An Efficient Secure Electronic Payment System for E-Commerce

Article *in* Computers · August 2020

DOI: 10.3390/computers9030066

3 authors:

Md Arif Hassan
Universiti Kebangsaan Malaysia
12 PUBLICATIONS **13** CITATIONS
SEE PROFILE

Zarina Shukur
Universiti Kebangsaan Malaysia
122 PUBLICATIONS **544** CITATIONS
SEE PROFILE

Mohammad Kamrul Hasan
Universiti Kebangsaan Malaysia
137 PUBLICATIONS **279** CITATIONS
SEE PROFILE

computers

MDPI

Article

An Efficient Secure Electronic Payment System for E-Commerce

Md Arif Hassan *, Zarina Shukur and Mohammad Kamrul Hasan

Center for Cyber Security, Faculty of Information Science and Technology, National University Malaysia (UKM), UKM, Bangi 43600, Selangor, Malaysia; zarinashukur@ukm.edu.my (Z.S.); mkhasan@ukm.edu.my (M.K.H.)

* Correspondence: arifhassane72@gmail.com; Tel.: +60-102483220

Received: 8 June 2020; Accepted: 22 June 2020; Published: 27 August 2020

Abstract: E-commerce implies an electronic purchasing and marketing process online by using typical Web browsers. As e-commerce is quickly developing on the planet, particularly in recent years, many areas of life are affected, particularly the improvement in how individuals regulate themselves non-financially and financially in different transactions. In electronic payment or e-commerce payment, the gateway is a major component of the structure to assure that such exchanges occur without disputes, while maintaining the common security over such systems. Most Internet payment gateways in e-commerce provide monetary information to customers using trusted third parties directly to a payment gateway. Nonetheless, it is recognized that the cloud Web server is not considered a protected entity. This article aims to develop an efficient and secure electronic payment protocol for e-commerce where consumers can immediately connect with the merchant properly. Interestingly, the proposed system does not require the customer to input his/her identity in the merchant's website even though the customer can hide his/her identity and make a temporary identity to perform the service. It has been found that our protocol has much improved security effectiveness in terms of confidentiality, integrity, non-repudiation, anonymity availability, authentication, and authorization.

Keywords: e-commerce; electronic payments system; payments gateway

1. Introduction

E-commerce was introduced to the consumer and business worlds as a unique approach in 1990 [1]. E-commerce has expanded since then and improved enormously, giving the world's customers and companies incredible benefits. E-commerce history is closely linked to Internet history. When the Internet was open to the public in 1991, online shopping was made possible [1,2]. E-commerce is characterized as a primary business model by means of the selling process of goods, the purchasing of resources, and the distribution or exchange over the Internet of items, services, and knowledge [3]. E-commerce can be used with mobile payment systems, which allows customers to pay for their shopping by using smartphones [4,5]. Mobile business is a major e-commerce extension that enables customers with wireless handheld devices, e.g. tablets, smartphones, and laptops, to carry out online commercial transactions [6]. E-commerce is becoming very popular nowadays since the customer can spend from home; solutions are affordable, with items delivered to the home with no hassle. The popularity of e-commerce is mainly because of its online business perspective. It makes it possible to gain and sell goods online, to provide various services and information through the Internet, and to exchange money immediately between businesses [7]. Many individuals are excited about obtaining their own online website for their company, as it is possible to market items online around the world. Customers are also interested in online shopping since they do not wish to waste valuable time shopping. E-commerce implies an electronic purchasing and marketing process online by using typical Web browsers. It is described as selling and buying of services or goods through wireless technology.

Developed nations tend to be more acquainted with systems, whereas Internet shopping is exploding in developing nations. The foremost goals of an electronic payment system are increasing efficiency, improving protection, and improving customer convenience and ease of use.

In the electronic payment system, the payment gateway is an essential component of the infrastructure to confirm that such exchanges happen with no concerns and to ensure that the common security over electronic systems is maintained [8,9]. Such a system will help secure a purchase along with a person's transaction information. A payment gateway defends transaction information by encrypting personal information, such as credit/debit card details, to guarantee that information is transferred securely between a consumer and the transaction processor. Each online exchange should go through a managed transaction gateway. The secure electronic payment structure includes four system segments [10]. The interaction between the segments operate through protected communication tunnels. Secure communication tunnels offer a protected method for interaction between two or more people, or between segments, such as the buyer to the merchant, on the transaction gateway. The e-payment system must be harmless for online transaction applicants, for instance, fee gateway server, bank account server, and merchant server.

This paper is divided into six sections. Section 1 introduces electronic payments and their related study. Section 2 includes an overview of the existing system and the formulation of the problem. Section 3 describes the RSA cryptosystem. Section 4 addresses how the model will be implemented. Section 5 discusses the security analysis and proposed method advantages. Finally, the last section presents the conclusions and future work.

2. Literature Review

Electronic payment systems have continued to grow over recent years because of the increase of online banking and shopping. As the world advances much more with technological advancements, we are able to see the growth of e-payment methods and transaction processing devices. A payment gateway is a service provider that offers equipment to procedure a transaction between buyers and merchants, along with banks over the World Wide Web. It supports secure a purchase along with a person's transaction information inside a transaction. A payment gateway defends transaction information by encrypting sensitive information, to guarantee the information is transferred securely between a consumer and the transaction processor. To help make it secure between each element, particularly between the client and the Internet payment or merchant gateway, a few strategies are recommended. Specifically, online buyers have to feel comfortable that their personal information and banking details are protected and cannot be seen by hackers. Thus, a connection that is secure it needed to assure payment transactions. Identity theft and phishing fraud are the two most popular types of fraud found within the Internet store [11].

