

## Development of Transactions Authorization Protocol for Ubiquitous Commerce Systems

Safiriyu I. Eludiora<sup>1</sup>, Fatai A. Anifowose<sup>2</sup>

<sup>1</sup> Department of Computer Science and Engineering, Obafemi Awolowo University,  
Ile-Ife 22005, Osun State, Nigeria.

<sup>2</sup> Centre for Petroleum & Minerals, King Fahd University of Petroleum & Minerals,  
Dhahran, 31261, Kingdom of Saudi Arabia.

*safiriyue@yahoo.com, anifowo@kfupm.edu.sa*

**Abstract.** Transparency in transactions can only be achieved through a controlled coordination of the real and cyber worlds. The success of Ubiquitous Commerce Systems (UCS) relies on the convergence of both worlds. The mobile devices are ubiquitous; they can be used anytime and anywhere. This poses a lot of security challenges in a ubiquitous society where business transactions will be involved. With the emergence of electronic payment and other business transaction solutions, ubiquity has the potential to make commerce freer and the transaction flows easier. However, privacy, security and mutual trust are critical to its development and use. Hence, for users of UCS services to have full confidence in the system, most especially while operating in a cashless society, absolute security must be put in place by stakeholders. This paper presents a Transactions Authorization Protocol (TAP) for the UCS. TAP is conceptualized to enhance security for UCS users. This protocol is less intrusive and it allows stage by stage authentication before final authorization of the users' requests.

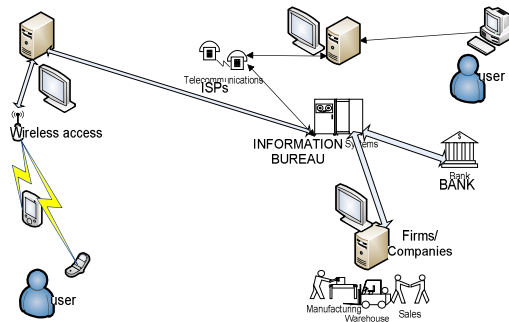
**Keywords:** Security, Ubiquitous, Transactions, Protocol.

### 1. INTRODUCTION

The trends in technological advancement have opened opportunities in different areas of human endeavor. Traditional commerce is restricted to physical marketplaces where buying and selling can take place. Today, people can transact businesses through the internet (electronic commerce platform), cell phones and other mobile devices such as iPods and iPads (mobile commerce platform) seamlessly. The ubiquity of mobile devices such as cell phones and Personal Digital Assistants (PDAs) coupled with their computational functionalities has made continuous access to the cyber world a necessity rather than a luxury.

Integrating different communication technologies with mobile users' devices allows the users to do their business transactions. This is achieved using a Ubiquitous Commerce System (UCS), which is one of the application areas of Ubiquitous Computing [1], [2], [3]. Ubiquitous Computing can be defined as a

post-desktop model of human-computer interaction in which information processing has been thoroughly integrated into everyday objects and activities [4]. UCS was also defined by [5] as “the use of ubiquitous networks to support personalized and uninterrupted communications and transactions between a firm and its various stakeholders to provide a level of value over, above and beyond traditional commerce”. UCS architecture describes the communication between the users that are using mobile devices (wireless access) and those that are using wired network. This is shown in figure 1.



**Figure. 1.** The architecture of Ubiquitous Commerce System

There is the need to discuss some key words in these definition viz. ubiquitous networks, personalized, uninterrupted communications and transactions. Ubiquitous networks are described as where all users’ devices are connected to the cyber world for the users to have access to the UCS services. Internet and communications technologies will enable users to remain connected to the cyber world. A cell phone is a good example [2],[6].

The word "personalized" can be explained as the personal needs of users that UCS can provide. Unique solutions to user’s requests based on user’s profile are possible. An example of this is the Short Message Service (SMS). UCS advertisements and product promotions can be also be sent to individual electronic mail addresses and cell phones’ numbers [5].

Uninterrupted communications means that users will continue to have access to the cyber world without hindrances. The mobile users’ devices will remain connected to the UCS network without any interruption. This will ease transactions in UCS environment since the services will be accessible and available seamlessly [5], [7].

