FRAUD DETECTION IN ONLINE PHANTOM TRANSACTIONS

Enroll. No. - **122210**

Name of Student - **ANKIT MUNDRA**

Name of supervisor(s) - **Prof. Dr. S. P. Ghrera**

May – 2014

Submitted in partial fulfillment of the Degree of

Master of Technology

DEPARTMENT OF CPMPUTER SCIENCE AND ENGINEERING

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY,

WAKNAGHAT

Table of content

CERTIFICATE

This is to certify that the work titled "**Fraud Detection in Online Phantom Transactions**" submitted by "**Ankit Mundra**" in partial fulfillment for the award of degree of M. Tech of Jaypee University of Information Technology, Waknaghat has been carried out under my supervision. This work has not been submitted partially or wholly to any other University or Institute for the award of this or any other degree or diploma.

Signature of Supervisor ……..

Name of Supervisor Prof. Dr. S.P. Ghrera

Designation HOD, Department of CSE and ICT

Date ……..

ACKNOWLEDGEMENT

I take this opportunity to offer my honor and profound greetings on the success of my project to the supervisor Prof. Dr. S.P. Ghrera , HOD-Department of Computer Science and Engineering & ICT, Jaypee University of Information Technology, Waknaghat, for his generous help and great support. I felt motivated from his incredible guidance and this project would not have been possible without his contribution.

I would like to greatly thank Dr. Nitin Rakesh, HOD-Department of CSE and CCE, Chandigarh University, for being part of my project and for positive encouragement. His constant support with valuable suggestions boosted up my energy in completing this project in time.

I would like extend my sincere gratitude to the entire faculty of Department of Computer Science and Engineering, Jaypee University of Information Technology, for their suggestions and support which helped complete this project successfully and efficiently.
Finally, would like to express my heartfelt thanks to my family and friends who have been my inspired me with their ideas and motivating contribution in making this project a possible one successfully.

Signature of the student ……..

Name of Student Ankit Mundra

Date ……..

SUMMARY

The Thesis presents a framework for preventing, detecting and eliminating the three most frequent online frauds i.e. Online Auction Fraud, Identity Theft/Credit Card Fraud and Non-Delivery Merchandise fraud. The proposed framework (Online Hybrid Model) contains three modules one is user second is OHM server and third is web-server. Further OHM is responsible for monitoring the regular interaction between user and web-server. OHM consist of three approach i.e. 1) OHM-P which stands for OHM for prevention and provides the authentication mechanism. 2) OHM-D which stands for OHM for detection it provides policies for web-server and attribute based monitoring mechanism for user interaction. And 3) OHM for elimination of online frauds which adopts extra authentication mechanism for eliminating the possibility online frauds. Further I have implemented the proposed framework by developing the JAVA modules for each mechanism.

Signature of Student	Signature of Supervisor
Name: Ankit Mundra	Name: Prof. Dr. S.P. Ghrera
Date:	Date:

LIST OF FIGURES

LIST OF SYMBOLS AND ACRONYMS

Sr. No.	Symbol/Acronym	Connotation
1	IC^3	Internet Crime Complain Center
2	SDFS	Shill Deterrent Fee Schedule
3	ATM	Agent Trust Model
4	OHM	Online Hybrid Model
5	OC	OHM Certificate
6	OHM-P	OHM for Prevention
7	OHM-D	OHM for Detection
8	OFDM	Online Fraud Detection Mechanism
9	OFEM	Online Fraud Elimination Mechanism
10	HMM	Hidden Markove Model
11	V_i	Observation Symbols in HMM
12	S_i	State in HMM
13	A_{ij}	State transition probability
14	B_{ij}	Observation probability
15	α	Sequence probability
16	$\Delta \alpha$	Deviation in sequence probability
17	r_{ij}	Correlation coefficient
18	$\prod$	Initial probability estimation

1. Introduction:

The current trend of online commerce enables enhanced and more rapid services for users who perform online shopping and makes it more profitable for the merchants also. But just parallel with this the internet becomes most popular platform for fraudsters to commit online fraud with ease. 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 presented by Department of U.S. Commerce, Forrester Research, Internet Retailer, ComScore. Inc. [2] the online sell is increased rapidly from past few years and it shows why e-commerce is becoming popular Shown in table and table 2).

Table 1. Online sells data U.S.

Year	**U.S. 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

Increasing growth of online business and consumers over internet has 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. Further in many countries like India, Sri-Lanka or in other Asian countries the legitimate users are very easy to be victimized due to improper legislation or lack of laws.

Table 2. Top consumer reasons

Top Consumer Reasons For Shopping Online	**Percent 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 %

According to National White Collar Crime Center internet fraud can be classified in [3]: 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, Counterfeit card fraud.

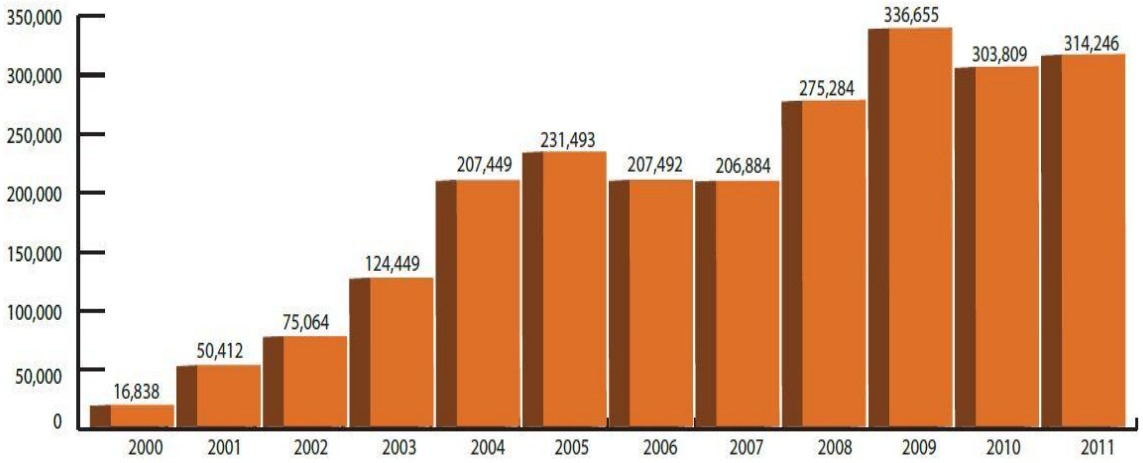

Figure 1. Yearly complain received by IC[3][4]

Figure 1. Shows the statistics of the total number of complain received by the Internet Crime Complain Center till the year 2011. This analysis shows that after the year 2007 the internet fraud complains surges.

1.1 Types of Online Fraud:

Here, we discuss each type of fraud one by one:

1.1.1 Identity Theft Fraud: This is a very new fraud and currently most frequent type of online fraud among all other online frauds. Identity theft fraud occurs when some fraudster user stole the identity of other legitimate user and uses his/her identity to commit a fraud or other online criminal act especially in the e-commerce applications. On the internet platform fraudsters can easily get the information which is need to guess the identity of legitimate user from a variety of sources, including by stealing the wallet of user, rifling through trash, or by compromising users' credit card or bank details. The most current way of stealing the others identity is like approach by telephone and act like a bank officer to ask your card and other information, or on the Internet via sending the promotional emails etc. and ask you for the desired information. The basic idea behind this type of fraud that it is not very difficult to get the information of any legitimate user because this information is easily available on several sources [3].

1.1.2 Auction Fraud: This is the most frequent form of Internet fraud. Auction fraud is increases day by day as the electronic medium offers more and more facility to conduct the auction process online. This strategy also helps the seller to getting more profit as compared to offline auctioning process because it involves the bidders from worldwide. Auction fraud occurs when an internet user visits the auction websites in order to buy and sell several items via online auction process. Now a day several items are posted for the online auction such as property, antique watches and other merchandise things, stamps, sports equipments of famous players, some books etc [5]. After posting these items on the auctioneer (website which provide the auction platform) by the seller, prospective buyers can bid for their desired item for auction. Now, the possibility of fraud occurs when the legitimate bidder either does not receive the item or receives an item which has less valuation as compared to the advertised item. In online auction fraud, the detection of fraud is very difficult as the bidders have only information about the seller is his or her email id. Further, the auction fraud can be divided in following types:

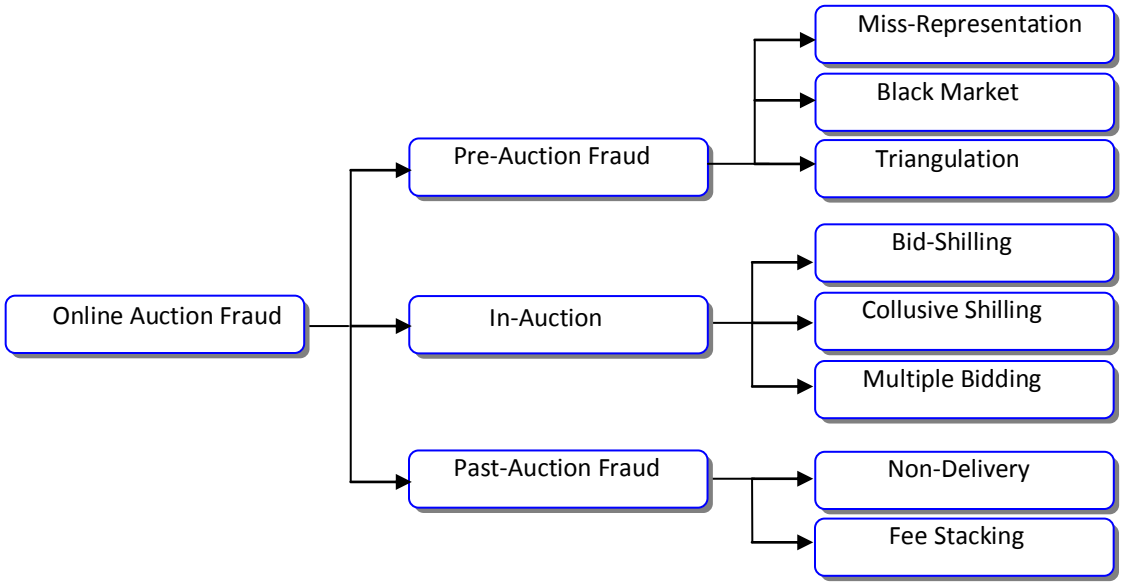

Figure 2. Classification of Online Auction Fraud [5]

Figure 2. shows that, Online Auction fraud can be classified in 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 most unpredictable. Further this has 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 completed. Further this consist two types of frauds 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 shills bid drive up the price of the seller's item and seller makes high profit by mislead to honest buyers because they also makes higher bid in trying to purchase item [5].

2. Collusive-Shilling: When multiple groups starts shilling in auction process [5]. This behavior is more complex to detect.

3. Multiple Bidding: This type of bidding occurs when in an auction process a user perform multiple bidding in which some bids are very high and some bids are low and the interesting thing is that all the bids are placed for the same item but using different aliases. Further, in these multiple bids the high bids are used to drive up the price by the same user, which scares off other legitimate users from bidding. But the fraudster user withdraws the high bids just before ending the auction in order to buy the item with the much lower bid [5]**.**

According to the 2011 internet crime report by IC^3 [4] total loss due to auction fraud exceeds $8,288,098.73 in 4066 complaints.

1.1.3 Non-Delivery/Merchandise fraud: In this type of fraud user does not receive items which he/she purchased or if receive than that is different from the item which he/she purchased. According to the 2011 internet crime report by IC^3 [4] of year total complains for non-delivery payment/merchandise fraud exceeds 22404. Non-delivery is easily facilitated with obscurity over the Internet because on the internet it is very easy to hide your contact information or to provide the false information. This type of fraud comprises several fraudulent online schemes such as to induce the users to send payment for merchandise and then deliver nothing in return or an item of far less value than expected. On the other hand, merchants can also be victimized when it delivered merchandise in good belief prior to receive payment from the buyers, but in the end merchant does not receive any payment for the buyers. The other form of this type of fraud is like, non-deliver services. Means the services which are demanding the advance payment for several services such as travel ticket fees, hotel booking fees, some reservation fees which are paid via online transactions.

Afterward, after paying the fee the user does not receives the actual service for which he/she is demanding and pay. On the other hand, this case may also happen with the service providers who provide such kind of services which are first delivered and then required the payment/fees such as web site design, software projects etc. After successful delivery of required service the provider never receive the fees. So in short, both consumers and providers can be victimized by non-delivery in online frauds.

1.1.4 Business Opportunity Schemes: Opportunity is the main idea behind this type of fraud. Because every person want to get rich and earn profit very quickly on low investment. And this prospectus of user make him victim to business opportunity scams. We can understand this type of fraud scheme with a example in which a legitimate person is asked to invest few dollars and can get the profit of thousands of dollars while working at home anywhere in the world on internet.

Another possible scheme involves an Internet-based business opportunity to use your home computer to earn money like email pays you sort of jobs and some data entry types of task. But in reality after investing the money the user does not get any benefit and the

demanding person stop contacting the payer. Finally a legitimate user become victim of Business opportunity schemes fraud.

1.1.5 Credit Card Fraud: This type of fraud is also one of the frequently committed online frauds. It is a multi-faceted crime and it is also associated with the identity theft fraud. Initially, a fraudster uses the stolen or forged credit card numbers of the legitimate users to purchase items from e-commerce websites [4]. After that upon received the payment recipient ships the ordered product to the fraudster buyer. When the victim get to know about the transaction which is not performed by him, he/she makes a complain to the credit card issuer. Upon finding that the credit card number has been used illegally, a "charge-back" is made by the credit card issuer to the merchant. But as the product is already shipped to the fraudster user, the merchant is left without the merchandise and also without payment because it has to rollback the transaction.

In the most of credit card fraud cases, multiple entities become victimized because more then one party is involved in a single credit card transaction such as the merchant, the card-holder, and the card issuer. And all the parties who get victimized have to spend time as well as more money to resolve the issue of credit card fraud.

1.1.6 Spam/Spim: This is also another type of online fraud. In this, Spam can be defined as the process of sending unwanted e-mail in immensity and these are equivalent of junk mail in the mailbox. Whereas, spim can be defined as the process of sending unwanted bulk messaging this is actually performed by targeting some goal. According to a study which is carried out in University of Maryland, "total money wasted by investing the time in deleting spam costs American businesses nearly $21.6 billion a year.[3]"

1.2 Motivation and Problem Formulation:

According to IC^3's annual reports of year 2004 to 2010 [4], it is clear that the Online Auction fraud, Non-Delivery/Merchandise and Identity theft are most frequent types of frauds. We have studied all seven years report and create a statistics for these three frauds from the year 2004 to year 2010 (Figure 1), it shows that Online Auction and Non-Delivery/Merchandise frauds are very frequent in all the seven years but after year 2008 the another fraud i.e. identity theft comes in to picture.

According to IC^3 report 2011 the statistics is as follows:

- Total complaints received: 314,246
- Complaints reporting loss: 115,903
- Total Loss: $485,253,871
- Median dollar loss for those reporting a loss: $636
- Average dollar loss overall: $1,544
- Average dollar loss for those reporting loss: $4,187

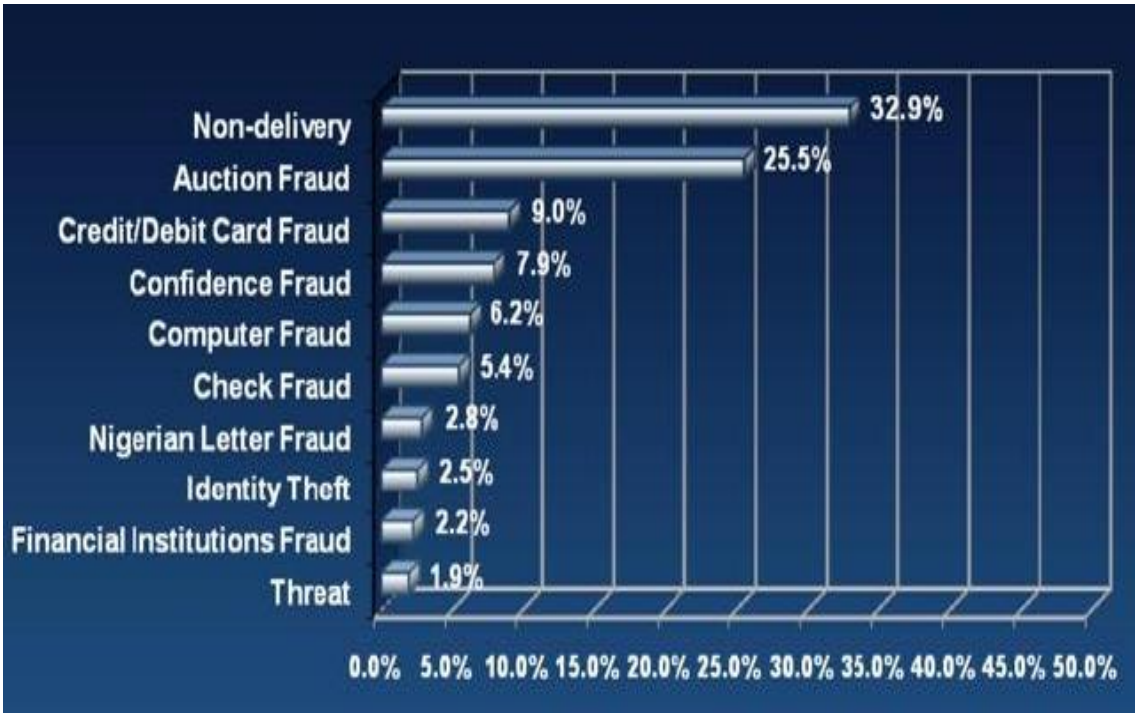

Figure 3. Fraud Statistics according to IC^3 for the year 2011[4]

According to the last six years reports of National White Collar Crime Center [3] most frequent internet frauds are Non-delivery/Merchandise fraud, Auction fraud, and Identity theft fraud (figure 4). During the last decade several approaches (probabilistic credit card fraud detection system [6], data mining approach for internet auction fraud detection [7], online banking fraud detection based on local and global behavior [8], and online modeling of practical restraint system for online auction fraud detection [9]) have been proposed for

detecting online frauds. But no robust approach exist which can prevent the possibility of online frauds.

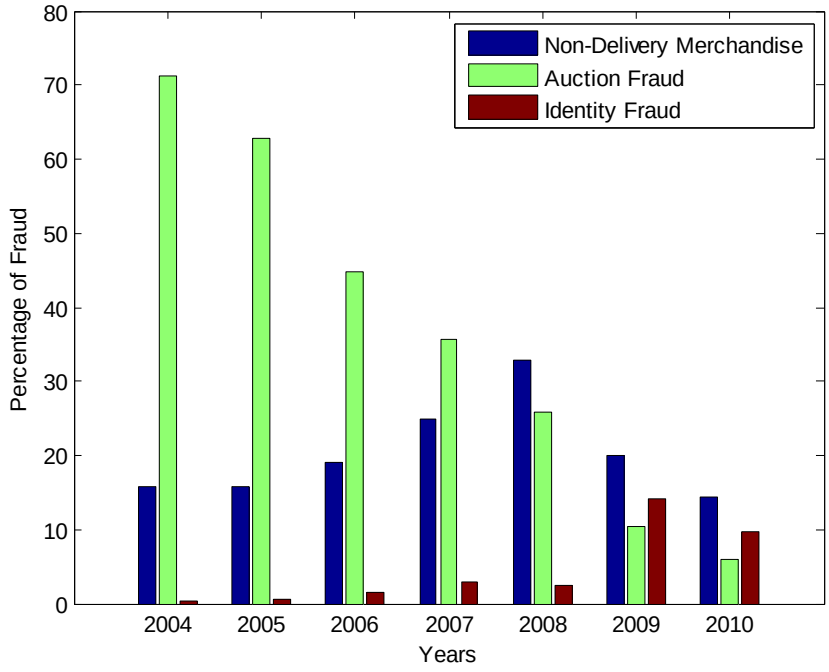

Figure 4. Statistics of online frauds [10]

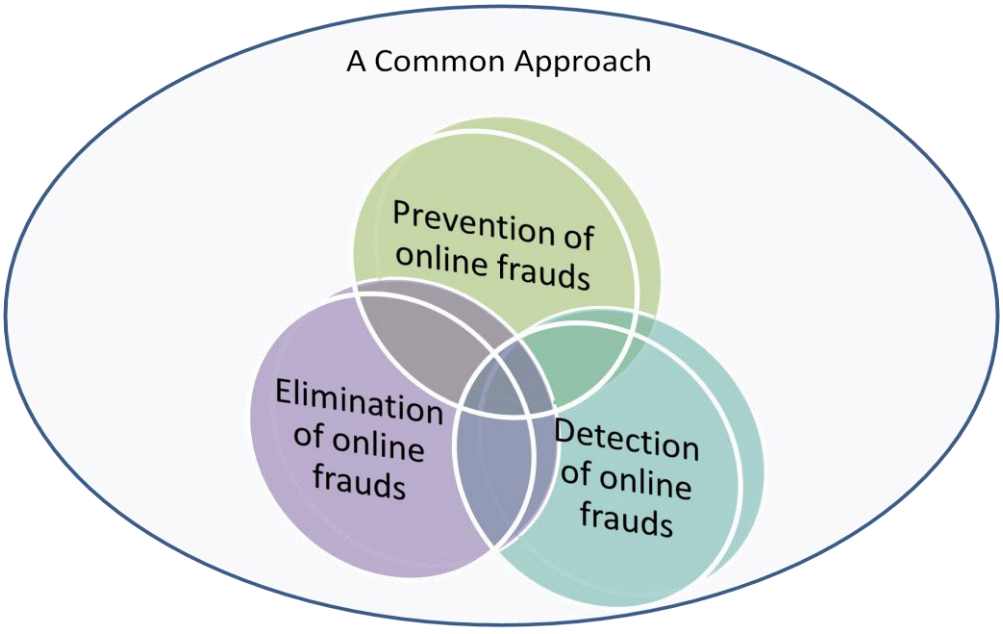

Figure 5. Goal of our Work

To develop a common framework which can prevent, detect and eliminates the frequent online frauds i.e.

- Identity theft frauds
- Credit card frauds
- Online Auction frauds

2.Literature Review:

In previous chapter we have discussed several types of internet frauds and their effects on e-commerce. In this chapter we have briefly depict the several approaches available in literature for resolve the online frauds. The current e-commerce trend is widely dependent on the platform provided by information technology, and due to this reliability any weakness which encountered in information systems can be easily used by the fraudster users to maximize their profits by making fool of legitimate users. Due to this, several different kinds of frauds occurs. Further, in particularly auction fraud has an important influence on e-commerce sector, till date no real time mechanism is available to handle the auction frauds and its effects. In the continuation of this topic the first paper which is have referred is a survey paper i.e.

2.1 Combating Online In-Auction Fraud: Clues, Techniques and Challenges [5]

Table 3. Bidding Strategies

STRATEGY	DESCRIPTION
Skeptic	It can be defined as the multiple bidding with the times but biding as low as possible each time.
Proxy bidding	This can be used to specify a maximum amount of bid initially and then authorize the proxy to bid automatically as many times as required up to the maximum.
Sniping	This is referred to the process which says, bid in the last seconds, leaving no time for anyone else to outbid.
Unmasking	This can be defined as the strategy of bid several times in a short period of time with the reason of revealing the maximum bid or the highest bidders.

This is the survey paper which described the auction frauds in detail. In this they have also discussed various strategies of online bidding (shown in table 3)

Further in this paper author have classified the online auction in to three parts, and role of Auctioneer and Sellers also i.e.

a. the types of Online auction fraud
    1. Pre-Auction
    2. In-Auction
    3. Post Auction

b. Role of Auctioneer
    1. Provide a transaction platform and services to both sellers and bidders.
    2. Make arrangements for auctions
    3. lace advertisements for auctioned items

c. Role of Seller
    1. Run the auction by posting item descriptions and pictures, and taking bids
    2. Receive payments and provide the auctioned item(s) to the winner pay commission fees to the auctioneer

Further in this paper author have defined the several terms which comes under the online auction fraud.