To mitigate both types of fraud, a new secure electronic payment gateway to offer authorization was proposed by Izhar et al. [12]. The main objective of this proposed method was to provide authorization confidentiality, integrity, and availability for transactions. In their study, the authors utilized the Triple Data Encryption Standard (TDES, more often referred to as 3DES) cryptosystem to encrypt the transaction information and accomplish a greater speed of transactions within the payment gateway. The 3DES algorithm utilizes the data encryption standard (DES) cipher three times to encrypt its information. DES is a symmetric key algorithm based on the Feistel cipher [13]. As a symmetric crucial cipher, it applies a similar element for both encryption and decryption processes. The Feistel cipher can make both processes almost precisely the same, which results in an algorithm that is more effective to put into action. DES has both a 64-bit block and key measurement but, in training, grants just 56 bits of security [13]. 3DES was created as a safe option due to DES's small crucial length. In 3DES, the DES algorithm is operated three times with three secrets and is regarded as safe in the event that three individual keys are used. To protect vulnerable cardholder information during transmission, good cryptographic and security protocols must be used. They encourage cryptographic libraries, such as certified AES and 3DES [14]. However, the most recent improvement, referred to as AES, is

slow. Therefore, 3DES is safer and faster [12]. There is another popular cryptosystem used in payment systems [15], namely RSA. An RSA e-commerce security system (RSA-ESS) is implemented in [16], which resolves the security and privacy issues of credit card information in e-commerce transactions. In such systems, RSA is utilized to key the transaction information and realize greater speed in e-commerce transactions. This method is only used for privacy and security of fee information. A study of privacy and security of the e-banking adoption approach can be found in [17], where the authors proved a secure model of trust in an electronic payment system. Figure 1 shows the functional flow of a payment gateway.

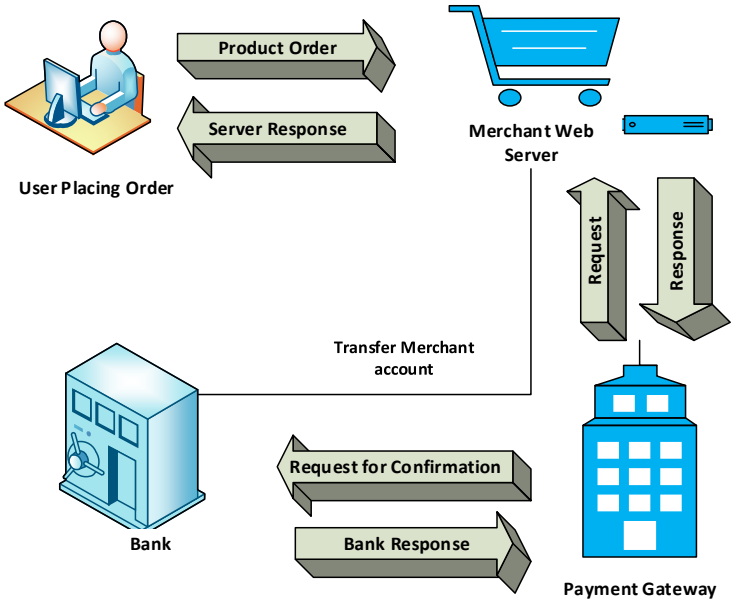

Figure 1. How a payment gateway works [15].

A related review conducted for online banking security and privacy issues in Oman can be found in [18]. A secure and privacy-preserving electronic payment approach can be found in [19], where the authors suggested electronic tokens as being an abstraction of basic fiat currency of equivalent benefit in order to provide privacy and protection in digital payments, presenting an intermediate entity in the method that mediates a transaction between the payer and the payee. A software tool to investigate distributed guessing attacks in the payment transaction process is implemented in [20]. In this study, the authors analyzed that remote Internet banks and merchants with their very own security policies cannot be protected by such attacks. Thus, the number of guessing actions is restricted to avoid repeated invalid efforts produced within a particular time span, and the posting code is confirmed to identify the invalid address information stored by the card-issuing bank account. To obtain credit/debit card details, an adversary is able to utilize a web merchant's transaction page in order to speculate the data: the merchant's reply to some transaction attempt is going to state whether the estimate was correct.

A secure electronic payment gateway for a secure e-payment approach can be found in [21]. In the system, a consumer's monetary information is delivered straight to a transaction gateway, known as a Trusted Third Party (TTP), rather than over an Internet merchant. The method was created by secure socket layer (SSL) with RSA utilized to improve the additional relationship in the payment process. A similar RSA algorithm-based universally unique identifier approach is used to avoid fraudulent activity in e-commerce in [22]. An efficient e-payment protocol for the mobile environment is proposed in [23], where mobile consumers can link directly with the merchant. Presently, numerous techniques are utilized for e-commerce payment systems. In this area, we briefly discuss three existing forms of e-commerce payment. A secure e-commerce protocol is explained here, which is a modified form of an efficient e-electronic for mobile users proposed in [23]. The existing systems and their proposed properties are summarized in Table 1.

Table 1. Related work with their properties.

Author	Method	Remarks	Drawback
Izhar et al. [12]	Triple Data Encryption Standard (TDES)	The proposed system designed and implemented a secure electronic payment gateway to provide authorization, confidentiality, integrity, and availability for transactions.	The proposed method is for the local environment. This payment architecture did not address security issues (i.e., non-repudiation and anonymity).
Nwoye [16]	RSA cryptosystem	The proposed system implemented an RSA e-commerce security system (RSA-ESS), which addresses the security and privacy difficulties with credit card information in e-commerce transactions. In this system, RSA is used to secure payment information and achieve the required speed in an e-commerce transaction.	The proposed system can be used only for the security and privacy of payment information.
Zay Oo [21]	RSA cryptosystem	Through this method, a customer's monetary data (credit or debit card information) are sent straight to a payment gateway, also called TTP, instead of directing them through an online merchant.	The payment gateway plays an essential role as each of the entities communication is concluded in the transaction gateway for the fee payment request. Furthermore, the consumer cannot talk interconnectedly in the merchant to the device doing the payment request. The cardholder and private data are kept in cloud servers and might be subject to compromise of cloud products/services with malware and exploitation of potential vulnerabilities in the program implementation of e-commerce services [24].

