Journal of Computer Science 3 (5): 329-334, 2007
ISSN 1549-3636

Secure Mobile Trade Agent

Musbah M. Aqel, Sattar J. Aboud and Mohammed A. AL-Fayoumi
Middle East University for Graduate Studies, Department of Computer Information Systems
Amman, Jordan

Abstract: E-commerce on the internet has the ability to produce millions of transactions and a great number of merchants whose supply merchandise over the internet. As a result, it is difficult for entities to roam over every site on the internet and choose the best merchandise to trade. So, in this paper we introduced a mobile trade agent that visit the sites to gather and evaluate the information from merchant servers and decide to trade goods on behalf of the user. We observed that the combination of public key cryptosystem with distributed object technology make this proposed scheme more secure and efficient than the already existed schemes.

Key words: Mobile trade agent (MTA), e-commerce, public key encryption scheme.

INTRODUCTION

Data presented on the internet are so great; it becomes difficult for entity to roam every site on the internet[1], and analysis it to decide where it is the best to purchase or to vend goods on behalf of the user. Therefore, people want e-agents who can visit every site on the internet and trade on their behalf[2-4].

In this paper we introduce MTA that has the aptitude to visit each site on the internet to gather related information and employ it to decide to trade goods on behalf of the user. We will illustrate that the Authorization Server (AS) could be employed to authorize transactions and pay for merchandise purchased via the MTA. In addition, The MTA has the aptitude to roam various other merchant servers and implement at these servers. But once it is used at unknown server. it is liable to attacks from such servers[5, 6]. Therefore, we illustrate that the MTA is used as distributed objects, can logically roam a various network servers, but, physically sustain protected within the defensive environments of the Agent Depository (AD). The MTA is given more security via ciphering the messages between entities and other agents on the internet using the public key encryption scheme

Mobile trade agent: The MTA is certainly one of the rapid growing issues of information technology[7, 8]. It is employed and roamed for uses as e-commerce, information system, etc. The MTA can be considered as a program that stimulates a human being by performing certain things that another entity might do[9]. Also the MTA is an independent program that able to manage its decision relied on its intelligence, in seeking for one or more goals[10]. However, there are more than one kind of agent is available. The simplest one is the static agent that moves through a considerable amount of information and show apart from this information as handy information to another entity. An instance of this is an agent that scrutinize and evaluates each new e-mail, and directs it to the right agent for respond[11]. The MTA have the aptitude to roam around many sites on the internet to achieve its jobs and send back its results. The MTA would usually collect and evaluate information from a considerable number of sites on the internet, and show apart from this information to another entity[12]. An instance of such an agent is that a bookshop that roams every virtual bookstore, and show to its entity a list of the available books and the best price offered for every one[13]. This MTA could also work as middlemen for users, for instance, a sign on means can sign on also many systems easing the entity from entering the password for each system[11]. Also, such MTA has several benefits. For instance, it can let traders to reply rapidly to market opportunities and provide them with the competitive prices that are necessary in present e-commerce day. Also, the MTA has the aptitude to roam various sites in the internet, evaluate the information at every site and decide which merchandise must be traded at each site. In addition the MTA is an independent program, and it can determine where to move on a network and what goods to trade without human participation. Also, the MTA must be an

Corresponding Author: Musbah M. Aqel, Middle East University for Graduate Studies, Department of Computer Information Systems, Amman, Jordan

