International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 12 | Dec 2021 www.irjet.net p-ISSN: 2395-0072

Fraud Detection Techniques for Online Transaction in E-Commerce

Abhishek Kumar Singh

Student, Information Technology, Jawaharlal Nehru Technological University, Hyderabad, India

---

Abstract - *The "use of the internet" [1] has become more prevalent globally since the Covid-19 Pandemic and the surge of the utilization of digital technologies, we are currently witnessing a rise in online fraud, security breaches [1]. The wide variety of information that is available on the web has greatly impacted our lives. Due to the increasing number of hackers, the security measures related to online transactions have also become more stringent and to the surge of users who share their private information while shopping online, the security dangers of this have become more prevalent. Worldwide card fraud misfortunes added up to 28.65 billion US dollars in 2020 and are predicted to increase to more than 34 billion by 2022[3]. Numerous precautionary measures have been taken to keep up with the development of these dangers. There are various ways to safeguard the sensitive data of the users. These include implementing a strong "fraud detection system" [4] (FDS) at the source Bank which issues Cards to the users and Behavior Analysis techniques and keeping the data secure [4]. Usually, we are using Captcha, OTP and I am not a robot method, but we can't guarantee that these are 100% secured, moreover if any fraudulent transaction patterns are detected by the system, it will block the user-procedure, but only after three invalid attempts. To plan a strong and effective Fraud Detection System to consider the peculiarities of the fraud phenomenon, and various methodologies have been implemented for Fraud Detection [2]. To prevent such incidents, the system must be regularly updated, and re-verification is performed on all transactions. The increasing number of breaches and hacking attempts on user data could also lead to a spike in the number of transactions. This paper shows the methodologies utilized in Fraud detection in E-commerce.*

Key Words: **Key *Internet, Fraud Detection, Techniques, Online Fraud, E-commerce***

1.INTRODUCTION

In modern technological frameworks, fraudulent exercises have happened in numerous spaces of day-to- day life. For example, E-commerce, online banking, mobile communications. As we see in the current modern technological world, numerous small-scale, mid-scale, and large-scale business have put their organization online to help the customer. Due to this, we can see a significant increase in fraud occurrence as speedy development internet usage is everywhere. The E-commerce-based business draws on modern technologies such as online transactions, internet banking, electronic fund exchange, etc. Consequentially, fraud identification has turned into a significant issue to be explored.

Fraud detection involves recognizing fraud as fast as conceivable whenever it has been executed andfraud detection techniques are consistently evolved due to fast adaption technologies by scammers and adapting to their strategies. It is found from inconsistencies in data and patterns combine. The improvement of new fraud detection techniques is made more difficult because of the serious limitation of the exchange of ideas and data in fraud detection. Data sets are not made accessible, and results are frequently not disclosed to the public. The fraud cases must be identified from the available data sets. As of now, fraud detection has been executed by various techniques like Artificial Intelligence, data mining, and various security measures. In a fraud detection framework, it is important to define performance metrics [6]. The types of e-commerce frauds in this paper are classified into Internet and Merchant. As a rule, the target of fraud detection is to expand correct predictions and keep up with wrong predictions at an adequate level.

2. SIGNIFICANCE OF ONLINE FRAUD WITH WEB SECURITY

Before E-commerce business fraud detection has acquired significance lately, as e-commerce business fraud patterns are on the rise and frauds have become harder to recognize. To secure a business, each merchant and bank ought to follow the recent fraud detection technique. Moreover, e-commerce businesses should keep updating the security protocols about the common types of online frauds so that they don't fall prey to them.

The recent COVID-19 pandemic has fundamentally adjusted how people and organizations approach their day-to-day exercises. For e-commerce business players, the online movement has surged as consumer volumes keep on fluctuating impressively. The expanding number of online users has not just impacted how e-commerce business merchants approach their business practices but has also influenced a pattern of fraud occurrences. Based on recent studies, users now account for nearly 30% of all online

transactions and "Online retail sales share of total retail sales from 16% to 19% in 2020" [7]. In addition, a five-fold growth in "new online account openings were accompanied by an increase in false declines and a rise inomnichannel fraud including a 55% jump in buy online pickup in-store (BOPIS) fraud" [8][16]. As per the LexisNexis Risk Solution in [9] "Every $1 of fraud now costs U.S. retail and e-commerce merchants $3.60 which is 15% higher than the pre-Covid study in 2019 which was at $3.13" [9]. An increase in digitalization and the current pandemic is leading users to shop online and this may lead to a surge in online fraud, spam, identify theft, and issues related to online shopping as it is a serious issue in the web-technology world. Exploring the web while keeping away from these threats can be a challenging task.