2.1.1 Shill bidding: this can be defined as the activity in which a seller or a correlate of a seller bids on auction owned by the seller. This type of bidding can be perform either by the seller or friends and family members of the seller, basically these seller related peoples have the secret information about the auction product that is not available to the other users who have participated in the auction [11-12]. Further author have discriminated three types of behaviors which are possible in shilling and these are based on the seller's or shill's inspiration to trick the other legitimate bidders and these are describe as:

(1) *Competitive shilling:* this behavior of shill bidding is a process of trick the users by making the bides which actually artificially drives up the bidding price of the auctioned item and the bidders intention is not to buy the auction item or the item for which he/she is bidding. The main intention is to craft a legitimate bidder to pay

for the particular auctioned item which has less valuation than the winning bid value, so that the seller can gain more and more profit [11]. This type of shilling behavior can occur in both type of auction process i.e. live/physical auction and online auctions and this behavior can successes as long as the relation involving the seller and the shills remain unknown to the other bidders and also to the auction house. Further, this behavior tricks other bidders by inducing them to pay more for the item than the auctioned item would have without the shill bids. In order to understand the competitive shilling behavior we can consider a simple example which is written below. In this author have taken a scenario in which a seller hosts an auction on a auctioneer platform of an item, suppose the auctioning item is an unlocked cell phone. Initially, they have assumed that no user placed any bid for the auctioned item. Now, to pull the legitimate user towards the auction, the seller start performing bidding process by using some other name or account alias, start placing a competitive shill bid for the purpose of stimulating other bids. After, seeing this scenario that someone outbids the shill bid, the seller places another shill bid for the purpose of driving up the bidding price. Further, all these bids which have placed on behalf of the seller or by the sellers friends or associative can be categorized as competitive shill bids and the bidding behavior is called competitive shilling bidding behavior.

(2) *Reserve price shilling*, this is the type of shill bidding behavior and it is first defined by Kauffman and Wood [13], it is a bidding behavior motivated by the desire to not to pay the reserve price to the auctioneer web-server. Because, before starting the auction process each seller has to pay the reserve price decided by the auctioneer. In order to minimize the reserve price set by auction house, but seller still want to reserve the item below a certain price so that he/she has to pay less reserve fee, but in this scenario some lofty volume sellers will not set an “official” reserve price but instead engage shills to place bids on their auctions. To understand this author has taken an example: suppose a seller who may wish to sell an item at $200 and for the auction process seller chooses eBay’s optional service. Thereafter seller has to pay a reserve price of $200, and it will be automatically applied by the eBay and it is estimated about $3.00 as the reserve fee (according to eBay’s fee

structure of 2008). Now, a fraudster seller want to avoid payment of the reserve price fee but the seller still want reserve the item. Now, consider a state if the final bid for the item is under $200, and in this case seller might first list the item at $9.99, and against this listing price seller is paying the auction house a low insertion fee of $0.35. Then, either a correlate user of the seller, or the seller himself with some alias, places a bid at the price of $200 in hopes that a legitimate bidder will make a purchase at $201 or more. Further we have to note that sellers do take a financial risk when employing reserve price shilling: because if nobody makes a purchase at more than the hidden reserve price, the seller must still pay both an insertion fee and a final value fee so in this case seller has to face the financial loss [5].

(3) *Buy-back shilling*, this is the third type of shelling behavior which also existing in the online auction process. It can be define as a bidding behavior functioning by sellers, or other shills as agents of the seller or the associates of seller, when the legitimate bidders do not bid an acceptably high price the seller or shills would rather buy back the item and sell it again in the another auction process [13]. In this buy-back shilling behavior, shill bidders behave as a normal bidder with the goal of buying the item at a bargain price and after winning the auction the pay the final payment and buy the auctioned item. Such kind of activity tricks the other bidders by miserly them of purchasing an item at a bargain price. Further to understand this sort of shilling behavior we can take an example, as in the previous example a seller may wish to sell an item at $200 but initially sets the starting price at $9.99, and pay an insertion/commission fee of $0.35. When the auction is close to termination, if the highest bid has only reached $15, the seller may place a shill bid at $16.00 in order to buy the item back, even though the seller must pay the auction house a final value fee of $1.40 in addition to the $0.35 insertion fee as the exiting commission fee or exit fee which is charged by the auctioneer. However, this cost to the seller is insignificant compared to the profit-loss the seller would have incurred if the item was sold at $15. Further, from this example we can understand that the profit incur due to of buy-back shilling is obvious

The above discussed three behaviors of shill bidding can be enacted by the any of the below discussed form and this is depending on who performs the shill bidding:

1. Acting alone: in this seller, or proprietor himself/herself start shill bidding in his/her own auction. This is possible due to lake of authentication mechanisms used by the auctioneer. And because of this seller is able to register several IDs or account in an auction house, e.g., eBay or uBid. And then using these different IDs and account seller pretending to be different legal bidders in order to bid multiple times in the seller's own auction, the seller can drive up the final auction price and profit of self auction process [14].

2. Seller collusion: As the name represents itself, in this several sellers or associates of seller help each other to place bids on each others' transactions for their mutual benefits [14].

3. Accomplice: A seller hires or invites family members and friends to serve as shills who will place bids on the seller's item, but instructs them to avoid winning [15].

Other types of in-auction fraud are described as follows.

2.1.2 False bidding: In a second price sealed-bid auction, each bidder bids only once in the auction and the winner pays the second highest bid rather than the highest. An auctioneer can help a seller profitably cheat by examining the bids under the table after all buyers have submitted their bids. Knowing all bids, the auctioneer can submit an extra bid to make the second highest price very close to the current highest price such that the seller can gain more profit [14].

To understand this in a better way we take an example, in an online auction process after all the buyers have submitted their maximum bids, the auctioneer learns that the highest bid is $200.00 for the auctioned item and the second highest bid which is also placed for this item is $120.00. The auctioneer (who could possibly be working on behalf of the seller) can help the seller insert an extra bid, say $198.00, which is quite close to the highest bid $200.00, but not beyond the highest bid. After the auction ends, the seller receives $198.00 rather than $120.00, and the extra $78.00 in revenue is gained by false bidding. This type of auction fraud may appear in auctions held by eBay when bidders are

using the auction site's automatic bidding proxy system. Every buyer using the bidding proxy has to submit a sealed maximum bid to the bidding proxy. The bidding proxy then bids repeatedly by setting increments until the bid exceeds the buyer's predetermined maximum bid. When the seller is able to obtain all existing maximum bids, this seller can then place a second highest bid as a shill bid, which is slightly lower than the highest maximum bid. By doing so, the seller's revenue increases.

Till now, we have discussed the types of frauds which can occur in online auction process is performed by the sellers', but several types of frauds are also possible which can be performed by buyers in online auctions. Bid shading, multiple bidding and bidding rings are common cheating approaches used by buyers in the online auctions:

2.1.3 Bid shading: This type of online auction fraud can only happens in first price sealed-bid auctions; in this type of auction the winner of the auction pays the highest bid. And if a bidder is able to know the highest bid value by using some unfair methods, before the bids are disclosed, then the bidder could insert a bid which just above the highest bid. And the fraudulent bidder would thereby increase the possibility of winning while minimizing the payment to the seller [16].

To better understand this we take an example of an auction of the game console. In this example we assume that bidder of id 6 is willing to pay up to $400 for the game console before submitting any bid. And when the auction process starts, all the other bidders except bidder having id 6 submit their individual bids. Further these bid values are lower than bidder 6's estimation, which is ranging from $200 to $300, this scenario is shown in Figure 6. Since the auction is a conserved one, an individual bidder is not able to see the highest bid which is placed by some other participators. And in case a user is able to know the highest bid by some unusual way, he/she may guarantee a win by placing a bid at $301 (in our example) and this is known as bid shading [17].

Further one more biding strategy which is slightly different that is not regarded as fraudulent also goes by the name of bid shading. In this case, bidders place bids below their true valuation of the item in order to avoid overpaying for the auctioned item.

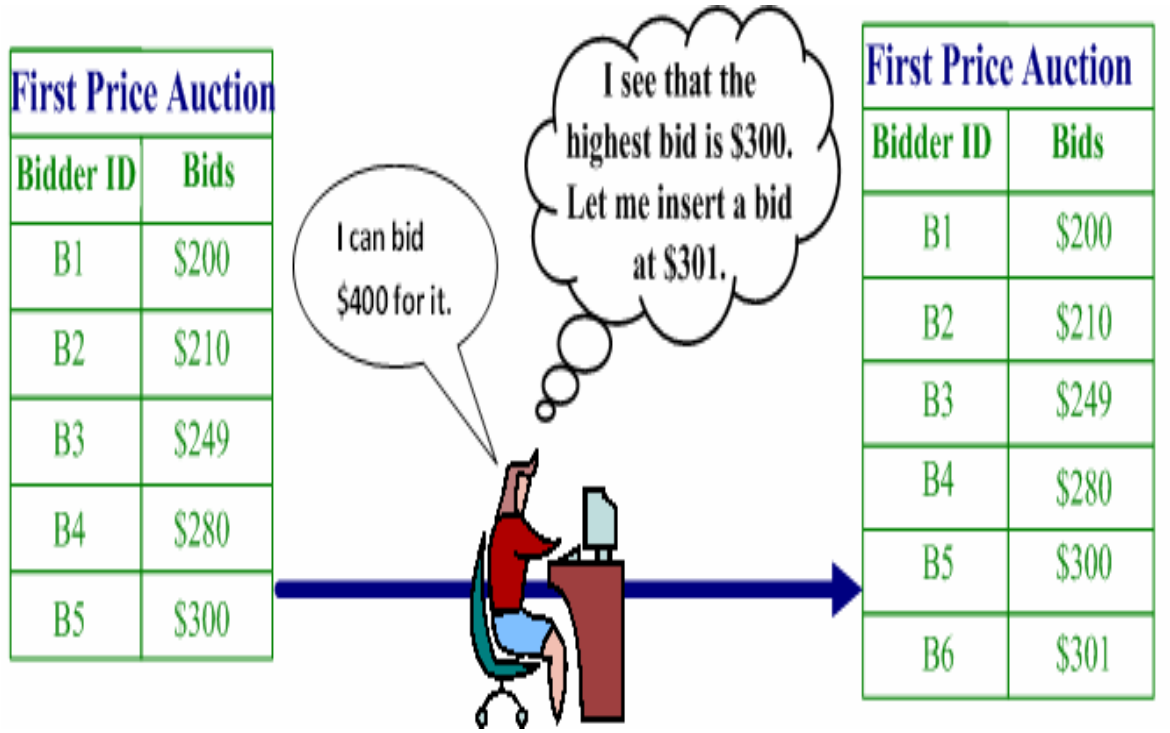

Figure 6. An Example of Bid Shading

2.1.4 Multiple bidding: Multiple bidding, also known as bid shielding, is similar to shill bidding except that it is a fraudulent behavior of buyers rather than sellers. The buyers register several aliases and use them to place multiple bids for the same item. By driving up the price with multiple auction identities, the buyers discourage other potential competitors. After that, they retract all high bids, leaving the lowest winning bid on the auction. At the end, the winner gets the auctioned item at a much lower price. For instance, consider a scenario for a Motorola Razor cell phone auction in which Bidder 3 bids $134.90. Bidder 1, who may have bid previously on this item, now realizes that Bidder 3 is a potential competitor. In order to try and force Bidder 3 out of the competition, Bidder 1 places 3 bids consecutively, namely $135.00, $270.00 and $280.00. The last two bids are obviously much higher than the previous bids; thus, when risk-neutral bidders see this situation, they will quit the auction instead of paying beyond the valuation. Therefore, Bidder 1 can secure the winning position. But, the cheating behavior comes about when Bidder 1 retracts the two high bids at the last minute of the auction, leaving only the

$135.00 bid, which is the lowest cost to win the auction. This cheating method works only at auction websites that allow retracting bids. While almost all current auction websites' rules generally disallow retracting bids, they still allow retracting bids under exceptional circumstances such as a typographical error in entering the bid [18].As we observe, bids retractions occur often in many active auction websites.

2.1.5 Bidding Rings: Bidding rings is also a term related to bidders' fraud. It refers to collusive auction fraud behaviors conducted by several bidders. Several fraudulent bidders form a ring, and the ring members have an agreement not to bid against each other, either by avoiding bidding on the auction or by placing phony (phantom) bids to not compete with each other. The result is that the winner can win the auctioned item at a very low price.

Current Internet auction systems rely solely on feedback based reputation systems to evaluate both buyers and sellers. Nevertheless, the existing traditional reputation system for auction houses has already shown its weakness in providing trusted information. Several researches have shown that the reliability of the reputation system of current auctions house, e.g., eBay, is debatable [17-18]. First, the positive feedbacks are overwhelming but the negative feedbacks are deflated. Deceptive auction users take advantage of the weakness of current rating mechanisms in reputation systems by helping each other artificially build up a good reputation history regardless of their actual behaviors. Rubin, et al. found 95% of eBay sellers have good reputation and 98% of their feedbacks are positive. Furthermore, existing reputation systems are easily manipulated. Malicious users could first accumulate a high feedback score by selling low value goods, and then deal high value goods with that good reputation. For example, a seller first sold pencils and gained a good rating. Now the same seller is selling used cars on the same auction site. Can we trust this seller? No. Because the seller could cheat some used car buyers and then shift again to rebuild a reputation from pencil buyers. Moreover, the existing reputation system provides little information about sellers' degree of honesty. Users may find auction fraud information in feedbacks but when dealing with a seller with a long history, it is impractical to look at the feedbacks page by page. Unfortunately, the anti-fraud information has not been directly reflected in the reputation system so far. In all,

the current reputation system can no longer satisfy people's need for evaluating trustworthiness in online transactions. Rubin, et al. [17] proposed a new reputation system for auction sites to help users protect their interests by indicating auction fraud. The reputation score in the system is a 3-tuple <*N*, *M*, *P*>, where each variable is a number between 0 and 100 (100 indicates 100% confidence of anomaly, and 0 indicates no signs of fraud). The three variables come from three statistical models: average number of bids model (*N*), average minimum starting bid model (*M*), and bidders' profile model (*P*), respectively. The first model identifies sellers whose auctions, on average, attract more bids than auctions posted by other sellers. In this case, the abnormal situation could be produced either by fierce competition among buyers or by shilling behaviors. The first model does not provide an explanation of the cause for this abnormal situation. The second model, *M*, identifies sellers who have a large number of bids that cannot be explained by their low minimum starting bid (in the statistical model considered by the authors, each starting bid is associated with a number of bids it can attract) [19]. Although statistical results show a correlation between minimum starting bid and high volume of bids, it is still not reasonable for the anomalous auctions to attract an overly-high number of bids. Finally, the *P* model identifies anomalous sellers, whose auctions include a group of bidders who bid repeatedly and lose repeatedly as well. The last model explains that the high average number of bids is possibly caused by shill activities. This detection method is indeed a statistics based method.

2.2 Shill-Deterrent Fee Schedule Mechanism [11]

In this paper author have suggested a shill deterrent fee scheduling mechanism and they prove that in the English auction process the fraudster bidder can maximize his or her profit by performing the shill bidding. To deter shill bidding, they have introduced a mechanism which makes shill bidding unbeneficial and this mechanism is known as *SDFS*. This *SDFS* mechanism highlights the role of an auctioneer. This approach apply the two types of charges on the seller i.e. commission fee based on the difference between the winning bid and the seller's reserve fee which is also known as entry fee. Commission rates vary from market to market and are mathematically determined to guarantee the non-

profitability of shill bidding. Further they also demonstrate through examples how this mechanism works and analyze the seller's optimal strategy.

In current online auctions, an auctioneer controls a seller mainly in two ways: whether or not to allow the seller to have an auction in his auction site and the intermediation fee charged to the seller. A strict control over the accessibility has a side-effect; it limits the auctioneer's profit. Besides, it is difficult to recognize who are the potential shill bidders to turn the back on. Therefore, they look into the design of fee schedules to control sellers.

Current fee structures and policies of online auction houses are not theoretically designed to prevent online fraud. For instance, the listing fees and commission rates charged by eBay are so low that in auctions with high value goods these intermediation fees – the seller's loss – can be easily exceeded by the seller's expected gains from shill bidding. This creates an incentive for fraud. If for a final sale of $10,000 the commission fee is only $138 rather than a higher value, say $800, a shill bid aiming to raise the final bid above $10,138 (to be exact, above $10139.87) is less risky than a shill aiming to raise the winning bid above $10,800. Therefore, they suggest that an auctioneer charge a variable listing and commission fees that reward honest sellers and punish dishonest ones. Under this guidance, they design a variable intermediation Shill-deterrent Fee Schedule (SDFS). Our SDFS English auction is conducted according to the following rules:

1. The seller sets the reserve price at r , only bids greater than or equal to r will be accepted by the auctioneer.
2. The buyer with the highest bid v ($v <= r$) wins, and pays his/her bid.
3. *SDFS:* The seller pays the auctioneer a listing fee $(1 - c)/r$ before the auction and a commission fee $(1 - c)(v - r)$ if the item is auctioned off, where $0 \leq C \leq 1$ hence; the seller receives a final payment of $r + c(v - r) - \frac{1-c}{r}$ for the auction sale.
4. Further the seller has to pay the commission fee/entry fee to the auctioneer even if the winning bidder does not pay, unless the seller can prove to the auctioneer that the non-paying winning bidder is not the seller himself or is not affiliated with the seller.

With these rules, shill bidding is riskier because if a shill bid wins, the seller loses not only his listing fee but also $(1 - c)$ times the difference between the shill bid and reserve. If the seller announces too low a reserve price, the seller will be punished with a higher commission fee when the final sale value remains the same. If too high, the seller will be punished with a higher listing fee and a higher risk of no sale.

The intricacies in SDFS English auction rules work hand in hand to encourage sellers to truthfully disclose their optimal reserves before the auction starts. Besides, to ensure the non-profitability of shill bidding, the commission rate $(1 - c)$ is carefully chosen to increase the risks from shill bidding, that is, the seller's loss from shills outweighs his possible gain.

5. In each auction market, varies and is mathematically determined by the characteristics of the market: the buyers' value distribution. An auctioneer would probably charge a higher commission rate in a private-value antique auction market where a shill bid is most likely to be profitable than in a common-value palm pilot auction market.

   Another positive aspect of SDFS English auction rules is that they do not affect honest bidders and do not punish honest sellers.

6. To honest bidders, the rules are the same as in a traditional English auction where the best strategy for each bidder is to raise her bid as long as it is below her valuation. To honest sellers, they can still minimize their intermediation fees because SDFS rewards their truthful disclosure of their optimal reserves.

"Drawbacks: this Mechanism does not able to reduce auction fraud due to collusive bidding, multiple bidding etc."

2.3 Collusive bidding detection algorithm [12]

As we already know that Shill bidding is known as the bogus bids which are commence into an auction in order to drive up the final price for the seller or the profit of the seller, thereby this shill bids are used to cheats legitimate bidders. Trevathan and Read have proposed an algorithm to which detect the occurrence of shill bidding in online auction process. The algorithm performing the action by monitoring bidding patterns over a series of auctions or the bidding strategy which has used over a period of online auction process. After the analysis it gives each bidder a *shill score (based on his/her behavior over a period of time in several auction process)* to indicate the likelihood that they are engaging in shill behavior. Whereas the proposed algorithm is somewhat able to categorize those users who are having some suspicious behavior according to their shill score. However, there are several possible situations exists where there may be two or more shill bidders working in collusion with each other. Colluding shill bidders are able to engage in more sophisticated strategies that are harder to detect. This paper proposes an approach for detecting colluding shill bidders, which is referred to as the collusion score (discussed above in this paragraph). Further, collusion score is used to detect the fraudster user by either forming a collusive graph or colluding group, or it forces the colluders to act individually like a single shill also.

Collusion Graph:

The collusion graph indicates which bidders are likely to be in collusion with each other. There are two different forms of the collusion graph based on whether shills use the alternating bid, or the alternating auction strategy.

To detect colluding groups employing the alternating bid strategy, bidders are represented as a graph $G = (V;E)$. V is the set of bidders, and E is an edge between two bidders, indicating that they have both participated in the same auction.

The goal of the collusion graph is to find a subset; C is subset of V, which contains the bidders that are most likely to be in collusion with each other. A bidder initially has no edges connecting it to other bidders (i.e., the set E is empty).

Given two bidders, $v_i; v_j \in V, i \neq j$, that participate in the same auction, an edge $e_{i;j}$ is added to E that connects these two bidders together. If bidders $v_i; v_j$ participate in more than one

auction simultaneously, weights are added to the edge $e_{i;j}$ to indicate the number of auctions they were present in together. The idea is that *G* will form a graph connecting colluding bidders together.

The higher the edge weighting between two bidders, the greater the likelihood that the two bidders are in collusion with each other. Figure 7 gives an example of a collusion graph. Here there are two colluding bidders. In general, shills will have the most number of edges (i.e., highest degree), and higher edge weightings than legitimate bidders.

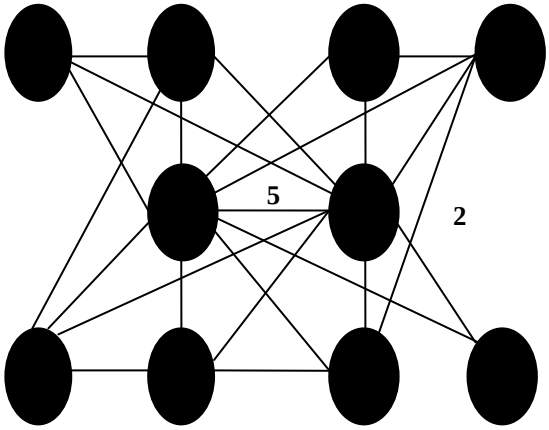

Figure 7: Example Collusion Graph [12]

Given a node with degree *k*, each edge weight is denoted as wj , $1 \leq j \leq l$. The base collusion rating,

n'_i, for a bidder *i* is calculated as the sum of the edge weights incident to the node:

$$n'_I = \sum_j^k w_j \qquad \ldots(1)$$

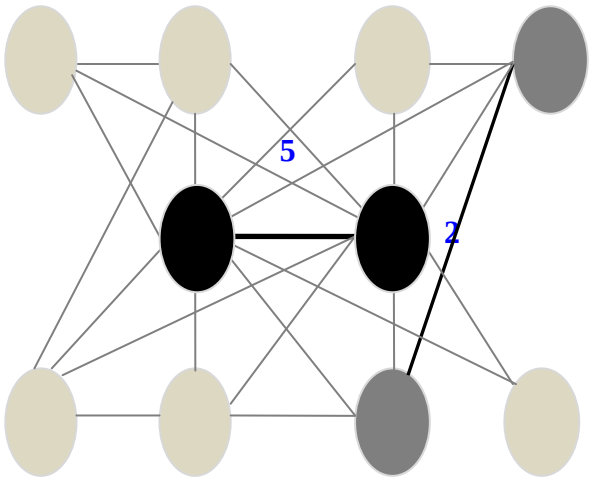

Figure 8. Potential Colluding Bidders

Figure 8 shows the previous example of the collusion graph after the algorithm has been run. The bold nodes indicate the suspect bidders.

- "Collusive score" to detect collusive shills controlled by one seller analysis takes place according to three strategies
    - Alternating bidding strategy
    - Alternating auction strategy
    - Hybrid Strategy
- Based on collusive score auction fraud can be minimized

Drawbacks: Not much efficient if fraudsters are clever enough

2.4 Hidden Markov Model approach *[6,21]*

Abhinav shrivastva et.al [6] proposed the HMM based approach for credit card fraud detection. Before starting this approach they have classified the credit card into two types: 1) physical card and 2) virtual card. In the shopping or purchase which is performed by physical card, the buyer presents his card physically to a merchant for making a payment. To carry out fraudulent transactions in this kind of purchase transaction, fraudster has to steal the credit card of other. If the cardholder does not comprehend the loss of card, it can

lead to a significant financial loss to the credit card company. In the second kind of purchase with the virtual credit card, buyer has to provide only card number, expiration date, and secure code/cvv code in order to make the required payment. It is not necessary to have the credit card physically present. Usually such kind of purchase is performs on internet medium or any e-commerce platform via telephone. In this type of credit card purchase it is very easy to commit fraud. Because in to cheat the legitimate user a fraudster only required obtaining the card details (such as credit card number, cvv number and expiry date). In many time, the legitimate cardholder is not aware that someone has seen or stolen his/her card information to commit fraud. So in this case to prevent possible online frauds we required some approach which analyze the behavior pattern of user for his/her expenditures. Fraud detection based on the analysis of existing purchase data of cardholder is a hopeful way to prevent the credit card frauds over internet.

