No attacks.	
S phdProtocol,s1 Secret k	Ok	Verified No attacks.	
phdProtocol,s2 Secret R	Ok	Verified No attacks.	
phdProtocol,s3 Secret BB	Ok	Verified No attacks.	
phdProtocol,s4 Secret B	Ok	Verified No attacks.	
phdProtocol,s5 Secret C	Ok	Verified No attacks.	
phdProtocol,s6 Niagree	Ok	Verified No attacks.	
phdProtocol,s7 Nisynch	Ok	Verified No attacks.	
M phdProtocol,m1 Secret k	Fail	Falsified At least 1 attack.	1 attack

Figure 6: Scyther verifies or falsifies security properties for the proposed authentication protocol.

CONCLUSIONS

This paper analyzes the vulnerabilities in Amlan et.al. user authentication protocol for cloud computing [15]. However, pseudonymity and information confidentiality are broken in this protocol. A revised authentication protocol is proposed by new security scenario. The new solution is efficient to tackling the various security threats such as replay, man-in-the-middle and DOS attacks. The revised authentication protocol is expected to provide better security to authenticate cloud computing systems.

REFERENCES

- [1] National Institute of Standards and Technology, "The NIST definition of cloud computing," Information Technology Laboratory, 2009.

- [2] K. Stanoevska-Slabeva, T. Wozniak, and S. Ristol "Grid and cloud computing- a business perspective on technology and applications," Springer-Verlag, Berlin, Heidelberg, 2009.
- [3] Z. Huang, C. Mei, L. Li, and T. Woo, "Cloud Stream: delivering high quality streaming videos through a cloud-based SVC proxy," Proc. Of 2011 IEEE Infocom, USA, 2011.
- [4] C. Robertson, B. MacIntyre, B. Walker, "An evaluation of graphical context as a means for ameliorating the effects of registration error," IEEE Transactions on Visualization and Computer Graphics, vol. 15, pp.179-192, 2009.
- [5] Y. Chen, Z. Du, M. Garcia-Acosta, "Robot as a Service in Cloud Computing," Proc. of 2010 Fifth IEEE International Symposium on Service Oriented System Engineering, USA, 2010.
- [6] Piotr K. Tysowski, M. Anwarul Hasan, "Re-Encryption-Based Key Management towards Secure and Scalable Mobile Applications in Clouds", 2012.
- [7] Jaya Nirmala, S. Mary Saira Bhanu, Ahtesham Akhtar Patel, "A Comparative study of the secret sharing algorithms for secure data in the cloud," International Journal on Cloud Computing: Services and Architecture (IJCCSA), Vol.2, No.4, August 2012.
- [8] J.-H. Yang and C.-C. Chang, "An ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem," Computers & Security, vol.28, pp.138-143, 2009.
- [9] J.H. Yeh, "A PASS scheme in cloud computing -protecting data privacy by authentication and secret sharing," Proc. of International Conference on Security and Management, 2011.
- [10] X.J. Tian, et al., "Analysis and improvement of an authenticated key exchange protocol for sensor networks," IEEE Communications Letters, vol.9, pp.970-972, Nov 2005.
- [11] R.B. Ash, A Pari/Gp Tutorial, <http://www.uiuc.edu/r.ash/GPTutorial.pdf>.
- [12] S. Wong, PARI-GP Tutorial, <http://www.umass.edu/siman/09.791N/tutorial.pdf>.
- [13] T.K. Mendhe, P.A. Kamble, and A.K. Thakre, "Survey on security, storage, and networking of cloud computing," International Journal on Computer Science and Engineering, vol. 4, pp. 1780-1785, 2012.
- [14] S. Lee, I. Ong, H.T. Lim, H.J. Lee, "Two factor authentication for cloud computing", International Journal of KIMICS, vol 8, Pp. 427-432, 2012.
- [15] Amlan Jyoti Choudhury, Pardeep Kumar and Mangal Sain, "A Strong User Authentication Framework for Cloud Computing," IEEE Asia-Pacific Services Computing Conference, 2011.
- [16] Noudjoud Kahya, Nacira Ghoualmi, Pascal Lafourcade, Formal Analysis of PKM using Scyther Tool International Conference on Information Technology and e- Services, 2012.
- [17] Ahmed M. Taha, Amr T. Abdel-Hamid, and Sofiene Tahar Formal Verification of IEEE 802.16 Security Sublayer Using Scyther Tool ESR Groups France, 2009.
- [18] Kahya Noudjoud, Debbah Adel and Nacira Ghoualmi WiMA Security – A Formal Analysis using Scyther tool International Conference on Computational Techniques and Artificial Intelligence (ICCTAI'2012) Penang, Malaysia, 2012.