Journal of Information Hiding and Multimedia Signal Processing ©2023 ISSN 2073-4212
Ubiquitous International Volume **14**, Number **3**, September **2023**

Mitigating Man-in-the-middle Attack In Online Payment System Transaction Using Polymorphic AES Encryption Algorithm

Huwaida T. Elshoush

Computer Science Department
Faculty of Mathematical Sciences and Informatics
University of Khartoum, Sudan
htelshoush@uofk.edu

Roua M. Mohammed

Computer Science Department
Faculty of Mathematical Sciences and Informatics
University of Khartoum, Sudan
roua.mortada@yahoo.com

Mona T. Abdelhameed

Computer Science Department
Faculty of Mathematical Sciences and Informatics
University of Khartoum, Sudan
monatharwat274@gmail.com

Amel F. Mohammed

Computer Science Department
Faculty of Mathematical Sciences and Informatics
University of Khartoum, Sudan
amelfadl4997@gmail.com

Received October 2022; revised June 2023

Abstract. *Unquestionably securing online payment systems (OPSs) with its different platforms, viz web applications, mobile applications ... etc., is a vital role. Hence, many researchers have utilized various techniques and methods for eliminating threats distributed across the internet, specifically man-in-the-middle attack. However, there are still some remaining exploitable vulnerabilities. By scrutinizing previous studies, we concluded that the polymorphic advanced encryption standard (P-AES) algorithm can provide the most appropriate security level for monetary transactions. This proceeds in modeling the proposed online payment architecture including the main parties involved in the process, and then applying the dynamic advanced encryption standard on the payment transaction, named OPS_{P-AES}. In the evaluation of the algorithm, we conducted a penetration test, in which the penetrator tries to intrude into the payment process and catch the customer's credentials. Based on the results, we found that our proposed OPS_{P-AES} model confirmed that dynamic P-AES is the most suitable algorithm for securing the online payment transaction and achieving the confidentiality of customer's credentials even from the sophisticated insiders. Assuredly, the experimental results affirms efficacy of the proposed OPS_{P-AES} model and proclaimed its effectiveness.*
Keywords: Online Payment Systems, Man-in-the-Middle Attack, Card-Not-Present, SSL Technique, Polymorphic Advanced Encryption Standard

1. **Introduction.** The growth of the technologies, internet usage and e-commerce services provided the ease for the customers all around the world to purchase their products online without card presence. Online payment methods include credit and debit cards, mobile wallets, mobile payments and electronic cash [1]. The online payment transactions suffer from many vulnerabilities and security issues, violating the customer credentials. Thus, protecting the online payment system is emphasized on customer authentication, confidentiality and data integrity [2–7].
There are actions and parties with different responsibilities involved in processing the online payment. These parties are card-holder/customer, online merchant, payment gateway, card payment network and the issuing bank [8][9].
This research constitutes a relatively new idea which has emerged from the existence of threats and attacks during the online payment transactions. This phenomenon has been widely observed and in order to solve it, there are a lot of used approaches and the most common one is the cryptography which scrambles the information using a strong encryption cipher that suits these payment applications and hence secures the whole payment transaction [10]. One of the common problems that seems to be arising in the environment of online payment systems is man-in-the-middle (MITM) attack. The main goal of this attack is to commit identity theft and fraudulent actions [11, 12].

The secure electronic protocol (SET) is an open standard transaction protocol that was determined and adopted by MasterCard and Visa. SET is an early communication protocol used by the e-commerce websites and facilitates the secure transmission of consumer card information via electronic internet portals. The protocol allows for the verification of customers' card information without the need of card details, hence securing customers credentials from unauthorized access, account theft, et cetera. Each time a transaction happens electronically, by establishing an order or making a purchase, a digital certificate is employed by the SET protocol in order to ensure authenticity and verification of identity of the involved parties in the payment process. These certificates are mandatory for the authentication stage [13].