3. SURVEY

In this paper, a survey is presented discussing the various kind of fraud techniques, prevention, and management that how it is categorized into card and merchant-related frauds. For example, numerous E- commerce business organizations rely on various independent entities such as payment card processors and call centers. These organizations may likewise employ project contractors like work-at-home customer assistance agents which are blooming after Covid-19. It is hard for an employee at one entity to know or be 100% sure if an email sender is a subsidiary with one of the different connections in the e-commerce business chain. It is crucial to understand the way fraudsters work online because they usually adopt several common ways to deceive users and corporations and crucial to comprehend the way fraudsters work online since they utilize various normal ways to deceive clients and organizations: Let's consider the most widely recognized situations to more likely get where the underlying of frauds might begin.

- Data Breach
- Denial of Service
- Malware
- Phishing/Spoofing

4. HOW FRAUD DETECTION WORKS

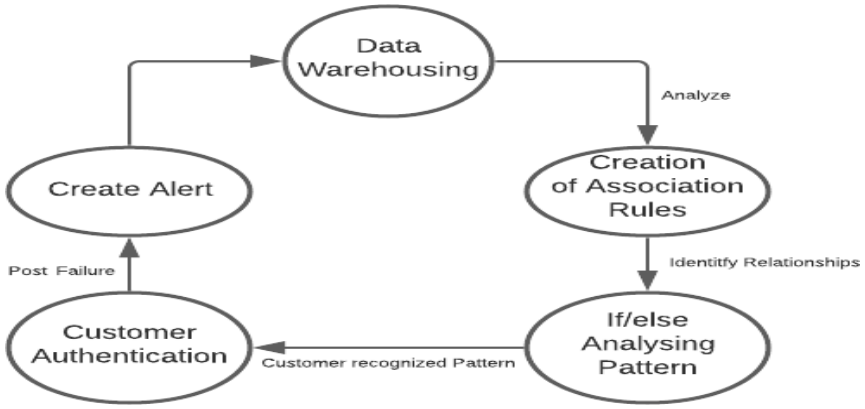

Figure 1 Fraud Threats

4.1 Fraud Techniques

As indicated above the E-commerce Fraud root, there are many ways in which fraudsters execute a fraud online. Fraudulent activities can be broadly categorized into two categories i.e., types of E-commerce fraud

- Internet frauds
- Merchant related frauds

4.1.1 Internet fraud:

The internet has given an ideal ground to fraudsters to commit fraudulent activities merely. Fraudsters lately have begun to operate on a high transactional level and with the development of worldwide social, financial, and political spaces the web has turned into a new world market catching shoppers from most nations globally. The most usually utilized procedures in internet fraud techniques are described below:

False merchant sites:

These websites regularly offer the customer a very modest service. The site demands a client's complete card details like name and address in return for admittance to the content of the website [18]. The greater part of these websites to be free yet require a valid card number to confirm a people age, these websites are set up to collect as many cards as possible and the websites themselves never charge a customer for the service they give, they are normally part of a bigger criminal network that either utilizes the details it gathers to raise incomes or sells legitimate card details in the black market which is known as the dark web.

Interception:

In this sort of fraud, the fraudster makes an order where the billing and delivery address matches the location related to the card. Then at that point, they will attempt to track the package by utilizing one of these strategies:

- Asking customer care to change the location on the order before shipment [19].
- Asking the shipper to re-address the order to where they can intercept the stolen order [19].
- Waiting for the order to arrive at the original cardholder address and dupe the shipper that they are the owner and receive the order and sign for the package [19].

