Fake Order Mitigation: A Profile Based Mechanism

Prabhat Kumar, Yashwanth Dasari, Ayushi Jain, and Akash Sinha(✉)

Computer Science and Engineering Department, National Institute of Technology Patna, Patna, India
{prabhat,dasari134763,ayushi.cspg16,akash.cse15}@nitp.ac.in

Abstract. The ever-increasing need and interest of the consumers in online purchases has been a major driver in shaping the persistent and prominent role of e-commerce industry. Business – Consumer trust is a very important factor which should be harnessed for the well-being of this e-commerce community. Such a relationship can be easily hampered owing to the fraudulent behavior of either the consumer or the seller. From a consumer point of view, placement of fake orders can be considered as a breach of trust relationship which may attribute to the losses incurred to the e-commerce industry. Fake orders are those orders which are intentionally cancelled post the packaging and shipment stage. Motivated from this idea, this paper proposes an efficient mechanism to mitigate the fake orders, thereby, reducing the loss of packaging and shipment cost and improving the Business – Consumer relationship. The necessity to reduce the number of fake orders has been discussed eloquently in this paper. A qualitative analysis has been performed to elucidate the efficiency of the proposed mechanism. This mechanism, if implemented, has the potential to mitigate the fake orders which will inherently increase the profit of a company.

Keywords: Fake order · E-commerce · Trust · E-wallet · Virtual cash · Business-Consumer trust

1 Introduction

In the present world where everyone is running behind their goals with a busy schedule, no one has the time for offline shopping. This is one of the prime reasons behind the wider acceptance of the e-commerce platforms in the present context. E-commerce platforms provide a greater advantage with a variety of options by providing millions of brands on a single platform. The range of discounts provided by them is also a vital point which cannot be neglected especially in the consumer context. The global B2C e-commerce turnover is expected to reach $2.352 trillion in the year 2017 [12]. Day by day the users of the e-commerce community are increasing. Taking this into account, the e-commerce industry must withstand with the problems which it is facing today.

One of the major challenge of the e-commerce industry is that there is no unified model to correlate various factors which affect the trust and trade between the seller and the consumer. Also with reference to the Indian context, fake orders are one of the key problems being faced by the industry. Fake orders can be considered as those orders that

A.K. Kar et al. (Eds.): I3E 2017, LNCS 10595, pp. 276–288, 2017.
DOI: 10.1007/978-3-319-68557-1_25

have been placed initially but are intentionally cancelled by the consumers as a later stage. Such an activity can be considered as an intentional attack upon the economy of the target e-commerce industry since the cost incurred in packaging and shipping the order is wasted. This problem has a serious adverse effect on the industry resulting in the net decrease of the profit and hampering the trust between the seller and the consumer community.

In the Indian context, most of the users prefer the option of the Cash on Delivery (COD) [28]. This option of payment has both pros and cons. The consumer always wants to stay on the safe side with this option and as such, the essence of this option of payment in attracting the large number of consumers to an e-commerce portal cannot be overlooked. However, the COD mode of payment is also a significant antecedent of the loss incurred due to fake orders. If the number of fake orders increases the seller may be at a risk. The magnitude of this problem can be understood by the fact that FLIPKART, the Indian e-commerce tycoon that has banned the orders above INR 10,000 in the states of Bihar and Uttar Pradesh [8]. It is, hence, high time to find a consumer effective solution so that this problem doesn't reach its zenith. Further, it is required that the solution should not be only consumer friendly but also seller friendly. The remaining paper is organized as follows: Sect. 2 gives the motivation of this work; Sect. 3 reviews the existing literature in this field of research; the proposed system has been discussed in Sect. 4; Sect. 5 presents a qualitative analysis of the proposed mechanism; a case based on the proposed strategy has been discussed in Sect. 6; Sect. 7 provides a discussion about the research findings; and finally, Sect. 8 presents the concluding remarks and future works.

