ISSN 2278-3091
Volume 9 No.2, March - April 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse178922020.pdf
https://doi.org/10.30534/ijatcse/2020/178922020

Enhancing the Security of Online Card Payment System

Srivani Bobba[1], Renu Deepti Surapaneni[2]
[1]Department of Information Technology, VNR VJIET, India, srivani_b@vnrvjiet.in
[2]Department of Information Technology, VNR VJIET, India, renudeepti_s@vnrvjiet.in

ABSTRACT

The present on-line card payment system has characteristic security issues caused by the variations in however payment gateways work. This system encourages a disseminated speculating attack. This attack subverts the payment practicality from its planned motivation behind confirmative card subtleties, into serving to the attackers to get all security knowledge fields needed to make on-line exchanges. This distributed guessing attack is feasible because of the heterogeneous security checks created by completely different payment sites. These flaws within the on-line card payment system's security may be improved by remodeling it. The mechanism consists of countering the distributed guessing attack through the implementation of a newly created algorithm that promotes the utilization of a unified security check done at the payment gateway and downscales the system's inability to handle multiple invalid request. Being the time of super computers, the transactional knowledge that is being stored should be encrypted using algorithm that has higher quality whereas breaking down the encrypted data.

Key words: AES, Decryption, Encryption, RSA, SHA-512

1. INTRODUCTION

Cards are the significant methods for paying for online buys. Be that as it may, as the estimation of online deals has expanded, so has the measure of online misrepresentation for instance, UK online deals in 2014 was worth £45 billion, which speaks to a 16% development somewhere in the range of 2013 and 2014. In a similar timeframe, the estimation of hooked up extortion in the UK has expanded by 33% to £217 million [1]. This connected extortion is presently the only one biggest classification of card misrepresentation in the UK, speaking to 45% of the complete estimation of the misrepresentation submitted against UK credit and platinum cards [2]. Right now, present the online installment scene in detail. Specifically, we make a plan of feature the various habits in which online installment is performed, and the shifting safety efforts set up by online dealers[3] – examine just the card number and the expiry date, to completely developed brought together bank roll systems [4], for example, 3D Secure. The number of inquiries we might want to speak: Does the distinction cause a security issue? On the off chance that it does, how regular is the issue and would it be able to be abused? What amount of harm should be possible? What's more, how might it be settled later on? To decide the degree of the issue, we review the 'online installment scene', making a mapping of different shipper installment usage.

We show the viability of misusing the amenabilities with programming which executes the appropriated speculating attack. The effect of these culpability is generous on the grounds that the card subtleties produced by the conveyed assault can be utilized to move cash from an unfortunate casualty's ledger to an unknown beneficiary abroad utilizing a money related administrations organization, for example, the Western Union as a channel [5].

The vulnerabilities portrayed right now to cards that don't uphold brought together checks across exchanges from various locales. Our investigations were directed utilizing Visa and MasterCard as it were. While MasterCard's unified system identifies the speculating attack after less than 10 endeavors (in any event, when those endeavors were disseminated over various sites), Visa's payment environment doesn't forestall the attack. Since Visa is the most well-known payment organize on the planet, the found accountability enormously influence the whole worldwide online installments framework [6].

IEEE have completed a dependable revelation practice with the installment destinations influenced by these vulnerabilities. Of the 342 powerless sites, we introduced our discoveries to the main 36 of these destinations (regarding the seriousness of the amenableness and the relative extent of their client use), observed their reactions, and dissected the progressions these sites have actualized to manage our exposure. Some sites, including the absolute biggest and most mainstream sites on the planet, changed their way to deal with amount preparing after our revelation, as we will report later right now. To ensure the influenced destinations, we avoid explicitly uncovering their identities and their accountabilities. At last, we see the latent answers for the issue. Above all, makes to investigate how present online installment framework works.

2. LITERATURE SURVEY

There are several reasons to improve the security of the online card payment system. The online card security approaches will undoubtedly stay impossible since the dispersed activity upon the distributed internet was not intended for that. A significant number of the arrangements, for example, 3D Secure as it may be viewed as untimely ideas, and they battle to increase far reaching reception [7]. Any arrangement would need to consolidate specialized worries with money related and business operational concerns, and its appropriation will rely upon legitimate and monetary elements. We investigate and talk about these issues from the points of view of the five gatherings.

A. Client/Cardholder: Since the conveyed speculating assault depicted right now shipper sites and card installment system to get all the card subtleties, there isn't a lot of a cardholder can do to forestall it. Simultaneously, the cardholder is seriously affected by the assault: cash might be lost, cards may must be blocked, and the outcome is an exercise in futility and exertion and a diminished suspicion that all is well and good.

