

# An Effective Method for Identifying Online Auction Fraud Using Triangulation Detecting Techniques

Thiagu K<sup>1</sup>, Maheswari B<sup>2</sup>, Dr. Karthik .S<sup>3</sup>

PG Scholar, Department of CSE, SNS College of Technology, Coimbatore-35<sup>1</sup>.

Assistant Professor, Department of CSE, SNS College of Technology, Coimbatore-35<sup>2</sup>.

Professor and Dean, Department of CSE, SNS College of Technology, Coimbatore-35<sup>3</sup>.

## ABSTRACT

Online auction have large trade, with oodles of items for sale at any given period. Tens of thousands people around the world presently make full-time living and selling items through Internet auction houses. The nature of internet auction is high degree of clandestineness, number of authorized occasions to buy and sell. Fraudsters can easily inaugurate frauds in auction activities, triangulation is the one of the key fraud in online auction. Clear fact is that information disproportionateness between sellers and buyers and lacking of product immediately examining genuineness of the goods, the purchaser can't verify the seller and the physiognomy of the merchandise until after the accomplishment of transaction. Triangulation classifies the different e-auction frauds and gives idea to detect triangulation frauds. Through our simple methods, buyers can easily keep away defraud in auction activities.

Key words---- Fraud detection, e-commerce, Auction fraud, Credit card fraud.

## 1 INTRODUCTION

### 1.1 Online Auction

Auction the word is from Latin which means increase. Auctions have existed for years. Auction is a place or offer for process of buying or selling and services offered take place. There are a number of different types of auctions and certain rules exist for each auction. There are variations for an auction which may include smallest price limit, highest price limit and time limitations etc. Depending upon the auction process bidder can contribute remotely or in person. Remote auction include participating through telephone, mail, and internet. [8]

Many economic transactions are conducted through auctions. Art work, antiques, cars, and houses are sold

by auctions. Government contracts are awarded by procurement auctions, which are also used by firm to buy inputs or to subcontract work. There are four commonly used and studied forms of auctions, it's are given below. Ascending order Bid Descending order Bid.

- First-Price preserved Bid
- Second-Price preserved Bid

These forms are classified according to the price and order of attempt. Most e-auction houses are used the ascending order bidding methods, it is very easy to manage. [7]

- Ascending order Bid: In this bid auction, the price is raised until only one bidder remains, and that bidder wins the object at the final price.
- Descending order Bid: In this bid auction the auctioneer starts at a very high price and lowers it continuously until someone accepts the currently announced price. That bidder wins the object at that price.
- First-Price preserved Bid: In this bid auction, each bidder submits her bid in a sealed envelope without seeing other's bids, and the object is sold to the highest bidder at her bid.
- Second-Price preserved Bid: In this bid auction, Bidders submit their bids in a sealed envelope; the highest bidder wins but pays the second highest bid.

In the above types the ascending order auctions are claimed to be the most common form of e-auction format used and is deemed to appear the most unsophisticated of all the forms.[6]

### 1.2 Online Auction Fraud

The vast profits of online auction also attract the attention of criminals who use fraud to cash in on the

profitable online trading market. According to annual reports of the Internet Complaint Centre, online auction fraud ranks as one of the top two serious Internet crimes in recent years, causal to a risky situation for online auction participants [19]. Most online auction houses realize that fraud corrodes not only their trustworthiness but also the prosperity of the entire market. For instance, multiple online identities are easy to create and a fraudster could use his many accounts to execute complicated schemes, while camouflaging his malicious target and escaping traditional detection methods that simply examine individual identities [21]. As more and more inexperienced traders become targeted victims, they begin to distrust the market, resulting in fewer buyers and fewer sellers [19]. To help promote trust in the online market, auction houses developed reputation systems to assist users in evaluating potential trading partners.

## 2 AUCTION FRAUD CLASSIFICATION

Here we concentrate on the category of online auction frauds. To be aware of online auction fraud, it is suitable to first classify the various types of online auction fraud according to the two time periods in which the fraudulent behaviour can take place, it is offline behaviour and online behaviour. In the auction frauds falsification of items, selling of black market goods and triangulation usually happen before the auctions start and non-delivery of goods and fee stacking happen after auctions close, so here classify them as offline behaviour fraud.

