

Card Payment Security Using RSA

Sejal Kaul

Department of Computer Science
Engineering,

Manav Rachna International Institute of
Research and Studies

Manav Rachna Campus Rd, Gadakhor
Basti Village, Sector-43, Faridabad,
Haryana 121004

Aayush Garg

Department of Computer Science
Engineering,

Manav Rachna International Institute of
Research and Studies

Manav Rachna Campus Rd, Gadakhor
Basti Village, Sector-43, Faridabad,
Haryana 121004

Sanya Sharma

Department of Computer Science
Engineering,

Manav Rachna International Institute of
Research and Studies

Manav Rachna Campus Rd, Gadakhor
Basti Village, Sector-43, Faridabad,
Haryana 121004

Rishika Arora

Department of Computer Science
Engineering,

Manav Rachna International Institute of
Research and Studies

Manav Rachna Campus Rd, Gadakhor
Basti Village, Sector-43, Faridabad,
Haryana 121004

Priyanka Grover

Department of Computer Science
Engineering,

Manav Rachna International Institute of
Research and Studies

Manav Rachna Campus Rd, Gadakhor
Basti Village, Sector-43, Faridabad,
Haryana 121004

Abstract— Security is the most important aspect when it comes about the payment transactions on the internet. The internet is not a secure and dependable source these days, when the data is being enormously stored over the network. E-commerce applications are exposed to a variety of security pressures. The electronic payment system must be protected for participants in Internet transactions, such as payment gateway servers, bank servers and commercial servers. The system's security architecture is supported by the use of a lot of security protocols and approaches that reduce fraud that takes place with theft. Mastercard or revolving credit card payment data and customer data. In this post, we explain that a reliable communication channel technology could also be a reliable e-payment system that can secure standard transaction data.

Keywords— Client, card payment, RSA, encryption, decryption.

I. INTRODUCTION

In the e-commerce industry, the security techniques are continuously challenged in the growing world of cyber-attacks. As a result, there is a huge demand for efficient security techniques that can secure the credentials of an authorised user and can ensure as high a level of security as possible. The modes of payments that majorly include mobile payment and electronic payment are broadly divided into three major categories, that are as follows:

- Credit Card based transaction method
- Check based e-payment method
- Electronic cash transaction method
- E-card transaction does not assist offline payment and requires multi-party online certification and the

transfer of information between buyers, merchants, banks and credit card service providers during each payment process. This payment failed to protect consumer privacy and information about each business is easily accessible through the credit card section. Paying by credit card is a critical "deferred" mode of payment and allows for an overdraft.

- The check-based electronic payment system could support offline payments, and couldn't expect a payment rejection and an overdraft from the customer. Supports secure sales along with a person's transaction information within a transaction.. A payment gateway defends the transaction data by encrypting the confidential data to ensure that information is transmitted securely between a consumer and therefore the transaction processor. To support security between individual items, especially between the customer and thus the payment over the Internet or the commercial gateway, some strategies are recommended. People especially let's say online shoppers should feel confident that their banking or personal details are secured and hidden.

- The Electronic-cash payment is part of the prepaid transaction system, where the user receives the Electronic-cash, which is not directly connected with any account and assists offline transactions. So in comparison to the previous transaction options. Cash transaction has these security options:

Anonymous: Third party was unable to retrieve historical payment data and cannot obtain consumer information, The World Health Organization initiated payment for the entire payment transaction, it could not even be determined whether two payments were initiated by the same consumer or number.

Offline: The E-cash bought by the consumer at the bank can definitely be reserved offline.

Unrepeatable: the consumer could not repeatedly pay for the electronic money they already used.

Transactional independence: like paper money, the consumer can perform E-cash authentication and complete all transactions without involving the bank.

Precisely, it can be concluded that there is a unit of various Electronic-cash transaction systems, while the most important unexceptional area units like Apple Pay, PayPal, Bitcoin, Amazon Pay, etc., then move on to Electronic-cash. is compatible with the current Electronic-cash transaction system, this document suggests a completely independent secure Electronic-cash transaction subject. The theme could satisfy the demand for Electronic-cash with just some public keys that support the ownership of the module operation and solve the problem of change of payment through victimisation of blind signature and direct signature. Therefore, the planned theme can be used well for online electronic-commerce transactions.