2 Background

Human behavior cannot be judged because it is subjected to many variations under different contexts, different scenarios and different perspectives [17]. What is of prior importance in one's view may be a subject of post importance in others view. This human incognito tendency is uncertain and varies in an uncanny fashion [17]. The present e-commerce trading system lacks a unified model for evaluating the trustworthy behavior of the consumers. A customer may show his order choice to his friends or family members and ask for their opinion and if the opinion is positive he won't cancel the order. However, if the opinion is negative there is a high chance that he may cancel the order because he has got a negative response from his known people.

It is also important to consider the economic issues which is very vital in the business-consumer community. A consumer may find a low price of the same product on a different platform or he may change his mind considering that the product may not be worthy enough for investing large amount of money on it. Consequently, this shall ultimately result in the rejection or cancellation of the order. This type of abnormal behavior is very common in the e-commerce community and as stated above it varies in an uncanny fashion. Hence there is no chance of getting to know which type of orders are cancelled the most and by what type of users even by applying data mining or statistical analysis.

The above discussed scenarios consider the case of genuine and honest users. However, an adverse user may plan a targeted attack on the e-commerce industry with the intention of hampering the financial gains of the merchant sellers. Such users tend to place the order and later cancel it post-shipment, thereby reducing the net profit of the retailers. Prabhat et al. [19] proposed a mechanism to deal with such socio-technical attacks on the ecommerce business. The authors considered the behavior of the fake users that aim to defame the product retailers thereby, instigating financial loss to the retailers. Such users shall intentionally order those products which involve high packaging and shipment cost. This may incur a good amount of loss to the product seller. If such attacks are made on large scales, it may attribute to a substantial amount of financial loss to the e-commerce industry when considered massive. It is for this reason that, the Indian E-commerce tycoon "Flipkart" decided not to accept high value orders from the states of Bihar and Uttar Pradesh if the payment mode is chosen to be COD [8]. It is vital to state that there are obvious possibilities that these states also incorporate honest users. If such users genuinely require to order valuable goods, then it is a loss to the retailers since the e-commerce platform has restricted the acceptance of such orders. In this context, the mechanism proposed in this paper will play an effective role in controlling the behavior of such untrusted users.

3 Literature Review

Internet has changed the face of business industry enormously. Consequently, the e-commerce industry witnessed an exponential growth in the past few years and as such has attracted the attention of many researchers and practitioners [21]. Several important studies [1, 4] [5] have emphasized upon the need to cater the security and privacy issues of the e-commerce industry. This can be attributed to the fact that the consumers are still not willing to perform high value transactions on the e-commerce portal owing to the security concerns. Moreover, these concerns can be considered to be the significant drivers of the business-consumer trust [12, 14, 22] which is an essential factor for the success of any business activity. In the case of e-commerce, trust becomes even more necessary since the online services and products are not immediately verifiable. Salam et al. [23] indicated in their study that the consumers just don't trust online merchants to take part in exchanges including cash and personal information. Owing to the lack of direct interactions [22] in the e-commerce industry, the authors in [16] investigate the significance of the established dimensions of trust for interpersonal relationships and traditional business-to-consumer (B2C) commerce in shaping the consumer trust in online merchants (e-trust).

Significant research has been performed in the past years regarding the e-commerce trust in various domains of Management, Economics, Sociology and Computer Science. The authors in [9, 18] debated that fraudulent vendors artificially increase their reputations by trading positive feedback ratings on eBay. Xiong and Liu [28, 29] proposed an adaptive trust model, PeerTrust, for quantifying and comparing the trustworthiness of peers. The model relies upon a weighted sum of the factors including feedback records, feedback scope, credibility, transaction context and community context. Bizer and

Oldakowski [6] outlined a trust architecture that has trust policies combining reputation, context and content-based trust mechanisms. It can be clearly observed that most of the work has been performed to mitigate the fraudulent activities of the online sellers. However, not much consideration has been given to the fraudulent behavior of the consumers on the e-commerce portal. As such, there is hardly any literature catering the issue discussed in this paper.

In fact, several works such as [7, 11] that aim to simplify the e-commerce experience of the consumers have inadvertently increased the risk of fake orders. Cameron et al. [7] devised a computerized order entry system and method for placing an order by a user using display mounted terminal. Eggebraaten and Prentice [11] patented a mechanism to add the last order list or a default order list to cart in an automated manner. However, simplifying the modification of the placed orders has led to an increase in the number of fake orders, thereby, posing a serious challenge to the ecommerce companies.

