International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 2 Issue: 5 1282– 1288

A Proposed Security Model for Software Agent Security using DPHE and Publiccryptosystem

Sachin Upadhye[1], P.G. Khot[2]

Assistant Professor, Computer Application Deptt., Shri Ramdeobaba College of Engg. and Management, Nagpur

Email : sachupadhye@gmail.com

Professor, P.G.T.D., Deptt. Of Statistics, RTM Nagpur University, Nagpur

Email : pgkhot@gmail.com

Abstract--Software agent technology has become a driving force for recent advances in distributed systems. The concept of mobility in software agent is executable code, it raises major security problems. In this paper we deal with the protection of software agent code from possibly malicious hosts. We conceptualize on the specific cryptographic problems posed by mobile code. We are able to provide a solution for some of these problems.We present techniques how to achieve "non–interactive evaluation with encrypted functions" in certain cases and give a complete solution for this problem in important instances. We further present a way how an agent might securely perform a cryptographic primitive, blind signing, in an untrusted execution environment. Our results are based on the use of homomorphic encryption schemes and function composition techniques use Pailliar Cryptosystem.A propose a software agent security model for secured communication between the agents and platform. Data confidentiality is ensured using Dynamic programming with Pailliar cryptosystem additive/Multiplicativehomomorphic encryption property. The scheme ensures that the data possessed by theagents is secured at all times when it is executing at any of theuntrusted hosts. Paper also explain how the Additive homomorphicproperty of Pailliar scheme, Blind signature to be integrated with our model.

Weanalyse security aspects of mobility from acryptographic point of view. In section I introduce some fundamental of software agent security as well as discuss the constraints on cryptographic solution. Section II describing thePreliminariesof model such as Blind Signature, Pailliar Cryptosystem, Dynamic programming Homomorphic Encryption. Section III explain propose security model. Section IV focus on Discussion of the proposed model and Section V conclude the topic.

Keywords--*Software agent Security, Dynamic programming, Homomrphic Encryption Techniques, Blind Signature, Pailliar cryptosystem*

*****

Introduction:

Agent is anything that can be viewed as perceiving its environment through sensors and acting upon that environment through effectors. According to the IBM the software agent is a software entity that carries out some set of operations on behalf of a user or another program with some degree of independence or autonomy, and in so doing, employs some knowledge. Within the context of our research, we thus define an agent as an entity that receives inputs from its environment, evaluates the conditions and performs autonomous actions, perceiving and acting through its own environment to achieve its objectives. In Software Agent, Mobile Agent is regarded as an important new networking technology which, however, suffers from considerable security problems. Because it is based on the execution of mobile programs on remote and possibly untrusted computers, many observers question its fitness e.g., for E-commerce.

Security Problems:

We briefly describe the software agent code concept for discussing related security threats. This also enables to identify the specific constraints that mobile code imposes on cryptographic solutions [5]. The most evident security concern for mobile software agents is host security: hosts must be protected from the effect of foreign code which in much respect resembles network worms or computer viruses. The other concern is the security of the software agents themselves: the software agent's code and data is at the full understanding of the executing host. So far little research was done on protecting a mobile agent from malicious hosts: the main focus was on making the execution of mobile code efficient and safe for the host. This list also points to the problems of using mobile code in security sensitive applications. In the case of E-commerce, for example, a shopping agent could be "programed" by a malicious server so it forgets the best prices collected tofar. Furthermore, itwould be unwise to let themobile agentdigitally sign an order form because this implies that theagent carries the user's private key. Eavesdropping at the agent's data also permits stealing attacks either on electronic money or on other electronic credentials (passwords, capabilities). Similar threats with perhaps even more disastrous consequences can be produced for active networks and battlefield agents too. Thus, the challenge for cryptography is to find answers to the following problems:

- _Can a mobile agent *protect itself against tampering* by a malicious host? (code and execution integrity)
- _Can a mobile agent remotely *sign a document* without disclosing the user's private key?
- (computing withsecrets in public) _\
- Can a mobile agent *conceal the program* it wants to have executed? (code privacy)

As security concern the software agent security threats can be generally classified into threecategories:-

- Disclosure of Information

An agent may pose as awell-known service provider and tries to claim entity of atrusted agent and try to convince the other agent with creditcard no, bank account information or other privateinformation.

