



A Prototype Design for Secure e-commerce Payment System Model

Akinyede, R. O¹, and Akinyede, A. S²

^{1,2}Department of Computer Science, Digital Research Centre (DRC),
The Federal University of Technology, Akure, Ondo State, NIGERIA.

Abstract: *In the beginning, heaven and earth were created, God charged the man he had created to increase, multiply, dominate and have authority over everything He had created. As a result of this charge, man in a global perspective is becoming increasingly technology driven; and across every sector of society, from government to consumer and in every endeavour, from work to play, man invented technology is transforming the way we live. There is no better illustration of this manifestation than the financial services sector, because, for centuries, banks have provided the means for efficient business processes, by enabling and supporting the buying and selling of goods and services. However, as commerce grows, market grows; the level of transaction –buying and selling –increases and the rate at which money is being carrying about also increases. The security report shows that theft is on the high side, hence, there is need for a better payment method. In our research paper, we develop a prototype for a secure e-commerce payment system model.*

Keywords: *Mobile devices, ecommerce, payment system, and financial institution.*

I. INTRODUCTION

Mobile devices, such as cellular phones, Personal Digital Assistants (PDAs), or wireless laptop computers, have been considered as the accelerator that aids the emergence of payment method via wireless (mobile) communication technology. They offer the ability to access the Internet in order to perform electronic transactions (e-transactions). These mobile devices are connected via modems or wireless network adapters and this has greatly offers convenience to users who want to carry out e-transactions from remote distances at any time of the day. Performing e-transactions where at least one engaging participant is a mobile device is called mobile commerce (or *m-commerce*) and mobile payment (or *m-payment*). Just recently, e-transaction has been receiving considerable attentions, which have greatly increased its growth rate. The unfortunate thing is that this new technology, e-transaction using mobile devices in a wireless (mobile) network, has not fully taken off in Nigeria; and people have attributed this to some technical problems which we would like to categorise into two (2) as follows. The first problem concerns the issues regarding security of the payment system itself in a wireless (mobile) network. Though many researchers have designed protocols and deployed different cryptographic operations, many of them lack one or more transaction security properties that are important in a wireless network. The second is the technical limitations of the wireless (mobile) devices in terms of cost, power, latency, and bandwidth [1]. As a result of these, the research work tries to overcome the technical limitations and security considerations by exploring tools that provide for a standard subset of Java technologies for server. Java Micro Edition (Java ME) was used because of its ability to run on memory-constrained devices like cellular phones and PDAs, which the proposed designed system was based on. The system was grouped into three (3) parts: (1) The server module, which was responsible for controlling the application layer, where the data was stored in storage level (database), the payments actions and the control of processing. (2) The storage level using MySql relational database management system, this is where records would be arranged in the database associated with the server. (3) The client-side application, this is primarily the customer's level. It consists of classes and interfaces, the most important are the BankMIDlet class, which is the main application class that provides the communication operations and services. The MIDP application is packaged inside a Java archive (JAR) file, which contains the application class and resource files. With the tools mentioned above, an e-commerce model was developed for secure mobile payment system that allows mobile users to conduct e-transactions over wireless networks and also supports the related secured transactions between the merchant server, transaction host payment server and mobile clients. It also formalizes the interactions among the engaging participants and conditions to be satisfied by the system. An e-commerce performance indices, such as, the protocols and cryptographic technique was formulated, which would not only increase transaction performance when applying it to a mobile network but also specify transaction security properties of the system.

II. THE NIGERIA FACTOR

There are many factors that has made Nigeria a ready market for eCommerce payment system. Among them are the following:-

1. Population issue. Presently, Nigeria mobile phone users' population is 112,777,785 as at 2013 [2] and everyone is likely to use mobile phone to transact business in the nearest future.