B. Online Merchant: Alone, a shipper can do next to no to forestall disseminated speculating attacks. All shippers would need to concur or be compelled to utilize a similar number of fields so the speculating attack can't be organized. Simultaneously, a vendor can abstain from being misused in the assault either by just utilizing cards that utilization an installment arrange that isn't defenseless from the assault, or by utilizing 3D Secure advances prescribed by the installment card enterprises, for example, the American Express 'Safe Key', 'Checked by Visa' and MasterCard 'Secure Code'.

C. Payment Gateway: One can't anticipate that the entirety of the doors should have the option to arrange adequately to forestall the appropriated speculating attack. All things considered, installment entryways can give propelled highlights to their dealers, and these highlights ought to in any event make it increasingly hard to abuse a site for the attack. In particular, entryways may utilize IP address speed channels, which are executed to distinguish rehashed invalid endeavors made inside a specific time length from a similar IP address. However, with no coordination between various portals, these speed channels can undoubtedly be dodged just by changing to a site that uses an alternate installment entryway.

D. Card Payment Network: The clearest protection against the conveyed speculating attack would be at the degree of the card installment organize. In any case, we are not in a situation to know whether installment arrange suppliers could change their system foundation to recognize installment demands from numerous, internationally spread installment portals, searching for suspicious exercises on a solitary card disseminated over different shipper sites.

E. Card Issuing Banks: The bank becomes possibly the most important factor at the last phase of the installment procedure, to support the exchange of assets, yet it would not be involved with every individual supposition (except if 3D Secure is utilized). Banks assume a significant job in constraining the harm that should be possible if aggressors get hold of card data. Numerous giving banks are presently running shrewd misrepresentation identification frameworks which recognize exchanges which are outside their client's ordinary ways of managing money. The giving bank at that point has the alternative to obstruct the installment, or approach the client for affirmation, or acknowledge the installment facing a determined challenge that an exchange might be seen as false later. So, considering the above challenges, in this paper made three modifications of online card payment system.

1. Designing a unified architecture to eradicate the distributed guessing attack.

2. Restricting the limit on invalid entry of a card's details for a single transaction.

3. Encrypting the communication and storing the encrypted form of credit/debit card details in the database.

3. PROPOSED ARCHITECTURE

We see that different sites have different input fields in their payment processing page like some have Card no., Exp, CVV; and some have an additional field as card holder name; some sites don't have cvv, instead they have 3D secure pin. This difference in the input fields and number of fields makes it easy for the hacker to steal the data. Some sites fixed their checkout framework by including a location confirmation field. Be that as it may, this is certifiably not a smart thought since it won't give extra security, yet rather opens up another road for speculating.

So it is recommended for all the merchant sites to use the same architecture for the payment process. Using the unified architecture can

1. Eradicate distributed guessing attack to most extent.
2. Can be implemented with the latest security algorithms.
3. Can be easily updated later in the future.

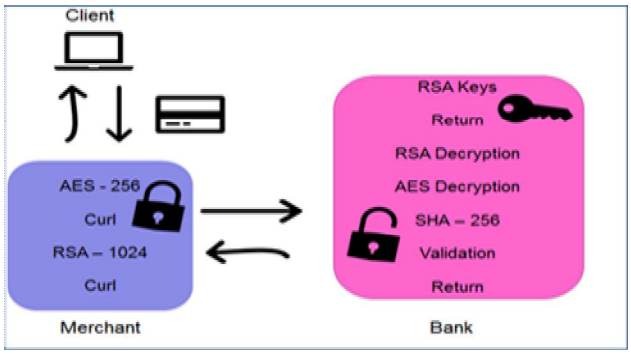

Figure 1: Architecture

Figure1 shows the structural design of communication flow between merchant and the bank.

4. METHOD

Step 1: The user enters his/her credit card details on the merchant site. On submission the data is sent to the merchant server.

Step 2: AES key and AES Initialization Vector (IV) for 256 bit AES encryption are generated.

Step 3: The above generated AES key and AES IV are used to encrypt the data acquired from the merchant site with AES 256 bit in Chain Block Ciphering (CBC).

Step 4: After the encryption, merchant server sends a request to the bank server using cURL for an RSA public key which is required to encrypt AES key and AES IV with RSA 1024.

Step 5: On the reception of RSA public key at merchant server AES key and AES IV are encrypted using RSA.

Step 6: RSA encrypted AES key & AES IV and AES encrypted card details are sent to the bank server using cURL.

Step 7: After the data is received at the bank server, AES key and AES IV are decrypted using RSA private key which is generated along with the RSA public key in Step 4.

Step 8: The decrypted AES key and AES IV are used to decrypt the card details encrypted at merchant server using AES 256.