Secure socket layer (SSL) protocol is a network protocol, which is employed by the payment gateway, merchant, and customer in a way that provides the best level of security. A highly secured communication channel is maintained using SSL protocol which encodes the whole session between two links for security concerns [13, 14]. E-commerce applications utilize SSL protocol in their web portals [15], which is used to secure the point-to-point links – between server and client – at the session layer and supports encryption and key exchange between parties – customer and merchant website - involved in the secure communication [16]. SSL protocol widely provides attributes to validate data integrity during network transmission hence preventing interception.

With the rapid increase popularity of online payment all over the world and recently in our country, we considered the security of personal information against frauds as an important concern and this has motivated the whole idea of this research. Our main objectives is to implement a secure online payment system that achieves the best level of security by applying polymorphic AES encryption algorithm as a solution to mitigate man-in-the-middle attack. Furthermore, the proposed OPS_{P-AES} model is assessed and evaluated using some security penetration tests, thus ensuring that it fits the market, technologies, customers and business to satisfy their needs.

Hence, our contribution can be summarized as follows:

- Securing the online payment system using polymorphic AES (P-AES) encryption algorithm.
- The proposed OPS_{P-AES} model mitigates man-in-the-middle attack.

- Testing the proposed method using penetration tests give evidence to its efficacy.

The remainder of the paper is structured as follows: the recent related work in securing online payments are examined in the next section. Section 3 explicates the proposed method. The experimental results are evaluated and analyzed in section 4. Finally, the paper is concluded in section 5 and some future work is recommended.

2. **Related work.** A succinct study on online payment systems was presented by Khan et al. [1]. They analyzed the previous developments with charts, and discussed the present impacts together with security aspect. One of their considerations is the payment gateway as a fundamental part of the online transactions. Moreover, a detailed comparison with the popularly used online payment systems with different factors is being made. They also mentioned the 3D secure technology as a future consideration.

Additionally, despite of their large-scale use, payment gateways present some security issues. Therefore, came the idea of providing security mechanisms for the payment gateways by research [10]. Recently, due to the growth and the use of internet and network, different encryption methods are used to provide the network and data security. As specified by recent research, AES is the most efficacious in monetary transactions regarding speed, time, and avalanche effect [17].

Ali et al. [18] have presented that there are so many challenges facing online payment landscape. To improve security, a set of software tools were utilized to perform distributed guessing attacks on some commercial known websites, and they have come up with the result that distributed guessing attack is a real threat and attackers can use multiple bots at the same time. They use only the technique of 3D secure as a solution during their experiments. On the other hand, Hudaib [19] has discussed and solved brute force attacks against weak ciphers using SSL technique.
Regarding also brute force attacks, Hole et al. [3] also mentioned that they can be combined with the DDoS attacks to gain more access to the costumer's bank information, besides the cracker uses botnet to run the attacks. They believe that to enhance security, certain banks utilize PIN calculator that obtains one-time password (OTP), hence aim to proffer two-factor authentication. The researchers have put more focus on highlighting the possible attacks for banks to be more aware about what they are facing and to make solutions. Nevertheless, the study faces problems in getting enough data and in altering banks and other large institutions to investigate security weaknesses.
Khrais et al. [20] found that to increase security of customers' data and verify user's identity, there is a need to use strong authentication such as two factor authentication, viz passwords and device fingerprint. The authors give a general overview of the e-banking process and the attacks nature, and focus only on web-based transactions without considering mobile applications which is considered a limitation.
On the other hand, Bhasme et al. [8] agree using combination of techniques: visual cryptography, image steganography, and blowfish algorithm so as to prevent the identity theft in online payment. Using blowfish algorithm as an encryption technique provides a benefit as it is freely available for all users to deploy, but it also has some limitations because of its slow performance compared to others. In contradiction, Welpulwar et al. [9] found that online transactions are nowadays becoming less secure with more vulnerabilities in ATM PIN or ATM card. Accordingly, they combine a technique of cryptography using AES and image steganography that supports customer data privacy and averts data misuse.

Like the encryption techniques mentioned above, Devadiga et al. [11] use the AES encryption algorithm for encrypting client's data, then the key being used for the encryption process is further encrypted using the RSA algorithm. This provides two layers of security by using cryptography itself and thus making the online transaction process more guarded. On the server side of the system fraud detection has been ensured by using data mining technique. Likewise, Mare et al. [21] introduced a secret data communication system consisting of RSA and AES as cryptography techniques with image steganography, focusing on interception as the major attack. The joining of these techniques add to the general trustworthy of a secure communication channel. It represents unidirectional encryption system, where only the receiver can decode, and moreover, an unidentifiable communication stream.

