AN AGENT BASED TRUST FRAMEWORK MODEL FOR SECURED E- PAYMENT TRANSACTIONS

A.Chandil kumar M.Sreeram kumar R.Madhurima P.Jyoshna J.Sheik Mohamed
Sreenivasa Institute of Technology and Management Studies,
Chittoor, Andhra Pradesh, India
E-Mail: chinna4s.chandra@gmail.com, sreeram4evr@gmail.com , r.madhurima28@gmail.com,
jyosthsna@gmail.com,sheik_50@yahoo.co.in

Abstract

As we know that security is one of the major tangible assets in E-Business environment, we proposed a framework model to provide security for Information transfer and communication, using hiding and agent techniques to control the transactions during self residence and communication in order to control all the activities which involves on the E-payment transactions, in this paper.

Key Words

Bargain Hunter, Purveyor, Stegnography, Trusted Third-party, and Trusted Agent.

1. INTRODUCTION

The main study made us to propose this framework model is that we found some of the draw backs that are present in the paypal system procedure. The paypal system is all about offering the secure service to which the funds can be transferred from one PayPal account to another. The transfer is immediate and guaranteed. It won't transfer funds unless the Bargain Hunter has a credit line to make the transfer. It suggests that the PayPal is not a bank.

If we are running an E-Business through paypal we can limit the people who are members in the concerned organization. We may not think that it is such a weak problem since the service has millions of customers but compared to the number of people who have credit cards we are limiting those who can use the system.

The major drawback in the paypal system [1] is as it had been popular among card holders because it does not require the input of card details online. Instead a valid email address is considered as a paypal account identifier and used for the online payment. However paypal has poor authentication during it's registration through which payment information such as card details or account number and sort code are associated with a valid email address. Once the association is created using the valid email address and the correct password will make the bank account or credit card to pay for a purchase. An intruder may easily register by bank account details and email address, and get rights to pay for shop pings later on. Due to false information provided by Paypal system, which sometimes, it would be preceded by legal authority and ruins the life of many peoples those who do online business transaction through this system. Many money conversion scams are also taken place in Paypal systems

2. PROPOSED MODEL

Our model suggests that the above mentioned limitations can overcome by introducing a money transformation through Trusted Third-Party (TTP), with security by using stegnographic techniques adapted with agent techniques as shown in the below figure.

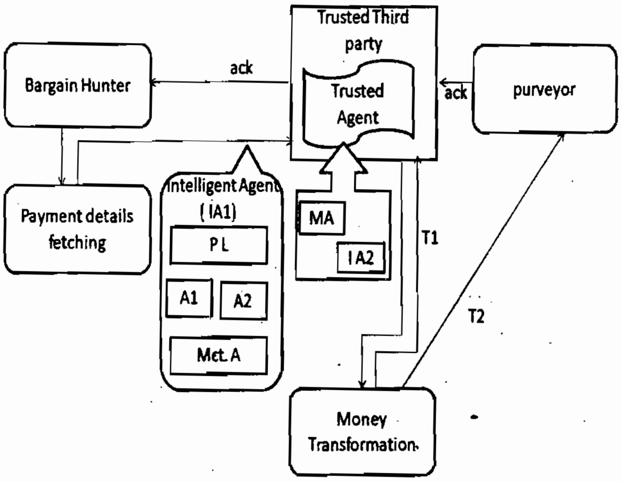

Fig 1: Block Diagram for Trusted Stego Agent based Frame work Model.

Notations in above figure are:

PL: Encryption Layer to hide the data in an Image

Al, A2: Agents that maintains communication security to the encrypted information.

Mct. A: Mycroft Agent, which acts as an interface between the Bargain hunter and detection layer.

MA, IA2: Mobile Agents, Intelligent Agents Which are used to the security and destegnography.

Tl, T2: Transfer of amount from Money transformation to Receiver as well as commission to the Trusted Third Party.

Ack: Acknowledgement sent by purveyor to TTP and further to Bargain hunter.

