Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 7– No. 23, December 2018 – www.caeaccess.org

A Critical Analysis on the Evolution in the E-Payment System, Secuiry Risk, Threats and Vulnerability

Jerrin Yomas
Research Scholar
Visvesvaraya Technological University, Belagavi, Karnataka, India

Chitra Kiran N, Phd
Professor and Head, Department of ECE, Alliance College of Engineering and Design Alliance University, Bengaluru, Karnataka, India

ABSTRACT
At present, payment system through the internet has been trending at the furious pace. There are different ways and varieties of e-payment systems are existing to facilitate ease of transaction at the most active security level. However, parallelly the cyber-attacks strategies are growing at the advanced level as security protocols. In this research study, have analyzing the evolution of e-payment system and its terminology followed by different conventional e-payment mechanisms. Also demonstrates lack of security provisions and solution strategies. The main contribution of the present survey study is providing the landscape of digital e-payment system and its opportunities for future e-commerce systems. In the last, have briefly discussing and analyzing the fraudulent transaction rates which will become the benchmark for the development of secure e-payment system.

Keywords
Debit/Credit card, Electronic Payement System, E-Cash Transcation, Mobile-Payement, Security, Secure E-Transaction (SET), QR code.

1. INTRODUCTION
With the fast growth of the internet and information technology, most of the consumers, as well as a vendor, are depending upon electronic-commerce (i.e., E-commerce) system. It is a process of buying and selling the goods and services or financial transaction, over the internet [1]. For example, e-payment or online payment, which is also known as EDI (Electronic data interchange). In the current digital world, internet banking or e-banking system has become most rapidly adopting technology for multiple purposes especially for online shopping, money transaction, e-ticket booking, and many more applications. An e-payment or e-banking system provides a service to make a financial transaction for goods and services via an electronic system, without using any cash or check. The e-payment technology has to place a new era over the past decades owing to the popular online-based shopping and internet banking [2]. As rapid growth in the development of e-banking system can notice the increasing use of e-payment system has provided tremendous opportunities and services for the users. The services offered from the internet banking are becoming the prevalent medium of money transactions and can be taken as major requirements in current financial industry [3]. As of simplifying e-banking operations, these services offer any time access to banking services [4]. As per the research report of [5], <29 percentage of online consumers accessed the e-banking sites in the year 2012, which is a very low access rate [6].

In the e-banking system, the essential aspect is that establishing the important technical infrastructure, for example; E-payment system. Generally, E-payment system can be grouped into different categories; one is cash-based payment (i.e., E-cash, and pre-paid card) and second is account based payment system (i.e., credit card, debit card, and E-check). The E-payment process mainly depends upon time and location, and it happens with the help of the smart device that is named as M-payment (mobile payment) system. In this procedure, operators and network carriers have to communicate with banks or financial institutions, because, like example; cash-based payment system often managed over the accounts of citizens. In the state sector, there are multiple enterprises to offer E-payment for the citizens to protect the electronic payments is made by government organizations to pay for public services. With the tremendous growth in the information & communication technology (ICT), mobile services achieved broad coverage and extensive use, not only helping in the public sector but also in economic or business activities becoming essential service for improving business revenue. According to the report of ARCOTEL [7], mobile access surpasses 100%, with the coverage over 90% throughout the public region. In [8], Ecuador financial institution estimated that in the year 2014, less than 50% of the population was using e-banking, i.e. no alternative use of physical money payment.

The key factor of E-banking service is to understand the customer's satisfaction and requirements. To improve the E-payment system adoption rate, the factors which affect customer adoption must be better managed [6]. Despite the huge investment made on internet technology in the banking sector, the case study shows that few customers although following physical money transaction, are reluctant to utilize the system. This shows the research required to figure out the influencing factors for the adoption of e-payment system [9]. Multiple electronic banking methods have been explored to define the factors influencing the customer's adoption of E-payment. The major influencing factors are; flexibility during payment system, payment operations, data management, privacy and system security [10]. Always, customers of E-payment system fears about using the internet services for online money transactions. The major problem of trust occurs when high risk is involved. Therefore, security and trust can be considered as a primary factor influencing customer contentment in the use of E-payment.

The establishment of M-payment system began more than ten years ago. However, in real scenario adoption of M-payment is quite different. Till now, 70% of Indian customers are being aware of M-payment system, don't adopting the technologies. The primary reason for this less adoption rate is because of high fear of privacy and security incorporations provided by different services [11]. With the adoption of mobile phones and related services, various applications (M-Pesa) has been launched in our country which can be utilized for financial transactions, E-recharge, E-bill payments, and cash withdraw from ATM.

However, information community believes that M-commerce has to rise and to move in the area of M-payment system with existing personal computer and smart device services available [12].

Secure mobile payment methods are typically needed in mobile access channels; it is vital to apply them when using mobile payment applications, which begin as a result of the increase in e-commerce. Currently, there are some payment methods that most of them can be used when conducting transactions but, they differ in terms of functionality, usability, costs or security. Some of the problems in this field related to security and trust mechanisms including comparisons of various technology alternatives, mobile payment transaction protocols including roaming between mobile networks, comparisons of the benefits and limitations of main mobile payment service architectures, and descriptions of near field communication (NFC) and short-range wireless technologies in general. Moreover, authentication, as well as authorization, is not that robust with the existing cryptographic measures that are quite easier to be compromised. Hence, this study highlights a security protocol that intends to address a majority of the security issues associated with M-payment exclusively in the wireless environment.