- Denial of Service

  Agents can distribute false or useless information to prevent other agents from completing their task correctly and on time for example repeatedly sending messages that is spamming agents with messages with cause's slow performance of agents. Sometimes an agent participating in a transaction or communication never took place which can lead to serious disputes.

- Unauthorized Access

  An Agent can directly interfere with another agent by accessing and modifying agents data or code which inturnchanges the agent behaviour.

In our discussion we focus mainly on these three types of security threats. In any mobile agent paradigm mainly four types of Security threats can arise namely

- Agent attacking another Agent
- Agent attacking another Agent Platform
- Agent Platform attacking an Agent
- Others(Agent or Agent Platform) attacking another Agent Platform.

Constraints on Cryptographic Solutions

Network of Untrusted Nodes:

Creating a network ofmutually trusted nodes alleviates many mobile agent protectionproblems: users can trust the executing computersnot to tamper with their agents. Cryptographic solutions should presume anetwork of untrusted nodes.

Non-Interactive Protocols:

Ideally a security solutionfor mobile agents does not rely on an interactive protocolbetween the agent and its originating site: otherwise trulydetached operations become difficult and result in a quitelimited form of task delegation. In the example of theshopping agent, the user Alice would like to go off-lineinstead of keeping in touch with the shopping mobile agentshe sent off. Cryptographic solutions therefore should conceiveprotocols requiring minimal interaction between anoriginator and its mobile agents.

Provable Mobile Code Security:

We expect that mobilecode based applications will not be used in securitysensitive fields if provably security cannot be provided.Making tampering of agents just "difficult" without beingable to prove that there are no simple attacks seems to be toovague of a solution, even for risk management cost/benefitarguments. Consider, for example, E-commerce transactions: Because an agent's buying actions should becomelegally binding operations, customers as well as providers require security guarantees. The protection offered to mobileagents must therefore be provable and truly cryptographic by linking the difficulty to alter an agent or spy itout to mathematically hard problems.. Cryptographic solutions for themobile agent protection problem therefore are subject tothe following constraints:

- Mobile agents should be allowed to execute in untrustedhosts but still have guarantees for their correctexecution.
- Mobile agents should not require interactive protocolswith their originator.
- Protection mechanisms should be provably secure.

Software agent technology suffers from two drawbacks. The first is the possibility of being attacked by malicious unknown mobile agents. The second is that, in transactions, service hosts may breach the fairness principle. We, therefore, propose an improvement model that would not only protect service hosts but also guarantee the fairness of on-line transactions.

Preliminaries

Blind Signature

[10]proposed blind signatures for untraceable payments based on the RSA public-key cryptographic system[11]. Themajor contribution of Chaum's scheme is the designof a signature protocol that allows signers toauthenticate applicants' identities, generate validdigital signatures for legal applicants, and verifythe signatures, but leave no clues as to whose signaturesthey are.In 1982, David Chaum invented a blind signature [12], that scheme allows the sender to have a given message signed by the signers, without revealing any information about the message or its signature. In 1996, Mambo, Usudu and Okamoto [13] proposed a new concept, proxy signature. In a proxy signature scheme, the original signer delegates his signing capacity to a proxy signer who can sign a message submitted on behalf of the original singer. Mambo, Usudu and Okamoto [14] proposed complete proxy signature, partial proxy signature and signature with an entitlement certificate. Zhang [15], and Kim, Park, and Won [8] proposed threshold proxy signature. In 2007, Li et al.[16] proposed a proxy blind signature scheme using verifiable self-certified public key, and compared the efficiency with Tan et al. In 2008 Xuang Yang and Zhaoping Yu proposed new scheme [17] and showed their scheme is more efficient than Li et al.[16] which is again modified by AungNway and NilarThein in 2009[18] and shown that their scheme is more efficient with low computation. This paper shows the scheme is more efficient and takes very less computational cost than the previous one. We study the security of blind signatures, especially for their application in electronic cash systems: we first define adequate security notions for blind signatures, then we propose the first schemes for which security arguments can be given.blind signature scheme is useful in several applications such as e-voting, e-payment and mobile agent environments. The security properties for a good proxy blind signature scheme are shows in Figure 1

