DOI: 10.21917/ijct.2019.0310

A NOVEL APPROACH OF DESIGNING RFID AUTHENTICATION PROTOCOL BASED ON SIMPLE SYMMETRIC KEY (SSK) ALGORITHM

Prakash Kuppuswamy[1], Shanmugasundaram[2] and Rajan John[3]

[1]*Department of Computer Networks and Engineering, College of Computer Science and Information Technology, Jazan University, Saudi Arabia*

[2,3]*Department of Computer Science, College of Computer Science and Information Technology, Jazan University, Saudi Arabia*

Abstract

RFID uses radio frequency waves to transfer data using components such as tag, the reader and back-end server for device identification. Radio Frequency Identification technology (RFID) providing unique identification and tracking any device that has a tag attached to safeguard the products and protect from unauthorized users. There are many kinds of protocols to resolve these problems have been researched. Though, the security, cost, time and task of RFID are accountable to identify the feasible authentication protocol according to the business environment. In this research article, we proposed new authentication protocol as a method to protect privacy, especially for affordable cost and functionalities and have limited power consumption, memory and effective security process. The proposed protocol called as simple symmetric key (SSK) algorithm using random integers based on modulo 37. The proposed authentication protocol is secure against spoofing and replay attack and also it is suitable to support distributed database environment.

Keywords:

RFID, Security, Symmetric Key Algorithm, Authentication, SSK, AES, DES

1. INTRODUCTION

Radio Frequency Identification (RFID) is an emerging technology which can help to track the devices and equipment. Every device attaches with RFID tag and it can be readable by RFID readers through radio communication to avoid the theft and unauthorized user access [1]. Each RFID tag has its own unique identity (ID) and is attached to an object or device. Then readers identify the tag ID through the wireless communication between RFID tag and reader to make alert for unauthorized usage of the device or equipment. [2]. RFID system practices radio wave frequency technique to transfer signal and track any object that has a tagged with particular device. RFID system has three main components: the tag, the reader, and the back-end server. RFID tag is basically fixed on devices and has secret key identification values and an identifier stored in its memory device. The same memory device values are also stored in the back-end server, and the tag can authenticate itself by sending and receiving its values to the server through a reader. The reader queries tag by sending radio frequency (RF) signals to ask the tags for their identification values in order to authenticate device [3]-[5]. RFID system helps to work in many user and device application without any intervention of external entities. Currently, RFID has been extensively used in many fields such as device tracking, supply chain management, Home and office logistic control and many more [2] [6].

In recent years, there are many kinds of interventions such as tag tracing, impersonation, desynchronization attack and physical attacks and clone attacks targeting at RFID system. Such type of similar threatening always affects RFID security and privacy policies. The security and privacy of RFID systems are threatened by these attacks. Because of the hardware limitation of an EPC Gen2 tag, the security problem becomes even more complicated [7]. Many research studies have explored the security problems in smart systems, such as access control, key agreement and data upload smart systems contain many network technology problems to be solved [8]-[10],[32]-[35]. The technical requirements of a smart system involve many aspects, especially proposing novel network security schemes [11]-[15]. RFID tag consist special cipher code, ciphers are very popular due to more significant features such as high speed, can be implemented easily in hardware, have limited propagation errors and are particularly suitable for all environments where alphabet symbols are processed on RFID tag [16], [18]-[21].

RFID is an automatic identification system has been used in many industry and companies to secure their products from the holdup. The RFID tag comprises unique identification number designed by the manufacturing companies. RFID tags is designed with low cast consist small microchip and antenna, that can be capable to read by the server with the help of RFID reader. The unique identified RFID tag is capable to readable via short-range of radio frequency by the reader. The RFID reader transmits signals to the server about the object which can be attached with the manufacturer device [28]-[31]. For the aspects of security concern of wired networks and wireless networks facing various vulnerabilities by the trespassers. Therefore, it is essential to fulfill following security requirements as mentioned in Fig.1. RFID tools need strong security aspects, which need to be tackled in order to make this technology more robust and reliable. The key security properties like confidentiality, integrity, availability, authentication and anonymity need far more attention [26].