3. RSA Cryptosystem

RSA was planned and created by Ron Rivest, Adi Shamir, and Leonard Adleman around 1978 [25]. It is probably the supreme identified cryptosystem for replacing digital or key autograph or perhaps for enciphering chunks of information [26]. The RSA algorithm is the basis of a cryptosystem—a sequence of cryptographic algorithms that are used for special purposes or for specific safety services—that allows public-key encryption and is used extensively for protecting sensitive data, especially if sent via an insecure network such as the Internet [27]. RSA makes use of an adjustable size encryption block along with a variable size key. The RSA algorithm is contingent upon the top number since it is tough to clap the big prime number [28]. It runs on two key numbers to create private and public keys. The sender encodes the idea with the public element of the receiver, and the receiver on buying the idea decrypts it with its own personal key.

RSA usually involves three steps: key generation, decryption, and encryption. RSA has numerous bugs in its strategy and thus is not encouraged for financial use. The most crucial security services that come with RSA are privacy and secrecy, authentication, integrity, and non-repudiation [26], because they prove RSA's being an excellent security public-key cryptosystem. The RSA algorithm has many advantages, namely it has quick encryption and verification processes; offers a high level of security; and sustains data privacy, non-repudiation, and data reliability [22,26,29]. The approach presented in this research paper requires a high level of safety, which can be effectively achieved and

fulfilled by RSA. The following is the algorithm of the RSA cryptosystem. Figure 2 shows how RSA public Key Cryptosystem works [30].

To generate the encryption and decryption keys, we can proceed as follows.

P and Q both Prime, P ≠ Q

$\emptyset$ = (p-1) (q-1) 1

1 < e <$\emptyset$

gcd (e,$\emptyset$) = 1

Public Key = {e, n}

Private Key = {d, n}

Plaintext Encryption:

M < n

Cipher text: C = Me mod n

Cipher text Decryption:

Plaintext: M = Cd mod n

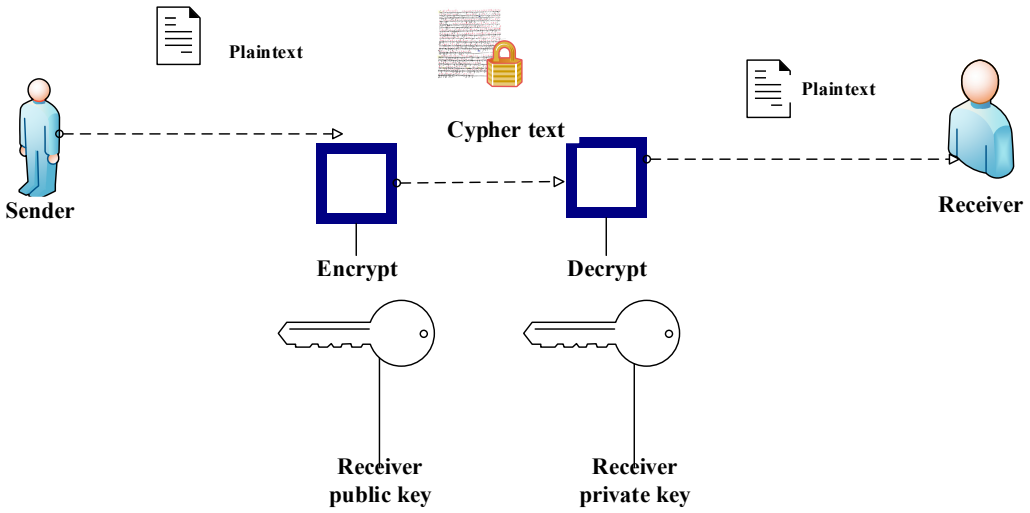

Figure 2. How RSA Public Key Cryptosystem works.

4. The Proposed Method and System Architecture

Security is a key concern and vital issue for the success of e-commerce. In previous work, a secure electronic payment gateway for e-commerce was proposed. In this paper, we propose a secure protocol in e-commerce to enhance the security of the e-commerce process, which can also improve the security of existing work. Interestingly, the proposed system does not require the customer to input his/her identity in the merchant website even though the customer can hide his/her identity and make a temporary identity to process a request for the service. The proposed system is made up of five entities: client (C), merchant (M), payment gateway (PG), user bank (B), and merchant bank.

They perform as follows. Each entity, that is, the client, merchant, user banks, and merchant bank, registers with the payment gateway to create its secret key with the gateway. Secret key elements are necessary to secure communication. Additionally, the user and merchant also create a secret key between themselves. The customer examines the merchant and requests for the product, now with his/her temporary identity created in the merchant website, and the merchant sends the request to the payment gateway. The proposed model of the e-payment system is shown in below Figure 3.

