Payatron – Secure electronic transaction processing system

Stefan Kostoski
Contemporary Sciences and Technologies
South East European University
Tetovo, Republic of North Macedonia
E-mail: kostoski92@gmail.com

Marika Apostolova
Contemporary Sciences and Technologies
South East European University
Tetovo, Republic of North Macedonia
E-mail: m.apostolova@seeu.edu.mk

2021 10th Mediterranean Conference on Embedded Computing (MECO) | 978-1-6654-3912-1/21/$31.00 ©2021 IEEE | DOI: 10.1109/MECO52532.2021.9459722

***Abstract* - As online transactions continue to grow and become a significant part of the global economy, the ability to accept online payments is becoming more important for businesses. Each e-commerce provider should offer to the customers reliable and secure payment procedures. The procedures should ensure fast payments processing and minimizing the possibility for complains at same time. This would result in faster delivery of goods and encourage customer loyalty. In this paper we are going to present our custom developed system for processing electronic transactions (payment processor) – Payatron.**

Keywords: e-commerce, payment processor, payment, transactions, secure, payment gateway, payment system.

I. INTRODUCTION

Technology is evolving very fast and makes our lives undoubtedly much easier. The Internet has become the basis of all communication, while electronic commerce is becoming more and more current in society. The reasons for switching to this method of shopping are lower costs, simpler procurement of goods and services, better management of storage of the goods, greater marketing opportunities, better customer service, etc. This type of business has changed as the Internet itself has changed. In the beginning, companies used the Internet exclusively for their presentation, but today that is not enough.

E-businesses offers buyers and sellers a new form of communication and the opportunity to create new markets. E-commerce is the process of doing business through computer networks. A person sitting in front of a computer can access all the objects on the Internet to buy or sell products. Worldwide e-commerce emerged in the mid-90s to experience a real expansion over the past decade. Thereby, the number of transactions realized through online sales in developed countries is seriously approaching to the one realized in a traditional selling. There are data that worldwide in 2018 more than 1.4 billion people shopped online, representing almost one-fifth of the world's population [1]. It is important to note that the rapid changes that have taken place in the first 20 years of e-commerce are just the beginning. The twenty-first century will be a period of digital connection of the social and business sector, and the development today can only be predicted. There are estimates that all world trade by 2050 will be based on e-commerce [2].

Because this type of business evolving very fast, the need of secure transactions becomes a critical issue.

II. ONLINE TRANSACTIONS WITH CREDIT CARDS

Credit card payment is most commonly used in e-commerce, it is important to understand how an online credit card transaction works and to discover the strengths and weaknesses of this type of payment system.

An online credit card transaction at first glance is done just like a regular purchase with the same card. However, the big difference is that online sellers never see the card being used, nor can they physically pass it through the card reader, and the transaction is not signed. Online credit card transactions are similar to transactions made through telephone. This type of purchase is called **CNP** (Card - Not - Present) [3] and they are the biggest reason for payments to be later rejected by the buyer.

Because the seller never sees the credit card and does not receive a signature from the buyer when a problem arises, the seller risks disabling and rejecting the transaction, even the seller has already sent the order, or the customer has downloaded the order digitally.

In electronic commerce there are five parties that participate:

1. Buyer,
2. Seller,
3. Clearing house,
4. The seller's bank,
5. The bank that issued the credit card to the buyer.

978-0-7381-3361-4/21/$31.00 ©2021 IEEE

After receiving the credit card payment, the seller must have his own account in a bank or in a financial institution.
As shown in Figure 1, an online credit card transaction begins with a purchase. When a buyer wants to buy something, he adds the products to the cart on the seller's website. When a customer wants to pay for a product, a security tunnel is created over the Internet using the SSL (Security Socket Layer) protocol. SSL encryption provides security in entire process and protects the data from unauthorized intrusion from the Internet. SSL does not identify either vendor or consumer. Both parties must have mutual trust in each other.

