



E-PAYMENT SYSTEMS RISKS, OPPORTUNITIES AND CHALLENGES FOR IMPROVED RESULTS IN E-BUSINESS

Mohmed Hassan Nasr

Mohamed.Hassan16690@gmail.com

Business Analyst at Omniex international,
Caior, Egypt

Mohamed Farrag

Mohamed.Farrag@Fayoum.edu.eg

Information Systems Department,
Faculty of Computers and Information
Fayoum University, Fayoum, Egypt

Mona Mohamed Nasr

M.Nasr@helwan.edu.eg

Information Systems
Department, Faculty of
Computers and Information
Helwan University, Cairo,
Egypt

Abstract: *E-payment is the key function for any e-business as it is rising exponentially in today's business world as e-business grows. E-payments made it easier for people to survive and helped them save a lot of money and time. Using various forms and devices, our payments are more exciting and convenient to press on your mobile phone and pay for your orders. In order to obtain better results in e-business, it must be linked to e-payments. E-payments have many systems and opportunities in the field of e-business, but it is facing many risks and challenges. This paper presents an overview study for e-payments opportunities, challenges and different risks for e-payments specially fraud as it is one of the most critical threats to e-payments field and it is causing huge losses. Paper also discusses different types of e-payments, benefits and the future of e-payment.*

Keywords: *E-payments; E-Commerce; Fraud detection; Online payments*

1. Introduction

Technology and e-payments have been one of the most significant obstacles every company faces in the internet age. Simplicity of payment helps consumers to buy, saving effort and time. Today, most companies, government departments and corporations have embraced electronic transactions to improve their profitability or efficiency in selling goods or services in areas such as credit card, banking, health insurance, automobile insurance, online auction, etc. E-payment systems allow financial institutions, businesses and the government to offer a diversity of payment options to their customers. Electronic payment systems are replacing the old methods of payment that involved personal contact between buyers and sellers. E-payment systems help cut costs for businesses and consumers alike. Businesses save on production and manufacturing costs mostly due to a decrease in technical costs. The e-payment system is

considered to be the foundation of e-commerce and one of its most important aspects. The viability of e-payment system depends on how it overcomes the practical and theoretical challenges facing various online payment methods. This paper presents research study of different risks for e-payments and discusses the types and benefits of e-payments.

2. Background

We may consider that e-payment is a subset of an e-commerce transaction that involves electronic payment for the purchase and selling of products or services provided over the internet and that e-payments may simply be defined as paying goods or services over the internet. There are several other meanings for e-payments, in which the e-payment method is a type of financial agreement that includes the purchaser and the seller, facilitated by the use of electronic communications. Another definition describes e-payment as any form of transfer of funds through the internet. The area of e-payment is growing very quickly, and this involves increasing e-payment forms and also increasing e-payment opportunities, risks and challenges.

3. E-payment types and cycles

One of the most disturbed areas of the business by innovative technologies such as artificial intelligence, block chain, machine learning, and cloud computing is payment and settlements [2]. In the real e-business world nowadays many e-payment types established some of the most important e-payment types and its cycles are discovered below. E-payment systems are important mechanisms used by individual and organizations as a secured and convenient way of making payments over the internet [12].

Credit Card

Cards are the most common type of electronic payment. For online transactions, credit cards, charge cards and debit cards are among the payment options available. Nonetheless, credit card is the most common form of payment for online purchases. Visa and MasterCard are one of the most common credit cards used for online transactions. Credit card cycle start when customer (card holder) do some purchases and want to pay to merchant using his credit card. Merchant enter transaction's details into his terminal to be sent to acquirer. Merchant will have signed a merchant service agreement with its acquirer to process payment card transactions. The agreement also include the acquirer to provide one of its own terminals, known as an acquirer owned terminal. The acquirer process the transaction to be send to the relevant card issuer for authorisation and settlement but before sending it to issuer it is send to card schema. Card schemes are organizations which manage and monitor the processing and clearing of card payment transactions according to the rules of the card scheme. Card schemes are responsible for transmitting the details of the card transaction from the purchaser to the issuer and for returning the payments to the purchaser who pays the merchant. Example for card scheme organizations (Visa, MasterCard, American Express). After card scheme revision transaction sent to card issuer which is the credit card holder's bank. Figure 1 below shows credit card cycle.

