OPPORTUNITIES AND CHALLENGES OF ELECTRONIC PAYMENT SYSTEM

JITHINKRISHNA I V
RISHEEN E A
TREESA SOYET JOY

MR. DIJESH P
Department Of Computer Application
Vidya Academy of Science & Technology, Thrissur-680501

Abstract: In this paper an overview of electronic payment methods and systems is given. E-commerce provides the capability of buying and selling products, information and services on the internet and other online environments. In an e-commerce environment, payment take the form of money exchange in an electronic form, and are therefore called electronic payment. Today India is at a stage of demonetization so; in the present scenario this study is inevitable to makes electronic payments at any time through the internet directly to manage the e-business environment. This study aimed to identify the issues and challenges of electronic payment systems and offer some solutions to improve the e-payment system. Security is the protection of e-commerce assets from unauthorized access, use, alteration, or destruction. Dimensions of e-commerce security-Integrity, Non-repudiation, Authenticity, Confidentiality, Privacy, Availability.

1. INTRODUCTION

The electronic payment system is considered as the backbone of e-commerce and one of its most crucial aspects. It can be defined as a payment service that utilizes the Information and communication technologies including integrated circuit (IC) card, cryptography, and telecommunication networks' (Raja et. al., 2008). An efficient electronic payment system lessens the cost of trading and is thought to be essential for the functioning of capital and inter-bank markets. With the advancement of technology, electronic payment system has taken many forms including credit cards, debit cards, electronic cash and check systems, smart cards, digital wallets contactless payment methods and mobile payments and so on.

E-commerce has become a rapidly growing market today. With the proliferation of tablets and smartphones, the use of electronic payment methods has grown up to 21% in 2012 (Rau, 2013). The use of credit cards was the major international means of online payment that dominated in a variety of transaction markets. It was estimated that 95% of all e-commerce transactions in the United States are performed using credit cards(Abrazhevich, 2004). Other widely used online payment alternatives are debit cards (with rising number of users worldwide) and online payment systems like Paypal, Stripe or Skrill. With the availability of a variety of electronic payment means including

mobile payments, mediating services, and electronic currency, an appropriate option can be chosen for a particular type of transaction (Paunov and Vickery, 2006).

The future of a specific electronic payment system depends upon how it overcomes the practical and analytical challenges faced by various means of online payments. These challenges include issues of law and regulation (buyer and seller protection), technological capabilities of e-payment service providers, commercial relationships, and security considerations such as verification and authentication issues (Paunov and Vickery, 2006).

2. MAJOR ONLINE PAYMENT SYSTEMS

Studying various systems of electronic payments, Koponen (2006) explained that there are a wide variety of online payment systems that have been developed in past few years and these systems can be broadly classified into account-based and electronic currency systems. Account-based systems allow users to make payments via their personal bank accounts; whereas the other system allows the payment only if the consumer possesses an adequate amount of electronic currency. These systems offer a number of payment methods that include:

•Electronic payment cards (debit, credit, and charge cards)
• E-wallets
• Virtual credit cards
• Mobile payments
• Loyalty and Smart cards
• Electronic cash (E-cash)
• Stored-value card payments

Paunov and Vickery (2006) gives a description of electronic payment methods in their report evaluating the online payment systems for e-commerce, a summary of this description is given here to look at various characteristic features of the most commonly used online payment services.

2.1. Credit Cards

The most commonly used online payment mode so far was the use of credit cards. Initially, the security concerns hindered in the adoption of credit cards for making online payments but later with the provision of more secure features to protect every transaction made, customers developed trust on the use of credit cards. Applicability of credit cards is a strong factor that contributed to its wide use throughout the world. Credit card companies have established a wide network for their consumers ensuring a huge user base for a number of different transactions. However, it is considered a less-suitable method for small businesses and customers that need to make small payments due to high fees for credit cards (Paunov and Vickery, 2006). Aggregation or cumulative payment solution can be a way to adapt credit card payment system for micropayments. One of the major advantages of credit cards is their easy to use functionality with making online transactions in no time and from anywhere. These cards are easy to obtain and use as customers don’t need to purchase any extra software or hardware to work with them. Cardholder authentication procedure is also simple, with the provision of a name, credit card number, and expiry date. For the

security of consumers' personal information, credit card companies have developed a number of complementary systems including MasterCard SecureCode and Verified by Visa. These systems allow users to create a password and use it when they shop online through their credit cards.

