Online Hybrid Model for Online Fraud Prevention and Detection

Ankit Mundra and Nitin Rakesh

Abstract The current trend of online business enables better and faster service for users and makes it more profitable for merchants. On the other side, the Internet has become the most popular platform for fraudsters to commit online fraud with ease. Several solutions have been proposed in the literature to overcome these online frauds. But, complete and efficient way out from this problem is still in research. In this paper, we have proposed online hybrid model (OHM) which extensively prevents the possibilities of online fraud, and further, if any possibility is present, then it detects and fixes this possibility. The OHM approach is proposed exclusively for in-auction, non-delivery/merchandise and identity theft frauds. OHM further is applicable to several other online frauds. We have evaluated the performance of this model and have shown that OHM is a robust and highly effective online fraud prevention and detection approach.

Keywords Auction fraud · Credit card fraud · Identity theft fraud · HMM

1 Introduction

Online business is the modern business methodology which uses direct marketing, selling, and services. The growth of Internet has a special significance in the growth of e-commerce [1]. According to a report by US Commerce Department, Forrester Research, Internet Retailer, ComScore. Inc. [2], the online sell is

A. Mundra (✉) · N. Rakesh
Department of Computer Science and Engineering, Jaypee University of Information Technology, Waknaghat, Solan 173234 Himachal Pradesh, India
e-mail: ankitmundra8891@gmail.com

N. Rakesh
e-mail: nitin.rakesh@gmail.com

D. P. Mohapatra and S. Patnaik (eds.), *Intelligent Computing, Networking, and Informatics*, Advances in Intelligent Systems and Computing 243,
DOI: 10.1007/978-81-322-1665-0_81, © Springer India 2014

Table 1 Online sales data

Year	US online sales
2012 (Quarter 1)	$50,270,000,000
2011	$255,600,000,000
2010	$172,900,000,000
2009	$155,200,000,000
Year	Global online sales
2011	$763,200,000,000
2010	$680,600,000,000

Table 2 Top consumer reasons

Top consumer reasons for shopping online	Percentage of survey citing reason
Time saving	73
More variety	67
Easy to compare prices	59
No crowd	58
Lower prices	55
Spend less on gas	40
Less taxes	30
Other	3

increased rapidly from past few years and it shows why e-commerce is becoming popular.

Increasing growth of online business and consumers over Internet (shown in Tables 1 and 2) [2] have also increased illegal activities simultaneously. Fraudulent behavior over Internet is in general not easy to trace and prosecute. Fraudsters can easily hide their information from large pool of victims without incurring significant cost. One of the key reasons for Internet fraud is the unawareness of the user regarding fraudster's attacking mechanism through Internet medium. Because of the lack of legislation and consequently the information drive in many countries like in Asia, many Asians are victimized by fraudsters [3]. According to National White Collar Crime Center, Internet fraud can be classified as follows [4]: auction fraud, non-delivery/merchandise fraud, business opportunity schemes fraud, identity theft, credit card fraud, online investment scheme fraud, overpayment, money transfer fraud, spam/spin fraud, charity fraud, automotive, and counterfeit card fraud. Among these frauds, three most frequent frauds are as follows: online auction fraud, non-delivery/merchandise fraud, and identity theft. Online auction fraud is one of the most common types of Internet fraud (see Sect. 2). The process of online auction fraud can be seen as follows: First, online users visit auction Web sites to buy and sell various items. Then, interested buyers can bid for the auction item. Upon winning, the buyer pays for the auction item. The fraud occurs when the victim does not receive the item or receives an item of lesser value than advertised [5]. Second is non-delivery payment/merchandise, which is also one of most fraud areas created by fraudster Internet marketing and retail Web sites, which provide variety of products and services. The victim is misled, by a legitimate-looking site and effective marketing. Then victims give their credit card information or send payment by some other means for goods and services provided by fake sites. The goods never arrive, or if they arrive, then the product's worth will be less than their real price [4]. Third is identity theft; when a person pretended to become another person by using the information like credit card detail of that person to commit fraud [4].

In this paper, we have proposed a model to prevent and detect online in-auction fraud and non-delivery payment/merchandise due to their high probability among the Internet fraud. Our model is the online hybrid model (OHM) that works in two stages. One is it prevents both the users and Web servers from fraud; secondly, if fraud occurs in the system, then it detects the fraud and informs to victim. OHM is able to prevent and detect frauds like auction fraud, Internet marketing and retail fraud, card theft fraud, and identity theft fraud.