2. Mobile phone's maturity. New development in mobile (phone) technology industry has increased its efficiency in terms of computational power, battery lifetime, memory, input mechanism, and graphical user interfaces that supports ecommerce payment system.
3. Bank's perspective. Most Nigerian banks believe in and thereby offer Internet banking services. They look for ways of increasing online financial transactions, which are cheaper for them to process, by persuading their customers to use ATM machines regularly. In some banks, they allow withdrawal of N150,000.00 per day. In addition, transactions using Internet banking can be up to N1 million. With ecommerce payment system, online financial transactions will increase, and this will help in differentiating them from their competitors.
4. Regulatory bodies. Nigeria regulates financial institutions through the Central Bank of Nigeria. These regulatory bodies try to integrate as many financial services as possible. The CBN adopted the following initiatives to reduce the cash intensity in the economy, encourage electronic payments and enhance the Nigerian Payments System [3]:
 - Fixed a daily cumulative limit of N500,000 and N3,000,000 on free cash withdrawals and lodgements by individual and corporate customers of banks respectively.
 - Disallowed encashment of third party cheques above N150,000 over the counter. Value for such cheques shall be received through the clearing house.
 - Directed that Cash-in-transit lodgements services rendered to merchant-customers by banks shall cease. However, customers could engage the services of CBN licensed CIT companies to aid cash movement to and from their banks at mutually agreed terms and conditions.
 - Stipulated that card schemes, foreign or local, shall not operate exclusive acquirer agreement or contract in Nigeria with effect from June 1, 2011. This is expected to facilitate interoperability of local currency POS transactions and increase its operational efficiency.

As the Japanese and South Korean experiences have shown, government participation is essential to successful deployment of the technology [4].

III. SECURE E-COMMERCE PAYMENT SYSTEM DESIGN MODEL

According to [4], atleast one of the participants involved in mobile payment solutions need to be connected to some back end payment server via either the short message service (SMS) or Global System for Mobile Communications (GSM)/code division multiple access (CDMA)-based technology. The proposed secure e-commerce payment system model extracted some of the features of payment protocol proposed in [5, 6, 7, 8, 9, 10, 11, 12, 13, 14]. From such systems, we can formally describe the secure e-commerce payment system as the combinations of the following:

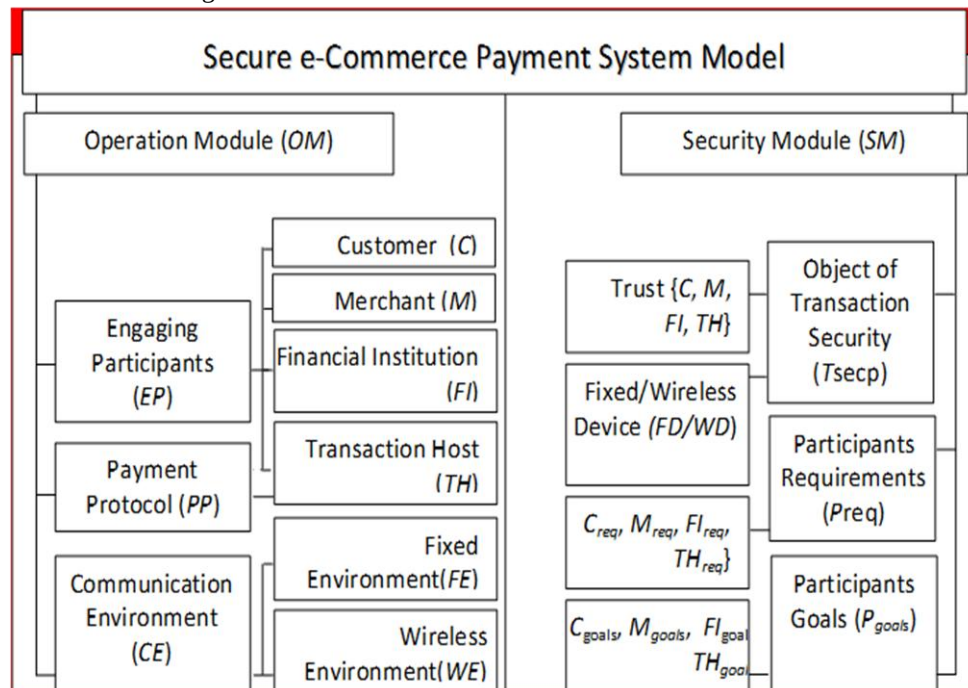


Figure 1: The Prototype of the Proposed Secure e-Commerce Payment System Model

With reference to figure 1 above, the payment system is an operational network - governed by laws, rules (protocols) and standards - that links bank accounts and provides the functionality for monetary exchange using bank deposits [15]. The payment system is the infrastructure (consisting of institutions, instruments, rules,

procedures, standards, and technical means) established to effect the transfer of monetary value between parties discharging mutual obligations. Its technical efficiency determines the efficiency with which transaction money is used in the economy, and risk associated with its use [16].

A payment system cannot be considered to be secured if it lacks any of the components of the above prototype and if it does not satisfies or meet the goals, Trust (*Trust*) that exists between the engaging participants, security and workability of the system.

Therefore, a secure e-commerce payment system P is hereby defined as the combination of the set of components of participants in P as shown in figures 1 above [9]:

$$P = \{OM\} + \{SM\} \quad (1)$$

Where

- P is the combination of e-commerce components, *operational module (OM)* and *security module (SM)* for buying and selling of goods or services offered through the Internet.
- The operational module (OM)'s components are the engaging participants (EP), payment protocols (PP), and communication environment (CE).
- The engaging participants (EP) are the customer C who wants to make purchase from merchant M . Merchant M who establishes sales on the Internet. He also establishes an account with an acquirer (M 's financial institution) A . Transaction host TH performs payment transactions on behalf of the issuer I and the acquirer A on the Internet side and on behalf of C and M on the banking private network side. Financial institution, FI , which can either be issuer I (C 's financial institution) or acquirer A (M 's financial institution). It performs payment clearing as a result of the request from transaction host. The transaction is performed under a banking private network. The security module (SM)'s components are the object of transaction security, T_{secp} , engaging participant requirement P_{req} , and participant goals, P_{goals} that is, the set of aims and goals of EP regarding the transaction being conducted
- The object of transaction security comprises of the Trust among the engaging participants. The communication environment can either be fixed or/and wireless networks. The fixed network, FN , needs fixed device, FD , to function while the wireless network, WN , needs wireless devices, WD , to function. The FD is a personal computer (PCs or laptops). FN represents a set of wired connections among the devices in FD . WD is cell phones, Personal Digital Assistants (PDAs), held by engaging participants, EP . FN represents the Local Area Networks (LANs) or Wide Area Networks (WANs). WN represents a set of wireless communication infrastructure in which the members in EP communicate with one another. WN is composed of a number of wireless links among the devices in WD . The examples of WN are wireless LANs, cellular networks and wireless WANs.

IV. SECURE E-COMMERCE PAYMENT SYSTEM MODEL PROPERTIES/ GOALS

According to [17, 18, 9], there are five (5) important safety properties/goals that are needed by any payment systems to be achieved and they are participant authentication, transaction privacy, transaction integrity, non-repudiation of transactions and transaction security properties. They must be satisfied as follows:

- Party authentication (P_{auth}) - Each engaging participant in the system must be able to authenticate the participant whom she is communicating with before committing to a payment. In addition, the customer will want assurance about the delivery of goods and services.
- Transaction privacy (T_{priv}): The confidential user's data on the mobile device as well as the device itself is protected from unauthorized use. The security mechanisms employed here include user authentication (e.g. personal identification number -PIN or password authentication), secure storage of confidential data (e.g. subscriber identity module -SIM card in mobile phones) and security of the operating system.
- Transaction integrity (T_{intgty}): Each engaging participant's received messages are not altered during transmission.
- Non-repudiation of transactions ($NonRepofTrans$): This security property guarantees that a transaction cannot be later denied by one of the participants involved.
- Transaction security (T_{secp}): It makes it possible to identify the possible points or nodes of attack (e.g. so as to prevent diversion of fund or stolen of payment information).