2.2. Debit Cards

The popularity of the debit cards is constantly rising and currently debit cards the most popular non-cash payments instrument globally (Capgemini and RBS, 2013). In contrast to credit cards, payments through debit cards are withdrawn directly from the personal account of the consumer instead of an intermediary account. This makes it difficult for consumers to handle payment disputes as there funds don't have an extra protection in a debit account. For debit payments, providing the account number is enough without the necessity of producing a physical card or card number. The use of debit cards is particularly high in most countries with a specific user base depending on the conditions and regulations attached to the issuance of credit cards. However, debit payments may not popular on merchant websites as debit cards do not cater the demand for payments made by international customers (Paunov and Vickery, 2006). Since there are lower costs for using debit cards unlike credit cards this method is suitable for micropayments. In addition, the overall security of debit card payments is found to be higher than that of credit card payments with extensive identification requirements demanded by the banks.

2.3. Mobile Payments

According to Hoofnagle, et al. (2012), payments made through wireless devices like mobile phones and smartphones are thought to provide more convenience, reduce the fee for the transaction, and increase the security of electronic payment. This payment system has also made it easier for businesses to collect useful information about their customers and their purchases. Paunov and Vickery (2006) found the applicability of mobile payment systems to be quite wide due to the remarkable growth and greater penetration of mobile devices as compared to other telecommunication infrastructure.

Mobile payment methods are suitable for offline micropayments as well as for online purchases. This method is a potential attraction for online traders due to an enormous user base of mobile phones. The use of mobile payment service does not only reduce the overall cost of a transaction but also offer a better payment security. However, mobile payment systems have encountered certain challenges in obtaining a significant consumer base for a number of reasons including privacy issues and their inability to cater international payments.

2.4. Mobile Wallets

In a study regarding consumer adoption of mobile wallets, Doan (2014) explained that ‘Mobile wallet is formed when your Smartphone functions as a leather wallet: it can have digital coupons, digital money (transactions), digital cards, and digital receipts’. Mobile wallet service allows the user to install an application from online stores in their smartphones and use them to

pay for their online and offline purchases. Using latest technologies that connect smartphones to the physical world such as NFC (Near Field Communication), sound waves, and QR codes, cloud-based solutions, mobile wallets are believed to provide more convenient payment solutions to the customers in future (Husson, 2015).

2.5. Electronic Cash

During initial stages of introducing online payment systems, electronic cash systems proposed in the form of DigiCash or CyberCash. However, these systems were not much appreciated and disappeared soon. At present, smart card-based systems are more common in use for the payment of small amounts by many businesses. Smart cards usually rely on specific hardware and card reader for their use and authentication. In addition to smart cards, numerous electronic cash systems have also been established such as Virtual BBVA and Clic-e. These systems work with the use of pre-paid cards or electronic tokens that represent a certain value and can be exchanged for hard cash (Paunov and Vickery,2006).

3. REQUIREMENTS AND LIMITATIONS

3.1. E-Wallets

Requirements	Transaction Process	Limitation/Risk
1. Online Account in Digital Wallet. For example few popular e wallets are PayUmoney, Paytm, Pockets, Oxygen wallet, Mobiwiki etc. 2. A mobile phone with wallet app loaded. Bank wallets are also used operated through Desktop PC. 3. Internet connection.	1. Download wallet app in mobile and create account using mobile no. Mobile number is treated as wallet account no. 2. Load money using debit/credit card or net banking. 3. Link your bank account with digital wallet to transfer money in advance to your wallet. 4. Transfer money from one wallet to other using mobile number.	1. Consumer Wallet Limits: Rs.20, 000/month for all. Rs.1 lakh/month with KYC 2. Merchant Wallet Limits: Rs.50, 000/month with Self Declaration. Rs.1 lakh/month with KYC 3. Money can be transferred to same company wallet.

