International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 9 Issue 5 ǁ 2021 ǁ PP. 06-09

An Overview of E- Payment Systems

Jaskirat Kaur
Department of Computer Science, Sri Guru Granth Sahib World University, Fatehgarh Sahib, India

Sandeep Singh
Department of Computer Science, Sri Guru Granth Sahib World University, Fatehgarh Sahib, India

Abstract
The Era of Information and Communication Technology (ICT) and digital innovation lead to dynamic changes in the business environment, where business transactions continue to shift from cash-based transactions to electronic-based transactions. The e-payment system was not introduced to replace cash but as a better alternative to cash and trade barter. Electronic payments can be understood as a payment mechanism using electronic media that does not involve cash. Electronic payment system (e-payment) is an important aspect of e-commerce. This study aimed to identify the issues and challenges of electronic payment systems and offer some solutions to improve the e-payment system quality.

Keywords: *Cyber Cash, Digital Signatures, e-Cash, Electronic Payments, Encryption, Net Bill, Secure Electronic Transaction Protocol.*

Date of Submission: 16-05-2021 Date of acceptance: 31-05-2021

I. INTRODUCTION

Electronic payment system is a mode of payments over an electronic network such as the internet. E-payment is a method in which a person can make Online Payments for his purchase of goods and services without physical transfer of cash and cheques, irrespective of time and location. It makes electronic payments at any time through the internet directly to manage the e-business environment. With a large number of organizations conducting business this way, it has become evident that the field of e-commerce has a promising future ahead and businesses are going to obtain maximum benefit from it (Dennis, 2004). In real world we /have two distinct types of payment systems:

i. INTERNET-BASED PAYMENT SYSTEM-There are four models of Internet-Based payment system, e-cash, Credit Card, Debit Card, Smart Card.

ii. ELECTRONIC TRANSACTION-BASED PAYMENT SYSTEM- There are four models of Internet-Based payment system, Secure Electronic Transaction, Cyber Cash, Net Bill, First Virtual Holdings.

II. OBJECTIVES

- To create awareness about various methods of online payments systems.
- To create awareness about various frauds of electronic payments.
- To motivate people to use online payments systems.
- To make online payments safe and secure.

III. METHODS OF E-PAYEMNT SYSTEM

3.1 E-cash-

E-Cash is a software-based, anonymous, untraceable online token payment system that runs on UNIX, Windows, and Macintosh. When consumers buy tokens, the e-Cash program keeps digital money on the customer's computer, which is under the bank's supervision. Users may spend digital money at any store that accepts e-Cash without having to give their credit card information.

3.2 Credit Card-

A credit card is a plastic card that allows you to borrow money to buy products and services. The consumer fills out the order form with the card number, expiration date, and billing address so that the vendor may check the information and ensure payment (Kumaga D, 2010).

On the Internet network, there are three sorts of credit card payments.

(a) Payment using a standard credit card

(b) Payment using encrypted credit card details
(c) Payment using third party verification.

3.3 Debit Card-

A debit card is a bank card that has been augmented with ATM and point-of-sale functions to allow it to be used at merchant locations. A debit card is connected to a person's bank account and allows funds to be withdrawn at any time. Without writing a cheque, you can use an ATM and a point of sale. A debit card holder pays for his purchases straight through his bank. It takes the place of actual currency and checks. Customers that use a debit card system deposit money in advance and withdraw it at the moment of purchase (Capgemini and RBS, 2013).

3.4 Smart Card-

Motorola was the first company to manufacture a smart card in 1977. It is a tiny, credit card-sized piece of plastic with a half-inch-square input-output region that acts as the card's input-output mechanism. A smart card has a programmable chip, RAM and ROM storage, and may be recharged by connecting to a bank. It's called a smart card since the chip's capacity to retain information in its memory makes it such (Kumaga D, 2010) .

3.5 Secure Electronic Transaction (SET)-

A secure electronic transaction (SET) is an online payment system that ensures the security of online financial transactions. VISA and Mastercard produced the SET specification, which is an open technological standard for commerce. It allows for secure card payment transactions over the internet. Throughout the transaction, a digital certificate creates a trust change, validating cardholders and merchants.

