International Journal of Sciences

Research Article Volume 7 – February 2018 (02)

Developing a secured Mobile-Agent-Based Electronic Commerce Using Crypto-Steganography

Araoye O. I.[1],Adewale O.S.[2],Alese B.K.[2],Akinyede O. R.[2]

[1]The Federal Polytechnic, Ado-Ekiti, Nigeria
[2]The Federal University of Technology, Akure, Nigeria

Abstract: Mobile agent is gaining attention in the research community because of its potential to replace traditional client-Server application in computer network system. Mobile agent has the ability to migrate autonomously from one server to another server as specified in its itinerary in computer network. Areas where mobile agent profit includes network management, information retrieval and electronic commerce. Mobile agent can be delegated to carry out all stages that are involved in electronic commerce such as Product brokering, Merchant brokering, Negotiation and Purchase. However there are security vulnerability issues with mobile agent system such as the need to ensure confidentiality of information of the agent from malicious parties, integrity of the data of the agent and non-repudiation from parties involves in the transactions. Security measure by agent developers has been mobile cryptography. This research combines Elliptic curve cryptography (ECC) and Steganography known as crypto-steganography to secure its agent. The agent was developed using PHP 5.0, Javascript, HTML, Wampserver and MySQL. The system was tested on a local area network with six computer systems, one of the computers represent client and the other five as servers. Performance evaluation was carried out to test for execution time and workload effect on the system. The result was compared with the existing secured agent-based electronic commerce systems in term of response time. The result shows that the proposed security is faster than RSA but a little slower than ECC only. A trade off was observed between a more secured system and response time of the system.

Keywords: Mobile agent, Electronic Commerce, Crypto-Steganography, Security, Client-Server

1.0 Introduction

Mobile agents are programs bundled with data and execution state that can suspend execution, migrate to other computers connected over a network, and resume execution there (Bradshaw, 1997). Mobile agent is a form of code mobility which is an aggregate of code on demand and client-server. A mobile agent can migrate from its home, move on to the site of the required information resource and perform a locally custom-retrieval task. Only the results are transmitted back to its home (Robert, *et al.*, 2001).

Moreover, the mobile agent can carry on a task while the connection to destination server is temporarily lost and then continue once the link returns to send the found result. Mobile agent can exploit the high processing power available in the server machines by shifting the computations into the server side. Client-server is an alternative to mobile agent; several researches had been done to compare the two paradigms in (Antonio, *et al.*, 1997; 2001; Giovani, 1998; Mario et al., 1997 Gian, 1998; Mario and Gian, 1998).

Mobile code is an alternative to client/server. In the client sever paradigm, an application is divided into two processes, a client process running locally that asks for services and a server process on a remote site that give services to the client.

A limitation of the client-server model is that the client is limited to the operations provided at the server. If the client needs a service that a particular server does not provide, it must find a server that can satisfy the request by sending out more messages to other servers. Mobile agents provide a solution for the dynamic environment of the mobile devices because they do not rely on server operations. The mobile agent appears to tackle significant problems whether in wired or wireless communication such as disconnection operations, increased network traffic and others. Mobile agents offer advantages such as autonomous delegation of task, off-line principle, low

Published at: http://www.ijsciences.com/pub/issue/2018-02/
DOI: 10.18483/ijSci.1550; Online ISSN: 2305-3925; Print ISSN: 2410-4477

Araoye Olalekan (Correspondence)
araoyek@yahoo.com
+

communication cost and bandwidth. However, security problem is a major challenge of mobile agent especially when money is involved.

2. Literature Review

The Internet has become an essential business platform for trading, distributing and selling products between organizations, among organizations and consumers, and even between consumers. This has brought e-commerce to an entirely new level (Barnes and Vidgen, 2000; Berners-Lee, 1999). E-Commerce has grown in popularity over the years, mainly because people find it convenient and easy to buy various items comfortably from their office or home. (Sougata, *et al.*, 2012)

Shopping activities over the internet have been growing in an exponential manner over the last few years. One of such environment in which there is a prominent job for the agents would be internet-shopping in which a customer is able to delegate agents the responsibility of buying instead of shopping himself (Kwang, *et al.*,2000).