Phishing:

E-commerce based business exercises and online exchanges require trust and certainty by the customer in the e-commerce website and its security. Subsequently, the e-commerce business is particularly defenseless to phishing attacks because phishing is “nothing more than a confidence game” [10] making a misguided feeling of certainty and fooling customers into succumbing to a scam. Phishing is characterized as “the utilization of spoofed messages and false websites intended to trick receivers into divulging individual and financial information” [11] Furthermore, keeps on viewing that "the broad objective is identity fraud; phishers attempt to trick web visitors into revealing their login details, sensitive data, or card numbers” [12] only to gain an advantage over visitors.

Internet users will first and foremost be sent a spoofed email [10]. These email messages are hard to distinguish by visual checks and spam filters and are intended to be highly conceivable and reliable. Different internet-based devices make them simple to spoof and because they can be sent off huge quantities of individuals all at once, it is the most utilized and favored technique for the attack. They will regularly likewise be portrayed as an urgent call to action, empowering customers to follow a hyperlink letting them know that they will get a prize for consenting, or suffer a punishment over failing to agree, consequently guiding them to the phisher's website.

Site cloning:

“Site cloning is the place where fraudsters clone a whole website or simply the pages from which you submit your order, customers have no good reason to accept they are not managing the organization that they wished to buy goods and products from since the pages that they are seeing are similar to those of the genuine site” [18]. The cloned website will get these details and send the customer a receipt of the exchange through email similarly as the genuine organization would. The customer suspects nothing, while the fraudsters have every detail, they need to do fraud.

Account Takeover Fraud:

This sort of fraud happens when a fraudster wrongfully gets substantial customer's personal data. The fraudster takes control of legit accounts either by providing customer's account details or the card number [18]. The fraudster then contacts the card provider by taking on the appearance of the legit cardholder, to ask that mail/order to be diverted to another location.

4.1.2 Merchant Related Frauds:

Merchant fraud is a strategy that permits criminals to open a fake merchant account and mimic a genuine dealer i.e., merchant to acknowledge payments. This type of frauds is started either by the owner of the merchant foundation or their employees and are classified as below:

Triangulation:

This type of fraud is called triangulation because it involves an "authentic customer, an E- commerce business, and a fraudster" [19]. The fraudster in this type of fraud operates from a website, goods are offered at heavily discounted rates and are also shipped before payment as the website appears to be legitimate [18]. The customer while placing orders online provides all the personal details including card details to the website. Once fraudsters receive these details, they "order goods from a legitimate website using stolen card details" and place the order [17]. The fraudster then goes on to purchase other goods using the card numbers of the customer [18]. This process is designed to cause a great deal of initial confusion, and the fraudulent internet company in this manner can operate long enough to accumulate a vast amount of goods purchased with stolen card numbers.

Merchant Collusion:

This type of fraud happens when merchant owners and their employees plan to commit fraud utilizing their customer's card details and personal data. "Merchant owners and potentially their employees give the data about cardholders to fraudsters" [18].

5. FRAUD PREVENTION AND MANAGEMENT:

"The best way to combat fraud is to identify why fraud is occurring in the first place and then develop strategies to prevent and protect against these attacks to secure your e-commerce site" [20]. To begin, we have to "identify the type of fraud that is occurring on your platform and then address it directly" [20]. As fraudsters are utilizing complex strategies to get access to credit card data and execute fraud, new technologies are accessible to help merchants to distinguish and prevent fraudulent transactions [18].

5.1 Take Advantage of Fraud Detection Solutions

This is possibly the best way to fight against all types of e-commerce business fraud. It is a third-party solution that spends significant time recognizing red flag transactions and shielding e-commerce business merchants from card testing fraud and all other fraud. A fraud detection solution is useful for e-commerce business organizations. All things considered, it very well may be significant for more modest organizations who don't have the resources, assets, or knowledge to carry out their fraud solutions.

5.2 Maintain PCI Compliance

The Payment Card Industry Data Security Standard (PCI) is a generally regarded set of prerequisites guaranteeing organizations putting away and handling card and cardholder data like e-commerce business organizations keep a secure environment. PCI compliance brings about essential security safeguards including things like creating a firewall between your internet connection and any framework like storing card details [20]. Eventually, PCI consistency is mandatory so that you should guarantee that you are maintaining significant PCI rules to stay away from any authorizations or penalties.