3.2 Unified Payments Interface (UPI)

Requirements	Transaction Process	Limitation/Risk
1. A Bank account for registration only 2. Any smartphone with internet connections 2G/3D/4G/wifi. 3. UPI Apps of bank (28 banks have enabled upi)	1. Download bank UPI app of mobile banking apps of banks 2. Register by creating your Virtual Payment Address (VPA) e.g *sujith@icici* or *julieebi@s bi* 3. For money sending you just need the VPA of payee 4. After entering amount and VPA of payee you will be asked for confirm payment and it is done. 5. Account details of payee is not required only VPA is required	1. Maximum transaction limit is Rs 1 lakh 2. Sender and Receiver of money must have VPA (Virtual Payment Address) for fund transfer 3. Smartphone is required

3.3 Debit/ATM Cards

Requirements	Transaction Process	Limitation/Risk
1. Issue of Debit Cards by Bank. Card Pin/password or mobile for OTP (One Type Password) verification. 2. Bank ATMs 3. Swipe machine or POS (Point of Sale) machine at merchant. 4. Online payment portal	1. Bank issue ATM card with a PIN no. 2. Used to withdraw cash from any ATM machine using PIN no. 3. Used at any POS for shopping. Also for online shopping 4. SMS notifications come in mobile for every transaction.	1. POS of Swipe machine at merchant is a must. 2. Cloning of card is a security threat.

3.4 Credit Cards

Requirements	Transaction Process	Limitation/Risk
1. Issue of Credit Cards by Bank. Card Pin/password or mobile for OTP (One Type Password) verification. 2. Swipe machine or POS (Point of Sale) machine at merchant. 3. Online payment portal	1. Bank issue Credit cards with a PIN no to only eligible customer. 2. There is credit limit for issued cards, limit vary from person to person depending upon income. 3. Used at any POS for shopping. Also for online shopping or transaction. 4. Every month Bill is generated, the total dues is to be paid before the due date, otherwise interest is charged. 5. SMS notifications come in mobile for every transaction.	1. Every card has a credit limit, beyond that you cannot shop. 2. Cash withdrawal is possible but at huge interest rate. 3. POS of Swipe machine at merchant is a must. 4. Cloning of card is a security threat.

:

4. SECURITY

Viruses are a nuisance threat in the e-commerce world. They only disrupt e-commerce operations and should be classified as a Denial of Service (DoS) tool. The Trojan horse remote control programs and their commercial equivalents are the most serious threat to e-commerce. Trojan horse programs allow data integrity and fraud attacks to originate from a seemingly valid client system and can be extremely difficult to resolve. A hacker could initiate fraudulent orders from a victim system and the ecommerce server wouldn‘t know the order was fake or real. Password protection, encrypted client-server communication, public private key encryption schemes are all negated by the simple fact that the Trojan horse program allows the hacker to see all clear-text before it gets encrypted.

4.1 PURPOSE OF SECURITY

1. Data Confidentiality – is provided by encryption /decryption.
2. Authentication and Identification – ensuring that someone is who he or she claims to be is implemented with digital signatures.
3. Access Control – governs what resources a user may access on the system. Uses valid IDs and passwords.

4. Data Integrity – ensures info has not been tampered with. Is implemented by message digest or hashing.
5. Non-repudiation – not to deny a sale or purchase Implemented with digital signatures.
   __ Plaintext/Cleartext – message humans can read.
   __ Ciphertext – unreadable to humans, uses encryption. Reverse process is call decryption.
   __ A cryptographic algorithm is called a cipher. It is a mathematical function. Most attacks are focused on finding the ―key.

4.2. SECURITY ISSUES

E-commerce security is the protection of e-commerce assets from unauthorized access, use, alteration, or destruction. While security features do not guarantee a secure system, they are necessary to build a secure system. Security features have four categories:

1. Authentication: Verifies who you say you are. It enforces that you are the only one allowed to logon to your Internet banking account.
2. Authorization: Allows only you to manipulate your resources in specific ways. This prevents you from increasing the balance of your account or deleting a bill.
3. Encryption: Deals with information hiding. It ensures you cannot spy on others during Internet banking transactions.
4. Auditing: Keeps a record of operations. Merchants use auditing to prove that you bought a specific merchandise.
5. Integrity: prevention against unauthorized data modification
6. Non-repudiation: prevention against any one party from reneging on an agreement after the fact
7. Availability: prevention against data delays or removal.