One of the advantages of internet commerce, particularly during a holiday season, is that it eliminates the need to wait in long lines or search from shop to shop for a particular item. (Sougata, *et al.*, 2012). Agent- based e-commerce helps to save more time on the internet searching from one shop to another shop for a particular item at a lower or affordable price.

Agent-based e-commerce has received much attention in the last two decades (Fasli, 2007). According to Bahrammirzaee, *et al.*, (2013), this is due to the fact that agent based e-commerce offers many advantages with respect to traditional e-commerce, such as (semi-) autonomous behavior so that agents perform transactions on behalf of their users.

There are no proper mechanisms to facilitates electronic transaction and automate shopping process on behalf of customers. So a human buyer is still responsible for gathering commodity information from multiple suppliers on internet, making decision about each commodity, then making the possible selection and ultimately performing the e-payment. So it takes lot of time to buy things over the internet Richard and Jose, (2009).

Maes, *et al;* (1999) identified electronic commerce stages for which mobile agent can be dispatched and delegated. These are stated below

a. Product brokering: Involves getting information from several merchants about a certain product that the user is looking for acquiring.
b. Merchant brokering: Consists in evaluating a set of alternatives, discovered in the previous stages in order to decide where to make the purchase.
c. Negotiation stage: The final terms of the transaction are set.
d. Payment and Delivery: The goods are delivered against currency or its electronic equivalent

2.1 Security Issues in Mobile Agent-Based Electronic Commerce

Certain security threats that are possible to a mobile agent executing on a remote host in electronic commerce were mentioned in Dave and Bart, (2004).

a. Modification of other offers: A malicious host can alter the offers made by a precious host in order to sell its product. This problem has to deal with integrity of information supplied by individual host. Once information is tampered with its integrity is impaired.
b. Deny of an offer: A particular host can deny an offer which it has previously made. Non-repudiation is a requirement that must be met in an agent based system. A malicious host could try to steal the private key of the mobile agents. If it succeeds, then it can sign arbitrary document and probably get credit card information.
c. Denial of service attack: A lot of denials of service attack are possible. The easiest one for a malicious host is simply is not to execute the mobile code. This can be resolved using multiple agents.

Hohl, (1996) identified various types of attacks they may be carried out by malicious hosts as Spying out and manipulating codes, data and control flow, Incorrect execution Returning wrong result of system calls to agents and Masquerading.

Mir and Borrell, (2003) identified two security problems of mobile agent system.

a. The protection of host against agents (host security problem)
b. Protection of agents against host (Agent security problem).

3. System Design and Development

The design of the secure agent-based electronic commerce was contained in Araoye, et al., (2017). The various interfaces of implementation were shown in Figure 1 to Figure 5.

3.1 The Home Page

The home page in Figure 1 is the first page that is shown when the network address of the agent is clicked. New users are to first register their details which include Full Name, Phone-number, User Name, Password, Payment card-number. New users

are expected to confirm their password. After entering the required details, the user now click the register button which will take him or her to the next page as shown in Figure 2