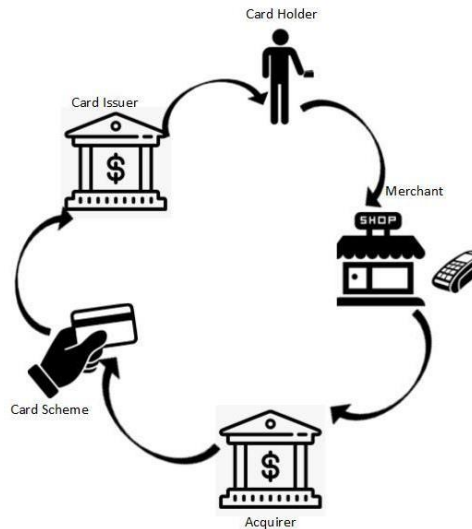


Figure.1 Credit Card Cycle

Mobile Payment

Since you only need to download software, connect it to your credit card or mobile billing details to start making payments, you are one of the fastest types of e-payment systems. You only need to make this setup once, and then instantly make payments through text message requests. This payment form, while fast, is the most vulnerable to security threats. Mobile payment cycle as shown in figure 2 start when customer use an application on his phone device that allow him to pay for products and services. Customer charge his application balance and send request to pay to service provider though his mobile internet.

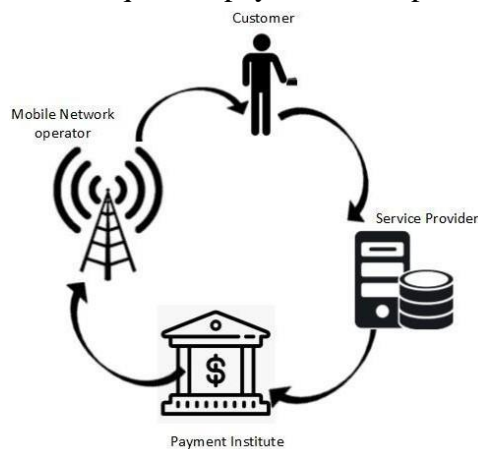


Figure. 2 Mobile Payment Cycle

E-Payment Gateway

An electronic payment gateway system is a software service that connects with retailer and service provider networks and enables consumers to make payments through these. E-payment processing providers provide a wide network of agents that can be paid by consumers through these agents. As shown in figure 3 cycle start when customer went to one of those merchants and ask to pay for a service. Merchant use an application on his terminal to send payment request to e-payment provider and e-payment send request to service provider to be paid.

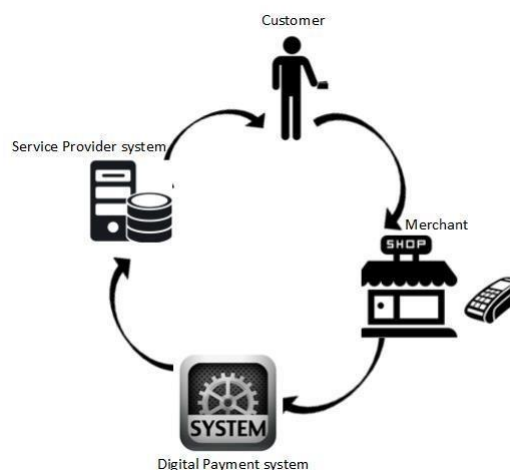


Figure. 3 E-Payment Gateway Cycle

Internet Banking

Technology has arguably made our lives easier. One of the technological innovations in banking, finance and commerce is the Electronic Payments [3]. Online banking was first introduced in the early 1980s in New York, United States [5]. It is the safest one among types of e-payment system as you can just pay for any product or service you like by using the money in your bank account. You do not need a credit or debit card to make the payment through internet banking, and you just need to provide your bank id and password to complete the transactions. When customer want to pay for a service or a product he use his bank application on his mobile or on the bank website which allow him to pay to service provider as figure 4 shows.