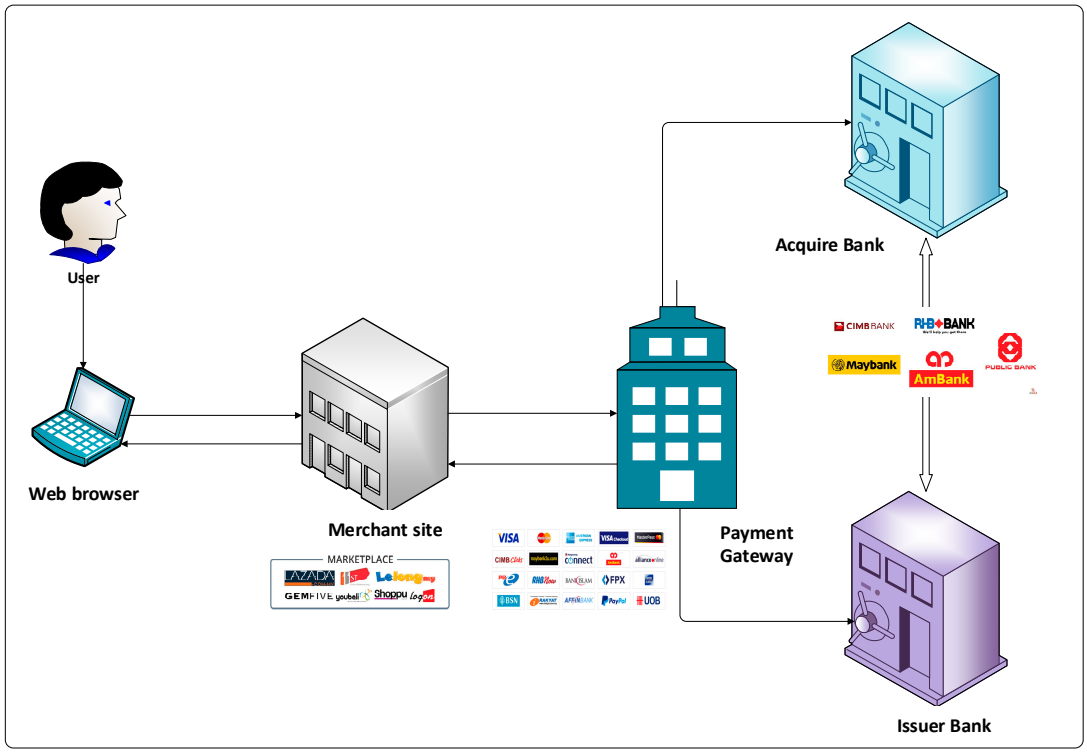

Figure 3. Proposed model of the e-payment system.

The gateway performs several verification steps and forwards the petition to the client's registered bank. At exactly the same time, the payment gateway forwards some encrypted communications to the server. Upon receipt of the quantity subtraction demand, the user bank authenticates it and takes it to the transaction gateway and acknowledges the deduction gateway, after which it sends the authenticated data to the payment gateway. The payment gateway calculates the required result and also forwards it to the bank, wherein the bank captures different versions and amount responses, which are acceptable after verification. The user initiates the transaction by mailing his short-term identity to the server. Be aware that the public key pair continues to be accredited through the certification authority.

4.1. Preliminaries of the Proposed System

- Online customer

A consumer is a person who is going to purchase items by creating payments in a timely manner. In the electronic payment process, an Internet customer is an individual or maybe an organization that gets, consumes, or maybe purchases something online and will choose from various suppliers and goods.

- Merchant

A merchant is an enterprise or a person who offers a service or product. An e-commerce merchant is somebody who offers a service or product solely over the Internet. A merchant sells products to a customer for a price, and, by law, has a duty of hygiene to the consumer because of the expertise of the merchandise he is on the market (e.g., Lazada, Aeon, and Shoppee).

- Client bank

A client bank is a kind of bank that holds the client's account and authorizes him or her during account registration. It generally has the money of numerous customers and is specially designed for the goal of keeping the client's cash on trust (e.g., Maybank, CIMB, and RHB).

- Merchant bank

A merchant bank is a monetary institute, which involves underwriting and company loans, catering mainly to the requirements of big companies and individuals with substantial net worth. In e-commerce, a merchant bank is a kind of bank that permits companies to accept payments through credit or debit cards and is liable for fraud management (i.e., Maybank, CIMB, and RHB).

- Payment gateway

A payment gateway is an essential component of a structure that guarantees worry-free transactions and ensures the common safety among electronic systems. A payment gateway acts as an entrance point to the national banking system [8]. Every transaction that takes place online is created via payment gateways, which serve as points that economic institutions can access. A payment gateway is attached wholly to consumers, banks, and merchants through the Internet and is responsible for the speed, reliability, and safety of all transactions (i.e., ipay88, FPX, and Mol Pay).

4.2. Design Consideration

E-commerce describes all the deals done over the Internet with the help of digital innovation. Mainly, there is an exchange of money for products or solutions across the boundaries of the organization. In this paper, a secure protocol to enhance the security in an e-commerce system is introduced. This secure protocol makes a temporary identity of the client to provide an extra layer of security in e-commerce systems. Whenever the client sends a request to the merchant site for a search of a product, the secure protocol first generates a client's temporary identity to protect client information. Thus, if anything goes wrong during request processing or any malicious data are found, the protocol discards the request and terminates the entire transaction. To understand better, we can classify e-commerce design considerations and challenges separately. From the analysis of the above roles, we can extract some key design considerations for e-commerce.

- Each entity, that is, the client, merchant, user bank, and merchant bank, registers with the payment gateway to create each of their secret key with gateway.
- The client and merchant also create a secret key between themselves.
- The client can connect his/her temporary identity to the merchant site to make an order. After the order has been made, RSA encryption is executed to hide customer card information in order to get ciphertext.
- Once the order has been placed, merchant redirects to the payment gateway for the encryption and decryption processes.
- The client bank along with the client use the RSA signature to execute an electronic signature on the document by making use of the private key.
- The public key set has actually been licensed by a certificate authority.
- The payment gateway executes some verification steps (encryption, decryption, and validation) and forwards value subtraction request to the issuer and some encrypted message to the acquirer. The primary purpose of this system is to create public and private keys for traders and banks. It stores keys in the key database to be distributed to customers after the key generation process. In the decryption process, RSA collects the customer's card details after receipt of the ciphertext from the customers and decrypts the ciphertext. The payment gateway validates the authorization for the payment phase after the customer's card details have been decrypted.
- The ciphertext is decrypted by RSA decryption to get the customer's card information from the bank's website after it receives the ciphertext from the payment gateway. After the customer's card details have been decrypted, the bank shall validate the payment transaction, on the basis of the client's confirmation. Following the transaction, the bank will then inform the customer and the merchant of the payment confirmation.