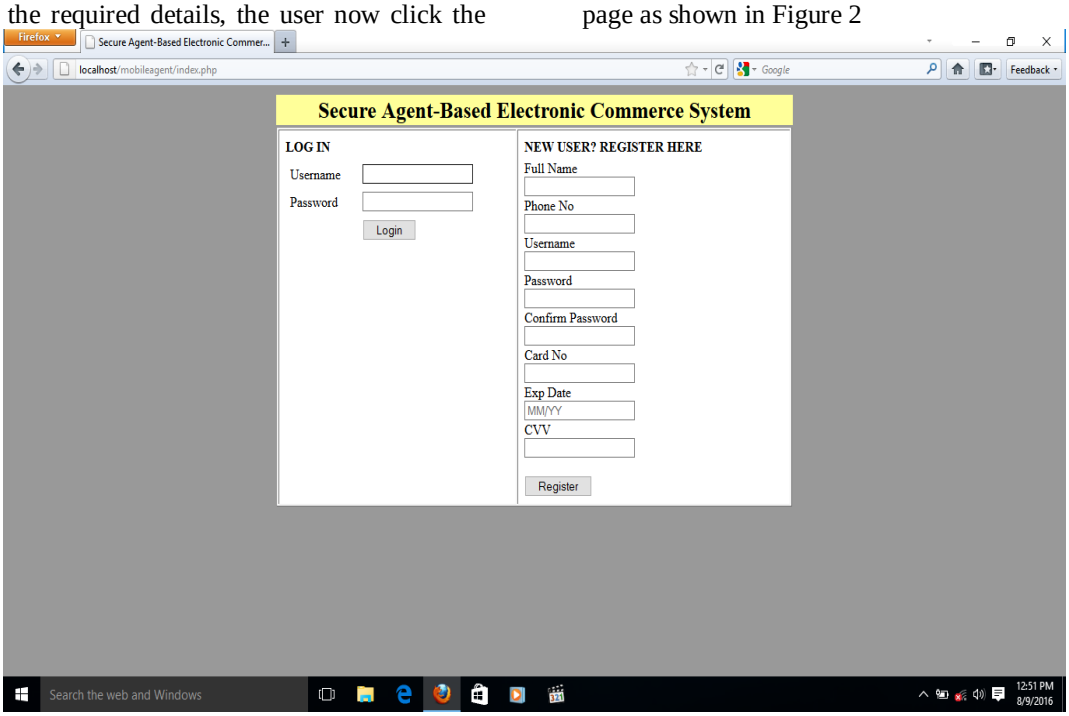

Figure 1: The home page

3.2 Login Page

Existing users are expected to enter their user's Name and password to get to this page from the home page. The user's name will be displayed on welcome page as shown in Figure 2

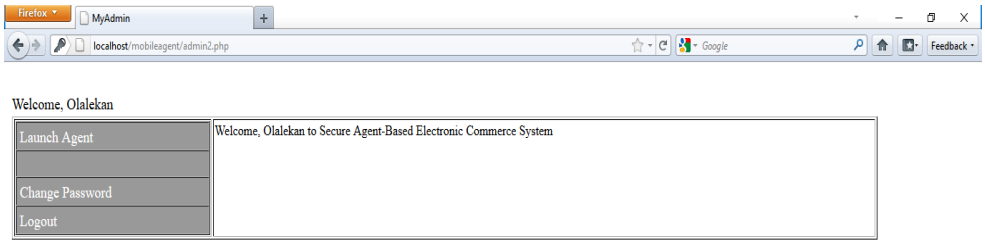

Figure 2: Agent's Login Page

3.3 Agent's Lunch Page

After successful log-in, the user is allowed to select items of his choice. In this page, a single item is selected and corresponding image is displayed. After selection, lunch Agent button is clicked to lunch the agent into network for shopping process as show in Figure 3.