Algorithm used:

The RSA (Rivest Shamir Adleman) algorithm is an asymmetric cryptographic algorithm used to encrypt and decrypt messages. Asymmetric means that it consists of two different keys. This is often referred to as public key cryptography, as one of the keys is kept public while the other key must be kept private. The algorithm is based on the fact that finding the factors of a very large number is difficult: if the factors are prime no., it is called prime factorization. It is also a public key and a private key generator key pair. RSA also consists of keys private and public. The common public key is kept public and is used to encrypt messages. Messages can be encrypted with a full public key and can only be decrypted with the help of a private key.

It is an asymmetric encryption technique with the following steps as it's procedure:

- i. Let p = prime
- ii. q = prime
- iii. $n = p * q$
- iv. totient $(\Phi) = (p-1) * (q-1)$
- v. e = exponent $1 < e < \Phi$
- vi. $\text{Gcd}(e, \Phi) = 1$
- vii. d = private key $d = e^{-1} \pmod{\Phi(n)}$
- viii. public key = $\{e, n\}$
- ix. private key = $\{d, n\}$
- x. plaintext encryption: plaintext mod $n = C$

- xi. cyphertext decryption: cyphertext mod $n = P$

II. PROBLEM DEFINITION & REQUIREMENT ANALYSIS

The basic problem definition in the proposed project is regarding a safe successful transaction from the client side to the merchant. The proposed project aims at resolving the issue of securing the sensitive credentials of the user which are being entered online in order to implement the transaction.

Also, the second problem which is being observed through this project is regarding the authentication of the client before making the transaction a success. This parameter will be covered by sending an unique OTP on the registered email of the user.

III. DESIGN & IMPLEMENTATION

The key concept behind the proposed project is to cover all the aspects of safe and secured transactions through a properly built gateway with ideal frameworks via which all the transactions will take place.

The proposed architecture consists of the following entities:

- Client
- User Bank
- Payment Gateway
- Acquirer
- Merchant

Client:

The buyer may be the one to receive the items by creating payments at the right time. In the process of electronic payment, the Internet the customer is a private company or even acquire, eat, or even own you buy something online and you can choose between different providers as well goods.

User Bank:

The customer bank may be the bank that holds the account account as well authorizes him at the time of customer registration. They usually possess money of various clients and is specially made for the ultimate motivation customer money on loyalty.

Payment Gateway:

The payment gate is an integral part of the structure ensures trouble-free transactions and ensures normal security in between electrical systems. The payment gateway serves as an access point for the country-wide banking industry. All online transactions are processed through payment gateways, which operate pointing to economic institutions. The payment gateway is completely appended to clients, banks, with web advertisers and is answerable for the reliability, speed, and security of all the transactions.

Receiver:

A receiver might be a financial institution that specializes in underwriting and business loans, primarily for large corporations and high-net-worth people. In e-commerce, an acquirer might be a quiet bank that permits businesses to take credit or debit card payments and manages fraud.

Merchant:

Merchant is a business or individual who possesses a service or product. An E-commerce merchant is an individual who possesses a service or product on the web in particular. The merchant offers products to the client at a reasonable cost, and, legally, imposes a clean duty on the purchaser because of the innovation of deals that are not available on the market.

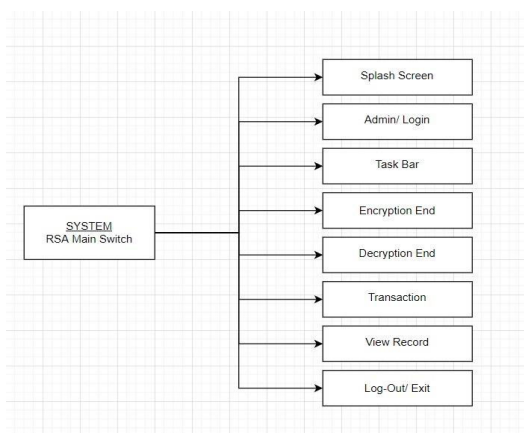
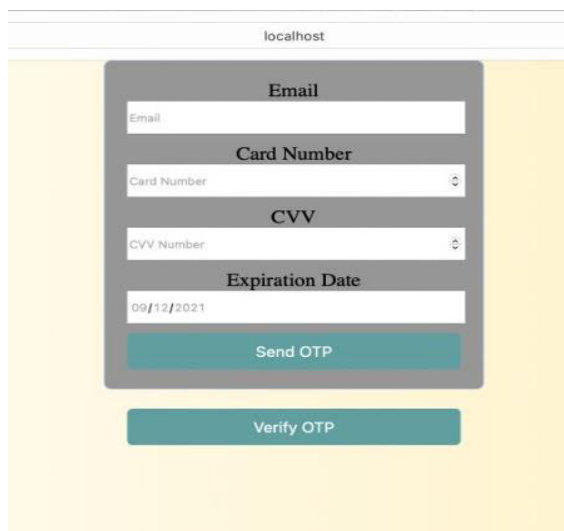
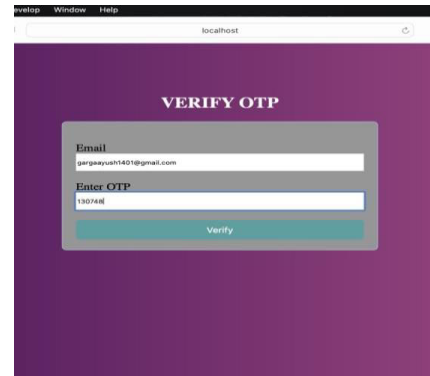