 ISSN: 2321-8169
1282– 1288

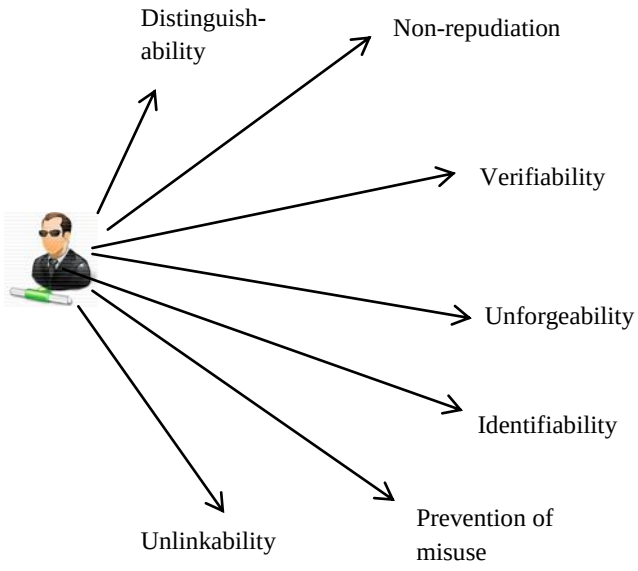

Figure 1: Blind Signature Scheme property

- *Distinguishability:*The blind signature must be distinguishable from the normal signature.
- *Non-repudiation:*The original signer can sign message instead of the other party, the original signer cannot deny their signatures against anyone.
- *Verifiability*: The blind signature can be verified by everyone.
- *Unforgeability*: Only the originatorsigner can create the proxy blind signature.
- *Identifiability*: Anyone can determine the identity of the corresponding blind signature.
- *Prevention of misuse*: It should be confident that key pair should be used only for creating Blind signature, which conforms to delegation information.
- *Unlinkability*: When the signature is verified, the signer knows neither the message nor the signature associated with the signature scheme.

To describe Chaum's idea clearly, we delineate the concept of Chaum's blind signature protocol using the following scenario. In this scenario, we assume that Bob wants to get a message M signed by Alice. Alice chooses two prime numbers, p and q. Let n =p*q. Let Alice's private key be d and her public key be e. Chaum's algorithm is illustrated as follows:

1. Bob chooses a random number r¸Z as the blind factor, produces a message digest H(MÞ for message M by a hash function H(), and uses rto blind the message digest H(M) Then he uses Alice's public key e to encrypt this message to produce $M^!$. $M^!=H(M)r^e(\text{mod } n)$.
2. Bob sends the message $M^!$to Alice.
3. Alice gets the signature $\sigma(M^!)$by using $M^!$andher private key to perform the computation as follows:$\sigma(M^!) = M^{!d} \text{mod } n$
4. Alice sends the signature $\sigma(M^!)$To Bob.

After receiving $\sigma(M^!)$Bob uses the blind factor r, performs the following computation to ''unblind'' his received message, and then generates the message signatureσ(M)
$\sigma(M) = \sigma(M) / r (\text{mod } n) = H(M)^d * r/r = H(M)$
When Bob sends the pair of messages M and σ(M)to Alice, Alice uses the hash function to get therelative digest H(M!) and uses Bob's public key todecrypt the signature to get $H(M)^!$. Finally, Alice compares H(M) with $H(M)^!$. If the result is equal, it means that the signature σ(M) is related to the message M, andσ(M) is indeed generated by Alice.

Paillier Cryptosystem and there Additive Homomorphic Property (AHP)

Pascal Paillier introduced his cryptosystem in the 1999 published paper "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes" [2]. The proposed technique is based on composite residuosity classes, whose computation is believed to be computationally difficult. It is a probabilistic asymmetric algorithm for public key cryptography and inherits additive homomorphic properties.

