Ensuring Security of Ecommerce Online Payment Systems

Kessahou Judichael, Jiang Linhua
School of Information Engineering, Huzhou University. Huzhou, China
jkessahou@gmail.com

Abstract

Nowadays E-commerce is important because most businesses are done online. Examples of e-commerce are Alibaba express, Amazon…etc. As businesses are done on e-commerce, many transactions are done so it is important to provide security. There are three main security issues relevant to doing business online: verifying the identity of the person through which doing business, ensuring that messages sends and received have not been tampered performed. Cryptography is about constructing and analyzing protocols that overcome the influence of adversaries and which are related to various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation, Application of cryptography include ATM cards, computer passwords, and electronic commerce. The aim is to study the security of different online payment systems, the threats to which users are exposed and some solutions to strengthen the security.

Keywords: e-commerce security-integrity, authenticity, confidentiality, privacy, availability

DOI: 10.7176/CEIS/13-2-02

Publication date: March 31st 2022

1.0 INTRODUCTION

By definition, e-commerce is the utilization of computer tools and telecommunication networks to buy-sell products services of all kinds. Nowadays the thought of living without e-commerce seems unbelievable and an inconvenience. It was not until only a few years ago that the idea of e-commerce had even appeared. Ecommerce was introduced 40 years ago and, to this day, continues to grow with new technologies, innovations, and thousands of businesses entering the online market each year. The convenience, safety, and user experience of e-commerce have improved exponentially since its inception in the 1970s.

E-commerce, short for electronic commerce, is trading in products or services using computer networks, such as the Internet. E-commerce draws on technologies such as mobile commerce, electronic funds transfer, supply chain management, Internet marketing, online transaction processing, electronic data interchange (EDI), inventory management systems, and automated data collection systems. Modern Ecommerce typically uses the World Wide Web for at least one part of the transaction's life cycle, although it may also use other technologies such as e-mail. It covers a range of different types of businesses, from consumer-based retail sites, through auction or music sites, to business exchanges trading goods and services between corporations. It is currently one of the most important aspects of the Internet to emerge. Ecommerce allows consumers to electronically exchange goods and services with no barriers of time or distance. E-Commerce has expanded rapidly over the past ten years and is predicted to continue at this rate, or even accelerate. Shortly the boundaries between "conventional" and "electronic" commerce will become increasingly blurred as more and more businesses move sections of their operations onto the Internet. People use the term "e-commerce" or "online shopping" to describe the process of searching for and selecting products in online catalogs and then "checking out" using a credit card and encrypted payment processing. An agreement between a buyer and a seller to exchange goods, services, or financial instruments. In accounting, the events that affect the finances of a business must be recorded on the books. Transactions are recorded in what is known as "journal entries." Each entry describes a single transaction and states its date and amount.

2.0 LITERATURE REVIEW

The reference [1] stated that information privacy and security would be the major obstacles in the development of consumer-related e-commerce. They described that risk perceptions regarding Internet privacy and security have been identified as issues for the consumers. They explained that the early research suggested that the risk perception would not affect e-commerce much. However, recent studies revealed that consumer risk perceptions would be the main obstacle to the growth of e-commerce. They explained that the higher Internet experience would reduce the risk perception of e-commerce, which includes system security, retailer fraud, and privacy. They suggested that further research is needed to find out how risk perceptions influence e-commerce, how retailers should manage it, and how the management of risk perceptions may affect consumer welfare.

According to the annual survey released by Greenwich, Conn.-IVANS (Insurance Value Added Network Services), even though Internet has provided convenience for the consumer to purchase services and products, they prefer to purchase goods than services, especially in insurance online. One of the reasons given is the e-commerce security threat. Other reasons are that insurance products are not commodities and they are not tangible. However, according to Clare DeNicoal, an IVANS (Insurance Value Added Network Services) representative, the strong interest in purchasing consumer goods will lead them to purchase services online in the future especially in banking and insurance. According to the survey, people interested in online purchases of any goods and services increased from 50 % to 61 %. Besides that, others factors such as age, income, and education level play a role in online insurance. Finally, this survey concluded that insurance could ensure consumer loyalty by tightening security measures and adding personal touches.