The primary reason for the present study is to investigate the consequences of perceived security and trust in E-payment system adoption. Another reason is to investigate the essential factors affecting E-payment system security. Additionally, the study shows the statistical graph on annual online fraud rate.

Problem Identification: Generally, the biggest hazard in network security is the incompetence of network users or administrators. The existing security protocols are not efficient to full fill the secure provision for future networks forms the highly determined hackers; still, in various wireless networks, these performance metrics are not implemented. However, the symmetric approach has some disadvantages as compared with the asymmetric approach. One of the advantages of the asymmetric approach upon symmetric is the capability to find the message originator from its digital signature, while this functionality could not be achieved from the symmetric approach. It is impossible to identify the symmetric ciphertext message originator because the third party who has shared key can generate the message.

The structure of the survey study can be organized as follows section-II illustrates the terminology of the e-Payment system, followed by different e-Payment mechanisms in section-3. The literature works on the e-Payment system is presented in section-4. Section -5 describes different security strategies in the state of art of the e-Payment system. Section-6 illustrates about the landscape of digital e-payment system and its opportunities. In the last section-7, the study provides a statistical report on global fraudulent transaction rate. Section-8 deals with the conclusion of the study.

2. UNDERSTANDING E-PAYMENT TERMINOLOGY

In 1960s electronic payment system has been discovered and has been rapidly expanding and growing in complexity. After the discovery of the traditional payment system, e-Money transaction-based payment method came into existence. This was the first electronic-based fund transfer system, which doesn't depend upon centralized processor [13]. Online fund transaction is a financial application which sends e-Checks or credit card numbers through secure private communication channels between merchants and banks. This process became a new direction toward the development of a digital currency transaction system. However digital currency has a significant impact on money transaction system with increasing implications far beyond more transaction efficiency.

Therefore, in this section have briefly discussed the terminology of E-payment system is pictorially resenting in the figure-1. Multiple processing tasks are undertaken to perform E-payment process. Such provisions are; gateway service, payment processor, payment provider, payment system and merchant account.

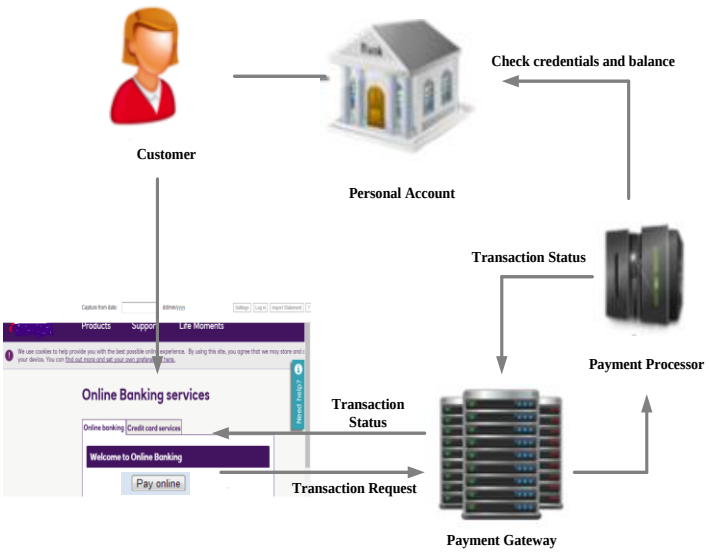

Fig.1 Terminology of E-Payment System

Though all provision has distinct qualities and responsibilities to provide the service and perform like a payment middleware among website and customer, and among both user and user bank accounts, each provision assists for completion of E-transaction and eases the online payment processing.

The first service is the payment gateway, which receives the payment request from the website and connects it to the payment processor. Then payment processor verifies the customers credential details and confirms if the user has enough balance into their financial account to continue the payment process. If the user account contains sufficient balance, the E-transaction is authorized, and the amount is transferred from his account. The status of the fund transaction is reverted to the gateway which again forwards an account status message to the website administrator.

The payment service provider is a company the processes the payment gateway or services. While the payment system provides several types of payment services including with multiple features- it is referred into as a payment system. Example; PayPal- payment provider which offers multiple payment services such as PayPal express and PayPal pay flow pro [14]. The last essential factor is a merchant account. Once the E-transaction is completely done, the amounts are transferred from the customers account to merchant account; a specific financial account is utilized to hold the balance received from debit and credit card transactions. To accept the E-payment, usually, customers require setup the merchant account with their payment service provider. Money accumulating in a merchant account is transmitted to the customer's bank account on a regular basis.

The most popular electronic credit card enablers are i) PayPal, ii) Google checkout and iii) authorize.Net. All these enable established the finance relationship with business organizations to accept the E-payment system for their dealer clients. The (www.paypal.com) has quickly arisen dominant in E-transaction processing [15]. Initially, PayPal established as peer to the peer fund transaction system for eBay. Whereas "Google Checkout" provide an E-payment service only for credit card transactions. Another payment gateway-Authorize.Net manages the e-payment transactions for credit card holders also provide service between the dealers and finance processing networks [16].