Trust = trust that exists between the *EPs*.

Philosopher Sissela Bok wrote: "...trust is a social good to be protected just as much as the air we breathe or the water we drink. When it is damaged the community as a whole suffers; and when it is destroyed, societies falter and collapse." [19]. In principle, trust among participants can be represented straightforwardly, as a function from pairs of participants to trust levels,

$$Trust = Participant\ a \rightarrow Participant\ b \rightarrow TrustDegree \quad (2)$$

Where, *Trust* is a function which associates to each principal *b* the value of *a*'s trust in *b*.

Trustworthiness is a word 'noun' derived from trust. According to [20], trustworthiness can be evaluated through three (3) dimensions, reputation, performance and appearance. Therefore, trustworthiness can hereby be defined as the set the three components mentioned above.

Trustworthiness =

$$\{P_{reputation}, P_{performance}, P_{appearance}\}$$

(3)

V. CONCEPTUAL SCHEMA OF THE PAYMENT SYSTEM

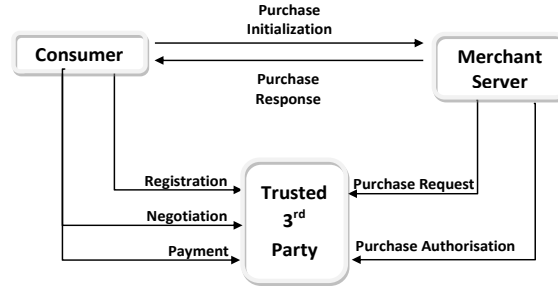


Figure 2: Conceptual Schema of the Mobile Payment System

According to [21], the conceptual schema of the above design, figure 2, shows that payment system is merely registering and forwarding the authorized and validated payment transactions [22, 23]. Payment system life-cycle includes initialization of request, authorization of payment request, and commitment of payment request [24]. There are four principal participants here, and they are: the consumer, who subscribes to a service, merchants, who provide product or service to consumers, payment service provider, which controls the payment process and the trusted third party that administers the authentication of other players and the authorization of payment settlement. As reported in [25], different roles can be merged into one party and act as one player. For example, payment service provider, which controls payment process and trusted third party, can act as the same participant.

VI. SECURE E-COMMERCE PAYMENT SYSTEM MODEL -IMPLEMENTATION TECHNIQUES

We introduced authentication into the design, and a Click will request the Customer to enter his Account Number and Password. If the entry is successful, a Welcome Page is displayed through the *LoginServlet*.

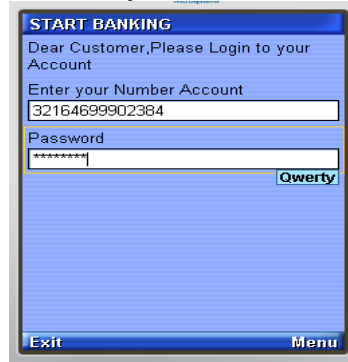


Figure 3: Login Interface

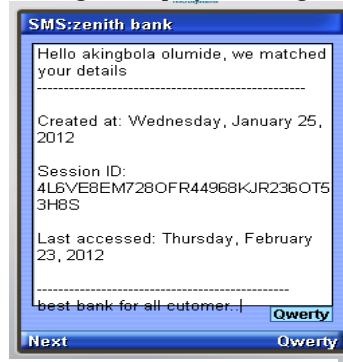


Figure 4: Authentication Page

The *LoginServlet* is responsible for customer *Cs* logging authentication (Figure 3), it decrypts the customer *C* account number and password from the http request and matches the details of customer *C* from database and generates welcome message with customer *C* session key (Figure 4). Then, it allows the customer *C* access to the system.

The security analysis - Login Authentication.

When *U* wants to access the *CA*, he carries out the following steps.