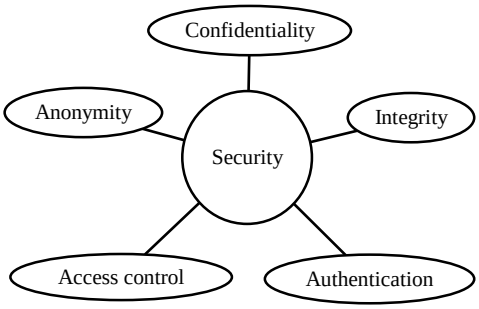

Fig.1. RFID security features

- **Confidentiality**: Data transmitted in a message must be confirmed only by qualified objects. Adversaries must be prevented from knowing the traffic characteristics of the

data source; the destination, frequency, length, or communication network.

- **Integrity**: Transmitted messages must not be forged, deleted or modified and the user must confirm any modifications.
- **Authentication**: Messages transmitted or the source of the electronic document sent by the user requesting a service must be verified in order to prevent false identification.
- **Access control**: Disqualified users must be prevented from using the service.
- **Anonymity**: Third parties must be prevented from knowing the service requested by the user [30].

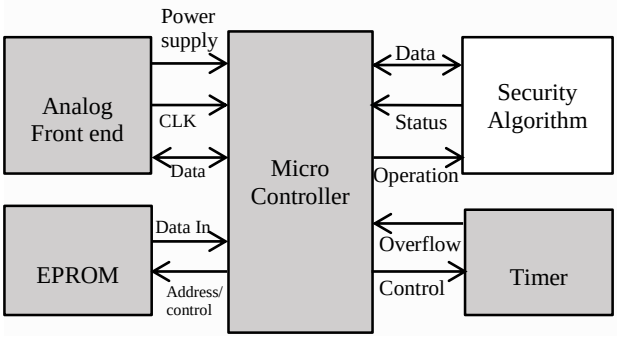

Fig.2. Block diagram of an RFID with security module

In Fig.2, the general Block diagram of an RFID structure consist Micro controller attached with Analog frontend and Erasable programmable read only memory and other side Timer unit and Specifiable security algorithm unit committed with micro controller. The significant advantages of RFID systems are capable to provide automated and multiple identification capture and system analysis, also it is capable to read several tags automatically at the same time to track the tagged devices. The security module implemented on the tag, it consists of alphabets and digits that can be readable by the readers. Basically RFID system is a low-cost design with limited memory and power and capable to support wireless communication. Therefore, it is essential to introduce low-cost module cryptographic algorithm for privacy and security for the device [31].

In this research, we proposed new algorithm for RFID tag authentication and security threats issues, and discuss the performance of new authentication protocol. In section 2 reviews related work and examines existing schemes used in the RFID tag. Next, we proposed tools of new authentication mechanism in section 3. The execution process of RFID tag id allocation and RFID tag reader authentication mechanism discussed with example in section 4. In section 5 analyses the protocol and its significant usage in RFID tag discussed. In section 6 concluded the usages, application of proposed algorithm in other sector and future research on proposed scheme were discussed.

2. LITERATURE REVIEW

Chien [27] discussed low-cost RFID based on ultralight weight RFID authentication protocols, it resists all possible attacks and threats. Existing model ultra-lightweight authentication schemes are vulnerable to various attacks. In this article author proposes a new ultra-lightweight RFID authentication protocol that provides better authentication scheme and strong integrity protection of its signal transmission. Proposed protocol works based on simple bit-wise operations on the tag and can prevent all the possible threaten. These features make it very attractive to low-cost RFIDs and very low-cost RFIDs [27].

Pham [28] proposed knapsack cipher based method. This model makes the cipher higher security and efficient. Author enhanced with new knapsack cipher and it can be applied widely in the systems which need high safety. In addition to that, author describes knapsack cipher 0/1, both the encryption and decryption operators are required to access to each bit of data. This makes the process of encryption and decryption very slow. To make the efficient performance knapsack cipher 0/1, author suggest new model is called knapsack cipher 0/255. It is safer than the knapsack cipher 0/1 with the complexity of O(256N) and O(2N), respectively. The research work initiates in electronic signature and e-commerce based on knapsack cipher 0/255 [28].

Kuppuswamy et al. [29] proposed e-commerce Security model. It is essential to protecting data and web application on open communication channel. Users and application systems requires a combination of managerial, technical and physical controls to protect device. In this research article, authors proposed hybrid cryptographic system that combines familiar RSA cryptography and symmetric key algorithm. In this security scheme, author used simple integer for symmetric key and modular 37 and RSA public key algorithm. On implementation of this combination of hybrid algorithm concluded many significant point [29].