2.4.1 HMM Background:

An HMM is a double embedded stochastic process with two hierarchy levels. It can be used to model much more complicated stochastic processes as compared to a traditional Markov model. An HMM has a finite set of states governed by a set of transition probabilities. In a particular state, an outcome or observation can be generated according to an associated probability distribution. It is only the outcome and not the state that is visible to an external observer. HMM-based applications are common in various areas such as speech recognition, bioinformatics, and genomics. They classify TCP network traffic as an attack or normal using HMM [22-24].

Now, to make use of Hidden Markove Model in the credit card fraud detection it is mandatory to map the credit card transaction performed by the user over the HMM. In order to do so author has start by first deciding the observation symbols in the required HMM. Than we have to quantize the purchase values x into M price ranges V_1, V_2, . . . V_M, forming the observation symbols. The actual price range for each symbol is configurable based on the spending habit of individual cardholders. These price ranges can be determined dynamically by applying a clustering algorithm on the values of each cardholder's transactions, they use V_k, k = 1, 2, . . .M, to represent both the observation symbol, as well as the corresponding price range. In this work, they consider only three

price ranges, namely, low (l), medium (m), and high (h). Set of observation symbols is, therefore, V= {l, m, h} making M= 3. For example, let l = (0,$100], m = ($100,$500] and h = ($500, credit card limit]. If a cardholder performs a transaction of $190, then the corresponding observation symbol is m. A credit cardholder makes different kinds of purchases of different amounts over a period of time. One possibility is to consider the sequence of transaction amounts and look for deviations in them.

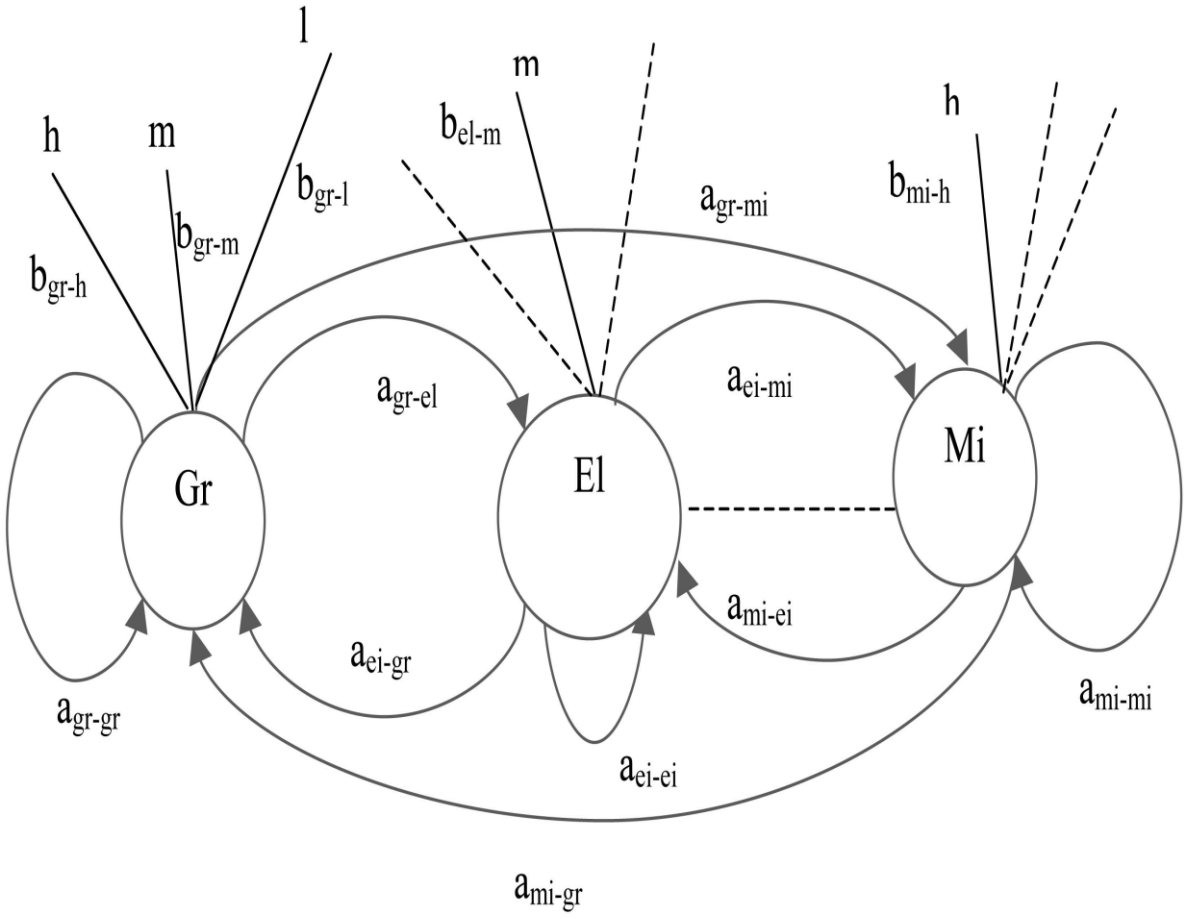

Figure 9. HMM for credit card fraud detection [6]

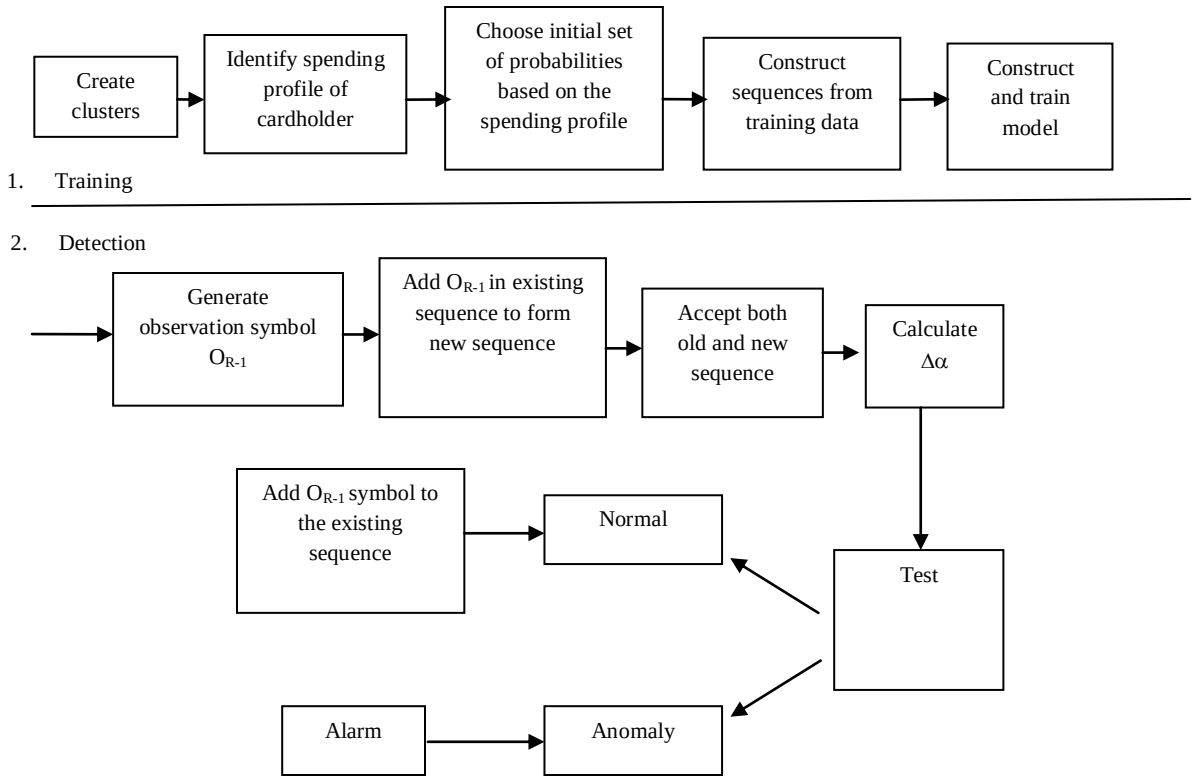

Figure 10. Process flow of the proposed FDS [6]

2.4.2 Choice of Design Parameters:

Since there are three parameters in an HMM, we need to vary one at a time keeping the other two fixed, thus generating a large number of possible combinations. For choosing the design parameters, they generate transaction sequences using 95 percent low value, 3 percent medium value, and 2 percent high value transactions.

The reason for using this mix is that it represents a profile that strongly resembles a ls customer profile. For parameter selection, the sequence length is varied from 5 to 25 in steps of 5. The threshold values considered are 30 percent, 50 percent, 70 percent, and 90 percent. The number of states is varied from 5 to 10 in steps of 1. They consider both TP and FP for deciding the optimum parameter values.

Drawbacks: Not efficient is case of new user with no previous feedback

2.5 *ATM* (Agent based trust management) for detecting online auction frauds) [20]

A multi-agent system (MAS) consists of a number of software agents that can work autonomously, but need to coordinate with each other to accomplish tasks and missions. Each agent is built with enough capability to work independently. The coordination model based on asynchronous message passing among agents provides a uniform interface for their interaction; while the mechanism of storing and routing messages enhances the fault tolerance capability of the whole system. Figure 11 is an overview of an agent-based trustworthy online auction house. The auction house is a multi-agent system, which consists of a main agent, an agent-based trust management (ATM) module, and a number of auction agents. The main agent manages the auction house and provides an interface for the auction house administrator to manipulate and monitor the auction house. The main agent is responsible for initializing the ATM module and generating an auction agent for each auction started. A user or a bidder can join one or more than one auction at the same time, and put in bids on auctioned items concurrently. All auction data is stored in a local or remote auction database. The agent-based trust management (ATM) module in an auction house is the key component for maintaining trustworthiness of the online auction system. The major tasks of the ATM are to detect shills and update the trust levels of the shill bidders. When a shill bidder is detected, the ATM informs the responsible auction agents, and the auction agents will then notify all involved users and cancel the corresponding auctions immediately.

2.5.1 Agent-based trust management module:

Figure 11 shows the general architecture of the agent-based trust management (ATM) module for online auction systems, which consists of three types of agents, i.e., the security agent, the analysis agent and the monitoring agent.

From Figure 12, we can see that before a user can start trading in an auction, she must first be authenticated to get the initial pass. The authentication process is based on the user's credential as well as her user name and password.

After the authentication process is completed, the authorization process starts. In their ATM module, they have adopted the role-based access control (RBAC) mechanism to effectively.

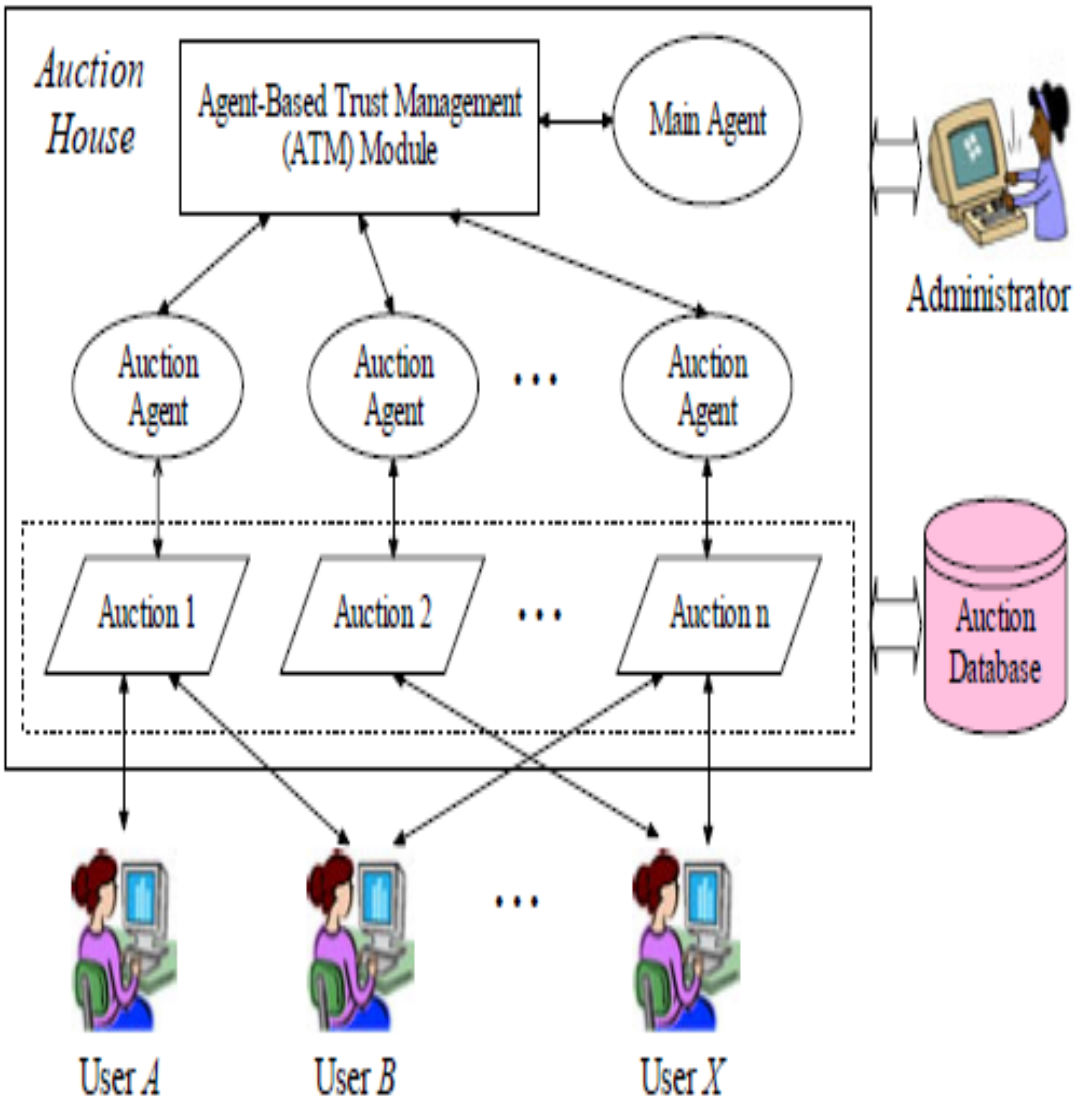

Figure 11. A trustworthy online auction house

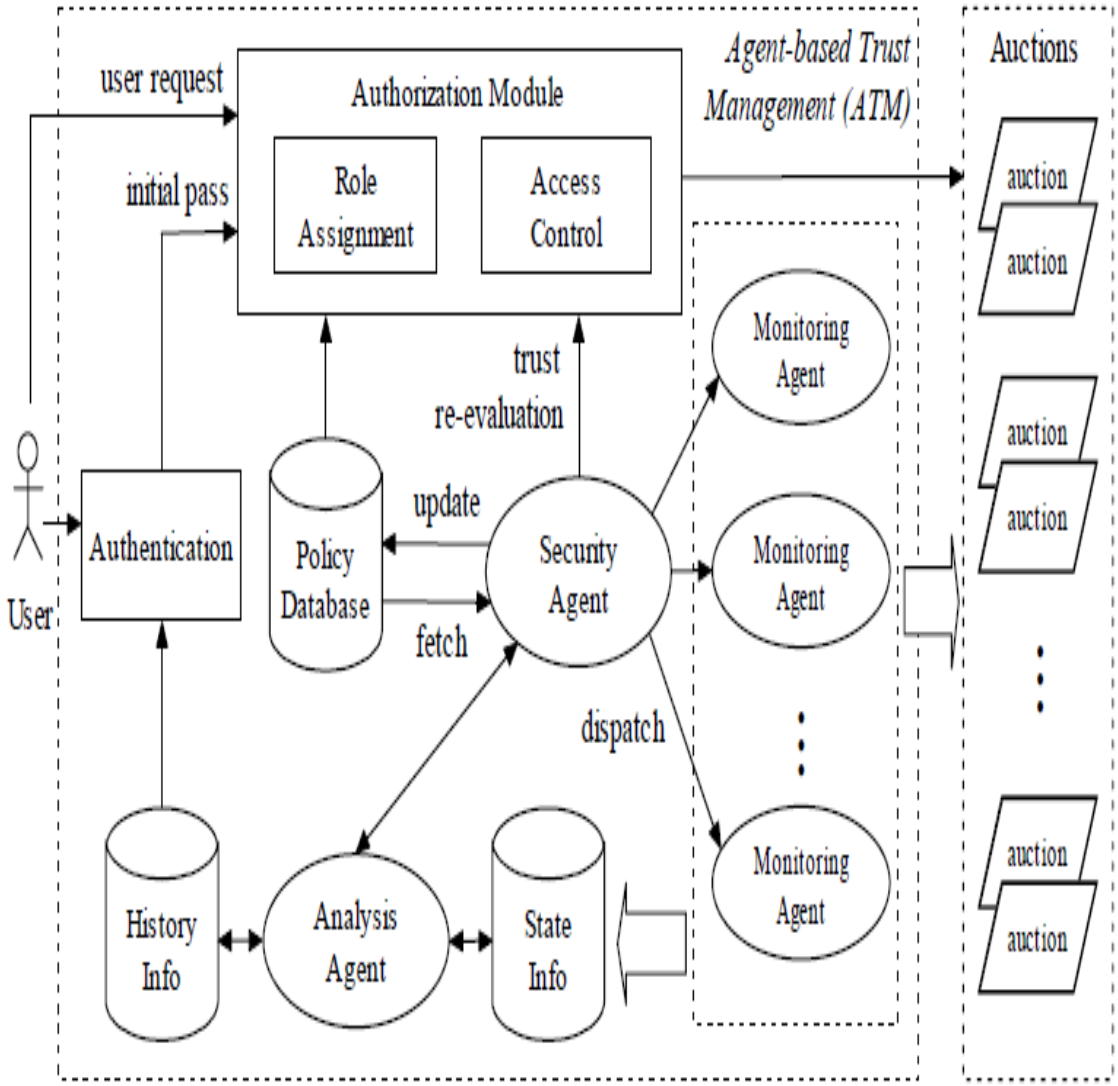

Figure 12. Agent-based trust management (ATM) module [20]

2.5.2. Agent communication in ATM module:

Software agents typically use asynchronous message passing for agent communication. One of the major agent communication standards is called FIPA-ACL (Foundation for Intelligent, Physical Agents – Agent Communication Language). FIPA-ACL is grounded in speech act theory, which states that messages represent actions or communicative acts – also known as speech acts or performatives. FIPA-ACL defines a set of 22 communicative acts, such as inform, request, agree, not understood, and refuse. In Figure 13, by using

UML sequence diagram to they have illustrated the communication protocol for shill detection among various agents, namely the security agent (SecurAgent), the analysis agent (AnalyAgent), the monitoring agent (MonAgent), and the auction agent (AucAgent).

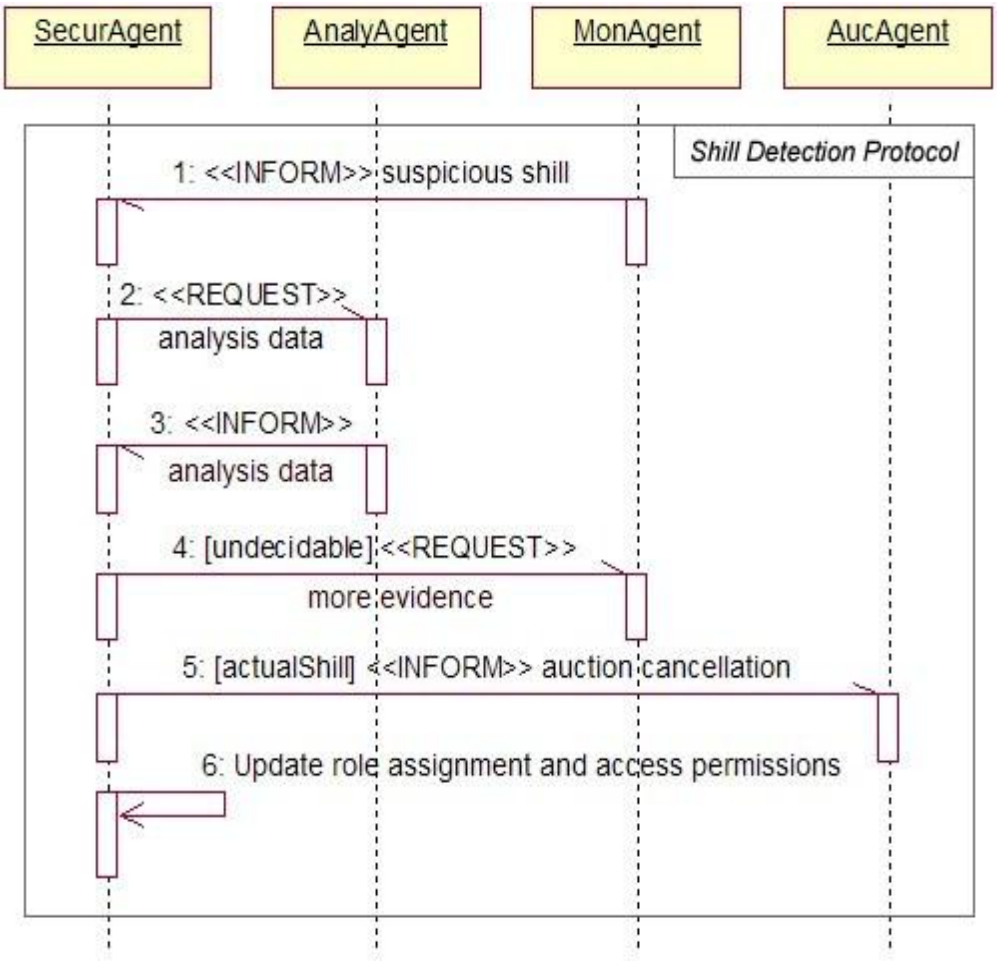

Figure 13. Interaction protocol for shill detection [20]

From the diagram, we can see that the monitoring agent first informs the security agent about a suspicious shill, say bidding agent *B*1. Upon receiving this message, the security agent requests analytical data, such as shilling score and reputation score of B1, from the analysis agent. After analyzing the auction data as well as the history information of *B*1, the analysis agent informs the security agent about the analytical results. When the security agent receives the analytical data, it verifies if the suspicious shill is an actual shill. In case

the security agent will not be able to make such a decision, it will request more evidence from the monitoring agent. In this case, steps 1-3 of the communication protocol must be repeated (for simplicity, we did not show the loop in Figure 13). When an actual shill is detected, the security agent informs the involved auction agent to cancel the affected auction, and it also updates the role assignment and access permissions of the shill bidder.

Drawback: Again for new user not appropriate

2.6 Online Banking Fraud Detection Based on Local and Global Behavior [8]

This paper presents a fraud detection system proposed for online banking that is based on local and global observations of users' behavior. Differential analysis is used to obtain local evidence of fraud where a significant deviation from normal behavior indicates a potential fraud. This evidence is strengthened or weakened by the user's global behavior. In this case, the evidence of fraud is based on the number of accesses performed by the user and by a probability value that varies over time. The Dempster's rule of combination is applied to these evidences for final suspicion score of fraud [25].

In the global analysis approach, each device is monitored and classified as legitimate or fraudulent with certain probability based on global information. This is based on three assumptions. First, it is assumed that each device used for online banking has a single identification. The second assumption is based on the fact that the probability of a transaction being a fraud increases with the number of accounts accessed by the same source that requested the current transaction. The third assumption comes from the fact that the only way to know that a fraud has been perpetrated is when the customer reports it. The major contribution of this paper is the finding, by empirical analysis of a real-world transaction dataset, that the effective identification of access devices and monitoring the number of different accounts accessed by each device is a very promising supplement for other methods in detecting fraudulent behavior in online banking applications [26].

An empirical analysis performed on real-world transactions datasets revealed that most of frauds had the following behavior characteristics:

- Large number of different accounts accessed by a single fraudster;
- Transactions involving small values in many accounts;
- More payment transactions than usual in a single account;
- Increased number of password failures before the occurrence of frauds.

While the latter two characteristics can be detected by differential analysis using local attributes, the first two characteristics need information about similar attacks in other accounts. The fraud detection system described in the next section takes these characteristics into account.