Transactions in the context of UCS will allow users to trade online, make payments using electronic means and other solutions such as VISA and MASTER cards in a secured and reliable environment. These e-payment solutions will make transactions easier for the buyers and sellers. There is no need of handling cash as the digital monetary value stored in these cards can be used in place of checks or cash [7],[8].

In this paper, a protocol to authorize transactions on the ubiquitous platform and that uses a scalable security protocol for the UCS is presented. The protocol has been shown to have the capability to address security challenges raised in UCS. Developers of this protocol however need to put into proper consideration the various limitations and constraints on the resources of mobile devices. Such constraints include memory, power and the Central Processing Unit (CPU).

## **2. RELATED WORK**

Security and mutual trust were the key issues discussed by [14]. The work showed that security architecture for the ubiquitous technology must be based on mutual trust. It emphasized that user authentication and access control being used in traditional stand-alone personal computers do not have the capability to address the current security trends in ubiquitous networks. The author proposed a Trusted-based security infrastructure (TBSI). According to the authors, the TBSI manage trust and risks by supporting authentication and authorization to unknown users. However, more works needed to be done on the access control and intrusion detection policies as electronic transactions have become the order of the day. Cheng et al. [15] proposed Mobile Ubiquitous Privacy Protection for Electronic Transactions MUPPET which is an information brokerage framework that gives users control over the release of their data.

A flexible authorization management framework was proposed by [16]. This framework provides flexible protocol for negotiation and exchange of authorized information in networking environments. An attribute-based authentication and authorization infrastructure AAI and ABAC was proposed by [17]. It provides integrated federations of security services to users. The AAI and ABAC provide mechanisms for customers' privacy and vendor's needed information.

In [20] authors proposed trust model that can be used in handling transactions. The work used case study of taxi call centers and use encryption key management for the security enhancement. Also, in a section of that paper, the authors were of opinion that the work can address privacy and security. The trust model proposed in this paper is domain specific and it can easily be managed by the operators, but may not work in all situations. Our paper envisaged the general situations of real and cyber world crimes that can create high level of financial risks for the business men. Our proposed protocol considered the real world, where profiles of individuals, organizations and firms are kept. And cyber worlds where information provided on the internet match with the existing physical information provided in real world.

Payment session protocol was proposed in [21]. The authors were addressing payment system in a ubiquitous environment for various services rendered. Their work was similar to our on ubiquitous advertising model for revenue collection. Our paper proposed a general security measures for all transactions in real and cyber world. The proposed work by [21] can be integrated into our protocol. It can be a session within our proposed authorization section.

A survey of [22] ubiquitous commerce was carried out. We have discussed some issues mentioned in their paper in section three. Their paper was not really a technical work, but reviewing of the concept of ubiquitous commerce.

### **3. POTENTIALS OF UBIQUITOUS COMMERCE SYSTEM**

The potentials of the UCS are categorized into four areas namely finance, industries, transportation and home. Financial transactions and banking systems make it possible to have e-finance in the UCS with different financial services such as the trade finance that users will have access to with much ease. UCS incorporates e-business where business management is flexible using relevant technologies. UCS adds functionality to the e-banking system by integrating e-payment technologies into its system, thereby making e-transaction of businesses convenient [7], [8],[9]. Since industries are many, only the relevantly prominent ones that can easily be found around us are discussed in this paper viz. tourism, manufacturing, media and insurance.

Most countries want to improve on their tourism industry. The UCS has potentials to manage this industry. UCS services provides information regarding the country viz. locations of tourism centers, contact detail of hotels and taxis, which are made available at airports. These services will ease the tasks of tourists and make the trip less stressful [7], [8].

E-manufacturing can be achieved using UCS. E-manufacturing technology incorporates necessary users' devices that can work with UCS, for collaboration between the manufacturing sector and business world. Good quality of production/distribution of goods and services can be achieved using UCS. The production unit can use sensors or smart devices to remotely monitor the performance of industrial machines and when these machines are altering production specifications, these devices can send signal to the person in charge for corrections. The Radio Frequency Identification (RFID) technology makes distribution of goods easier and there will be no accidental mix-up of products as sorting of products are flexible [2], [7].