The Definition of Paillier's Cryptosystem
Pick two large primes p and q and let n = pq. Let λ denote the Carmichael function, that is, λ (n) = LCM(p - 1; q – 1). Pick random g Є Zn^2 such that $L(g^{\lambda} \text{mod } n^2)$ is invertible modulo n (Where L(u) = u-1/n). n and g are public; p and q (or λ) are private. For plaintext x and resulting cipher text y, select a random r Є Z_{n^*}. Then,

$$E_K (x, r) = g^m r^n \text{ mod } n^2$$
$$D_K (y) = [L(y^{\lambda} \text{ mod } n^2) / L(g^{\lambda} \text{ mod } n^2)] * \text{mod } n$$

PaillierAlgorithm:

1. Select two large primes, p and q

2. Calculate the product n=p * q, such that gcd(n,Φ(n)) = 1, where Φ(n) is Euler Function.
3. Choose a random number g, where g has order multiple of n or gcd(L(g^{λ} mod n^2) n) = 1 where L(t)= (t- 1) / n and λ(n)=lcm(p -1 q- 1)
4. The public key is composed of (g, n), while the private key is composed of (p,q,λ).
5. The Encryption of a message m< n is given by: c=gmrn mod n2.
6. The Decryption of cipher text c is given by:m=(L(g^{λ} mod n2)/L(g^{λ}mod n2))mod n.

Additive Homomorphic Property

The additive homomorphic property of Paillier encryption follows that

$$E(X \otimes Y) = E(X) \oplus E(Y).$$

And the generalized form is

$$\prod_{i=1}^{l} E(mi) = E(\sum_{i=1}^{l} mi)$$

The Paillier scheme is known to be additively homomorphic. What might seem confusing at first is the fact that the two group operations are different,namely the product of two cipher texts will decrypt to the sum of their plaintexts.In comparison to that, the product of two RSA cipher texts decrypt to the productof their plaintexts. Hence the Paillier scheme is additively homomorphic and RSAmultiplicatively.

The given cipher texts c_i are valid encryptions of plaintexts m_i, $c_i = Enc(m_i) = g^{m_i} r^{n_i} \bmod n^2$. The following properties hold

C_1	=	$g^{m_1} x_1^{n} \bmod n^2$
C_2	=	$g^{m_2} x_2^{n} \bmod n^2$
$C_1 * C_2$	=	$g^{m_1} x_1^{n} . g^{m_2} x_2^{n} \bmod n^2 = g^{m_1 + m_2}(x_1 x_2)^{n} \bmod n^2$

Table 1: The homomorphic property of the Paillier Cryptosystem

This means that the encryption of the addition of two plaintexts M_1 and M_2 is exactly the multiplication of the associated ciphertextC_1 and C_2.

Dynamic Programming Homomorphic Encryption Techniques

Dynamic programming [19] was developed by R. Bellman during the late 1950's. Dynamic programming is a powerful method that can be applied to various combinatorial optimization problems. Many planning and control problems involve a sequence of decisions that are made over time. The initial decision is followed by a second, the second by a third, and so on. The process continues perhaps infinitely. Because the word dynamic describes situations that occur over time and programming is a synonym for planning, the original definition of dynamic programming was "planning over time." Dynamic programming has been described as the most general of the optimization approaches because conceivably it can solve the broadest class of problems. In many instances, this promise is unfulfilled because of the attending computational requirements. Certain problems, however, are particularly adaptable to the model structure and lend themselves to efficient computational procedures; in cases involving discontinuous functions or discrete variables, dynamic programming may be the only practical solution methodology. An example application of this protocol is the combinatorial auction, where multiple servers can solve a winner determination problem, i.e., they can find the combination of bids so that the sum of the bidding prices is maximized. Although the servers can compute the optimal solution correctly, the information of the bids that are not part of the optimal solution is kept secret even from the servers [20]. DP model represents a sequential decision process rather than an algebraic statement of a problem. The two principal components of the dynamic programming model are the states and decisions. A state is like a snapshot of the situation at some point in time. It describes the developments in sufficient detail so that alternative courses of action starting from the current state can be evaluated. A decision is an action that causes the state to change in some predefined way. Thus a decision causes a movement from one state to another. The state transition equations govern the movement. A sequential decision process starts in some initial state and advances forward, continuing until some final state is reached. The alternating sequence of states and decisions describes a path through the state space.

A proposed Security Model

Based on Constraints of cryptographic solution and software agent security issues it is sufficient to use a very simple one, consisting of only two main components: the agent and the agent platform. An agent comprises the code, state and data needed to carry out some computation. Multiple agents cooperate with one another to carry out some application. Mobility allows an agent to move or hop among agent platforms. The agent platform provides the computational environment in which an agent operates. An agent comprises the code, state and data needed to carry out some computation. Multiple agents cooperate with one another to carry out some application. Mobility allows an agent to move or hop among agent platforms. The agent platform provides the computational environment in which an agent operates. The platform where an agent originates is referred to as the home platform, and normally is the most trusted environment for an agent. It is assumed that the platform can eavesdrop on the agents data and communication hence confidentiality is required for both. It is also assumed that the platforms would not collude tocompromise the data. An agent platform may support multiple locations or meeting places where agents can interact. Figure 2, which show the movement of an agent among several agent platforms.