When the seller receives the credit card information from the buyer, the program contacts the clearing house. The clearinghouse is a financial intermediary that identifies the credit card and checks the account balance. The clearing house contacts the bank that issued the credit card and then it checks the balance of the account. When the credit card is checked, the bank that issued the card transfers the money to the seller's account. Then the purchase information is sent to the buyer.
Protecting online payment is very important. For example, VeriSign is a leader in providing Internet protection services. This software collects transaction data from the seller's site and then sends it via a payment gateway. Then VeriSign checks whether the buyer is authorized for each specific transaction. At the end of this chain of transactions is the transfer of money to the seller's account.
There are a few limitations to the existing credit card payment system, such as security, risk taken by the seller / buyer. The existing system in terms of security has many weaknesses. Neither the seller nor the buyer is sufficiently protected. The seller may be a criminal organization that collects credit card numbers, and the buyer may use a stolen credit card [4].
Alternative payment systems overcome most of these limitations. The credit card industry itself has made efforts to address the security issue through new standard of Internet protocols called SET (Secure Electronic Transaction).

III. SET (SECURE ELECTRONIC TRANSACTION) PROTOCOL

SET was developed by the SET Consortium, established in 1996 by Visa and MasterCard in cooperation with GTE, IBM, Microsoft, Netscape, SAIC, Terisa Systems, RSA, and VeriSign [5].
The SET transaction process itself is similar to a standard online credit card transaction, except that there are multiple identity verifications. As shown in Figure 1, after filling out the application, the buyer selects the option "payment via SET" and then chooses which credit card to make the payment with (e.g., Visa, MasterCard, Discovery, etc.). When it receives the completed application, the seller's server accesses the buyer's digital wallet in order to collect credit card information. The seller's server verifies the buyer's identity by using the digital certificate within the digital wallet in the same way that the buyer's computer verifies the seller's identity. When the identity is verified, an encrypted message is sent to the seller's server containing all the payment details. The vendor server then sends an encrypted message to the vendor's bank to decrypt it. The clearing house further identifies the seller and the holder of the credit card, so that the transaction is further extended like any other credit card purchase. The seller receives permission to deliver the order, the product is further sent to the buyer and finally it is considered that the funds for that purchase are deducted from the buyer's account.

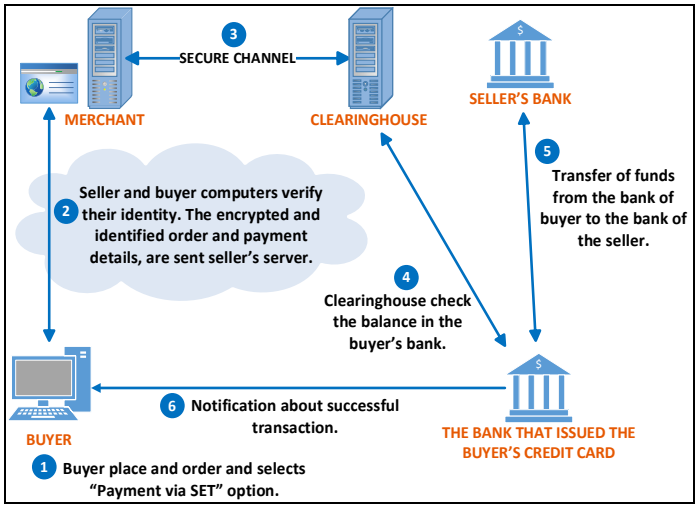

***Figure 1. SET transaction process* [6].**

IV. PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS)

The PCI DSS standard has 6 objectives divided into 12 requirements that every business must fully meet [7]:

- Build and Maintain a Secure Network and Systems
- Protect Cardholder Data
- Maintain a Vulnerability Management Program
- Implement Strong Access Control Measures
- Regularly Monitor and Test Networks
- Maintain an Information Security Policy

PCI DSS standard provides the basis for technical and operational requirements, designed to protect user account data. PCI DSS standards applies to all entities involved in payment card processing, including merchants, payment processors, payment service providers and banks. In addition to these requirements, legislation or regulatory requirements may require specific protection of personal information or other data elements (for example, cardholder name).

PCI DSS standards does not exceed local or regional laws, government regulations or other legal frameworks. By meeting the PCI DSS standards, business activities will improve the security of card transactions and protect cardholder information from theft. Failure to meet these standards leads to severe penalties, loss of customer trust, reduced sales, legal disputes, termination of payment card acceptance rights and even bankruptcy [8].

V. PAYATRON – SECURE ELECTRONIC TRANSACTION PROCESSING SYSTEM

The electronic transaction processing system - Payatron will be easy to use and can be implemented on any platform. For

testing purpose, together with the payment processor we developed custom web store where we will make a payment.

Payment gateways or payment processors are defined as companies that are authorized to process credit card transactions between buyers and sellers. To make a payment through online channels, the customer needs to submit the information from his credit card [9].