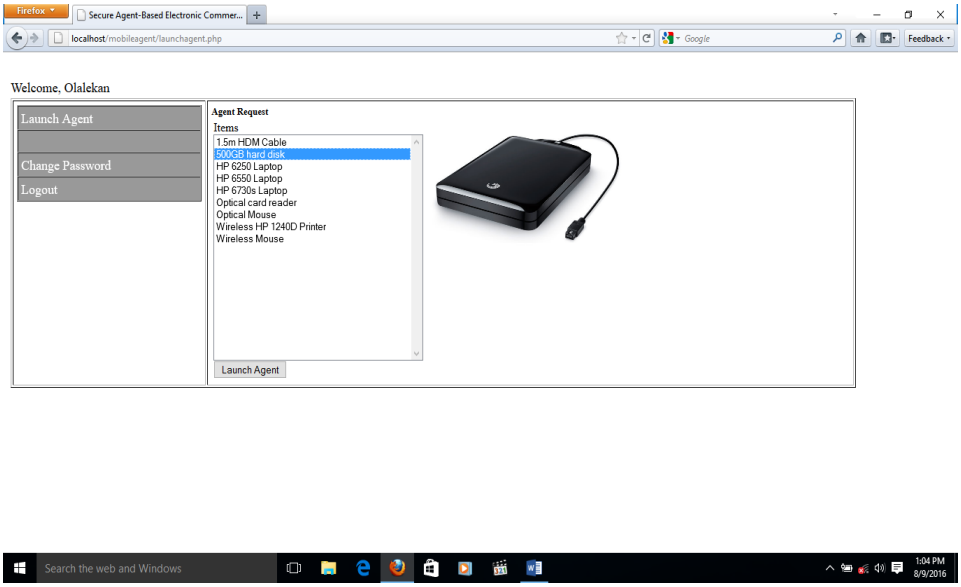

Figure 3: Shopping for an Item

3.4 Agent's Report

The agent is launched and returned with item price collected from each store. The agent also display the shop that sells at the minimum price to test for its intelligence and then the invoice number for the item purchased from the shop that sells at the minimum price as shown in Figure 4.

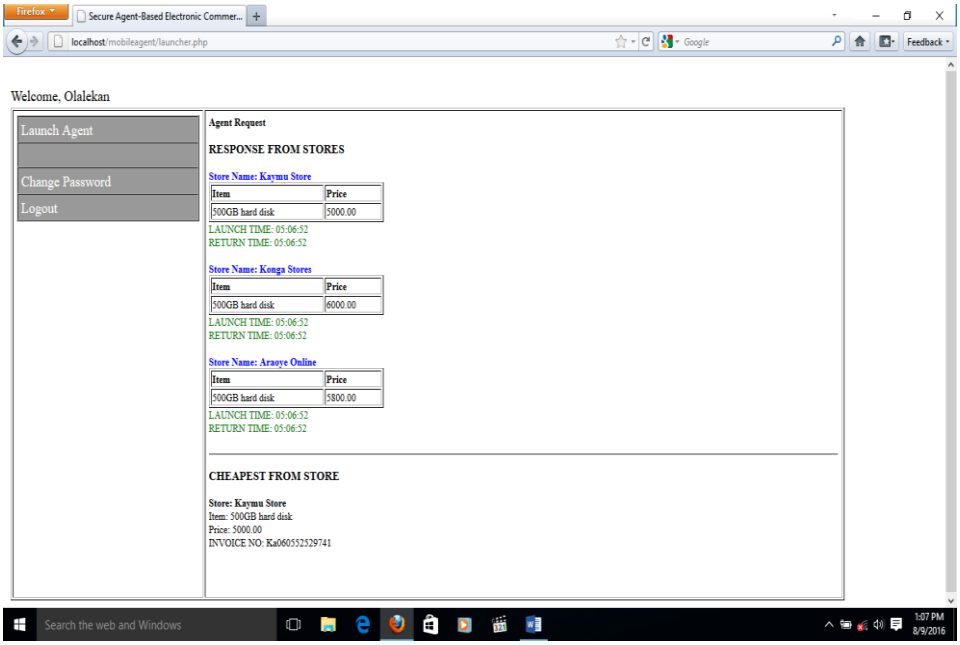

Figure 4: Agent's Report

4. Experimental Results and Discussion

The developed Secured Agent-Based Electronic Commerce was tested with six systems. One as a client and the remaining five as servers. The arrangement is shown in Figure 5. The quarry of the agent is represented by q while the replies from the server is represented by r and are labeled as r1, r2, r3, r4 and r5 from server1 to server5 respectively. The movement of the agent is indicated by directional arrow and the object on the arrow represents the agent.