This paper is classified into five sections. Section 1 introduces the classification of Internet frauds and describes its categories: online auction fraud, non-delivery/merchandise fraud, and identity theft fraud. Section 2 shows the literature review for preventing these frauds and formulates the problem regarding these frauds. Further in Sect. 3, we describe the OHM approach for the prevention and detection of frauds and propose OHM prevention algorithms. Thereafter, in Sect. 4, we have evaluated the performance of proposed OHM approach to show the advantages of our model. Section 5 is conclusion and future work continued with references.

2 Related Work and Problem Formulation

We have already discussed various types of Internet frauds in Sect. 1. In this section, we briefly depict the literature to resolve the online frauds and formulate the problem due to above-categorized frauds.

2.1 Related Work

In the field of in-auction fraud [3] prevention and detection, Wang et al. designed a Shill-deterrent fee schedule (SDFS) mechanism [6]. But, this mechanism was not able to reduce auction fraud due to collusive bidding, multiple bidding etc. Later on, Wang et al. proved that there is no symmetry without shill bidding by analyzing shill bidding in multi-round online English auction [7]. In the in-auction frauds, prevention happens to be the best strategy, but sometimes, this strategy cannot work so we have to adopt detection scheme for auction frauds. To prevent honest users from becoming victim, Porter and Soham proposed a strategy to counteract bid shading and false bids [8]. They have estimated winning probability to identify the possibility of cheat.

Later on, for collusive bidding detection, Trevathan et al. proposed an algorithm [9]. “Collusive score” to detect collusive shills controlled by one seller. Analysis takes place according to three strategies: (1) alternating bidding strategy, (2) alternating auction strategy, and (3) hybrid strategy. In the field of identity theft, a hybrid model is proposed by Nitin Rakesh et al. on Problem Reduction in Online Payment System using Hybrid Model [10]. This hybrid model consists of two models: mobile authentication model and HMM model proposed by Abhinav Srivastava et al. [11]; according to this, hidden Markov model can be used to detect online fraud by examining the behavior pattern of users.

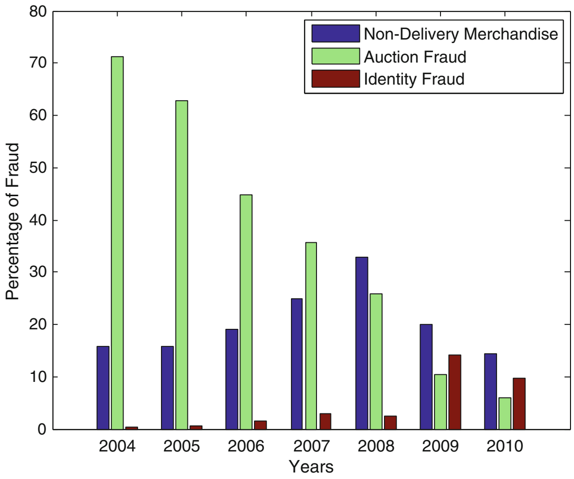
2.2 Problem Formulation

According to IC^3’s annual reports of year 2004–2010 [12], it is clear that the online auction fraud, non-delivery/merchandise, and identity theft are most frequent types of frauds. We have studied all 7 years report and created a statistics for these three frauds from the year 2004 to 2010 (Fig. 1); it shows that online auction and non-delivery/merchandise frauds are very frequent in all the 7 years, but after year 2008, another fraud i.e., identity theft comes into picture.

Auction Fraud: This is the one of the most frequent frauds committed over Internet. According to the 2011 Internet crime report by IC^3 [12], total loss due to auction fraud exceeds $8,288,098.73 in 4,066 complaints.

Figure 2 shows that online auction fraud can be classified into three parts: First is pre-auction fraud. This occurs before bidding process for the auction item starts. Further, it comprises of three types of frauds that are miss-representation fraud, black market fraud, and triangulation fraud. Second is in-auction fraud; this occurs during the bidding process, and this is the most unpredictable. Further, this has

Fig. 1 Statistics of online frauds



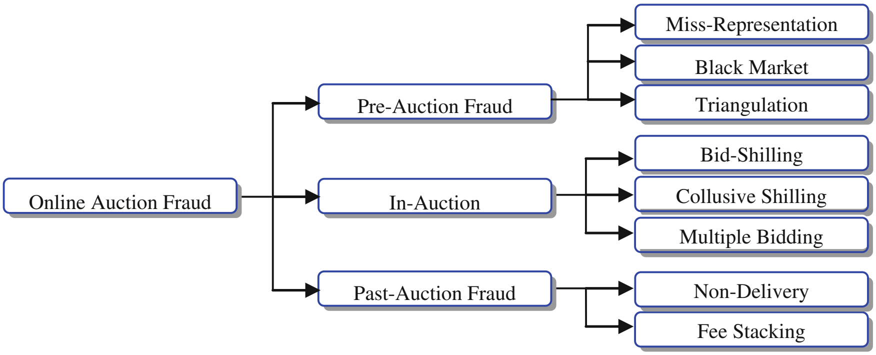


Fig. 2 Classification of online auction fraud [3]

three types of frauds that are bid shilling, collusive shilling, and multiple bidding. The third part of online auction fraud is post-auction fraud; this occurs after the auction process gets completed. Further, this consists of two types of fraud; one is non-delivery, and second is fee stacking. In this paper, our focus is to prevent and detect the in-auction frauds.

