IRJIF. I.F. : 3.821

North Asian International Research Journal of Sciences, Engineering & I.T.

ISSN: 2454-7514 Vol. 3, Issue-11 November-2017

THE DESIGN OF A SECURED MOBILE AGENT-BASED ELECTRONIC COMMERCE USING CRYPTO-STEGANOGRAPHY

ARAOYE O. I.[1], ADEWALE O.S.[2], ALESE B.K.[3], & AKINYEDE O. R.[4]

[1] The Federal Polytechnic, Ado-Ekiti, Nigeria. E-mail:araoyek@yahoo.com

[2],[3],[4] The Federal University of Technology, Akure, Nigeria.

ABSTRACT

Electronic commerce is a driving force for Information Technology (IT). Mobile agents profit from this development, and offer substantial advantages such as autonomous delegation of task, off-line principle, low communication cost and bandwidth for certain electronic commerce applications in return. Electronic Customers are curious in searching for an electronic shop that can offer them goods and services at the affordable price. The present electronic commerce transaction allows at a time, interaction between a customer and a shop, a technology that can be referred to as client-server system. In a situation whereby a Customer is interested in searching for information from many electronic shops at a time is not possible with this technology. Mobile agent technology allows a customer to interact with many electronic shops at a time, such a shop must also be agent based. The customer sends its agent from his own customer agent-based platform to electronic shops that are also agent based. Interaction takes place between Customer-Agent (CA) and Shop-Agent (SA) for various transactions that are involved. A major requirement to build confidence in mobile agent technology is the availability of adequate security mechanisms. The security concern is how to ensure integrity, confidentiality, authenticity and non-repudiation for the data involved in the transaction. The existing security technique that had been deployed for agent-based electronic commerce is cryptography. This paper considers hybridization of cryptography and steganography which formed crypto-steganography to secure agent-based electronic commerce application.

Keywords: ***Electronic Commerce, Mobile-Agent, Electronic-Shop, Steganography and Cryptography***

1. INTRODUCTION

Mobile software 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).

As an executing program, a mobile agent is made up of code, data and execution state and is embedded with some intelligence and the ability to autonomously migrate across the network (Arekete *et al;* 2013).

A feature being frequently attributed to mobile agents is autonomy, the ability to perform certain tasks without guidance or intervention by a human user (Araoye, 2005).

Mobile agent is a form of code mobility which is an aggregate of code on demand and client-server. Mobile agent is yet to be received in the internet community, since issues such as reliability and security are yet to receive developer's confidence (Giovani, 2004). However because of available tools, mobile agents have become extensively popular not only in the research community but also in industrial projects (Christian, *et al.*, 2001). One of the most attractive applications of mobile agents is the notion of distributed information processing. This is shown in the mobile computing scenarios where users have portable computing devices with only intermittent, low bandwidth connections to the main network. 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, 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. The client and server processes must communicate with each other in order to carry out their tasks successfully. Communication is done by means of message exchange. There are at least two problems with the client/server paradigm.

a. It has a high network bandwidth requirement due to the large number of messages exchanged
b. It usually requires users to respond to computation results interactively, under different situations. Neither the client nor server would make decisions for users autonomously.

2. LITERATURE REVIEW

Mobile agents have been vastly considered in many application areas such as e- commerce, network monitoring and management, distributed information retrieval, telecommunications, remote device control and configuration,

Internet etc. (Paulo *et al.*, 2000, Jin, *et al.*, 2009; Boutaba and Xiao, 2002).

The diagram in Figure 1 and Figure 2 show how mobile agent has been able to reduce communication cost over traditional client-server system.