1. *U* submits the computed *ID*, *yId* and *Id* and generates random number *a*, such that $a \in [1, n - 1]$.
2. Calculates $Q_i = q_i P$ and then $p_i = h(Q_i)$, $X = q_i K_{pub_ib}$ and $g = h(ID || Id || p_i || T_i)$
3. Select random number *a*, calculates $Q_i = q_i P$ and then $p_i = h(Q_i)$, $X = q_i K_{pub_ib}$ and $g = h(ID || Id || p_i || T_i)$.

4. U computes the hashed password $Y = yId$, dynamic identity $dID = p_i H(ID_i)$ encrypted and sends message to CA server
5. Decrypt $p_i H(ID_i)$
6. Verify both certificate & signature

User interface

The system has the merchant and customer interfaces. Merchant's goods are uploaded using the merchant interface. At the same time, items to be sold are made available for shopping. What happens here is that when the customer chooses the desired merchant, the items that are available in his store will be displayed. Then, the customer selects the needed items from the item list and adds them to the cart. When icon "Add Item" is clicked, item ID, item name, price, quantity and cost can be seen on the table. The purchase total amount is shown under the table. After pressing "OK" button, the purchasing goods quantity will be added to the remaining goods or items (see figure 4). Payment will be initiated as follows:

Verify PIN

IF PIN is correct THEN

$\{mp\ A: [[PI, signed], CID]]\}$

ELSE terminate

$C \rightarrow M: \{\{Ordered\ Items, Tr.ID, M.ID\}K^{-1}\}K^{secret}$

$M \rightarrow C: \{Item, M.ID, Tr.ID, ID_{CA}\}K^{secret}$

$C \rightarrow M: \{\{PaymentOrder, Tr.ID, M.ID\}K^{-1}\}K^{secret}$

The merchant, M , processes the order and starts the payment phase by forwarding the payment instructions to the transaction host, TH . Note that the TH will obtain transaction data via the network and processes the payment transaction on behalf of a financial institution FI that holds the account of the customer C for the payment method selected.

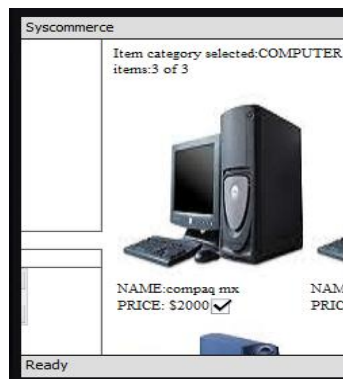


Figure 5: Selected Items and the Prices Displayed

In this case, mobile payment is selected.

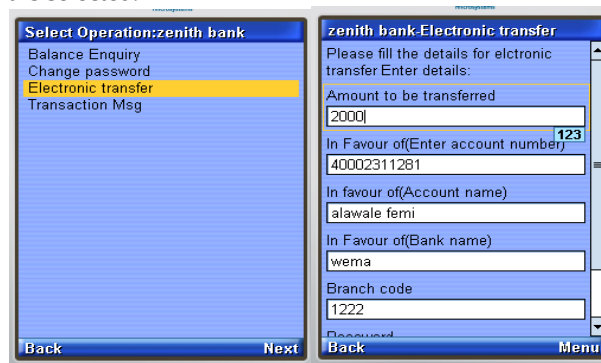


Figure 6: Payment Interface

Figure 7: Fund Transfer Page

On a Click on an option "Electronic Transfer" will make the electronic transfer interface to be displayed as shown in Figure 6. The system will request the customer C to fill the details of the amount to be transferred. It will also request the merchant name, bank account number and customer C 's PIN. The execution of *EtransferServlet* will take the following steps: (1) Verification of customer C 's PIN (2). If correct, then, the Transfer of fund to M 's account. The *EtransferServlet* is also responsible for decrypting the confidential data

received in an encrypted form and send ACKnowledgement to the customer *C* with transaction id. In summary, customer *C* gives the details of the fund to be electronically transferred (see Figure 7).