So the offline behaviour frauds that can often easily be noticed by buyers and sellers, examination of such frauds relies more on real-world evidence than on online prevention and detection mechanisms. However, online behaviour frauds happens while transactions are in progress, thus it may occur without leaving direct bodily evidence, and worst of all may not even be noticed by the victims.[7]

Types of auction frauds are classified. The table shows the auction frauds are classified two ways, one is offline behaviour and next is online behaviour. Here offline auction frauds are classified in five types it happened before the auction start or after the auction close and online auction frauds are classified five types, it happens while transaction are in progress. The description of fraud types are tabulated in Table I. [7]

In Online Behaviours the shill bidding is very dangerous; Shill bidding is the act of bidding on your own auction abutting other bidders in order to increase the value at which your product will ultimately sell. It is an infringement of both eBay law and federal law. The most real-life auctions, a bid on a product from anyone related to the seller in almost any way, from friends and family to business associates and roommates, is considered to be a shill bid, will not be honored, and will almost certainly disqualify the seller-even if the bidder would have purchased the item. Another online behaviour auction fraud is Dummy bidding. The dummy bidding is the false bidding, the false bidding is done chumpunadulterated buyers into thinking tangible

buyers are bidding. But, as you will see, pretend bidding is also used to get sellers to decrease their prices.

TABLE I AUCTION FRAUDS DESCRIPTION

Internet auction fraud types	
<i>Fraud type</i>	<i>Description</i>
<b>Misrepresenting</b>	Seller purposely describes an item incorrectly.
<b>Black Market Goods</b>	The illegal business of buying or selling goods in violation of restrictions such as price controls or rationing.
<b>Credit Card Fraud</b>	Using Stolen credit card to pay purchased amount.
<b>Non-Delivery</b>	Seller never sends the goods after the auction complete.
<b>Hidden Costing</b>	Seller adds hidden costs such as handling charges to the item after the auction ends.
<b>Shilling</b>	Seller bids on own auction to drive up its price.
<b>Dummy Bidding</b>	Two bidders collude on an auction: One makes a low bid, while the second makes an inflated bid. Seconds before the auction ends, the high bidder withdraws.
<b>Bid Shading</b>	Bidder could use an unfair method to know the highest bid before the bids are disclosed
<b>Several Bidding</b>	The buyers register several aliases and use them to place multiple bids for the same item.
<b>Bidding Rings</b>	It refers to collusive auction fraud behaviours conducted by several bidders.

## 3 SURVEY ON FRAUD DETECTION APPROACHES

### 3.1 Feedback Based Reputation Systems

One of the simplest fraud detection system is Feedback based reputation system. In this systems helps buyers to decide whether to purchase a product based on the feedback score. After the accomplishment of auction, both the seller and the buyer can put down their ratings and feedback comments on the other party. These comments and feedbacks build up in the merchant's transaction history, of which the feedback score is one part. So it is easy to understand the type of reputation system. It uses positive, neutral, and negative to denote the level of fulfilment for a trade.

Analyze the reputation system capacity of identifying fraudulent compartment; it has major hitches. Most online auction houses subscribe to reflexive approaches to the organization of reputation systems and management policies.

### 3.2 Could address fraudulent schemes.

The online auctioning become safer though, the users had more proactive approaches, such as an automatic fraud detector. The simple methods are used in most auction houses in development of reputation systems. After transaction is completed only the traders can rated on a positive, neutral and negative scale in the auction houses used the method of marking rates. The both buyer and seller try to increase the positive feedback, if they want to be a good name, so some of them try to increase their reputation with vague means. Swindlers could attract buyers by fabricating transaction records that inflate their feedback scores in order to hide their malicious intent. In online auction the buyer can make several mini business to earn more positive feedback rating score using the common fraudulent trick, but then cheat later on the first expensive product.

Multiple identities in online auction is the another common type fraud. In this type multiple identities are created by the fraudsters first, then dividing them into two groups, fraudsters and legitimate. Then, the fraudsters use the legitimate to exaggeratedly increase their reputations by leaving positive ratings. In adding the positive rating, the negative feedback can be intolerant by fraudulent traders as well. By checking the history of buyer and seller they can be worthy of negative feedback ratings, intimidate the positive rating by leaving their trading partners, regardless of the actual experience. Here we propose a method to increase the confidentiality of reputation system, by using the combination of statistical modelling and the automatic anomaly detection based reputation system, is the best way to improve the quality of reputation system [5, 22].

