Online Bank Transaction Processing System : An Operational Overview

Amit Hajare
Dept. of Information technology,
MIT College of Engineering, Pune 411038
Email: amithajare03@gmail.com

Dr. Kishor R. Kolhe
Dept. of Information technology,
MIT College of Engineering, Pune 411038
Email: kishor.kolhe@mitcoe.edu.in

***Abstract*:**

The paper presents a brief overview of Online Bank Transaction Processing system which addresses entire process of online trading starting from the basic Terminologies to functionality offered by each components & then heading towards actual work flow. As we all know how much secured and confidential bank account details are than what actually makes it possible for middleware's like Flipkart, Paytm, Snapdeal to look into clients account and smoothly carry out transaction process, by deducting the exact payment and that too without causing any security issues. The payment Gateway is responsible for offering n number of features such as customer & merchants account authentication, unforgivable proof by customer to merchant & bank. Most importantly personal credentials of user are highly secured.

The security architecture of the system is designed by using Security Protocols Techniques such as Secured Socket Layer, Secured Electronic Transaction protocol, Tunneling protocol and Encryption standard which include 56bit DES (Data Encryption System), 168bit TDES (Triple Data Encryption System), and AES (Advance Encryption Technique).

***Keywords**: Payment Gateway, Merchant Account, SSL, SET, DES*

***OS family:** Android OS, Desktop OS*

***Target:** Smart Phone, Tablets, Websites.*

1. INTRODUCTION

In this paper a brief overview of Online Transaction system is provided which addresses the entire process of online trading starting from the initial scenarios in trading and circumstances faced by traders leading to development of e payment systems which bought the entire market to a single touch. In Later stages many of the users experienced several types of attacks on e payment systems which indeed presented the vulnerability in online transactions to the entire world. To overcome this situation an idea of Payment gateways presented which is nothing but armed code consisting of merchant's account information and all the respective banks from which the customer may proceed the payment. The payment Gateways offers n number of features such as customer & merchants account authentication, unforgivable proof by customer to merchant & client, primarily private credentials of users kept extremely secure. Asymmetric key cryptosystem Method used with help of Security Protocol. Secure communication tunnel techniques added value to security issues & can protect conventional Transaction data such as account numbers, amount and other information**.**

The security architecture of the system is designed by using Security Protocols and Encryption standards, which eliminates the fraud that occurs today with stolen credit card/debit card information and customer information. More than this the Payment Gateways are secured enough to neutralize network attacks such as Spoofing, Spoofing, and Capture Relay, PIN guessing & various Cryptographic Attack.

DES (Data Encryption Standard) is a 56 bit key encryption standard which builds a protected shield by encoding credentials. But later is proved to be short. Therefore, advanced standard of it was developed, termed as Triple DES. It uses 168 independent key bits. That has been used in proposed gateway. Then there is current advancement known as AES (Advanced Encryption Standard) but it is very time consuming process. So, Triple DES is preferred over Online Transactions.

2. TERMINALOGIES

Merchants:

A merchant is a Trader who is willing to sell his products online, & will receive payments made by customer.

Client:

A Client is an entity who will buy products by making payments using credit/debit card.

Banks:

Two banks are involved.
1. Client bank
2. Merchant bank

Client bank:

Client bank holds Information about client's bank account and validate Transaction if provided credentials matches with bank database.

Merchant bank:

Merchant bank holds control of merchant bank account. It is responsible of management of transaction, fraud control, Authentication & authorization etc.