 ISSN: 2321-8169
1282– 1288

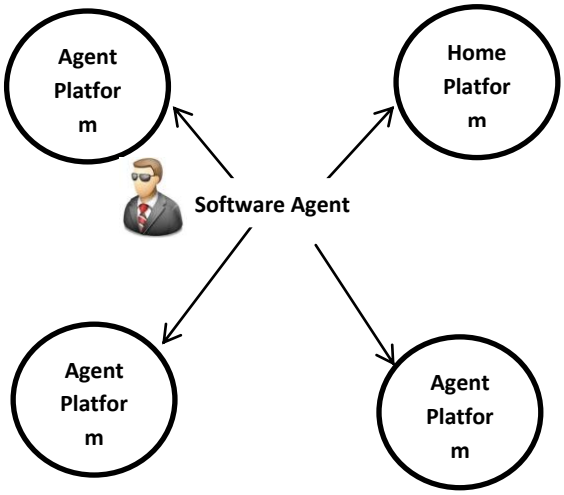

Figure 2: Software Agent Communication model

Software agent technology has been widely used to develop on-line shopping, auctioning, and other transactions. Users can set up software mobile agents and send them to collect product information, process an order, join an auction, pay for an order, and so on, instead of being totally involved in the transaction. Software agent technology enhances the convenience of electronic commerce. However, it suffers from two drawbacks. The first is the possibility that service hosts may be attacked by malicious unknown mobile agents. The second is that service hosts may breach the fairness principle in transactions. To overcome the first shortcoming, several solutions have been proposed. In our model we used Pailliar cryptosystem with Homomorphic additive property. The fairness principle is especially required for e-commerce money transaction, and other electronic commerce activities that emphasize the fair treatment of customers by service hosts. However, the current authentication scheme that is adopted by service hosts still has some fairness problem. It can be quite easily misused by unfair service hosts. Therefore, in this paper, we propose a fair and secure mobile agent environment. The proposed mobile agent based environment not only provides a novel authentication scheme that safeguards service hosts from being attacked especially malicious attack.

The commercial activity is a significant part of the network infrastructure allowing an open market of the services The commercial activity is a significant part of the network infrastructure allowing an open market of the services. Al Jaljouli et al [11] have implemented type of software agent in e-commerce to search and to filter information of interest from electronic markets. They describe also robust security techniques that ensure a sound security of information gathered throughout agent's itinerary against various security attacks, as well as truncation attacks. The figure 6 describes the sequence of processes carried out during the agent's lifetime. The authors utilize two co-operating agents where the initial verification terms are securely stored within a Software agent (SA) that resides at the initiator and cooperates with a Mobile agent (MA) that traverses the Internet. Nipur et al. [12] propose a fault tolerant comparison internet shopping system BestDeal. The author has conducted the simulation by launching nine shopping mobile agents where each has to visit five supplier sites to get the best deal for different products. Performance is measured in terms of execution steps as well as execution time of the simulation.. The design and implementation of a mobile agent platform for M-commerce applications is discussed in this paper. the advantage of adopting mobile agents for M-commerce is to scale up to large, dynamic world market places distributed over the Internet and to ease the access and participation of mobile users. We start by a discussion of the initial setup for the trading environment. In its simplest form, a trading environment is a market where some participants possess goods, and others want to consume them.

Steps of A proposed Model

1. A Software Agent host (SA) having the both the Static and Dynamic Data, Static data is the Object / Task of the Agent which want to communicate with Mobile Agent host (MA).
2. As SA is Blind Sign by the static data for the authentication purpose and encrypted by the private cryptosystem and SA use Pailliar public cryptosystem to encrypt the dynamic data.
3. MA first authenticate the static data after that decrypted by the static data and using public cryptosystem of homomorhic encryption additive /properly encrypted the MA resulted and pass it on to next host
4. After completion of predefined path the SA compute theauthenticate the static data and decryption of dynamic data, and find out the solution of Object / Task.