Certain attempts have been made to cater the challenges arising due to the fraudulent behavior of the consumers on the e-commerce portals. A 4D authentication mechanism have been discussed in [24] that considers the importance of comprehensive validation of the consumers upon the placement of any order on the e-commerce portal. The validation may include the verification of the consumer's email address, contacting the consumer over call for verifying the order, confirming the order before shipment, and finally using certain software to perform security checks. Such type of validation can be helpful in establishing the credibility of the consumers to certain extent. Sussman in [26] devised a system to electronically verify a customer using Address Verification Service (AVS). These attempts clearly highlight the urge of incorporating suitable mechanisms to counter the dishonest behavior of the consumers on the e-commerce portals.

4 Proposed Methodology

This section discusses the proposed mechanism which shall facilitate the e-commerce portals to limit the number of fake orders and maximize their financial gains. The objective of this research is neither to demoralize the customers nor disprove their loyalty. This research aims to help the e-commerce organizations to maintain benign relations with the customers so as to make these platforms more reliable.

The proposed mechanism considers the notion of adding certain amount of "virtual cash" to the e-wallet of a user. This virtual cash cannot be used for purchasing purpose unlike the present e-wallet cash. This virtual cash acts as a delimiter to stop the fake orders.

Let X is the amount in rupees credited to the account of the customer when he creates the account for the first time. For placing an order, the software will first check the amount of virtual cash present in the e-wallet. If the amount is sufficient, the order will proceed to the payment option. Else the order will be declined. After the payment is done through the available options the same amount will also be deducted from the e-wallet too. Without loss of generality, it is required that some virtual amount should also be credited to the e-wallet of the users in case of successful orders. However, in case of fake orders the users shall be penalized in terms of virtual cash. The above six are

grouped into three pairs in which every case is dealt separately. By intuition in every case the amount returned will also vary. The Algorithm is as follows:

Proposed Algorithm

1. `Place Order`
2. `Order_Payment_Options(order_amount)`
3. `Debit_Money_From_Ewallet (order_amount)`
4. `Update_Ewallet()`
5. `Exit ()`

The proposed algorithm considers the following Global Variables:
`g_ewallet_amt, g_total_orders, g_total_fake_orders`

Pseudocode for Order_Payment_Options

The following function is used to investigate which payment option is applicable for the order. The function requires the value of the order being placed (order_amount) to evaluate the applicability of COD for that order. If ewallet_amt_status is 1 and the number of fake orders by the consumer is less than the threshold value, then the option for COD along with other pre-payment method shall be available for the customer. Otherwise, the COD option shall be disabled and only pre-payment is allowed. Customer can pay through debit/credit card, net-banking etc. in pre-payment option.

```
ORDER_PAYMENT_OPTION (order_amount)
{
  F = g_total_fake_orders;
  S = ewallet_amt_status(order_amount);
  If (S==YES && F<=25 || F*100/no_of_items<60)
  {
       Payment Options Available:
       Cash on Delivery (COD)
       Pre-payment Methods (Debit/Credit Card, Net Bank-
       -ing, Payment Gateway)
  }
  Else
  {
       Cash on Delivery (COD) unvailable.

       Payment Options Available:
        Pre-payment Methods (Debit/Credit Card, Net Bank-
        -ing, Payment Gateway)
  }
}
```

Auxiliary Function required by the Algorithm for ORDER_PAYMENT_OPTION().

```
boolean ewallet_amt_status order_amount)
{
 if (order_amount <= g_ewallet_amt)
        return 1;
 else
        return 0;
}
```

The above function compares the value of the order being placed with the amount of virtual cash available in the e-wallet. If the virtual cash present in the e-wallet is greater than the value of the current order, it returns 1 else 0.