The e-commerce websites exploit an e-payment method to make ease transaction and more convenient to pay for their customers. It includes multiple benefits given as;

- Concerning time: more effective and more convenient for transactions. Since, it's just one click and makes a transaction in a minute, without wasting of consumer's time.
- It lowers the transaction cost.
- Nowadays, it is very easy to add payments to the accounts; even nontechnical person also can implement the transaction within a minute and start for online transaction.
- Reduces the technology cost: day by day, the network technology is reducing down for example; at present computers are very cheap, and the internet is freely available almost entire the world minimum operational & processing cost: owing to the minimum technology cost, the processing cost of e-commerce activities becoming very cheap. That's the reason from the e-payment systems customers can save both paperwork and time.

3. MOST POPULAR E-PAYMENT METHODS

With the growing advancement in the e-commerce transaction system, different e-Payment transaction methods have discovered in the last decades. There is a multiple of e-payment systems are already exists. They can be broadly classified into four types on the basis of what data is being forward online [17]. i.e., i) online credit card payment method, ii) e-Check system, iii) e-fund system and iv) smart/digital card-based e-payment system.

Fig.2 Most popular e-Payment methods

According to the current statistics, debit/credit cards have become the most adaptable technology in this digital world. The payment sources say that more than 83% of e-transaction is made by credit/debit cards [18]. Selection of right payment methods helps the online shoppers credible as well as accessible to the online retailer.

The credit/debit card payment system is the most widely adopted technology particularly in the retailer market [19]. This kind of e-payment system has multiple advantages; where traditional payment methods never have unique features. Most important features are; integrity, privacy, high transaction efficiency, good mobility, less fraud risk and many more. Additionally, to avoid complexities associated with e-cash, e-cheques, customers and retailers are also debit/credit card adopting e-card based payment system.

This method is perfectly suitable for individuals who have used digital cards issued from financial institutions. One more thing, debit cards are linked with customer's accounts. But it has raised security related problems. This means that e-card payment seeks to tackle multiple drawbacks for online retailers; for example; lack of authentication, credit/debit card frauds. Also, it seeks to address the online customer's fears exploiting credit card, i.e. having to disclose credit information on the number of sites and continuously trying to communicate with secret information using the internet.

The online credit/debit card payment system is a simple process. If the customer wants to bay or shop anything, they need to send their card information to the service providers, and card organization handles the entire payment process.

The similar kind of e-payment transaction method is the digital wallets: which works in the same fashion as normal wallets utilized in mortar stores. Like as debit/credit cards, the digital wallet is connected with the person's checking account. In multiple cases, the most popular browsers like Firefox and Google Chrome will ask online retailers to preserve the information which includes billing address or shipping address. From this technology, customers can proceed with their payments very quickly by clicking their mouse instead of typing the detail information again and again during the transaction process [18].

The one more popular e-payment method is online shopping through the mobile app which is works like as digital wallets. In this payment, process information is stored and distributed via mobile phone or smartphone. The advantage of this method is to offer online shopping much simple and easier which resulted in high popularity by adopting. The electronic fund's transfer method provides a special kind of payment method by which an exchange of a certain amount from one bank account to another via the electronic-based system. The most popular and common e-fund transaction methods are e-bill payment, insurance debts, utilities, and mortgages on the internet.

Another method is "payment service provider method" which is widely adopted over the world [18]. In this provider define third-party network which offers online retailers to connect with various types of currencies into the single source. By this method, retailers can secure themselves against frauds. In this way, they can transfer the money to their payment service provider's account, and online retailers can shop without any fear. The most popular online payment service providers are; VISA, PayPal, Payoneer, Skrill, and Payza, etc.

However, smart card-based e-Payment system receiving huge popularity in terms of online payment or e-cash exchange. Initially, smart cards are equipped with memory chips and embedded microprocessors where it serves as a storage device to hold the information with inbuilt transaction processing capacity. As security concerns, smart cards contain a unique encrypted key which is matched with a secret key stored on the cardholder processor. Due to considerable flexibility, these cards are widely utilizing in multiple applications, e.g., highway toll payment, prepaid mobile recharge, etc. with the recent advancement in the m-Commerce, these smart payment systems are increasingly utilizing in our day to day purpose. As already described, e-Payment systems have the facility to transfer funds electronically for purchasing goods and services which is an integral part of e-commerce. The primary reason for the extensive growth in the development of e-Payment transaction is the rapid development and adoption of different e-payment methods. In developed countries, debit/credit cards already utilized even before the discovery of the internet. At the beginning have classified various e-Payment systems into 4 categories and comparing those methods based on their requirements and features shown in table-1.