The reference [9] stated that the rapid growth of e-commerce has a significant impact on the computer market and people's working styles. Their study in South Africa revealed that over 50 % of the respondents are not willing to give their credit card information in a secure transaction on the Internet while purchasing goods and services. The most common reason is that they are concerned about the safety of their credit card information when conducting online business. Another reason they provided is that they were concerned that a hacker could intercept their credit card number. Besides that, their study also indicated that consumers with information technology (IT) knowledge are more willing to buy products or services over the Internet and have better knowledge and awareness of information security knowledge.

They concluded that the problem of trust and consumers‟ perceptions of safety measures should be addressed to convince them to use e-commerce. They stated that the principal factor is trust. They suggested that further research in e-commerce perceptions of the rest of the population as well as developing a model of trust in e-commerce is needed for the human-computer interrelationship. The limitation of the article is that they did not explain how to overcome the problem of trust and consumers‟ perception of safety measures in e-commerce. On top of that, their study is only limited to South Africa. The reference [3] stated that e-commerce has revolutionized the modern-day business world. However, they explained that the major concern cited by most decision-makers is security. They explained that inside Internet commerce, there are two major risks, which are business risks and technology risks. These two risks are overlapping and thus they cannot be categorized as either purely business risks or purely technology risks. Some of the criteria or phenomena under the business risks are the business world is becoming more reliant on technology, the dizzying pace at which changes are happening in the business and technology environments, information technology-related crimes are on the increase, there is a serious shortage of information security professionals, and the responsibility or liability for risks incurred on the Internet is unclear. As for the technology risks, they described that the dynamic environment of the Internet, the availability of hacker tools, the complexity of measures to secure the Internet, and the unpredictable nature of Internet technology are some of the risks. They stated that the improvement of Internet security technology would not depend on better technology, but rather on the more effective utilization of existing technology. They explained that risk analysis should be performed to determine what Internet-security technologies are required, as well as what level of protection is appropriate. They concluded that a new approach is required to identify and solve security, suited to e-Commerce. The limitation of the article is that they never explained whether these risks would affect the consumer perception of the security issues.

2.1 .E-commerce Transaction

Transaction security in E-commerce is important in today's century so that we get to know what and how much work is done in this field. This field is an interesting part to discuss. Following are some researchers who work in this field let's see what work these people have done.

The reference [5] has done work on the present status and growth of online payment systems in worldwide markets and also takes a look at its future [7]. In this paper, a comprehensive survey on all the aspects of electronic payment has been conducted after analysis of several research studies on online payment systems. Several online payment system services, the associated security issues, and the future of such modes of payment have been analyzed. This study also analyses the various factors that affect the adoption of online payment systems by consumers.

The reference [4] has done work on "Transaction security for E-commerce application". As a web-based application, efficiency matters a lot for this application. As transaction in E-commerce faces problems such as database exploits, log data mining, etc. can be resolved by using different security measures security is important in an E-commerce application. They have secure E-commerce by integrating security technologies into trust infrastructure. The work done by them was the first step in establishing a trust to make transactions secure.

The reference [5] has done work on "A Secure Electronic Transaction payment protocol Design and Implementation"[5]. Based on research done on security schemes and the requirement of electronic payment they have designed a secure and efficient E-payment SEP Protocol. This SEP Protocol offers an extra layer of protection for cardholders and merchants. SEP Protocol is a good transaction protocol for credit card payment. Design system how well SEP protocol meets E-payment security implementation and identified end-user implementation requirements.

The references [6] have done work on "Secure E-Commerce Protocol "[6]. The present system has a token-based secure Ecommerce protocol. Have a paradigm that is capable of satisfying security objectives by using a token-based security mechanism. Done work on secure transactions so that both parties will get transaction tokens and can communicate with each other. There are many security E-commerce protocols like SSL, PGP, and SET. Have used SET (Secured Ecommerce Transaction) to protect against security threats. Some steps need to be performed between customer and merchant. SET provides security aspects in E-commerce like Authentication, Non-Repudiation, Integrity, Replay Attack, and Man in Middle attacks. Due to some issues in E-commerce Transactions, they have used SET to protect against attacks. SET presents a security mechanism to increase the level of security objectives using simple cryptographic techniques. Cryptography is the practice and study of techniques for secure communication in the presence of third parties (called adversaries). More generally, it is about constructing and analyzing protocols that block adversaries; various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation are central to modern cryptography. Modern cryptography exists at the intersection of the disciplines of mathematics, computer science, and electrical engineering.

