**IOSR Journal of Engineering (IOSRJEN)** **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 17-20

# Discussion on E-Payment System, Payment Gateway and Security

[1]S.Uma Mageshwari, [2]Umme- Iman taskeen
[1]*Asst.Professor in PG Department of Computer Science, Islamiah Women's Arts & Science College, Vaniyambadi.*
[2] *PG Department of Computer Science, Islamiah Women's Arts & Science College, Vaniyambadi.*

***Abstract:*** *The electronic payment system has grown increasingly over the last decades due to thegrowing spread of internet-based banking and shopping. When it comes to payment options, nothing is more convenient than electronic payment. One need not have to write a check, swipe a credit card or handle any paper money; all we have to do is enter some information into your Web browser and click your mouse. It's no wonder that more and more people are turning to electronic payment -- or* ***e-payment*** *-- as an alternative to sending checks through the mail. This research paper reviewsthe types of electronic payment, discuss its benefits and limitations and explain about the security in electronic transactions.*
***Keywords:*** *E-payment, Security, Transaction.*

## I. Introduction

**In 1994** Stanford Federal Credit Union was established – **the firstfinancial institution** which offered online internet banking services to all of its members.However, first online payment systems weren't user-friendly at all and required specializedknowledge of encryption or data transfer protocol.

E-commerce sites use electronic payment, where electronic payment refers to paperless monetary transactions. Electronic payment has revolutionized the business processing by reducing the paperwork, transaction costs, and labor cost. Being user friendly and less time-consuming than manual processing, it helps business organization to expand its market reach/expansion.Listed below are some of the modes of electronic payments:

1. **Credit Card** — A form of the e-payment system which requires the use of the card issued by a financial institute to the cardholder for making payments online or through an electronic device, without the use of cash.
2. **Debit Card**— A financial transaction in which the account holder instructs the bank to collect a specific amount of money from his account electronically to pay for goods or services.
3. **Smart card ---** A plastic card with a microprocessor that can be loaded with funds to make transactions; also known as chip card.
4. **Electronic Fund Transfer:** It is a very popular electronic payment method to transfer money from one bank account to another bank account. Account can be in the same bank or different bank. Fund transfer can be done using Automated Teller Machine (ATM) or using a Computer.
5. **E-cash** is a form of an electronic payment system, where a certain amount of money is stored on a client's device and made accessible for online transactions.
6. **Stored-value card** — a card with a certain amount of money that can be used to perform the transaction in the issuer store. A typical example of stored-value cards are gift cards.

With growing numbers of e-commerce and m-Commerce transactions, there are new opportunities for cyber criminals. It is important that we are all aware of the mandatory security protocols for e-commerce websites; so that we can avoid fraudulent situations. As the saying goes, prevention is better than cure.

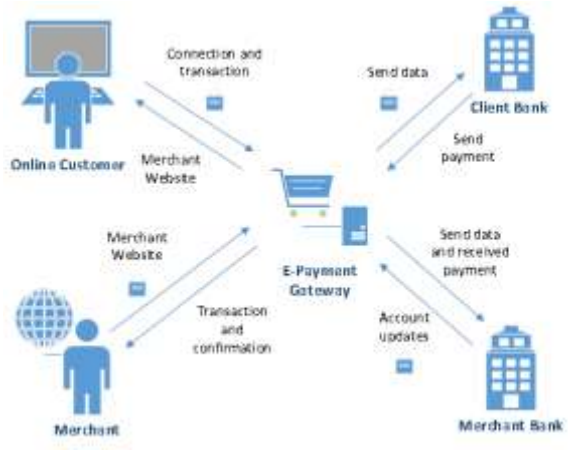
## II. Literature Review

Many papers have been written on this topic. Literature survey is presented with the paper [1] which provides a wide knowledge about electronic payment systems, payment gateways and their security considerations.
These are the following information that have been reviewed in my study

**Process of ElectronicPayment through a Payment Gateway:**
Five participants are involved as shown in Figure
1. Server (Electronic Payment Gateway)
2. Customer
3. Merchant
4. Client Bank

5. Merchant Bank

Online Shopper will be connected to the e-payment gateway by means of the Internet. The gateway will make a connection to the bank and check whether the customer's financial balances are sufficient to purchase the said item. The online client can likewise visit Merchant's site by means of the Gateway. The payment gateway has frameworks set up to interface with different banks, credit card organizations, clearing houses, and other economic establishments. In case of online credit card system, the company does the processing of credit cards for the vendors. For such companies, the payment processors process credit cards for the vendors and enable them to connect to its site. These kinds of organizations host the webpage for payments that asks the client to enter the information of their credit cards. After the client gives all his details and finishes the exchange, the payment processor checks these details and later directs the client back to the shipper's page.