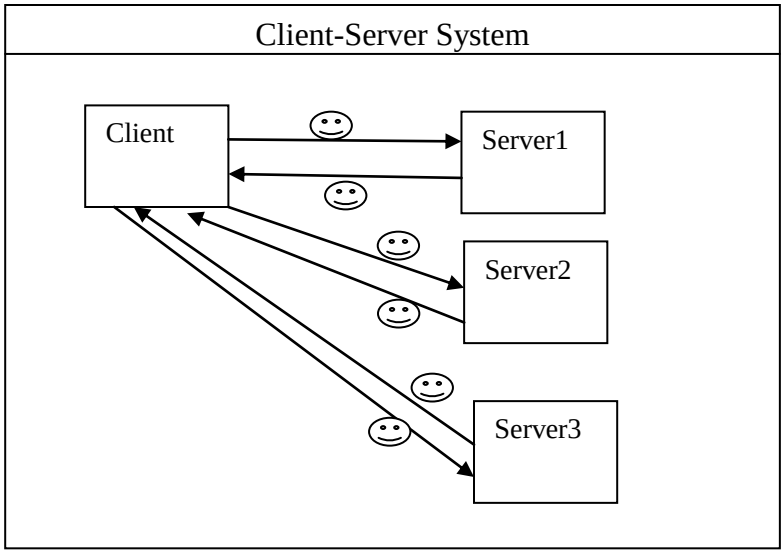

Figure 1: Client-Server System

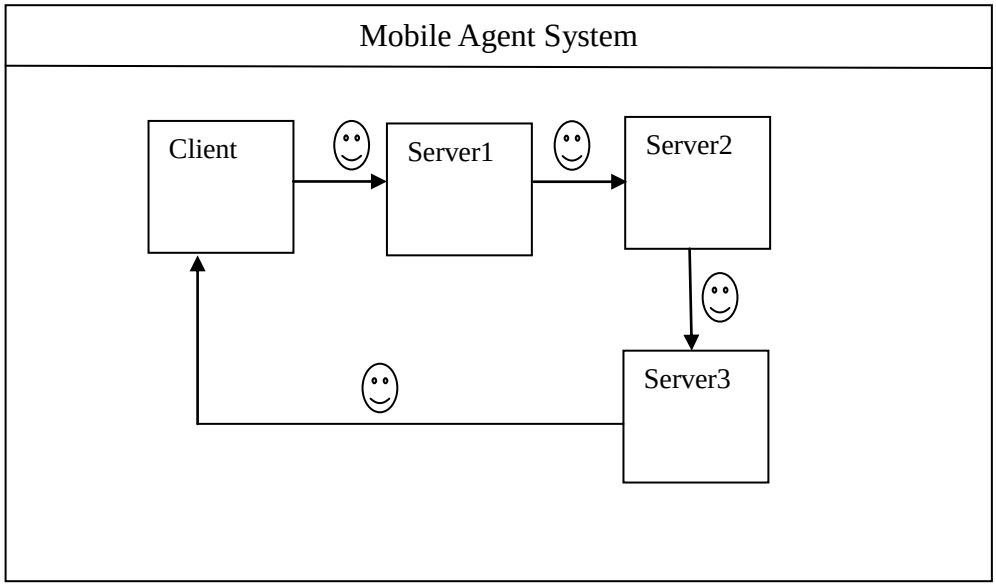

Figure 2: Mobile Agent System

If each arrow in the figure represents one message sent, it can be seen that using a mobile agent actually saves two messages in a network of three servers compared with using client-server. In general, if there are n servers, (n-1) messages can be saved using mobile agents.

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.

Mobile agents may contribute in three ways to electronic commerce according to Christoph *et al.*, (2000) which are:

a. Optimizing decisions in electronic markets show increasing market transparency resulting in superior resource allocation (Malone, *et al.*, 1989; Bakos, 1991). However, the ideal of increased market transparency cannot be realized at low cost in an interactive electronic marketplace such as online shops on the WWW. Mobile agents provide economical and fitting technical means for autonomous, fast and exhaustive information research. Thus, mobile agents can lead to almost optimized decisions for the allocation of goods.
b. Providing mobility, flexibility and autonomy tasks in an electronic commerce environment are often repetitive and sometimes time critical, for instance monitoring of stock prices. Mobility of agents minimizes communication delays. Flexibility of agents by cloning itself enables almost unlimited scalability regarding the amount of input. The advantages of this autonomous flexibility hold for customers as well as merchants
c. Increasing market efficiency for all parties to conclude mobile agents can increase efficiency by saving time and costs, for instance profit margins of intermediaries. These potential savings together with increased convenience

are the added value of mobile agents in an electronic commerce scenario.

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.