intelligent to pay the cost of merchandise purchased to merchants by using smart cards. Also, it should be possible to discontinue the MTA from migrate the sites on the internet and order it to return back to the centre. However, the centre is not the user client computer since user does not all the times use the same client computer and could not even be logged-in whilst the agent roams the sites on the internet. Therefore, we present the idea of the Agent Depository (AD) in which all agents are kept and interiorly sustained and controlled. The MTA is, by no means, stored at a user client computer, but the AD holds all MTAs. The user of the MTA is not passing its MTA straight to any server. It gives order to the AD to simulate the MTA and order it to migrate the sites in the internet. One from the security benefit of the AD is that it will simulate the MTA for its authorized the user, and it will initially authenticate the MTA user prior to consider any orders from the MTA entity[14]. The MTA should be able to pay for the merchandise purchased and accept payment for merchandise vends[15]. We develop a scheme in which the MTA can supply a merchant the user smart card number. The merchant uses this data to demand payment from the Authorization Server (AS) which plays the bank role. The user smart card number is encrypted using a public key encryption scheme. The AS ensures that merchants only reclaim payment for merchandise purchased by the MTA and confirms that merchants receive the funds when the MTA purchases merchandise from them. Figure 1 illustrates the role of both AS and AD in the program. The figure also illustrates the steps of the scheme and shows the secure payment method that is employed; in addition, the figure shows also the other security matters in the scheme such as authentication and secures messages. Also figure 1 show that the MTA roams the sites and trades goods at three variants merchant servers on the internet. The following steps illustrate the proposed MAT scheme which is a mobile agent with the aptitude to roam different sites on the internet, evaluate the information at every site and to decide where it is the best to trade goods on behalf of the user. However, this MTA is smart since it can determine when to trade merchandise and when to visit the next server with no human involvement. Note that prior to the user at client computer issue any orders to its MTA, it should be authenticated by the AD. For example, any authentication scheme says an encrypted password can be employed.

- The user composes its MTA to using it by supplying it with a list of e-commerce rules and a listing of merchants to roam and to trade goods with them.
- The user directs its MTA to begin roaming the sites on the internet and select the best goods available employing the rules provided. But at any time the user can suspend from its client computer and let the agent to trade alone.
- The AD directs the MTA to visit the sites on the internet which results the MTA to move to $server_1$
- The MTA start trades with merchant at $server_1$. The MTA should be able to pay for merchandise purchased. So we will illustrate how the transaction is authorized and payment provided. The payment scheme should be secure by employing the public key encryption scheme
- The MTA provides $server_1$ its user smart card number. This data is encrypted via the user using AS public key and user secret key. The AS holds a copy of the encrypted data of the user smart card number. This denotes that just the AS can recover the document and it can only be the user that generates the document
- The MTA generates the document showing that goods are purchased. This data is encrypted using AS public key and MTA secret key. This denotes that just the AS can recover the document and it can only be the MTA that generate the document. The MTA transmits this document to the merchant at $server_1$
- Merchant at $server_1$ wants the AS to permit the transaction and guarantee payment. The MTA should provide the merchant at $server_1$ the user financial record with a letter showing what goods are purchased. The AS will just permit the transaction if merchant at $server_1$ and the MTA can consent that they are traded specifically the corresponding goods for the identical price. To work this merchant at $server_1$ creates the same report regarding the merchandise vended as the MTA operated. This report is encrypted using $server_1$ secret key and AS public key. The merchant at $server_1$ transmits the three reports to the AS for validation
- The AS recovers every document employing AS secret key, $server_1$ public key and MTA public key. It verifies whether merchant at $server_1$ reports and the MTA reports regarding goods traded are matching. The AS would usually be a bank which will verify whether user has enough money and if this is true, the transaction is allowed and the AS will transfer the funds to the merchant at $server_1$. The AS can be acted as a bank and shall utilize a traditional fund transfer method to guarantee that payment is transferred to the merchant at $server_1$

bank account. At this step the transaction is completed.

- The MTA visits new sites on the internet and e-commerce with new merchants. If necessary, the AS should permit the transactions.
- The user directs the MTA by the AD to end marketing and return to the centre; it is also possible to develop a new MTA which can normally ends marketing when some requirements are encountered; for instance, a particular number of merchandise are purchased.
- The AD bides for the MTA to come back and direct it to go home that is to the centre.
- The user could check the MTA basket to see the types of goods traded.