Kuppuswamy et al. [30] described security aspects of Cyber-crime. Basically, internet and web are open network and it is very easy to breach and steal the web user's information. There are many data protection security models available to secure financial data from cyber criminals. Authors proposed scheme works on arbitrary data, is based on alphabetic a-z and integers 0-9. Proposed algorithm supports large amount of message encryption without assuming prior knowledge of the text message. The implementation of proposed protocol not more expensive and data conversion is very high and more secure. The algorithm designed into key generation process, data decryption process and data decryption process and it provides more confidential and flexible data control [30].

Zhu et al. [2] discussed about RFID is the key techniques for Internet of Things, which has been widely adopted in many applications for object identification. RFID always threatened by various security and privacy issues. Mainly, RFID tag is very easy to clone, it is one of the most serious threats is to clone tags for the goal of counterfeiting original device or equipment. The cloning method creates very danger and it causes huge financial loss to all. Finding solution to the above problems, there are many authentication protocols are proposed based on physical unclonable features that can safeguard an anti-counterfeiting feature. In this paper, author proposed a lightweight RFID mutual authentication protocol for ideal PUF. The proposed protocols are immune to physical attacks and clone attacks since the tag stores no secrets and equips with a PUF. Besides, it supports low-cost tags and the applications with a large amount of tags and it's more suitable to enhance the security and privacy for IoT applications [2].

Khalid et al. [31] discussed about significant of IOT network and device or object identification. The RFID system is one of the significant device that communicate between network and end device. Specifically, it is efficiently functioning on insecure wireless communication channel. Open network channel, an authentication mechanism is required to protect device or equipment to avoid the malicious activities. In this algorithm, comparative study is delivered to highlight the common problems and weaknesses of the existing authentication algorithms. Also, it emphasizes on the lack of security standardization for the resource constraint IoT network perception layer. The security and privacy of the IoT network are of utmost concern since a large amount of user-specific data is being generated on a real-time basis. In this paper newly proposed EGP for IOT model implanted and avoids existing model complicated issues. The performance comparison of the EGP protocol shows that it outperforms compared to its contending UMAPs in terms of security. This remarkable feature makes EGP the best choice for extremely low-cost IoTs sensors and RFID tags [31].

3. PROPOSED SCHEME

The proposed scheme assumes that the communication between the server and the tag reader is based on an authenticated channel and its confidentiality is ensured. Their scheme consists of two phases: an initialization phase and an authentication phase. The algorithm used for securing smart card application based on the 26 alphabets and 0-9 numbers, it can be fulfilling any type of messages, so that we used modulo 37 to process the smart card application process. Our proposed smart card security model designing based on symmetric key algorithm using simple text and numerals. The major advantage of symmetric cryptography is to use same keys for the encryption and decryption. The processing and accessing method between user and system described in Fig.3. The user and system authentication processing has three stages, first step registration process, user authentication process and finally access verification process, these stages were as follows:

3.1 KEY DISTRIBUTION PROCESS

Step 1: Select any random number say as *n*.

Step 2: Find the Inverse of the random number using modulo 37(key 1) say *k*.

3.2 TAG ID GENERATION

Step 1: User can choose any value as a security number of RFID

Step 2: Calculate messages with '*n*' and mod 37

Step 3: Remainder value called as his secret message store in smartcard

3.3 TAG READER VERIFICATION

Step 1: Verification stored message calculate with '*k*'

Step 2: Calculate with modulo 37

Step 3: Now user authentication variable and accessing variable same then access granted

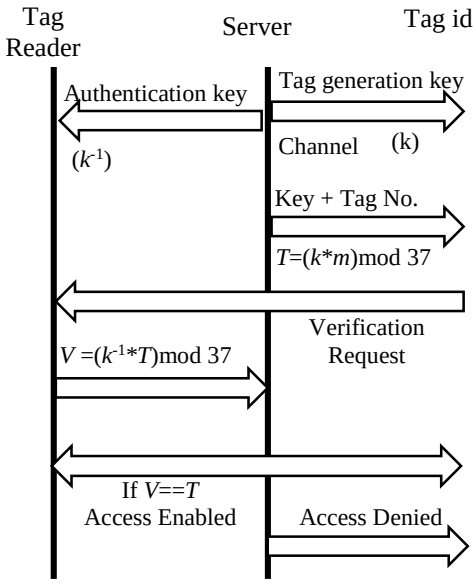

Fig.3. Smart card authentication process

4. IMPLEMENTATION PLAN

The proposed symmetric key RFID authentication approach based on simple mathematical calculation based suitable for small scale device. In this technique we have generated by the server key based on the random number and inverse of the number generated and distributed to the tag id allocation and tag reader to verify tag information to authenticate the device.