5.3 Address Verification System:

This procedure is applicable in "card-not-present" situations. Address Verification System (AVS) coordinates with the initial few digits of the street address and the ZIP code data given for "delivering/billing" the purchase to the relating data on record with the "card issuers". A code addressing the degree of match between these addresses is return [18].

5.4 Negative AND Positive Lists

A negative list is a data set used to recognize "high-risk" transactions dependent on specific information fields. An illustration of a negative list would be a record containing all the card numbers that have delivered chargebacks before, used to stay away from additional fraud from repeat fraudsters [18]. Also, a merchant can assemble a negative list dependent on billing names, street locations, email, and IPs that have brought about fraud or attempted fraud, blocking any further attempts [18]. One more famous illustration of the negative list is the "SAFE" record circulated by the card issuers to merchants and banks. This list contains card numbers that could be possibly utilized by fraudsters e.g., cards that have been accounted for as lost or taken in the quick ongoing past [18].

Positive documents list is regularly used to perceive "trusted customers", maybe by their card number or email address, and along these lines by specific checks. Positive records address a significant device to forestall unnecessary in handling legit orders [18].

5.5 Payer Authentication

Payer authentication is an arising innovation that vows to get another level of security to e-commerce businesses. "The program depends on a Personal Identification Number (PIN) related to the card, like those utilized with ATM cards, and a secure direct verification channel between the customer and the responsible bank" [18]. The PIN is given by the bank when the cardholder enrolls the card with the program and will be utilized only to approve online transactions [18]. At the point when enrolled cardholders look at a participating merchant's site, they will be promoted by their responsible bank to provide their password, when the password is confirmed, the merchant might finish the transaction and send the confirmation data to their client [18].

5.6 Lockout Mechanisms

Auto card number generators address one of the new technological tools as often as possible used by fraudsters [18]. These tools are effectively downloadable from the internet and able to generate many legitimate card numbers.
The characteristics of fraud started by a card number generator are the following:

- Numerous transactions with the same card numbers [18].
- Countless declines in obtaining bank/merchant websites can set up counteraction mechanisms explicitly intended to identify number generator tool fraud [18].

5.7 Fraudulent Merchants

The Card manufacturers distribute a record of merchants who have been known for being associated with fraud transactions previously. These records could give valuable data to acquirers right at the time of merchant enrollment preventing possible fraud transactions.

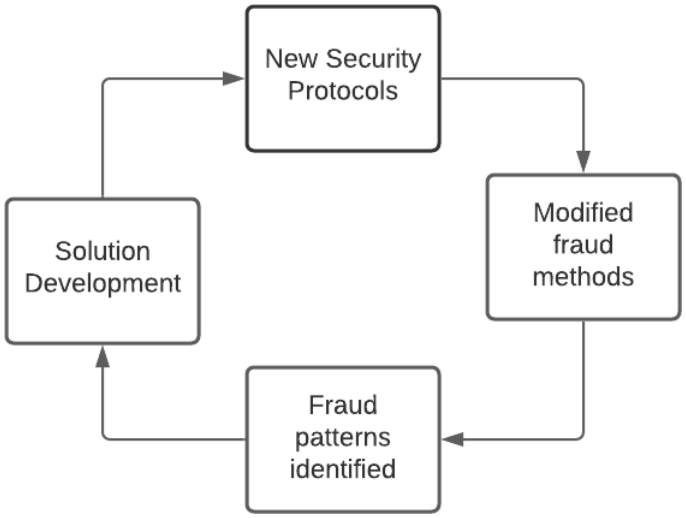

Figure 2 Threat Cycle

6. PREVENTION MEASURES:

Everything you can manage in the present circumstance is to not allow fraudsters to utilize the data they took. You can do this by executing a fraud prevention service that would consequently recognize fraudulent behavior patterns. "The layers of a fraud prevention framework need to incorporate safe validation, device analysis, navigation, and the likelihood to coordinate these data sources with a real-time fraud prevention solution "[19].