4.3. Transaction Phase

The customer begins the transaction by mailing his/her momentary identity to the server. In the entire transaction process, the customer immediately contacts the merchant, while, for interaction with the account, the payment gateway was demanded both by the merchant and by the customer to facilitate contact. The symbols used in the transaction phase are as follows:

TIDc—temporary identification of client
IDC—the identity of the product
G—goods details including price, date, and transaction identification
QC ReQ—value claim request
QC ReS—value claim response
PR ReQ—product request
PR ReS—product response
Vs ReQ—value subtraction request
Vs ReS—value subtraction response

A detail explanation of the process is provided below; "Alice' → Bob: C" indicates a message C is delivered to Bob by Alice. The proposed transaction protocol phase is presented in Figure 4.

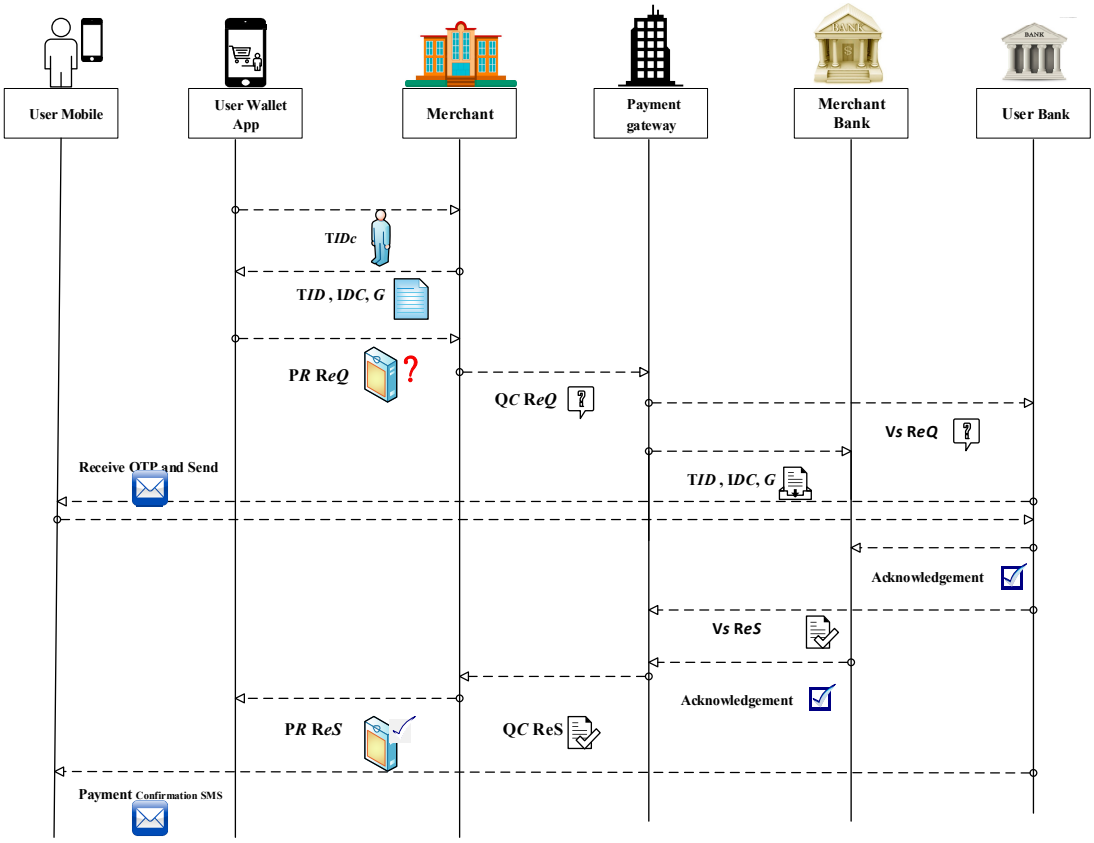

Figure 4. The proposed transaction phase protocol.

Step 1
Start:

Client → Merchant: The client sends a request to the merchant using his/her temporary identity (***TIDc***).

Merchant → Client: The merchant sends back to the client the identity of the product and goods details including price, date, and transaction identification (***IDC, G***).

Step 2

Client → Merchant: The client sends a request for the product (**P*R*** **R*eQ***) to the merchant.

Step 3

Merchant → Payment Gateway: The merchant sends to the payment gateway the value claim request (**Q*C*** **R*eQ***), and the same time payment gateway also (***IDC, G***) to the merchant bank.

Step 4

Payment Gateway → Client Bank: The payment gateway sends the value subtraction request (**V*s*** **R*eQ***) to the client bank.

Step 5

Client Bank → Client Phone: The client bank sends the verification ***OTP*** to the client's mobile phone, and then the client responds to the ***OTP*** verification code. Once verification is complete, the client bank sends an acknowledgment to the merchant bank.

Client Bank → Client: OTP request

Client → Client Bank: OTP response

Merchant → Payment Gateway: Acknowledgment

Step 6

Client Bank → Payment Gateway: The client bank sends the value subtraction response (**V*s*** **R*eS***) to the payment gateway, and the merchant bank sends an acknowledgment to the payment gateway.