1. *Bid Shilling*: In this, seller puts higher bids for his/her own item to drive up the price of that item. Generally, shilling is accomplished by the sellers themselves or some associative of the sellers (friend or family member). As a result, shill bid drives up the price of the seller's item, and seller makes high profit by misleading honest buyers because they also make higher bid in trying to purchase item [6].
2. *Collusive Shilling*: This occurs when multiple groups start shilling in auction process [3]. This behavior is more complex to detect.
3. *Multiple Bidding*: This occurs when a buyer places multiple bids (some high and some low) on the same item using different aliases. The multiple high bids by the same buyer cause the price to escalate, which scares off other potential buyers from bidding. Then, in the last few minutes of the auction, the same buyer withdraws their high bids, only to purchase the item with their much lower bid [3].

Non-Delivery Payment/Merchandise: In this type of fraud, user does not receive items which he/she purchased or if he/she receives, then that is different from the item that he/she purchased. According to the 2011 Internet crime report by IC^3 [12] of year total complains for non-delivery payment/merchandise, fraud exceeds 22404.

Identity Theft fraud: According to IC^3, identity theft can be defined as unauthorized use of a person's information such as personal identity, credit card detail, etc. to commit fraud or other crimes. For committing this type of fraud, fraudster steals some other person's identity and plays as that person, for gain credit information and other benefits on that person's behalf. By this, the victim suffers from many adverse effects because fraudster can use his/her identity number or credit card number to commit fraud or crimes on the victim's behalf.

3 Online Hybrid Model

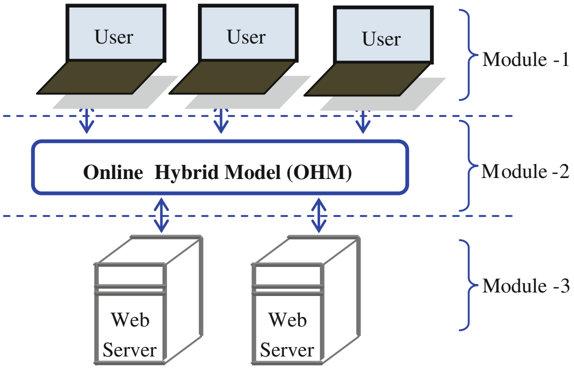
In order to prevent and detect the online in-auction, non-delivery/merchandise and identity theft frauds, this section illustrates the OHM approach. The glimpse of OHM approach is shown in Fig. 3 which shows that it contains three modules i.e., Users, OHM, and Web servers. The working of these modules is defined below.

1. *Users*: They can be of two types either buyer or seller. Each user, when he/she wants to interact with any e-commerce Web server for participating in any auction process or to buy goods, it is required that they must verify from OHM.
2. *OHM*: It is the approach that authenticates both user and Web server and also regularly monitors the interaction process between users and Web server. After authentication, OHM issues the OHM certificate (OC) that certifies the both Web servers and users and helps to reduce online frauds. It is mandatory for both users and Web servers to have the OC.
3. *Web Servers*: This module provides platform and management approach for auction and retail services like buying and selling of goods. The authenticity of a Web server is also decided by OHM by issuing an OC to the Web server. Each e-commerce site which is dealing with the money matters should have a digitally signed certificate from the authority. It is mandatory for a Web server to display the OC on its Website so that user can review this.

3.1 OHM Approach

We classify the OHM approach in two parts: One is OHM for prevention and second is OHM for detection; we will discuss both of them one by one.

Fig. 3 OHM approach



1. *OHM for Prevention*: This approach provides the verification and authentication steps to prevent the online fraud. This fraud prevention scheme contains three parts as follows:

   a *User authentication*: To authenticate the user, OHM takes the following attributes in care along with registration form.