1. Initially, the e-payment starts with payment detailed entries by the bargain hunter which includes the nature and type of money transaction cards.
2. The information entered will be encrypted and hided by the Processing layer of the Intelligent Agent (IA1) using LSB based data hiding in image using image stegnography.
3. If either the stego-image is hacked by intruders, or it doesn't reaches the TTP, then one of the layers of IA1 smashes the whole information.
4. After reaching TTP, a copy of stego-image will be sent to money transformation. The encrypted informationwhich is embedded in the original stego image is extracted and secured using Trusted Agent (MA+IA2).
5. While sending the copy of stego image from TTP to Money Transformation through trusted Agent by monitoring, the processing layer of IA2 associated with MA will again extract the encrypted information of stego image and decrypted.
6. After that, the decrypted information is compared with the existing information of Money transformation. If it is matched, then it transforms the specified amount by the bargain hunter to purveyor as well as commission to the TTP rely on restriction.
7. If the purveyor receives the money then, it sends an acknowledgement to TTP which in turn sends to Bargain Hunter.
8. After sending an acknowledgement to the bargain hunter by TTP, then Authentication scheme of MA in TTP deactivates the buyer's personal stego-image file using secure Authenticated key agreement (SAKA) protocol which is retained with Trusted third-party
9. Once again the same bargain hunter wants to make any transaction with the help of available information in TTP, the bargain hunter has to send the activation signals to the trusted party on which it maps to the personal stego-image file based on the status ID.

3. TECHNIQUES USED IN THIS MODEL

The stegnographic and agent based techniques are elaborately explained as follows

3.1. Data Hiding Technique

After fetching the information from the Bargain hunter, initially it is encrypted and then hiding process in an image is adapted by using **"An LSB based Data hiding Technique using Prime Numbers"**. The encryption and the data hiding can be performed by the processing layer of IA1 and it not only allows one to embed the secret message in image bit planes but also it do's without much distortion with a better stego image quality in a secured manner.

In the prime number decomposition method, we generate a new set of virtual bit planes and embed data bit in it using LSB data hiding technique.

3.1.1. Prime Decomposition Technique

Let us consider a cover image of k-bits to embed the secret data. Our primary target is to increase the image quality without much distortion in image. To do this, a function 'f ' that increases the number of bit planes of a cover image 'k' to 'n', where n>=k.

We are converting the bits into some other binary system with different weights. The number of bits that were represented in virtual bit plane is greater than the cover image bit plane in less abrupt, change in pixel value. The following figure explains the above concept. For that, we are framing Number system.

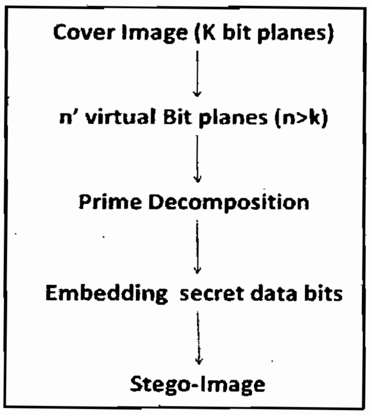
Cover Image (K bit planes)
n' virtual Bit planes (n>k)
Prime Decomposition
Embedding secret data bits
Stego-Image

Fig 2.

3.1.2. Number System

We define a Number system by,

1. we define a number of system completely by the pair(r,w(.)), r is integer and w(.) is weight function where w(i) denotes weight corresponding to i^{th} bit.

2. In our Number system representation, we will have value $D=\sum d_i w(i)$, where d_i $\varepsilon\{0,1,2...k-1\}$ in decimal.

3. A k-bit pixel value P_K is represented as $P_K = \sum b_{ic} .2^i$,where b_{ic} $\varepsilon\{0,1\}$.

Now a function 'f' converts P_K to some virtual bit plane. Function f, finding a new weight function, w(.) i.e., w(i), for every i$\varepsilon\{0,n-1\}$ denotes weight of i^{th} virtual bit plane.

$$P'_n = \sum_{i=0}^{n-1} b'_{ic} .w(i), b_{ic} \varepsilon\{0,1\},$$

Satisfying $(P_K)(2,2(.)) = (P'_n)(2,w(.))$

3.1.3.Proposed Prime Number Decomposition.