3.6 Cyber Cash-

Cyber cash is a web-based service that automatically validates and validates a customer's credit card information before debiting and crediting the customer's account electronically. Cyber cash servers serve as a link between the online merchant and the bank's secure financial network. Digital signatures are used in this system for the purpose of security in electronic payment systems.

3.7 Net Bill-

A micropayment system, Net Bill is a micropayment system. The net bill payment system makes safe and cost-effective payments for products and services purchased via the internet. The net bill server keeps track of both consumers and merchants' accounts, allowing customers to pay merchants for products that have yet to arrive. The products are provided digitally. A software program that checks receipts of commodities is available. As a result, the electronic payment net bill system allows communication between the money tool, the merchant server, and the net bill server.

3.8 First Virtual Holdings-

First Virtual was one of the first internet payment systems to provide a third-party verification technique for online transactions. In the sense that it does not employ encryption, the first virtual payment system is unique. Because the internet is an open network, a core idea of the payment system is that some information should not move through it. These details are mostly connected to credit card information. The transactions are completed using a first virtual PIN, which is issued by the first virtual organization, rather than credit card information. Because it functions like Id, these PIN numbers may be sent over the internet.

IV. ELECTRONIC PAYMENT SYSTEM PROBLEMS AND CHALLENGES

4.1 Inadequate Usability-

Electronic payment systems often need a lot of information from end users or make transactions more difficult by employing complicated internet interfaces. Credit card payments via a website, for example, are not the simplest method of payment since this system necessitates the entry of a considerable quantity of personal information and contact information in a web form.

4.2 Inadequate Security-

Online payment systems are an obvious target for thieves looking to steal money and personal information. Customers must supply credit card and payment account information, as well as other personal information, via the internet. This information is occasionally sent in an insecure manner (Kolkata and Whinston, 1997). Providing these data via mail or over the phone comes with its own set of security concerns (Guttman, 2003, Laudon and Traver, 2002)

4.3 Problems with e-Cash

The biggest issue with e-cash is that it is not widely accepted since business establishments must accept it as a payment option. Another difficulty is that when we pay with e-cash, both the client and the salesperson must have accounts with the same bank that issues e-cash. Other banks will not accept the money (yang,2009).

4.4 Lack of Trust-

Electronic payments have a lengthy history of fraud, abuse, and limited dependability, and they are a new system with a poor image. This danger is frequently cited by potential consumers as the primary reason they do not trust payment providers and so do not make online transactions (yang,2009).

a. User Perceptions of Electronic Payment Systems Acceptance-

The acceptability of users is a critical aspect in deciding whether an information system project succeeds or fails. Many researches on information technology have found that user attitudes and human factors are essential variables in the effectiveness of any information system (Davis, 1993). (Davis, 1989, Burkhardt, 1994, Rice & Adyn, 1991). Users' acceptance, according to Dillion and Morris (1996), is "the demonstrated willingness within a user group to utilize information technology for the tasks it is meant to enable."

4.6 Lack of Knowledge-

Making an internet payment is a difficult process. Even well-educated people have difficulty making internet payments. As a result, they always opt for conventional buying over Internet purchasing. Customers who attempted to make online payments but were unable to do so due to a technical difficulty on the server. As a result, they stay away from it.

4.7 Online Payments are Impossible in Rural Regions-

The populace of rural areas is illiterate and computer-illiterate. They are uninterested in online payments because they are uninformed of technical advancements. As a result, locals are unable to use internet payment methods.

4.8 Expensive and Time Consuming-

Electronic payment systems are expensive because they contain set-up costs, machine costs, and administrative costs, among other things, and this way of payment takes longer than physical payment.

V. PROBLEM SOLVING IN ELECTRONIC PAYMENT SYSTEMS

Despite the fact that e-commerce is a growing field with an increasing use of its online payment services, its further development and widespread use in future are dependent upon the security and authentication stability of various electronic payment systems (Aigbe and Akpojaro, 2014).