Focusing on the security mechanisms perspective, it has been found that image steganography is sometimes not preferred for its disclosure to some kinds of attacks, such as statistical attacks detecting the secret hidden data; and that happens for various reasons, one of them is the simplicity of stegosystem way of embedding data in a cover image [15]. So many researchers have introduced and developed a method that uses a combined application of text-based steganography and visual cryptography, with some differences in the way of promoting security. For instance, Roy et al. [22] prefer using text based steganography based on Vedic Numeric Code method with visual cryptography in gaining customer confidence and avoiding identity theft, and they promote the security of the payment system by involving another party, Certificate Authority in the payment process. They use the method of steganography technique for too many advantages regardless of some hardness. Later on, More et al. [23] have used the same previous combined method to protect and prevent customer data theft with the technique of OTP for more security concerns especially in the case of Card Not Present (CNP).
Moreover, Akolkar et al. [24] have proposed the same above method that uses text-based steganography and visual cryptography providing two-way authentication, but this time the OTP generation depends on some restrictions during the payment process. The method provides limited information for fund transfer, secures costumer's data, and increases costumer's confidence.
Lately, in response to the rapid growth of internet technology usage, some researchers introduced some enhancements in the AES algorithm, by making it more secure, dynamic and confidential, naming it P-AES [13].

Due to the inferred limitations in the research area for solving the intrusion of man-in-the-middle-attack, we proposed a OPS_{P-AES} method for online payment process to withstand it, together with other security attacks viz. credential exposure.

3. The Proposed OPS_{P-AES} Method.

The proposed method OPS_{P-AES} provides a solution to the online payment process against security threads like credential exposing and man-in-the-middle attack. The main idea is based on the use of secret sharing and certified authority as a trusted third party between the customer who purchases the product, the merchant who provides it, and the payment gateway as a communication between them all. Figure 1 demonstrates the main idea of the process. Moreover, according to [16], the use of SSL protocol will guarantee the security of communication. Furthermore, we used P-AES algorithm in the proposed model to add an additional layer of security. The experiment was conducted to show the validity of the P-AES at securing confidentiality of the payment process, besides measuring the reasonable time for the payment process.

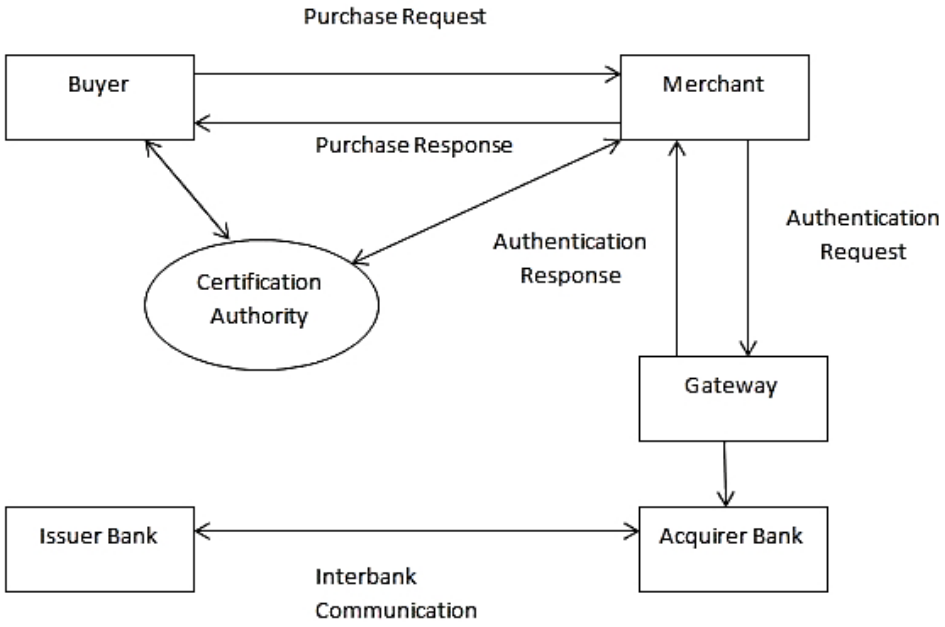

FIGURE 1. The OPS processes [16]