Paulo, *et al.,* (2000) identified security requirements in each stage of an electronic transaction as specified in Table 1

Table 1: Security Requirements in Each Stage of Electronic Commerce (Source: Paulo et al.,2012)

Stages	Security Requirements
Product Brokering	▪ Offers made by a host should not be readable by other hosts ▪ It must not be possible for hosts to modify offers without being detected. ▪ Host must not be able to delete or add false offers in the name of others ▪ Hosts must not be able to disclose the decision making logic of agents on how acquisition are made. ▪ Host may not be able to read sensitive information maintained by the agent
Merchant Brokering	▪ The state of the agent and data transported by it must not be spied or altered by the host. ▪ The code of the agent must not be spied or altered while

	it is executing. ▪ The flow of execution of the agent should not be spied or altered while it executing
Negotiation and Purchase	▪ The information obtained in the previous stages should not be modifiable without being detected. ▪ The agent should be able to give selected sensitive information to the host in order to make the purchase, being assured that the information is not disclosed to third parties. ▪ The owner of the agent actually gets the asset bought and a receipt is issued as a proof of the purchase

Sougata, *et al*., (2012) indentified security features for the agent based electronic commerce as follows.

a. Confidentiality: This is to make sure that the information of the customer's agent or Merchant agent cannot be read by a malicious host or other agent making information unintelligible to an intruder.

b. Integrity: This is divided into two according to Vikas, (2010)

i. Integrity of transaction: When money is sent form Customer to Merchant, the value of that money must not be changed; it must be maintained. Debit and credit amount must not change to avoid inconsistency.

ii. Delivery of product: The customer must receive the product according to specification and in good condition. It is undesirable that customer pay the money without receiving the product.

c. Availability: It ensures that end system (host) and data should be available whenever required by the authorized user.

d. Accountability: The identities of all users are assured and are made responsible for their action. (White, 2011)

e. Authentication: It ensures that the people using the computer are the authorized users of that system before transacting.

f. Non-Repudiation:- It makes sure that none of the Customer or Merchant can deny communication or other action regarding information or resources at a specific time. Non-repudiation in e-commerce can be viewed in three forms according to Ritu and Gaurav, (2010).

i. Non-repudiation of origin: The ability to identify who sent the information originally versus which intermediary forwarded it.

ii. Non-repudiation of receipt: The ability to identify that the customer receives the receipt of his payment in a manner that cannot be denied by the customer.

iii. Non-repudiation of delivery: Making sure that good and services get to the buyer in a way that the buyer cannot deny it.

g. Copy protection: This feature ensures protection from unauthorized copying of intellectual information (Salah, *et al.*, 2006).

There are a number of solutions proposed by Tschudin, (1999) to protect agents against malicious hosts, which are:

a. Establishing a closed network: limiting the set of hosts among which agents travel, such that agents travel only to hosts that are trusted.
b. Agent tampering detection: using specially designed state-appraisal functions to detect whether agent states have been changed maliciously during its travel.
c. Agent tampering prevention: hiding from hosts the data possessed by agents and the functions to be computed by agents, by messing up code and data of agents, or using cryptographic techniques

Page and lndrawan, (2004); Sander and Tschudin, (1998) proposed the following solutions to protect mobile agent respectively.

a. Protected agent state when is basically signing and encrypting of agent states based on public-key cryptography.
b. Mobile cryptography for code integrity. Code integrity should be maintained

Paulo, *et al;* (2000) stated that security of agents for e-commerce must be viewed in a realistic and pragmatic way.

a. Some host in the network can be trusted
b. More than one agent can be used in order in order to build a secure mobile agent environment.

Steganography is the art and science of covert communications among trusting parties, where the confidential message is embedded imperceptibly about an innocent looking cover signal so that nobody apart from the sender and intended recipient can detect the existence of the hidden data. (Gabriel, 2015). It is also defined according to Neil and Sushil, (1998) as the art of hiding information in digital media through the techniques of embedding hidden messages in such a way that no one except the sender and the intended receiver(s) can detect the existence of the message.

The main goal of steganography is to hide the secret massage or information in such a way that eavesdroppers are not able to detect it (Neil and Sushil, 1998) .Another goal of steganography is to send safely in a completely undetectable manner. The various forms of data in steganography can be audio, video, text and images e.t.c. Hiding data is the process of embedding information into digital content without causing perceptual degradation (Chen, *et al.*, 2008).

3. SYSTEM DESIGN

The design of a secured agent-based electronic commerce is conceptualized in Figure 3. In this design, the hybridization of cryptography and steganography is shown at the client side where the private key of the agent and the cipher text of credit card details are hidden in the item image. Mobile agent which is referred to as customer agent (CA) is launched into the internet with the aid of a launcher. CA moves to the internet with its private key and credit card details which shall be used for decryption and buying purpose respectively. Movement of CA and its communication with the stationed agent which is called shop agent (SA) is represented by the directional arrows.