Payment Gateway:

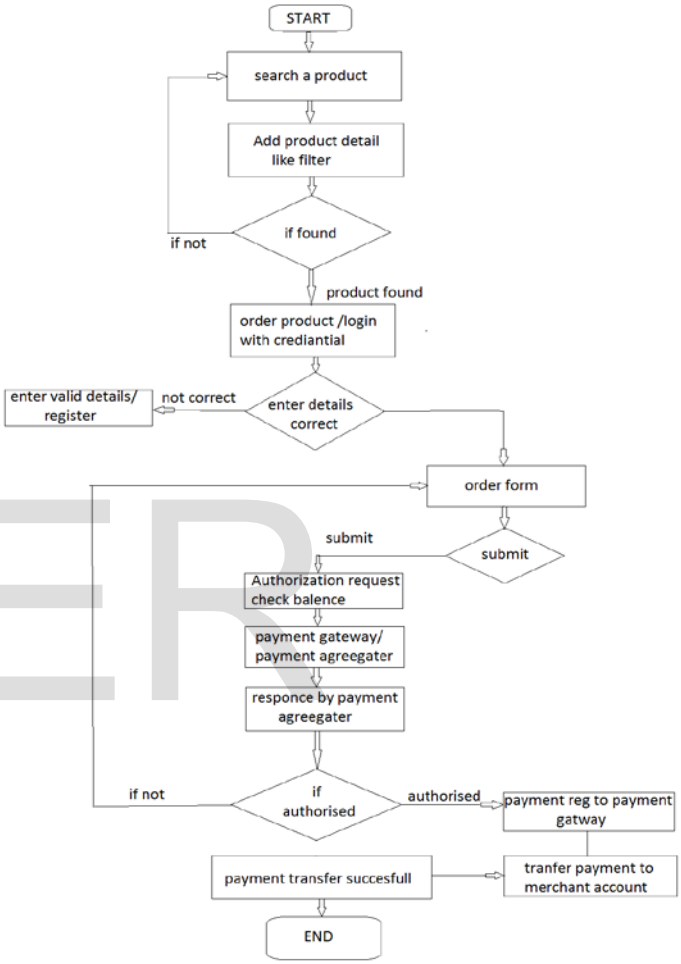
A payment gateway is e-commerce service provider application that acts as a middleware between client & Merchant. Payment Gateway is connected to all sort of customers, merchants & banks through medium of Internet and responsible for the security and reliability of all transactions that takes place.

PCI-DSS:

Which stands for Payment Card Industry's Data Security Standards developed by leading credit card companies such as American Express, Visa, Master Card, which consist of mandatory set of rules and regulation created to reduce frauds made by malicious users.

It's a group created in 2004 to create a universal platform that prevents fraud whenever credit card information is being transmitted over Network.

3. Flowchart & Algorithm:



Application/Web Side Algorithm:

- Start: Customer browse merchant's website
- Select Category, Go to Item list of selected category
  Select Item
- If Want to buy selected item, choose place order, Else return to category

- Fill the Order form, required fields like credit card No, CCV, Address and telephone no.
- Submit.

Client Bank

- Establish connection
- If connected
- Receive client account info & payment Info.
- If client's info is present in bank database forward message to server "This customer is Authorized" Else Send message that customer is not Authorized
- If customer is gets Authorized
  {
  Save payment request into database, Deduct amount from Client bank account & Send that amount to corresponding Payment Gateway
  }

Payment Gateway

- Establish connection
- If connected, Receive payment info, Else display Not Connected
- If receive payment message

{
Decrypt message
Add to database sent acknowledgement to Client bank.
Transfer payment to Merchant bank
}

Merchant Bank

- Establish connection
- If connected
- Receive payment info including merchant's account number.
- If merchant's account is present in database of bank
  {
  Receive payment, Transfer payment to Merchant's account
  }

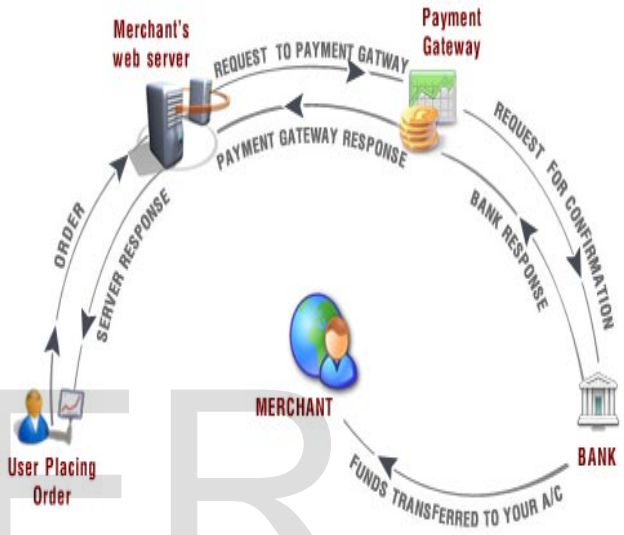
Else Send forward Invalid account no.