3.1. **The Proposed OPS$_{P-AES}$ Architecture.** The proposed model OPS$_{P-AES}$ emphasizes securing customers information during the transaction process. The model consists of four main parties: customer, merchant website (online shopping website), payment gateway and the issuing bank. Man-in-the-middle attack may occur during each stage of data transmission, as illustrated in figure 2.

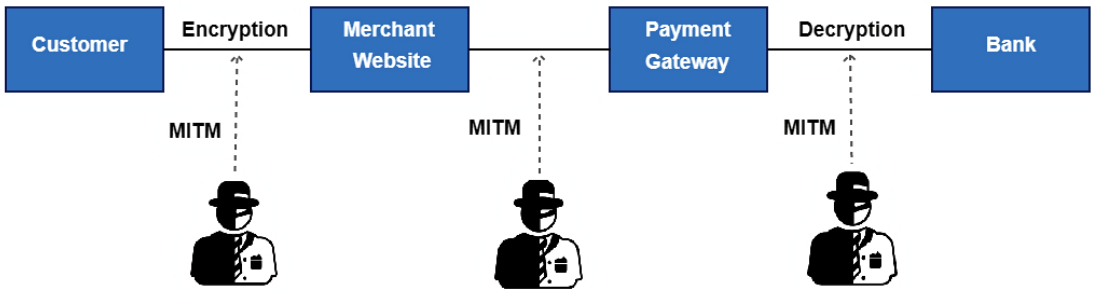

FIGURE 2. The MITM attack throughout the payment process

In this research the focus will only be between the customer, merchant, and the payment gateway. Thus, SSL is used to authenticate and transfer the private data (e.g. Card Verification Value (CVV) that is usually located on the back of the card) by producing a channel that is uniquely encrypted. This protocol is utilized by the payment gateways to deliver a better and secure service for both customers and merchants; using polymorphic AES encryption algorithm [9].

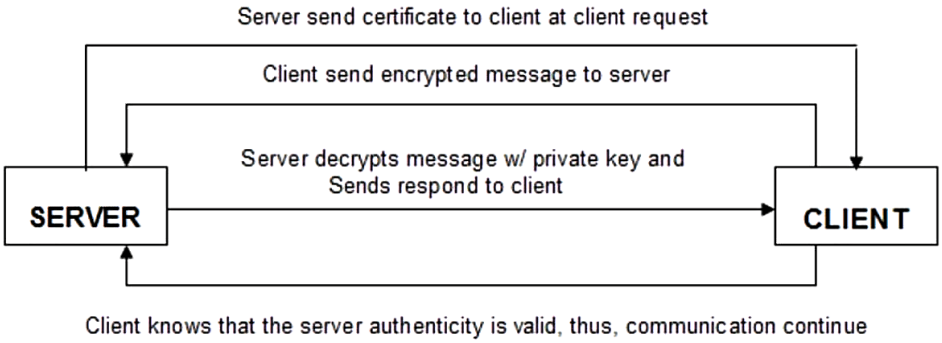

FIGURE 3. SSL Certificate Description [19]

This proposed method uses the SSL handshake sub-protocol, which provides authentication for both server and client. This research uses SSL version 2, which supports the encryption of communication between customer and merchant website with the help of their certificates in some sort of predefined steps.