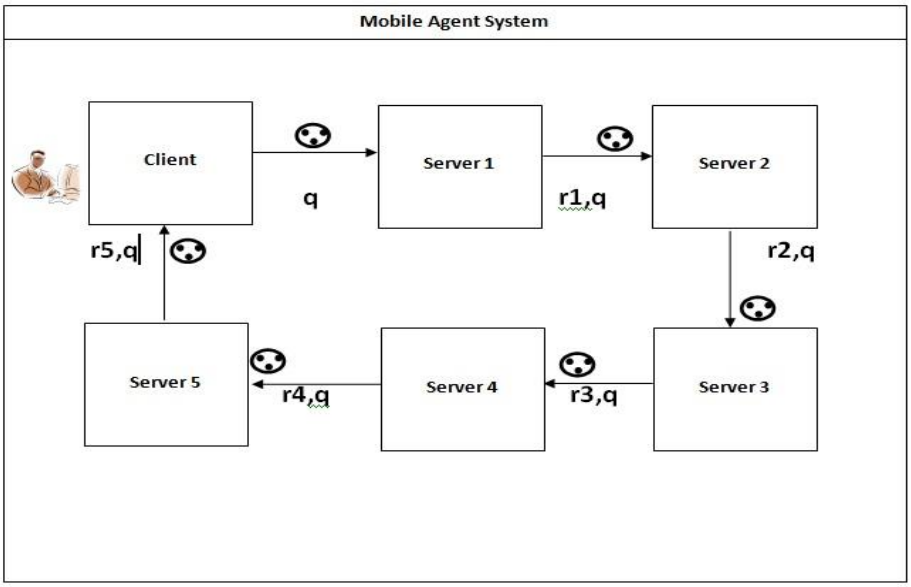

Figure 5: Diagram Showing the System Arrangement for the Experiment.

4.1 Execution Time Result

In this section the results obtained from the experiment carried out is presented. The Execution time for the agent to migrate and return was measured for each server. The servers were labeled as S1, S2, S3, S4 and S5. Agent was lunched three times for each item selected and average execution time was calculated as shown in Table 1.

Table 1: A Table Showing Average Execution Time for Each Server Host

Host Server(Label)	Execution Time(t) (E_T) Seconds			Average Execution Time (AE_T) Seconds
	E_1	E_2	E_3	
1	9	9	10	9.33
2	34	33	34	33.66
3	62	62	62	62
4	118	119	119	118.66
5	339	339	339	339
Total Average Execution Time (TAE_T)				562.65

Three experiments were carried out as E1, E2 and E3 on each server labeled as S1, S2, S3, S4 and S5.
Average Execution Time (AE_T) for each server = $(E_1+E_2+E_3)/3$
Total Average Execution Time (TAE_T) = $AE_{T1}+ AE_{T2}+ AE_{T3}+ AE_{T4}+ AE_{T5} = 562.65$
Average Execution Time Estimated for a Single Server $AE_T S = 562.65/5=112.53$
Total Average Execution Time (TAE_T) in minutes = 562.65/60 = 9.3775 Minute
Graphical representation of average execution time for each server S, from S1 to S5 is shown in Figure 6.