Table.1 Comparative analysis on different e-Payment systems based on their feature

Features	**E-card payment**	**E-cash method**	**E-cheque**	**Smart/digital card**
Payment time	Post paid	Pre-paid	Postpaid	Pre-paid
Online/offline transaction	Online payment	Online payment	Offline payment allowed	Offline payment allowed
Transaction detail requirements	The bank and retailer verifies the status of the credit card	Free transaction. No need to mention the name of the parties involved	e-payment indication should be endorsed	Both parties of smart card holder make the transaction
Bank involvement	Card account makes the transactions	No involvement	Bank account makes the transactions	Digital card account makes the transactions
Customers involvement	Authorized user	Anyone	Anyone with bank account holder	Anyone or credit card holder
Source to which transaction is made out	Bank	stockpile	stockpile	stockpile
Customers transaction risks	Risk are created by distributing bank, customers need to bear part of the risk	Customer is at risk where money get lose or misused.	Mostly Customers bears the risks, but they can stop transaction at any time	Customer is at risk of digital card getting stolen or misused.
Popularity rate	Card organizations validate for certification and allow for purchasing. Hence it can be utilized over the world and this is very common and popular e-payment method	Not able to meet internet banking standards in the international level	It is not much popular and can't meet international banking standards	The card organizations validate for authentication then allow for purchasing, it can be utilized Worldwide and becoming more popular.
Anonymity	Totally, or partially anonymous	Fully anonymous	No	Fully anonymous

Storage security	Secures regular e-card account information	Need to secure data repository and manage records from the serial number of e-cash used	Secures regular account information	Secures regular account information
Payment information face value	Can be sign and freely issued in compliance with limit	Often set and changes not possible	Can be sign and freely issued in compliance with limit	Free deduction with limit
Real or virtual world	Partially utilized in real world	Virtually utilize	Virtually less, but can check account in the real world	Both real and virtual world
Transaction limit	Depends upon credit card limit	Based on pre-paid amount	No limit	How much fund is saved
Mobility	Yes	No	No	Yes

4. RELATED WORK

This section discusses different types of existing e-Payment transaction methods which are introduced by different researchers by their efforts — this survey study analyzing and evaluating those methods based on their performance metrics and providing brief description upon the study.

From the past three decades to still, there is continued development in information and communication technologies; financial organizations follow an electronic mediate multi-channel policy for fund transactions [20]. The first ATM is launched in the year of 1970, followed by telephonic banking service in the 1980s, online banking services in the 1990s, and m-banking from the past decade [21]. However, the adoption rate of e-payment system is less than its development rate [22]. The major challenges are; data security, privacy, and safety, the information leakage by retailers and 3rd parties, remain as stronger in e-payment. Such problems have a negative impact directly on adopting e-banking services and trust of users [23].

Cao and Zhu [24], have presented a privacy-preserving secure e-cash transaction scheme for ride-hailing services. Additionally, the author introduced an authenticated hash chaining mechanism to keep e-payment divisible and reusable, which extends the flexibility of transaction systems. The mobile payment mechanism is presented in [25] applying a one-time password scheme. Whereas in [26] the author proposed a novel framework for m-payment systems which secures the mobile wallet using a digital signature mechanism and pseudo-identity methods. Both studies [25], [26] reveals the relationship among the user's real identity and user's pseudonym. Here, if the user wants, he/she can track all transactions.

Zahra et al. [27], presented an investigational study on factors affecting trust during online payments over Iran country. They collected determinant influencing factors of trust and developed a security model based on transaction information, accessibility, and usability of the payment system. Finally, the authors compared the results with similar studies. The similar approach is carried by Karmi et al. [28], where author investigated significant factors, i.e. social websites, marketing strategies, trust, usability, relationships with customers, accessibility, etc. which influence the e-market system.

Nowadays, several e-payment systems are available which performed on smart devices and provided better communication with minimum cost. But user's anonymity is quite challenging because current payment systems provide only transaction privacy, also high-security feature is not up to the mark.

Therefore, as user's anonymity viewpoint Breaken [29] introduced an improved version of the e-Payment system for blind & visually impaired users. This mechanism is also applicable for the development of the payment system on retail outlet for customer exploiting mobile phone as a proxy. In [30] & [31] authors solved the user's anonymity problems and showed security weakness points. With the rapid adoption of e-payment method through mobile or smartphones, the user's daily life and their work become easier as well as convenient. The e-payment via mobile phones is ubiquitous in rising commercial fields [32]. However, a quick response code (i.e., QR code) is the new communication technology which facilitates data storage, transmission, and recognition, and the mobile device can decrypt information from any place [33]. QR code technology is increasingly utilizing in much security sensitive application areas [34] for example as payment systems.

In [35] Suryotrisongko et al. proposed a novel of mobile payment system for the cooperative enterprise under developing countries. This study improves the prior QR payment strategy by reducing the network connectivity problem because some developing countries are facing difficulties in internet connection. Additionally, introduced two major factors, i.e. authentication and QR encrypted information to enhance the security. Hence, the proposed scheme facilitates more convenience and strong security to transfer money using the mobile phone easily. Therefore, authors conclude that this mechanism applies to current developing countries.

Dey et al. [36], introduced an alternative approach of QR code which enables the user interface and exploited to embed the information into a graphic format with the help of mobile apps on smartphones. In another research study, Lu et al. [37] utilized a similar mechanism of QR code due to its profitable features, especially for the mobile payment system. Also introduced a visual cryptographic method which demonstrated the feasibility and security factor for m-payment authentication.

In [38] ChitraK et al. have presented a digital card module using a biometric system which is named as a swing-pay method. The objective of the proposed method is to utilize a user's fingerprints for authentication. This method provides an efficient and secure payment system with the help of GSM, power unit, Cortex-M3, Bluetooth device, etc. From the experimental analysis can conclude that from this method, the user can get the transaction received a message from the server for the payer.