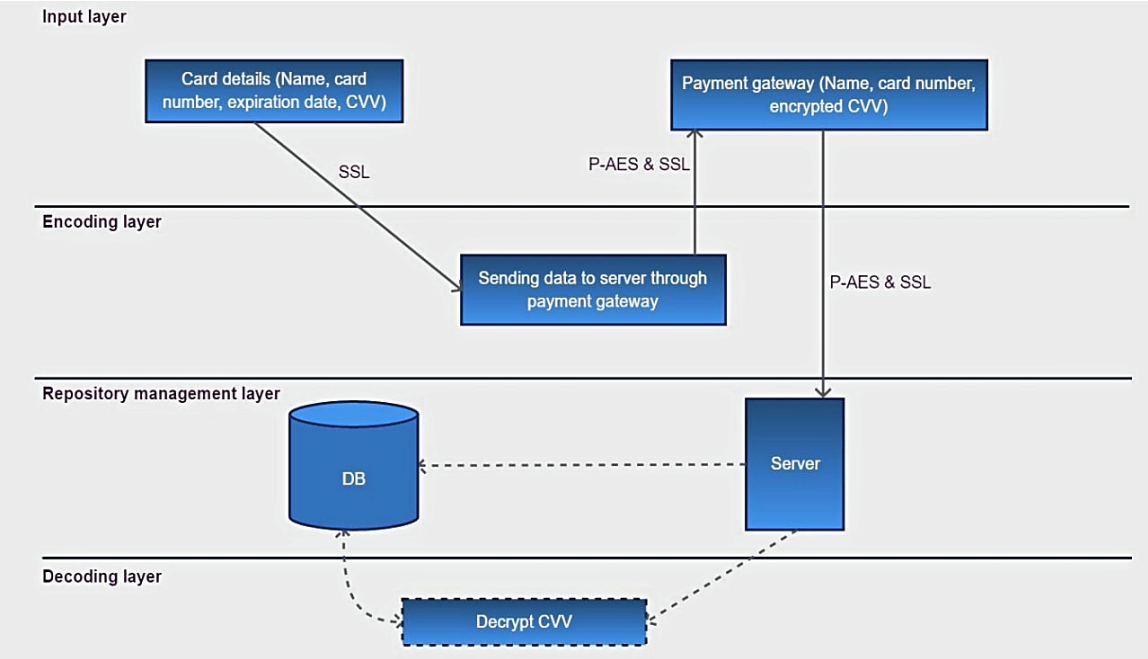

FIGURE 4. The OPS_{P-AES} architecture adopted from [11]

The OPS_{P-AES} architecture consists of four layers where the transaction goes through [11], as depicted in figure 4:

1. **Input Layer** The starter layer from which the transaction takes place. The data in this layer is not encrypted; it will be transmitted to the next layer in the architecture to be encrypted via dynamic AES encryption algorithm.
2. **Encoding Layer** The second layer in the architecture where the encryption process occurs. The CVV of the customer's card is encrypted using dynamic AES encryption algorithm. The data will be transmitted through the payment gateway to the server.
3. **Repository Management Layer** In this layer, the data will be transmitted to be stored in the database repository. Also, the CVV will be transmitted to the decoding layer for the decryption.

4. **Decoding Layer** This is the last layer in the architecture where CVV is decrypted and validated using dynamic AES decryption algorithm. Our proposed model's main concern is in the first and second layers as follows:

3.2. **Polymorphic AES Pseudo Code.** The pseudo codes describing the steps of the P-AES VaryingSubBytes stage, the P-AES VaryingShiftRows stage, and the P-AES VaryingMixColumns respectively in both encryption and decryption operations are as delineated in algorithms 1, 2, 3, 4, 5, and 6 [13]:

Algorithm 1: P-AES Encryption VaryingSubBytes Stage

Input: State Matrix S
Output: NewState Matrix S' (in bytes)
for $i = 0$ *to* 3 **do**
  for $i = 0$ *to* 3 **do**
    $Si, j \leftarrow CyclicallyLeftShift(Si, j, 7 - ByteSubstitutionIndex)$;
    $Si, j \leftarrow S - Box(Si, j)$;
  end for
end for

Algorithm 2: P-AES Decryption VaryingSubBytes Stage

Input: State Matrix S
Output: NewState Matrix S' (in bytes)
for $i = 0$ *to* 3 **do**
  for $i = 0$ *to* 3 **do**
    $Si, j \leftarrow Inverse\ S - Box(Si, j)$;
    $Si, j \leftarrow CyclicallyRightShift(Si, j, 7 - ByteSubstitutionIndex)$;
  end for
end for