2.3 Security online

Security is a part of the Information Security framework and is specifically applied to the components that affect e-commerce that include Computer Security, Data Security, and other wider realms of the Information Security framework [11]. Ecommerce security has its particular nuances and is one of the highest visible security components that affect the end-user through their daily payment interaction with business. E-commerce security is the protection of e-commerce assets from unauthorized access, use, alteration, or destruction. Dimensions of e-commerce *Security-Integrity, Nonrepudiation, Authenticity, Confidentiality, Privacy, Availability* [12]. E-Commerce offers the banking industry great opportunity, but also creates a set of new risks and vulnerabilities such as security threats. Information security, therefore, is an essential management and technical requirement for efficient and effective Payment transaction activities over the internet. Still, its definition is a complex Endeavour due to the constant technological and business change and requires a coordinated match of algorithm and technical solutions.

2.4 Different payment systems in e-commerce and how they work

2.4.1 How to ensure the payment system

Online shopping has become an increasingly popular trend in the past few years as people find it more convenient to buy from the comfort of their homes. You can get pretty much anything and everything from online stores: groceries, clothing, jewelry, electronics, and other household items.

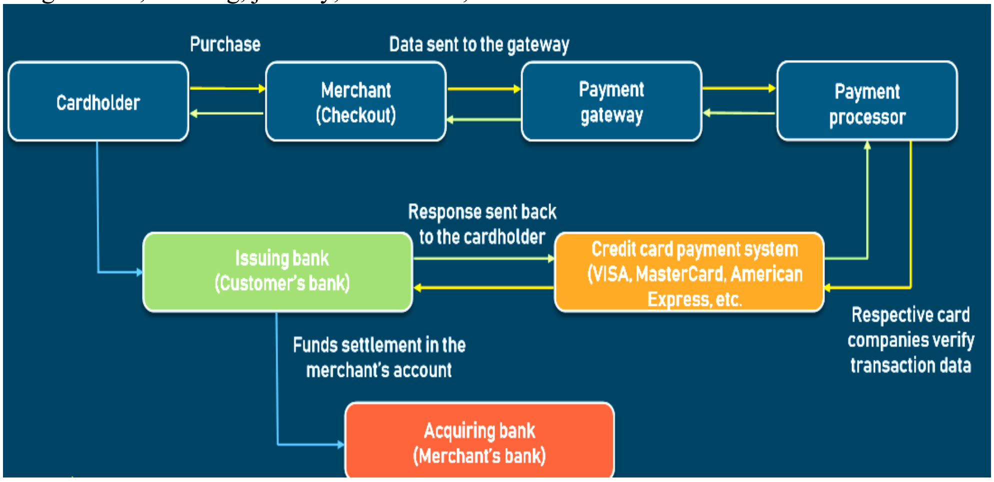
Purchase
Data sent to the gateway
Cardholder
Merchant (Checkout)
Payment gateway
Payment processor
Response sent back to the cardholder
Issuing bank (Customer's bank)
Credit card payment system (VISA, MasterCard, American Express, etc.
Respective card companies verify transaction data
Funds settlement in the merchant's account
Acquiring bank (Merchant's bank)

Figure 1: Processes of payment

There are quite several online payment services that have been developed within the payment system around the globe. These include electronic cheques, e-cash, credit cards, and electronic fund transfers [14] [15].

1) Credit Cards

Credit cards are by a long shot the most well-known mode of online payment. In the beginning, security concerns hampered their reception yet gained customer trust later when security features were provided for each exchange. Credit card pertinence is one of the strongest components, which contribute to its extensive use everywhere throughout the world. Nonetheless, it is not considered feasible for making little payments or private ventures since they require huge fees [16]. The most significant advantage of credit cards is the ease of use they provide in performing exchanges online from any piece of the world and in a matter of moments. Moreover, they can be obtained easily without the burden to possess any extra hardware or software for making them work.

2) *Debit Cards*

Debit cards are picking up notoriety as time passes and have become the most mainstream cashless payment method everywhere throughout the world [17]. As compared to credit cards, the payments made using debit cards are pulled back from the consumer's financial balance and not from any intermediary account. Along these lines, users neglect to have extra security in their debit accounts thereby alarming them while dealing with payment disputes. However, just the record number is required for making debit payments with no need to produce a card number or a physical card.