Merchant

- Merchant Start connection
- If connected

{
Receive message and decrypt it .Make and update database of Merchants account.
} Else retry to connect

Process Model:



DES (Data Encryption Standards):

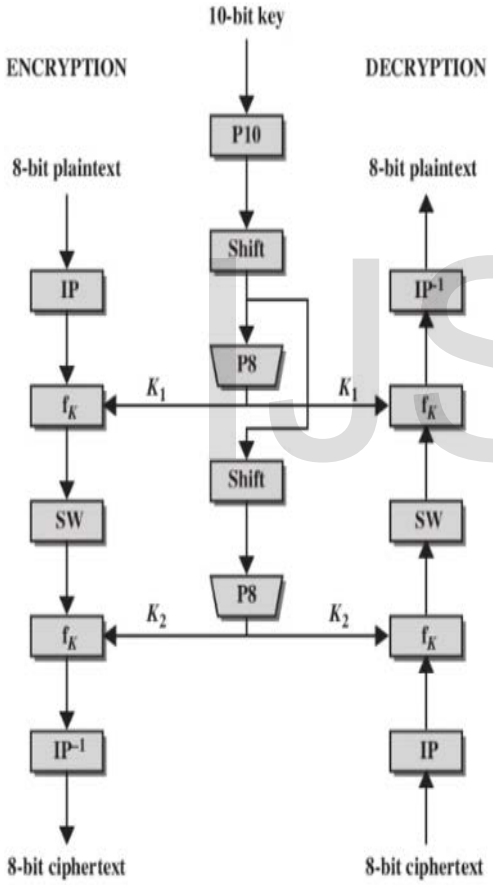
The Data Encryption Standard (DES) is an Asymmetric Encryption key scheme elected as standard in the USA in 1977. It uses a 56-bit key, which is considered to be short by many as it can with moderate effort be cracked by using brute force attack. An advanced standard called Triple-DES (TDES or 3DES) uses a comparatively longer key and is more secure. Most recent research in Encryption standard revolves around Advanced Encryption Standard (AES) & is expected to supersede DES and 3DES as the standard encryption algorithm. But time consuming approach of AES emerged the need of continuing with TDES.

.

How 56bit DES (Elementary Standard) works??

DES (Data Encryption Standard) is a 56 bit encoding technique which makes use of predetermined set of permutations for formatted scrambling of highly confidential credentials. DES generated two separate keys called K1 and K2 which are used to initially permute the credentials and operations like Ls-2 and Ls-1 (Left Shifts) are carried out for effective encoding.

Entire Process goes through the fixed sequence of procedure which is cleared by flowchart for encoding and to decode the same procedure is performed backward to retrieve the original text.



SDES Operations:

- P10 (permutate)

```
Input : 1 2 3 4 5 6 7 8 9 1
Output: 3 5 2 7 4 10 1 9 8
```

- P8 (select and permutate)

```
Input : 1 2 3 4 5 6 7 8 9 1
Output: 6 3 7 4 8 5 10 9
```

- P4 (permutate)

```
Input : 1 2 3 4
Output: 2 4 3 1
```

- EP (expand and permutate)

```
Input : 1 2 3 4
Output: 4 1 2 3 2 3 4 1
```

- IP (initial permutation)

```
Input : 1 2 3 4 5 6 7 8
Output: 2 6 3 1 4 8 5 7
```

- IP^{-1} (inverse of IP)
- LS-1 (left shift 1 position)
- LS-2 (left shift 2 positions)

Attacks & Vulnerabilities:

Apart from having such protecting shield there are some cases where attacker was able to penetrate the Transaction process and get in.