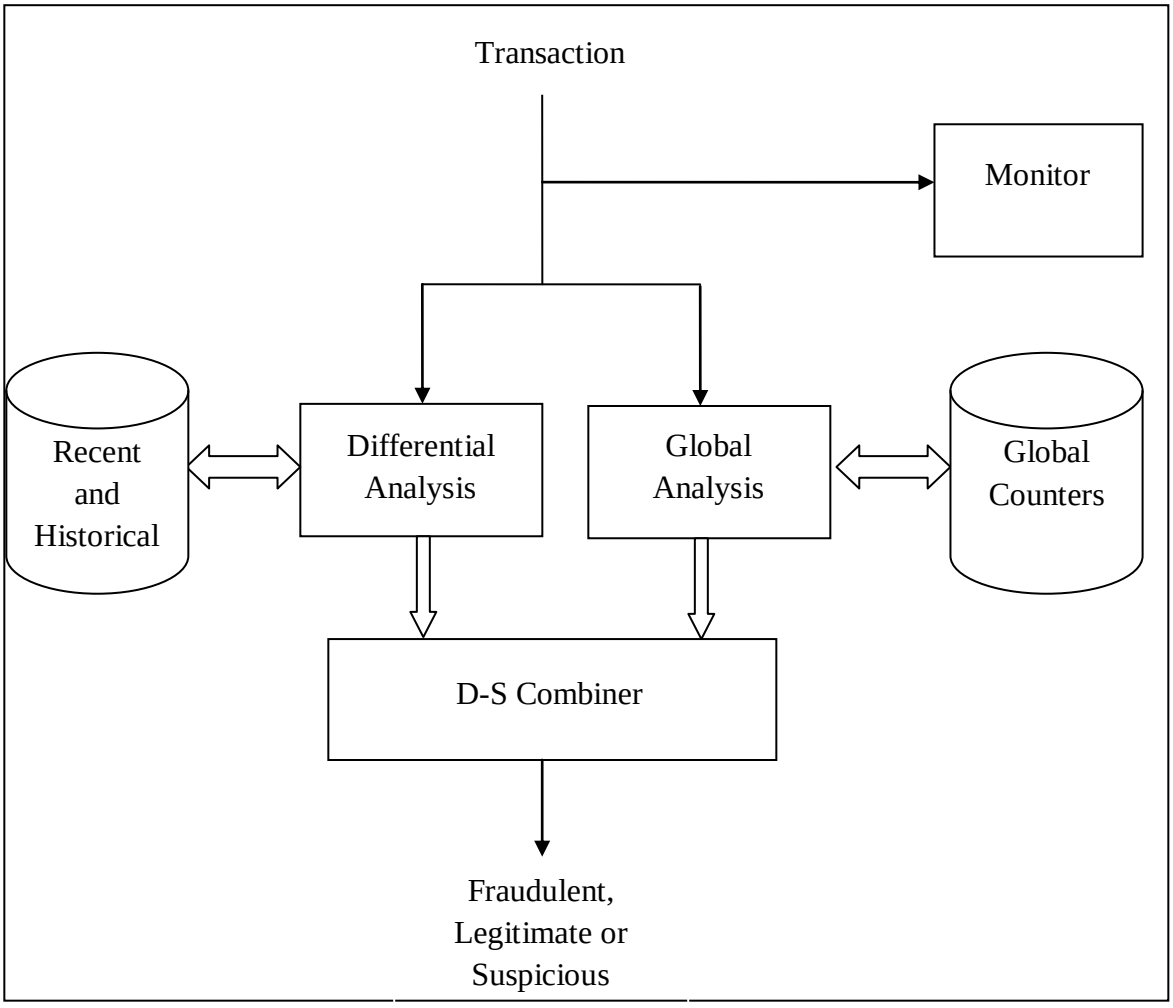

Figure 14. Fraud Detection System

2.7 A Cost-Effective Method for Early Fraud Detection in Online Auctions [27]

A cost effective method for early fraud detection will be introduced in this section. The proposed method conducts a set of detection processes without lengthy computation and intractable data downloading. In particular, the detection accuracy can be maintained by such a method, which would be greatly helpful in developing an online fraud early detection system.

For a given data set, a detection model can be built by applying a learning algorithm with an attribute set to refine hidden information in the data set. In practice, fewer measured attributes result in less computational costs. Thus, we are going to develop a method to reduce the number of measured attributes used for modeling. The number of elements in the attribute set is corresponding to the data dimensionality of the built model.

The capability of an early fraud system is mainly determined by discovering the abnormal or irregular patterns hiding in the training data. To detect fraud effectively, a detection system is required to determine two proper key components: 1) a set of measured attributes, 2) a learning algorithm for modeling. For the measured attribute set, we have evaluated different measured attribute candidates in our previous research with different evaluators, and then selected a concise set of ten measured attributes to meet the requirements for effective fraud detection (See Table 4). These measured attributes can describe significant abnormal and fraudulent behavior clues and thus will be used as input data for measured attribute reduction testing in this study.

Since the strategies used by fraudsters will fluctuate over time, it is difficult to identify fraudsters using single static 184 models. Fortunately, the effectiveness of a fraud detection system can be adapted by continuously applying learning algorithms on newly-added instances or devising new attributes for describing novel tricks.

Since the trend of online auction fraud is to maximize the profit in a short period, the lifecycle of fraudsters has been gradually shortening in recent years. For instance, fraudsters could fabricate a lot of positive ratings by fake transactions in about a month, and then start defrauding quickly. As a result, by the time users have identified a fraud, it is usually too late to react. While the user becomes a victim, the fraudster has closed his account. However, if data for modeling only extracted features that occur in the last part of

transaction histories, the problem of misjudgment and late detection can be alleviated effectively [28].

Table 4.. Measurment attributes [27]

S.No.	Measured Attribute	Description
1	DensityOfPos	Density of positive ratings
2	EndCloseToPos	Average time to obtain positive rating after closing bid
3	RatioOfPos	Ratio of positive ratings to total feedback count
4	RatioOfSTos	For a seller, the ratio of positive ratings from other sellers to all positive ratings
5	LastNegCloseToCur	Time difference from the last negative rating to the current time
6	RatioOfNeg	Ratio of negative ratings to total feedback count
7	SellingNumberLast30	Number of sold items in the Last 30 days
8	SellingNegativeNumberLast30	Number of negative ratings from selling in the Last 30 days
9	NumberOfPositive	Number of Positive ratings
10	EasypayRating	Numerical rating from Easy Pay System

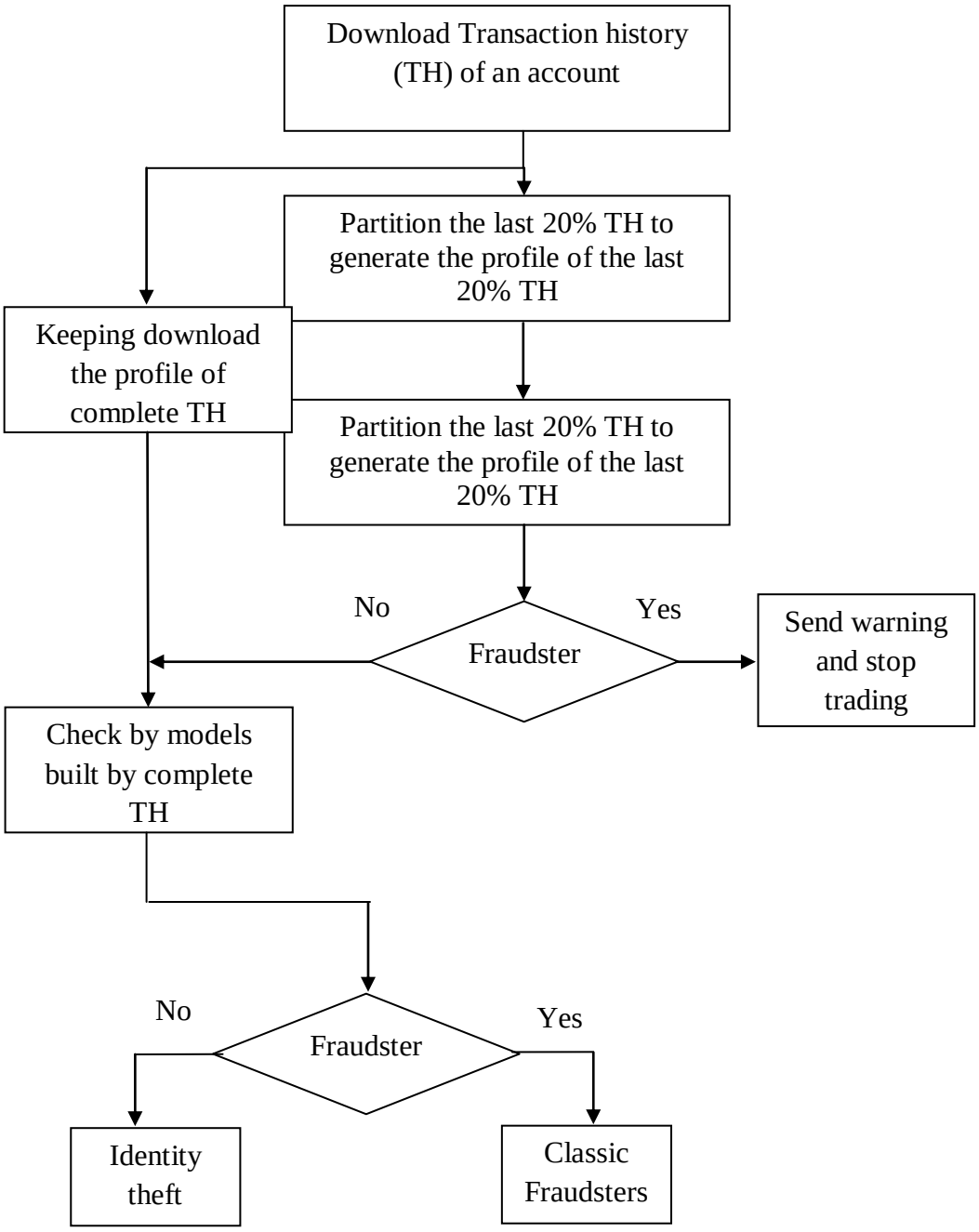

Figure 15. Procedure of the cost-effective detection method [27]

3. Proposed Framework:

In this chapter, I have elaborated the proposed framework *(Online Hybrid Model)* for the prevention, detection and elimination of online frauds. Firstly we have described the architecture of the proposed framework followed by its lifecycle. After that we have discussed the several methodologies which are involved in the process of prevention, detection and elimination.

3.1 Online Hybrid Model (OHM): Architecture [10]

In order to prevent and detect the online in-auction, non-delivery/merchandise and identity theft frauds, OHM provides a three layer architecture. Further, each layer is treated as individual modules which are interacting with each other. The glimpse of each layer is approach is shown by Figure 16 which shows it contains three modules i.e. Users, OHM and Web-Servers. The working of these modules is defined below.

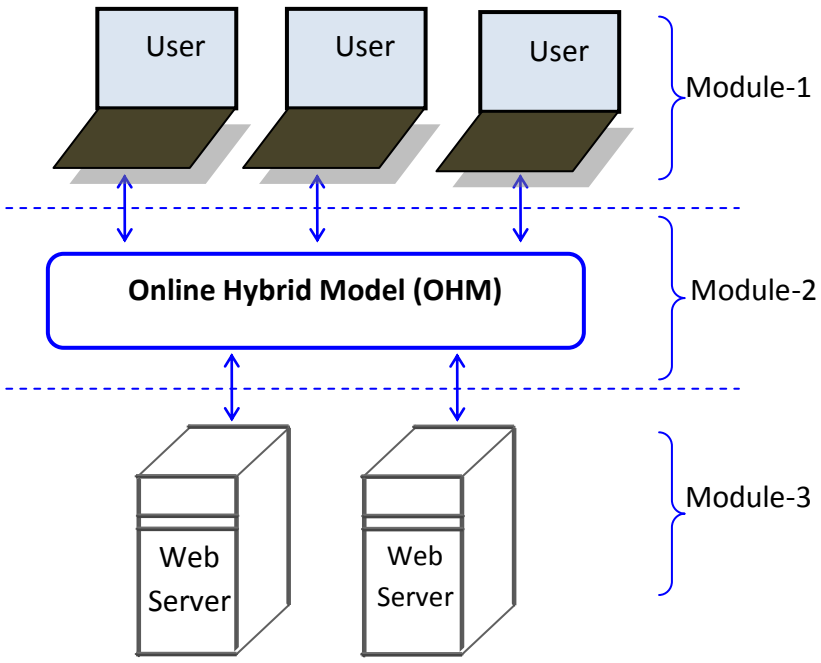

Figure 16. OHM Architecture

1. **Users:** they can be of two type either buyer or seller. Each user, when he/she wants to interact with any E-Commerce web-server for participate in any auction process or to buy goods, it is required that they must verify from OHM.

2. **OHM**: it is the approach which authenticates both user and web-server also regularly monitored the interaction process between users and web server. After authentication OHM issues the OC (OHM Certificate) that certifies the both web servers and users and helps to reduce online frauds. It is mandatory for both users and web-servers to having 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 digital 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.

3.2 *OHM* Life Cycle (*OHMLC*) [29]

The main idea behind the *OHM* is to minimize the possibilities of fraud at very beginning level so that both resource and time can be saved. Further *OHM* adopts variety of mechanism for different possible frauds. *OHM* is mainly design for the most frequent frauds like online auction, merchandise/non-delivery, and identity theft frauds. Apart from these frauds *OHM* can handle various other possible frauds such as credit card fraud, money-transfer fraud, and online investment scheme frauds.

Further *OHM* Life Cycle (*OHMLC*) works for three modules, i.e. User, *OHM* and Web-Server (figure 17). *OHMLC* starts with interaction of user with web-server where *OHM* regularly monitors this interaction and performs the appropriate action according to the interaction behavior. *OHMLC* is responsible to implement prevention/detection/elimination in accordance to the monitored behavior. Both user and web-server entities work within this

OHMLC environment. *OHMLC* starts from the prevention approaches of *OHM* during the initial phase of user/web-server interaction. The basic steps of *OHMLC* are shown in Table 5. In first two steps *OHM* performs fraud prevention while in last two steps *OHM* studies the behavior of user/web-server interaction and detects any possibility of fraud and then eliminates it.

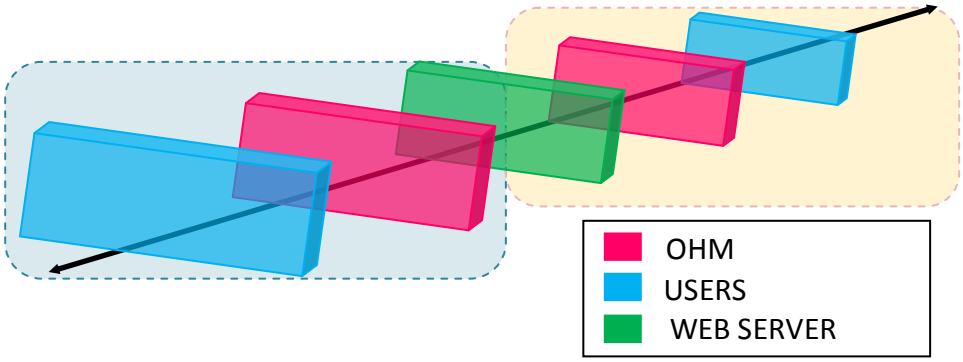

Figure 17. Online Hybrid Model Life Cycle (*OHMLC*)

Table 5. OHMLC Steps

Step	**Input**	**Output**
Registration of User	User personal details	Issue OC to certify user
Registration of Web-Sever	Web-Server Information	Certify the Web-Server
Detection of Fraud	Users Behavior pattern	Mark the user ID and Monitoring of User
Elimination of Fraud	Suspicious user activities	Block the user and stop process

3.4 OHM Approach [10][29]:

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.

3.3.1. OHM for Prevention (OHM-P): This approach provides the verification and authentication steps to prevent the Online fraud. This fraud prevention scheme contains three parts as:

a. *User authentication:* for authenticate the user OHM takes 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 match with address provided by user. The difference between the two addresses should below the threshold level otherwise user registration is 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 require this id for authentic the permanent address of user.

4. *Credit / ATM / Debit card information:* OHM requires the any of the card information (which is use by user to perform final transaction) except password. OHM verifies this detail and gets the last 5transaction statement from the bank with their location also. If the locations where the card has been used from last one 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 is 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 the mark then it cancel 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.

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 required 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 ≥ 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)

{

Verify: *If*[(average_location - current_location) ≤ 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 ;}

b. **Web server authentication:** OHM authenticate the web server by taking these 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.

Algorithm for web server authentication:

This algorithm authenticates the web-server according to HMM [30] and user's feedback with verification of digital signature of web-server.

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]≥feedback_behavior_threshold)

/*feedback behavior[HMM] obtain by HMM*/

Then Issues OC with OHM_Rank and store in OHM_DB;

Else

Authentication failed;

c. Exit }

For this it required some input and after execution it authenticates the user by issuing OC.

*3.3.2. OHM for Detection (OHM-D)***:** this is the fraud detection scheme which is exclusively design for auction fraud i.e. during the auction process only. Because after authentication of both users and web server there might be chances of frauds like Bid shilling, Collusive shilling, Multiple bidding**.**

OHM regularly monitors the auction process by adopting SDFS mechanism, which reduce the extra profit earn by shill bidding by the seller. 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 provide auction platform. On the whole, SDFS inhibit shilling behavior also. Which provide shill deterrent fee. And monitoring the bidding behavior (i) incremented bid: when the bid for a item increases suddenly (ii) alternating bid strategy: when two bidders bid alternatively in the same auction by more than threshold time (iii) alternating auction strategy, where bidders alternatively bids on different auctions.

Further, this has two phases one is monitoring phase in which OHM monitors the user-web server interaction and second is detection or active monitoring phase in which based on user attributes OHM closely monitors the behavior of user. OHM-D also works on two preliminary policies i.e. check-out policy and reserve price setting policy. First we have described the OHM policies and then we have elaborated the OHM-D.

3.3.2.1 OHM Policies: OHM uses two policies which help in detecting and preventing the online frauds. Here we describe both the policies which are as follows:

3.3.2.1.1.Check out policy: This policy implements when user check-out form the e-commerce website and enters the payment credentials than OHM verifies the shopping amount (current amount which is paying by user) with the user's expenditure behavior based threshold amount.

If the shopping amount exceeds the threshold than an authentication is required. For this authentication purpose user is asked to submit the mobile verification code which is sending on the associated mobile number with the OHM ID. Figure 18 show the flow of steps involved in implementing the check-out policy.

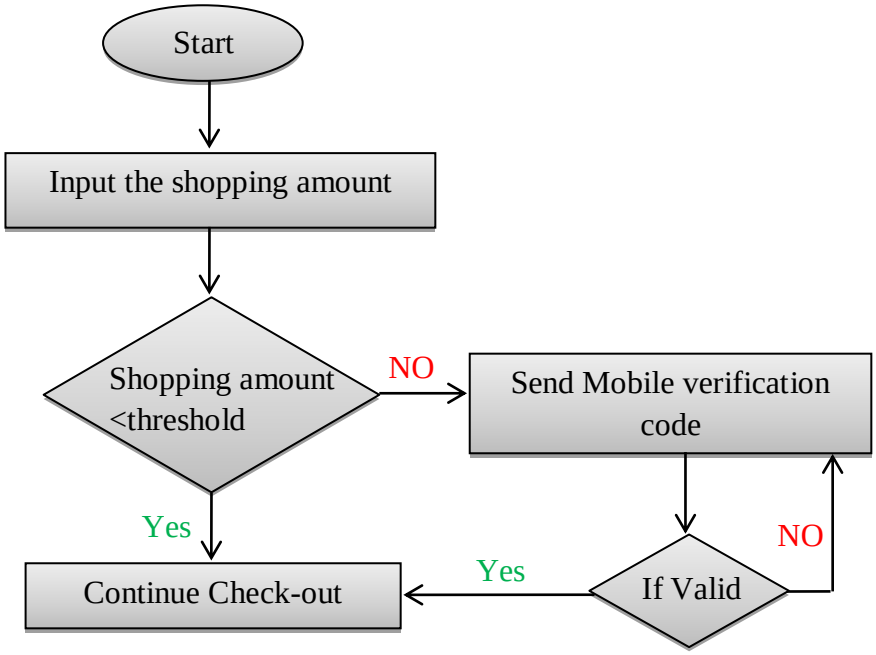

Figure 18. Check-out policy flow

Algorithm for Check-out policy

Initial Condition:	shopping_amount, threshold_amount,mobile_number;
Local Variable:	mobile_code;
Final Condition:	Either check out or stop process

User Authenticate {

a. Input: shopping_amount/* provide by user */
Mobile_number /* from ohm registration DB */

b. Calculate:

If [{(shopping_amount<threshold_amount)
Then
Go to step d;
Else
Go to step c;
End else;
End if;

c. Send mobile_code to the registered mobile number of OHM ID;

Verify:

If(mobile_code=true)
Then
Go to step d;
Else
Stop;

d. Continue to check out;

e. Exit. }

3.3.2.1.2 *Reserve price policy for auction:* While in Auction events OHM follows the SDFS mechanism [6]. According to this OHM enforced the auctioneer to charge the entry fee end commission fee to the seller. Entry fee corresponding to the initial reserve price of the auction object and commission fee charged on the difference between winning bid and initial reserve fee.

$$Net\ Profit = W - ((W_C + R_C) + R \quad \ldots. (2)$$

Here:

R= Initial reserve price

R_C= Reserve price commission rate

W_C= Winning price commission rate

W= Last winning bid amount

So, if seller sets higher reserve price than he/she has to pay more entry fee and if he/she tries to do shilling than it costs in higher commission fee. So this mechanism forced the seller to set reserve price honestly.

Algorithm for Reserve price setting:

Initial Condition:reserve_price, win_bid_value;

Local Variable: earn_value;

Final Condition: entry_fee, commission_fee;

Reserve price{

a. Input: reserve_price ;

b. Calculate:

Entry_fee= % of reserve_price;

c. Input: win_bid_value;

d. Calculate:

$$Net\ Profit = W - ((W_C + R_C) + R$$

Exit. }

3.3.2.2 OHM Monitoring: This is the first phase of OHM-D approach. In this OHM monitors the interaction between the users and web-server continuously. Especially in the in-auction process when the possible chances of shill bidding is high than OHM monitoring process helps to detect shill bidding behavior. For this we find the correlation between the two bidders and this can be done using Pearson's Correlation formula. The value of correlation coefficient ranging from -1 to 1. The correlation coefficient (r) shows the relation between two data sets as:

Highly related if $0.5 < r < 1.0$ or $-0.5 < r < 1.0$, Medium related, if $0.3 < r < 0.5$ or$-0.3 < r < 0.5$, Less related if $0.1 < r < 0.3$ or $-0.3 < r < -0.3$

The Pearson's correlation coefficient formula can be given as:

$$r_{x,y} = \frac{\sum_{i=1}^{n}(x_i - \overline{x})(y_i - \overline{y})}{\sqrt{\sum_{i=1}^{n}(x_i - \overline{x})^2}\sqrt{\sum_{i=1}^{n}(y_i - \overline{y})^2}} \quad \text{....(3)}$$

In OHM-D x and y representing the bidding data of two bidders and n represents the total number of bids.Thus, if the value of r is closer to 1 than it shows that the user behavior is much related to each other and the possibility of shilling is less. On the other hand if the value of r is less than .5 than the possibility of shilling is high.

3.3.2.3 Active Monitoring: This is the second phase of OHM-D approach. This is also known as active monitoring of the suspicious user behavior. In order to detect frauds OHM uses some attributes, which are known as user's features. Set of user features [8]. Further we have taken these set of features into the count because.

- In any auction when shilling is happens that generally it involves higher number of bides per seller ratio.
- The fundamental purpose of shilling is to avoid the wining of auction.
- Fraudulent user generally places the shill bids in the beginning of auction because they initially try to attract the other user for the participation in auction.
    - For this sellers could setup a higher hidden reserve price
    - The higher early bid attracts the user by serve as stimulating bids.
    - In internet auction process shills generally do not receives the much number of feedback (here feedback implies positive feedback)

1.Auction count: It is calculated as the number of auction event in which user is participated.

2.Reputation: The reputation of a particular user is calculated as the percentage of positive feedback of that user.