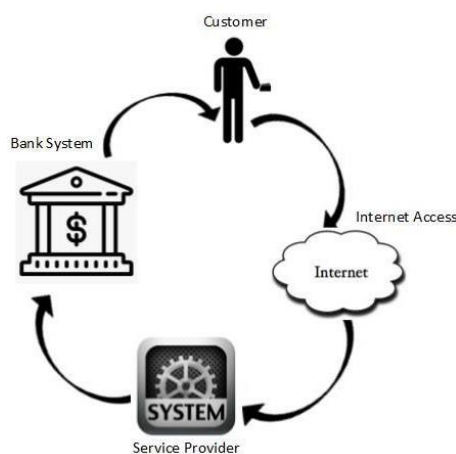


Figure. 4 Internet Banking Cycle

E-Wallet

A form of prepaid account that stores user's financial data [1]. This kind of online payment service includes PayPal, Google Pay and Apple Pay. The company helps customers to make prepayments and bank transfers to cover online payments. PayPal is the pioneer in this sector with more than 200 million active users. Unlike e-wallets like Apple Pay, which only operate on a specific smartphone brand, PayPal

works across all types of devices that can access the internet. Figure 5 shows e-wallet cycle as it start when customer open a bank account and download his bank e-wallet application on his mobile. E-wallet application allow customer to pay to merchant, transfer money to other wallets for same bank or other banks, receive money from other e-wallets accounts, make cash in and cash out and pay for his bills.

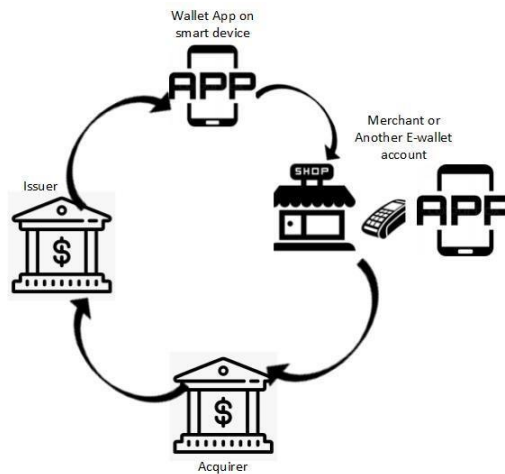


Figure. 5 E-Wallet Cycle

E-Checks

Many payment processors require you to collect electronic checks or "E-checks" from your customers. Many payment processors require you to collect electronic checks or "E-checks" from your customers. The purchaser enters your bank routing number and account number in your online order form. These details are then forwarded to the processor who completes the transaction and deposits the net funds in your bank account. Many payment processors require you to collect electronic checks or "E-checks" from your customers. The purchaser enters your bank routing number and account number in your online order form. These details are then forwarded to the processor who completes the transaction and deposits the net funds in your bank account. One downside of e-checks is that they do not work instantaneously as credit cards do. This means that a customer can write a bad e-check to your company. Figure 6 below shows e-check cycle.

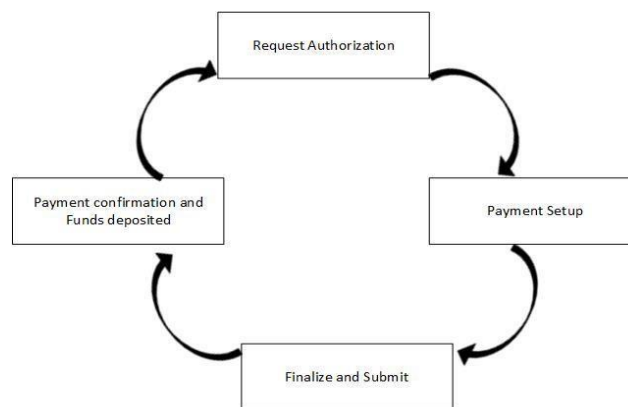


Figure. 6 E-Check Cycle

4. E-payment returns

E-payments have many benefits and advantages for individuals and businesses. On the individual level, e-payments facilitate the payment process as for effort and time spent. On the business level, it helps to

increase the number of customers and provide services and products to these customers at the lowest cost and in the fastest time through a completely safe environment, which helps to increase customer confidence. In the below figure 7 we try to introduce some of the benefits of e-payments, whether for individuals or businesses.