Fig. (i) Basic Architecture of the platform



The screenshot shows a web form titled 'Credentials Page' on a localhost browser. The form has a yellow background and contains the following fields: 'Email' (with a placeholder 'Email'), 'Card Number' (with a placeholder 'Card Number'), 'CVV' (with a placeholder 'CVV Number'), and 'Expiration Date' (with a placeholder '09/12/2021'). Below these fields are two buttons: 'Send OTP' and 'Verify OTP'.

Fig. (i) Credentials Page



The screenshot shows a web page titled 'Verification Page' on a localhost browser. The page has a purple background and contains a form with the title 'VERIFY OTP'. The form has two input fields: 'Email' (with a placeholder 'gargapayush1401@gmail.com') and 'Enter OTP' (with a placeholder '130748'). Below these fields is a 'Verify' button.

Fig. (iii) Verification Page



Fig. (iv) Verification Successful

IV. METHODOLOGY

The customer, receiver, user bank, and merchant all register with the transaction gateway in order for each of their secret keys to be used for accessing the gateway. A private key is additionally made between the client and the merchant for communication purposes.

To complete the purchase, the client can connect their temporary identity to the merchant site. After the transaction is finished, RSA encryption is utilised to encrypt the client card data and produce ciphertext. This shows up in the form of OTP on the gadget of the approved client.

When an order is placed, the merchant refers the client to a payment gateway for encryption and decryption. The user bank and the client utilises the RSA algorithm so as to create a one-of-a-kind electronic signature with the use of a private key.

The payment gateway performs encryption, decryption, and validation prior to sending the value deduction request. The primary objective of this strategy is to generate public and private keys for merchants and banks. After the key creation

process, it stores keys in the key database to be given to customers..

Following receipt of the ciphertext from the purchasers, RSA gets the client's card information and decrypts the ciphertext.

After the client's card information has been encrypted, the payment gateway checks the authorization for the payment phase.

At a point, when the bank gets the ciphertext from the payment gateway, it utilises RSA decryption to extract the client's card data from the bank's website.

After decoding the client's card data, the bank must authenticate the transaction based on the customer's validation. The bank then, at that point tells the client and the merchant of the transaction validation succeeding the payment.

TABLE I. APPROACH FOR CARD PAYMENT SECURITY

AES	SHA	RSA
The AES algorithm is a data encryption and decryption symmetric block cypher. Encryption converts plain text content into cipher text, which is indecipherable, while decryption converts cipher-text back to plain-text. The AES algorithm can encrypt and decode data in 128-bit blocks using cryptographic keys of 128, 192, or 256 bits.	A set of cryptographic hash functions is known to be the secure hash algorithm. SHA is a cryptographic algorithm that is used to hash data, certificate files, and other cryptographic applications, including in cryptocurrencies like bitcoin. These hashing algorithms contribute to the security of current internet infrastructure's backbone.	Asymmetric cryptography is used by RSA algorithm which makes use of both the keys private and public. The key which is shared openly is public key and the other which isn't distributed amongst anyone is private key.

CONCLUSION

The principal issue in today's technologically advanced world is regarding a better and secured payment system interface along with online verification on both client and the server edge both of them in expansion and within the flourishing of electronic commerce. During this study, we made a structured and secured e-payment gateway set-up for electronic commerce transactions. Our introduced set-up and other remaining set-up which made use of DES and RSA to assure

credit/debit card information and let them be concealed were compared. There are many e-commerce programs which most of the clients want to have, as there are a lot of benefits. There is a requirement of such a set-up as it fulfils all the needs and is an adequate set-up.

We suggested a protected e-payment set-up for the electronic commerce domain on the basis of the needs we knew. The payment portal acts as a substitute to connect the bank and the client. The protection examination indicated the introduced method has a good impact in administration of confidentiality, anonymity, integrity, non-repudiation, availability.