3.Average Bid Amount: It is calculated as the average of the value of all bids made by user.

4.Increment in Bid: It is calculated as the increment in the last bid over the average bid.

5.Bids per Auction: It is calculated as the number of bids made by the user in an auction.

By using these attributes OHM monitors the behavior of user when he/she interacting with the web-server. Before detection and elimination of fraudulent activity OHM accomplishes certain tasks i.e.

1. When any suspicious user activity get detected (according to monitoring mechanism discussed above), OHM puts the respective user id into monitoring log. (Monitoring log is the temporary file which is used for active user monitoring).
2. Then OHM starts active monitoring of users which have their ids in log file. When OHM detects or found any fraudulent activity of a user than OHM stores that id information in database and take the action accordingly

Further OHM informs the other entire user about the fraudulent activities so that others can save themselves to become a victim. Figure 19 shows the steps involved in the OHM-D mechanism.

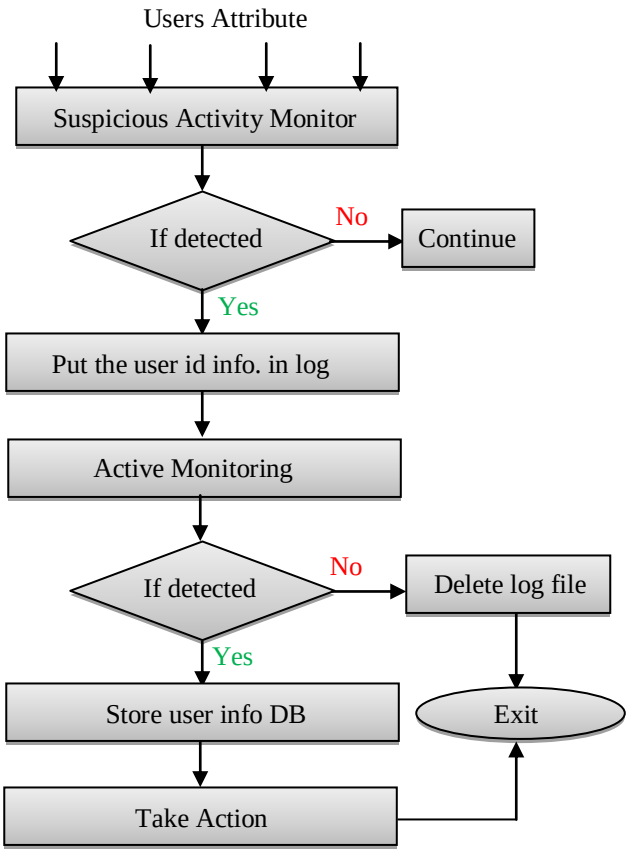

Figure 19. OHM-D approach flow

3.4 Requirement Engineering and Logical Design for OHM

Requirement engineering outlines the logical requirements for the *OHM* modules (User, *OHM* and Web-server). Further logical design shows logical structure of *OHM* modules. Here we discuss all the three *OHM* modules one by one.

Module-1 User:

This module of *OHM* consists of entities which are willing to access web-servers for their services like online shopping, online selling of products, online auction, online entertainment etc. In order to access these services, *OHM* bounds the user for registration process. As shown in figure 20, users are classified into two groups i.e. buyers and sellers. Buyer is one who access web-server for buying goods. Further they are classified in two categories: non-auction and auction buyers. Non-auction buyer directly buys the goods from merchants via web-servers. While auction buyers participates in auction process with intension to buy the auctioning goods.

The second type of user of *OHMLC* is seller who registers themselves on the web-server to sell their goods or products. Sellers are also classified in two categories: non-auction and auction sellers. Non-auction seller sells their goods or products via e-commerce website (e.g. olx.in, quickr.com etc.). While auction sellers post their items for auction and is responsible for conducting the auction process through the auction websites (e.g. eBay. in, etc.).

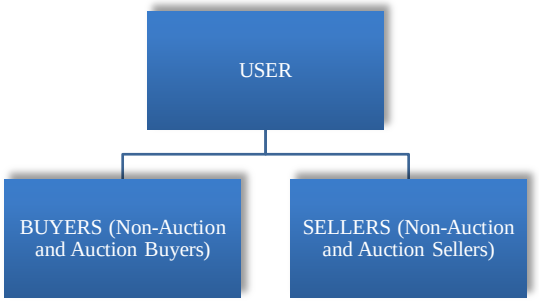

Figure 20. Classification of Users [29]

OHM ensures registration of each type of user for authentication. The process flow diagram of user module is shown in figure 21 which describes that whenever a user desire to access web-server then web-server verifies *OHM* ID of respective user. If user has valid *OHM* ID then it allow access to user otherwise it redirect the user to *OHM* for the registration process.

Module -2 OHM:

OHM performs all the verification, validation process for prevention of online frauds. Further it is responsible for the detection and elimination of possible frauds. Figure 22 shows the work flow classification of *OHM* module. Initially, *OHM* approaches are classified into two types one is prevention and another is detection. Further prevention consists of registration process which is for both user and web-server and policies which consists *OHM* rules and regulations to prevent online frauds.

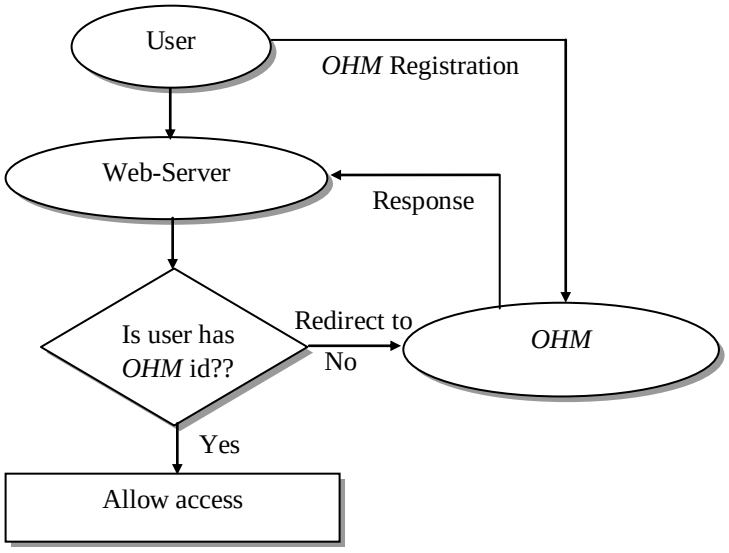

Figure 21. User Process Flow [29]

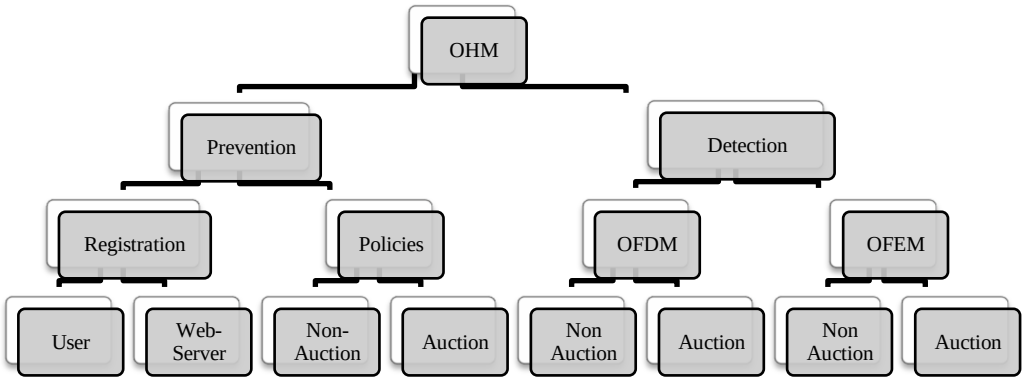

Figure 22.Classification of *OHM* Work Flow

Again *OHM* has separate policies for non-auction and auction process. The detection consists of two approaches one is online fraud detection mechanism (OFDM) which is different for non-Auction and auction process. Furthermore another is online fraud elimination mechanism (OFEM) for both non-auction and auction process.

Prevention: OHM system provides concrete registration process and policies which efficiently guard form possibility of any fraud. Registration is the main process which is responsible to prevent online frauds at very early stage. Due to robust registration mechanism for both user and web-server the possibilities of fraud occurrence are diminished. First we will discuss the registration process for the user.

User Registration: Figure 23 shows the logical design flow for the user registration process. This is divided into four modules and the output of one module is the input for another module. Here for each module requirement engineering is defined by the tables.

- **Registration Module (A):** This is the first module of user registration. In this *OHM* verifies the basic details of user such as *user's name*, *date of birth*, *sex*, *permanent address*, *nationality*. This information is verified by the user ID. Table 6 shows the requirement engineering of this module.

TABLE 6. REQUIREMENTS FOR MODULE A

Verification Attributes	Verified by
Name of user DOB Sex Permanent Address Nationality	Identification proof i.e. passport no., Country unique id, Driving license, Pan card No.*

- **Registration Module (B):** This module verifies the current address of the user with the user's mobile information. This is done by tracking the mobile location via GPS device; *OHM* verifies that the difference between current location and the mobile location must be less than threshold value. Table 7 shows the requirement engineering of this module.

TABLE 7. REQUIREMENTS FOR MODULE B

Verification Attributes	Verified by
Mobile number Current address	Location of mobile tracked by GPS. Further a verification code is send to users mobile

- **Registration Module (C):** This module verifies the user's email address by sending a link to the user's email. Table 8 shows the requirement engineering of this module.

TABLE 8. REQUIREMENTS FOR MODULE C

Verification Attributes	Verified by
E-mail address	The verification code sends to user's email.

Note: Mobile number and email address must be same as registered with bank account

- **Registration Module (D):** Card detail of the user is verified by this module. *OHM* verifies the user's card information by contacting the corresponding bank server. Further this module cross verifies the above discussed modules (A), (B) and (C). Table 9 shows the requirement engineering of this module.

Table 9. Requirements for Module D

Verification Attributes	**Verified by**
Card Information	
Module (A)	The detail of the user associated with the
Module (B)	bank account and card.
Module (C)	
Expenditure behavior	By *HMM*,

Furthermore, it contains the background process which analyzes the behavioral pattern of the user expenditure. *OHM* undertakes last ten transaction details of user bank account and based on the expenditure nature *HMM* generates a behavioral pattern which is monitored by *OHM*. Further this pattern is used when user is detected with any suspicious activity. After verification of all the information *OHM* issues an *OC* (*OHM* Certificate) to the user. *OC* consists of i) name; ii) address; iii) contact number; iv) email address; v) user *OHM* login ID and password and; vi) photograph of user.

Web Server Registration: It consists of four modules which insure the legitimacy of the web-server. Similar to the user registration the output of one module is the input for next module.

- **Registration Module (E):** This module verifies the organization registration details of the web-server. In the proposed approach we considered that each web-server which provides e-commerce services must have prior authenticated registration. Thus it is having unique organizational registration ID. *OHM* will verify this information with the registering authority. Table 10 shows the requirement engineering of this module.

Table 10. Requirements for Module E

Verification Attributes	**Verified by**
Organization registration number	Contacting organization registration department

- **Registration Module (F):** This module insures the registration process of two individuals who are the member of registering organization. *OHM* precedes the same registration process (discussed in starting of this section). Table 11 shows the requirement engineering of this module.

Table 11. Requirements for Module F

Verification Attributes	**Verified by**
Two people associated to web-server	User Registration process

- **Registration Module (G):** This module validates the services provided by the web-server such as auction, merchandise, buying/Selling, insurance etc. These services are considered to define and impose policies on the web-server accordingly. Further *HMM* analyzes the behavioral pattern of the web-server. This patter is accumulated by *OHM* based on the past feedback and reviews of web-server. On the basis of that result *OHM* ranks the web-server on the scale of 10 which is defined by *OHM* based on user feedback. Table 12 shows the requirement engineering of this module.

TABLE 12. REQUIREMENTS FOR MODULE G

Verification Attributes	**Verified by**
Web-services Web-Server behavioral pattern	Authenticated by *OHM* and behavioral pattern generated by *HMM*

- **Registration Module (H):** In this final module of web-server registration *OHM* imposes the policy agreement on the web server organization. Then this agreement is signed between the organization and *OHM*. Table 13 shows the requirement engineering of this module.

TABLE 13. REQUIREMENTS FOR MODULE H

Verification Attributes	**Verified by**
Policy agreement	*OHM* policy agreement sign. Authority

After the completion of all agreements and verifications *OHM* issues an *OC* to web-server. It contains of i) organization name; ii) name of the both registered person; iii) address of organization; iv) organization *OHM* ID; v) rating of the web-server on the scale of 10.

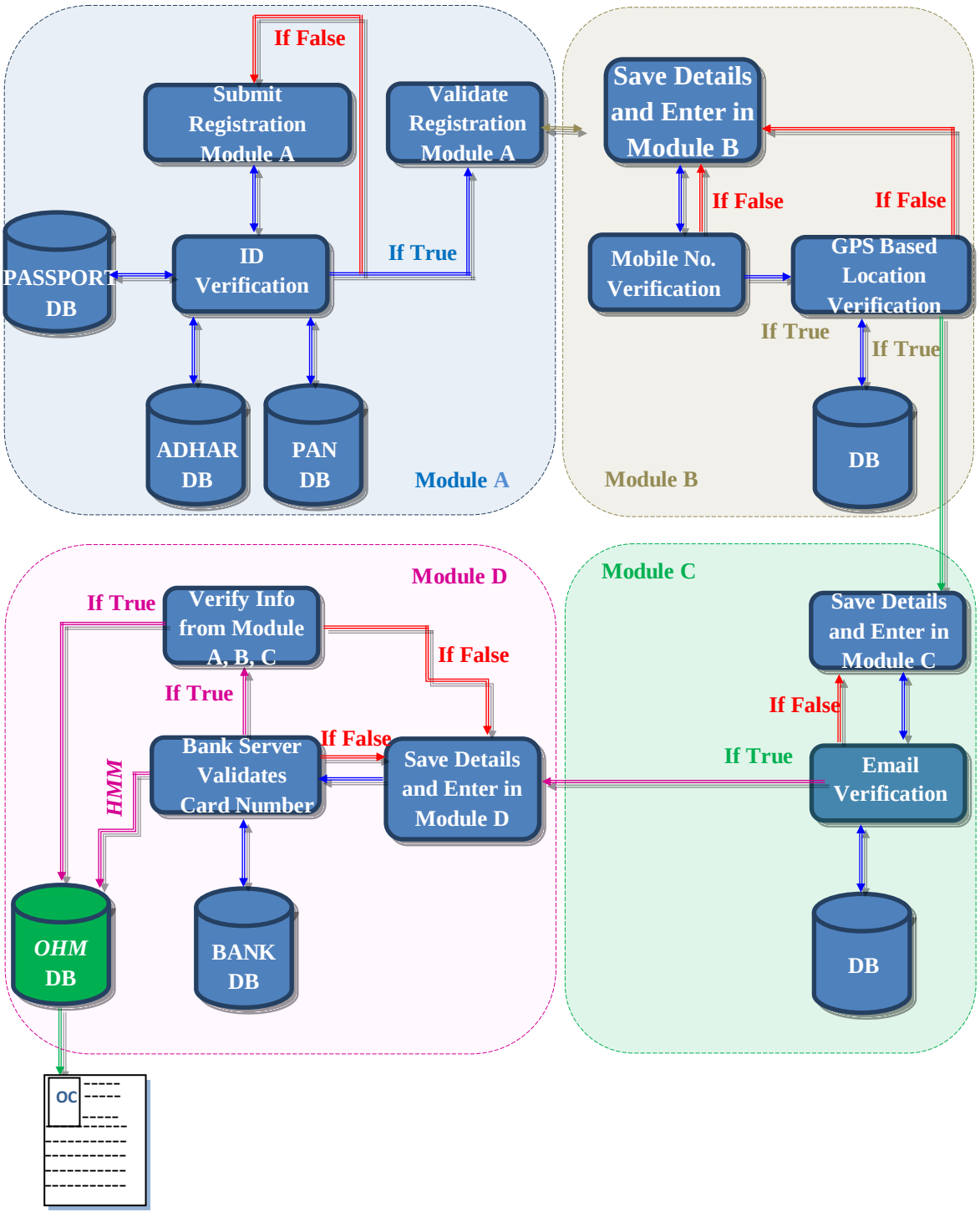

Figure 23. OHM Logical Design for USER Registration [29]

Policies: OHM defines the separate policies for both auction and non-auction services. We are not discussing those policies here although just provide an example for that; for the web-server providing auction process has to agree upon fixing the entry and exit fee for the user who initiates the auction. Further the web-servers have to implement OFDM and OFEM mechanism with their system so that frauds are detected and if necessary eliminated.

Detection: This is the second approach of OHM. It introduces when, there are some possibilities of frauds present during the web-user interaction. OHM provides two detection mechanisms.

We are just introducing those mechanisms and not discussing in detail. These will discuss in future research work.

Online Fraud Detection Mechanism (OFDM):OHM enables detection mechanism for both non-auction process and auction process. For the Non-Auction process detection mechanism identifies the fraudulent user when he/she trying to access web-services by providing fraud identities such as: wrong card information, wrong permanent address, wrong contact information, wrong id etc.

Further (as discussed previously) in the Auction process *OHM* detects the frauds by combining Shill-Deterrent Fee Schedule(SDFS) mechanism along with three detection strategies i.e. i) alternate bidding ii) alternate Auctioning iii) sudden incremental bidding. After detecting any suspicious activity of user, *OHM* starts doing close monitoring of that user id by keeping its information in monitoring log record.

*Online Fraud Elemination Mechanism (OFEM):*This, further divide in two parts one for non-auction process another for auction process. After the close monitoring process if *OHM* founds that the behavior of user is as fraudulent, *OHM* blocks that user. In Auction process if any fraud is detect than *OHM* stops the auction process and notifies all other auction participants about the user.

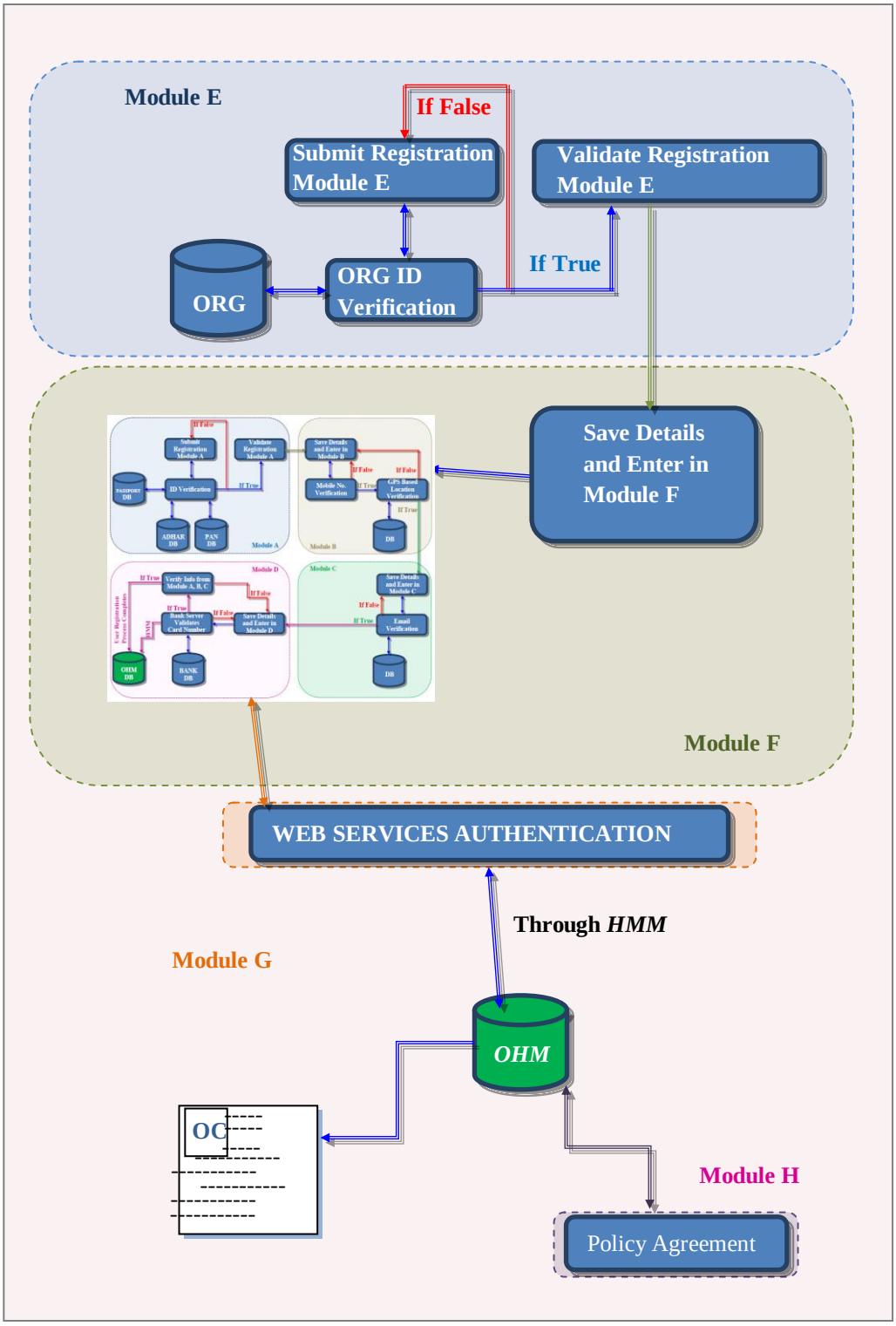

Figure 24. OHM Logical Design for Web Server Registration [29]

Module -3 Web-Server:

This module consist the web-servers which provides e-commerce services to their users. A web-server has to certify itself by *OHM* certification process.

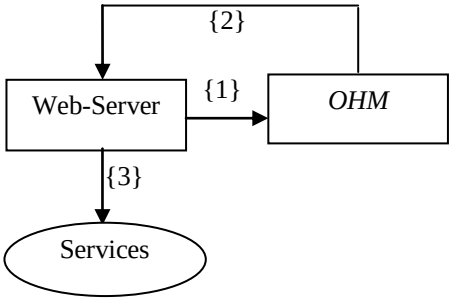

Figure 25.Web-Server process flow

Figure 25. shows the basic process flow for the web-server. In this there are 3 steps consist of i) Web-Server registration from *OHM* ii) *OHM* certifies the web-server iii)Than only web-server provides the services abvailable to users.

After discussing the logical design of *OHM* prevention approaches we have shown the operational interaction between each module (user, *OHM* and web-server).

Figure 26 shows the operation interaction between the *OHM* modules using three-way handshaking. The very first interaction starts with user who interacts with the web-server. Then it will be redirected to *OHM* for the registration process. After registration an *OC* is sent to both web-server and user (here we consider that web-server has already certified by *OHM*). After registration completion user is allowed to access services on the web-server. In between, *OHM* regularly monitors this interaction using *OFDM/OFEM* approaches.

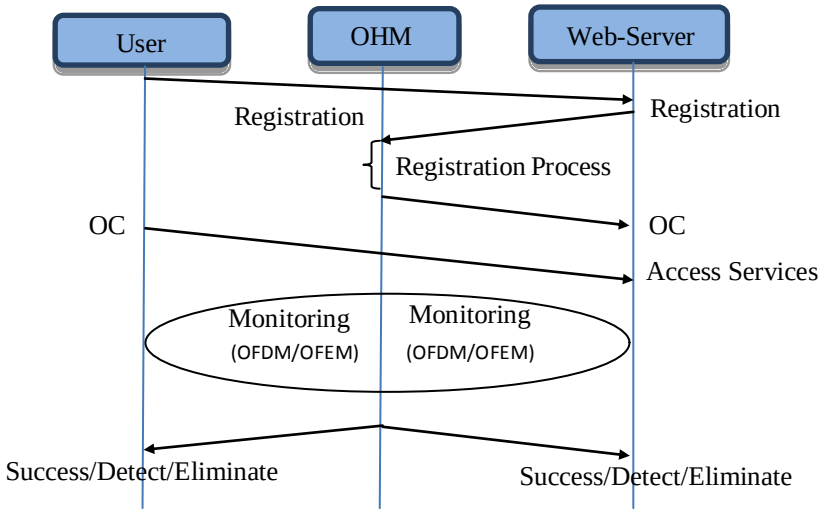

Figure 26. Operational Interaction of *OHM* modules [29]

4. Implementation and Results:

This chapter elaborates the implementation of proposed Online Hybrid Model *(OHM)* and the result of the framework in terms of performance of *OHM* against the online frauds.