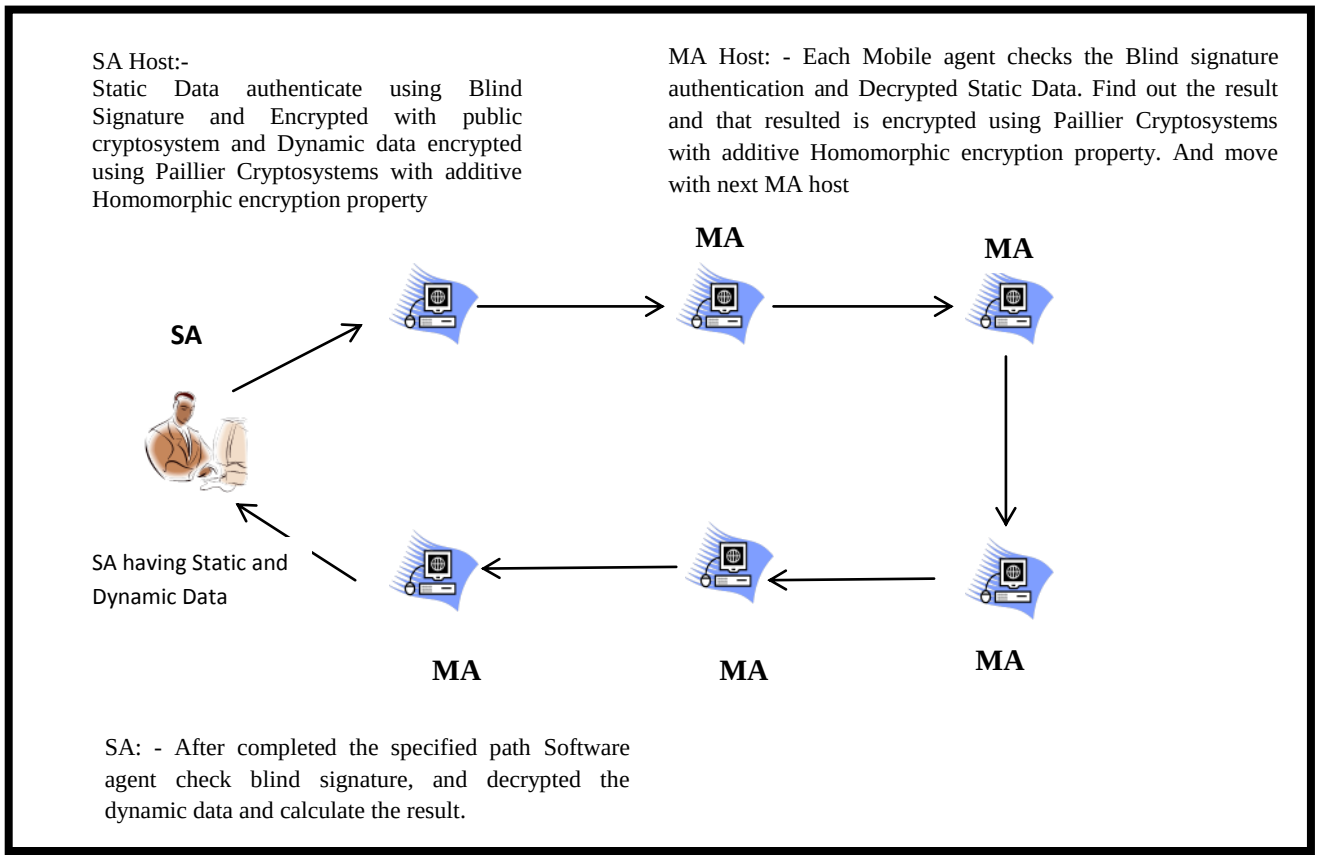

Figure 3. A proposed Model Software Agent Security model for E-Commerce

Conclusion:

Current E-Commerce buy/Sell product schemes employ an additive homomorphic encryption algorithm (e.g. Paillier encryption) to encrypt the sell value and exploit additive homomorphism of the encryption algorithm to recover the value for any host or choice with a single decryption. The contribution of this paper is a design of aadditivehomomorphicscheme. In additive homomorphicauction value, no single value isdecrypted in additivehomomorphic, so sell value for each host privacy is protected. The area of mobile agent security is still in somewhat immature state. Both the agent and the agent platform should to be protected by developing techniques and mechanisms.