4.1 INITIALIZATION PHASE

The backend server first generates by chosen random integer '*k*' and its equivalent inverse using mod 37 called as k^1. These key can be used to generate the RFID tag for the device and authentication for the verification.

4.2 RFID TAG GENERATION PHASE

Each and every RFID tag can be allocating by unique id, it can be capable to create by the companies using any alphabets and integer combination. This RFID tag generation can be done by the $T = (k*m)\text{mod}37$.

4.3 RFID TAG AUTHENTICATION PHASE

RFID reader can verify the device tag information using by $V = (k\text{-}1*T)\text{mod}37$. RFID tagged device id '*T*' and RFID Reader authentication message 'V' is equal then access can be allowed by the server otherwise server will give alert message.

In order to provide quick and simple example of execution method of RFID authentication function, we have chosen here sample message combination of alphabets and numbers i.e. 'RFID123'. We have chosen 3 different key 3, 4 and 8. When we are choosing 3 as a key to generate and allocate RFID number i.e. RFID123 becomes QR0LJMP as a Tag number to be fixed on the device. Similarly, if we choose key is 5 and Tag number becomes P3HT27B and if we choose key is 8 then tag number is 6K85BJR shown in the Table.1.

Table.1. RFID tag generating process

	Value	Key = 3	Key = 5	Key = 8
R	18	Q=17	P=16	33=6
F	6	R=18	3=30	11=K
I	9	0=27	H=8	35=8
D	4	L=12	T=20	32=5
1	28	J=10	2=29	2=B
2	29	M=13	7=34	10=J
3	30	P=16	B=2	18=R

RFID tag reader authentication or verification process through the authenticated server which is stored the inverse of 3 on mod 37 is 25, inverse of 5 is 15 and inverse of 8 is 14 mentioned in the Table.2. RFID tagged message and RFID reader message is equivalent, then the server will allow the RFID tag devices otherwise it will create alert message.

Table.2. RFID reader verification process

$Key3^{-1}=25$	$Key5^{-1}=15$	$Key8^{-1}=14$
(25*17) mod 37=18	(15*16) mod 37=18	(14*33) mod 37=18
(25*18) mod 37=6	(15*30) mod 37=6	(14*11) mod 37=6
(25*17) mod 37=9	(15*8) mod 37=9	(14*35) mod 37=9
(25*17) mod 37=4	(15*20) mod 37=4	(14*32) mod 37=4
(25*17) mod 37=28	(15*29) mod 37=28	(14*2) mod 37=28
(25*17) mod 37=29	(15*34) mod 37=29	(14*10) mod 37=29
(25*17) mod 37=30	(15*2) mod 37=30	(14*18) mod 37=30

5. BENEFITS OF PROPOSED PROTOCOL

Mostly in RFID schemes not implemented by the complex and high secured computational algorithm due to the considerable features of cost, power consumption and storage capacity of RFID tag. Proposed scheme data stored in a tag has very less memory occupied. The computational requirement is not complicated; therefore, it required minimum power supply. The data transmission of the proposed system, from the tag to tag reader and tag to server consist less bandwidth since we have chosen simple integer numbers. The server can generate to make the different combination readable format of the tag with the help of choosing simple random integer key. Proposed mode can perform an in-depth search to identify individual tags in the large population.

6. CONCLUSION

We have presented a new RFID authentication protocol designed to meet the performance, cost and power energy. The significant idea of this paper to identify flexible and low cost RFID tags authentication schemes for small scale environments to suitable for wired and wireless network conditions. In this paper, the proposed mechanism only discusses authentication, and the authorization schemes. There are many protocols such as LMAP, M2AP, EMAP used in RFID, In the future we will analyze the comprehensive study of proposed scheme and existing scheme with the parameter of performance, power consumption, security threats, storage capacity and cost.