   1. *User's address and photo*: This is the address of user where he/she currently resides. User's current photo for identification.
   2. *Mobile Phone Information*: By taking the mobile phone information, OHM verifies the address of user by tracking the location of mobile phone and then matches it with the address provided by user. The difference between the two addresses should be below the threshold level; otherwise, user registration will be rejected. OHM also verifies that the mobile phone should be active from a specified time period.
   3. Identification (ID) Proof: It is the unique id for a user. It can be among passport id/unique country ID/driving license number, etc. OHM requires this id to authenticate the permanent address of user.
   4. *Credit/ATM/Debit card information*: OHM requires any of the card information (which is used by user to perform final transaction) except password. OHM verifies this detail and gets the last 5 transaction statements from the bank with their location also. If it locates where the card has been used from last 1 month, then the difference between average location of transaction and current location should be less than threshold distance. When the current location exceeds the threshold limit, the card is rejected. And by credit card detail, again the address and phone number of user are verified.
   5. *Behavioral Pattern of User*: OHM gets the behavior pattern of the user by adopting hidden Markov model, and if that is not up to the mark, then it cancels the registration of user.
   6. *Certificate issuing*: after the complete verification of user, OHM issues an OHM certificate (OC) to user and sends a copy to Web site also.

   b. *Web server authentication*: OHM authenticates the Web server by taking the following steps:

   1. OHM verifies the digital signature certificate which insures that this is a registered Web server.
   2. OHM verifies the past transactions of Web server and feedback of different users of that server. Based on these two, OHM generates a ranking for that server.
   3. Then, OHM generates OC to that server which contains the ranking of Web server also.

2. *OHM for Detection*: This is the fraud detection scheme which is exclusively designed for auction fraud i.e., during the auction process only. Because after the authentication of both users and Web server, there might be chances of frauds like bid shilling, collusive shilling, and multiple bidding [3].

OHM regularly monitors the auction process by adopting SDFS mechanism, which reduces the extra profit earned by shill bidding by the seller [6]. In SDFS mechanism, the auctioneer charges entry fee and exit fee to the seller. The seller sets only a single starting bid or a reserve price. The entry fee is charged on initial reserve price, while exit fee is commission fee calculated on the difference between the winning bid and the reserve price. If the reserve price is too high, then it costs higher entry fee. If the reserve price is set too low in intension to pay less entry fee, then the difference between the reserve price and the selling price will be high, and it costs high commission fee. Therefore, SDFS bounds sellers to set the reserve prices honestly. The commission rates vary from server to server, which provides auction platform. On the whole, SDFS inhibit shilling behavior also. Which provide shill-deterrent fee. And monitoring the bidding behavior (1) incremented bid: when the bid for a item increases suddenly (2) alternating bid strategy: when two bidders bid alternatively in the same auction by more than threshold time (3) alternating auction strategy, where bidders alternatively bids on different auctions [9].

3.2 Algorithm for User Authentication

This algorithm authenticates the user when he/she wants to access the service provided by the Web server. For this, it requires some input, and after execution, it authenticates the user by issuing OC.

```
Initial Condition:User for registration
Local variable:location_threshold, time_threshold, mobile_location, mobile_use_time, address[ID], photo[ID]
Final Condition:Authentication or Rejection of user
User Authenticate {
a.Input: permanent_address, current_address, photo,
mobile_number, user_identification_proof,
card_detail;/* provide by user */
b.Verify: If [{(current_location - mobile_location) ≤ location_threshold} &&(mobile_use_time ≥ time_threshold)]/* mobile_location is traced by GPS, location_threshold, time_threshold decide by OHM, mobile_use_time obtain by mobile number information */
Then
If (permanent_address == address[ID])/* address[ID] is the address written on ID proof*/
Then
If (photo == photo[ID])/* photo[ID] is the photo on ID proof*/
Then Call: card_verification();/* function written just below this algorithm */
If (card_verfication() == true)
Then If (user_behavior_pattern $\geq$ behavior_pattern_threshold)/*behavior_pattern obtain by HMM, behavior_pattern_threshold decided by OHM */
Then OHM issues OC with username and password and stores in OHM_DB;
Else
Authentication failed;
c. Exit.}
card_verification(permanent_address, current_address, mobile_number)/* Function to validate car detail and user's detail */
{Verify: If [(average_location - current_location) $\leq$ card_location_threshold)]/* average_location and card_location_thresold are the local variables obtain by taking last 5 card transactions */
Then If [(permanent_address == address[card]) && (mobile_number == mobile_number[card])] mobile_number[card],address[card]/*obtain by the mobile number and address registered for that card */
Then Return true;
Else
Return false;}
```