When CA visits a shop to collect item price, there is a communication between it and SA that represents the shop owner. In order to allow for confidentiality, SA gives out the cipher text of the item price using the public-key of the agent which it initially possessed. By this provision, information provided by the current shop cannot be seen by the previous shop.

When CA has visited all the shops in itinerary, it performs extraction process to obtain its private key hidden in the item image for decryption purpose of all the cipher text of the item prices in order to obtain their plain text form.

CA compares the various prices collected and moves to the shop that sells at the minimum price. The SA of the shop that sells at the minimum price checks if the CA has sufficient credit for the purchase of the item. If the CA has enough credit, then CA goes home with invoice number from the shop. The agent owner can check for the list of item price collected by CA to know if the agent has performed the required function. The complete flowchart of activities is detailed in Figure 4.

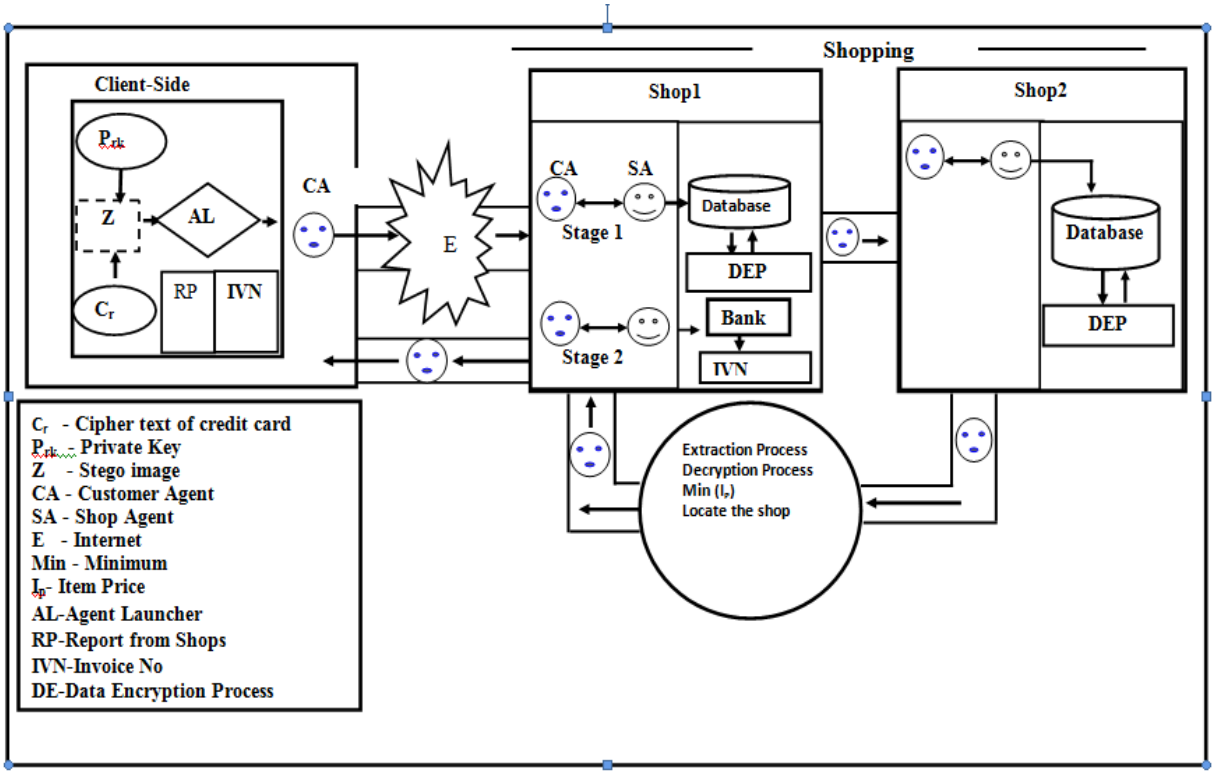

Figure 3: Architectural Design of a Secured Agent-based Electronic Commerce Using Crypto-steganography

In the security design, credit card information $C_{r\inf o}$ is encrypted using elliptic curve Cryptography algorithm E and public key of the agent P_{bk} for encryption to get a cipher text C_r of the credit card details to avoid the information from being seen by any of the shops to be visited by the agent.

$$C_r = E(P_{bk}, C_{r\inf o}) \quad (1)$$

The cipher text C_r is further hidden in an item image M to produce a stego image Z_1 using embedded function F and key K. This forms a new security technique known as crypto-steganography.

$$Z_1 = F(M, C_r, K) \quad (2)$$

Steganography technique helps to hide the presence of credit card details from the various shops to be visited by the agent.