Merchant Bank → Payment Gateway: Acknowledgment

Step 7

Payment Gateway → Merchant: The payment gateway sends the value claim response (**Q*C*** **ReS**) to the merchant.

Step 8

Merchant → Client: The merchant sends the product response (**P*R*** **R*eS***) to the client.

Merchant → Client: Acknowledgment

Client Bank → Client: OTP confirmation

Stop:

5. Security Analysis and Advantages

Nowadays, e-commerce is a key component of contemporary businesses. Credit cards or debit cards happen to be popular for remote or on-site transactions, decreasing the demand for inconvenient money transactions. However, along with their popularity comes a substantial number of credit card fraud cases online because of security vulnerability. Solutions have been proposed in the past to avoid the issue, but many of them had been inconvenient and did not satisfy the requirements of merchants and cardholders at exactly the same time. Consumers consider confidentiality, data integrity, authentication, and non-repudiation as essential requirements for creating secure payments over the Web [7,31–34].

- Confidentiality

Confidentiality is important within the e-commerce community because of the chance that hackers might get one's very sensitive information. It is indisputable that, when two parties engage in a transaction, they both usually make sure that it will not be denied. Only an authorized receiver should be able to acquire the encrypted message, so that others cannot read its content [35,36]. In our proposed system, we continually encrypt data before moving it with the additional talking party using the RSA cryptosystem. If opponent A interrupts in between the transaction, it obtains the encrypted note that cannot be decrypted if the key element is missing. Hence, confidentiality is definitely satisfied.

- Integrity

Integrity is one of the major concerns of any company as well as for an e-commerce system. The integrity of the data refers to the concept that information will not be considered a malicious

modification within the system of transmission and that the information is obtained by the receiver at exactly the same time the sender delivered it, that is, the precision of data transmitted to the receiver [37]. The receiver can find out whether any changes were made to the original message. When funds are delivered from customers to suppliers, the integrity of performance should be given particular attention; that is, credit and debit of money must be mapped within an integrated manner.

- Non-repudiation

Non-repudiation signifies that individuals who made a transaction are not able to deny doing it. This means individuals cannot avoid making a payment once electronic signatures are in place. The sender not able to refute he sent a statement. To achieve non-repudiation, plaintext/clear text is used so that people can understand. Ciphertext, which is unreadable to individuals, uses encryption. The reverse procedure is called decryption [36,37]. The issuer makes use of the client's signature to make sure that the legitimate person directs the petition to subtract the payment from his/her bank account. The customer additionally can confirm the issuer's signature. If there are a few issues, the customer along with the issuer cannot deny the fact that they run the signature themselves. Therefore, here non-repudiation is achieved.

- Anonymity

Privacy in e-commerce means anonymity of customers who engage in Internet transactions. The buyer who spends his/her E-cash on something should remain anonymous against the receiver of the cash along with the bank. The possibility for the identity of the buyer to be revealed should happen only when the money is spent illegitimately [38]. Nevertheless, anonymity imposes potential threats, for example counterfeiting, blackmailing, and money laundering. Thus, strengthening anonymity in technologies will ensure the secrecy of the sender's private information and further improve the security of transactions. The examples of personal information that relates to banking are the amount of the transaction and the date and time of the transaction [39]. In our proposed method, the identity of customers is concealed during the transaction, and customers use a short-term identity that is centered on communication. Consequently, it stops the client's anonymity.

- Availability

In e-commerce, services should have accessibility, which not only satisfies the security needs of subjects taking part in a transaction but also provides user comfort. Accessibility is when transactions are done with ease anytime the users wish [40]. Availability describes the accessibility of information resources. In electric payments, availability means prevention against information delays or even removal [41]. The system is liable for delivering, processing, and saving information that will be accessible to those who need it. In our proposed method, every entity is registered with the payment gateway and creates a secret key with the gateway exclusively. Therefore, here availability is achieved.

- Authorization and Authentication

The owners of organizations engaged with financial transactions have implemented different secure authentication and authorization procedures at all stages in order to deter electronic transaction fraud [40]. Only approved users must be eligible on the basis of electronic transfers, and only authorized users must, therefore, be able to access details exchanged for payment [42]. On the other hand, strong client authentication should shield the initiation of online payments besides access [43]. In the proposed method, before the payment procedure, the client bank first asks for client authentication to ensure that the prospect is an authorized person who will receive the verification code to transfer a certain amount from the his/her account to the merchant bank. Therefore, here authorization and authentication are achieved.

Table 2 summarizes the all the security measurements and evaluation that are discussed in Section 5.

Table 2. Security evaluation of the suggested system with related systems.

Parameters	Izhar et al. [12]	Nwoye [16]	Kyaw Zay Oo [21]	Our Proposed Method
Confidentiality	Yes	Yes	Yes	Yes
Integrity	Yes	Yes	Yes	Yes
Non-repudiation	No	No	Yes	Yes
Anonymity	No	Yes	No	Yes
Availability	Yes	Yes	Yes	Yes
Authentication	No	No	No	Yes
Authorization	Yes	Yes	Yes	Yes

6. Conclusions

E-commerce has extremely enhanced in popularity over the last decades, and, in methods, it is changing typical payment methods right into online. With the increasing popularity of e-commerce, the market for digital payments has exploded in the last decades, and payment in e-commerce, particularly mobile payment, is currently extremely preferred and plays a growing role. The principal issue is a better requirement for a secure payment system and online authentication on the client side and the Web server side both in growth and in the development of e-commerce. In this research, we suggested an efficient, secure electronic payment system for e-commerce. We introduced a comparison between our suggested framework and the other three existing systems, which use RSA and DES to secure debit/credit card details and keep them anonymous. Most of the clients want an e-commerce program, as there are many advantages. Clients need such a secure system, because it satisfies all specifications and is a sufficient system. We proposed a secure electronic payment system for e-commerce environments on the basis of these requirements. In our proposed method, the transaction gateway functions as a proxy to communicate between the client/merchant and the bank. The security analysis demonstrated that the proposed plan has better protection effectiveness in terms of confidentiality, non-repudiation, integrity, availability, and anonymity. The extension of this article will focus on the utilization of our proposed framework in real-world applications by proving its ability to avoid various attacks and determine the time necessary for electronic payment.