### 3.3 Data Mining Based Fraud Detection

Data mining, the other name is knowledge discovery, is a powerful computer-assisted process developed to analyze and take out most useful information from historical data [21]. Data mining allows users to analyze data from dissimilar magnitude or vistas in order to expose harmonious patterns, anomalies and systematic correlations between data elements. In different areas data mining technique used, the ultimate objective of data mining is to predict future behaviours and trends based on the discovered patterns and association rules. In the area of research most of the researchers have adopted data mining methods to identify skill associations and suspicious patterns. The main steps for implementing this approach for fraud detection within a business organization are [23].

- In order to converting them into data mining objectives, analyse the fraud objectives and the possible fraudsters,

- Data collection and understanding.
- Preparation for the algorithms and Data cleaning
- Experiment design.
- Evaluation results in order to review the process.

Data mining requires large amount of historical data, like reputation approaches, and to get result it take a very long time to. Using data mining approaches to have the advantage of accuracy compared to reputation systems.

## 4 C4.5 ALGORITHM

A set of records to be given. Each record has the same structure, consisting of a number of attribute/value pairs. Any one of the attributes represents the category of the record. Here the problem is to identify a decision tree on the basis of answers to questions about the non-category attributes predicts correctly the value of the category attribute. Normally the category attribute takes only the values {true, false}, or {success, failure}, or something equivalent. In any case, one of its values will mean failure.

If we have n records for our instances, we'll have a n-dimensional space to the classes. And the Decision Trees (DT's) will create hyperplanes (or partitions) to divide this space to the classes. A 2D space is shown in Figure 4.1, and the lines means the hyperplanes in this dimension.

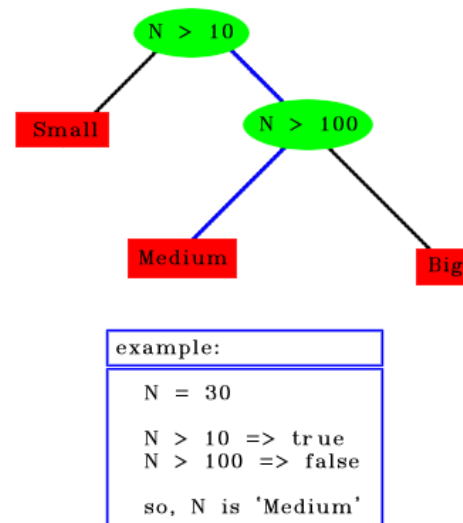


Figure 4.1. Simple example of a classification process.

The DT's can deal with one record per test node or with more than one. The former approach is called Univariate DT, and the second is the Multivariate method. This article explains the construction of Univariate DT's and the C4.5 algorithm, used to build such trees (Section 2). After this, we discuss the

ultivariate Approach, and how to construct such trees (Section 3). At the end of each approach (Uni and Multivariate), we show some results for different test cases.

### 5 TRIANGULATION DETECTION SYSTEM

The internet services will increase the business potential in various ways. However, e-auction requires an assurance to securing transaction details from others, including credit card details from customers.

As e-auction has grown, so we have security threats. Identify theft, data security separations and continue to top the list of complaints from the consumers. All of these factors weaken trust in digital business, and that is why it's important for any small commerce to take the necessary steps to decrease customer affairs about auction and online banking.

The Objective to identify the fraudulent person in the user-friendly auctioning site. In these site different kind of items can be auctioned and provides the value-added services to the bidders and the sellers. Fig 4.1 shows the detection system architecture. [25]

- Create consumer preference to buy at online auction store. Educates customers and raises their comfort level with secure processing system.
- Authentication messaging helps prepare the customers for the authentication process.
- A dynamic password enhances consumer confidence. Cardholder alerts and avoids disruption in the transaction process and ensures the sale completes.

First build both dynamic and static information. The dynamic information is the user transaction time behaviour and static information is already proven fraudulent activities.