We are defining a new number system, denoted as (2,P(.)), where the weight function p(.) is defined as,

P(0)=1, P(i)= P_i for all i □ z^+, P_i=9^{th} prime,
P(0)=1, P(1)=2, P(2)=3, P(3)=5, ...

The weight function composed of prime numbers named as prime number system and decomposition as prime decomposition. Here we are taking 3-bit prime number system namely 100 and 011.

Prime Number Decomposition as
$1{*}P_2 + 0{*}P_1 + 0{*}1 = 1{*}3 + 0{*}2 + 0{*}1 = 3$
$0{*}P_2 + 1{*}P_1 + 1{*}1 = 0{*}3 + 1{*}2 + 1{*}1 = 3$

Here 100 is lexicographically higher than 011. So we choose 100 as valid representation for 3 in prime number system.
$3 = \max_{lexicography}(100,011) = 100$

Hence, valid representations of prime number decompositions.

000↔ 0, 001↔1, 010 ↔2, 100↔3, 101↔4, 110↔5, 111↔6.
By using these decompositions we embed secret data into virtual bit-plane simply by replacing. The resulting representation is valid then embed otherwise skip it.

3.1.4.Embedding Algorithm

1. Find set of all prime numbers that are required to decompose a pixel value in a k-bit cover image i.e. find a number n ε N such that all possible values in range $[0,2^k-1]$ can be represented using first n primes in our n-bit prime number system to get n virtual planes after decomposition.

2. Using Gold Beach conjecture[2,3],that all pixel values in the range $[0,\sum_{i=0}^{m-1} P_i]$ can be represented in m-bit prime number system.

3. We need to find n such that $\sum_{i=0}^{n-1} P_i \geq 2^k-1$, highest number can be represented in n-bit prime number system is
$$\sum_{i=0}^{n-1} P_i$$

4. Map binary decomposition and prime decomposition pixel values for valid representation.

5. For each pixel of cover image choose a virtual plane, say P^{th} bit-plane, embed secret data bit in it, without invalid representations. After embedding the secret message, we convert the resultant sequence in prime number and get the stego-image.

Now the cover image 'k', is converted into the stego-image in which data is embedded and it will send to the TTP in secured way through IA1. In TTP the Trusted Agent will receive Stego-image. The Trusted Agent is associated with Mobile Agent(MA) and Intelligent agent(IA2). The MA will carry the Stego-image to Money transformation and IA2 will de-Stegnography the Stego-image using the reverse algorithm of the LSB based data hiding technique . The agent techniques which we applied in this model are

3.2. Agent Techniques

Agent

Agent systems are a special category or software which is designed to carry out a specific task on behalf of an entity.In our model Intelligent agent and Trusted Agent play a vital role in securing the information sent by Bargain hunter.

The agents that we are using in this model can exhibit the Autonomy, Social ability, Responsiveness, Proactiveness.

3.2.1. Intelligent Agent (IA1)

This agent gives high performance in detecting the intruders during the transfer of information between Bargain hunter and TTP. In this agent we are trying heterogeneous anomalies detection methods and cooperating agents. It is based on extension of trust modeling techniques with representation of uncertain identities, context representation and implicit assumption. The basic principle is used to detect and recoverage. It consists of three layers: 1. Processing Layer

2. Security Layer

3. Interface Layer

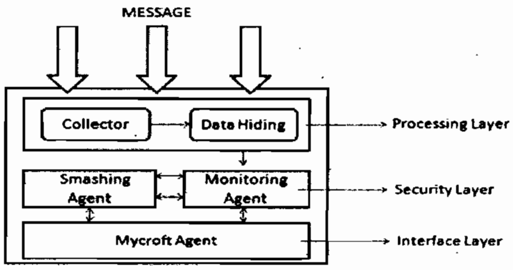

Fig 3: Layers of Intelligent Agent

Each layer demands of online processing and visualization process vary a lot.