REFERENCES

[1] Dang Nguyen Duc and Kwangjo Kim, "Defending RFID Authentication Protocols against DoS Attacks", *Computer Communications*, Vol. 34, pp. 384-390, 2011.

[2] Feng Zhu, Peng Li, He Xu and Ruchuan Wang, "A Lightweight RFID Mutual Authentication Protocol with PUF", *Sensors*, Vol. 19, No. 13, pp. 1-13, 2019.

[3] B. Song and C.J. Mitchell, "RFID Authentication Protocol for Low-Cost Tags", *Proceedings of 1st ACM Conference on Wireless Network Security*, pp. 140-147, 2008.

[4] S. Kardas, S. Celik, M. Sariyuce and A. Levi, "A Secure and Private RFID Authentication Protocol based on Quadratic Residue", *Proceedings of International Conference on Software, Telecommunications and Computer Networks*, pp. 1-6, 2012.

[5] Abdulhadi Alqarnia, Maali Alabdulhafitha and Srinivas Sampallia, "A Proposed RFID Authentication Protocol based on Two Stages of Authentication", *Proceedings of International Workshop on Privacy and Security in HealthCare*, pp. 503-510, 2014.

[6] R. Gadh, G. Roussos, K. Michael, G.Q. Huang, B.S. Prabhu and P. Chu, "RFID-A Unique Radio Innovation for the 21st Century", *Proceedings of the IEEE*, Vol. 98, No. 9, pp. 1546-1549, 2010.

[7] S. Karda, M.S. Kiraz, M.A. Bingol and H. Demirci, "A Novel RFID Distance Bounding Protocol Based on Physically Unclonable Functions", *Proceedings of International Workshop on Radio Frequency Identification: Security and Privacy Issues*, pp. 78–93, 2011.

[8] E. Fernandes, A. Rahmati, J. Jung and A. Prakash, "Security Implications of Permission Models in Smart-Home Application Frameworks", *IEEE Security and Privacy*, Vol. 15, No. 2, pp. 24-30, 2017.

[9] P. Kumar, A. Braeken, A. Gurtov, J. Iinatti and P.H. Ha, "Anonymous Secure Framework in Connected Smart Home Environments", *IEEE Transactions on Information Forensics and Security*, Vol. 12, No. 4, pp. 968-979, 2017.

[10] P. Kumar, A. Gurtov, J. Iinatti, M. Ylianttila and M. Sain, "Lightweight and Secure Session Key Establishment Scheme in Smart Home Environments", *IEEE Sensors Journal*, Vol. 16, No. 1, pp. 254-264, 2016.

[11] Jian Shen, Chen Wang, Tong Li, Xiaofeng Chen, Xinyi Huang and Zhi-Hui Zhan, "Secure Data Uploading Scheme for a Smart Home System", *Information Sciences*, Vol. 453, pp. 186-197, 2018.

[12] X. Chen J Li, J. Weng, J. Ma and W. Lou, "Verifiable Computation over Large Database with Incremental Updates", *IEEE Transactions on Computers*, Vol. 65, No. 10, pp. 3184-3195, 2016.

[13] J. Li, Y. Zhang, X. Chen and Y. Xiang, "Secure Attribute-based Data Sharing for Resource-Limited users in Cloud Computing", *Computers and Security*, Vol. 72, pp. 1-12, 2018.

[14] J. Shen, C. Wang, A. Wang, Q. Liu and Y. Xiang, "Moving Centroid based Routing Protocol for Incompletely Predictable Cyber Devices in Cyber-Physical-Social

Distributed Systems", *Future Generation Computer Systems*, Vol. 45, No. 3, pp. 1-16, 2017.

[15] J. Shen, T. Zhou, D. He, Y. Zhang, X. Sun and Y. Xiang, "Block Design-Based Key Agreement for Group Data Sharing in Cloud Computing", *IEEE Transactions on Dependable and Secure Computing*, Vol. 16, No. 6, pp. 996-1010, 2017.

[16] Fuster Sabater, "Computation of Filtering Functions for Cryptographic Applications", *Proceedings of 14th International Conference on Computational Science*, pp. 2013-2023, 2014.