Pseudocode for Debit_Money_From_Ewallet
This function deducts the virtual cash equal from the Ewallet upon placing an order. The amount of virtual cash to be deducted is equal to the value of the placed order.

```
Debit_Money_From_Ewallet (order_amount)
{
        g_ewallet_amt-=order_amount;

}
```

Pseudocode for Update_Ewallet
The Update_Ewallet function shall be used to credit/debit virtual cash to the ewallet as per the status of the order. The variable ‘order’ can be considered as a structure containing the value of the items comprising the order. The variable T refers to the threshold value for classifying the order as real or fake.

```
Update_e_wallet ()
initialize i=0;
If (Item status = Accepted/exchange)
          add_money_to_ewallet (2*order. item [i].value)
          amt = amt +2* order. item[i].value
Else if (item status = Cancelled before Shipment)
          add_money_to_ewallet(order.item[i].value)
             amt = amt + order. item[i].value
Else
/* Case of cancellation after
Shipment / Rejection */
          add_money_to_ewallet (0)
End If
i=i+1
Repeat step 1to 12 until i<=no_of_items
If(amt<T)
/*fake order*/
          g_total_fake_orders= g_total_fake_orders +1
End If
End If.
End.
```

Auxiliary Function required by the Algorithm for Update_Ewallet().

```
add_money_to_ewallet (float amt)
{
        g_ewallet_amt+=amt;
}
```

The above function is used to credit virtual cash to the ewallet.

Deciding the Initial Amount (X)

Originally, the option of COD was made available for the customers who do not own a credit card or do not have access to online payment modes. Later, it increased impulse purchases as payment was not due at the time of ordering.

The initial amount X is set to the maximum limit of COD amount offered by a particular online purchasing site. This maximum amount differs from one website to other. For instance, the maximum COD limit of FLIPKART is 50000 [13] while that for AMAZON is 30000 [2].

The choice was kept to a maximum and not any other intermediate value. Consider a scenario where the value of X is set to be 10,000. If a customer purchases goods worth 1,000 then the initial amount deducted from e-wallet is 1000. Upon acceptance of the order by the customer, the amount credited to his e-wallet is 2,000 and the total available virtual cash becomes 11,000. Subsequently, he purchases goods worth 7,000 and cancels

his order after shipment due to some genuine reason. After deducting 7,000 he is left with virtual cash amounting to 4,000. Now, if he wants to buy an item worth 10,000 and has no access to any online payment mode then in that case he cannot purchase it.

5 Qualitative Analysis

This section presents a qualitative analysis of the proposed algorithm. The following discussion explains the efficacy of the proposed algorithm under different circumstances. There can be five types of situations which may arise when an order is placed. The order can be accepted, exchanged, cancelled before shipment, cancelled after shipment, or rejected. These situations have been analyzed under two different conditions: *virtual cash is sufficient* and *virtual cash is insufficient*.

5.1 Virtual Cash Is Sufficient

For an item, there can be three cases if the virtual cash present in the user's e-wallet is sufficient, i.e. the total value of the virtual cash is equal to or exceeds the value of the order that needs to be placed.

Case 1. If the status of the item is "accepted" then the amount credited to the e-wallet of the customer will be twice the value of the order. Also, there can be a case that the customer has some issues such as fit, colour, style, size etc. In that case, he opts for an "exchange" request. Even in that case the amount that will be credited to the wallet is twice because penalizing the customer in this case is not genuine since the order is eventually accepted.

Case 2. If the status of the item is "cancelled before the shipment" then also the deducted amount will be returned to his wallet. This type of cancellations happens due to human incognito tendency, cash issues etc.

Case 3. If the status of the item is "cancelled after shipment" then the deducted amount will not be returned to his wallet. If the status of the item is "rejection" then also the deducted amount will not be returned to his wallet. For an order, there can be following cases:

Case 3a. If "total" of all items in an order is greater than threshold value 'T' then the order is not fake order. It will be considered as a real order.

Case 3b. If "total" of all items in an order is less than threshold value 'T' then this type of orders can be termed as fake orders because these have high chances of cancellation or rejection. These types of orders can be placed by the adversaries to reduce the net profit. This can also be termed as a planned attack to waste the resources of a particular e-commerce site. In this case the customer is penalized because nothing is returned to his e-wallet.