However, it has been found that payment gateways pose some security issues despite their growing popularity and large-scale use.Then come to the next paper [2] this paper provides the information about the types of attack done in online transaction, purpose of security and some security tips. This paper provides some information about the security protocol and proccess that needs to be followed in order to combat the security issues possessed by the payment Gateways.

## III. Payment Gateway

In order to avoid any kind of security issues, a good Payment Gateway must follow some of the security protocols and processes. They are as follows:

1. TLS Encryption
2. PCI-DSS Compliance
3. Tokenization
4. 3D Secure
5. Address Verification Service
6. Fraud Prevention

**1.TLS Encryption**

The TLS Certificate tells users that the data transmitted between theweb server and their browser is safe.Without TLS Encryption in place, all data sent over the Internet is unencrypted and is visible to anyone with the means and intent to intercept it. An easy way to check if the ecommerce websites are SSL certified is to look at the URL and see if it uses '*http://*' or '*https://*' protocol. The additional's'signifies a secure e-payment system. We can also look for the padlock icon at the beginning of the URL.

**2.PCI-DSS Compliance**

The PCI Security Standards Council is a global organization that maintains and promotescompliance rules for managing cardholder data for all e-commerce websites and onlinepayment systems.Payment Card Industry Data Security Standards (PCI DSS) tell merchants how sensitive data used in payments should be secured. It requires data encryption to provide payments without using real card data that's visible while processing.

**3.Tokenization**

Tokenization is a process by which a 16-digit card number gets replaced by a digital identifier known as a 'token'. Credit card tokenization helps e-commerce websites improve security, as it eliminates the need for storing credit card data, and reduces security breaches.

**4.3D Secure**

3D Secure creates a secure password for the shopper'sCredit card. Every transaction is then verified with the password, which adds anadditional layer of security. It can decrease the number of fraudulent transactionsand boost revenue.

**5.Address Verification Service**

Address Verification Service requires customers to provide the billing address associated with their credit card. When the address on the card matches with the one in bank's documents, the transaction will go through.


**6.Fraud Prevention**

Apart from these mandatory protocols, most e-commerce websites and payment gateways have their own fraud and risk prevention systems. Big data analytics and machine learning play a huge role in devising these risk prevention and mitigation systems.

## IV. Security

- Bank will never ask for your card data/passwords up front. Banks and financial service providers have a safe protocol to gain admin access to an account if the need ever arises.
- Passwords are safer when you don't write them down. Keep strong passwords that you can remember, change them frequently, and refrain from writing them down somewhere.
- Right to dispute suspicious charges on your card or accounts. Raise a chargeback request for any unidentified transaction on your card.

## V. Conclusion

The electronic payment system has grown increasingly over the last decades due to the growing spread of internet based banking and shopping. As the world advances more with technology development, we can seetheriseofelectronicpaymentsystemsandpaymentprocessingdevices.As these increases, improve, and provide evermore secure online payment transactions the percentage of check and cash transactions will decrease.

In this papera brief explanation about the electronic payment is explained. The process involved in electronic payment through a Payment Gateway has been discussed. The Security protocols and processes for preventing Security issues has been explainedandalsogivessometipsforfraud prevention. With thehelpofsecuritytipsyouwill be abletoprotectyourdata.

## References

[1]. A survey on E-payment System Elements, Adoption, Architecture, Challenges and Security Concepts by Muddassir Masihuddin Burhan UL islam khan, M mueen UL Islam matoo and Rashidah F Olanrewaju-**Indian Journal of Science and Technology,** *Vol 10(20), DOI: 10.17485/ijst/2017/v10i20/113930, May 2017*
[2]. Security in electronic transaction by Smita kakade, Jyoti charade ,Volume: 04, Issue: 04, Apr -2017
[3]. https://securionpay.com/payment-security/
[4]. How Secure Are Your Online Payments-https://razorpay.com/blog/online-payment-security
[5]. https://securionpay.com/blog/e-payment-system/
[6]. https://www.tutorialspoint.com/e_commerce/e_commerce_security.htm