To extract the cipher text C_r from Z_1, extraction function F^{-1} and key K is applied on Z_1

$$C_r = F^{-1}(Z_1, K) \quad (3)$$

To get plaintext $C_{r\inf o}$ of the credit card details by the agent, decryption function E^{-1} andprivate key P_{rk} of the agent are applied

$$C_{r\inf o} = E^{-1}(P_{rk}, C_r) \quad (4)$$

In order for the agent to travel with its private key so that it will not be seen by any other party involves in the transaction, the private key is also hidden in the item image

$$Z_2 = F(M, P_{rk}, K) \quad (5)$$

The agent represented its owner in a network for the purpose of searching for the price of an item from different agent- based electronic shops and then purchased the item at a shop that was selling at minimum price.

Let the shops to be visited by the mobile agent in itinerary be $S \in \{S_1, S_2, S_3, ..., S_n\}$; the unit price $P \in \{P_1, P_2, P_3, ..., P_n\}$ and quantity ordered from each shop for each item be X. The agent buys from a shop given that the total cost $U \in \{U_1, U_2, U_3, ..., U_n\}$ is minimum. That is,

$$MinU = Min\{P_1X, P_2X, P_3X, ..., P_nX\} \quad (6)$$

The mobility behaviour of the agent is described by a destination vector $S = (S_0 ..., S_n)$. For the $i-th$ interaction, the agent moves to destination location S_i. Thus migration takes place between $(i-1)-th$ and $i-th$ interaction only if $S_i \neq S_{i-1}$.

Let $J = (I_i, ..., I_n)$ be a sequence of interactions, the i-th interaction is described by

$$I_i = \{R_{i,} m_{i.} B_{qry,} B_{res,} \sigma_i\} \quad (7)$$

where R_i is the remote location with which the communication should take place. Each communication consists of m_i (local or remote) procedure calls with request size, $B_{qry,}$ reply size $B_{res,}$ and selectivity σ_i.