Secure Electronic Transaction:

Secure Electronic Transaction (SET) is a framework and electronic protocol to guarantee the integrity and security of exchanges directed over the web. E-commerce business websites executed this early protocol to secure electronic payments made through cards. SET isn't a payment system but a set of security protocols. It utilizes a few parts of a Public Key Infrastructure (PKI) to address worries around privacy, credibility, and security in e-commerce business applications [13]. The essential objective of SET is to secure card exchanges as they occur online. It gives a secured and classified exchange environment for everybody associated with the e-commerce business transaction including the customer and merchant. It additionally confirms the clients with the assistance of digital certificates [14]. SET was designed to fulfill the requirements for e-commerce security that were not being fulfilled by SSL and Transport Layer Security (TLS). To secure card transactions and protect purchasing information, SET uses both symmetric (Data Encryption Standard or DES) and asymmetric (PKI) cryptography.

SET was intended to satisfy the prerequisites for e-commerce business security that were not being satisfied by SSL and Transport Layer Security (TLS). To secure transactions and protect purchasing data, SET utilizes both symmetric (Data Encryption Standard) and asymmetric (PKI) cryptography.

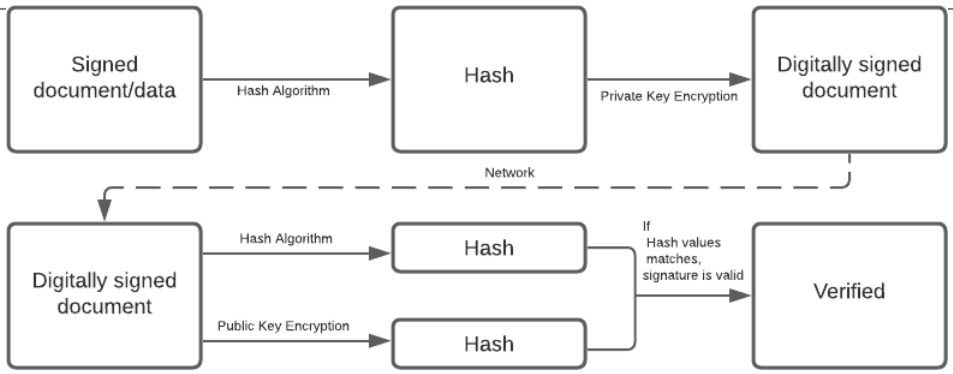

Figure 3 Digital Signature Process

The security properties of SET are better than SSL and the more current TLS, especially in their capacity to prevent e-commerce-based business fraud. However, the greatest disadvantage of SET is its complexity. SET requires both customers and merchants to install unique software (card readers and digital wallets) - implying that transaction participants needed to do more jobs to carry out SET. This complexity additionally slowed down the speed of e-commerce business transactions. SSL and TLS don't have such issues, visa and other card suppliers ultimately took on the three-dimensional(3-D) secure system for securing client's digital payments. This XML-based protocol is intended to give extra security to online transactions.

7. FINDINGS:

Considering the E-commerce business several frauds are occurring online, e-commerce businesses and organization leaders are fighting hard to minimize the occurrence of fraud.

From my findings, E-commerce is deploying machine learning technology and it's playing a vital role in fraud prevention systems with the recent surge in e-commerce utilization all around the world and the chance of an online fraud attack is at a peak. "A new study from Juniper Research has found that the value of losses due to e-Commerce fraud will rise this year from $17.5 billion in 2020 to over $20 billion by 2021" [15]. Customers want to have the assurance that they can purchase products without experiencing a false decline and merchants want to feel that they can trust the legitimacy of new incoming transactions. Clients need to have the affirmation that they can buy items without encountering a false decline and merchants need to feel that they can trust the authenticity of new transactions. "We can recognize fraudulent e-commerce scenarios identified with online purchases, transactions, and chargebacks "[19].

In general, we can recognize which activity occurs from a hacked customer account. Machine learning for e-commerce utilizes supervised and unsupervised anomaly identification strategies that track fraudulent patterns in online transactions data or customer behavior patterns [19].