3) Mobile Payments

As per [17], the payments that are made utilizing wireless devices, for example, advanced cells and mobile phones are assumed to offer a reduction in exchange fees and an increase in online payment security and convenience. Such a payment method has facilitated businesses in the collection of valuable data regarding their customers just as their purchases. As indicated by [18], mobile payment systems are applicable all-inclusive because of their shocking development and the out-and-out attack of mobile devices in contrast with other telecommunication infrastructure. Mobile payments have been seen as feasibly used for both online purchases and offline micropayments. Since mobile phones have a huge consumer, base, online traders are potentially attracted to this payment method.

4) Mobile Wallets

As indicated by [10], "Mobile wallet is formed when your smartphone capacities as a leather wallet: it can have computerized coupons, advanced money (exchanges), advanced cards, and computerized receipts". Utilizing mobile wallets, users are allowed to introduce the application in their advanced cells, which they can employ for making offline just like online purchases. In the future, mobile wallets are assumed to offer more convenience to customers in making exchanges with the help of technologies that connect advanced cells and the physical world through sound waves, cloud-based arrangements, NFC (Near Field Communication), QR codes, etc.)

5) Electronic Cash

In the underlying phase of online payment system presentation, electronic money systems by the name CyberCash or Digi Cash. One of the best apparatus that the Internet offers in today's world is the ability to shift one's business wherever they want using a website. This is the reason it became noticeably vital to buy employing the Internet through numerous payment service providers. The most well-known payment techniques that are typically provided are bank transfer, real-time orders, and credit cards. Some popular systems of online payments are *Stripe, PayPal, Alipay, WeChat pay, Worldpay, Eway, from American Express, Intuit GoPayment, Icepay, Amazon Payments, WePay, Visa MasterCard, and Google Wallet/Google. Checkout.*

3.0 PROPOSED SECURITY MODEL OR APPROACH

3.1 How to Ensure Security of Online Payment Systems

Though ARP plays a vital role in successful local area network (LAN) communication, its vulnerabilities are used by attackers every day and by far have made it the leading point for refined LAN attacks such as; denial-of-service (DoS) and man-in-the-middle (MITM). Detecting and preventing network attacks are necessary for network solidity as any disruption in the network performance resulting from an attack can lead to loss of resources. The reference [14].

3.1. Security threats

With the proliferation of online transactions and the massive accumulation of user data, the risks of cyber-attacks, fraud, and identity theft are multiplied. Criminals who usurp the identity of the alleged victim introduce these.

This is linked in particular to the increase in industrial espionage and cybercrime, where malware is increasingly used for hacking data for profit. For example, users who log into unsecured connections or who willingly share their personal information on public sites are potential victims of identity theft. Likewise, online identity thieves are interested in collecting user-profiles and Personal information such as credit card information, bank account numbers, and driver's license. These online security breaches exacerbate various fraud problems such as counterfeit cards and other bank frauds.

3.2. Security Demands in EPS

In all data systems, the security of information and data is of huge importance. Information Security involves methodology, technology, and practices that guarantee that information is secured from

1) Alteration or unintentional change **(integrity),**
2) unauthorized access **(confidentiality),** while
3) Promptly accessible **(accessibility)** to approved clients on demand.

Figure 2 illustrates aspects of security of data assurance that encompass the methods, practices, and technology involved.

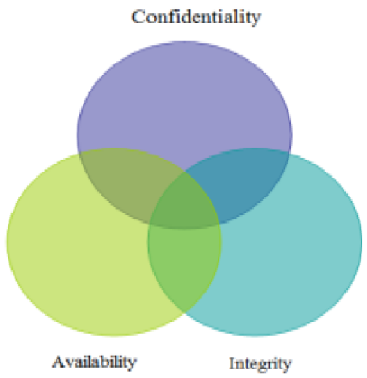

Figure 2: Security Demands in EPS

A safe economic exchange electronically needs to meet some prerequisites as explored by [19]. They may be stated as follows:

a) Integrity and Authorization

Integrity may be characterized as the validity, accuracy, and completeness of data as per business qualities and desires. In payment systems, integrity implies that no cash is taken from a client lest a payment is approved by the client. Additionally, customers need not accept any payment without the absolute permission of the clients; this is alluring when clients need to keep away from unwanted bribery.

b) Confidentiality

Confidentiality may be defined as the safety of private or sensitive data from unapproved divulgence. A few organizations included may want to have confidentiality in their exchanges. Confidentiality in this setting implies the confinement of knowledge about different snippets of data, which are related to the exchange; the verification of payer/payee, buy content, sum, and so forth. Commonly, members included wanting to guarantee that transactions are secret [10] where un-traceability or anonymity is sought; the prerequisite might be to make available this information to only certain specific subsets among the participants.

c) Availability and Reliability:

Availability is guaranteeing that data frameworks and information are prepared for utilization when they are required; regularly communicated as the rate of time that a framework can be utilized for profitable work. All factions need to have the capacity to make or get payments whenever the need arises [10]. End-user requirements include flexibility, usability, availability, affordability, speed of transactions, and reliability.