Among several e-payment applications, transit payment services are the most commonly utilizing application for mobile payment

systems. The prior transit service application isn't able to handle the passengers secrete information from the organizations (i.e., transit agencies, banking institutes, mobile carriers, and smart card providers, etc.). Therefore, in the study of [39], Kang and Nyang proposed a simple approach of the privacy-preserving m-payment system to preserve the passenger's mass transit information. Furthermore, this approach facilitates the proactive blocking approach for mishandling passengers, transfer discount and postpaid facility.

There are multiple e-payment schemes have been proposed where primary motive is to enhance the security level while e-transaction process. But some traditional methods do not offer non-repudiation requirement from the client side. Therefore, an attacker or malicious node can easily deny the e-transaction and retailer may not get the money. To overcome such type of challenge, Yang and Lin [40] investigated an anonymity m-payment mechanism for cloud computing. The proposed method offers non-repudiation requirement from the client side with minimum computational cost. From the comparative analysis, authors conclude that the proposed e-payment mechanism is fairer, secure and highly efficient and suitable for real-time cloud computing.

In the research study of Kang and Xu [41] introduced a quite similar approach to anonymity secure e-cash payment system to ensure the customer's privacy. In this research study authors point out Chen et al. work is subject to some disadvantages. The contribution was to present offline e-cash mechanism with mystery revocation. Additionally, the proposed study ensures the feature of avoiding retailer frauds. The similar research study on offline e-cash payment system is proposed by Fan et al. [42]. Also, authors designed an electronic cash renewal protocol, where customers can exchange their expired and unused currencies for another one.

In [43] and [44] Chitra K and N. Kumar presented a reliable and secure micropayment mechanism. In paper [43] author designed a robust and secured micropayment system architecture for the wireless network. For the security process, the author utilized the hash chaining approach, and simple public key cryptosystem which facilitates secure routing during m-transaction also offer an efficient method for digital coin system. Whereas in the paper [44], the authors presented an extended version of the previous study that addressed the security implications of a micropayment system using a mobile agent. As compared to the previous study, this paper has challenged to offer reliable and secure lightweight approach for offline payment method in m-commerce system.

5. SECURITY IN E-PAYMENT SYSTEM

The lack of trust, privacy, and security have always been reported in the business analysis as one of the significant factors hampering the progress of e-commerce system. With the rapid adoption of e-payment system increasing the opportunity for the attack on the internet, privacy and security are becoming an essential factor for every e-payment system. In this section, have mainly focusing study towards security protocols for securing the e-payment systems in this section mainly discussing security requirements for futuristic e-payment systems. With the increasing growth of digital technologies, security provisions are also rapidly increasing with the aim of robust, low cost and efficient security protocol for current as well as upcoming e-payment systems. As compared with traditional transaction methods with trending e-transaction methods for example e-card or digital wallet, the retailer provision is the digital signature of the cardholder and sometimes they need a photo as an identity factor for credit card holder which will help for the validation of cardholder identity. In the virtual process, the information required are the card number, verification code and billing information to validate the cardholder identity.The most prominent challenges that retailers have to deal with are; web fraud, product return, claims on non-delivery, and many more. In the existing e-payment system, the fraud rate is very high as compared to traditional payment systems analyzed in [45]. Usually, the transaction information can be stolen or changed in multiple ways by cyber attackers [46]. Once this is done, the stolen information can be utilized for purchasing goods and other things from online and deliver to the fake address. During this, if frauds are detected, the attackers would quickly disappear from the spot. This losing transactional information on internet recurrently prevents online customers from doing online shopping. Most of the people fear that the online users are mostly in a critical phase of being cheated, however, the reality is that always retailers will be on target of cybercriminals. Hence, an efficient security model is provided to address these security challenges which could become immunity factor for the online payment users as well as for retails. The most popular and significant security protocols are discussing in this section, which is considered as benchmarks for developing secure e-payment system for the future application.

The SSL (secure socket layer) and SET (secure electronic transaction) are the two-standard e-payment security protocols that balance the integrity of the online transaction process [47]. Both SET and SSL protocols are mainly utilized to secure data where information is encrypted and digitized before the data transmission over the internet. The SSL protocol is developed by Netscape, and it is utilized for the development of several web browsers like; Microsoft Internet Explorer, Netscape Communicator and so on whereas SET is designed by Master card International and Visa International with the aim to secure and manage the entire online transaction process for both retailers and customers.Therefore, in the current scenario, there is a huge requirement of efficient, reliable and trustworthy security protocol which will provide a safe and secure model for current as well as futuristic e-payment system.

6. DIGITAL E-PAYMENT LANDSCAPE AND OPPORTUNITIES

The global e-Payment landscape is rapidly changing. The digital payment system is unsettling relationships. The financial institutions and credit card service providers are now afraid of advanced digital service providers, whose mobile transaction or m-payment solutions are becoming much cheaper, transparent and customer oriented. That's the reason at present most of the customers are highly adopting m-payment systems. By integrating the m-payment systems, retailers lay themselves in the place where they can exploit the transaction information to notify and guide their customers. This can benefit for connecting relevant digital services like as ordering and purchasing products, analyzing offers, product comparisons, etc. Therefore, the new generation m-payment applications are utilizing, and those are roughly classifying into two categories, i.e. proximity payment and remote payment [48].