3.3 Algorithm for Web Server Authentication

This algorithm authenticates the Web server according to HMM [11] and user's feedback with verification of digital signature of Web server. For this, it requires some input, and after execution, it authenticates the user by issuing OC.

```
Initial Condition: Digital signature certificate, HMM behavior pattern
Local variable: feedback_and_behavior_threshold, OHM_Rank
Final condition: Authentication or Rejection of web server
Web Authentication{
a.Input: digital_signature_certificate/* provide by web-server */
b.Verify: If (digital_signature_certificate == true)
Then
If (feedback_and_behavior[HMM] $\geq$ feedback_behavior_threshold)
```

Table 3 OHM's effects on the online frauds

Internet fraud	Effect of OHM	Reasons
Online in-auction fraud • Multiple bidding • Bid shilling • Collusive shilling	Reduces	Due to unique OHM ID, Thru-in auction OHM process
Non-delivery/ merchandise	Reduces	By providing OC to authenticated Web servers
Identity theft	Reduces	By verifying user's details with card detail

```
   /* feedback behavior[HMM] obtain by HMM, feedback behavior threshold decide by OHM */
   Then Issues OC with OHM_Rank and store in OHM_DB;
   Else
   Authentication failed;
   c.Exit}
```

4 Evaluation of OHM

In this section, we examine the performance of OHM for the two below-given cases.

Case 1. When user is fraudster: For prevention of fraud activities performed by the non-legitimate user, OHM verifies the current address, mobile number, permanent address, photo id, and card detail of user (according to algorithm as in Sect. 3.2). When a fraud user tries to access Web server to commit fraud and enters any of the false information, then OHM detects it and does not authenticate the user. As a result, user does not get the OC and will not able to access Web server.

Case 2. When a Web server is fraud: OHM prevents the users from being cheated by Web server by providing an OHM rank written in OC, which is issued to authenticated Web server (according to algorithm as in Sect. 3.3). By seeing the OC, user can decide whether this Web server is legitimate or not. In Table 3, we have shown the effect of OHM on various Internet frauds by explaining the cause of effect.

5 Conclusion and Future Work

In this paper, we have proposed OHM approach for prevention and detection of the Internet frauds. Implementation of OHM approach is evaluated efficiently for the following: online in-auction fraud, non-delivery/merchandise fraud, and identity theft or card theft fraud. By using the OHM, both the user and Web -server can save themselves from being an online fraud victim. OHM is also effective to detect various other frauds like spam/spin fraud, counterfeit card fraud, etc. Thus, OHM is a robust and highly effective online fraud prevention and detection approach. In future work, we will experiment OHM approach on real-time online fraudulent situations to study its response more effectively.

References

1. Prasad, B.: Intelligent techniques for E-Commerce. J. Electron. Commer. Res. **4**(2), 65–71 (2003)
2. U.S. Commerce Department: Forrester Research, Internet Retailer, ComScore., http://www.statisticbrain.com/total-online-sales/
3. Donga, F., Shatza, S.M., Xub, H.: Combating online in-auction fraud: clues, techniques and challenges. Comput. Sci. Rev. **3**(4), 245–258 (2009)
4. National White Collar crime center: Report on Internet fraud, www.nw3c.org/docs/whitepapers/internet_fraud.pdf?sfvrsn=7, June 2008
5. Chui, K., Xwick, R.: Auction on the Internet: A Preliminary Study, http://repository.ust.hk/dspace/handle/1783.1/1035, July 2008
6. Wang, W.L., Hidvègi, Z., Whinston, A.B.: Shill Bidding in English Auctions, Technical report, Emory University, http://oz.stern.nyu.edu/seminar/fa01/1108.pdf (2001)
7. Wang, W.L., Hidvègi, Z., Whinston, A.B.: Shill Bidding in Multi-Round Online Auctions. In: Proceedings of the 35th Annual Hawaii International Conference on System Sciences, Jan 2002
8. Porter, R., Shoham, Y.: On cheating in sealed-bid auctions. J. Decis. Support Syst. Special issue of the fourth ACM Conference on Electronic Commerce, **39**(1), 41–54 (2005)
9. Trevathan, J., Read, W.: Detecting Collusive Shill Bidding. In: Proceedings of International Conference on Information Technology: New Generations, pp. 799–808 (2007)
10. Singh, S.P., Shukla, S.S.P., Rakesh, N., Tyagi, V.: Problem reduction in online payment system using hybrid model. Int. J. Manag. Inf. Technol. **3**(3), 62–71 (2011)
11. Srivastava, A., Kundu, A., Sural, S., Majumdar, A.K.: Credit card fraud detection using hidden Markov model. IEEE Trans. Dependable Secure Comput. **5**(1), 1062–1066 (2008)
12. Internet Crime Complain Center: Internet Crime Report, 2004–2011, http://www.ic3.gov/media/annualreports.aspx