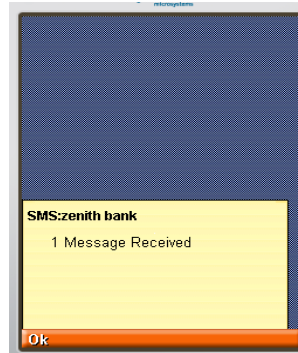


Figure 8: Payment Interface

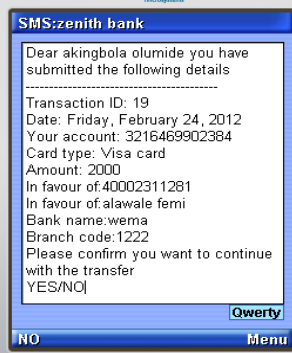


Figure 9: Fund Transfer Page

After submitting the Electronic Transfer details to the bank, the banks will send an SMS through *SMSServlet* to the customer confirming the transfer as shown in figures 8 and 9. Note that the *SMSServlet* is used to generate an SMS to the customer *C* for transaction confirmation. It automatically retrieves the cell phone number of the customer *C* that it sends SMS for confirmation to and each of the transaction is identified by a *Transaction.ID*. Transaction Identification (*Transaction.ID*) is a one-time randomly generated code that uniquely assigned to the customers by their financial institution to perform online secure financial transactions. It uniquely identifies each of the transaction performed by the system.

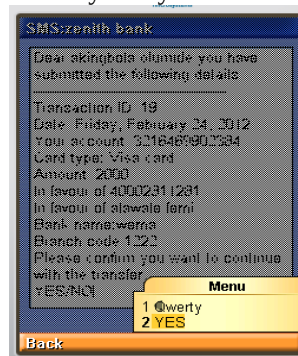


Figure 10: Transfer Confirmation Page

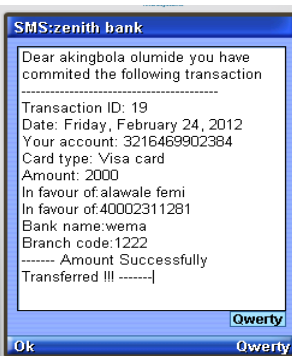


Figure 11: Fund Transferred Page

The *ConfirmServlet* receives the response of the Customer confirmation SMS and takes action accordingly as shown in Figures 10 and 11. If customer *C* has chosen “YES” then it commits the transaction on the payment transaction host *TH* server and generates ACKnowledgement message to the customer *C*. If the customer *C* has chosen “NO” then it CANCELled the transaction and generates cancellation message to the customer *C*.

VII. CONCLUSION

This paper has suggested a prototype for secure ecommerce payment system model. The user-side ecommerce payment system in mobile environment that takes users -clients as principal players. Functionality and performance testing of the proposed system was carried out. The result obtained from this research may serve as a basis for payment system designers and implementers to design and implement a secure payment system for e-commerce in a wireless (mobile) network in Nigeria.

REFERENCES

- [1] Akinyede, R. O. (2012), Modelling a Secure e-Commerce Payment System for Wireless (Mobile) Network in Nigeria, Ph.D Project Report, Department of Computer Science, FUT, Akure.
- [2] ITU, (2013), ICT Facts and Figures. <http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx>
- [3] CBN, (2014), Payment system. <http://www.cenbank.org/Paymentsystem/>
- [4] Rajesh, K. B. and Narayan, R., (2009), The Digital Wallet: Opportunities and Prototypes. IEEE Computer Society.
- [5] Kailar R., (1995), Reasoning about Accountability in Protocols for Electronic Commerce, Proceedings of the 1995 IEEE Symposium on Security and Privacy, (1995) 236-250, IEEE Computer Society Press
- [6] Teppo H., (2002), A System for Secure Mobile Payment Transactions, Helsinki University of Technology, Department of Computer Science and Engineering, January 2002.
- [7] Rolf, O., (2003), Security technologies for the World Wide Web.. 2nd ed., (Artech House computer security library) ARTECH HOUSE, INC. 685 Canton Street Norwood, MA 02062.