Algorithm 3: P-AES Encryption VaryingShiftRows Stage

Input: State Matrix S
Output: NewState Matrix S' (in bytes)
for $i = RowShiftingIndex$ *to* $(RowShiftingIndex+3) mod\ 4$ **do**
  $Rowi \leftarrow CyclicallyLeftShiftBytes(Rowi, i)$;
end for

Algorithm 4: P-AES Decryption VaryingShiftRows Stage

Input: State Matrix S
Output: NewState Matrix S' (in bytes)
for $i = RowShiftingIndex$ *to* $(RowShiftingIndex+3) mod\ 4$ **do**
  $Rowi \leftarrow CyclicallyRightShiftBytes(Rowi, i)$;
end for

Algorithm 5: P-AES Encryption VaryingMixColumns Stage

Input: State Matrix S
Output: NewState Matrix S' (in bytes)
foreach $i = rowi\ 2\ MixColumnsMatrix$ **do**
  $Rowirow(i + ColumnMixingIndex)mod4$;
end foreach
Apply the AES MixColumns using the modified MixColumnsMatrix

Algorithm 6: P-AES Decryption VaryingMixColumns Stage

Input: State Matrix S
Output: NewState Matrix S' (in bytes)
foreach $i = rowi\ 2\ InverseMixColumnsMatrix$ **do**
  $Rowirow(i + ColumnMixingIndex)mod4$;
end foreach
Apply the AES InverseMixColumns using the modified MixColumnsMatrix

Algorithm 7: The OPS P-AES Encryption Algorithm

Data: Customer Credentials Data
Result: Encrypted Credentials Data
for $action = submit$ **do**
  Call : $P - AES \leftarrow CredentialsData$
end for

4. **The Proposed OPS$_{P-AES}$ Method Algorithm.** The proposed OPS$_{P-AES}$ method algorithm is outlined in algorithm 7.

The encrypted data will be transmitted to the server through the payment gateway, considering that the issuing bank has given the authorization response message.

5. **Experimental Results and Analysis.** The implementation phases were deployed using Visual Studio 2019 Community version. The first phase focuses on utilizing a desktop application form to test the encryption of plaintext using the Polymorphic Advanced Encryption Standard (P-AES) cipher with various key sizes (128-bit, 192-bit, 256-bit). Second phase involves displaying a simple web-page portraying the payment method in order to enter the client or customer credentials via textboxes on the page, and all of these credentials will be encrypted using the prior tested P-AES cipher once the customer makes the request using the submit button.

5.1. **Localhost SSL Certificate.** Localhost SSL certificate is a self-signed digital certificate that authenticates a website's identity and permits a secured and an encrypted connection. SSL works as follows:

1. A server seeks connection to an SSL secured web server.
2. The server (or browser) asks the web server to identify itself.
3. The web server responds by sending a copy of its SSL certificate to the server (or browser).
4. The server (or browser) checks the trustworthy of the SSL certificate, and if confirmed proclaims this to the web server.

5. A digitally signed acknowledgment is sent back by the web server to initiate an SSL encrypted session.
6. Finally, encrypted data is shared between the server (or browser) and the web server.

5.2. **Testing Strategy.** Burp Suite is considered as one of the most popular penetration testing tools, it also finds the most dangerous vulnerabilities and is used specifically for checking the security of web applications. The test is done by functional test, which was performed to ensure that the customer's credentials represented on the CVV security code are encrypted properly. By sending a request from the client side to the server side, the packet sent can be intercepted in between and checked if the CVV (the most sensitive information) is encrypted or it is just plaintext as the other credentials.
Algorithm 8 delineates an example of a penetration testing processes when Burp Suite tool operates as a proxy server between a browser and a targeted application.