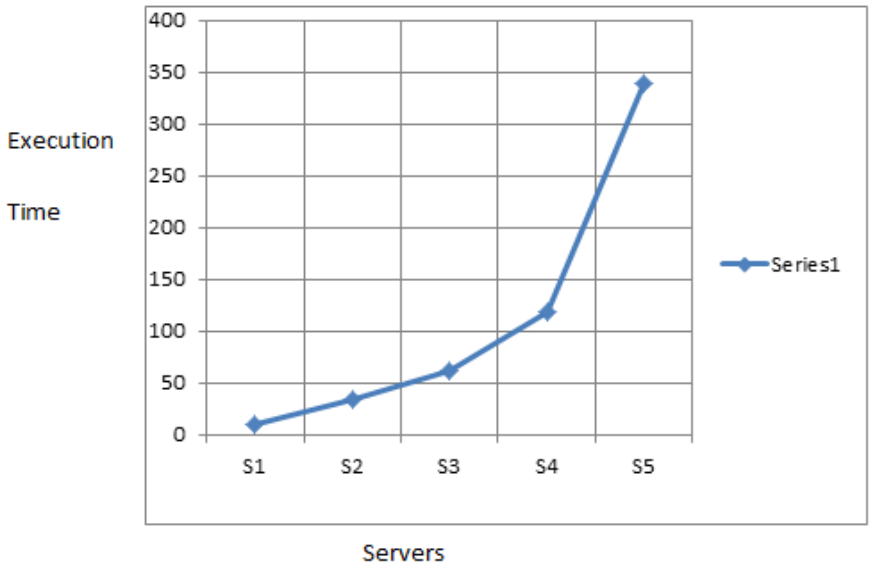

Figure 6 : Average Execution Time Graph

4.2 Workload Results

Workload effect on the system performance was carried out by varying the number of items selected for each server. Items were selected for each server at random ranging from one to five items and agent was lunched to measure its return time. Two experiments E1 and E2 were carried out for a particular selection and average execution time AVE was calculated for each server. The result obtained is shown in Table 2

Table 2: Workload effect on the system performance.

No Of Item	S1 (Sec)		S2 (Sec)		S3 (Sec)		S4 (Sec)		S5 (Sec)	
	E1	E2	E1	E2	E1	E2	E1	E2	E1	E2
1	**9**	**9**	**94**	**94**	**63**	**63**	**119**	**119**	**339**	**339**
2	**9**	**9**	**87**	**89**	**62**	**62**	**119**	**119**	**339**	**339**
3	**9**	**8**	**94**	**93**	**62**	**62**	**119**	**117**	**279**	**339**
4	**8**	**9**	**97**	**94**	**72**	**62**	**118**	**118**	**339**	**340**
5	**10**	**9**	**94**	**94**	**63**	**63**	**119**	**118**	**339**	**279**

Average Execution Time (AE_T) = (E1+E2)/2 for a number of items selected for each server is shown in the Table 3
Table 3 Average Execution Time for a number of items selected on each server.

No of items selected	S1 AE_T (Sec.)	S2 AE_T (Sec.)	S3 AE_T (Sec.)	S4 AE_T (Sec.)	S5 AE_T (Sec.)
1	**9**	**94**	**63**	**119**	**339**
2	**9**	**88**	**62**	**119**	**339**
3	**8.5**	**93.5**	**62**	**118**	**309**
4	**8.5**	**95.5**	**67**	**118**	**339.5**
5	**9.5**	**94**	**63**	**118.5**	**309**

4.3 Result Evaluation with the Existing Systems

The proposed system was compared with the existing systems in Kannamal and Iyengar, (2007) that used RSA only and Sougata *et al.*, (2012) that used ECC. Table 5 shows difference in results in terms of average execution time or response time. The average response time shows that RSA takes a longer time than the proposed system while ECC is a little faster than the proposed system which combined ECC and steganography. Crypto-steganography may be a little slower in average response time than ECC, it is considered more secured than ECC only. There is a trade-off between security and response time.

Table 5: Proposed system compared with existing secured agent systems

Authors	Security used	Average Response time in (seconds)
Kannamal and Iyengar(2007)	RSA	255.29
Sougata *et al*.,(2012)	ECC	101
Proposed	ECC combined with steganography	112.53

The research also evaluated the system as a client-server; server 5 was taken as a case study
Average Execution Time for server5= 339 seconds
For five tours, Average Execution Time = 339x5 = 1695 seconds = 28.25 Minutes+ Likely delay in input (D) seconds as a client server.
Total Average Execution Time (TAE_T) for mobile agent as shown in Table 5 = 562.65 seconds = 9.3775 Minutes. No delay as input is done once.
Difference in TAE_T between mobile Agent and Client Server = 1695+D-562.65 = (1132.35+D) seconds = (18.8725+D) minutes
From the above result, it shows that mobile agent technology is a promising technology in time and network management.