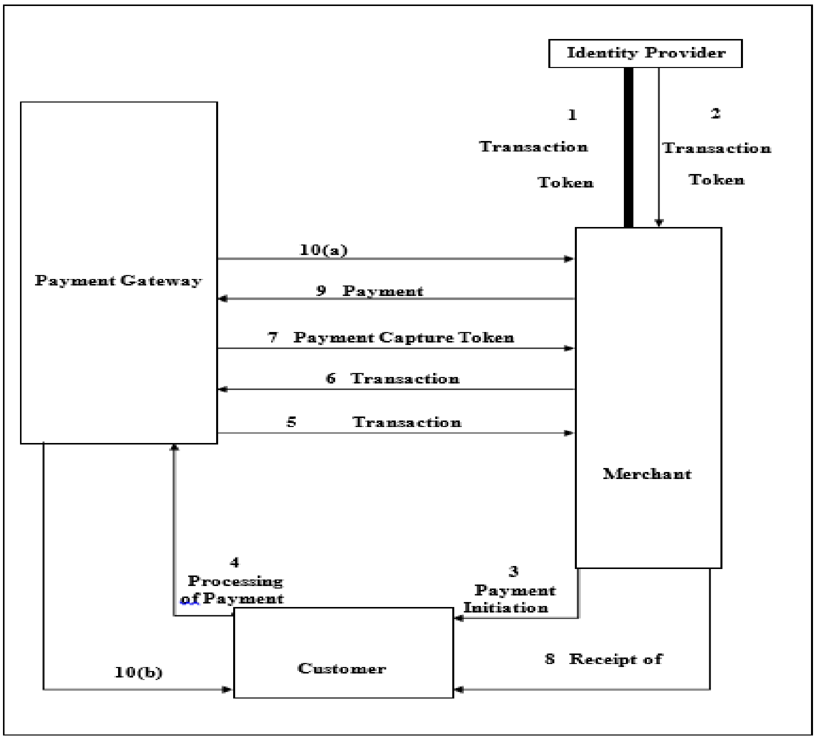

Figure 3: Diagram representing Proposed Security Model

After computing a transaction's *identity attribute*, a merchant encrypts the identity attribute (*identity attribute*) with his private key and sends it to an identity provider along with his unique *merchant id*. This entire message is encrypted with the identity provider's public key so that only the corresponding private key can decrypt it. The *transaction token* request message sent by the *merchant, M,* to an *IP* is as follows:

$$\boxed{\boldsymbol{M \qquad IP: \{(A)_{M(Pr)}, Merchant\_id\,\}_{IP(Pu)}}}$$

where,
A = identity attribute of a transaction
Merchant_id = Merchant's unique identification with the Identity Provider;
M(Pr) = Merchant's Private Key
IP(Pu) = Identity Provider's Public Key

Including a merchant's id in a *transaction, a token request* message helps the *IP* identify a merchant. Since a merchant has to be registered with an *IP*, the *Merchant_id* allows the *IP* to check the merchant's registration and obtain his public key for decrypting *A*.

3.3 Enhancing Online Payment Security

As more and more people are connected to the Internet, the popularity of online commercial activities is growing as well. Nevertheless, the risks associated with online payment systems are factual and multiply day by day. As per the survey conducted by the Association of Financial Professionals in the year 2013, it was found that about 60 percent of organizations fell prey to successful or attempted fraud payments whereas up to 63 percent of organizations showed up adoption of new security measures or preparation to do the same in the time to come [11]. Therefore, for their wide acceptance all over the world, online payment methods must follow an efficient protocol ensuring a higher level of security for performing online transactions. The most widely recognized strategy for securing online payments is utilizing cryptographic-based innovations, for example, digital signatures and encryption [12]. On application, these innovations lessen speed and proficiency and thus trade-off must be made amongst effectiveness and security. Two commonly used protocols viz. Secure Electronic Transaction (SET) and Security Socket Layer Protocol (SSL) have been identified after analyzing the study of [13] ensuring the security of online commerce transactions. Among these, SSL is found to be the most commonly used protocol that encodes the whole session between computers involved in the transaction process thereby enabling safe communication over the Web. In this way, encryption of communication is achieved in SSL using public-key cryptography between the client and server. In contrast to this, SET prevents the transfer of the whole credit card number of the user over the Internet by allowing only a part of it to be transferred during the communication process. Furthermore, SET also endows the users with the provision of business data verification, information integration, and sensitive information coding by making use of the latest technologies like data encoding and digital signatures.