Algorithm 8: Example of the Burp Suite Penetration Testing of the Proposed OPS P-AES Method

Input:
"amount": 0,
"cardHolderName": "roua",
"cardNumber": "374245455400126",
"cardExpiryMonth": 12,
"cardExpiryYear": 2020,
"cardCvv":"/u9475/uD12F/u3FD1/u957B/u4948/uAB14/u047F/uB371" ;
`// HTTPS request containing customer's credentials`

1 **Screen message = Interception(**$Input$**) Output:**
Plain Text: 1479
Card CVV Cipher Text:
/u9475/uD12F/u3FD1/u957B/u4948/uAB14/u047F/uB371 ; `// unreadable text format or the encrypted CVV with P-AES`

2 **Function** `Interception(`$Input, Output$`):`
3 **Open Burp Suite's embedded browser**
4 **for** $action == intercept$ **do**
5 **web application not responding**
Display : $HTTPS \leftarrow$ **Start** : $intercepting$
6 **end for**
7 **Web application responding**
8 **Return:** $Output$
9 **Print: Screen Message**

5.2.1. *The Burp Suite Penetration Testing Algorithm of the Proposed OPS P-AES Method.*

1. Use the Burp Suite's embedded browser to capture all the traffic, and we can test the HTTPS request.
2. After inserting the customer credentials, but before pressing "submit" go to Burp Suite and start intercepting the going request.
3. In Burp we can see in the browser's request message -after pressing submit- that all the customer credentials are displayed, but the CVV is encrypted.
4. While intercepting there will be no response in our web application, when intercept is off -by clicking forward button- in Burp then the response will appear.

5. Also, with Burp we can see all the HTTPS messages that have been passed through the proxy.

6. **Conclusion.** As a result of continuous advances in online payment systems and sophisticated threats, effective security is needed. To achieve that, the proposed model OPS_{P-AES} is implemented which provides additional layer of security along with SSL certificate to the transaction and mitigates man-in-the-middle attacks that may occur between trusted participating parties or even insiders.
We have examined and proved that by penetration testing using software tools such as web browser inspector, Wireshark and specifically Burp Suit application software represents a proxy between client and server to catch the packet traffic. When the packets were caught by the software, the CVV of customers' cards are still secured because it was encrypted by P-AES. Thus, confidentiality of customers' data is ensured.
As a future work, researchers can enhance the security level using the proposed solutions:

- Ensure the integrity of customers' information when stored in the database using for example risk-based validation.
- Using image steganography to provide an additional layer of security along with used cryptography thus enhancing the data confidentiality and integrity.
- Further security metrics can be measured and analyzed for the proposed model OPS_{P-AES}, to reach more desirable results.

Additional Information - The data is available at GitHub: OPS-code

REFERENCES.

[1] B. U. I. Khan, F. O. Rashidah, A. M. Baba, A. A. Langoo, and S. Assad, "A compendious study of online payment systems: Past developments, present impact, and future considerations, " *Int. journal of advanced computer science and applications*, vol. 8, no. 5, pp. 256-271, 2017.

[2] M. F. Mridha, K. Nur, A. K. Saha, and M. A. Adnan, "A new approach to enhance internet banking security, " *Int. Journal of Computer Applications*, vol. 160, no. 8, 2017.

[3] K. J. Hole, V. Moen, and T. Tjostheim, "Case study: Online banking security, " *IEEE Security & Privacy*, vol. 4, no. 2, pp. 14-20, 2006.

[4] R. Oruganti, S. Shah, Y. Pavri, N. Prasad, and P. Churi, "JSSecure: A Secured Encryption Strategy for Payment Gateways in E-Commerce, " *Circulation in Computer Science*, vol. 2, no. 5, pp. 13-17, 2017.

[5] S. Saxena, S. Vyas, B. S. Kumar, and S. Gupta, "Survey on online electronic paymentss security, " presented at the *2019 Amity Int. conf. on Artificial Intelligence (AICAI)*, pp. 756-751, IEEE, 2019.

[6] F. R. S. Taka, "Secure Communication by combined Diffe-Hellman key exchange Based AES Encryption and Arabic Text Steganography, " *Journal of Information Hiding and Multimedia Signal Processing*, vol. 12, no. 4, pp. 186-198, December 2021

[7] J. Liu, C. Fan, X. Tian and Q. Ding, "Email Encryption System Based on AES Algorithm and DH Algorithm, " *Journal of Information Hiding and Multimedia Signal Processing*, vol. 9, no. 1, pp. 11-20, January 2018

[8] S. Bhasme, A. Arvind , K. Gandhi, and R. Phadnis, "Visual Cryptography and Steganography Techniques for Secure E-Payment System, " *Int Res J Eng Technol*, vol. 3, no. 3, pp. 1018-21, 2016.