4.3. SECURITY THREATS

Three types of security threats:

1. *denial of service,*
2. *unauthorized access, and*
3. *theft and fraud*

4.3.1. Security (DOS): Denial of Service (DOS)

Two primary types of DOS attacks: spamming and viruses

1. Spamming
   –Sending unsolicited commercial emails to individuals
   –E-mail bombing caused by a hacker targeting one computer or network, and sending thousands of email messages to it.
   –Surfing involves hackers placing software agents onto a third-party system and setting it off to send requests to an intended target.
   –DDOS (distributed denial of service attacks) involveshackers placing software agents onto a number of third-party systems and setting them off to simultaneously send requests to an intended target
2. Viruses: self-replicating computer programs designed to perform unwanted events.
3. Worms: special viruses that spread using direct Internet connections.

4. Trojan Horses: disguised as legitimate software and trick users into running the program

4.3.2 Security (unauthorized access)

•Illegal access to systems, applications or data
•Passive unauthorized access –listening to communications channel for finding secrets.
–May use content for damaging purposes
•Active unauthorized access
–Modifying system or data
–Message stream modification
•Changes intent of messages, e.g., to abort or delay a negotiation on a contract
•Masquerading or spoofing –sending a message that appears to be from someone else.
–Impersonating another user at the ―name‖(changing the ―From‖field) or IP levels (changing the source and/or destination IP address of packets in the network)
•Sniffers–software that illegally access data traversing across the network.
•Software and operating systems‘ security holes

4.3.3Security (theft and fraud)

•Data theft already discussed under the unauthorized access section
•Fraud occurs when the stolen data is used or modified.
•Theft of software via illegal copying from company‘s servers.
•Theft of hardware, specifically laptops.

5. CONCLUSION

Electronic payment refers to the mode of payment which does not include physical cash or cheques. It includes debit card, credit card, smart card, ewallet etc. E-commerce has its main link in its development on –line in the use of payment methods, some of which we have analyzed in this work .The risk to the online payments are theft of payments data, personal data and fraudulent rejection on the part of customers. Therefore, and until the use of electronic signatures is wide spread, we must use the technology available for the moment to guarantee a reasonable minimum level of security on thenetwor

6. REFERENCES

1. Bhasker, Bharat (2013). Electronic Commerce, Framework, Technologies and Applications. McGraw Hill Education (India) Private Limited., p.9.2-9.16.

2. Madan, Sushila (2013). E-Commerce, Mayur Paperbacks. P.4.4-4.35.
3. Noor, Aaihan Ab Hamid, Aw Yoke Kheng. A Risk Perception analysis on the Use of Electronic Payment Systems by Young Adult, Wseas Transaction Information Science and Applications.p.1to3 and 8.
4. S.S.Hugar, Trends and challeges to Indian Banking, Deep & Deep publications, New Delhi.
5. Kaur Manjot, E-Commerce, Kalyani Publcation, New Delhi
6. Abrazhevich, Dennis, 2004. Electronic Payment Systems: a User-Centered Perspective and Interaction Design. Netherlands: Technische Universiteit Eindhoven.

7. Aigbe, Princewill and Akpojaro, Jackson, 2014. Analysis of Security Issues in Electronic Payment Systems.
8. Nigeria: International Journal of Computer Applications (0975-8887), Vol. 108 No, Capgemini and The Royal Bank of Scotland (RBS) (2013), World Payments Report 2013, Capgemini and The Royal Bank of Scotland
9. Doan, Ngoc, 2014. Consumer adoption in Mobile Wallet. The Turku University of Applied Sciences.
10. Hoofnagle, Chris Jay, Urban, Jennifer M. and Su Li, 2012. Mobile Payments: Consumer benefits and new privacy concerns. BCLT Research Paper. Husson, Thomas, 2015. The Future of Mobile Wallets lies beyond Payments. U.S.A.: Forrester Research Inc.
12. ISACA, 2011. Mobile Payments: Risk, Security and Assurance Issues. U.S.A.: ISACA Emerging Technology White Paper.
13. Ismaili, Houssan, Houmani, Hanane and Madrroumi Hicham, 2014. A Secure Electronic Transaction Payment
14. Protocol Design and Implementation. Morocco: International Journal of Advanced Computer Science and Applications, Vol.5, No.5.