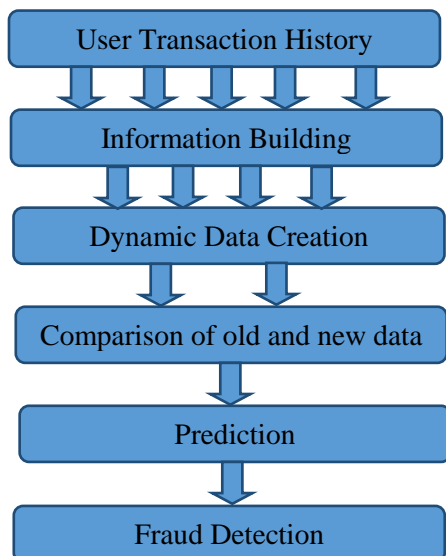


Figure5.1 Fraud detection System

In this system, each verification is submitted for incoming transaction. System receives the details of the card and the purchase value to verify whether the transaction is genuine or not. The types of goods that are bought into that transaction are not known to the system. It tries to find any irregularity based on the transaction spending profile of the cardholder. If the system confirms the transaction to be malevolent, it raises an alarm and the issuing bank to cancel the transaction. Here mainly used four steps,

- Information building
- Comparison
- Prediction
- Detection

Next step is compared present user behaviour and already proven fraudulent behaviour. And then forecast the result using both behaviours. Finally using the above steps the system can tell whether the user is legitimate or fraudulent. [25]

### 6 CONCLUSION

With the reliable increase in Internet auction fraud tiding yearly and the increasing number of internet users and Internet auction participants, it is impatiently apparent that this offense is not going to disappear anytime soon and demands the attention of all law enforcement and Internet auction house officials. The fact that this offense has been able to stay below the radar is not only confusing, but discouraging, because of the amount of loss it continues to stand up. Here we explained three methods to detect online auction frauds it has own advantages and disadvantages, so that the public and law enforcement can be made more aware and informed about it. Continual research needs to be conducted on the crime, to raise awareness of the current trends, latest statistics, and the tools that are being developed to prevent the crime. Without that Internet auction fraud will continue to grow and cause disorder in cyberspace.

### 6 REFERENCES

[1] Wen-Hsi Chang, Jau-Shien Chang(Feb 2012) "An effective early fraud detection method for online auctions", Graduate Institute of Management Sciences, TamKang University, Taipei County, Taiwan 25137, Republic of China, Department of Information Management, TamKang University, Taipei County, Taiwan 25137, Republic of China.

[2] Cecil Eng Huang ChuaNanyang(Sep 2001) "Fighting Internet Auction Fraud: An Assessment and Proposal", Technological University Jonathan Wareham ESADE, Barcelona.