FUTURE ENHANCEMENTS

In this project, we aimed to make a secured platform for payment where transactions can be safer and more secured. For the above purpose, we used the RSA algorithm to provide a secure platform and encrypted the credentials of the authorized user. Future enhancements for this project would be that we will be adding a grid method in this project for the further authentication purpose. Also, we will be using hashing techniques to make our platform more reliable for safer transactions.

ACKNOWLEDGMENT

The successful realization of the project is an outgrowth of a consolidated effort of people from disparate fronts. We are thankful to Miss Priyanka Grover (Assistant Professor) and for their variable advice and support extended to us without which we could not be able to complete our project for success. We are thankful to Dr. Kritika Taneja, Project Coordinator, Assistant Professor, CSE department for her guidance and support.

We express our deep gratitude to Dr. Tapas Kumar Head of Department (CSE, IBM Program) for his endless support and affection towards us. His constant encouragement has helped to widen the horizon of our knowledge and inculcate the spirit of dedication to the purpose. We would like to express our sincere gratitude to Prof. (Dr.) Harish C. Rai, Dean, FET for providing us the facilities in the Institute for completion of our work. Words cannot express our gratitude for all those people who helped us directly or indirectly in our Endeavour. We take this opportunity to express our sincere thanks to all staff members of the CSE department for the valuable suggestion and also to our family and friends for their support.

REFERENCES

- [1] "D. O. Mahony, M. Perice, H. Tewari. Electronic payment systems for E-commerce. Boston: Artech House, 2003.", <https://repository.dinus.ac.id/docs/ajar/2343->
- [2] "Zhong Ming, Yang Yixian. Electronic cash based on zero knowledge proof[J]", <https://journal.bupt.edu.cn/EN/Y2000/V23/I3/87>
- [3] "Sönmez, F.; Abbas, M.K. Development of a Client/Server Cryptography Based Secure Messaging System Using RSA Algorithm. J. Manag. Eng. Inf. Technol.", https://www.researchgate.net/publication/333802735_Development_Of_A_Client_Server_Cryptography-Based_Secure_Messaging_System_Using_RSA_Algorithm-
- [4] "Hassan, M.A.; Shukur, Z. Review of Digital Wallet Requirements. In Proceedings of the 2019 International Conference on Cyber Security (ICoCSec), Negeri Sembilan, Malaysia, 25–26 September 2019; pp. 43– 48. ", <https://ieeexplore.ieee.org/document/8970996>
- [5] "PHP Send email using php mailer and gmail SMTP", <https://www.youtube.com/watch?v=aBbmo1pi5B0>
- [6] "Rivest Shamir Adleman Wikipedia", [https://en.wikipedia.org/wiki/RSA_\(cryptosystem\)](https://en.wikipedia.org/wiki/RSA_(cryptosystem))
- [7] "Card payment security ", <https://nevonprojects.com/card-payment-security-using-rsa/>
- [8] "Using PHPmailer", <https://www.youtube.com/watch?v=-B1L0O6S-88>
- [9] "Card Payment Security Using RSA", <https://www.jetir.org/papers/JETIR2107241.pdf>
- [10] "RSA Encryption Secure Card Payment", <https://www.youtube.com/watch?v=Gf7zjHRz28c>
- [11] "Houssam El Ismaili, Hanane Houmani, Hicham Madroumi, 'A secure Electronic Transaction Payment Protocol Design and Implementation', IJACSA, Vol. 5, No. 5, 2014, pp:172-180", <http://www.warse.org/IJATCSE/static/pdf/file/ijatcse178922020.pdf>
- [12] "C.-S. Leigh, and K. Y. Chen, "Generating visible RSA public keys for PKI", International Journal of knowledge Security, Vol. 2, No. 2, Springer-Verlag, Berlin, (2004), pp. 103-109.", <https://mscr.org.my/cryptology/proceeding/Cryptology2014.pdf>
- [13] "RSA-BASED SECURE ELECTRONIC CASH PAYMENT SYSTEM", [HTTPS://IEEEXPLORE.IEEE.ORG/ABSTRACT/DOCUMENT/4419522/SIMILAR](https://ieeexplore.ieee.org/abstract/document/4419522/similar)
- [14] "Securing Online Transactions with Cryptography And Secured Authentication Methods", <https://www.ijrte.org/wpcontent/uploads/papers/v8i1/A3278058119.pdf>
- [15] "Everything you should know about payment security", <https://securionpay.com/payment-security/>