[17] J. Wang, X. Chen, J. Li, J. Zhao and J. Shen, "Towards Achieving Flexible and Verifiable Search for Outsourced Database in Cloud Computing", *Future Generation Computer Systems*, Vol. 67, pp. 266-275, 2017.

[18] N. Nagaraj, "One-Time Pad as a Nonlinear Dynamical System", *Communications in Nonlinear Science and Numerical Simulation*, Vol. 17, No. 11, pp. 4029-4036, 2012.

[19] C. Paar and J. Pelzl, "*Understanding Cryptography*", Springer, 2010.

[20] R.A. Rueppel, "*Analysis and Design of Stream Ciphers*", Springer, 1986.

[21] A.J. Menezes, "*Handbook of Applied Cryptography*", CRC Press, 1997.

[22] Jung Sik Cho, Sang Soo Yeo and Sung Kwon Kim, "Securing against Brute-Force Attack: A Hash-based RFID Mutual Authentication Protocol using a Secret Value", *Computer Communications*, Vol. 34, No. 2, pp. 391-397, 2011.

[23] K. Finkenzeller, "*RFID Handbook*", 2nd Edition, Willey and Sons, 2002.

[24] EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID, Available at: https://www.gs1.org/sites/default/files/docs/epc/Gen2_Protocol_Standard.pdf

[25] Juels, "RFID Security and Privacy: A Research Survey", *Selected Areas in Communications*, Vol. 24, No. 2, pp. 381-394, 2006.

[26] Y. Yousuf and M. Vidyasagar, "A Survey of RFID Authentication Protocols", *Proceeding of 22nd International Conference on Advanced Information Networking and Applications*, pp. 441-447, 2008.

[27] Hung-Yu Chien, "SASI: A New Ultra lightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity", *IEEE Transactions on Dependable and Secure Computing*, Vol. 4, No. 4, pp. 337-340, 2007

[28] Anh Pham, "The Improvement of the Knapsack Cipher", *Computer Communications*, Vol. 34, No. 3, pp. 342-343, 2011.

[29] Prakash Kuppuswamy, Rashida Banu and Nithya Rekha, "Preventing and Securing Data From Cyber Crime using New Authentication Method Based On Block Cipher Scheme", *Proceedings of 2nd International Conference on Anti Cyber Crimes*, pp. 113-117, 2017.

[30] Prakash Kuppuswamy and Saeed Q.Y. Al-Khalidi, "Securing E-Commerce Business using Hybrid Combination based on New Symmetric Key and RSA Algorithm", *MIS Review*, Vol. 20, No. 1, pp. 59-71, 2014.

[31] Madiha Khalid, Umar Mujahid and Najam-Ul-Islam Muhammad, "Ultralightweight RFID Authentication Protocols for Low-Cost Passive RFID Tags", *Security and Communication Networks*, Vol. 2019, pp. 1-25, 2019.

[32] H. Zhang, M.E.E Alahi, H. Ghayvat, S.C. Mukhopadhyay, Y.T. Zhang and W. Wu, "A Novel Secure IOT-based Smart Home Automation System using a Wireless Sensor Network", *Sensors*, Vol. 17, No. 1, pp. 69-87, 2016.

[33] S. Singh, P.K. Sharma and J.H. Park, "S.H. Secnet: An Enhanced Secure Network Architecture for the Diagnosis of Security Threats in a Smart Home", *Sustainability*, Vol. 9, No. 4, pp. 513-531, 2017.

[34] M. Wazid, A.K. Das, V. Odelu, N. Kumar and W. Susilo, "Secure Remote User Authenticated Key Establishment Protocol for Smart Home Environment", *IEEE Transactions on Dependable and Secure Computing*, Vol. 14, No. 2, pp. 337-340, 2017.

[35] Jong Sik Moon and Im-Yeong Lee, "An AAA Scheme using ID-Based Ticket with Anonymity in Future Mobile Communication", *Computer Communications*, Vol. 34, No. 3, pp. 295-304, 2011.

[36] S. Weis, S. Sarma, R. Rivest and D. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems", *Proceedings of International Conference on Security in Pervasive Computing*, pp. 454-469, 2003.

[37] Ming Huang Guo, Horng Twu Liaw, Der Jiunn Deng and Han Chieh Chao, "An RFID Secure Authentication Mechanism in WLAN", *Computer Communications*, Vol. 34, No. 3, pp. 236-240, 2011.