Attacks are broadly categorized in two types,

1. Cryptographic attacks

Second most important type of attack is cryptographic attack, it should not be said but one should felicitated the brilliance of attacker that he not only breaks the armed code but gets inside the process to retrieve private credentials of user and carry the attack.

The types of attack are listed below,

2.1 Chosen plaintext attack

Chosen-plaintext (CP) attack where the adversary needs to pick (adaptively) plaintexts of his choice and by exploiting the various encryption mechanism he sees their Encryption key value.

2.2 Chosen-cipher text (CC) attack

Chosen-cipher text (CC) attack where in addition to access to encryption mechanism the adversary can pick (adaptively) cipher texts of his choice and by using the various decryption mechanism he gets the corresponding plaintexts (message)

2.3 Cipher text-only attack

Cipher text-only attack where he adversary sees only cipher texts and tries to obtain plain text using trial and error methodology.

2.4 Known-plaintext attack

Known-plaintext attack are in which the attacker already knows the plaintexts (messages) and the respective cipher texts transmitted.

2. Network Attacks

Network attacks are those where attacker builds its attack for exploiting the Network vulnerabilities by positioning himself in such a position where he is able to view entire traffic flowing. Examples of Network Attacks are,

1.1 Tampering

An attacker monitors traffic over network and maliciously modifies data in transit (consider example, where attacker may change the contents of email message).

1.2. Hijacking

Once a legitimate user gets authenticated, a spoofing attack used to "hijack" the connection and penetrate the process.

1.3 Snooping

An attacker views entire network traffic as it passes and records interesting data, such as private credentials of user.

1.4 Spoofing

An attacker forges data travelling over Network, appearing to come from a various network address than it actually comes from. This kind of attack can be used to fraud target systems that authenticate depending upon host information (e.g., an IP address).

To overcome above mentioned security issues and vulnerabilities some of highly armed protocols were developed which not only secure the transaction process but also helped the growth of online trading business eliminating the security overheads.

SSL (Secured Socket Layer Protocol)

Netscape Inc. created the Secure Sockets Layer (SSL) protocol. On the basis of its popularity and acceptance, it is now implemented in all sort of web browsers. SSL is a great boon over the traditional network protocols, because it makes it easy to include confidentiality and integrity services.

It also provides authentication services, the most important one being that clients can determine if they are talking to the intended one or not, or some attacker that is actually spoofing the server.

SSL has two main objectives:

1. To ensure confidentiality, by encrypting the data that travels between the communicating parties (client and server).
2. To enable authentication of session partners, using RSA algorithm.

SSL inhabits two more protocols, underlying SSL features.

A. SSL Handshake protocol, in which the communicating channels (client and server) authenticate themselves and negotiate upon encryption key. Point to note here is the SSL Handshake adds significant overhead in starting up an SSL session.

B. SSL Record protocol, in which the session data is exchanged in between the communicating channels (client and server) in encrypted fashion.

2. Secure Electronic Transaction on (SET) Protocol

To carry out transactions efficiently and & that too without compromising security, business community, financial commitments and companies offering technological solutions rigorously wanted a protocol that will ensure confidentiality and will add the values to credibility. American Express, Visa and MasterCard, leading credit card companies formed a consortium along with computer vendors as IBM and developed a protocol which emerge as a standard in Online Transaction Process.

The core business requirements for SET are:

1. To provide confidentiality about payment information and enable integrity of order information that is to be transmitted along with the payment information.

2. Provide authentication that cardholder is genuine user of a branded payment card account.

3. Provide authentication that a merchant can accept transactions made by branded payment card through its Relationship with acquiring financial institution.

4. Ensure the use of best security practices and system design architecture to protect all genuine parties in an electronic transaction.

5. Integrity of Information (Payment Info & order Info) should be maintained throughout to meet entirely secured transaction requirement.