Payment portals are also defined as processors for collection of funds through credit card payments or e-cash. The credit card payment processor it is linked to several objects, such as the merchant's website, the merchant's bank, and the credit card holder's bank. Whole this connection is enabled through secure channels.

THE IDEA BEHIND OUR SYSTEM

According to other online payment systems like Braintree acquired by PayPal, which using Ruby programming language for it's back-end operations [10], for our project we have used C# programming language.

The overview of the system architecture can be seen on Figure 2, showing its primary components.

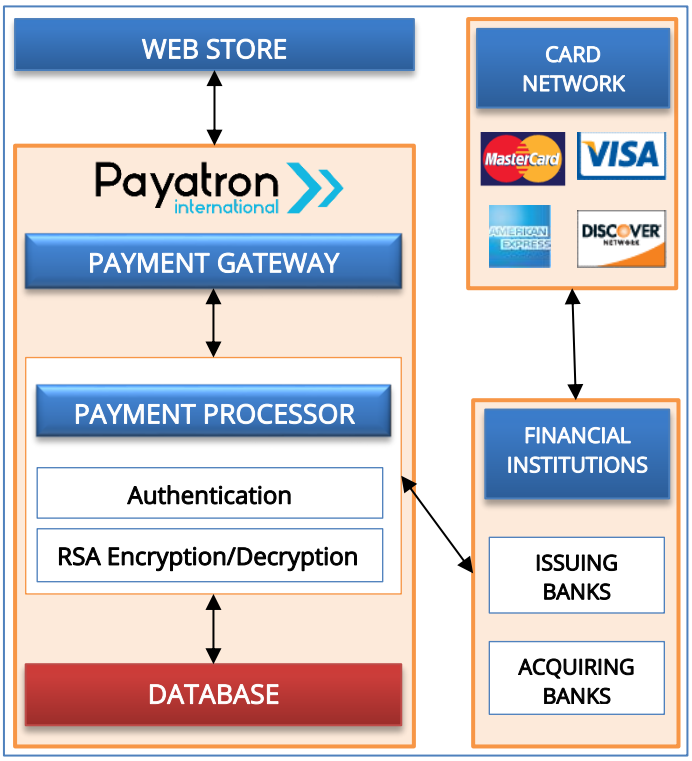

Figure 2. The Payatron architecture.

PROGRAMMING TECHNIQUES AND FRAMEWORKS

As a main framework we have used ASP.NET Core (WebAPI – Application Programming Interface) which is specifically designed for building REST-full services where we have used HTTPS request/response pipeline to transfer data between platforms (e.g., e-commerce website and acquiring banks).

```
// Sign data with Payatron private key
        using (var rsa = RSA.Create())
        {
            RsaExtensions.FromXmlString(rsa, apiSigningKey);
            var aesParams =
CryptographyExtensions.GenerateKey();
            var key =
Convert.FromBase64String(aesParams[0]);
var iv = Convert.FromBase64String(aesParams[1]);
            var serializedModel =
JsonConvert.SerializeObject(model);
            var dataObject = new
            {
               Model = serializedModel,
               Timestamp = DateTime.UtcNow
            };
            var data =
JsonConvert.SerializeObject(dataObject);
            var signature = Convert.ToBase64String(rsa
               .SignData(Encoding.UTF8.GetBytes(data),
HashAlgorithmName.SHA256,
RSASignaturePadding.Pkcs1));
            // Encrypt with acquiring bank public key
            string encryptKey;
            string encryptIv;
            using (var encryptionRsa = RSA.Create())
            {
               RsaExtensions.FromXmlString(encryptionRsa,
bankKey);
               encryptKey =
Convert.ToBase64String(encryptionRsa.Encrypt(key,
RSAEncryptionPadding.Pkcs1));
               encryptedIv =
Convert.ToBase64String(encryptionRsa.Encrypt(iv,
RSAEncryptionPadding.Pkcs1));
            }
            var encryptedData =
Convert.ToBase64String(CryptographyExtensions.Encrypt(
data, key, iv));
            var json = new
            {
               EncryptKey = encryptKey,
               EncrypdIv = encryptIv,
               Data = encryptedData,
               Signature = signature
            };
var serializedJson = JsonConvert.SerializeObject(json);
            var request =
Convert.ToBase64String(Encoding.UTF8.GetBytes(serialize
dJson));
            return request;
}
```

Figure 3. Encryption process of credit card data.