The proximity payment method needs a mobile device to make links with the payment terminal, i.e. NFC (near field communication device) in instant environs. The majority of mobile phones are integrated with the NFC device. Whereas, remote payment system performs independently and perform payment process by the app which facilitate the customers to make online shopping. The most popular m-payment providers are; PayPal and pay by text. From this method, the user can make

the payment by entering a secret code into an online environment and transfer the amount automatically from the bank account.

As security benefit, large-scale companies like Google, Apple, and Samsung are adopting biometric-based secure m-payment applications. For example; Microsoft uses the "Windows Hello" camera to scan face or iris for identity verification. Another biometric-based m-payment application is "Qualcomm" which uses the ultrasound to scan the user's fingerprints and able to recognize the DNA through finger scanning [49].

Till now, most of the m-payment applications are focusing on providing peer to peer transactions. With the provisions in customer's behavior, the primary research on enabling m-payments at the point of the scale. Smartphones have permissible advance technologies to enlarge into offline services also. Whereas card-based payment system moving into downstream from large space to small retailers, the present trend is wishing to adopt a new and secure payment system because of fraud and time consumption. Additionally, the mobile phones can preserve the information securely and allow exchanging the information as well as payments data.

7. FRAUD RATE STATISTING ON E-PAYMENT

According to the comprehensive ACI reports [50], the fraud rate attempts based on population rage in 2015 reached up to 1.5% as compared to 1.4 in 2014. Also analyzed fraud rate in the year 2014 & 2015 at festive shopping seasons. In both years, the fraud attempts the highest rate by millions of transactions from retailers.

Smart devices or mobile phones are becoming more popular in the field of online shopping. However, the attackers know that mobile devices are more vulnerable as compared to PC's or laptops, as commercial companies have yet to utilize the same security level as they are using over the internet.

According to "Anti-fraud command center," in 2015 42% of customer e-payment transactions were attempted from mobile phones. In the same year, the transaction fraud rate via mobile phones increased to 142% as compared to the previous year, however internet fraud rate increased by only 3% during the same year.

According to the RSA reports [51]; nowadays most of the retailers are influencing from e-payment frauds, with 13% of transaction fraudulent, were computers or electronics, followed by fund transfer at 16% and airlines and travel services at 46%. The following pi-chart represents the percentage of fraudulent transactions for top retailers (figure-2).

From the case study also found that the total rate of fraud transitions is higher than of total legitimate transaction. For example; in airline tickets, the normal legitimate ticket booking is 606 dollars, while the normal fraudulent ticket booking is 1,930 dollars, i.e. three times higher than normal value. The statistical report of the average value of Fraud and Transaction is shown in figure-3.

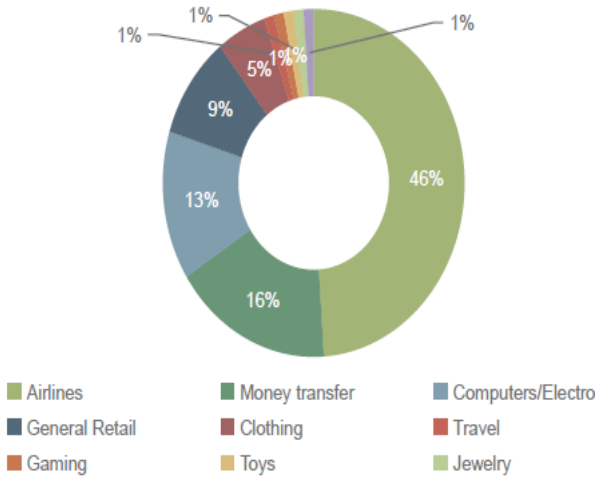

Fig.3 Transactions Fraud rate with respect to top retailers.

Based on attack volume, the world-famous countries targeted by attackers in 2014 (e.g., US, UK, and China). These countries influence by total 75% of attack volume. In UK and US, most of the retailers have had the large experience of dealing with fraudulent issues, and hence the topmost countries are majorly concentrating on solving the fraudulent online problems.

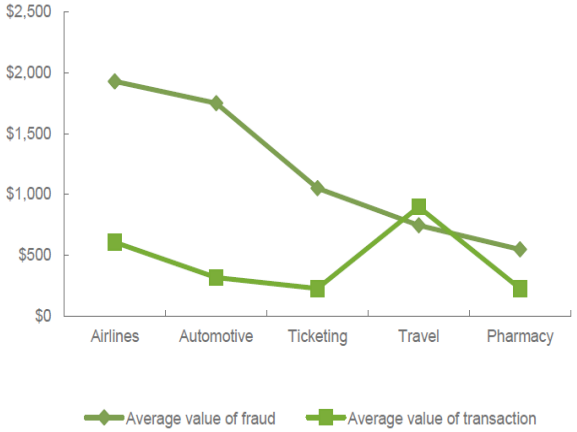

Fig.4 Average rate of fraudulent transactions

8. CONCLUSION

The motive of the present study is to research the mobile payment system and to thoroughly understand the methods and trending techniques that could be beneficial for both parties (i.e., retailers as well as customers) concerning e-payment security and usability. Initially, the study covers the terminology of e-payment system followed by different payment methods (i.e., online credit card payment method, e-Check, e-fund, and smart/digital card payment systems). From the literature surveys, It evaluated the performance of traditional e-payment systems and most trending attack or fraudulent strategies against them.