Media can use the e-newspaper technology where ubiquitous advertisements are possible using UCS. The e-newspaper will require the use of e-reader devices and the use of e-reader devices make the reading of newspapers more enjoyable. This development allows the users to read the paper at his/her convenient time. Mobile adverts can be personalized depending on user's requests [10], [18].

Insurance companies can monitor their equipment using UCS services such that the use of vehicles under premium would be constantly tracked and monitored. The Global Positioning System (GPS) technology can be installed in the vehicles so that it will be sending real-time data of their use to the insurance company's office [5].

Transportation can be subdivided into four main areas: air, roads, trains, and water. The UCS services can buy air flight tickets, make seat reservation requests and book hotel accommodation for travelers. It can also make payment using e-payment facilities. It can send text messages to travelers detailing departure and arrival information. The road users use UCS to monitor roads traffic situation to

enable them plan their journey in case there is road hold-up on the route they are planning to travel. UCS can help the accident victims by sending alert message to the nearby hospital for emergency medical attention while describing the location of the incident using the GPS. The UCS can make tracking of ships and trains easy with the installation of GPS equipments. Luggage with RFID tags can easily be monitored when offloading at the ports or terminals [7], [8].

UCS services can monitor the stock level of home foods and household needs such as toiletries by sending alert messages and requesting orders when they are out of stock. UCS services will cause smart devices and sensors to be incorporated in the customers' store and fridge at home. These devices can send reports to the retail shop and the threshold would have been programmed such that the moment any item fall below a preset threshold, the alert messages will be sent to the owner of the house and retail shop for foods for such items to be replenished [11].

## **4. SECURITY CHALLENGES OF UBIQUITOUS COMMERCE SYSTEM**

### **4.1. Basic Security Challenges of UCS**

Security measures based on cable-networked computers may not be effective in the case of mobile users' devices with resources restrictions such as low memory and processing power.

**Authentication.** This is a process by which one entity verifies the identity of another which can be person or program. The authentication process can be done in three ways: something that a user knows such as password and login name, something that a user has such as a Personal Identification Number (PIN) and something that is naturally unique to a user such as finger print, voice or face [19]. There is also an authentication system that determines the source of a message.

An authentication process can also be machine-machine in addition to the aforementioned human-machine. This can be client, server or mutual authentications. Client authentication involves the server verifying the client's identity, server authentication involves the client verifying the server's identity and mutual authentication involves the client and server verifying each other. In the context of UCS, a web server can be authenticated so that a user can deal with real website rather than a clone. Transport Layer Socket (TLS) can be used for this process.

**Authorization.** This is the process that ensures that a person has the right to access certain resources. A user will not be allowed to access any resources without knowing the attributes of such user. Users can have access rights to resources if the authority to do something is not within their reach. For example, a user can use ATM card to withdraw money from a machine, having been authenticated that he cannot withdraw beyond a certain maximum amount irrespective of any amount of

balance in the bank account. UCS uses these access control and authorization to regulate resources usage and minimize fraudulent practices [12].

**Auditing.** This is the process of collecting information about users attempting to access a particular resource or to perform some tasks. The login system must be able to record all actions performed on that resource. In case there is any problem, the log file can be checked to trace the activities of such a user.

**Confidentiality (Privacy).** This is an act that keeps private or sensitive information from being disclosed to un-authorized individuals, entities or processes. In UCS environment, it is important to maintain the confidentiality of transactions since e-payment devices like VISA are involved.

**Integrity.** This is the ability to protect data from being altered or destroyed by un-authorized persons or processes during the course of transmission. This is important in UCS, because the mobile devices use wireless medium and for this reason, data must be well protected.

**Availability.** An online site is available if a user or program can gain access to the pages, data, or services provided by the site whenever they are needed. This is critical to UCS as the unavailability of a website may hinder the on-going transactions and it may lead to loss of money and customers. Technologies such as load balancing hardware and software are aimed at ensuring availability [13].