Thus, I have developed JAVA based modules to implement the proposed framework. In order to firstly implement the *OHM-P* approach I have developed authentication interface for the registration of user and web-server. Further to implement the *OHM-D* approach I have simulated the HMM model over JAVA platform. To implement these interfaces we have used following software specifications (shown in Table 14):

Table 14: Software specification for OHM-P

Sr. No.	Specification	Description
1	Platform	JDK 1.6.0
2	Programming Language	J2EE
3	Development Tool	Netbeans IDE 7.0
4	Operating System	Windows 7
5.	Database Tool	Microsoft SQL server 2005

4.1 Implementation of OHM-P

Figure 27 shows the home page of the OHM system. This provides multiple services such as user registration, web-server registration, user account management, web-server account management. When a user or web-server has already registered on OHM system than OHM provides direct login to them for accessing their accounts. Whereas for a new user or

web-server OHM system provides the sign-up functionality where they can register with the OHM and get their respective OHM id and password.

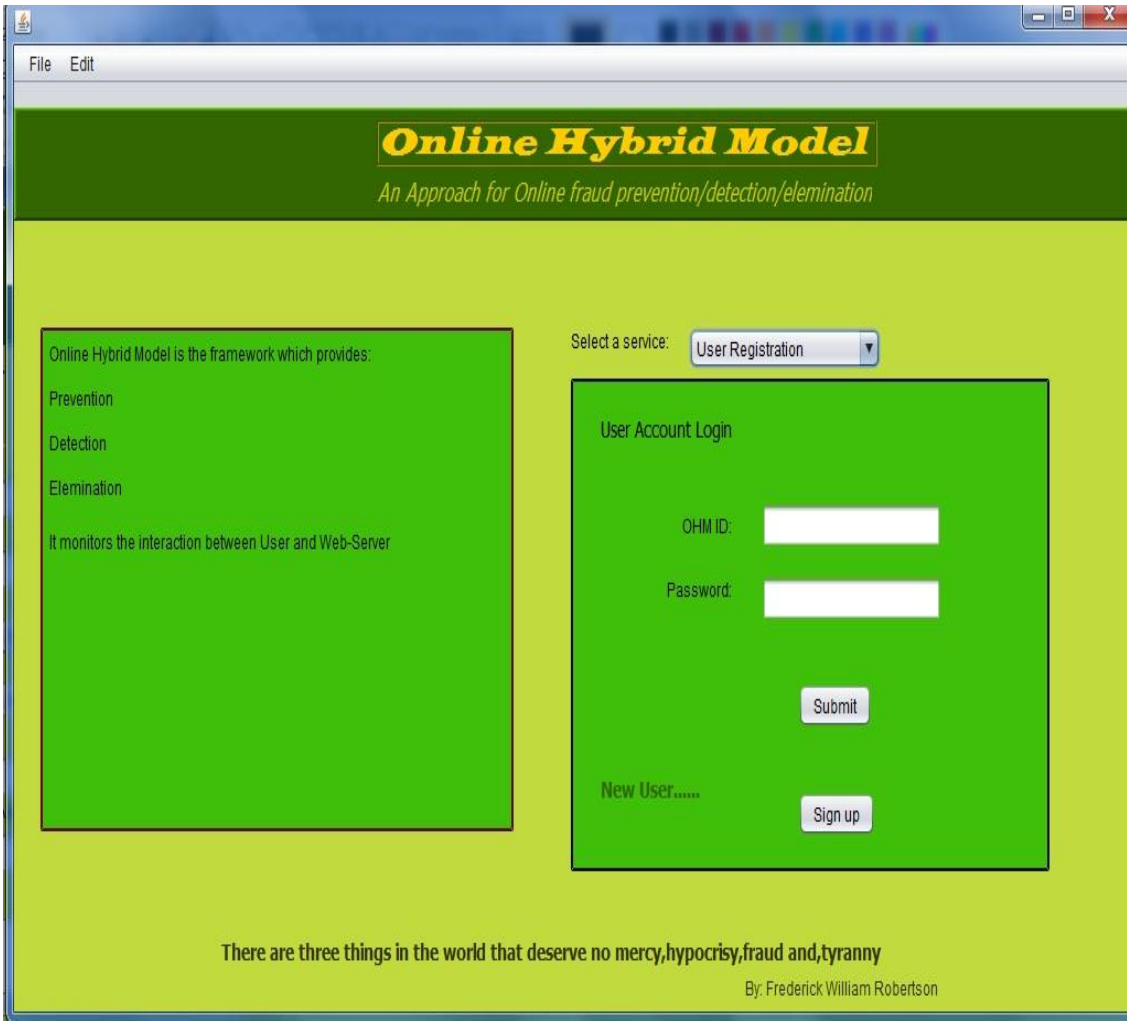

Figure 27: Home Page for *OHM*

After this figure 28 shows the interface for the user registration process. As deliberated in [10] that for each user it is necessary to register with the OHM in order to accessing the services of the web-server.

Figure 28: User registration module of OHM-P

As discussed in [29] that OHM user registration module consists of four sub-modules which are interrelated to each other. Module A, which takes the basic information of user and verifies that information by the id proof which is provided by user itself. Figure 28 shows that in Module A and when user clicks on confirm button than his/her information is submitted for verification. Then in Module B user inputs his/her mobile number and current address so that based on the location of mobile number (obtain using GPS) his/her

current address is verified and asking of the verification code to register that mobile number with OHM. Now, in Module C user inputs the email id which he/she wants to register with OHM. Further in module D user provides the card detail (ATM/Credit/Debit card) which he/she wants to register with OHM. And through this detail OHM system verifies all the previous details via contacting the bank server.

Also, OHM generates the user's expenditure behavior pattern by the last few user transactions (using HMM [31]). After verification of all the user information if OHM finds valid than it issues an OHM certificate (OC) to that user. OC contains the OHM id and password for the user and also having the time validity. I have discussed the complete format of OC in [29] (Shown in figure 0).

Figure 29. User's OC

Now, we are describing the web-server registration module. For preventing the legitimate users from the fraudulent web-server organization it is necessary for the web-server to register with OHM.

Figure 30 shows the interface for web-server registration. In this OHM needs the organization name, address, contact information (email, phone number) and most

important is the organization certificate which is issued by government to that organization. Also, the organization has to submit the proof of government registration.

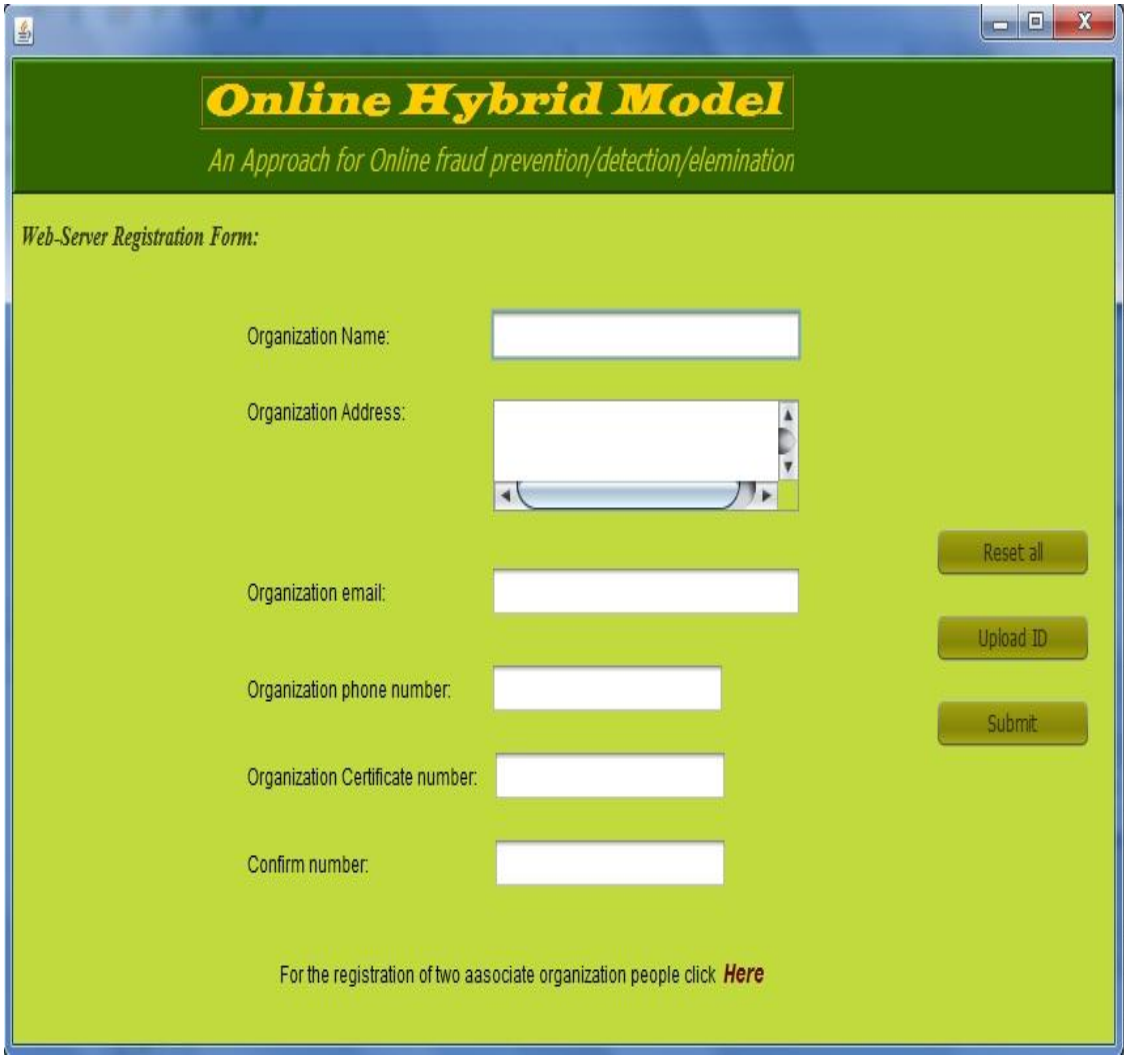

Figure 30: Web-Server registration module of OHM-P

Further OHM needs registration of two peoples who represent the organization. The registration process is same as user registration. For this user has to click on '*Here'* link (at the bottom of page) then it redirects the user to the user registration page.

Then the verification process takes some time and after validates all the information OHM issues an OC to the web-server organization. It is mandatory for an organization to make

visible this OC to its user so that a user can rely on the legitimacy of that web-server. The format and field of OC has been discussed in [29].

Online Hybrid Model

Web-Server Certification

Name: E-Shop

Name of Registered Person:

First: Ankit

Second: Ashutosh

Address: 27th Milestone, Katla bypass, Bagalore, India

OHM ID: 100101

Figure 31. Web-Server's OC

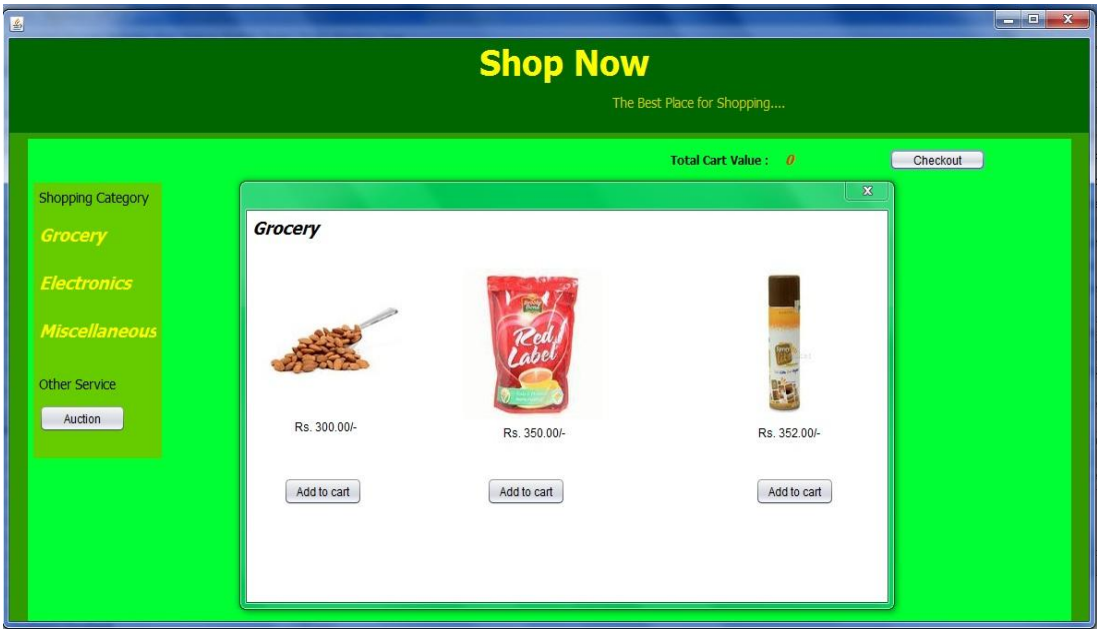

Figure 32: Web-Server shopping interface

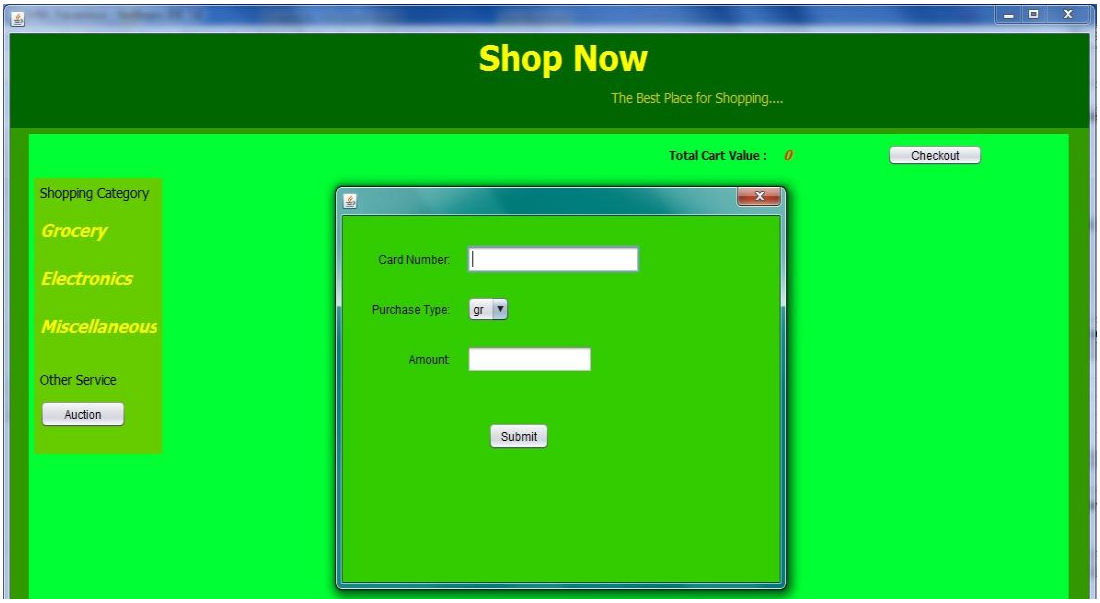

Figure 33: Check-out page for user

4.1.1. Interaction process of User and Web-Server:

The interaction process between user and web-server is took place as follows:

a. First both the web-server *A* and *B* registered themselves on OHM server through the interface shown in section 3.2. And after validated the information OHM issued the OC to the web-servers.

b. Now, among the five users three users want to access web-server *A*. And because they are interacting first to the web-server, they have redirected to the OHM server. Similarly remaining two users how want to access web-server *B*

c. Then, each user registers themselves on OHM server through the interface shown in figure y.

d. After verification of each user information, OHM issues OC to the users that contains the information shown in figure z3..

e. Thereafter, users are allowed to access the services of the respective web-servers by logged-in with OHM id and password.

4.2 Implementation of OHM-D

4.2.1. Checkout policy

As it is already define that each time a user is performing a new transaction on web-server the OHM performs the verification step in order to detect any fraud. For this I have simulated the HMM model over JAVA platform which is discussed below. Further the flow diagram of the check out policy is shown in figure 34. This shows that before confirmation of each transaction it has to be verified. And this verification is performed by HMM.

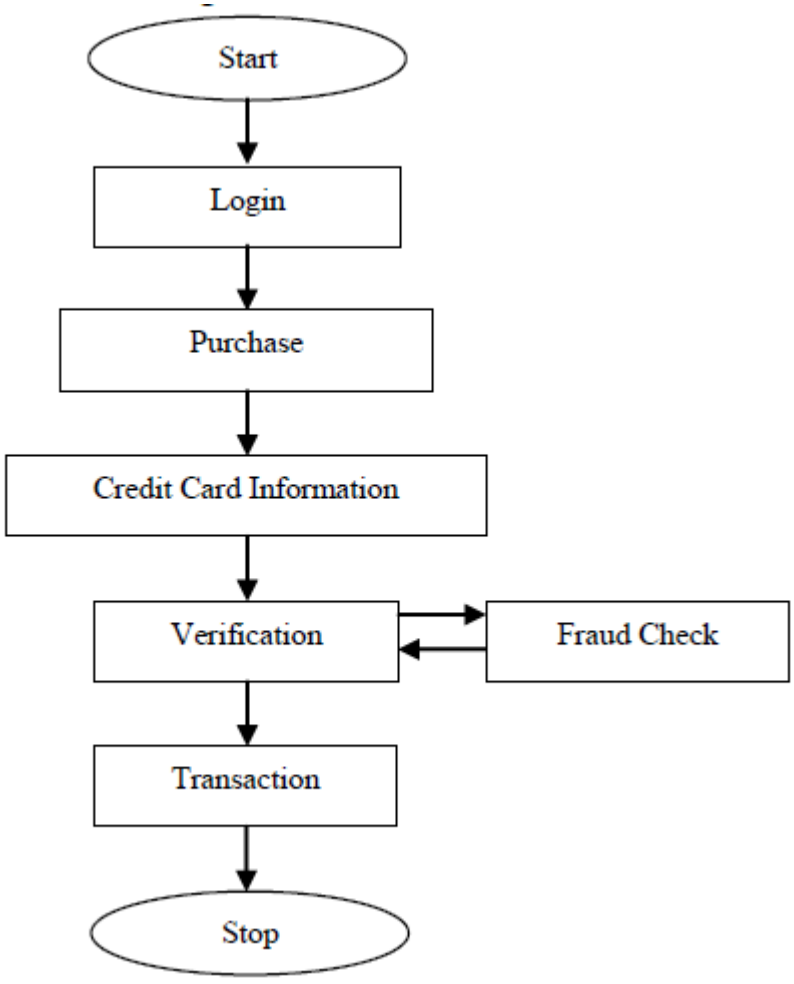

Figure 34. Flow chart of check out policy

4.2.1.1 Simulation of HMM:

In order to simulate the HMM we require some training data and test data. So, in the case of credit card fraud detection the training data and the test data are available in the form of user's transactions associated to the card. For this I have classified the user purchase amount x in to M price ranges V_1, V_2 . . . V_M. Then HMM dynamically determines the spending profile of the user by using k-Means clustering algorithm. In our approach for the prediction of spending profile I have created 3 clusters i.e. 1) low (l) 2) Medium (m) and 3) High (h). So that the spending profile of the user can be classified into three types i.e. low, middle and high spending profile. And in our model these clusters are also treated as observation symbols which is denoted by V { l, m, h}.Further, we can understand this by an example i.e. If user perform a transaction as $ 280 and user profile generated is to l (low) = (0, $ 100], m (medium) = ($ 200, $ 500], and h (high) = ($ 500, up to credit card limit], then in this scenario the new transaction belongs to middle profile group.

I have used Baum-Welch algorithm to estimate the HMM parameters for each cardholder. This algorithm has two phases one is forward procedure phase and second one is backward procedure phase. The Baum-Welch algorithm starts with initial values for the HMM input parameters i.e. A, B, and π and process then until it reaches to convergence or we can say that to the nearest local maxima calculated by a likelihood function. For initialize the algorithm in my approach I have considered uniform distribution probability means if there are N states, then the initial probability of each state is 1/N. Further the initial estimation of transition probability is also consider as uniform. Now, after initializing the input parameter for HMM, training phase is starts. For training the HMM, I have converted the users' transaction amount into observation symbols (as discussed above) and generate a initial training sequences form the last transactions. After completion of training phase, our HMM is ready for a specific user.

In various period of time, purchase of various types with the different amount would make by credit card holder. It uses the deviation in a purchasing amount of latest 10 transaction sequence (and adding one new transaction in that sequence) which is one of the possibilities related to the probability calculation [32].