5.1 Encryption- Online shoppers are wary of the perception that e-commerce is unsafe, especially when it comes to online payments. To increase security to the transfer of personal and financial information, most online payment systems employ an encryption method. To avoid online payment fraud, a variety of encryption algorithms are used.

5.2 Digital Signatures- To ensure transaction authenticity, parties participating in online payments and transactions should employ digital signatures.

5.3 Examine Whether or not the country is classified as a "High Risk" country- Orders being delivered to a foreign location should always be subjected to a more thorough check. If the card or the mailing address is in a high-risk location for credit card theft, pay extra care. Ukraine, Indonesia, Yugoslavia, Lithuania, Egypt, Romania, Bulgaria, Turkey, Russia, Pakistan, Malaysia, and Israel are the top 12 foreign sources of online fraud, according to a Clear Commerce® survey.

5.4 Firewalls- A firewall is an integrated collection of security measures designed to prevent unauthorized electronic access to a networked computer system to protect private network and individuals' machines from the dangers of the greater internet, a firewall can be employed to filter incoming or outgoing traffic based on a predefined set of rules called firewalls policies.*

There are three policy actions of firewalls:

- Accepted: Permitted through the firewall.
- Dropped: Not allowed through with no indication of failure.
- Rejected: Not allowed through accompanied by an attempt to inform the sources that the packet was reject.

5.5 Compare the country of the credit card issuing bank with the country of the billing address- Another important consideration is to double-check the issuing nation and billing address. Make that the nation of issue and the nation of billing address are the same. This is particularly critical since smaller banks may lack stringent identification processes.

5.6 Call the credit card providing bank to confirm credit card validity- If online merchants have any doubts about an order and need to validate the details, they can call the issuing bank and ask to validate the general account data. This is to prevent the card from being stolen. The first six digits of a credit card number, known as the Bank Identification Number, are used to determine the issuing bank's phone number (BIN).

5.7 Request more identification if you have any doubts-

While customers cherish their privacy and expect speedy web site purchase, it's critical to collect enough client identity information during the ordering process. Customers' names, credit card numbers, and expiration dates

are insufficient. If they have any worries, merchants should call them for verification over the phone or request a photo ID to be sent.

VI. CONCLUSION

The term "electronic payment" refers to a method of payment that does not include the use of physical currency or checks. Debit card, credit card, smart card, e-wallet, and other types of cards are included. The usage of payment mechanisms, some of which we have examined in this study, is the key link in the growth of e-commerce on the internet. Theft of payment data, personal data, and false customer rejection are all threats to online payments. It is hard to state that any of the payment mechanisms examined in this study is flawless, even if each one offers benefits over others. If the customer wishes to keep their information private, they should choose payment methods like E-cash or Net Bill Checks, which provide a better level of anonymity. Smart Cards should be used if security is a top priority. E-payment systems can benefit both consumers and service providers, resulting in increased national competitiveness in the long run.

REFERENCES

[1]. Dennis, Abrazhevich (2004). Electronic Payment Systems: A User Centred Perspective and Interaction design. Eindhoven: Technical Universiteit Eindhoven. p.1to12.
[2]. Delali Kumaga (Dec 2010) The challenges of implementing Electronic Payment Systems – The Case of Ghana's E-zwich Payment System.
[3]. Whiteley, David, (2007). e-Commerce, Strategy,- Technologies and Applications. Tata McGraw-Hill Publishing Company Limited. P.200-201.
[4]. Capgemini and The Royal Bank of Scotland (RBS) (2013), World Payments Report 2013, Capgemini and The Royal Bank of Scotland
[5]. Jing, Yang. (2009). Online Payment and Security of E-Commerce. International symposium on web Information system and application (WISA'09) Nanchang, P. R. China, May 22-24, 2009, pp. 046-050.
[6]. Bhasker, Bharat (2013). Electronic Commerce, Framework, Technologies and Applications. McGraw Hill Education (India) Private Limited., p.9.2-9.16.
[7]. Aigbe, Princewill and Akpojaro, Jackson, 2014. Analysis of Security Issues in Electronic Payment Systems. Nigeria: International Journal of Computer Applications (0975-8887), Vol. 108 No, 1