5. Conclusion

Security has been a challenge to most distributed applications because of hackers and intruders that are hanging all over the world. Effort should be intensified in the area of security to harness all the potentials of mobile agent technology. This research has been able to successfully show how cryptography and steganography a technique that is referred to crypto-steganography can be combined together to improve the security of mobile agent for most of our agent-based applications especially the electronic commerce. This research has provided an eye opener to agent developer to properly address the issue of security. The research proved time-benefit of mobile agent over the existing client-server system.

6. References

1. Antonio, C., Gian, P. P. and Giovanni, V. (1997), Designing Distributed Application with a Mobile Code Paradigm, Proceedings of the 19th International Software conference on Software Engineering, Seattle, USA, 22-32.
2. Araoye, O. I., Adewale, O. S., Alese, B. K. and Akinyede, O. R. (2017), North Asian International Journal of Sciences, Engineering & IT, Vol3, Issue 11
3. Bahrammirzaee, A.,Chohra, A.,Madani,K.(2013), An Adaptive Approach for Decision MakingTactics in Automated Negotiation. AppIntell. doi:10.1007/s10489-0130434-8.
4. Barnes, S. J.,Vidgen, R.T., (2000), An Integrative Approach to The Assessment of E- Commerce Quality, Working Paper. http:/www.webqual.co.uk/ papers/webqualbookshop.pdf.
5. Berners-Lee T. (1999), in: Weaving the Web, Orion Business, New York.
6. Dave S. and Bart P. (2004): Secure e-Commerce Using Mobile Agents on Untrusted Hosts, COSICInternal Report.
7. Gian, P. P. (1998), Understanding, Evaluating, Formulating and Exploiting Code Mobility, Ph.D Thesis, Politeccnico di Torino, Italy.
8. Giovanni, V. (1998), Mobile Code Technologies, Paradigms and Applications, Ph.D Thesis, Politecnico di Milano.
9. Hohl, F. (1998),A Model of Attacks of Malicious Hosts Against Mobile Agents, Proceedings of the ECOOP Workshop on Distributed Object Security 4th Workshop on Mobile Object Systems: Secure Internet Mobile Computations, INRIA, France,105 -120.
10. Kannamal, A. and lyenger, N. Ch.S.N. (2007, A Model for Mobile Agent Security in E- BusinessApplications, International Journal of Business and Information, 2(2),185-198.
11. Kwang, H. J., Tessuo, K. A., Nairo,S. (2000), Design and Implementation of an Agent Based Grocery Shopping system, IEICE, Vol. E83- D, No.ll.
12. Mario, B. and Gian, P. P. (1998), Evaluating the Tradeoffs of Mobile Code Design Paradigms in Network Management Applications, Proceedings of the 20th International Conference on Software Engineering, Kyoto, Japan, 146-155.
13. Mario, B., Silvano, G. and Gian P. P. (1997), Exploiting Code Mobility in Decentralized and Flexible Network Management, Proceedings of The First International Workshop on Mobile Agents, Berlin, Germany.
14. Richard, S., and Jose, G.O. (2009), Security Analysis of an Agent-Mediated Book Trading Application, International Journal of computing and ICT Research, Special Issue 3(1).
15. Sougata, K., Arifit, D., Zhang, Y., Li, L. and lyengar, Ch.S.N. (2012), Agent-Based Secured e-Shopping UsingElliptic Curve Cryptography, International Journal of Advanced Science and Technology, 38, 93-115.