After the completion of the learning parameter for HMM, the observation symbols are taken from the card holder's transactions training data in order to form the initial observation symbol sequence. This initial observation sequence is represented as $O_1, O_2, O_3, O_4, \ldots\ldots, O_R$ and this sequence is of length R. Now, in order to compute the first sequence acceptance probability we input this initial sequence to HMM. After this HMM generates the acceptance probability as:

$$\alpha_1 = P(O_1, O_2, O_3, O_4, \ldots\ldots, O_R|\lambda) \quad \ldots (1)$$

Now, assume that O_{R+1} is the new symbol which represents the new observation symbol generated by new transaction. And in order to determine the new observation sequence for HMM of length R we have to remove the first observation symbol i.e. O_1 and add new observation symbol O_{R+1} so the new observation sequence will be $O_2, O_3, O_4, O_5, \ldots\ldots, O_{R+1}$. After this in order to calculate the probability for the new input sequence we input this sequence to trained HMM. Now, suppose the new probability is:

$$\alpha_2 = P(O_2, O_3, O_4, O_5, \ldots\ldots, O_{R+1}|\lambda) \quad \ldots (2)$$

Let $\Delta\alpha = \alpha_1 - \alpha_2 \quad \ldots (3)$

Now suppose $\Delta\alpha > 0$, it represents that the new sequence probability is less than old sequence probability hence, HMM accept the new transaction with low probability, and there is a possibility that the new transaction is fraudulent one. So, in terms of threshold we can say that the new transaction can be fraudulent one if the percentage change in the probability is above a threshold, i.e.

$$\Delta\alpha/\alpha_1 \geq Threshold \quad \ldots (4)$$

sno	cardno	amt	type
1	9999	10000	ei
2	9999	90	gr
3	9999	500	ei
4	9999	300	gr
5	9999	757	mi
6	9999	2000	ei
7	9999	3500	ei
8	9999	119	gr
9	9999	250	mi
10	9999	32000	ei
11	9999	112	gr
12	9999	456	mi
13	9999	367	gr
14	9999	3400	ei
15	9999	890	mi
16	9999	12000	ei
17	9999	565	gr
18	9999	5678	ei
19	9999	1765	mi
20	9999	90	gr
21	9999	100	gr
22	9999	200	gr
23	9999	15000	ei
24	9999	3300	mi
25	9999	6500	ei

Figure 35. Transactions of User

4.2.1.2. Example of HMM for card number 9999 and purchased item ei (electronics) and amount is: 340

```
9999  ei 340
Gettin cluster and calculating centroid
Trans amount item purchased
Cluster for state groceries
[90, 300, 119, 112, 367, 565, 90, 100, 200, 1200, 456, 670, 400]
total elements 13
no. of cluster=  3   no. of elements  13
// At this step
Value of clusters
K1{ 90 90 100 }
K2{ 300 367 565 1200 456 670 400 }
K3{ 119 112 200 }
Value of m
m1=93.33333333333333  m2=565.4285714285714  m3=143.66666666666666
//At this step
Value of clusters
K1{ 90 112 90 100 }
K2{ 367 565 1200 456 670 400 }
K3{ 300 119 200 }
Value of m
m1=98.0  m2=609.6666666666666  m3=206.33333333333334
//At this step
Value of clusters
K1{ 90 119 112 90 100 }
K2{ 565 1200 456 670 }
K3{ 300 367 200 400 }
Value of m
m1=102.2  m2=722.75  m3=316.75
//At this step
Value of clusters
K1{ 90 119 112 90 100 200 }
K2{ 565 1200 670 }
K3{ 300 367 456 400 }
Value of m
m1=118.5  m2=811.6666666666666  m3=380.75
//At this step
Value of clusters
K1{ 90 119 112 90 100 200 }
K2{ 1200 670 }
K3{ 300 367 565 456 400 }
Value of m
m1=118.5  m2=935.0  m3=417.6
//At this step
Value of clusters
K1{ 90 119 112 90 100 200 }
K2{ 1200 }
K3{ 300 367 565 456 670 400 }
Value of m
m1=118.5  m2=1200.0  m3=459.6666666666667
//At this step
Value of clusters
K1{ 90 119 112 90 100 200 }
K2{ 1200 }
K3{ 300 367 565 456 670 400 }
Value of m
m1=118.5  m2=1200.0  m3=459.6666666666667
The Final Clusters By Kmeans are as follows:
K1{ 90 119 112 90 100 200 }
centroid    118
K2{ 1200 }
centroid    1200
K3{ 300 367 565 456 670 400 }
centroid    459
centroid for state groceries[118, 459, 1200]
gr_l  118
```

gr_m 459
gr_h 1200
amt for electronics[10000, 500, 2000, 3500, 32000, 3400, 12000, 5678, 15000, 6500, 220, 3456, 8888, 3200, 90000, 2400]
cluster for state electronic
[10000, 500, 2000, 3500, 32000, 3400, 12000, 5678, 15000, 6500, 220, 3456, 8888, 3200, 90000, 2400]
total elements16
no. of cluster= 3 no. of elements 16
//At this step
Value of clusters
K1{ 10000 32000 12000 15000 6500 8888 90000 }
K2{ 500 220 }
K3{ 2000 3500 3400 5678 3456 3200 2400 }
Value of m
m1=24912.571428571428 m2=360.0 m3=3376.285714285714
//At this step
Value of clusters
K1{ 32000 15000 90000 }
K2{ 500 220 }
K3{ 10000 2000 3500 3400 12000 5678 6500 3456 8888 3200 2400 }
Value of m
m1=45666.666666666664 m2=360.0 m3=5547.454545454545
//At this step
Value of clusters
K1{ 32000 90000 }
K2{ 500 2000 220 2400 }
K3{ 10000 3500 3400 12000 5678 15000 6500 3456 8888 3200 }
Value of m
m1=61000.0 m2=1280.0 m3=7162.2
//At this step
Value of clusters
K1{ 90000 }
K2{ 500 2000 3500 3400 220 3456 3200 2400 }
K3{ 10000 32000 12000 5678 15000 6500 8888 }
Value of m
m1=90000.0 m2=2334.5 m3=12866.57142857143
//At this step
Value of clusters
K1{ 90000 }
K2{ 500 2000 3500 3400 5678 6500 220 3456 3200 2400 }
K3{ 10000 32000 12000 15000 8888 }
Value of m
m1=90000.0 m2=3085.4 m3=15577.6
//At this step
Value of clusters
K1{ 90000 }
K2{ 500 2000 3500 3400 5678 6500 220 3456 8888 3200 2400 }
K3{ 10000 32000 12000 15000 }
Value of m
m1=90000.0 m2=3612.909090909091 m3=17250.0
//At this step
Value of clusters
K1{ 90000 }
K2{ 10000 500 2000 3500 3400 5678 6500 220 3456 8888 3200 2400 }
K3{ 32000 12000 15000 }
Value of m
m1=90000.0 m2=4145.166666666667 m3=19666.666666666668
//At this step
Value of clusters
K1{ 90000 }
K2{ 10000 500 2000 3500 3400 5678 6500 220 3456 8888 3200 2400 }
K3{ 32000 12000 15000 }
Value of m
m1=90000.0 m2=4145.166666666667 m3=19666.666666666668
The Final Clusters By Kmeans are as follows:
K1{ 90000 }
centroid 90000
K2{ 10000 500 2000 3500 3400 5678 6500 220 3456 8888 3200 2400 }
centroid 4145
K3{ 32000 12000 15000 }
centroid 19666

centroid for state electronics[4145, 19666, 90000]
ei_l 4145
ei_m 19666
ei_h 90000
amt for miscellaneous[757, 250, 456, 890, 1765, 3300, 450, 1200]
cluster for state miscellaneous
[757, 250, 456, 890, 1765, 3300, 450, 1200]
total elements8
no. of cluster= 3 no. of elements 8
//At this step
Value of clusters
K1{ 757 890 1765 3300 1200 }
K2{ 250 }
K3{ 456 450 }
Value of m
m1=1582.4 m2=250.0 m3=453.0
//At this step
Value of clusters
K1{ 1765 3300 1200 }
K2{ 250 }
K3{ 757 456 890 450 }
Value of m
m1=2088.3333333333335 m2=250.0 m3=638.25
//At this step
Value of clusters
K1{ 1765 3300 }
K2{ 250 }
K3{ 757 456 890 450 1200 }
Value of m
m1=2532.5 m2=250.0 m3=750.6
//At this step
Value of clusters
K1{ 1765 3300 }
K2{ 250 456 450 }
K3{ 757 890 1200 }
Value of m
m1=2532.5 m2=385.3333333333333 m3=949.0
//At this step
Value of clusters
K1{ 1765 3300 }
K2{ 250 456 450 }
K3{ 757 890 1200 }
Value of m
m1=2532.5 m2=385.3333333333333 m3=949.0
The Final Clusters By Kmeans are as follows:
K1{ 1765 3300 }
centroid 2532
K2{ 250 456 450 }
centroid 385
K3{ 757 890 1200 }
centroid 949
centroid for state miscellaneous[385, 949, 2532]
mi_l 385
mi_m 949
mi_h 2532
database sequence [e, g, e, g, m, e, e, g, m, e, g, m, g, e, m, e, g, e, m, g, g, g, e, m, e, g, m, e, e, g, m, e, e, e, e, g, g]
total elements37
total no. of rows in database 37
total groceries row in database 13
total electronic row in database 16
total miscellaneoud row in database 8
total groceri row having LOW spending 6
total groceri row having MEDIUMspending 6
total groceri row having HIGH spending 1
total electronic row having LOW spending 12
total electronic row having MEDIUMspending 3
total electronic row having HIGH spending 1
total miscellanous row having LOW spending 3
total miscellanous row having MEDIUMspending 3
total miscellanous row having HIGH spending 2

total transition row from gr -gr 3
total transition row from gr -ei 4
total transition row from gr -mi 5
total transition row from ei -gr 8
total transition row from ei -ei 5
total transition row from ei -mi 3
total transition row from mi -gr 2
total transition row from mi -ei 6
total transition row from mi -mi 0
Initial probability of groceri 0.35135135
Initial probability of electronic 0.43243244
Initial probability of groceri 0.21621622
probability of LOW spending on groceri 0.46153846
probability of MEDIUM spending on groceri 0.46153846
probability of HIGH spending on groceri 0.07692308
probability of LOW spending on electronic 0.75
probability of MEDIUM spending on electronic 0.1875
probability of HIGH spending on electronic 0.0625
probability of LOW spending on miscellaneous 0.375
probability of MEDIUM spending on miscellaneous 0.375
probability of HIGH spending on miscelaneous 0.25
transition probability from gr-gr 0.08108108
transition probability from gr-ei 0.10810811
transition probability from gr-mi 0.13513513
transition probability from ei-gr 0.21621622
transition probability from ei-ei 0.13513513
transition probability from ei-mi 0.08108108
transition probability from mi-gr 0.054054055
transition probability from mi-ei 0.16216215
transition probability from mi-mi 0.0
transamount item purchasded
400 gr
minimum difference or closeness to centroid59.0
Sequence [m]
670 gr
minimum difference or closeness to centroid211.0
Sequence [m, m]
2400 ei
minimum difference or closeness to centroid1745.0
Sequence [m, m, l]
90000 ei
minimum difference or closeness to centroid0.0
Sequence [m, m, l, h]
3200 ei
minimum difference or closeness to centroid 945.0
Sequence [m, m, l, h, l]
8888 ei
minimum difference or closeness to centroid 4743.0
Sequence [m, m, l, h, l, l]
1200 mi
minimum difference or closeness to centroid 251.0
Sequence [m, m, l, h, l, l, m]
456 gr
minimum difference or closeness to centroid 3.0
Sequence [m, m, l, h, l, l, m, m]
3456 ei
minimum difference or closeness to centroid 689.0
Sequence [m, m, l, h, l, l, m, m, l]
220 ei
minimum difference or closeness to centroid 3925.0
Sequence [m, m, l, h, l, l, m, m, l, l]
450 mi
minimum difference or closeness to centroid 65.0
Sequence [m, m, l, h, l, l, m, m, l, l, l]
1200 gr
minimum difference or closeness to centroid0.0
Sequence [m, m, l, h, l, l, m, m, l, l, l, h]
6500 ei
minimum difference or closeness to centroid2355.0
Sequence [m, m, l, h, l, l, m, m, l, l, l, h, l]

```
3300                    mi
minimum difference or closeness to centroid768.0
Sequence [m, m, l, h, l, l, m, m, l, l, l, h, l, h]
15000                   ei
minimum difference or closeness to centroid4666.0
Sequence [m, m, l, h, l, l, m, m, l, l, l, h, l, h, m]
final sequence  [m, m, l, h, l, l, m, m, l, l, l, h, l, h, m]
final reverse sequence  [m, m, l, h, l, l, m, m, l, l, l, h, l, h, m]
seq after reverse[m, h, l, h, l, l, l, m, m, l, l, h, l, m, m]
seq after reverse2[m, h, l, h, l, l, l, m, m, l, l, h, l, m, m]
New transaction label of ei     l
guiseq[h, l, h, l, l, l, m, m, l, l, h, l, m, m, l]
sequence after transaction from gui...[h, l, h, l, l, l, m, m, l, l, h, l, m, m, l]
Distance at iteration 0: 1.1509967695274406
Distance at iteration 1: 1.1572533963313194
Distance at iteration 2: 1.1527800960226666
Distance at iteration 3: 1.1499700834571818
Distance at iteration 4: 1.1501272300002239
Distance at iteration 5: 1.1541328294122901
Distance at iteration 6: 1.1578388707259373
Distance at iteration 7: 1.1482378091919592
Distance at iteration 8: 1.152131625504103
Distance at iteration 9: 1.1516099283862293
Resulting HMM:
HMM with 3 state(s)

State 0
  Pi: 0.3551067650847542
  Aij: 0.599 0.2 0.201
  Opdf: Discrete distribution --- l 0.523, m 0.353, h 0.124

State 1
  Pi: 0.33227478668685023
  Aij: 0.2 0.6 0.2
  Opdf: Discrete distribution --- l 0.437, m 0.349, h 0.214

State 2
  Pi: 0.3126184482283952
  Aij: 0.2 0.2 0.6
  Opdf: Discrete distribution --- l 0.36, m 0.354, h 0.287

training ends here.....
testSequence   [m, h, l, h, l, l, l, m, m, l, l, h, l, m, m]
Sequence probability  z1 : 1.450736226482778E-7
testSequence2   [h, l, h, l, l, l, m, m, l, l, h, l, m, m, l]
gui Sequence probability  z2 : 1.7950104178450927E-7
delta_alpha   -3.4427419136231464E-8
result   23.73099844600879
```

Transaction Accepted

Training HMM Observation Sequence (100) for (200) iterations:

i0[[m, m, h, m, l, l, l, m, l, m, m, h, m, h, m, l, l, m, m, h, m, m, h, l, m, h, l, l, l, l, l, m, m, l, m, l, l, l, h, m, h, l, m, l, l, m, m, h, l, l, h, l, m, l, l, m, h, l, l, h, l, l, h, m, l, h, l, m, m, h, l,
m, l, l, l, l, h, m, l, l, l, l, m, h, h, l, l, m, m, l, m, m, l, l, h, m, h, m, h, h]]

i1[[m, m, h, m, l, l, l, m, l, m, m, h, m, h, m, l, l, m, m, h, m, m, h, l, m, h, l, l, l, l, l, m, m, l, m, l, l, l, h, m, h, l, m, l, l, m, m, h, l, l, h, l, m, l, l, m, h, l, l, h, l, l, h, m, l, h, l, m, m, h, l,
m, l, l, l, l, h, m, l, l, l, l, m, h, h, l, l, m, m, l, m, m, l, l, h, m, h, m, h, h], [m, m, m, h, l, l, m, m, l, m, h, m, l, l, m, l, l, l, m, l, h, l, m, m, l, m, l, l, h, h, l, l, l, l, m, m, m, m, h, m, m, l,
h, l, l, m, m, m, l, m, l, h, m, l, l, m, m, l, m, l, m, h, m, l, h, l, m, l, l, m, m, h, l, m, l, l, m, l, l, h, m, m, m, l, l, l, l, l, m, h, l, h, m, l, l, l, m, h, l, h]]

i2[[m, m, h, m, l, l, l, m, l, m, m, h, m, h, m, l, l, m, m, h, m, m, h, l, m, h, l, l, l, l, l, m, m, l, m, l, l, l, h, m, h, l, m, l, l, m, m, h, l, l, h, l, m, l, l, m, h, l, l, h, l, l, h, m, l, h, l, m, m, h, l,
m, l, l, l, l, h, m, l, l, l, l, m, h, h, l, l, m, m, l, m, m, l, l, h, m, h, m, h, h], [m, m, m, h, l, l, m, m, l, m, h, m, l, l, m, l, l, l, m, l, h, l, m, m, l, m, l, l, h, h, l, l, l, l, m, m, m, m, h, m, m, l,
h, l, l, m, m, m, l, m, l, h, m, l, l, m, m, l, m, l, m, h, m, l, h, l, m, l, l, m, m, h, l, m, l, l, m, l, l, h, m, m, m, l, l, l, l, l, m, h, l, h, m, l, l, l, m, h, l, h], [h, h, m, l, l, l, l, l, m, h, m, h, l, l, m,
m, l, h, l, m, l, h, h, l, l, m, h, l, l, l, h, l, l, l, m, l, l, l, l, m, l, m, m, l, h, h, h, l, h, h, m, m, h, h, l, m, h, m, h, m, l, l, l, h, l, m, l, l, l, l, h, h, m, m, m, m, h, m, m, l, l, m, l, h, h, m, l, l, h,
l, h, m, l, h, m, l, l, m, m, h]]

i3[[m, m, h, m, l, l, l, m, l, m, m, h, m, h, m, l, l, m, m, h, m, m, h, l, m, h, l, l, l, l, l, m, m, l, m, l, l, l, h, m, h, l, m, l, l, m, m, h, l, l, h, l, m, l, l, m, h, l, l, h, l, l, h, m, l, h, l, m, m, h, l,
m, l, l, l, l, h, m, l, l, l, l, m, h, h, l, l, m, m, l, m, m, l, l, h, m, h, m, h, h], [m, m, m, h, l, l, m, m, l, m, h, m, l, l, m, l, l, l, m, l, h, l, m, m, l, m, l, l, h, h, l, l, l, l, m, m, m, m, h, m, m, l,
h, l, l, m, m, m, l, m, l, h, m, l, l, m, m, l, m, l, m, h, m, l, h, l, m, l, l, m, m, h, l, m, l, l, m, l, l, h, m, m, m, l, l, l, l, l, m, h, l, h, m, l, l, l, m, h, l, h], [h, h, m, l, l, l, l, l, m, h, m, h, l, l, m,
m, l, h, l, m, l, h, h, l, l, m, h, l, l, l, h, l, l, l, m, l, l, l, l, m, l, m, m, l, h, h, h, l, h, h, m, m, h, h, l, m, h, m, h, m, l, l, l, h, l, m, l, l, l, l, h, h, m, m, m, m, h, m, m, l, l, m, l, h, h, m, l, l, h,
l, h, m, l, h, m, l, l, m, m, h], [h, m, h, h, m, h, m, h, l, h, l, m, m, m, l, m, m, m, l, m, m, l, m, m, m, m, l, l, m, l, m, h, h, l, h, l, m, m, m, l, l, l, h, l, l, m, m, l, h, l, h, m, l, l, l, l, m, h, l,
m, h, m, l, l, l, m, m, h, m, l, l, m, l, l, h, m, m, m, m, h, l, m, l, l, m, m, h, h, m, l, m, l, m, l, l, l, l, m, h, l]]

i4[[m, m, h, m, l, l, l, m, l, m, m, h, m, h, m, l, l, m, m, h, m, m, h, l, m, h, l, l, l, l, l, m, m, l, m, l, l, l, h, m, h, l, m, l, l, m, m, h, l, l, h, l, m, l, l, m, h, l, l, h, l, l, h, m, l, h, l, m, m, h, l,
m, l, l, l, l, h, m, l, l, l, l, m, h, h, l, l, m, m, l, m, m, l, l, h, m, h, m, h, h], [m, m, m, h, l, l, m, m, l, m, h, m, l, l, m, l, l, l, m, l, h, l, m, m, l, m, l, l, h, h, l, l, l, l, m, m, m, m, h, m, m, l,
h, l, l, m, m, m, l, m, l, h, m, l, l, m, m, l, m, l, m, h, m, l, h, l, m, l, l, m, m, h, l, m, l, l, m, l, l, h, m, m, m, l, l, l, l, l, m, h, l, h, m, l, l, l, m, h, l, h], [h, h, m, l, l, l, l, l, m, h, m, h, l, l, m,
m, l, h, l, m, l, h, h, l, l, m, h, l, l, l, h, l, l, l, m, l, l, l, l, m, l, m, m, l, h, h, h, l, h, h, m, m, h, h, l, m, h, m, h, m, l, l, l, h, l, m, l, l, l, l, h, h, m, m, m, m, h, m, m, l, l, m, l, h, h, m, l, l, h,
l, h, m, l, h, m, l, l, m, m, h], [h, m, h, h, m, h, m, h, l, h, l, m, m, m, l, m, m, m, l, m, m, l, m, m, m, m, l, l, m, l, m, h, h, l, h, l, m, m, m, l, l, l, h, l, l, m, m, l, h, l, h, m, l, l, l, l, m, h, l,
m, h, m, l, l, l, m, m, h, m, l, l, m, l, l, h, m, m, m, m, h, l, m, l, l, m, m, h, h, m, l, m, l, m, l, l, l, l, m, h, l], [m, h, m, l, m, m, m, m, h, m, l, h, h, l, h, m, l, l, l, m, l, l, h, m, h, m, h, m, l,
h, m, h, m, m, m, m, l, l, m, l, l, l, l, l, m, m, l, m, h, h, l, l, l, m, l, m, l, l, l, l, l, m, l, l, l, m, m, l, h, m, m, h, l, l, m, m, l, l, m, h, m, m, m, l, l, m, m, h, m, m, h, l, l, m, l, l, l, m, m, h]]

i5[[m, m, h, m, l, l, l, m, l, m, m, h, m, h, m, l, l, m, m, h, m, m, h, l, m, h, l, l, l, l, l, m, m, l, m, l, l, l, h, m, h, l, m, l, l, m, m, h, l, l, h, l, m, l, l, m, h, l, l, h, l, l, h, m, l, h, l, m, m, h, l,
m, l, l, l, l, h, m, l, l, l, l, m, h, h, l, l, m, m, l, m, m, l, l, h, m, h, m, h, h], [m, m, m, h, l, l, m, m, l, m, h, m, l, l, m, l, l, l, m, l, h, l, m, m, l, m, l, l, h, h, l, l, l, l, m, m, m, m, h, m, m, l,
h, l, l, m, m, m, l, m, l, h, m, l, l, m, m, l, m, l, m, h, m, l, h, l, m, l, l, m, m, h, l, m, l, l, m, l, l, h, m, m, m, l, l, l, l, l, m, h, l, h, m, l, l, l, m, h, l, h], [h, h, m, l, l, l, l, l, m, h, m, h, l, l, m,
m, l, h, l, m, l, h, h, l, l, m, h, l, l, l, h, l, l, l, m, l, l, l, l, m, l, m, m, l, h, h, h, l, h, h, m, m, h, h, l, m, h, m, h, m, l, l, l, h, l, m, l, l, l, l, h, h, m, m, m, m, h, m, m, l, l, m, l, h, h, m, l, l, h,
l, h, m, l, h, m, l, l, m, m, h], [h, m, h, h, m, h, m, h, l, h, l, m, m, m, l, m, m, m, l, m, m, l, m, m, m, m, l, l, m, l, m, h, h, l, h, l, m, m, m, l, l, l, h, l, l, m, m, l, h, l, h, m, l, l, l, l, m, h, l,
m, h, m, l, l, l, m, m, h, m, l, l, m, l, l, h, m, m, m, m, h, l, m, l, l, m, m, h, h, m, l, m, l, m, l, l, l, l, m, h, l], [m, h, m, l, m, m, m, m, h, m, l, h, h, l, h, m, l, l, l, m, l, l, h, m, h, m, h, m, l,
h, m, h, m, m, m, m, l, l, m, l, l, l, l, l, m, m, l, m, h, h, l, l, l, m, l, m, l, l, l, l, l, m, l, l, l, m, m, l, h, m, m, h, l, l, m, m, l, l, m, h, m, m, m, l, l, m, m, h, m, m, h, l, l, m, l, l, l, m, m, h],
[l, m, m, h, h, m, l, l, m, m, l, m, l, l, m, h, m, l, h, l, h, l, l, l, l, l, h, l, l, l, h, m, h, l, l, l, m, l, l, l, l, l, h, m, l, l, h, l, l, l, m, l, m, h, h, m, m, m, m, l, h, l, l, m, l, l, m, l, l, m, m, h, l, l, m,
m, h, m, l, l, l, l, m, l, m, l, l, l, l, h, m, m, l, m, l, l, h, l, l, l]]

i6[[m, m, h, m, l, l, l, m, l, m, m, h, m, h, m, l, l, m, m, h, m, m, h, l, m, h, l, l, l, l, l, m, m, l, m, l, l, l, h, m, h, l, m, l, l, m, m, h, l, l, h, l, m, l, l, m, h, l, l, h, l, l, h, m, l, h, l, m, m, h, l,
m, l, l, l, l, h, m, l, l, l, l, m, h, h, l, l, m, m, l, m, m, l, l, h, m, h, m, h, h], [m, m, m, h, l, l, m, m, l, m, h, m, l, l, m, l, l, l, m, l, h, l, m, m, l, m, l, l, h, h, l, l, l, l, m, m, m, m, h, m, m, l,
h, l, l, m, m, m, l, m, l, h, m, l, l, m, m, l, m, l, m, h, m, l, h, l, m, l, l, m, m, h, l, m, l, l, m, l, l, h, m, m, m, l, l, l, l, l, m, h, l, h, m, l, l, l, m, h, l, h], [h, h, m, l, l, l, l, l, m, h, m, h, l, l, m,
m, l, h, l, m, l, h, h, l, l, m, h, l, l, l, h, l, l, l, m, l, l, l, l, m, l, m, m, l, h, h, h, l, h, h, m, m, h, h, l, m, h, m, h, m, l, l, l, h, l, m, l, l, l, l, h, h, m, m, m, m, h, m, m, l, l, m, l, h, h, m, l, l, h,
l, h, m, l, h, m, l, l, m, m, h], [h, m, h, h, m, h, m, h, l, h, l, m, m, m, l, m, m, m, l, m, m, l, m, m, m, m, l, l, m, l, m, h, h, l, h, l, m, m, m, l, l, l, h, l, l, m, m, l, h, l, h, m, l, l, l, l, m, h, l,
m, h, m, l, l, l, m, m, h, m, l, l, m, l, l, h, m, m, m, m, h, l, m, l, l, m, m, h, h, m, l, m, l, m, l, l, l, l, m, h, l], [m, h, m, l, m, m, m, m, h, m, l, h, h, l, h, m, l, l, l, m, l, l, h, m, h, m, h, m, l,
h, m, h, m, m, m, m, l, l, m, l, l, l, l, l, m, m, l, m, h, h, l, l, l, m, l, m, l, l, l, l, l, m, l, l, l, m, m, l, h, m, m, h, l, l, m, m, l, l, m, h, m, m, m, l, l, m, m, h, m, m, h, l, l, m, l, l, l, m, m, h],
[l, m, m, h, h, m, l, l, m, m, l, m, l, l, m, h, m, l, h, l, h, l, l, l, l, l, h, l, l, l, h, m, h, l, l, l, m, l, l, l, l, l, h, m, l, l, h, l, l, l, m, l, m, h, h, m, m, m, m, l, h, l, l, m, l, l, m, l, l, m, m, h, l, l, m,
m, h, m, l, l, l, l, m, l, m, l, l, l, l, h, m, m, l, m, l, l, h, l, l, l], [m, l, l, h, m, h, m, l, m, l, m, h, m, l, m, m, l, h, m, l, m, m, l, m, h, l, h, l, h, l, m, l, h, l, l, m, h, l, l, l, l, l, l, l, l, h, m, m, l,
m, l, m, m, h, h, h, m, l, m, l, l, l, h, l, m, l, m, m, l, m, m, l, l, l, l, h, h, l, h, l, m, l, l, l, l, l, l, h, l, m, l, l, h, m, m, l, m, m, l, m]]