**Non-repudiation.** This is the ability to limit parties from refuting that a legitimate transaction took place. UCS transactions involve money, hence it is important that the customer is committed through signature endorsement [4], [13]. It is a challenge to the UCS because it is not possible for any customer to buy an item using mobile device and get receipt. The public key infrastructure (PKI) may be used to generate digital signature, but it may not be possible on the mobile devices. The restrictions on resources cannot give room for these sophisticated key management schemes to be run on the mobile devices unlike the wired-network computer that has abundant resources.

**Unstable Connections.** This can occur when mobile device user is on the motion, either in a car or on motor cycle. The network may be epileptic. This may affect any transactions going as at that time, the two parties may not be able to comprehend each other. One way or the other, it can be used by attackers to compromise the transactions.

**Connection Settings.** It might be possible during the course of transmitting that the connections prematurely terminated. That is, after the connection is established, then it suddenly got terminated. This may create a security “gap”. This security gap may create a loop holes that would make the transaction vulnerable to attacks. In this case, data integrity is not guaranteed and it may pose a serious danger to the on-going transactions [4].

**Digital Divides.** This can be described as poor infrastructure deployments. For example, some communities may not have electricity supply for days. Within these people many may be cut-off from the benefits they can derive from having functional mobile devices. They may be cut-off from events, advertisements, promotions, warning messages or transaction alerts as well as other security issues that may not be delivered to their cell phones. This may affect their transactions with the UCS. Also in the rural areas the network signals may not be strong enough to allow connectivity, people in this kind of community have been divided digitally [7].

**Data Integrity.** It may not be possible to encrypt text messages using cell phones as it can be done on a personal computer. The reasons are due to constraints on resources and when data are traveling through a wireless medium, it may be difficult to predict what can happen. Data encryption can be achieved in wired network environment, but may be difficult to achieve in wireless communication network.

**E-payment Technologies.** Mobile users' devices may have problem with sending their credits/debits cards information over the wireless medium. In the future when market prices of base stations and some other equipment become cheaper, hackers can install their own and be using it to compromise and eavesdropping both data and transaction messages. This situation described here may affect business transactions generally beyond the UCS environment.

**Return of Goods and Orders' Cancellation.** A customer may agree and even pay for the item bought but, when delivered, may be found to have some faults. On the other hand, the orders already made and paid for may be canceled. This may affect the relationship between the supplier and buyer. The supplier may be discovered to be operating a virtual market where there is no warehouse. The supplier may find it difficult to collect the item returned or return the goods already shipped.

#### 4.2. Suggested Countermeasures

**Authentication and Access Control.** The new schemes should be less intrusive so that mobile users' devices can run a simple mutual authentication program that will require users' attributes. Stringent conditions should be put in place for mobile user devices on how it will be used to access resources. This may regulate abuse of rights and privileges of mobile clients. Trust models may ease the deployment of UCS and it may be one of the parameters for accessing customers' or merchants' attributes.

**Coordination and Convergence of Real-World and Cyber World.** Transparency of transactions can only be achieved when the real and the cyber worlds are effectively coordinated. For example, a company that has a website and transacting businesses with people without proper business and corporate registration. It is not enough to

have web site without a traceable attributes in the real world. There must be a point of convergence between the two worlds. A website can exist for few weeks and may not be available again after some time. The people who are transacting businesses with them may lose any monetary involvement.

**Open Source Software.** Open source software may be made available for developers. This will give them opportunities to develop security utility software to their taste using their native languages. There should be free training on how to use this software while ensuring that a forum where users of that software can discuss their problem is available. *JAva Development Environment (JADE)* framework is a good example of this.