7.1 Machine Learning for E-commerce works so well because of the following benefits.

7.1.1 Data Processing in Real Time:

Traditional detection frameworks can just work with situations that have happened already and prevent the sorts of frauds that have happened previously. Just when an attempt is successful can the framework make the right conclusion. With machine learning, it is distinctive since algorithms can think about changes in real-time and follow up on a fraud attempt and sometimes even before the attack.

7.1.2 Tracking the Hidden Patterns

A machine learning-based framework is constantly learning. Not just it is acceptable at tracking the hidden patterns past human abilities, yet in addition with each found threat it turns out to be better at tracking the new situations and preventing them.

7.1.3 Behavioral Analytics

At the point when the framework knows the common behavior standards of conduct of every customer, it can easily pick on deviations and spot suspicious behavior. Now and again, it tends to be a simple way of distinguishing a fraudster accessing a customer's record. In addition, customers and merchants should be aware of fraud techniques and the trends like phishing. They should also be aware of all functionalities of various websites and make sure that their card details are not shared with anyone.

8. FUTURE WORK:

As e-commerce business consistently changes, so does e-commerce business fraud. "While things like card testing fraud, friendly fraud, and chargeback fraud will probably persevere into the distant future" [20]. We can anticipate that fraudsters gain profit on several distinct trends and patterns.

"Account takeover attacks and fraud are expected to increment sooner shortly because an enormous number of high-profile data breaches have occurred in the past years" [20]. "With customer data close by, fraudsters can impersonate genuine individuals and make purchases on the website" [20]. They frequently use bots to execute this kind of fraudulent on a bigger scope, implying that clients and organizations should be ready. However, the headways given by algorithmic and behavioral ways to deal with fraud detection implies that e-commerce-based business organizations will be better prepared to battle against fraudsters. "Predictive and behavioral models controlled by machine learning help online business organizations better combat fraud attempts today" [20]. However, another issue in e-commerce business fraud has become progressively notable "the issue of false positives" [20]. Numerous famous fraud detection arrangements available today have depended on defective fraud instruments that coincidentally reject great clients attempting to make a buy. This adversely affects an organization's revenue primary concern in many cases, the net effect of misfortunes because of false positives is greater than the effect of fraud losses themselves [20]. At present already big players like Amazon are using the 'if. then' criteria to filter the transactions.
Here are the things which can happen in the future of e-commerce business to fight fraud detection

- Individuals will be able to purchase things online without a card number or validation. A person's computerized digital fingerprint will permit retailers/merchants to know who an individual is, just as how the person likes charges to be applied.
- Fraud prevention and detection will be totally automated and no manual review of transactions.
- Retailers/Merchants will get away from the responsibility for fraud, they can focus on developing deals and on the customer experience because of this new period of innovation and automation.

9. CONCLUSION

In this paper, various types of Fraud techniques and their prevention and measures are discussed. It presents the attributes of fraud types, the need for fraud detection frameworks, several current fraud detection techniques, and the possibility of future works.

In the present generation, online shopping will be well known and will reach its peak day by day. E- commerce business payment frameworks have become well known because of the far and wide utilization of web-based shopping and banking. After pandemic the amount of user's shopping at e-commerce across the world is also giving the chance of increasing in the number of fraudulent activities. Fast augmentation of this period, billions of dollars is lost each year because of fraudulent activities. Fraud is a demonstration of betrayal expected for individual utilization or to hurt a misfortune to somebody and the fraudster just needs to know the individual data identified with the card number, card expiry date, and so on. When starting or doing a business the businesses should always follows the latest trends and security strategies like PCI guidelines so that it's make convenient and dependable for business and customers to shop.