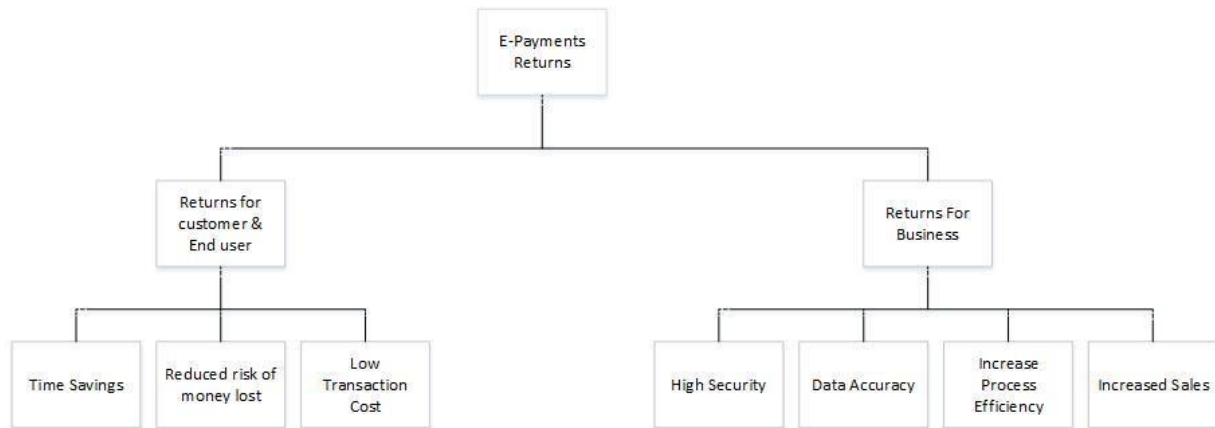


Figure. 7 E-Payment Returns

Returns for customers and end users:

- **Time Savings:** You don't have to wait and waste a lot of time waiting in the queues of the banks and the post office, and then your transaction will take hours or days. Using an e-payment program, you can make money transfers with no waste of time in just a few minutes.
- **Reduced risk of money lost:** While electronic wallets are virtual, it cannot be left somewhere or even robbed by someone. You just need to make sure you have a secure e-payment account
- **Low transaction cost:** Using e-payment system, you will face no additional charges for making a cash payment

Returns for Business:

- **High security:** E-payments system is unlike paper-based payment systems it is more secure. E-payment systems provide a real-time financial metrics for accurate audit trails and high visibility to avoid and detect fraudulent activity.
- **Data accuracy:** E-payment systems provide accurate data it also increases workflow efficiency of businesses and decreases costs incurred because of data entry mistakes. Also, because it becomes so much easier to monitor and track data, businesses are allowed to better fulfil with complex financial rules that apply to their respective activities.
- **Increase process efficiency:** E-payment system rises visibility into the financial supply chain. This enables positive decision-making. It also rises process efficiency, as is provides easy access to snapshots, reports and comprehensive financial history data. A greater visibility into payment statuses, collections groups, and internal customer service departments, which leads to better approvals and overall customer satisfaction.
- **Increased sales:** Businesses who allows customers to pay electronically gain a competitive advantage over those who accept only traditional payment methods. E-payment methods is more secure, easy and time saving than traditional methods.

5. E-payment challenges and risks

E-payments face many challenges and risks that prevent their expansion and spread. These challenges and risks are a top priority for anyone involved in the e-payments industry, from individuals, organizations, researchers and even governments. Below is a review of some of these challenges and risks.

Challenges

The challenges of e-payments vary between challenges related to restrictions, laws, awareness and culture of some societies. This type of restrictions needs to increase awareness of the importance of e-payments and change laws that would facilitate e-payments and challenges related to information security and the privacy of individuals and institutions. Figure 8 shows some of these challenges.