3.2.1.Functionalities of Layers of IA1

1. The encrypting and embedding of message in an image using Image Stegnography can be done through processing layer of IA1 can be explained in detail in 3.1

2. Security Layer consists of specialized heterogeneous agents that seek to identify intruders. Their collective decision regarding the degree of maliciousness of a flow which certain characteristics use a reputation mechanism

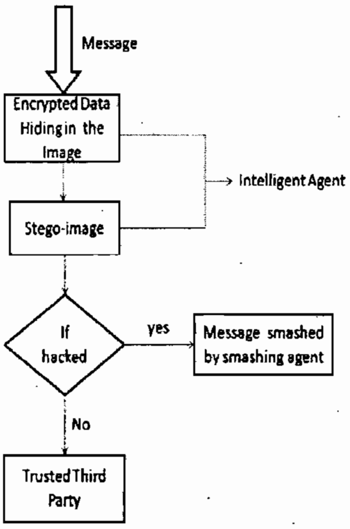

Fig 4: Flowchart for smashing message

3. Agent security platform is coordinated by intelligent Agent called MYCROFT[4]. The agent works as an interface between security and interface layer.

Every detected suspicious behavior on the network is automatically intimated to MYCROFT. It smashes the message by using the mother agent which was shown in fig., 4.

3.2.2 Trusted Agent

In this model is A Trusted Agent is Association of Mobile agent and Intelligent Agent. The Mobile agent should be able to travel between different platforms possibly carrying along all its data. Here, it maintains the encrypted information as it is, monitor the copy of stego image from TTP to

Money transformation and after completing the whole transaction the authentication will be done with IA1, to deactivate the information. Agent developers employ a number of security features in mobile agents like Authentication, Confidentiality, Integrity and Maintaining Information.

We are having several agent platforms like Aglets, Nomads, Mansion, Havana. In this model we are using *Mansion* [6,7] platform to provide the features of encrypted *Information Hiding* with TTP and *Authentication Scheme* from TTP to Bargain Hunter through MA of Trusted Agent.

Mansion employs an agent management service which is responsible for keeping track of actions of the agent throughout the lifetime and serves as a middle man for contacting the agent.
Mansion treats the whole platform has a world and divides into multiple rooms and zones in which an agent may interact with all entities in the mansion world have a set of private and public keys. Each and every agent protected by virtual machine as well as digital signatures by user.

An Audit system is employed and handoff protocol is used for securing the migration process. Communication security is achieved through use of asymmetric cryptographic mechanisms. The entities on the platform are virtually authenticated with the use of signatures and self certifying identifiers.

3.2.3. Information Hiding with TTP

After sending a copy of stego image to Money transformation, then IA2 of Trusted agent extracts , encrypted message from the original stego image MA2 maintains it in a secured way with TTP. It can done through the concept of Arbitrary Digital signature. For that we need to generate two keys

1. $K_{I,TP}$-Key between intelligent agent and TTP.
2. $K_{TP,MA}$-Key between TTP and Mobile agent.

The conventional security that the TTP doesn't see the message can be done through the following two statements.

$$I \rightarrow MA: ID_I || E(K_{I,TP}, M) || E(K_{i,MA}\ [ID_I || H(E(K_{i,TP}, M))])$$

$$MA \rightarrow TTP: E(K_{MA,TP}, [ID_I || E(K_{I,MA,TP}, M)]) ||$$
$$E(K_{I,MA}[ID_I || H(E(K_{I,TP}, M)) || T])$$

I:Intelligent Agent, TTP: Trusted Third Party
MA: Mobile Agent, M: Message, T: Time Stamp