4.0 SECURITY ANALYSIS OF THE PROPOSED MODEL.

The sending of a customer's payment information directly to a payment gateway prevents a merchant from obtaining a customer's sensitive financial information. This protects a customer's payment information from risks of data theft and data infringement on the merchant's side. In this section, we show that our approach for online payment is secure and protects both a customer's payment and payment information through security claims in the following ways. Only a registered merchant can obtain an identity token from an Identity Provider and initiate the payment process. Each merchant in our payment system is required to register with an Identity Provider (IP). An IP checks the identity of a merchant and creates a Pedersen commitment for the merchant's transactions. A Pedersen commitment, which is a unique identity of a transaction, is encrypted within the identity token and is provided to the merchant. A merchant cannot request and receive payment from a customer without an identity token. This is done to secure a customer's payment information and ensure that the transaction is being implemented by a registered merchant and not an imposter. For instance, let us assume that an attacker acquires the merchant id of a merchant. To initiate a payment process of a transaction, an attacker requires the Pedersen commitment of a transaction. To obtain a Pedersen commitment, an attacker needs to send an identity attribute, *A*, of the transaction to an IP as follows:

$$M - IP: \{(A)_{M(Pr)}, Merchant\_id\,\}_{IP(Pu)}$$

Now, even if an attacker computes an identity attribute, *A*, of a transaction, it has to encrypt *A* with the merchant's private key, which is known only to the merchant. This prevents an attacker from obtaining a transaction's identity token from an IP without which an attacker cannot request payment from a customer.

4.1 Only the rightful merchant can verify a transaction and obtain its payment

When a payment gateway receives a request for payment from a customer, it does not authorize the customer's payment immediately to a merchant. It sends the Pedersen commitment of the transaction and the dual signature of order details and transaction id to the merchant. A merchant, in response to the payment gateway's message, is required to send the identity attribute, *A*, of a transaction. The sending of a transaction's identity attribute by the merchant to the payment gateway validates the correctness of the transaction. The other reason why a payment gateway verifies a transaction from a merchant is to confirm that a customer's order details and transaction id have not been manipulated and match with the merchant's record. Let us assume that an attacker captures the *transaction check message* sent by a payment gateway to a merchant for the verification of a transaction. Since the transaction check message is encrypted with the merchant's public key, it can be decrypted only by the merchant's private key. This prevents an attacker from obtaining the information within the transaction check message. However, even if we assume that an attacker knows the merchant's private key, decryption of the transaction check message does not provide an attacker with any information related to the transaction.

The *transaction check message* contains the Pedersen commitment, *c*, and dual signature, DS_{TO}. The Pedersen commitment, *c*, unconditionally hides the identity attribute, *A*, of a transaction, and the dual signature of the transaction id and order details, DS_{TO}, also does not provide any information to the attacker about the transaction. Therefore, the attacker will not be able to send back the identity attribute, *A*, of the transaction for validation purposes. The payment gateway, without receiving a transaction's identity attribute, does not authorize its payment to a merchant. This protects a customer's payment from being obtained by any receiver other than the rightful merchant.

4.2 A customer's payment information is protected

The main objective of our proposed payment approach is to protect a customer's payment information from being stolen or misused. To achieve this, unlike the current payment approaches, we do not send a customer's payment information to a payment gateway through a merchant. We send a customer's financial information directly to a payment gateway and prevent a merchant from obtaining a customer's financial information even in encrypted form. When a customer shops online, he is exposed to various risks on the Internet. To avoid these risks, a customer provides his payment information to a payment gateway directly on a payment gateway's server. Payment gateways are more secure and trustworthy. They also communicate with banks for authorizing and issuing payments. Hence, providing a customer's payment information directly onto a payment gateway's server will protect a customer's payment information from being tampered with or compromised. A customer sends his payment information to a payment gateway as follows:

Customer PGW: {(Payment_Info, Payment Amount, ODMD, c, TIMD, $DS_{OP})_{Ks}$*,*
Digital Envelope, Customer's Certificate, Merchant's Certificate}
PGTW(Pu)

As shown in the message above, a customer provides his payment information and payment amount directly to the payment gateway. The message is encrypted with the payment gateway's public key allowing only the payment gateway to decrypt the message using its private key.