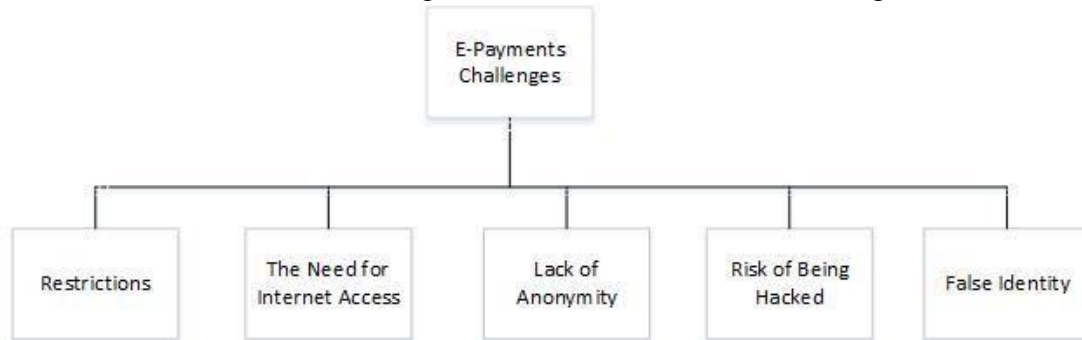


Fig.8 E-Payments Challenges

- **Restrictions:**

In every payment system, there is a limit with regard to the number of transactions you can do per day and the maximum amount you can withdraw.

- **The Need for Internet Access:**

When you have no Internet connection, you cannot transact on your online account.

- **Lack of Anonymity:**

Since the database of the payment system stores all your transactions - like the name of recipient, amount and time - the intelligence agency can access all your information. Decide on whether that is good or bad.

- **Risk of Being Hacked:**

E-payment system can be hacked it any time if they do not have powerful security system and also E-payment users can be hacked if they did not follow security regulations.

- **False Identity:**

There are no means to verify if the person entering information online is the same person, he claims to be. This is because unlike physical transactions, the individual is not present in person, and one's identity is not verified using a photograph or a physical signature.

Risks

Like any other field, e-payment field faces several risks. These risks need to be faced and limit their impact. The risks to e-payments are a major drawback. These risks cause many financial losses for companies and customers. Figure 9 shows some of these risks and we introduce explanation of some of these risks, especially the risk of fraud as it is one of the most critical risks that causes a lot of losses and we introduce some of the research papers that proposed different techniques for fraud detection in different payment areas.

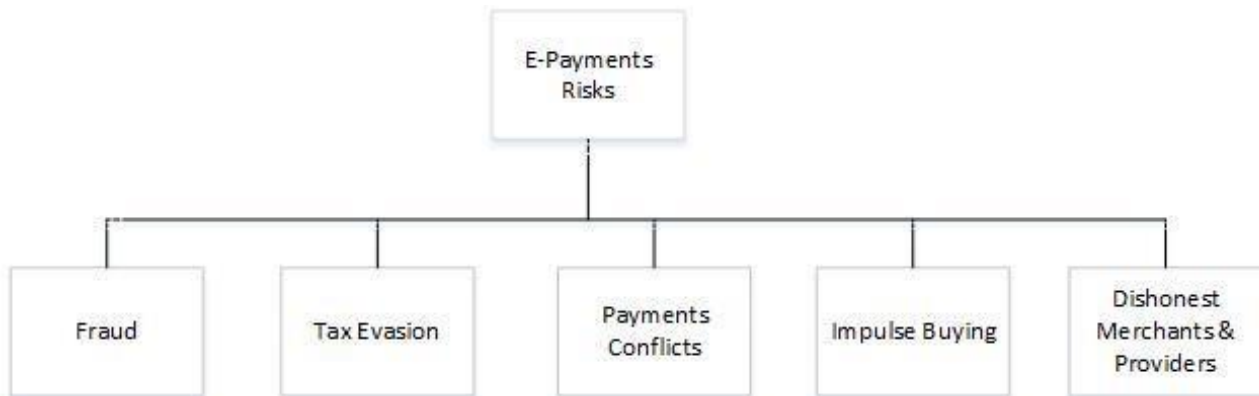


Figure. 9 E-Payments Risks

Fraud:

Fraud can be defined as the undesired activities taking place in an operational system [15]. E-payments companies and their customers suffer billions of dollars in fraud losses annually as it affects the entire e-payments industry. According to data from “ACI Worldwide” the number of fraud attempts based on total population in 2015 increased to 1.49% compared to 1.39% in 2014, i.e. one out of every 67 transactions was a fraudulent attempt in 2015 compared to one out of every 72 transactions in 2014. Which represents a 7.1% increase during the year. All this numbers show how it is very important to work against fraud attacks and how it is important to have solutions for those attacks.