10. REFERENCES

[1] Agarwal S., Sengupta D., Kulshrestha A., Anand S., Guha R. The Economic Times; 2017 Internet users to touch 420 million by June 2017: IAMAI report https://economictimes.indiatimes.com/tech/internet/420-million-to-access-internet-on-mobile-in-india-by- june-iamai/articleshow/58475622.cms. Retrieved on 10/15/21
[2] A. Dal Pozzolo, G. Boracchi, O. Caelen, C. Alippi, and G. Bontempi, "Credit card fraud detection and concept-drift adaptation with delayed supervised information," in Proc. Int. Joint Conf. Neural Netw. (IJCNN), Jul. 2015, pp. 1–8.
[3] HSN Consultants, Inc. (Oct. 17, 2020). The Nilson Report 2020. [Online]. Available: https://nilsonreport.com/upload/content_promo/1187_9123.pdf. Retrieved on 10/15/21
[4] C. Phua, V. Lee, K. Smith, R. Gayler, "A Comprehensive Survey of Data Mining-based Fraud Detection Research," Artificial Intelligence Review, 2005.
[5] K. Yufeng L. Chang-Tien, and S. Sirirat, "Survey of Fraud Detection Techniques in Networking, Sensing and Control", IEEE International Conference, 2, pp. 749 – 754, 2004. ISSN: 1810-7869.
[6] Vijay Kanade, What Is Fraud Detection? Definition, Types, Applications, and Best Practices, Jun.16,2021https://www.toolbox.com/it-security/vulnerability-management/articles/what-is-fraud- detection/ Retrieved on 10/28/2021

[7] Shamika N. Sirimanne. COVID-19 and e-commerce: a global review, Mar.11,2021. https://unctad.org/webflyer/covid-19-and-e-commerce-global-review. Retrieved on 11/04/2021
[8] Bryan Wassel. Delivery and BOPIS benefit, shopping centers not yet heavily impacted," Retail Touchpoints, March 11, 2020, https://retailtouchpoints.com/topics/omnichannel-alignment/coronavirus- update-delivery-and-bopis-benefit-shopping-centers-not-yet-heavily-impacted. Retrieved on 11/04/2021
[9] LexisNexis Risk Solution. The True Cost of Fraud™ Study, Jul. 05, 2021. https://risk.lexisnexis.com/insights-resources/research/us-ca-true-cost-of-fraud-study. Retrieved on 11/04/2021
[10] M. Jakobsson and S. Myers, "Delayed Password Disclosure" in 'Distributed computing' column of the ACM SIGACT News (2007), New York, NY:ACM Press, vol. 38, no. 3, pp. 56-75, 2007.
[11] S. Martin, B. Nelson, A. Sewani, K. Chen, and A. Joseph, "Analyzing Behavioral Features for Email Classification," CEAS, 2005.
[12] C. Karlof, J.D. Tygar, D. Wagner and U. Shankar, "Dynamic Pharming Attacks and Locked Same origin Policies for Web Browsers", the proceedings of the 14th ACM conference on Computer and Communications Security (Alexandria Virginia USA 2007), pp. 58-71, 2007.
[13] T. ElGamal, "A Public Key Cryptosystem and a Signature Scheme Based ondiscrete Logarithms", IEEE Trans. Information Theory, vol. IT, no. 4, pp. 468-472, 1985.
[14] R. L. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", Communications of the ACM, vol. 21, no. 2, pp. 120-128, 1978.
[15] Sam Smith. Ecommerce Losses to Online Payment Fraud to Exceed $20 Billion annually in 2021,Apr.26,2021.https://www.juniperresearch.com/press/ecommerce-losses-online-payment-fraud-exceed20bn#:~:text=Hampshire%2C%20UK%20%E2%80%93%2026th%20April,18%25%20over%20a %20single%20year. Retrieved on 11/08/2021
[16] Vijay Kanade. Top 10 Ecommerce Fraud Detection and Prevention Best Practices for 2021, Jun.25,2021. https://www.toolbox.com/it-security/vulnerability-management/articles/top-10-ecommerce- fraud-detection-and-prevention-best-practices. Retrieved on 11/10/2021
[17] Ekrem Malkoc, Organized Credit Card Fraud: The European Perspective, Apr 2005. https://www.academia.edu/9738866/Organized_Credit_Card_Fraud_The_European_Perspective Retrieved on 11/10/2021
[18] Tej Paul Bhatla, Vikram Prabhu & Amit Dua, Understanding Credit Card Frauds, Jun.2003. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.431.7770&rep=rep1&type=pdf. Retrieved on 02/11/2021.