In our project we used the asynchronous programming technique which helped us in supporting multiple requests in parallel, without locking a thread against a long-running process such as credit card data validation.
For the web store we have used ASP.NET MVC Framework where we implement our payment processor.

DATA ENCRYPTION AND DECRYPTION

Payment processors must follow the security standards of international card organizations (for example, Payment Card Industry Standard) which are not only a condition for obtaining a license, but also for its retention. This means that the operation of payment processors, especially from security aspects, is controlled by international card organizations [11].

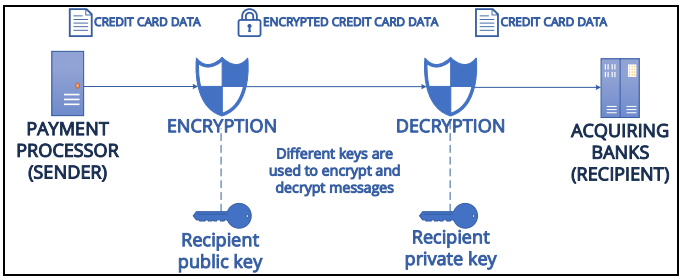

Figure 4. Credit card data encryption and decryption process.

In our project we are using the RSA cryptosystem, sometimes known as the Rivest-Shamir-Adleman algorithm, which is currently the most widely used asymmetric cryptographic scheme. The advantage of this encryption system is that two keys are generated, one public and one private. The Public key encrypts the messages to be sent and the private key decrypts the same messages. At the following code is showed the process of encrypting data from the credit card which payment processor needs to send to acquiring bank. It's important to be mentioned that the public key is used by the payment processor only to encrypt the data and the private key is only used by the acquiring bank to decrypt the data. At Figure 3, is showed the encryption process of credit card data.

FURTHER IMPLEMENTATIONS

Payatron - secure electronic transaction processing system has been developed so that more functionalities can be implemented as well as more modern security systems when purchasing and transacting funds.

The most modern system that can be implemented is the 3D secure system. The 3D secure system performs an automatic computer analysis of each Internet payment to ensure that the right cardholder initiates the transaction. Such background checks provide additional customer protection and prevent abuse before it occurs.
3D Secure is recognized as the highest international standard for the protection of Internet transactions. The mechanism of 3DES Secure is aimed at protection against identity theft of card users and protection against misuse of card data (card number, expiration date and CVC / CVV2 code) [12].

CONCLUSION

As it can be concluded, online shopping and credit card data transfer can be safe if security technologies are used in every process. The implementation of the RSA algorithm ensures secure scheme for sending encrypted messages between different platforms over internet.

REFERENCES

[1] "Global e-Commerce hits $25.6 trillion – latest UNCTAD estimates", Geneva, Switzerland, 27 April 2020.

[2] C. Kaufman, R. Perlman, and M. Speciner, Network Security, second Edition, Prentice Hall, 2002.

[3] Understanding Risk Management in Emerging Retail Payments (September 2008) Authors: Michele Braun, James McAndrews, William Roberds, and Richard Sullivan

[4] Card not present transaction (CNP) – payment card transaction - https://en.wikipedia.org/wiki/Card_not_present_transaction

[5] Merkow, Mark S. (2004). "Secure Electronic Transactions (SET)". In Hossein Bidgoli (ed.). The Internet Encyclopedia. John Wiley & Sons. pp. 247–260. ISBN 978-0-471-22203-3.

[6] K.Laudon, C.Traver, E-Commerce: Business, Technology, Society, 10th ed., Boston, Pearson Education, 2014.

[7] "PCI DSS Quick Reference Guide". Retrieved November 12, 2020.

[8] "Official PCI Security Standards Council Site - Verify PCI Compliance, Download Data Security and Credit Card Security Standards". www.pcisecuritystandards.org.

[9] Symposium proceedings - XVI International symposium Symorg 2018: "Doing Business in the Digital Age: Challenges, Approaches and Solutions" Edited by:Nevenka Žarkić-Joksimović, Sanja Marinković - University of Belgrade, Faculty of Organizational Sciences

[10] How We Built the Software that Processes Billions in Payments - June 29. 2011, https://www.braintreepayments.com/blog/how-we-built-the-software-that-processes-billions-in-payments/

[11] Electronic Payment Systems for E-Commerce Second Edition by Donal O'Mahony, Michael Peirce and Hitesh Tewari

[12] "3DES Encryption and Decryption in Microsoft. NET" - January 2010 by William J BuchananWilliam J Buchanan.