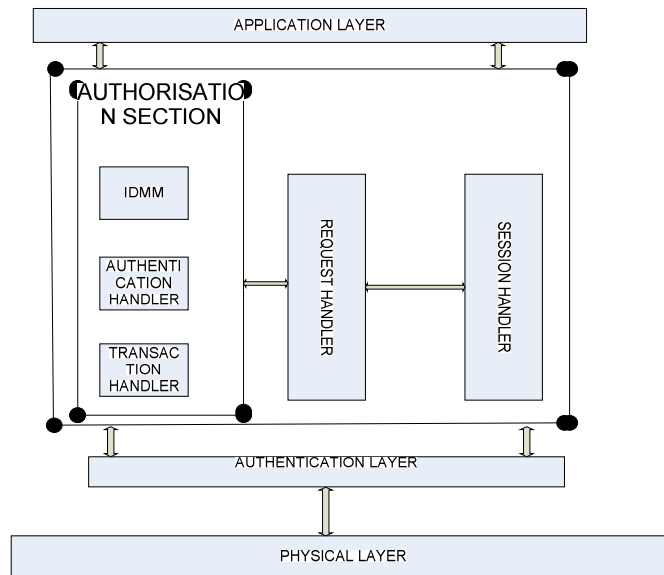
**The Role of Governments.** Government at all levels can enact laws that will address some of the problems discussed here and others not mentioned. There must be regulatory policies on the use of mobile devices and privacy of the customer. Government may enact laws on cyber crimes. The proposed framework is expected to address the challenges in line with the suggested counter-measures to ensure effective coordination and convergence of the real and cyber worlds.

## **5. THE PROPOSED AUTHORIZATION TRANSACTION PROTOCOL FRAMEWORK**

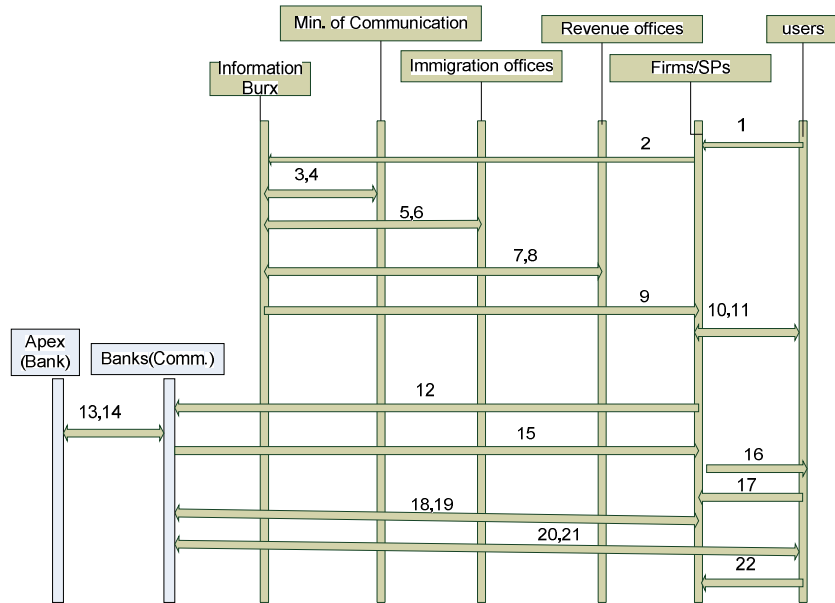
Transaction Authorization Protocol (TAP) is proposed to address the security challenges identified in section 4.1. The TAP has four layers: physical, authentication, authorization and application. Figure 2 shows the relationships between these layers.

The physical layer allows the user devices (wireless and wired) to communicate effectively with the UCS network. This layer uses different schemes to accept users' requests. Users' requests are forwarded to the authentication layer to verify the device as well as program being used by such user. The authentication layer carries out necessary security checks before forwarding it to the authorization layer. The authorization layer has three units: session, request and authorization handlers. The authorization handler further has three modules: Identity Management Module IDMM, transaction, and authentication. The session handler establishes the communication between the user's request and the request handler. Also, the session handler performs handshaking with the authentication layer where verified user's requests are forwarded to the request handler. The request handler performs some verification and transfers the request to the IDM module in the authorization section. Verification of the users' requests will be performed by the authentication handler and forwarded to the transaction handler. The transaction handler will classify the request to determine what needs to be identified with the user. Finally, if the user fulfills all the requirements, the transaction will be authorized, otherwise it will be rejected.