Author Contributions: Conceptualization, M.A.H.; Data curation, M.A.H., Z.S. and M.K.H.; Formal analysis, M.A.H. and Z.S.; Funding acquisition, Z.S. and M.K.H.; Investigation, M.A.H.; Methodology, M.A.H.; Resources, M.A.H.; Software, M.A.H., Z.S., and M.K.H.; Supervision, Z.S. and M.K.H.; Validation, M.A.H. and Z.S.; and Writing—review and editing, M.A.H., Z.S., and M.K.H. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Malaysia Ministry of Education (FRGS/1/2019/ICT01/UKM/01/2) and Universiti Kebangsaan Malaysia - Yayasan Tun Ismail (EP-2018-012).

Conflicts of Interest: The authors declare no conflict of interest regarding this paper.

References

1. Miva. The History of Ecommerce: How Did It All Begin?—Miva Blog. Available online: https://www.miva.com/blog/the-history-of-ecommerce-how-did-it-all-begin/ (accessed on 16 June 2020).
2. Alam, S.S.; Ali, M.H.; Omar, N.A.; Hussain, W.M.H.W. Customer satisfaction in online shopping in growing markets: An empirical study. *Int. J. Asian Bus. Inf. Manag.* **2020**, *11*, 78–91. [CrossRef]
3. Noor Ardiansah, M.; Chariri, A.; Rahardja, S.; Udin, U. The effect of electronic payments security on e-commerce consumer perception: An extended model of technology acceptance. *Manag. Sci. Lett.* **2020**, *10*, 1473–1480. [CrossRef]
4. Soare, C.A. Internet Banking Two-Factor Authentication using Smartphones. *J. Mob. Embed. Distrib. Syst.* **2012**, *4*, 12–18.

5. Satar, N.S.M.; Dastane, O.; Ma'arif, M.Y. Customer value proposition for E-Commerce: A case study approach. *Int. J. Adv. Comput. Sci. Appl.* **2019**, *10*, 454–458. [CrossRef]
6. Narwal, B. Security Analysis and Verification of Authenticated Mobile Payment Protocols. In Proceedings of the 4th International Conference on Information Systems and Computer Networks (ISCON 2019), Mathura, India, 21–22 November 2019; pp. 202–207. [CrossRef]
7. Bezhovski, Z. The Future of the Mobile Payment as Electronic Payment System. *Eur. J. Bus. Manag.* **2016**, *8*, 2222–2839.
8. Masihuddin, M.; Islam Khan, B.U.; Islam Mattoo, M.M.U.; Olanrewaju, R.F. A Survey on E-Payment Systems: Elements, Adoption, Architecture, Challenges and Security Concepts. *Indian J. Sci. Technol.* **2017**, *10*, 1–19. [CrossRef]
9. Liao, X.; Ahmad, K. Factors Affecting Customers Satisfaction on System Quality for E-Commerce. In Proceedings of the 2019 International Conference on Electrical Engineering and Informatics (ICEEI), Bandung, Indonesia, 9–10 July 2019; pp. 360–364. [CrossRef]
10. Mazumder, F.K.; Jahan, I.; Das, U.K. Security in Electronic Payment Transaction. *Int. J. Sci. Eng. Res.* **2015**, *6*, 955–960.
11. Choo, K.K.R. The cyber threat landscape: Challenges and future research directions. *Comput. Secur.* **2011**, *30*, 719–731. [CrossRef]
12. Izhar, A.; Khan, A.; Sikandar, M.; Khiyal, H.; Javed, W.; Baig, S. Designing and Implementation of Electronic Payment Gateway for Developing Countries. *J. Theor. Appl. Inf. Technol.* **2011**, *26*, 3643–3648. [CrossRef]
13. European Union Agency for Cybersecurity. *Algorithms, Key Sizes and Parameters Report—2013*; European Union Agency for Cybersecurity: Eracleon, Greece, 2013; pp. 1–5.
14. Liu, J.; Xiao, Y.; Chen, H.; Ozdemir, S.; Dodle, S.; Singh, V. A survey of payment card industry data security standard. *IEEE Commun. Surv. Tutor.* **2010**, *12*, 287–303. [CrossRef]
15. Pandey, A. Credit Risk Assessment of Payment Gateway Loans for Working Capital Funding of E-Commerce Industry. *Int. Educ. Sci. Res. J.* **2018**, *4*, 2–6. [CrossRef]
16. Nwoye, C.J. Design and Development of an E-Commerce Security Using RSA Cryptosystem. *Int. J. Innov. Res. Inf. Secur.* **2015**, *2*, 2349–7017.
17. Kaur, J.; Singh, H. E-Banking Adoption: A Study of Privacy and Trust. *Int. J. Technol. Comput.* **2017**, *3*, 314–318.
18. Musaev, E.; Yousoof, M. A Review on Internet Banking Security and Privacy Issues in Oman. In Proceedings of the 7th International Conference on Information Technology (ICIT 2015), Chiang Mai, Thailand, 29–30 October 2015; pp. 365–369. [CrossRef]
19. Rajendran, B.; Pandey, A.K.; Bindhumadhava, B.S. Secure and privacy preserving digital payment. In Proceedings of the 2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), San Francisco, CA, USA, 4–8 August 2017; pp. 1–5. [CrossRef]
20. Ali, M.A.; Arief, B.; Emms, M.; Van Moorsel, A. Does the Online Card Payment Landscape Unwittingly Facilitate Fraud? *IEEE Secur. Priv.* **2017**, *15*, 78–86. [CrossRef]
21. Zay Oo, K. Design and Implementation of Electronic Payment Gateway for Secure Online Payment System. *Int. J. Trend Sci. Res. Dev.* **2019**, *3*, 1329–1334. [CrossRef]
22. Hajira Be, A.B.; Balasubramanian, R. Developing an enhanced high-speed key transmission (EHSKT) technique to avoid fraud activity in E-commerce. *Indones. J. Electr. Eng. Comput. Sci.* **2018**, *12*, 1187–1194. [CrossRef]
23. Mohit, P.; Amin, R.; Biswas, G.P. Design of Secure and Efficient Electronic Payment System for Mobile Users. In *International Conference on Mathematics and Computing*; Springer: Singapore, 2017; Volume 1, pp. 34–43. [CrossRef]
24. European Union Agency for Network and Information Security (ENISA). *Security of Mobile Payments and Digital Wallets*; ENISA: Eracleon, Greece, 2016; ISBN 978-92-9204-199-1.
25. Sharma, M.K. Electronic Cash over the Internet and Security Solutions. *Int. J. Adv. Res. Comput. Sci.* **2017**, *8*, 229.
26. Sharma, N.; Bohra, B. Enhancing Online Banking Authentication using Hybrid Cryptographic method. In Proceedings of the 3rd International Conference on Computational Intelligence and Communication Technology, Ghaziabad, India, 24–26 November 2017; pp. 1–8. [CrossRef]