Tax Evasion:

Businesses are required by law to provide the government with records of their financial transactions so that their tax compliance can be checked. E-payment, however, can thwart tax collection efforts. Until a company discloses the numerous e-payments it has made or received during the tax period, the government will not know the truth that may lead to tax evasion.

Payment Conflicts:

Payment problems also occur because payments are not made manually, but through an automated system that can cause errors. This is particularly important when payment is made on a daily basis to several recipients. For example, if you do not review your pay slip at the end of will pay period, you could end up in a dispute due to such technical issues or anomalies.

Impulse Buying:

E-payment systems promote pulse transactions, particularly online, and consumers are likely to make a decision to buy an item they find on sale online, as it will cost only a click to buy it via a credit card. The buying of impulses leads to disorganized budgets and is one of the drawbacks of e-payment systems

Dishonest providers and Merchants:

Those who exploit and sell consumers 'personal data in order to be used by advertisers in ads often use this data for fraud purposes.

6. Overcoming fraud in e-payment

In order to overcome and limit fraud operations in e-payment field we should keep abreast of the new trends in fraud, partner with a checked processor for payment, encrypt emails and transactions which contain sensitive information, ensure tokens and authentication details are updated regularly and create a policy on access to sensitive information. Also using antivirus software to continuously run security tests and allow clients to sign in to a single account before making a purchase. On the side of scientific research one of the area’s that most vulnerable to fraud is e-payment area and this has attracted much researcher’s attention. We have tried to provide some of the research concerned with countering fraud, using different

methods and techniques in several types of e-payment as shown in Table 1. As per Prajal Save, et al. [8]. they have proposed a system which detect fraud in credit card transaction processing using a decision tree with combination of Luhn's algorithm and Hunt's algorithm In another research for credit card fraud detection Snehal Patil, et al. [13] they have proposed decision tree approach which reduces the sum of misclassification costs while selecting the splitting attribute at each nonterminal node is advanced and the act of this approach is compared with the well-known traditional classification models on a real world credit card data set. Rieke, et al. [14] applied a tool for predictive security analysis at runtime, which observes process behavior with respect to transactions within a money transfer service and tries to match it with expected behavior given by a process model. Tool analyze deviations from the given behavior specification for anomalies that indicate a possible misuse of the service related to money laundering activities. As per Y. Sahin, et al [17] they developed and applied classification models based on decision trees and support vector machines (SVM) on credit card fraud detection problem. They compared the performance of SVM and decision tree methods in credit card fraud detection with a real data set. Hao ZHOU, et al [4] introduce machine learning algorithms to perform fraud detection of bankcard enrolment. They introduce several traditional machine-learning algorithms and finally choose the improved gradient boosting decision tree (GBDT) algorithm software library for use in a real system. Shailesh S.Dhok, et al [18] modeled the sequence of operations in credit card transaction processing using a Hidden Markov Model (HMM) and show how it can be used for the detection of frauds. An HMM is initially trained with the normal behavior of a cardholder. If an incoming credit card transaction is not accepted by the trained HMM with sufficiently high probability, it is considered to be fraudulent. Hidden Markov Model helps to obtain a high fraud coverage combined with a low false alarm rate. Manisha, et al [7] they used Decision Tree technique; basically it provides a system which is supposed to classify a current transaction into fraud or non-fraud using split criteria. R.Dhanapal, et al [15] their paper presents a credit card fraud detection using decision tree algorithm they find out the fraudulent user through tracing fake mail and IP address. If the mail is fake, they trace all data about the owner of this IP address his location and other details. Sunil Mhamane, et al [16] modeled the sequence of operations in internet banking transactions processing using a Hidden Markov Model.