Step 9: Except the card number, the remaining card details are encrypted using SHA 512 as the details stored in the database are encrypted using SHA 512.

Step 10: The encrypted data is compared with the data present in the database for that particular card number.

Step 11: If the received data and data stored in the database are same, the state of the card is verified. If it is 0, true is returned to the merchant server and at the merchant site transaction successful page is displayed. If it is 1, false is returned to the merchant server along with the time and date at which the card was blocked and the merchant site displays transaction denied page along with date and time.

Step 12: If the received data and data stored in the database are not same, the state is verified. If it is 1, false is returned to the merchant server along with the time and date at which the card was blocked and the merchant site displays transaction denied page along with date and time. If it is 0, count is checked. If the count is 2, it is changed to 0 and state is changed to 1 and false is returned to the merchant site and the message is displayed that the card is blocked.

Step 13: If the state is 0 and the count is not 2, then the count is incremented and false is returned to the merchant server. Transaction denied page is displayed at the merchant site.

4.1 Limit on Invalid Entries

Distributed guessing attack is being successful because there is no limit on the invalid transaction online. It works by randomly guessing the value of any field and trying. For example, expiry month is to be guessed; the maximum attempts would be 12. The hacker tries all the 12 values and succeeds on any one. So in order to avoid this we are imposing a limit for the invalid transactions.

The customer will be given only 3 chances to enter the right detail. If he enters wrong credentials the third time his/her card will be blocked and further transactions on that card will not be possible. To unblock their card they have to contact their bank. This way it would be a tedious and impossible task for the hacker to track the customer's card details because unlike above the intruder will not have 12 chances to guess a field. He only has 3 chances to guess all the fields.

4.2 Encryption & Decryption

Even the communication also must be secure as the attackers can grab the data from our communication means. So the data must be encrypted [8] at the merchant site and decrypted at bank side with the robust algorithm. An attack can also be done on the bank servers so it is necessary to store the data in encrypted form in the servers [9]. We are using the following algorithms to safeguard the user data.

Table1: Algorithms Used

Algorithm	Use
AES (256 bit)	Encrypting the user details at merchant site
RSA (1024 bit)	To encrypt the 256 bit key of AES algorithm
SHA (512)	To encrypt the data in the bank server

The algorithms which have been used for encryption and decryption processes are specified in above Table1.

5. EXPERIMENTAL RESULTS

Firstly, when user enters the card details at the merchant site and submits, they get encrypted at the merchant server using AES (256bit). Then the merchant server requests the bank server to send the RSA [10] public key so that the AES key and AES IV each of 256 bits, are encrypted using RSA algorithm, after the key is encrypted the data is ready to be transmitted to bank.

When bank receives the data, which are RSA encrypted AES key, AES IV and AES encrypted card details, they are decrypted using the bank's RSA private key. Now using the

decrypted AES key and AES IV the user inputted data is decrypted.

Now for verification the decrypted data must be again encrypted using SHA (512) as the details are stored in encrypted form in the bank servers. If the verification is successful then payment is processed and message is sent to the merchant site that transaction is successful. If verification is unsuccessful count is raised by 1 and transaction denied message is sent to the merchant site. And if the count reaches 3 then the card would be blocked and further transactions will not be possible.

If another attempt is made by the genuine user when the card is blocked, he/she will be informed about the card blockage and it will also show the time and date, when the card was blocked.

Figure2 portrays Merchants' online payment design page. Firstly, merchant site has a payment processing page in which the input fields i,e. Card.no, CVV and Expiry date which are mandatory to fill and a 'Order' button that submits the data.

Figure 2: Merchants' online payment page

After entering the data in the first page it is encrypted in the back-end and sent to the bank server. At the bank server it is decrypted and verified with the details in the database. If the verification is successful then it returns true to the merchant server and transaction successful page is displayed. Figure3 portrays transaction successful page. In this page an image is placed that clearly indicates that the transaction successful. There is a text which tells user that 'Your transaction ID and Order details will be sent to your registered mobile number'.

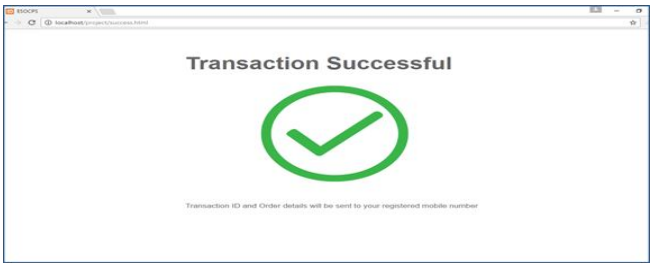

Figure 3: Transaction successful page

If the data that is verified at the bank server are not valid then it returns false to the merchant site and Transaction declined page id displayed that informs the user that details entered were wrong and that page redirects to the payment page in 5 seconds. Figure4 portrays transaction declined page. If it does not redirect, user can click a link 'here' that initiates the redirection.