i7[[m, m, h, m, l, l, l, m, l, m, m, h, m, h, m, l, l, m, m, h, m, m, h, l, m, h, l, l, l, l, l, m, m, l, m, l, l, l, h, m, h, l, m, l, l, m, m, h, l, l, h, l, m, l, l, m, h, l, l, h, l, l, h, m, l, h, l, m, m, h, l,
m, l, l, l, l, h, m, l, l, l, l, m, h, h, l, l, m, m, l, m, m, l, l, h, m, h, m, h, h], [m, m, m, h, l, l, m, m, l, m, h, m, l, l, m, l, l, l, m, l, h, l, m, m, l, m, l, l, h, h, l, l, l, l, m, m, m, m, h, m, m, l,
h, l, l, m, m, m, l, m, l, h, m, l, l, m, m, l, m, l, m, h, m, l, h, l, m, l, l, m, m, h, l, m, l, l, m, l, l, h, m, m, m, l, l, l, l, l, m, h, l, h, m, l, l, l, m, h, l, h], [h, h, m, l, l, l, l, l, m, h, m, h, l, l, m,
m, l, h, l, m, l, h, h, l, l, m, h, l, l, l, h, l, l, l, m, l, l, l, l, m, l, m, m, l, h, h, h, l, h, h, m, m, h, h, l, m, h, m, h, m, l, l, l, h, l, m, l, l, l, l, h, h, m, m, m, m, h, m, m, l, l, m, l, h, h, m, l, l, h,
l, h, m, l, h, m, l, l, m, m, h], [h, m, h, h, m, h, m, h, l, h, l, m, m, m, l, m, m, m, l, m, m, l, m, m, m, m, l, l, m, l, m, h, h, l, h, l, m, m, m, l, l, l, h, l, l, m, m, l, h, l, h, m, l, l, l, l, m, h, l,
m, h, m, l, l, l, m, m, h, m, l, l, m, l, l, h, m, m, m, m, h, l, m, l, l, m, m, h, h, m, l, m, l, m, l, l, l, l, m, h, l], [m, h, m, l, m, m, m, m, h, m, l, h, h, l, h, m, l, l, l, m, l, l, h, m, h, m, h, m, l,
h, m, h, m, m, m, m, l, l, m, l, l, l, l, l, m, m, l, m, h, h, l, l, l, m, l, m, l, l, l, l, l, m, l, l, l, m, m, l, h, m, m, h, l, l, m, m, l, l, m, h, m, m, m, l, l, m, m, h, m, m, h, l, l, m, l, l, l, m, m, h],
[l, m, m, h, h, m, l, l, m, m, l, m, l, l, m, h, m, l, h, l, h, l, l, l, l, l, h, l, l, l, h, m, h, l, l, l, m, l, l, l, l, l, h, m, l, l, h, l, l, l, m, l, m, h, h, m, m, m, m, l, h, l, l, m, l, l, m, l, l, m, m, h, l, l, m,
m, h, m, l, l, l, l, m, l, m, l, l, l, l, h, m, m, l, m, l, l, h, l, l, l], [m, l, l, h, m, h, m, l, m, l, m, h, m, l, m, m, l, h, m, l, m, m, l, m, h, l, h, l, h, l, m, l, h, l, l, m, h, l, l, l, l, l, l, l, l, h, m, m, l,
m, l, m, m, h, h, h, m, l, m, l, l, l, h, l, m, l, m, m, l, m, m, l, l, l, l, h, h, l, h, l, m, l, l, l, l, l, l, h, l, m, l, l, h, m, m, l, m, m, l, m], [l, l, m, l, l, m, l, m, h, l, h, h, m, m, m, l, m, h, m, l, h,
m, h, l, m, m, m, l, l, h, h, h, h, m, m, m, m, m, m, l, m, h, h, m, l, m, l, l, l, m, l, l, l, l, l, l, m, l, l, h, l, l, m, m, m, m, m, m, l, m, l, l, h, l, m, l, l, l, m, m, l, l, l, m, m, m, l, m, l, l, l, m, l,
h, l, m, l, m, m, m]]

i8[[m, m, h, m, l, l, l, m, l, m, m, h, m, h, m, l, l, m, m, h, m, m, h, l, m, h, l, l, l, l, l, m, m, l, m, l, l, l, h, m, h, l, m, l, l, m, m, h, l, l, h, l, m, l, l, m, h, l, l, h, l, l, h, m, l, h, l, m, m, h, l,
m, l, l, l, l, h, m, l, l, l, l, m, h, h, l, l, m, m, l, m, m, l, l, h, m, h, m, h, h], [m, m, m, h, l, l, m, m, l, m, h, m, l, l, m, l, l, l, m, l, h, l, m, m, l, m, l, l, h, h, l, l, l, l, m, m, m, m, h, m, m, l,
h, l, l, m, m, m, l, m, l, h, m, l, l, m, m, l, m, l, m, h, m, l, h, l, m, l, l, m, m, h, l, m, l, l, m, l, l, h, m, m, m, l, l, l, l, l, m, h, l, h, m, l, l, l, m, h, l, h], [h, h, m, l, l, l, l, l, m, h, m, h, l, l, m,
m, l, h, l, m, l, h, h, l, l, m, h, l, l, l, h, l, l, l, m, l, l, l, l, m, l, m, m, l, h, h, h, l, h, h, m, m, h, h, l, m, h, m, h, m, l, l, l, h, l, m, l, l, l, l, h, h, m, m, m, m, h, m, m, l, l, m, l, h, h, m, l, l, h,
l, h, m, l, h, m, l, l, m, m, h], [h, m, h, h, m, h, m, h, l, h, l, m, m, m, l, m, m, m, l, m, m, l, m, m, m, m, l, l, m, l, m, h, h, l, h, l, m, m, m, l, l, l, h, l, l, m, m, l, h, l, h, m, l, l, l, l, m, h, l,

Now, I have shown the performance of *OHM-P* by considering the security as parameter.

Table 15: Performance of *OHM-P*

ALGORITHM	SECURITY
User Registration Module (A): If ((name=name[ID]&&DOB=DOB[ID]&&sex=sex[ID]&&permanent_address = address[ID]&& nationality=nationality[ID]) /*Name[ID],DOB[ID],address[ID] is the information written on ID proof*/	User does not allow feeding false information. And the original information is stored in the database
User Registration Module (B): If [{(current_location – mobile_location)≤ location_threshold} &&mobile_code=*OHM*_code] /* mobile_location is traced by GPS, location_threshold decide by *OHM* , *OHM* verifies the code send to user's mobile*/	User have to give right current location and right mobile number
User Registration Module (C): If (email_code=*OHM*_email[code])	Eliminates the possibility of false email ID
User Registration Module (D): If [(card number = true)] Then If	Highly secure thus all the previous module and card detail cross verified. Further card is registered and user is allowed to use only that card.

[(name=name[card]&&DOB=DOB[card]&&permanent_address= address[card]) && (mobile_number= mobile_number[card]&&email = email[card])] /*mobile_number[card],address[card] obtain by the mobilenumber and address registered for that card*/	
Background process : User expenditure behavior is monitored using *HMM*	Abnormal expenditure behavior may tracked
Web-Server Registration Module (E): Verifies: Organization number	It ensures the organization should be registered one
Web-Server Registration Module (F): Two people registration same as previously define user registration	This ensures the legitimacy of web server organization
Web-Server Registration Module (G): Validation and Authentication of services	Policies are assigned according to the services. So standardization is monitored.
Web-Server Registration Module (H): Background process for ranking of web-server by *HMM* and Policy agreement verification	Provides a transparent view about the web-server

Further, performance of OHM-D against credit card fraud is shown in table 16. I have calculated the correctness accuracy of HMM with three states and over difference sequence length i.e. 5, 10, 15 and against the different % threshold 20, 40, 60.

Table 16: Accuracy of HMM over the past transactions of user

Threshold (%)	Average correctness over 3 state model over different sequence length			Average erroneous over 3 state model over different sequence length		
	5	10	15	5	10	15
30	0.56	0.59	0.63	0.05	0.05	0.03
40	0.58	0.62	0.52	0.06	0.05	0.04
50	0.47	0.58	0.45	0.04	0.06	0.04

Average correctness accuracy = ….(4)

$$\frac{\text{No. of good transaction detected as good} + \text{No. of bad transactions detected as bad}}{\text{Total No. of transactions}}$$

Average erroneous accuracy = ….(5)

$$\frac{\text{No. of good transaction detected as good} + \text{No: of bad transactions detected as bad}}{\text{Total No. of transactions}}$$

4.4 OHM against Online Auction Fraud:

4.4.1 Reserve price setting policy:

$$Net\ Profit = W - ((W_C + R_C) + R) \quad \ldots.(6)$$

Here:

R= Initial reserve price

R_C= Reserve price commission rate

W_C= Wining price commission rate

W= Last winning bid amount

Table 17. Reserve price setting policy example

Sr. No.	Reserve Commission Rate (in %)	Winning Commission Rate (in %)	Initial Reserve Price	Final Reserve Price	Net Profit
1	2	5	10	150	142.3
2	3	6	10	150	140.7
3	4	7	10	150	139.1
4	2	5	15	170	161.2
5	3	6	15	170	159.35
6	4	7	15	170	157.5

So, by taking the example where the for two auction items the final winning bid is $150 and $170 respectively and their reserve price commission rate and winning price commission rate also shown. This example shows that how net profit is varies according to the commission rates so this mechanism forces the seller to set the honest reserve price.

4.4.2 Trust score mechanism:

6.Auction count: It is calculated as the number of auction event in which user is participated.

Action Count = Sum of Auction event

7.Reputation: The reputation of a particular user is calculated as the percentage of positive feedback of that user.

$$\text{Reputation\_user} = \frac{\text{No. of Positive feedback}}{\text{Total No. of Feedback}} \times 100 \quad \ldots.(7)$$

Table 18. User Feedback taken from eBay (last 12 months)

User	Positive Feedback	Total Feedback	% of Positive feedback
votreblue	31	32	96.8
peggys_antiques	1896	1909	99.3
mcphoto	198	255	77.6
10nylight	25	28	89.2
Vc_golly	423	435	97.24

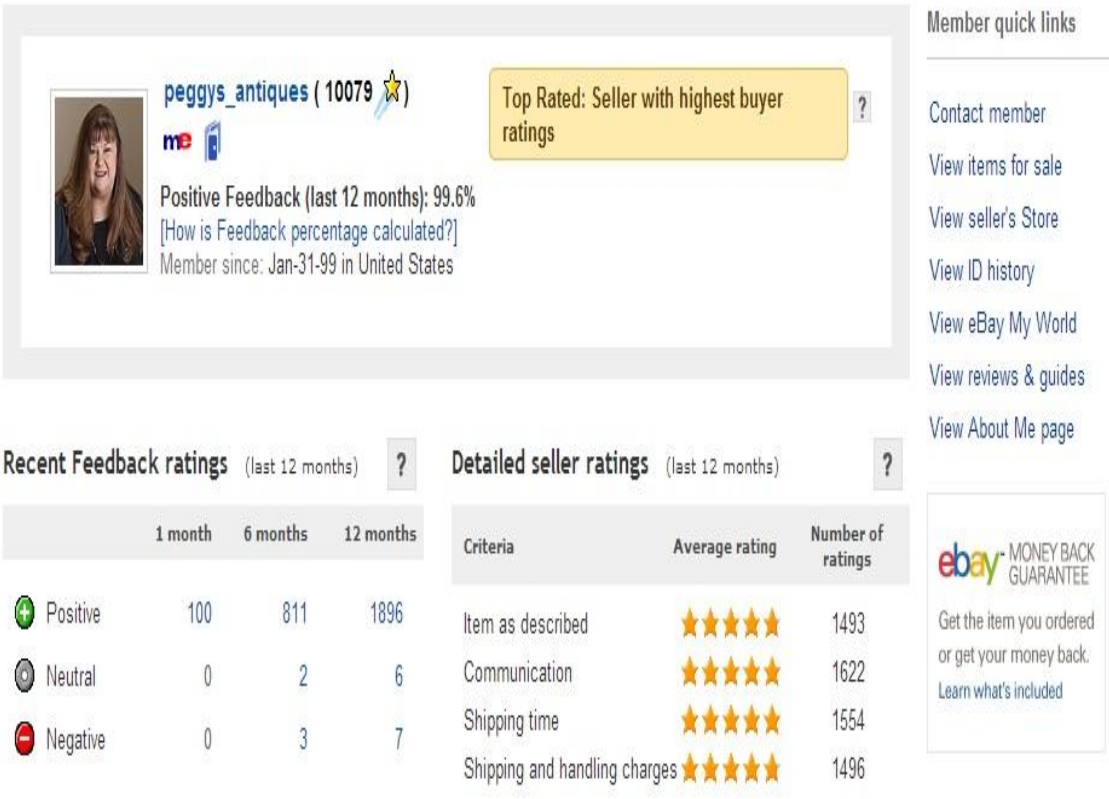

Figure 36: Feedback of user at eBay [33]

8.Average Bid Amount: It is calculated as the average of the value of all bids made by user.

$$\text{Average\_Bid\_Amount} = \frac{\text{Total amount of Bid}}{\text{Total no. of bid}} \times 100 \quad \ldots.(8)$$

Table 19 shows the example to show how the average bid amount calculated for a user during the auction process.

Table 19. Bids of user

Sr. No.	Bid Amount (in $)
1	34
2	37
3	42
4	47
5	51
6	56
7	57
8	76
9	79
10	89

$$\text{Average\_Bid\_Amount} = \frac{(34 + 37 + 42 + 47 + 51 + 56 + 57 + 76 + 79 + 89)}{10}$$

$$= \$\ 56.8$$

Similarly in each auction for each user average bid amount is calculated in order to compute the deviation of the current bid from average bid (shows below).

9.Increment in Bid: It is calculated as the increment in the last bid over the average bid. Now to understand this I have taken an example that suppose user have bid $ 94 as the latest bid than the deviation is calculated from the average bid amount as:

$$\text{Increment\_in\_Bid} = \frac{\text{Current\_Bid\_Amount - Average\_Bid\_Amount}}{\text{Average\_Bid\_Amount}} \times 100 \quad \ldots.(9)$$

Here in this example, $\text{Increment\_in\_Bid} = \frac{94 - 56.8}{56.8} \times 100$

$$= 65.49$$

10. Bids per Auction: It is calculated as the number of bids made by the user in an auction.

Table 20. No. of bids placed by user in last five auction events

User	Auction	No. of Bids
votreblue	Sotheby's Catalog	9
	Sotheby's Art	10
	Life Magazine	7
	The New Era Magazine	21
	American Art Review	5

4.5 OHM against Non-Delivery/Merchandise Fraud:

Due to authentication process each user and web-server has to provide the permanent address to the OHM. And when, any of the party tries to commit fraud then it will be easily recognized by the current location and address location. Further in the online auction

process also OHM maintains the user information in its database so if any seller tries to commit fraud by not ship the auctioned item to the buyer than he/she can easily be caught.

4.5 OHM against Identity-theft and Credit card Fraud:

Further the identity theft fraud is prevented by the authentication of users and web-server. And I have also shown that credit card fraud is detected by HMM model (shown above in this chapter).

5. Conclusion and Future Work:

In this research work I have proposed a framework *(Online Hybrid Model)* for preventing, detecting and eliminating the most frequent online frauds. Firstly we have shown that in the past 10 years three most frequent types of online frauds are: 1) Online auction fraud; 2) Identity theft fraud/Credit Card Fraud; and 3) Non Delivery Merchandise Fraud. Further studies of past approaches which are available in literature it is apparent that no single framework is exist for resolving these frauds. So, I have proposed a single framework which effectively works for all the three types of frequent fraud.

I have also implemented the proposed framework by developing the java modules. And I have tested the authentication algorithms by considering several cases for each module of registration for both user and web-server. Afterwards I have shown that the proposed framework provides a solid guard against online frauds by preventing the possibility of committing frauds in the early stage.

In future I will try to implement the auction fraud detection mechanism in real time scenario. And will try to implement this framework on a larger platform and study the result in more precise manner. Further this framework can be enhanced for other possible online frauds such as spam/spin, business schemes frauds, email-spam fraud, charity fraud etc.

References:

1. B. Prasad: Intelligent Techniques for E-Commerce, Journal of Electronic Commerce Research, 4 (2) 65-71, 2003.

2. U.S. Commerce Department, Forrester Research, Internet Retailer, ComScore., http://www.statisticbrain.com/total-online-sales/

3. National White Collar crime center, Report on Internet fraud, June 2008, www.nw3c.org/docs/whitepapers/internet_fraud.pdf?sfvrsn=7

4. Internet Crime Complain Center, Internet Crime Report, 2004-2011, http://www.ic3.gov/media/annualreports.aspx

5. Fei Donga, Sol M. Shatza and Haiping Xub: Combating Online In-Auction Fraud: Clues, Techniques and Challenges, Computer Science Review 3 (4) 245-258, 2009.

6. Abhinav Srivastava, Amlan Kundu, S. Sural, A.K. Majumdar: Credit Card Fraud Detection Using Hidden Markov Model , IEEE Transactions on Dependable And Secure Computing, 5 (1) 1062-1066, 2008

7. Yung chang Ku, Yuchi Chen, Chaochang Chiu, "A Proposed Data Mining Approach for Internet Auction Fraud Detection," Intelligence and Security Informatics Lecture Notes in Computer Science Volume 4430, 238-243, 2007

8. Stephan Kovach, Wilson Vicente Ruggiero, "Online Banking Fraud Detection Based on Local and Global Behavior," Proc. Of ICDS : The Fifth International Conference on Digital Society, 166-171, 2011

9. Liang Zhang Jie Yang Belle Tseng, "Online Modeling of Proactive Moderation System for Auction Fraud Detection," World Wide Web Conference (WWW), 669-678, 2012

10. Ankit Mundra, Nitin Rakesh, "Online Hybrid Model for Online Fraud Prevention and Detection," Advances in Intelligent and Soft Computing, Springer, Vol 243, pp 805-815, 2014.

11. W.L. Wang, Z. Hidvègi, and A. B. Whinston: Shill Bidding in English Auctions, Technical report, Emory University, 2001, http://oz.stern.nyu.edu/seminar/fa01/1108.pdf

12. J. Trevathan and W. Read: Detecting Collusive Shill Bidding, Proc. of International Conference on Information Technology: New Generations, 799-808, 2007.

13. R.J. Kauffman and C.A. Wood, "Running up the Bid: Detecting, Predicting, and Preventing Reserve Price Shilling in Online Auctions," Proc. of the 5th International Conference on Electronic Commerce, 2003.

14. R. Porter and Y. Shoham, "On Cheating in Sealed-Bid Auctions, Journal of Decision Support Systems," Special issue of the fourth ACM Conference on Electronic Commerce, 39 (1) 41-54, March 2005

15. B.K. Bhargava, M. Jenamani, and Y.H. Zhong, "Counteracting Shill Bidding in Online English Auction," International Journal of Cooperative Information Systems, 14 (2-3) (2005) 245-263.

16. D.H. Chau, S. Pandit, and C. Faloutsos, "Detecting Fraudulent Personalities in Networks of Online Auctioneers," Principles and Practice of Knowledge Discovery in Database, 2006, pp. 103-114.

17. S. Rubin, M. Christodorescu, V.J. Ganapathy, T. Griffin, L. Kruger, H. Wang, and N. Kidd, "An Auctioning Reputation System based on Anomaly Detection," Proc. of the 12th ACM Conference on Computer and Communications Security, 2005, pp. 270–279.

18. D. Gregg and J. Scott. The role of reputation systems in reducing on-line auction fraud. International Journal of Electronic Commerce, 10(3):95–120, 2006.

19. K. Zhu, Y. Guan, and L. Ying, "Detecting hidden communities in online auction networks," 2012, Technical Report, Iowa State University.

20. H. Xu, S.M. Shatz, and C.K. Bates: A Framework for Agent-Based Trust Management in Online Auctions, Proc. of the 5th International Conference on Information Technology: New Generations,149-155, 2008.

21. Sandeep Pratap Singh, Shiv Shankar P. Shukla, Nitin Rakesh and Vipin Tyagi, "Problem reduction in online payment system using hybrid model," International Journal of Managing Information Technology, 3 (3) 62-71, August 2011

22. D. Ourston, S. Matzner, W. Stump, and B. Hopkins, "Applications of Hidden Markov Models to Detecting Multi-Stage Network Attacks," Proc. 36th Ann. Hawaii Int'l Conf. System Sciences, vol. 9, pp. 334-344, 2003.

23. S.S. Joshi and V.V. Phoha, "Investigating Hidden Markov Models Capabilities in Anomaly Detection," Proc. 43rd ACM Ann. Southeast Regional Conf., vol. 1, pp. 98-103, 2005.

24. S.B. Cho and H.J. Park, "Efficient Anomaly Detection by Modeling Privilege Flows Using Hidden Markov Model," Computer and Security, vol. 22, no. 1, pp. 45-55, 2003.

25. C. Dellarocas, "Immunizing Online Reputation Reporting Systems against Unfair Ratings and Discriminatory Behavior," Proc. of the ACM Conference on Electronic Commerce, Minneapolis 2000, pp.150-157.

26. Bhattacharyya, S., Jha, S., Tharakunnel, K., & Westland, J. C. (2011). Data mining for credit card fraud: A comparative study. Decision Support Systems, 50(3), 602- 613. Elsevier B.V.

27. Chang, Jau-Shien, and Wen-Hsi Chang. "A cost-effective method for early fraud detection in online auctions." ICT and Knowledge Engineering (ICT & Knowledge Engineering), 10th International Conference on. IEEE, 2012.

28. C. Chiu and C. Tsai, “A Web Services-Based Collaborative Scheme for Credit Card Fraud Detection,” Proc. IEEE Int’l Conf. e-Technology, e-Commerce and e Service, pp. 177-181, 2004.

29. Ankit Mundra, Nitin Rakesh, “Empirical Study of Online Hybrid Model for Internet Fraud Prevention and Detection” accepted in IEEE International Conference on Human Computer Interactions – ICHCI-2013

30. C. Chiu and C. Tsai, “A HMM Based Collaborative Scheme for Credit Card Fraud Detection,” Proc. IEEE Int’l Conf.e-Technology, e-Commerce and e-Service, pp. 177-181, 2004.

31. Filippov, V.; Mukhanov, L.; Shchukin, B.; "Credit card fraud detection system," Cybernetic Intelligent Systems, 2008. CIS 2008. 7th IEEE International Conference on , vol., no., pp.1-6, 9-10 Sept. 2008

32. Federal Trade Commission (2011). Consumer sentinel network data book, annual report on consumer fraud, available: http://www.ftc.gov/ (2011, August 22).

33. www.ebay.com

Achievements:

1. **Ankit Mundra**, Nitin Rakesh, "Online Hybrid Model for Online Fraud Prevention and Detection," Advances in Intelligent and Soft Computing, **Springer International Publishing Switzerland**, Volume 243, pp 805-815, 2014.

   DOI: 10.1007/978-81-322-1665-0_81

2. **Ankit Mundra**, Nitin Rakesh, "Implementation and Performance Evaluation of Online Hybrid Model for Prevention (OHM-P)" ICT and Critical Infrastructure: Proceedings of the 48th Annual Convention of Computer Society of India- Vol II, Advances in Intelligent Systems and Computing**, Springer International Publishing Switzerland,** Volume 249, pp 585-592, 2014.

   DOI: 10.1007/978-3-319-03095-1_63

3. **Ankit Mundra**, Nitin Rakesh, S.P. Ghrera, "Empirical Study of Online Hybrid Model for Internet Fraud Prevention and Detection" accepted in **IEEE** International Conference on Human Computer Interactions – ICHCI-2013 *(in Press)*, Chennai, India.