- [8] Kungpisdan S., Srinivasan B., and Phu D. L., (2004), A Secure Account-based Mobile Payment Protocol, Proceedings of the International Conference on Information Technology: Coding and Computing, Vol. 1, Las Vegas, USA, 2004, pp. 35-39.
- [9] Kungpisdan, S., (2005), Modelling, Design, and Analysis of Secure Mobile.
- [10] Payment Systems. A Thesis Submitted for Fulfillment of the Requirements for the Degree of Doctor Philosophy. Faculty of Information Technology Monash University.
- [11] Akinyede, R. O., (2005), Development of a Payment System for e-Commerce and banking industry in Nigeria. A Thesis Submitted for Fulfillment of the Requirements for the Degree of Masters of Technology, Computer Science, The Federal University of Technology, Akure, Nigeria.
- [12] Tellez J. and Sierra J, (2007), Anonymous Payment in a Client Centric Model for Digital Ecosystem, IEEE DEST, 2007, pp. 422-427.
- [13] Akinyede, R. O. and Adewale, O. S., (2007), Development of a Payment System for Electronic Commerce and Banking Industry in Nigeria, Journal of Computer Science and its Applications, Nigeria, Vol. 14; 65-74.
- [14] Fun, T. S, Beng, L. Y., Roslan, R., and Habeeb S. H., (2008), Privacy in New Mobile Payment Protocol. International Journal of Computer and Information Science and Engineering. <http://www.waset.org>.
- [15] Akinyede, R. O, Adewale, O. S and Alese, B. K (2010), Securing Mobile Payment Systems: Using Personal Identification Number (PIN) Method, in proceedings of the 1st International Conference and Workshop on Software Engineering and Intelligent Systems (SEIS 2010), Covenant University, July 5th – 9th, 2010, Ota, Nigeria, Vol I, 23-33.
- [16] Bruce J. S., (2012), Payment Systems: Design, Governance and Oversight", Central Banking Publications Ltd, London, 2012, p.3.
- [17] Biago B. and Massimo C., (2001), The Oversight of the Payment Systems: A Framework for the Development and Governance of Payment Systems in Emerging Economies. The World Bank, July 2001, p.
- [18] Ahuja, V., (1996), Network and Internet security. Massachusetts- Academic Press Inc (Essay) Srce Filmbay IV 08 .html. http://books.google.ca/books/about/Network_and_Internet_security.html?id=GNtFAQAIAAJ&redir_esc=y
- [19] Park, D. G. Boyd, C. and Dawson, E., (2001), Micropayments for wireless communications. Lecture Notes in Computer Science, 2015:192(205).
- [20] Gizmodo (2012), How to Trust Your Neighbors in a Networked World. <http://gizmodo.com/5887528/how-to-trust-you-neighbors-in-a-networked-world>.
- [21] So, M.W.C. and Sculli, D., (2002), The Role of Trust, Quality, Value and Risk in Conducting e-Business. Industrial Management and Data Systems. Vol. 102. No. 9, 503–512.
- [22] Jan Ondrus, Y. P., (2004), "An Architecture for Mobile Payments and Couponing in the Retail Industry," in *17th Bled eCommerce Conference*, Slovenia, 2004.
- [23] Traummüller R., (2002), Information Systems: The e-Business Challenge, Springer, 2002.
- [24] Rotterdam, A. S. L., (2008), "Inter-consortia battles in mobile payments standardisation," *Electronic Commerce Research and Applications* , vol. 7, no. 2.
- [25] Timo Saarinen, M. T. A. (2005), Managing Business In A Multi-Channel World: Success Factors For E-Business, Idea Group Pub, 2005.
- [26] Wen Chen Hu C.-W. L. W. K.,(2005), Advances in Security and Payment Methods for Mobile Commerce, Idea Group Publishing, 2005.