This comprehensive research study illustrates the status report of e-payment transactions and mobile payment systems. From the analysis of different payment systems can conclude that all types of e-payment systems have some flows and drawbacks concerning privacy, security, anonymity and their performance. The purpose of this survey study is to understand the e-payment security mechanism thoroughly and finally conclude that; it is provision to enhance the security level of current e-payment

systems, concerning all fundamental functionalities to achieve reliable, secure and trustworthy payment system.

9. REFERENCES

[1] Heindl, Dr Eduard. "Online Payment Process." 2008

[2] Lerner, Thomas. Mobile payment. Springer, 2013.

[3] Haque A, Ismail AZH, Daraz AH (2009) Issues of e-banking transaction: an empirical investigation on malaysian customers perception. J Appl Sci 9(10):1870–1879

[4] Flavia´n C, Guinalı´u M (2006) Consumer trust, perceived security and privacy policy: three basic elements of loyalty to a web site. Ind Manag Data Syst 106(5):601–620

[5] comScore Inc. (2012) 1 in 4 Internet Users Access Banking Sites Globally, in: comScore Data Mine, comScore, Inc. https://www.comscore.com/Insights/Data-Mine/1-in-4-Internet-Users-Access-Banking-Sites-Globally

[6] Montazemi AR, Qahri-Saremi H (2015) Factors affecting adoption of online banking: a meta-analytic structural equation modeling study. Inf Manag 52(2):210–226

[7] ARCOTEL. (2015, September 29) Estad´ısticas 2015. [Online]. Available: http://www.arcotel.gob.ec/estadisticas/estadisticas/

[8] Superintendencia de Bancos del Ecuador. (2015, September 29) Compoatamiento del sistema financiero ecuatoriano. [Online]. Available: http://www.sbs.gob.ec/medios/PORTALDOCS/downloads/articulos financieros/Estudios%20Tecnicos/2014/AT7 2014.pdf

[9] Wang Y, Lin H, Tang T (2003) Determinants of user acceptance of internet banking: an empirical study. Int J Serv Ind Manag 14(5):501–19.

[10] Harris H, Guru BK, Avvari MV (2011) Evidence of firms' perceptions toward electronic payment systems (EPS) in Malaysia. Int J Bus Inf 6(2):226–245

[11] https://www.ey.com/Publication/vwLUAssets/EY-the-case-for-mobile-payments-in-india/$FILE/EY-the-case-for-mobile-payments-in-india.PDF

[12] L. Fuchs, G. Pernul, R. Sandhu, "Roles in information security e A survey and classification of the research area", ScienceDirect, Elsevier, 2011

[13] Barnes SJ, Corbitt B (2003) Mobile banking: concept and potential. Int J Mob Commun. 1(3):273–288

[14] "PayPal", https://www.paypal.com/us/cgi-bin/webscr?cmd=_payflow-gatewayoverview- outside (accessed June 12, 2008)

[15] "PayPal", http://checkout.google.com/support/sell/bin/topic.py?topic=8664 (accessed June 13, 2008)

[16] "What we Are", http://www.authorize.net/company/whatwedo/ (accessed June 15, 2008).

[17] "Electronic Payment and Security Systems", http://shodhganga.inflibnet.ac.in/bitstream/10603/113273/14/14_chapter%203.pdf, (accessed June 13, 2008)

[18] "Purpose", https://purposefultechie.com/, (accessed June 13, 2008)

[19] Laudon, C. Kenneth and Traver, Carol (2002), E-Commerce, New Delhi: Pearson Education.

[20] Black NJ, Lockett A, Ennew C, Winklhofer H, McKechnie S (2002) Modelling consumer choice of distribution channels: an illustration from financial services. Int J Bank Mark 20(4):161–173

[21] Barnes SJ, Corbitt B (2003) Mobile banking: concept and potential. Int J Mob Commun. 1(3):273–288 Bentler PM (1989) EQS, structural equations, program manual, program version 30. BMDP Statistical Software, Los Angeles

[22] Hoehle H, Scornavacca E, Huff S (2012) Three decades of research on consumer adoption and utilization of electronic banking channels: a literature analysis. Decis Support Syst 54(1):122–132

[23] Eastlick MA, Lotz SL, Warrington P (2006) An integrated model of privacy concerns, trust and commitment. J Bus Res 59(8):870–880

[24] Cao, Chenglong, and Xiaoling Zhu. "Practical Secure Transaction for Privacy-Preserving Ride-Hailing Services." Security and Communication Networks 2018 (2018).

[25] S. Abughazalah, K. Markantonakis, and K. Mayes, "Secure mobile payment on NFC-enabled mobile phones formally analysed using CasperFDR," in Proceedings of the 13th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom '14), pp. 422–431, IEEE, Beijing, China, September 2014.

[26] Z. Qin, J. Sun, A. Wahaballa, W. Zheng, H. Xiong, and Z. Qin, "Asecure and privacy-preservingmobilewalletwith outsourced verification in cloud computing," Computer Standards & Interfaces, vol. 54, pp. 55–60, 2017.

[27] Barkhordari, Maryam, Zahra Nourollah, Hoda Mashayekhi, Yoosof Mashayekhi, and Mohammad S. Ahangar. "Factors influencing adoption of e-payment systems: an empirical study on Iranian customers." Information Systems and e-Business Management 15, no. 1 (2017): 89-116.