Protection the MTA: When the MTA executes at unknown merchant server, it is susceptible to attacks from that server. So, in this section, we will illustrate how the MTA is secured with distributed objects. However, There are some security problems should be consider; for example, authentication of the user which is the sender of MTA, construction of the MTA integrity that is MTA must be secured from robbery and unauthorized changes and determination of the MTA aptitude to pay for goods supplied by the merchant server [16]. However, in this section, we explain secure MTA and illustrate the relations between, MTA, AD, merchant server and the user. We also, describe how they are encrypted using a public key encryption scheme.

Figure 1 depicted the MTA roaming from one merchant to another one to buy and sell goods with any merchant. The aptitude of the MTA to migrate the internet has a benefit that the MTA can travel various merchant servers to find out the well-known available merchant providers to trade merchandise with them. When the MTA roams from one merchant server to another merchant it means that it executes in the memory of these servers. No problem how we secure the MTA whilst a version of the MTA is in the memory of unknown server; it is susceptible to attack from such server; it means that its secret key may be copied and illegal transactions executed via the server. Therefore, we want a method that will authorize the MTA to roam unknown servers to buy and sell goods with them on behalf of a user, but physically stays in the protective environments of the AD. This indicates that logically the MTA still migrates from one merchant server to another, but physically it keeps in one protected location. The design that makes this type of migrating achievable is distributed object technology.

The Java object encapsulates data fields and functions in one class, and can be specified by inheritance, but it can not reach across the address memory environment. However, in comparison distributed objects are packaged as binary elements which are accessible to remote entities by method of invocation. Traders do not know which compiler constructed the server object [17]. They have to know its name and the interface it issues. If we use the MTA as a distributed object and have every merchant server show its merchandise to another distributed object, then these distributed objects that are MTA and merchant object can execute methods on every other without being in the same memory space. The figure also shows that the MTA is used as a distributed object, as a shopping with a merchant object, and also used as distributed object. The figure also depicts that the MTA used as a distributed object, executing methods at a merchant distributed object to get a list of merchandise vend by this merchant. The MTA selects to purchase this merchandise from the merchant who influences them to create a signed message, denoting what they shopped, and pass these messages to an authorization server for authorizations. It is significant to observe that every signed document is encrypted with the public and secret keys. The MTA secret key migrated with it to the server which meant that the merchant at this server can attack the MTA and can recover MTA secret key. But with the distributed object technology, the MTA is not transfer to the server, but in fact remotely calls methods on the server object. This indicates that the MTA remains within the protected environments of the AD and the MTA and therefore MTA secret key is not subjected to attacks from any merchant server. So, to generate protected communication, we employ the public key encryption scheme. So a message between the merchant server, MTA, AS and the AD is encrypted by RSA scheme.

Assume a merchant server passes a message m to the MTA and the message is encrypted as follows. A merchant server creates a private key d, encrypt m by d then $m_2 = e(m, d)$. Then merchant server encrypts the private key d by the MTA public key so $m_3 = e(d, MTA$ public key). The encrypted messages m_2 and m_3 both construct a digital envelope[18] that is passing to the MTA. Once receiving the digital envelope, the MTA recovers the RSA key with its secret key and employs this private key to recover the message. The public keys of the application servers and the MTA should be issued in the AD.