Figure 4: Transaction Declined Page

Each time the invalid inputs are given there is a count in the database that gets incremented. When the count reaches 3, the card used for transaction will be blocked and user will be notified about this in the transaction declined page with a text in red color- 'Card Blocked'. The below Figure5 portrays the transaction declined page with card blocked.

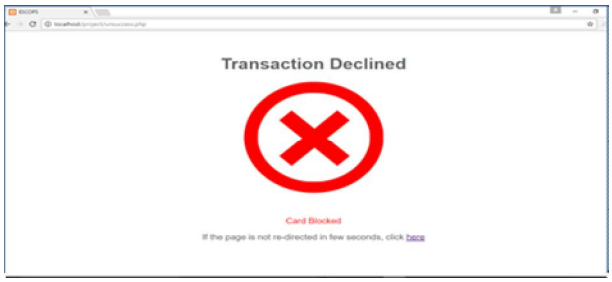

Figure 5: Transaction Declined - Card blocked

When the card is blocked and user tries to make a transaction bank returns the date and time when the card was blocked and it is displayed to the user that card is blocked and date and time is displayed. Figure6 portrays transaction declined and card is blocked since previous invalid transaction at specified time and date.

Figure 6: Transaction Declined – Card blocked previously

6. CONCLUSION

In this paper the major drawback of online payment system i.e., Distributed Guessing Attack and Data Breach's intensity has been reduced. We have successfully eradicated the major flaws that make databases prone to attack in an online payment system or a digital payment system. Not only in a payment system, we can also implement this architecture in where privacy or data security is given a higher priority like

CRM (Customer Relationship Management) and confidential government operations.

In fact, nothing is 100% secured in the world of internet, so a hacker can still hack the database consisting this architecture but the unique thing about this architecture is, it takes 1.9 X 1033 years (Approximately 1 billion billion years) using the current generations' super computers. But, as many new techniques of breaking security algorithm are being developed by the hackers, in coming future there can be a technique that breaks this architecture faster than it takes to hack now. However, this architecture can be updated easily if any new encrypting algorithms that are stronger and better than these algorithms come up, as every merchant will be using this.

REFERENCES

1. A. Aruna, Devansh Sharma, Manikanta Elluru, Subha Sarkar, 'Securing Online Transactions with Cryptography And Secured Authentication Methods', *IJRTE*, Volume-8, Issue-1, 2019, pp: 1424-1427.
2. Irma T. Plata, Edward B. Panganiban and Bryan B. Bartolome, 2019, 'A Security Approach for File Management System using Data Encryption Standard (DES) algorithm', *IJATCSE*-Volume 8 No. 5, pp:2042 – 2048. https://doi.org/10.30534/ijatcse/2019/30852019
3. Monica Thomas and Dr. Varghese S Chooralil, 2019,'Security and Privacy via Optimised Blockchain', *IJATCSE*-Volume 8 No. 3, pp:415 - 418. https://doi.org/10.30534/ijatcse/2019/14832019
4. 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. https://doi.org/10.14569/IJACSA.2014.050527
5. Shady Mohamed Soliman, Baher Magdy, Mohamed A. Abd EI Ghany, 'Efficient implementation of the AES algorithm for securing applications', International conference on system-on-chip(SOCC) proceedings, IEEE, 2016.
6. P C Lai, Design and Security impact on consumers' intention to use single platform E-payment, Interdisciplinary Information Sciences Vol. 22, No. 1 pp: 111–122, 2016. https://doi.org/10.4036/iis.2016.R.05
7. Bogdan-Alexandru urs, security issues and solutions in e-paymentsystems,http://www1.american.edu/initeb/sm4801a/epayment1.htm, 2015.
8. Augustine Takyi and Patrick Ohemeng Gyaase, 'Enhancing Security of Online Payments: A Conceptual Model for a Robust E-Payment Protocol for E-Commerce', International conference on E-business Technology and Strategy, Springer-2012, pp: 232-239. https://doi.org/10.1007/978-3-642-34447-3_21
9. Li, Y., Zhang, X.: Securing Credit Card Transaction with One-Time Payment Scheme. Electronic Commerce Research and Application, 413–426 (2005). https://doi.org/10.1016/j.elerap.2005.06.002
10. Yun Ling, Xun Wang, RSA-BASED secure electronic cash payment system, Industrial Engineering and Engineering Management, IEEE International Conference, 2008. https://doi.org/10.1109/IEEM.2007.4419522