- [3] David W. Aha, Marc K. Albert, (Aug 1999) "Instance-Based Learning Algorithms" Department of Computer Science, University of Illinois at Chicago, Chicago, IL 60607, USA.
- [4] Duen Horng Chau, (2011) "Detecting Fraudulent Personalities in Networks of Online Auctioneers", Shashank Pandit, and Christos Faloutsos School of Computer Science, Carnegie Mellon University.
- [5] Duen Horng Chau<sup>1</sup>, Christos Faloutsos<sup>2</sup> (2000) "Fraud Detection in Electronic Auction," Human-Computer Interaction Institute, School of Computer Science, Carnegie Mellon University.
- [6] eBay Inc. First quarter 2005 financial results, April 2005.
- [7] Fey Donga, Sol M. Shatz and Haiping Xub (2012) "Combating Online In-Auction Fraud: Clues, Techniques and Challenges" Department of Computer Science, University of Illinois at Chicago, Chicago, IL 60607, USA.
- [8] Wang, J., and Chiu, C. Q. "Detecting online auction inflated-reputation behaviours using social network analysis". In Proceedings of North American Association for Computational Social and Organizational Science 2005, Notre Dame, Indiana, June 26-28, 2005.
- [9] Isabelle Clopinet (1998) "An Introduction to Variable and Feature Selection," 955 Creston Road Berkeley, CA 94708-1501, USA.
- [10] Liang Zhang Jie Yang Belle Tseng (2012) "Online Modelling of Proactive Moderation System for Auction Fraud Detection," Yahoo! Labs 701 First Ave Sunnyvale, USA.
- [11] Dash, M., H. Liu "Feature Selection for Classification," Department of Information Systems & Computer Science, National University of Singapore, Singapore 119260.
- [12] Dash, H. Liu (Received 24 January 1997; revised 3 March 1997; accepted 21 March 1997) "Feature Selection for Classification," Department of Information Systems & Computer Science, National University of Singapore, Singapore 119260.
- [13] Mark A. Hall, Lloyd A. Smith (2005) "Practical Feature Subset Selection for Machine Learning," Department of Computer Science, University of Waikato, Hamilton, New Zealand.
- [14] Michael T. Goodrich (2009) "Privacy-Enhanced Reputation-Feedback Methods to Reduce Feedback Extortion in Online Auctions", Dept. of Computer Science University of California, Irvine Irvine, California 92697-3435 USA.
- [15] Networks Kai Zhu, Yong Guan and Lei Ying (2012) "Detecting Hidden Communities in Online Auction," Department of Electrical and Computer Engineering, Iowa State University.
- [16] Burge P, Shawe-Taylor, Cooke Moreau, Preneel C, Stoermann (2010) "Fraud detection and management in mobile telecommunications networks," Royal Holloway University of London, England; Vodafone, England; ESAT.K.U.Leuven, Belgium; Siemens A.G. Germany.
- [17] Pankaj Richhariya BITS (2009) "A Survey on Financial Fraud Detection Methodologies", Bhopal Prashant K Singh ISC Softwares.
- [18] Philip K. Chan, (2010) "Distributed Data Mining in Credit Card Fraud Detection", Florida Institute of Technology Wei Fan, Andreas L. Prodromidis, and Salvatore J. Stolfo, Columbia University.
- [19] Gavish, B., and Tucci, C. "Reducing Internet auction fraud". Communications of the ACM, 51, 5, 2008, 89-97.
- [20] Polo Chua (2011) "Suspicious network patterns may be the key to detecting criminals and fraudsters on e-commerce sites,".
- [21] [www.ic3.gov/media/annualreport/2009\\_IC3R\\_eport.pdf](http://www.ic3.gov/media/annualreport/2009_IC3R_eport.pdf).
- [22] Pandit, S., Chau, D. H., Wang, S., and Faloutsos, C. NetProbe: "A fast and scalable system for fraud detection in online auction networks". In Proceedings of the 16th international Conference on the World Wide Web, Banff, Canada, May 8-12, 2007, 201-210.
- [23] Rubin, S., Christodorescu, M., Ganapathy, V., Giffin, J. T., Louis Kruger, L., Wang, H., and Kidd, N. "An auctioning reputation system based on anomaly". In Proceedings of the 12th ACM Conference on Computer and Communications Security, Alexandria, VA, November 7-10, 2005, ACM Press, New York, NY, 2005.
- [24] Shai Rubin, Mihai Christodorescu, Vinod Ganapathy, Jonathon T. Giffin Louis Kruger Hao Wang: "Auctioning Reputation System Based on Anomaly Detection" Computer Sciences Department University of Wisconsin, Madison.
- [25] Abhinav Srivastava, Amlan Kundu, Shamik Sural, Arun K. Majumdar "Credit Card Fraud Detection using Hidden Markov Model".
- [26] E. Rozner, J. Seshadri, Y. Mehta, and L. Qiu, "SOAR: Simple Opportunistic Adaptive Routing Protocol for Wireless Mesh Networks," IEEE Trans. Mobile Computing, vol. 8, no. 12, pp. 1622-1635, Dec. 2009.



Thiagu K, B.E degree in Computer Science and Engineering from Maharaja Institute of Technology, Anna University, Chennai, Tamil Nadu India in 2011. Currently, pursuing M.E degree in Software Engineering from SNS College of Technology, Anna University, Chennai. His area of interest are networks, operating systems

and specifically, he is into Data Mining.



Maheswari B, is presently working as Assistant Professor in the Department of Computer Science and Engineering in SNS college of Technology, Coimbatore, Tamil Nadu, India. She completed her B.E degree in CSE from K.L.N College of Informamtion Technology, Madurai in the year 2007, completed her M.E degree in CSE From SNS college of technology, Coimbatore in the year 2010, Currently doing her PhD in Mobile ADHOC Networks.



Professor Dr.S.Karthik is presently Professor & Dean in the Department of Computer Science & Engineering, SNS College of Technology, affiliated to Anna University- Coimbatore, Tamilnadu, India. He received the M.E degree from the Anna University Chennai and Ph.D degree from Anna University of Technology, Coimbatore. His research interests include network security, web services and wireless systems. In particular, he is currently working in a research group developing new Internet security architectures and active defense systems against DDoS attacks. Dr.S.Karthik published more than 35 papers in refereed international journals and 25 papers in conferences and has been involved many international conferences as Technical Chair and tutorial presenter. He is an active member of IEEE, ISTE, IAENG, IACSIT and Indian Computer Society.