5.2 Virtual Cash Is Insufficient

If the customer doesn't have enough amounts in his e-wallet and still he wants to proceed for the payment through cash on delivery, then the order is declined. In this case the e-commerce organizations cannot take the risk of accepting an order from a fake user. Intuitively if he doesn't have enough balance he can be termed as a Sybil user. Consequently, the user shall be provided only with the payment options which do not include Cash on Delivery. Generally, this case has less chance of cancellation as customer has already paid the amount.

The policy for updating the virtual cash in the user's e-wallet will be the same as discussed above.

The analysis of the proposed mechanism clearly reveals that if someone is giving fake orders by continuously cancelling/rejecting them, it will eventually lead to that instance where virtual cash will not be left in the wallet. In this way, the targeted economic attacks by the adversaries and fake orders may be controlled up to a maximum extent and thereby increasing the net profit percentage.

6 Case Study

Suppose that the initial amount he has in his wallet is 5,000. The first order contains 3 items. The total amount of order is 2,000. He rejected or cancelled all the items after shipment. So as per the algorithm we won't return anything to his e-wallet. It will be a fake order according to algorithm. Now presently he is having 3,000 in his wallet. Now he wants to order 2 items of total worth 2,700 from the store. Even this time he repeated the same thing mentioned above. So, the amount in his e-wallet will come down to 300. It is also a fake order. Now he wants to order some items again but as per the algorithm, percentage of fake orders and total orders is greater than 60%. So, cash on delivery (COD) is disabled. He can place a COD order only when he will do pre-payment. Otherwise he can't place an order. Hence, we clearly state that within a short span of 2 orders we have been able to restrict him. The span may increase if he orders the articles of low cost. But still in that case the cost of transport and packaging will be nominal. Even in that case he may be restricted within a few orders albeit it is greater than 2. Now we see the other side of the coin. Here it can be assumed that, in the earlier stages he pretends to be an honest customer and he has increased the amount in his e-wallet by making certain number of successful orders. In this he has a chance to make more number of fake orders. But still the profit gained through the successful orders will compensate this loss making the net loss almost zero. In this way, the loss is compensated.

7 Discussion

The proposed mechanism aims to mitigate the number of fake orders placed as a result of fraudulent behavior of the consumers on the e-commerce portals. The algorithm proposed as a part of the mechanism runs in O(n) time and has the space complexity of

O(n). Incorporating the proposed mechanism into the e-commerce portals requires minimal changes in the current implementation of the portals.

The proposed mechanism may induce certain variations in the total number of real orders that are being currently placed on the e-commerce portal. However, it can easily be deduced, that there shall be a high rate of decrease in the number of fake orders on the portal. The following equation can be used to evaluate the percentage of reduction in the number of fake orders.

$$\text{Decrease in percentage of Fake orders} = \left(\left(F - F'\right)/F\right) * 100\% \quad (1)$$

In the above equation, F refers to the original number of fake orders while F' denotes the reduced number of fake orders.

Considering the above mentioned facts, it is vital to state that there will be a substantial decrease in the financial losses of the e-commerce retailer incurred due to fake orders. Consequently, the proposed mechanism will essentially increase the net profit of the e-commerce industry.

7.1 Contribution

The e-commerce industry is growing faster day by day [22]. However, the exponential growth of the e-commerce industry is being hampered by many challenges such as, fake orders. To the best of our knowledge. this is the first study of its type, which not only explores the context of fake users and orders but has proposes a formal mechanism to mitigate the financial loss incurred by the e-commerce industry due to such fake orders. Online purchasing offers an efficient and hassle free shopping experience to the customers. Owing to the facilities of returning, exchanging or cancelling the order at any time, this mode of shopping is being preferred by the most of the customers. However, it is not necessary that the seller gets profit all the time. If the customer is non-reliable or fake, then the seller may incur substantial loss. This research proposes a novel mechanism with the aim of minimizing the financial loss borne by the online retailers due to fake orders. The proposed mechanism ensures that the online retailer may not suffer any loss due to the order cancellation after the product has been shipped. In the context of the e-commerce industries, this research can be utilized for increasing the net profit of the ecommerce retailers.