In addition, figure 3 illustrates the flow of information between the user and other stakeholders in a typical TAP transaction. The user will initiate transactions, the NOs/ISPs will perform an authentication procedure on user's device to determine whether it can be granted access to the resources on that network. If it is verified as a genuine request, it will send the request to the firm. The firm will forward the request to the information bureau which will, in turn, send it to its database for verification. It will then get back to the firm where the outcome will be sent to the user through the information bureau. The firm will request for payment from the user/customer; the payment information will be sent to the firm who will send it to the bank for verification. The result will eventually be sent back to the firm to supply the goods or services to the customer.



**Figure. 2.** The Transactions Authorization Protocol layers.



**Figure 3.** Flow of information in the Transactions Authorization Protocol.

### 5.1. Procedural Steps

- 1) User sends requests through SP.
- 2) The SP forwards the requests to the information bureau (IB) confirmation of its status
- 3) Information bureau sends to the Ministry of Communication to confirm the status of SP.
- 4) The ministry returns the finds to the IB.
- 5) The IB requests for users status from immigration’s offices (IOs)
- 6) The IOs returns confirmation
- 7) The IB requests for the user, firms and SPs in terms of tax payments
- 8) The revenue offices (ROs) returns their status information
- 9) The IB returns the status of the user to the SPs.
- 10) The SP returns the status of the finds to the user.  
Transactions continue if the user meets the conditions otherwise terminated.
- 11) The firm forwards the user’s requests to the Commercial Bank
- 12) The Commercial Bank forwards requests to the Apex Bank for authorization
- 13) The Apex Bank authorized the transaction between the firm and the Commercial Bank
- 14) The Commercial Bank approves/disapproves the transactions

- 15) The information is convey to the user
- 16) The payments details are forwarded to the firm
- 17) The firm sends the payments information to the Commercial Bank
- 18) The Commercial Bank acknowledged the payment
- 19) The goods and services requested for by user is package and send.
- 20) The user acknowledge the receipts of the goods and services
- 21) The user sends the confirmation of the receipts of goods and services to the firm.

## **5.2. Implementation**

The framework can be implemented by information bureau (IB) of every country. The IB will be central to the implementation of this protocol. The coordination of real and cyber worlds will minimize cyber crimes and other related offences. The IB must be able to verify physical addresses being claimed by individual and firms. All the stakeholders must be informed of steps to be taken on the TAP.

The TAP as in figure 3.0 explains how transactions must be flowed among stakeholders. Section 5.1 has summarized the actions to be taken at the point of implementation of the proposed protocol.

## **6. CONCLUSIONS**

Ubiquitous Commerce Systems (UCS) has a lot of potentials that can be explored. It can be used in any situation as well as in any field of human endeavors. This paper addressed the challenges of the UCS framework with respect to security and privacy, offered some suggestions to overcome the identified challenges and proposed a novel Transactions Authorization Protocol (TAP) framework that is capable of practically addressing the challenges based on the suggested counter-measures. The proposed framework is practicable and has the potential to ensure a safe and secure operating platform for a given virtual transaction over a wired or wireless networked environment.

In the future, we will simulate this work to determine its security strengthens on mobile devices.

## **REFERENCES**

1. Roussos. G, and Moussouri, T, "Consumer Perceptions of Privacy, Security and Trust in Ubiquitous Commerce", *Journal of Personal and Ubiquitous Computing* 2004, 8 (6): 416-429.