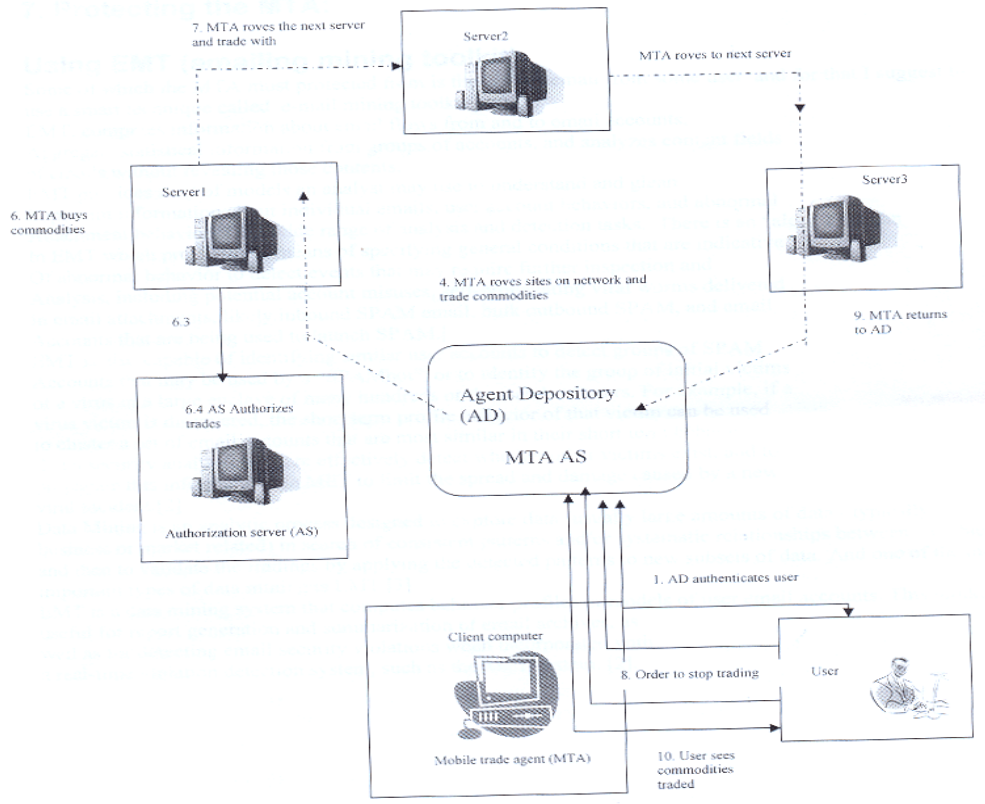

Fig. 1: The MTA Scheme

Applications of MTA: The MTA roaming the sites on the internet trading goods with the aptitude to as surely and rapidly receiving or paying funds make a considerable number of applications achievable such as demand and supply agents which show the employ of the MTA that we will discuss in this section.

Trade agents are categorized either user agents trading on behalf of the user, or business agents denoting suppliers[19]. There is no ground whether the MTA when directed skilfully can not represent a business or user agents. Such an agent could evaluate the goods in the market and once it can identify a demand for certain merchandise, it begins to migrate the sites on the internet and purchase these goods from merchants whose provide them with the optimum market price. The MTA then returns back to the rise of the demand and vends the merchandise with a commission. This demand and supply agent creates profits for its possessor by identifying demands and supply in these demands. The real merchandise never reaches the MTA possessor; instead the MTA ensures that any merchandise purchased are vended directly and carried to a new purchaser.

The potential technology of MTA: Just some years ago, it has been impossible to use the MTA in the internet permitting agent to safety roam over the sites and trade goods. Patented solution, for example General Magic[15] permits for travelling agents and produces agent-typed e-commerce possible but it is a closed standard with a restricted development environment[20]. The MTA will just be practical in an open market where they can travel easily to a considerable number of sites and doing business with them.

The distributed object technology makes a flexible network system, since it encapsulates data fields and functions in objects that can visit any site in the internet, execute on various platform, using inheritance applications via object oriented technique, and administrate them and the resources they control[21]. This type of distributed object technology illustrates that it is a fantastic application technology to use the MTA with. This means that the MTA could rapidly become something no e-commerce can be without. We stress that MTA visiting sites on a network, recommending entities when to trade goods is by now a actuality, for instance mobile trader[15] , but MTA securely travelling across thousands of sites over the internet with the aptitude to trade merchandise when they intellectualize it is relevant, has only become possible with the growing of the distributed object technology.

CONCLUSION

The MTA has the aptitude to decide where it is best to trade goods and with which merchants. This MTA produces e-commerce to be more open to market changes and permit them to utilize e-commerce opportunities once they occur. With the distributed object technology growing to a level were it is possible to use MTA that can visit the sites in the internet. The MTA can provide e-commerce the capability to respond rapidly to market prospects and increase profits.