Merchants can prove the validity of their transactions in case of dispute/chargebacks, when a customer submits a dispute to a payment gateway against a transaction, the PGW initiates an inquiry with the associated merchant. Current payment approaches allow a merchant to store some details of a customer's debit/credit card to prove the validity of a transaction. Our payment approach, however, restricts a merchant from obtaining any part of a customer's payment information. Instead, a merchant stores Pedersen commitment, c, of a transaction, a random number, r, used to compute the Pedersen commitment, an identity attribute, A, of a transaction, and the components used to compute A, which includes order details, customer id, and transaction id.

Insecurity analysis 1) and 2) we proved that a fraudulent merchant cannot initiate a transaction and obtain a customer's payment. Likewise, a merchant does not obtain any financial information of a customer which makes it very unlikely for a customer's payment information to be compromised from the merchant's side. Therefore, the only dispute a customer would have in our payment system is regarding a transaction's order details and payment amount.

However, before approving a payment, a payment gateway sends a transaction check message (Step 5) to the merchant to check the correctness of a transaction's order details and payment amount as follows:

PGW - M: (Payment amount, c, DS_{TO}*, Customer's Certificate, PGW's Key*
Exchange Certificate)$_{M(Pu)}$

The significance of this message is to let a merchant verify all details of the transaction, provided by a customer before a payment gateway approves the transaction's payment. This way a payment gateway confirms before authorizing a payment to the merchant that the purchase details of a transaction with both the customer and merchant are the same. In case a dispute arises regarding the transaction's order details and payment amount, a payment gateway then holds the merchant responsible for approving the wrong details of the transaction.

A merchant uses the Pedersen commitment, *c*, to identify the transaction. After identification, a merchant verifies the *order details* and *transaction id* of a transaction using the dual signature, DS_{TO}. During this process of verification and transaction check, a merchant identifies a customer through the customer's certificate. A merchant also confirms the correctness of the payment amount corresponding to the Pedersen commitment, c, and dual signature, DS_{TO}, by comparing it with the payment amount sent by the PGW in the transaction check message. A merchant is supposed to send an identity attribute, A, of the transaction to the PGW only if all details of the transaction match.

In case they vary, a merchant does not send back the identity attribute, A, in response to the transaction check message, and the payment is not authorized. If a merchant compromises on the purchase information and sends back A to the payment gateway, the dispute will prove his violations of the payment system's policies.

Therefore, to avoid disputes and chargebacks, our proposed payment system validates all required information before sending a customer's payment to a merchant. However, in case of a dispute, a merchant provides all purchase details of a transaction to a payment gateway for re-verifying them with the information provided by a customer. This also proves that the merchant does not require a customer's payment information to prove the genuineness of a transaction in case of a dispute.

5.0 Conclusion

The fact that online services invade our lives daily cannot be overlooked. In e-commerce, two areas of online services we are interested in: online payments and recommendation systems. Due to their ease of use and necessity, the number of transactions and shopping sites is increasing exponentially. However, different issues arise in these areas regarding the preservation of privacy, online trust, and decision-making.

Furthermore, the advancements in technology supporting mobile transactions and making them more convenient and transparent is developing trust among customers who are becoming habitual of employing this mode of payment. This change in the behavior of customers showing a transition from the traditional to an advanced online mode of payment is apparent in retailing and banking, and with nearly all available mobile devices. The statistics are shown in this study signify that the number of customers employing online modes of payment and making online transactions is continuously growing, hinting at an everlasting acceptance of online payment systems from academia as well as industry. However, the adoption and deployment of several rising technologies carry new opportunities and challenges to the implementation and design of secure online payment systems in the present day as well as in near future. This study concludes that better integration of online payment systems with the present financial and telecommunication infrastructure is necessary for a propitious future of this payment mode. Furthermore, establishing a common standard for a variety of service providers, improving the compatibility with a large number of customers, overcoming privacy and security concerns, and employing the latest technology could facilitate expeditious adoption of online payment methods and expand the market for such a mode of payment. Future work may be directed towards the legalization of various factors responsible for contributing to the efficacious adoption of online payment systems all over the world.