27. Rouse, M. What is RSA algorithm (Rivest-Shamir-Adleman)?—Definition from WhatIs.com. Available online: https://searchsecurity.techtarget.com/definition/RSA (accessed on 16 June 2020).
28. Balilo, B.B.; Gerardo, B.D.; Byun, Y.; Medina, R.P. Design of physical authentication based on OTP KeyPad. In Proceedings of the 2017 International Conference on Applied Computer and Communication Technologies (ComCom), Jakarta, Indonesia, 17–18 May 2017; pp. 1–5. [CrossRef]
29. Susanna, A.; David, S.; Kathrine, J.W.; Esther, A.G. Enhancing user authentication for mobile wallet using cryptographic algorithm. *J. Adv. Res. Dyn. Control Syst.* **2018**, *10*, 891–897.
30. Sönmez, F.; Abbas, M.K. Development of a Client/Server Cryptography-Based Secure Messaging System Using RSA Algorithm. *J. Manag. Eng. Inf. Technol.* **2017**, *4*, 6.
31. Ibrahim, R.M. A Review on Online-Banking Security Models, Successes, and Failures. In Proceedings of the 2018 International Conference on Electrical, Electronics, Computers, Communication, Mechanical and Computing (EECCMC), Tamil Nadu, India, 28–29 January 2018.
32. Khrais, L.T. Highlighting the Vulnerabilities of Online Banking System. *J. Internet Bank. Commer.* **2015**, *20*, 120. [CrossRef]
33. Poeng, K.P.; Chukwuere, J.E.; Agu, N.T. The issues affecting employees' adoption of online banking in mahikeng. In Proceedings of the 2nd International Conference on Information System and Data Mining, Lakeland, FL, USA, 9–11 April 2018; pp. 70–75. [CrossRef]
34. Hassan, M.A.; Shukur, Z. Review of Digital Wallet Requirements. In Proceedings of the 2019 International Conference on Cyber Security (ICoCSec), Negeri Sembilian, Malaysia, 25–26 September 2019; pp. 43–48. [CrossRef]
35. Karim, N.A.; Shukur, Z. Review of user authentication methods in online examination. *Asian J. Inf. Technol.* **2015**, *14*, 166–175. [CrossRef]
36. Shaju, S.; Panchami, V. BISC authentication algorithm: An efficient new authentication algorithm using three factor authentication for mobile banking. In Proceedings of the 2016 Online International Conference on Green Engineering and Technologies (IC-GET), Coimbatore, India, 19 November 2016; pp. 1–5. [CrossRef]
37. Hua, J. Study on mobile E-commerce security payment system. In Proceedings of the International Symposium on Electronic Commerce and Security (ISECS 2008), Guangzhou, China, 3–5 August 2008; pp. 754–757. [CrossRef]
38. Serrano, M.E.; Godoy, S.A.; Gandolfo, D.; Mut, V.A.; Scaglia, G.J.E. A Simple Off-line E-Cash System with Observers. *Inf. Technol. Control* **2018**, *47*, 118–130. [CrossRef]
39. Omariba, Z.B.; Masese, N.B. Security and Privacy of Electronic Banking. *Kidney Int. Suppl.* **2013**, *3*, 262. [CrossRef]
40. Kang, J. Mobile payment in Fintech environment: Trends, security challenges, and services. *Hum. Cent. Comput. Inf. Sci.* **2018**, *8*, 32. [CrossRef]
41. Bahtiyar, Ş.; Gür, G.; Altay, L. Security Assessment of Payment Systems under PCI DSS Incompatibilities. In *IFIP International Information Security Conference*; Springer: Berlin/Heidelberg, Germany, 2014; pp. 395–402. [CrossRef]
42. Khattri, V.; Singh, D.K. Implementation of an Additional Factor for Secure Authentication in Online Transactions. *J. Organ. Comput. Electron. Commer.* **2019**, *29*, 258–273. [CrossRef]
43. European Central Bank (ECB). *Recommendations for the Security of Internet Payments*; European Central Bank (ECB): Frankfurt, Germany, 2013; pp. 1–26. ISSN 978-92-899-0866-6.