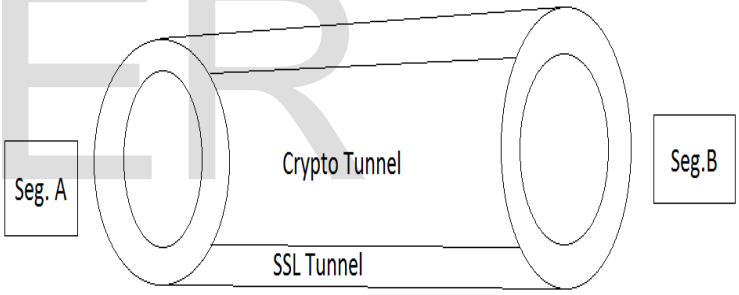
When the customer makes a purchase, the SET will authenticate the credit card against the details submitted by the customer. Transaction will occur between the two for the approval of the purchase. The e-commerce technology developed is very vital in the online Transaction system especially Payment Transfer system. It provides the customers a peace of mind while making transactions.

3. Secure Communication tunnel

Secured Communication Tunnel: A way of providing a secured way for communication between two or more peers or segments. Customer to merchant & merchant to payment gateway. Figure: Secure communication tunnel consists of SSL and nested crypto tunnel, created by employing cryptographic algorithms. The SSL is based on public key cryptosystem.

2.1 Working of Tunnel

The customer decides to buy something and go to merchant's web site. Customer sees number of items of merchant web site. During this time web server and web browser communicate through HTTP Protocol & Secure communication tunnel and key cryptosystem protects transaction data like account numbers, payment info and other information.



Here Web payment segment produces two messages.

1. First message contains order information.
2. The second message contains payment information-credit card number and other information like credit card type and validation date. The order information is encrypted using symmetric session key and signed digitally using customer's private key. The payment information is double encrypted, primarily using payment gateway public key and second time with symmetric session key.

Merchant cannot view the payment information because of the payment information is also digitally signed with the customer's private key.

Conclusion:

Thus on the basis of requirement and available local environment we propose Payment Gateway as an effective medium of Online Transaction provided that customer need to view security and credibility of respective merchant's website, his previous reviews and customer satisfaction ratios.

In today's date there are also some people who are fearful about making an online payment, if we are dreaming to make our nation digitally ahead and secure, spreading awareness about online transactions among entire society is crucial task that needs to be accomplished.

Young Entrepreneurs who are willing to sale their product online its great opportunity for them to start up their own business and make it renowned worldwide, and which could set up base for employability of various kind of skilled workers leading nation towards independent from foreign funding's.

Not only for the traders but for enthusiastic computer nurds could also share their hands for building efficient security standards which could be accepted as replacement over current once.

Authors Biography:

DR. KISHOR R. KOLHE obtained PhD from Shri JJT University, Jhunjhunu (Rajasthan), India in 2013, M. Tech. in Information Technology from the Bharati Vidyapeeth Deemed University, Pune [M.S.] in year 2010 and B.E (Hons) Electronics Engineering from S.G.G.S. Institute of Engineering & Technology, Nanded [M.S.] in year 1996.

He is currently working as Associate Professor in Information Technology Department at MAEER's MIT College of Engineering, Pune, India. He has more than 9 years teaching and 10.5 years of industry experience. His areas of interest are Software Engineering, Computer Network and Artificial Intelligence. He has published more than 15 research papers in journals and conferences. He has also guided fifteen undergraduate students and two postgraduate students.

Author of Paper Mr. Amit Hajare is perusing Bachelors of Engineering in Information Technology at MIT College of Engineering, Pune, and previously has been represented his paper presentation on National & state level and won with 1st prize. His area of interests are Team building and Innovative approaches for Business expansion.

Reference:

[1] Megawebsourse Technology, Kolhapur

[2] "Trends in Targeted Attacks" , published on trend Micro

[3] "Payment security system and e-commerce security issue"
By ms. Vaishnavi Deshmukh..

[4] www.ccavenue.com

[5] www.paypal.com