The proposed mechanism introduces the concept of virtual cash for limit the fraudulent behavior of the consumers. A customer must have sufficient virtual cash in the e-wallet in order to procure a product using COD option. Online shopping portals, such as Flipkart, Amazon, etc. can utilize this mechanism in their current portals to minimize the cases where orders are deliberately cancelled after shipment due to which the online retailer has to bear the expenses involved packaging, shipment, etc., since the payment option was chosen to be COD. Application of the proposed mechanism will help in minimizing such financial loss, thereby improving the net profit of the retailer as well as the e-commerce industry.

This research clearly differentiates the honest users from the fake users. If a person has a record of successful orders, the amount in his e-wallet increases substantially. He

can be termed as a reliable customer. In this way, the e-commerce retailers can make a set of reliable and non-reliable users. The proposed mechanism also ensures that there is no sign of "Mathew Effect" [20] which is deeply rooted in the e-commerce industry. Although, a consumer may have earlier cancelled few orders due to human incognito tendency, he can still rebuild his reputation by making some successful orders and thereby, increasing the virtual cash in his e-wallet. Hence this model can be seen as a Meta model because risk handling is inherent in this model.

8 Conclusions and Future Work

With the evolution of the e-commerce industry the requirement to sustain the Business–Consumer trust has become the focal point of many research work. The work proposed in this paper considers the behavior of the online consumers for mitigating the losses of the e-commerce industry incurred due to the placement of fake orders. The concept of virtual cash as an indicator of the customers' reputation is an effective strategy to cater the issue of the targeted economic attacks in the form of fake orders. The proposed mechanism is generic and as applicable to all platforms. Further, the implementation of the proposed model requires minimal change in the present architecture of the e-commerce portals. This aspect can be considered to be a significant determinant for the adoption of the proposed method by the e-commerce industry.

Due to the unavailability of the real-time data sets required for testing the model, we have qualitatively analyzed the proposed solution. Future research work may concentrate on upon implementing the proposed solution as a service and exposing the corresponding APIs to be integrated into the existing framework. Additionally, the algorithm can be fine-tuned by considering the other attributes of the consumers in terms of age, gender and location. A more generic solution can be suggested for the recently proposed scenario of Social Internet of Things [25] where the Business – Consumer trust builds upon the past transactions.

References

1. Ahuja, M., Gupta, B., Raman, P.: An empirical investigation of online consumer purchasing behavior. Commun. ACM **46**(12), 145–151 (2003)
2. Amazon: About Cash/Card on Delivery. https://www.amazon.in/gp/help/customer/display.html/ref=hp_gt_pt_cod?nodeId=201818150. Accessed 20 Apr 2017
3. Baabdullah, A., Dwivedi, Y., Williams, M., Kumar, P.: Understanding the adoption of mobile internet in the saudi arabian context: results from a descriptive analysis. In: Janssen, M., Mäntymäki, M., Hidders, J., Klievink, B., Lamersdorf, W., van Loenen, B., Zuiderwijk, A. (eds.) I3E 2015. LNCS, vol. 9373, pp. 95–106. Springer, Cham (2015). doi: 10.1007/978-3-319-25013-7_8
4. Basu, A., Muylle, S.: Authentication in e-commerce. Commun. ACM **46**(12), 159–166 (2003)
5. Bingi, P., Mir, A., Khamalah, J.: The challenges facing global ecommerce. Inf. Syst. Manage. **17**(4), 26–34 (2000)