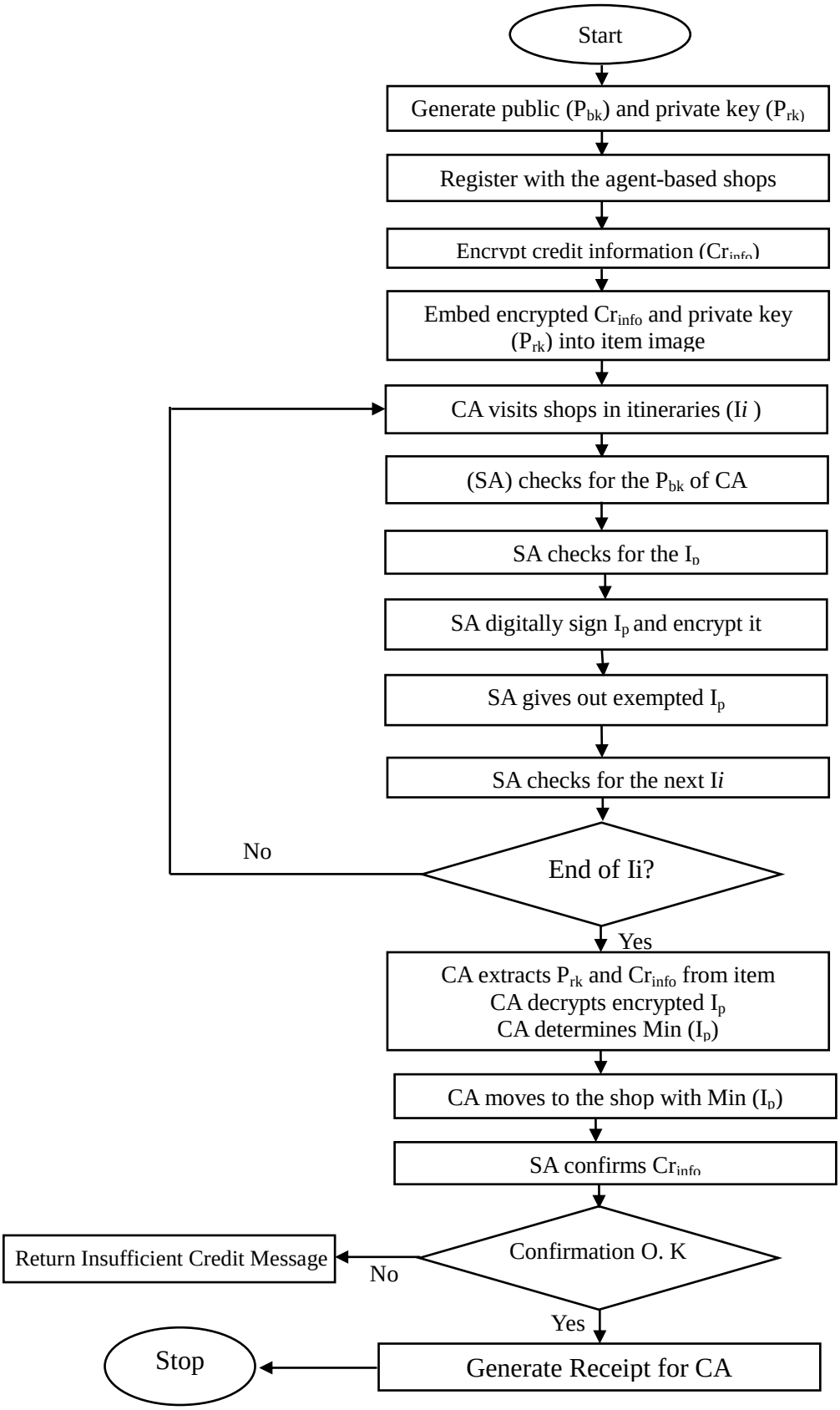

Figure 4: Flowchart Design of a Secured Agent-based Electronic Commerce using Crypto-Steganography

4. CONCLUSION

Cryptographic method had been a major security method being proposed by researchers on mobile agent based applications. This design had critically looked at a way to combine cryptography and steganography which formed crypto- steganography to secure agent-based electronic commerce application. Credit card details of customers are very important to be secured if the agent is to be given full autonomy as specified in the design. Also the private key of the agent needed to be more secured since the agent is to travel with the key for the purpose of decryption of the encrypted data collected from different shops. The design had successfully shown how credit details and private key can be hidden in an item image to be purchased which will enhance the security of the agent.

5. 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, 4(1), 22-32.
2. Araoye, O. I. (2005), Market Information Agent System(MIAS): Security and Reliability Issues, M.Tech Thesis, The Federal University of Technology, Akure, Nigeria.
3. Arekete, S. A., Akinyokun, O. C., Olabode, O., Alese B. K. (2013), Design of Mobile Agent for Monitoring Activities of Users, Computer Engineering and Intelligent Systems, ISSN2222- 1719(Paper) ISSN2222-2863(online), 4(3), 12-25.
4. Bahrammirzaee, A., Chohra, A., Madani, K.(2013), An Adaptive Approach for Decision Making Tactics in Automated Negotiation. AppIntell. doi:10.1007/s10489-0130434-8.
5. Bakos, J. A. (1991), Strategic Analysis of Electronic Marketplaces, MIS Quarterly 11 (4) 295-310.
6. Boutaba, R. and Xiao J. (2002), Network Management: State of the Art, Proceedings of the IFIP17th World Computer Congress, -TC6 Stream on Communication Systems, The State of the Art, 127-146.
7. Bradshaw, J. M. (1997), Software *Agents*, MIT Press, New York.
8. Christian, E., Peter, B. and Wilhelm R. (2001), Some Thoughts on Migration Intelligence for Mobile Agents, Technical Report, Friedrich-Schiller University, 1, 9.
9. Christoph, B., Volken, R. and Ralph, M. (2000), Perspectives on Electronic Commerce with Mobile Agents, Fraumhofer Institute for Graphische Datenverarbeitung, RundeturmstraBe, Darmstadt {busch/ Vroth} igd.fgh.de. 6, 642783
10. Dave S. and Bart P. (2004): Secure e-Commerce Using Mobile Agents on Untrusted Hosts, COSIC Internal Report.