Model	Technique	Payment Fraud Area
A Novel Idea for Credit Card Fraud Detection using Decision Tree [8]	Decision Tree	Credit Card
Credit Card Fraud Detection Using Decision Tree Induction Algorithm [13]	Decision Tree	Credit Card
Fraud Detection in Mobile Payment Utilizing Process Behaviour Analysis [14]	Process Behaviour Analysis	Mobile Money Transfer
Detecting Credit Card Fraud by Decision Trees and Support Vector Machines [17]	Decision Tree	Credit Card
Fraud detection within bankcard enrolment on mobile device based payment using machine learning [4]	Machine learning	Mobile payments.
Credit Card Fraud Detection Using Hidden Markov Model [18]	Hidden Markov Model	Credit Card
Credit Card Fraud Detection Using Split Criteria in Classification [7]	Decision Tree	Credit Card
Credit Card Fraud Detection Using Decision Tree for Tracing Email and IP [15]	Decision Tree	Credit Card

Fraud Detection in Online Banking Using HMM [16]	Hidden Markov Model	Online Banking
--	---------------------	----------------

Table. 1 Fraud Detection Techniques

7. E-payment opportunities in the future

E-commerce is undergoing huge growth in terms of the volume of goods and services that are being traded on-line. According to MEF’s third annual global mobile money report 2015, e-commerce and mobile banking continue to grow with 69% of mobile users carrying out their banking activity via mobile devices (Perelmuter, 2015). The report conducted a study of 15,000 mobile users across 15 different countries of the world [9]. New opportunities have been created through mobile payment systems for traders and consumers, as well as new privacy and security threats. According to the mobile payment study, careful preparation is needed in order to make protection an integral part of online payment methods in the future. In order to ensure a prosperous future for the mobile payment market, cell phone manufacturers, telecommunications companies and the payment industry need to work together to create a network to ensure the most safe environment for e-payment transactions.

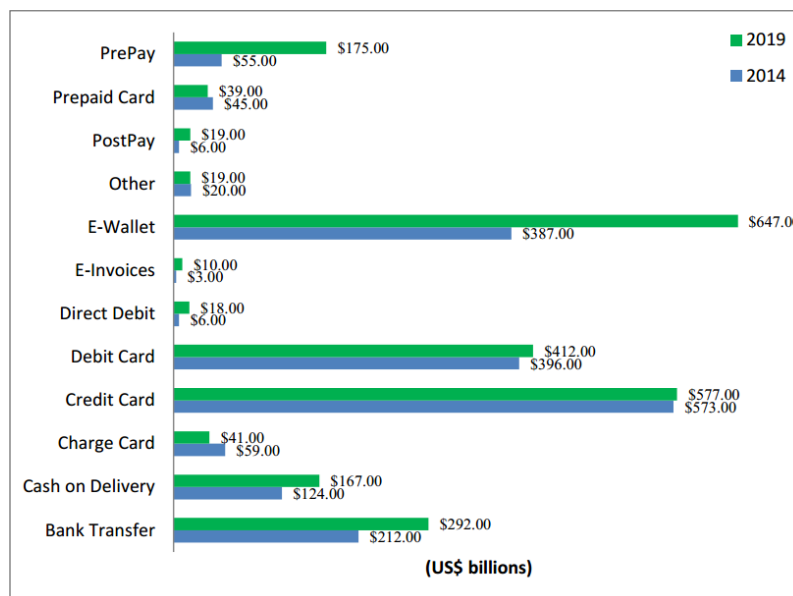


Figure. 9 Payment Methods Trends for Future [Source: Global payments report preview, World pay, November 2015]

8. Conclusion

Nowadays the field of e-payment is one of the most exciting with a bright future, but like every other field it faces many obstacles that need to be joined in efforts to find solutions and also help to expand the e-payments industry. In this paper we discussed the challenges, risks, benefits and future of e-payment in order to improve e-business field as improve customer experience for the whole process of e-payment. One of the most important threats facing e-payment is fraud, and we presented different research papers that implemented various strategies for detecting and preventing fraud in different forms of e-payments. We focus on fraud, which is the most important risk facing e-payment, and we have tried to demonstrate the new fraud detection and prevention models and techniques. Paper also introduced different types of e-payment and explained the cycle for each type. As concluded from this paper, the fraud detection techniques that we have explored have their advantages like enhance e-payment environment’s security,

reducing fraud attempts and increases confidence in e-payments but still having some drawbacks like complexity of some models, lack of accuracy and sometimes the slow execution of the e-payment transaction.