6. Bizer, C., Oldakowski, R.: Using context- and content-based trust policies on the semantic web. In: Proceedings of the Thirteenth International World Wide Web Conference, New York, NY, May 17–24, 2004, pp. 228– 229. ACM Press, New York (2004)
7. Cameron, P.S., Nash, J.C., Bloomer, R.C., Wollan, R.E., Kreutter, K.M., Olmstead, M.A.A. Renner, D.H., Bourne, R.D., Carnish, K.M., Jones, D.R.: U.S. Patent No. 5,592,378. U.S. Patent and Trademark Office, Washington, DC (1997)
8. Capitalmind: Flipkart Won't Deliver Orders More than 10 K to Uttar Pradesh (2013). https://capitalmind.in/2013/06/flipkart-wont-deliver-orders-more-than-10k-to-uttar-pradesh/. Accessed 27 June 2017
9. Dini, F., Spagnolo, G.: Buying reputation on eBay: do recent changes help? Int. J. Electr. Bus. **7**(6), 581–598 (2009)
10. Dwyer, F.R., Schurr, P.H., Oh, S.: Developing buyer–seller relationships. J. Mark. **51**(2), 11–27 (1987)
11. Eggebraaten, T., Prentice, J.: U.S. Patent Application No. 09/910,534 (2003)
12. eMarketer: Worldwide Retail Ecommerce Sales Will Reach $1.915 Trillion This Year (2016). https://www.emarketer.com/Article/Worldwide-Retail-Ecommerce-Sales-Will-Reach-1915-Trillion-This-Year/1014369. Accessed 27 June 2017
13. Flipkart: Help Center. https://www.flipkart.com/helpcentre/search?query=cash%20on%20delivery. Accessed 20 April 2017
14. Fukuyama, F.: Trust: The social virtues and the creation of prosperity (No. D10 301 c. 1/c. 2). Free Press Paperbacks (1995)
15. Gangeshwer, D.K.: E-commerce or internet marketing: a business review from Indian context. Int. J. u-and e-Service Sci. Technol. **6**(6), 187–194 (2013)
16. Gefen, D.: E-commerce: the role of familiarity and trust. Omega Int. J. Manage. Sci. **28**(6), 725–737 (2000)
17. Harre, R., Secord, P.F.: The Explanation of Social Behaviour. Rowman & Littlefield, Lanham (1972)
18. Jøsang, A., Ismail, R., Boyd, C.: A survey of trust and reputation systems for online service provision. Decis. Support Syst. **43**(2), 618–644 (2007)
19. Kumar, P., Dasari, Y., Nath, S., Sinha, A.: Controlling and mitigating targeted socio-economic attacks. In: Dwivedi, Y.K., et al. (eds.) I3E 2016. LNCS, vol. 9844, pp. 471–476. Springer, Cham (2016). doi:10.1007/978-3-319-45234-0_42
20. Merton, R.K.: The matthew effect in science. Science **159**(3810), 56–63 (1968)
21. Puthiran, S.H.H.: A study on impact of E-Commerce on Indian economy. Int. J. Commer. Manage. Res. **2**(10), 39–41 (2016)
22. Reichheld, F.F., Schefter, P.: E-loyalty: your secret weapon on the web. Harvard Bus. Rev. **78**(4), 105–113 (2000)
23. Salam, A.F., Rao, H.R., Pegels, C.C.: Consumer-perceived risk in ecommerce transactions. Commun. ACM **46**(12), 325–331 (2003)
24. ShipRocket: How to Avoid Fake Orders on Your eCommerce Website (2015). https://www.shiprocket.in/avoid-fake-orders-ecommerce-website/. Accessed 27 June 2017
25. Sinha, A., Kumar, P.: A novel framework for social internet of things. Indian J. Sci. Technol. **9**(36), 1–6 (2016)
26. Sussman, L.: U.S. Patent No. 6,836,765. U.S. Patent and Trademark Office, Washington, DC (2004)
27. Wikipedia: Cash on Delivery. https://en.wikipedia.org/wiki/Cash_on_delivery. Accessed 27 June 2017

28. Xiong, L., Liu, L.: A reputation-based trust model for peer-to-peer ecommerce communities. In: Proceedings of the 2003 IEEE International Conference on ECommerce, Newport Beach, CA, June 24– 27, 2003, pp. 275–284. IEEE Computer Society Press, Los Alamitos (2003)
29. Xiong, L., Liu, L.: Peer trust: supporting reputation-based trust for peer-to-peer electronic communities. IEEE Trans. Knowl. Data Eng. **16**(7), 843–857 (2004)