2. Babulak. E, "Ubiquitous Communications in Support of Automation", in Proceedings Fifth International Symposium Communication Systems, Networks and Digital Signal Processing", University of Patras Conference Centre Greece, 2006.
3. Venkataram. P, and Babu. BS, "An Authentication Scheme for Ubiquitous Commerce: A Cognitive Agent-based Approach", in Proceedings Network Operations and Management Symposium Workshops (NOMS), pp. 248 – 256, 2008.
4. Turban. E, King. D, Viehland. D, and Lee. J, "Electronic Commerce: A Managerial Perspective". Upper Saddle River: Pearson Prentice Hall, 2006.
5. Watson. RT, Pitt. LF, Berthon. P, and Zinkhan. GM, "U-Commerce: Expanding the Universe of Marketing", Journal of the Academy of Marketing Science 2002, 30 (4): 329-343.
6. Yeun. CY, Lua. EK, and Crowcroft. J, "Security for Emerging Ubiquitous Networks", in Proceedings 62nd IEEE Vehicular Technology Conference (VTC 2005), Vol. 2, pp.1242- 1248, 2005.
7. Katsumasa. S, "Ubiquitous Security-Towards Realization of a Safe and Secure Digital World", Issues on Ubiquitous Services/Reports on Exhibits at Telecom, Oki Technical Review, Issue 210, Vol.74, No.2, 2006.
8. United Nations, "VISA International: White Paper on e-Finance for Development", United Nations Conference on Trade and Development Financing for Development, Summit and Ministerial "e-Finance for Development", held in Monterrey, Mexico, 2002.
9. Stefano. R, "Acoustic Smart Cards: The Emergence of Ubiquitous Security", 2005. Online: [http://www.identita.com/files/acoustic\\_smartcard\\_whitepaper.pdf](http://www.identita.com/files/acoustic_smartcard_whitepaper.pdf)., Accessed on March 2, 2009.
10. Eriksson. CI, and Akesson. M, "Ubiquitous Advertising Challenges", in Proceedings 7th International Conference on Mobile Business (ICMB '08), pp. 9 – 18, 2008.
11. Kourouthanassis. P, and Roussos. G, "Developing the User Experience in Ubiquitous Commerce", in Proceeding International Conference of Ubiquitous Computing, UbiComp Workshop, 2003.
12. Treu. G, Fuchs. F, and Dargatz. C, "Implicit Authorization for Social Location Disclosure", Journal of Software 2008, 3 (1): 18-26.
13. Whiteman. ME, and Mattord. HJ, "Principles of Information Security", 2nd ed. Massachusetts: Thomson Course Technology, 2005.
14. Hung. LX, Phuong. TV, Giang. PD, Zhung. Y, Lee. S, and Lee. YK, "Security for Ubiquitous Computing, Problems and Proposed Solution", in Proceedings 12th IEEE International Conference on Embedded and Real-Time Computing Systems and Applications (RTCSA'06), 2006.
15. Cheng. W, Li. J, Moore. K., and Karp. AH, "MUPPET: Mobile Ubiquitous Privacy Protection for Electronic Transactions", Digital Printing and Imaging Laboratory, HP Laboratories Palo Alto, 2007.
16. Argyroudis. PG, and O'Mahony. D, "Towards Flexible Authorization Management", in Proceedings 10th IEEE Symposium on Computers and Communications (ISCC 2005), pp. 421- 426, 2005.
17. Schlager. C, Sojer. M, Muschall. B, and Pernul. G, "Attribute-Based Authentication and Authorization Infrastructures for E-Commerce Providers", Proceeding of the

International Conference on E-Commerce and Web Technologies (EC-Web'06), Computer Science (LNCS), Vol. 4082, pp.1-10, 2006.

18. Eludiora. SI, and Anifowose. FA, "Development of a Revenue Collection Model for Ubiquitous Advertising", under review, IJES International Journal of Emerging Sciences, 2011.
19. Anifowose. FA, "A Comparative Study of Gaussian Mixture Model and Radial Basis Function Frameworks for Voice Recognition", International Journal of Advanced Computer Science and Applications 2010, 1 (3): 1 - 9.
20. Konidala. MD, Robert. HD, Jianying. Z, and Kwangjo. K, "A Secure and Privacy Enhanced Location-based Service Transaction Protocol in Ubiquitous Computing Environment", Symposium on Cryptography and Information Security Sendai, Japan, 2004
21. Boddupalli. P, Al-Bin-Ali. F, Davies. N, Friday. A, O. Storz, O, and Wu. M "Payment Support in Ubiquitous Computing Environments", Proceedings of the Fifth IEEE Workshop on Mobile Computing Systems & Applications (WMCSA 2003), 2003
22. Zhang. L, Liu. Q, and Li. X, "Ubiquitous Commerce: Theories, Technologies, and Applications", JOURNAL OF NETWORKS, VOL. 4, NO. 4, JUNE 2009