This paper illustrates the MTA ability to migrate the markets in internet to trade on behalf of its user. In additional research this MTA could be applied in the current internet to consider the actual response of these agents in a physical environment. We are obsessed by the effect overhead these agents might cause.

REFERENCES

1. Canas, A.J., M. Carvalho and M. Arguedas, 2002. Mining the Web to Suggest Concepts During Concept Mapping: Preliminary Results. XIII Simposio Brasileiro de Informatica na Edicuacao, Porto Alegre, Brasil.
2. Canas, A., D.B. Leak and A. Maguitman, 2001. Combining Concept Mapping with CBR: Towards Experience-Based Support for Knowledge Modelling AAAI.
3. Cavaalho, M., R. Hewett and A. Canas, 2001. Enhancing Web Searches from Concept Map-based knowledge Models. SCI-World Multi-conference on Systemics, Cybernetic and Informatics
4. Lawrence, E., S. Newton, J. Lawrence, S. Dann, B. Corbitt and T. Thanasankit, 2003. Internet Commerce: Digital Models for Business, Brisbane: John Wiley and sons.
5. Elaine Lawrence and John Lawrence, 2004. Threats to the Mobile Enterprise, International Conference on Information Technology, Las Vegas, Nevada, USA
6. Stanifor, S., V. Paxson and N. Weaver, 2002. How to own the Internet in your spare time, Proceedings of the 11th USENIX Security Symposium. San Francisco, CA.
7. Suri, N., J.M. Bradshow, M.R. Breedy, P.T. Groth, C.A. Hill and R. Jeffers, 2000. Strong Mobility and Fine-Grained Resource Control in NOMADS. Proceedings of the 2nd International Symposium on Agents Systems and Applications and the 4th International Symposium on Mobile Agents, Springer-Verlag
8. Marco Carvalho, Thomas Cowin and Niranjan Suri., 2005. A Mobile Agent based Security Tool, J. Systemics, Cybernetics and Informatics, Number 6, USA.
9. Selker, T., 1994. A Teaching Agent that Learns, Communications of the ACM 37: 92-99.
10. Jennings, N. and M. Wooldridge, 1996. Software Agents, IEEE Review, pp: 17-20.
11. Wirthman, L., 1996. Gradient DCE has sign-on feature, PC Week, pp: 31.
12. Suri, N., M. Carvalho, R. Brandshaw, and J. Brandshtems, 2002. Small Mobile Agent Platforms. Autonomous Agent and Multi-Agent Systems Workshop on Ubiquitous Agents on Embedded, Wearable and Mobile Derives.
13. Netsurfer Digest, 1996. Book a good Idea that needs work, pp: 6.
14. Elliott, G. and N. Phillips, 2004. Mobile Commerce and Wireless Computing Systems, Pearson Addison Wesley.

15. Advanced Information Management Strategies, 1996.Payment Systems for the Internet, The Meta Group.
16. Harrison, C., D. Chess and A. Kershenbaum, 1995. Mobile Agents: Are they a good idea? IBM Research Report (T.J. Watson Research Center).
17. Suri, N., J.M. Bradshaw, M. R. Breedy, K.M. Ford, T. Groth, G.A. Hill and R. Saavedra, 2004. State Capture and Resource Control for Java: The Design and Implementation of the Aroma Virtual Machine. White Paper.
18. Fahn, P., 1993. About Today's Cryptography, Answers to Frequently Asked Questions, RSA Laboratories.
19. Orfali, R. and D. Harkey, 1994. Client/Server Survival Guide with OS/2, John Wiley and Sons.
20. Orfali, R., D. Harkey and J. Edwards, 1996. The Essential Distributed Objects Survival Guide, John Wiley and Sons.
21. Horberg, J., 1995. Talk to My Agent: Software Agent in Virtual Reality, Computer Mediated Communication Magazine, pp: 3.