[9] A. Welpulwar, P. Kalambe, P. Bhute, and S. Ramteke, "Securing E-Transaction Using Cryptography & Steganography, " *(2018)*.

[10] M. Masihuddin, B. U. I. Khan, M. M. U. I. Mattoo, and R. F. Olanrewaju, "A survey on e-payment systems: elements, adoption, architecture, challenges and security concepts, " *Indian Journal of Science and Technology*, vol. 10, no. 20, pp. 1-19, 2017.

[11] N. Devadiga, H. Kothari, H. Jain, and S. Sankhe, "E-banking security using cryptography, steganography and data mining, " *Int. Journal of Computer Applications*, vol. 164, no. 9, pp. 0975-8887, 2017.

[12] A. Mallik, A. Ahsan, M. M. Z. Shahadat, and J. C. Tsou, "Understanding Man-in-the-middle-attack through Survey of Literature, " *Indonesian Journal of Computing, Engineering and Design (IJoCED)*, vol. 1, no. 1, pp. 44-56, 2019.

[13] A. Altigani, S. Hasan, B. Barry, S. Naserelden, M. A. Elsadig, and H. T. Elshoush, "A Polymorphic Advanced Encryption Standard–A Novel Approach, " *IEEE Access*, vol. 9, pp. 20191-20207, 2021.

[14] Kaspersky, "What Is an SSL Certificate – Definition and Explanation, " *www.kaspersky.com, February 9, 2022. https : //www.kaspersky.com/resource − center/definitions/what − is − a − ssl − certificate.*

[15] M. Douglas, K. Bailey, M. Leeney, and K. Curran, "An overview of steganography techniques applied to the protection of biometric data, " *Multimedia Tools and Applications*, vol. 77, no. 13, pp. 17333-17373, 2018.

[16] A. G. Briones, P. Chamoso, and A. Barriuso, "Review of the main security problems with multi-agent systems used in e-commerce applications, " *ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal*, vol. 5, no. 3, pp. 55, 2016.

[17] G. Singh, "A study of encryption algorithms (RSA, DES, 3DES and AES) for information security, " *Int. Journal of Computer Applications*, vol. 67, no. 19, 2013.

[18] M. A. Ali, B. Arief, M. Emms, and A. V. Moorsel, "Does the online card payment landscape unwittingly facilitate fraud?, " *IEEE Security & Privacy*, vol. 15, no. 2, pp. 78-86, 2017.

[19] A. A. Z. Hudaib, "E-payment security analysis in depth, " *Int. Journal of Computer Science and Security (IJCSS)*, vol. 8, no. 2014, pp. 14, 2014.

[20] L. T. Khrais, "Highlighting the vulnerabilities of online banking system, " *The Journal of Internet Banking and Commerce*, vol. 20, no. 3, 2015.

[21] S. F. Mare, M. Vladutiu, and L. Prodan, "Secret data communication system using Steganography, AES and RSA, " presented at the *2011 IEEE 17th Int. Symposium for Design and Technology in Electronic Packaging (SIITME)*, pp. 339-344. IEEE, 2011.

[22] S. Roy, and P. Venkateswaran, "Online payment system using steganography and visual cryptography, " presented at the *2014 IEEE Students' conf. on Electrical, Electronics and Computer Science*, pp. 1-5. IEEE, 2014.

[23] S. S. More, A. Mudrale, and S. Raut, "Secure Transaction System using Collective Approach of Steganography and Visual Cryptography, " presented at the *2018 Int. conf. on Smart City and Emerging Technology (ICSCET)*, pp. 1-6. IEEE, 2018.

[24] S. Akolkar, Y. Kokulwar, A. Neharkar, and D. Pawar, "Secure Payment System using Steganography and Visual Cryptography, " *Int. Journal of Computing and Technology*, vol. 3, no. 1, pp. 58-61, 2016.