The above two statements provide the arbitration as before but also assure confidentiality. In this case, both intelligent agent and TTP share the secret key $k_{I,TP}$. Now IA transmits an identifier copy of the encrypted information with $k_{I,TP}$ and a signature to MA. The signature consists of the identifier and hash value of Stego-image, all using $k_{I,,MA}$, the key between the intelligent agent and mobile agent. As before MA decrypts the signature and checks the hash value to validate the message. *In this case Mobile agent is working only with the encrypted version and is prevented from reading it. Mobile agent that transmits everything that it received from Intelligent agent plus a time stamp all encrypted with k $_{MA,\,TP}$ to TTP.*

3.2.4. StegAnalysis

This is the technique performed to extract the information from stego image through IA2 of Trusted agent. The Extraction algorithm is reverse of the hiding technique.

1. From the stego-image, we convert each pixel with embedded data bit to its corresponding prime decomposition and from pth bit plane extract message.
2. Combine all bits to get the secret message.

By getting the secret message from the Stego-image we are checking secret message that will send by the Bargain Hunter for transaction with the existing information in money transformation . If it is matched the transaction will happens that the amount transfers to TTP as commission as well as to purveyor. Then purveyor sends the acknowledgement to the TTP that the amount is received and TTP sends the acknowledgement to the Bargain Hunter. After the sending the Acknowledgement to the Bargain Hunter the IA2 associated in Trusted Agent will deactivates the whole information by using authentication scheme.

3.2.5. Authenticated Scheme

To provide the authentication scheme from the mobile agent which is in TTP to IA1 through Intelligent Agent, we are using an Authenticated protocol. The main goal of this protocol is to achieve a mutual authentication and key confirmation in order to establish a secure channel for that we are using three flows and it is illustrated in fig 5. It applies elliptic curve digital signature algorithm and simple key agreement to enhance the safely level.

Mathematical notation

The indexes used in Authentication scheme can be explained as follows:

Index	Explanation
h()	Hash function
p, q	Prime numbers
P,Q	Random points
a,b	Randomly generated private keys
A,B	Agreed public key
x(Q)	x-coordinate of Q

IA1, select $E(Z_p)$ define on Z_p. IA1 chooses a random point called P with order n, is a large prime number.. In addition IA chooses a password pd, computes x=h(pd) and Q=x*P. Finally IA generates two prime numbers p and q where p=2*q+1 with this the following parameters (E,Q,P,p,q,pd) are generated, and transfers (E,Q,P,n) to Mobile agent in a secure way.

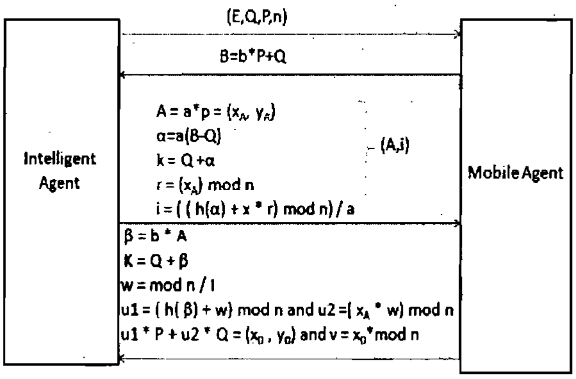

Fig 5: Block diagram of Authenticated Protocol

The session key generation procedure will be as follows:

1. Within the first flow, IA chooses a random number b, where $1 \leq b \leq n-1$, and calculates B Where B=b*P+Q and sends B to IA.

2. In the second flow IA chooses a random number a, $1 \leq A \leq n-1$, and calculates A, i as shown in fig.,5 and IA generate signatures pair (A, i) and transfer it to the MA .

3. In a similar way with in the third flow MA computes β, K, w, u1,and u2. In addition it calculates u1 * P + u2 * Q = (x_0 , y_0) and v = x_0*mod n

After calculating MA of Trusted agent checks the condition (v == x_A) and authenticates the Intelligent Agent , can be confirmed that IA1 has actually established same shared Session Key. Then MA computes Y_B = h(β) and sends to IA .