11. Fasli, M. (2007), Agent Technology for E-Commerce, Wiley, New York.
12. Gabriel, J. A. (2015), A Multivariate Polynomial-Based Post-Quantum Cryptographic Systemfor Security of Information over Enterprise Network, A Thesis in The Department of Computer Science, Submitted to The School of Postgraduate Studies, In Partial Fulfilment of The Requirement for The Award of Doctor of Philosophy, The Federal University of Technology, Akure, Ondo State, Nigeria.
13. Gian, P. P. (1998), Understanding, Evaluating, Formulating and Exploiting Code Mobility, Ph.D Thesis, Politeccnico di Torino, Italy.
14. Giovanni, V. (1998), Mobile Code Technologies, Paradigms and Applications, PhD Thesis, Politecnico di Milano.
15. Giovanni, V. (2004), Mobile Agent: Ten Reasons for Failure, International Conference on Mobile Data Management, IEEE, 298.
16. Hohl, F. (1998),A Model of Attacks of Malicious Hosts Against Mobile Agents, Proceedings of the ECOOP Workshop on Distributed Object Security and 4th Workshop on Mobile Object Systems: Secure Internet Mobile Computations, INRIA, France,105 -120.
17. Jigadam, V. K, Venkateshwar, R. (2013), Authentication of Secret Information in Image Steganography, International Journal of Latest Trends in Engineering and Technology, 3(1), 97-104 ISSN; 2278-621X
18. Jin, G., Ahn, B., and Lee, K. D. (2009), A Fault-Tolerant Protocol for Mobile Agent, Proceedings of International Conference on Computational Science and Its Applications. Springer, 993–1001.
19. Kannammal, A. and Iyengar, N. Ch.S.N. (2008), A Framework for Mobile Agent Security in Distributed Agent-Based E-Business Systems, International Journal of Business and Information, 3(1).
20. Maes, P., Guttmann, R., Moukas, A. (1999), Agents that Buy and Sell, In Communications of the ACM 42, 81-91.
21. Malone, T. W., Jates, J., and Benjamin, R. I. (1989), The Logic of Electronic Markets, Harvard Business Review, 67, (3), 166-172.
22. 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.
23. Mir, J. and Borrell, J.(2003), Protecting Mobile Agent Itineraries. In Mobile Agents for Telecommunication Applications (MATA), Lecture Notes in Computer Science, Springer Verlag, 2881, 275–285.
24. Neil, F.J. and Sushil, J. (1998), Exploring steganography: seeing the unseen, IEEE, 26- 34
25. Page, J., Zaslavsky, A. and Indrawan, M. (2004), A Buddy Model of Security for Mobile Agent Communities Operating in Pervasive Scenarios, ACM International Conference Proceeding Series;

Proceedings of the Second Workshop on Australian Information Security, Data Mining and Web Intelligence, and Software Internationalisation, (54),1725.

26. Paulo, J. M., Luis, M.S., and Joao, G. B. (2000), Security Mechanisms for Using Mobile Agents in Electronic Commerce, Departmento de Engenharia Informatica, Universidede de`Coimbra, Portugal.
27. 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).
28. Robert, S. G., David, K. and Ronald, A. P. (2001), Mobile Agents Versus Client-Server Performance, Scalability in an Information Retrieval Task, Proceedings of the Fifth IEEE International Conference on Mobile Agents, Atlanta, Georgia, 229-243.
29. Salah, I. K., Darwish, A., and Oqeili, S. (2006), Mathematical Attacks on RSA Cryptosystem, Journal of Computer Science, 656-671
30. Sander, T., and Tschudin, C. F. (1998), Protecting Mobile Agents against Malicious Hosts, In: Giovanni Vigna, ed., Springer, Mobile Agents and Security, LNCS 1419, 44-60.
31. Shazia, Y., Khalid, H. and Rashid, J. Q. (2012), Cryptography Based E-Commerce Security: A Review, IJCSI International Journal of Computer Science Issues, 9 (1)
32. Sougata, K., Arifit, D., Zhang, Y., Li, L. and lyengar, Ch.S.N. (2012), Agent-Based Secured e-Shopping Using Elliptic Curve Cryptography, International Journal of Advanced Science and Technology, 38, 93-115.
33. Vikals R. (2010), E-commerce Security Using PKI Approach, International Journal on Computer Science and Engineering, (IJOSE), 2(5), 1439-1444.