New technologies have to be exploited by organizations for simplifying and enhancing the user experience. This is because online payment systems have transformed the entire industry plus the potential for mobile payments, card-reader-equipped smartphones, and contactless cards can all proclaim the subsequent revolution.

Peer-to-peer payments have to be accommodated since they are responsible for expanding the market beyond the retailer world. Moreover, the necessity of exchanging funds has sparked off innovations past the existing banking model even in developing nations. The shift towards a cashless society should be accelerated by incorporating micropayments for vending machines, parking meters, highway tolls, etc. which otherwise involve cash handling inconvenience and other unnecessary costs. The compliance of the online payment systems with broader data privacy obligations has to be ensured. In this regard, the collection of PCI standards is used for data breach disclosure laws and privacy mandates, and the majority of these laws emphasize the significance of data related to payments and finance.

References

[1] Information Management and Computer Security, p. 154 – 157, ISSN 0968-5227, Volume 8 Number 3.

[2] Pradnya. B. Rana, Dr .B. B. Meshram "Transaction security for E-commerce application," published in IJECSE,ISSN-22771956

[3] Houssam E Ismaili, Hanane Houman, "A secure electronic transaction payment protocol design and implementation," published in IJACSA 2014

[4] Khalid Haseeb, Dr. Muhammad Arshad, Shoukat Ali, Dr. Shazia Yasin, "Secure Ecommerce protocol, "published in IJCSS 2011

[5] Khan, Burhan Ul Islam, et al. "A compendious study of online payment systems: Past developments, present impact, and future considerations." *International Journal of Advanced Computer Science And Applications* 8.5 (2017): 256271.

[6]Naeem, Marwah, Methaq Hameed, and Mustafa Sabah Taha. "A study of the electronic payment system."

IOP Conference Series: Materials Science and Engineering. Vol. 767. No. 1. IOP Publishing, 2020.

[7] Hemanth, D. Jude, et al., eds. *Emerging Trends in Computing and Expert Technology*. Vol. 35. Springer Nature, 2019.

[8] Hassler, "Security fundamentals for Ecommerce," published in IJCSI 2001

[9] Li Yuewen, "Research on E-commerce secure technology," published in IEEE computer society, 2010.

[10] M.A. Kabir, S.Z. Saidin and A. Ahmi, "Adoption of e-Payment Systems: A Review of Literature", International Conference on E-Commerce, Kuching, Sarawak, 2015, pp. 112120.

[11] Adjei, H.A., Shunhua, M.T., Agordzo, G.K., Li, Y., Peprah, G., & Gyarteng, E.S. (2021). SSL Stripping Technique (DHCP Snooping and ARP Spoofing Inspection). *2021 23rd International Conference on Advanced Communication Technology (ICACT)*, 187-193.

[12] K. Peffers and W. Ma, "An Agenda for Research about the Value of Payment Systems for Transactions in Electronic Commerce", JITTA: Journal of Information Technology Theory and Application, vol. 4, no. 4, pp. 1, 2003.

[13] C. Paunov and G. Vickery, "Online Payment systems for E-Commerce". Organization for Economic Co-operation and Development (OECD), 2006.

[14] A. Singh, K. Singh, Shahazad, M.H. Khan and M. Chandra, "A Review: Secure Payment System for Electronic Transaction", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 2, no. 3, pp. 236-243, 2012.

[15] C.J. Hoofnagle, J.M. Urban and S. Li, "Mobile Payments: Consumer benefits and new privacy concerns", BCLT Research Paper, pp. 119, 2012.

[16] M. Urban, "The Challenges & Opportunities in Electronic Payments Fraud | Bank Systems & Technology", Bank Systems & Technology, 2014.

[17] W. Taddesse and T.G. Kidan, "E-Payment: Challenges and Opportunities in Ethiopia", United Nations Economic Commission for Africa. 2005 Oct.

[18] A. Koponen, "E-Commerce, Electronic Payments", Helsinki University of Technology, Telecommunications Software and Multimedia Laboratory, 2006.

[19] Yeboah Derrick, George K. Agordzo, Lu Ye, "New Paradigm of Computing (Distributed Computing)", International Journal of Science and Research (IJSR), https://www.ijsr.net/get_abstract.php?paper_id=SR20702170939, Volume 9 Issue 9, September 2020, 1272 - 1276