Reference:

[1] T. Sander and C. Tschudin. Protecting Mobile Agents Against Malicious Hosts. In G. Vigna, editor, Mobile Agent Security, pages 44 60. Springer-Verlag: Heidelberg, Germany, 1998.

[2] Antonio Maña, Ernesto Pimentel, "An efficient software protection scheme", University of Málaga, Spain, 2002

[3] Joseph Tardo and Luis Valente, "Mobile Agent Security and Telescript," Proceedings of IEEE COMPCON '96, Santa Clara, California, pp. 58-63, February 1996, IEEE Computer Society Press.

[4] N. Jennings and M. Wooldridge, "Software Agents", IEE Review, January 1996, pp. 17-20. [2] O.A. Ojesanmi and A. Crowther, "Security Issues in Mobile Agents", International Journal of Agent Technologies and Systems, 2(4), pp. 39-55, October-December 2010, University, Nigeria.

[5] Upadhye-Khot, "Optimize Security solution for mobile agent security: A Review" International Journal Of Engineering And Computer Science, ISSN:2319-7242 Volume 2 Issue 1, Jan 2013 Page No. 322-329

[6] S. M..Moussa, G.A. Agha, "Integrating Encrypted Mobile Agents with Smart Spaces in a Multi-agent Simulator for Resource Management", Journal of Software, Vol 5, No 6 (2010), 630-636, Jun 2010.

[7]Upadhye-khot"Study of Existing Security Enhancement for Software Agent" ,International Journal of Advance Research in Computer Science and Management Studies Volume 1, Issue 7, December 2013 ISSN: 2321-7782 (Online)

[8] Sakarkar-Shelke ―A New classification Scheme for Autonomous Software Agent‖, IAMA'09,2009, IEEE Int. Conf. , India

[9] S.M.S.I. Rizvi, Z. Sultana, B. Sun, and Md. W. Islam, "Security of Mobile Agent in Ad hoc Network using Threshold Cryptography", World Academy of Science, Engineering and Technology 70- 2010.

[10] D. Chaum. Blind Signatures for Untraceable Payments. In Crypto '82, pages 199–203. Plenum, New York, 1983.

[11] R. Rivest, A. Shamir, and L. Adleman. A Method for Obtaining Digital Signatures and Public Key Cryptosystems. Communications of the ACM, 21(2):120–126, February 1978.

[12] D. Chaum, "Blind Signature Systems", *Proceedings of Crypto'83*, Plenum, pp.153. [2] B. Lee, H. Kim, and K.

Kim, “Strong proxy signature and its application”, *Australasian Conference on Information Security andPrivacy(ACISP’2001)*, LNCS2119, Springer-Verlag, Sydney, 2001, pp.603- 608.

[13] M. Mambo& K. Usuda and E. Okamoto, "Proxy Signatures for delegating signing operation", *Proc. 3rd ACM Conference on Computer andcommunications Security* , ACM Press, 1996. pp.48-57.

[14] M. Mambo, K. Usuda and E. Okamoto, "Proxy signatures: Delegation of the power to sign messages", *IEICE Trans. Fundamentals*, 1996, Vol. E79-A, (9), pp.1338-1354.

[15] K. Zhang, "Threshold Proxy signature schemes", *1997 Information Security Workshop* ,Janpan, 1997, pp.191-197.

[16] J.G. Li, and S. H. Wang, “New Efficient Proxy Blind Signature SchemeUsing Verifiable Self-certified Public Key”, *International Journal of NetworkSecurity*, Vol.4, No.2, 2007, pp.193–200.

[17] Xuan Yang, ZhaopingYu , “Efficient Proxy Blind Signature Schemebased on DLP”, International Conference on Embedded Software andSystems (ICESS2008).

[18] AungNwayOo and NilarThein, “DLP based Proxy Blind Signature Scheme with Low-Computation”, 2009 Fifth International Joint Conference on INC, IMS and IDC.

[19] E. Rasmusen. Games and Information.Blackwell, 1994.

[20] Makoto Yokoo, Koutarou Suzuki. Secure Multi-agent Dynamic programming based on Homomorphic encryption and its Application to Combinatorial Auctions.