In order to authenticate MA, IA will compute Y_A = h(α). After that IA will verify the value of Y_A.

With Y_B. If both are equal IA authenticates MA and IA can be conformed that MA has actually established same shared Session Key.

Finally IA and MA agree on the common Session Key k_s = h(ID(IA)|| ID(B) || K)

If all the above steps have been executed correctly then both the agents will agree on the session key. This Session Key's life time is up to the deactivation of whole transaction from TTP to bargain Hunter through IA.

3.2.6. Calculation of Hash function

The n-bit hash function of the Stego-image can be obtained by processing the block of the encrypted message with XOR operation at a time in an iterative fashion.

$$Ci=bi1 \oplus bi2 \oplus \ldots \oplus bim$$

Ci = i th bit of the hash code,$1 \leq i \leq n$

M = Number of n-bit blocks in the input.

Bij = ith bit of the jth block

$\oplus$= XOR Operation

This operation produces the simple parity for each position each n-bit hash value is equally likely, then the probability of the data error is resulted an unchanged hash value is 2^{-n} To improve the above mentioned matters a simple way to perform a 1-bit circular shift or rotation on the hash value after each block is processed.

1. Initially set the n-bit block hash value obtained from eq.(1) to '0'.
2. Process each successive n-bit block of data as follows.
    a. Rotate the current hash value to the left by 1-bit.
    b. XOR the block into hash value.

In the second transaction of the same Bargain Hunter he send the authentication to TTP to activate the information present in Stego-image and the copy of the image is used and follows as previously explained way transacting the information of the Bargain Hunter.

Conclusion

Measurable things -- Congested environment -- Tremendous change -- Dynamic situation -- Knowledge discovery vest with suitability of development. To believe is very dull, To doubt is intensely engrossing, To be on the alert is to live, To be lulled into security is to die. Thus, our framework model is an assumption which contains various entities must be considered by default to secure and trusted , which overcomes the limitation of Paypal system and provides more security with Authentication, Confidentiality and Integrity to achieve QoS&A, degree of service, non-existing feedback and its implementation is under progress.

References

[1] PayPal. PayPal's privacy to fight identity fraud. Available from: https://www.paypal.com/us/cgi-bin/webscr?cmd=xpt/cps/securitycenter/buy/Privacy-outside.

[2] F. Battisti, M. Carli, A. Neri, K. Egiaziarian, A Generalized LSB Data Hiding Technique, 3rd International Conference on Computers and Devices for Communication (CODEC-06), Institute of Radio Physics and Electronics, University of Calcutta, December 18- 20, 2006.

[3] Jessica Fridrich, Miroslav Goljan and Rui Du.Detecting LSB steganography in color and grayscale images, Magazine of IEEE Multimedia, Special Issue on Security, pp. 22-28, 2001.

[4] M. Rehak, , M. Pechoucek, K. Bartos, martin Grill, and P. Celeda. Network intrusion detection by means of community of trusting agents. In IEEE/WIC/ACM International Conference on Intelligent Agent Technology (IAT 2007 Main Conference Proceedings) (IAT'07), Los Alamitos, CA, USA, 2007. IEEE Computer Society.

[5] M. Rehak, M. Gregor, M. Pechoucek, and J. M. Bradshaw. Representing context for multiagent trust modeling. In IEEE/WIC/ACM International Conference on Intelligent Agent Technology (IAT 2006 MainConference Proceedings) (IAT'06), pages 737–746, Los Alamitos, CA, USA, 2006. IEEE Computer Society.

[6] G. van 't Noordende, F.M.T. Brazier, A.S. Tanenbaum "A Security Framework for a Mobile Agent System", SEMAS-2002, Bologna, Italy, July 2002. DFKI Research Report RR-02-03 pp. 43-50

[7] G. van 't Noordende, F.M.T. Brazier, A.S. Tanenbaum,"Security in a Mobile Agent System" , IEEE Symposium on Multi-Agent Security and Survivability , Aug 2004 pp35-45