9. Future scope

In this paper, we have tried to present an integrated picture of e-payments. We have talked about their types and returns, challenges and risks they face, as well as the future of e-payments. This was in an attempt to give a clear and general picture to those interested in the field of e-payments. Through this research, many points emerged that need to be explored in the future. One of the most important points is fraud in e-payments and how to confront and limit those using modern technologies and science such as data mining techniques and the importance of applying these to the Egyptian payments market, which is witnessing an extraordinary development in this field, driven by the support of the Egyptian government and all its ministries.

References

1. Patgaonkar, Aditi. "A Study of Electronic Payment Systems with perspective of Customers Adoption in India." (2020).
2. Ravikumar T, Suresha. B, Sriram. M, and Rajesh. R. "Impact of Digital Payments on Economic Growth: Evidence from India." *International Journal of Innovative Technology and Exploring Engineering (IJITEE)* ISSN: 2278-3075, Volume-8 Issue-12. (2019)
3. Kavitha, K. S. K. M., and K. Sampath Kumar. "A Study on Digital Payments System with Perspective of Customer's Adoption." *Eurasian Journal of Analytical Chemistry* 13.SP (2018): 189-200.
4. Zhou, Hao, Hong-feng Chai, and Mao-lin Qiu. "Fraud detection within bankcard enrollment on mobile device based payment using machine learning." *Frontiers of Information Technology & Electronic Engineering* 19.12 (2018): 1537-1545.
5. Franciska, A. Martina, and S. Sahayaselvi. "An Overview On Digital Payments." (2017).
6. Khan, Burhan Ul Islam, et al. "A compendious study of online payment systems: Past developments, present impact, and future considerations." *International journal of advanced computer science and applications* 8.5 (2017): 256-271.
7. Manisha, Neena Madan. "Credit Card Fraud Detection Using Split Criteria in Classification." *IOSR Journal of Computer Engineering (IOSR-JCE)* e-ISSN: 2278-0661, p-ISSN: 2278-8727, Volume 19, Issue 2, Ver. I (Mar.-Apr. 2017), PP 39-43
8. Save, Prajal, et al. "A novel idea for credit card fraud detection using decision tree." *International Journal of Computer Applications* 161.13 (2017).
9. Bezovski, Zlatko. "The future of the mobile payment as electronic payment system." *European Journal of Business and Management* 8.8 (2016): 127-132.
10. Garg, C. R. "Importance of E-Commerce Payment System in Less Paper Work." vol 2 (2016): 47-59.
11. Yaakub, Nor Asiah, et al. "analysis of e-payment applications: a case study of one of the zakat institutions in malaysia." *Journal of Techno Social* 8.2 (2016).
12. Kabir, Mohammad Auwal, Siti Zabedah Saidin, and Aidi Ahmi. "Adoption of e-payment systems: a review of literature." *International Conference on E-Commerce*. (2015).
13. Gaikwad, Jyoti R., et al. "Credit Card Fraud Detection using Decision Tree Induction Algorithm." *International Journal of Innovative Technology and Exploring Engineering (IJITEE)* 4.6 (2014).

14. Rieke, Roland, et al. "Fraud detection in mobile payments utilizing process behavior analysis." 2013 International Conference on Availability, Reliability and Security. IEEE, (2013).
15. Dhanapal, R., and P. Gayathiri. "Credit Card Fraud Detection Using Decision Tree for Tracing Email and Ip." International Journal of Computer Science Issues (IJCSI) 9.5 (2012): 406.
16. Mhamane, Sunil, and L. M. R. J. Lobo. "Fraud detection in online banking using HMM." International Proceedings of Computer Science & Information Technology (2012): 200-204.
17. Şahin, Yusuf G., and Ekrem Duman. "Detecting credit card fraud by decision trees and support vector machines." (2011).
18. Srivastava, Abhinav, et al. "Credit card fraud detection using hidden Markov model." IEEE Transactions on dependable and secure computing 5.1 (2008): 37-48.