[28] Karimi Anche F, Hozouri S, Mehdizadeh A (2014) An exploration investigation on important factors influencing e-marketing: Evidence from banking industry. Uncertain Supply Chain Manag 2(1):49–54

[29] Braeken, An. "An Improved E-Payment System and Its Extension to a Payment System for Visually Impaired and Blind People with User Anonymity." Wireless Personal Communications 96, no. 1 (2017): 563-581.

[30] Yang, J.-H., Chang, Y.-F., & Chen, Y.-H. (2013). An efficient authenticated encryption scheme based on ECC and its application for electronic payment. Information Technology and Control, 42(4), 315–324.

[31] Chaudhry, S. A., Farash, M. S., Naqvi, H., & Sher, M. (2015). A secure and efficient authenticated encryption for electronic payment systems using elliptic curve cryptography. Electronic Commerce Research, 16(1), 113–139.

[32] D. A. Ortiz-Yepes, "Areviewof technical approaches to realizing near-field communicationmobile payments," IEEE Security and Privacy, vol. 14, no. 4, pp. 54–62, 2016.

[33] P. Subpratatsavee and P. Kuacharoen, "Internet banking transaction authentication using mobile one-time password and QR code," Advanced Science Letters, vol. 21, no. 10, pp. 3189–3193, 2015.

[34] B. Zhang, K. Ren, G. Xing, X. Fu, andC.Wang, "SBVLC: secure barcode-based visible light communication for smartphones," in Proceedings of the 33rd IEEE Conference on Computer Communications (IEEE INFOCOM '14), pp. 2661–2669, Toronto, Canada, May 2014.

[35] H. Suryotrisongko, Sugiharsono, and B. Setiawan, "A novel mobile payment scheme based on secure quick response payment with minimal infrastructure for cooperative enterprise in developing countries," Procedia—Social and Behavioral Sciences, vol. 65, pp. 906–912, 2012.

[36] P. De and J. Eliasson, "An assessment of QR code as a user interface enabler for mobile payment apps on smartphones," in Proceedings of the 7th International Conference on HCI (IndiaHCI '15), pp. 81–84, Guwahati, India, December 2015.

[37] Terán, Luis, Celine Horst, B. Fausto Valencia, and Priscila Rodriguez. "Public electronic payments: A case study of the electronic cash system in Ecuador." In eDemocracy & eGovernment (ICEDEG), 2016 Third International Conference on, pp. 65-70. IEEE, 2016.

[38] ChitraKiran, N., Bhuvan Teja, Suchira Suresh, B. Krishna, S. M. Akarsh, and Jerrin Yomas. "A biometric based payment system by using payee and payer module." In Recent Trends in Electronics, Information & Communication Technology (RTEICT), 2017 2nd IEEE International Conference on, pp. 2252-2256. IEEE, 2017.

[39] J. Kang; D. Nyang, "A Privacy-Preserving Mobile Payment System for Mass Transit," in IEEE Transactions on Intelligent Transportation Systems , Vol.PP, No.99, pp.1-14, 2017

[40] J.-H. Yang and P.-Y. Lin, "A mobile payment mechanism with anonymity for cloud computing," J. Syst. Softw., vol. 116, pp. 69–74, Jun. 2016.

[41] Kang, Baoyuan, and Danhui Xu. "Secure electronic cash scheme with anonymity revocation." Mobile Information Systems 2016 (2016).

[42] Fan, Chun-I., Wei-Zhe Sun, and Hoi-Tung Hau. "Date attachable offline electronic cash scheme." The Scientific World Journal 2014 (2014).

[43] Kiran, Chitra N., and G. Narendra Kumar. "Implication of secure micropayment system using process oriented structural design by hash chaining in mobile network." International Journal of Computer Science Issues (IJCSI) 9, no. 1 (2012): 329.

[44] Kiran, N. Chitra, and G. Narendra Kumar. "Reliable OSPM schema for secure transaction using mobile agent in micropayment system." In Computing, Communications and Networking Technologies (ICCCNT), 2013 Fourth International Conference on, pp. 1-6. IEEE, 2013.

[45] http://shodhganga.inflibnet.ac.in/bitstream/10603/113273/14/14_chapter%203.pdf

[46] Various studies (Norton, 2003; Computer Crime Report, India, 2002) indicate that most of the time theses people are from inside the organization or the people who deals with the electronic payment system in any organization.

[47] Solat, Siamak. "Security of electronic payment systems: A comprehensive survey." arXiv preprint arXiv:1701.04556 (2017).

[48] Raina, Vibha Kaw. "Overview of mobile payment: technologies and security." In Electronic payment systems for competitive advantage in e-commerce, pp. 186-222. IGI Global, 2014.

[49] "The Mobile Payments Landscape and its Opportunities", https://www.accenture.com/t20160708T043705__w__/us-en/_acnmedia/PDF-25/Accenture-Acquires-Mobgen-Expand-European-Mobile-Payment-UK.pdf, (accessed June 15, 2008).

[50] "Security", http://www.securitymagazine.com/articles/86878-holiday-season-e-commerce-fraud-rates-rise, (accessed June 15, 2008).

[51] "Experian",https://www.experian.com/assets/decision-analytics/white-apers/juniper-research-online-payment-fraud-wp-2016.pdf,(accessed June 15, 2008).