CHAPTER 3

METHODOLOGY

3.1 HOW A TYPICAL MODERN ONLINE PAYMENT PROCESSING SYSTEM (OPPS) WORKS?

Online payment Processing System (OPPS) empowers the portals to be a powerful tool to make life simple and gives the luxury of making payments to any biller in any part of the world at the customer’s convenience. Online Payment is the best way of making payments for various purposes like making utility payments, transferring funds apart from supporting ecommerce to purchase products or services. There are various systems and complex processes involved in the online payment cycle even though for the user it may take only a few seconds to complete the payment.

Generally any typical OPPS that deals with the Merchants as their main vendors, who will cater to the online payment services of their customers, consists of the structure as detailed as given below, in figure 3.1.

The system will have three major players, namely, customers who will pay their bills or any online payments, merchant website which will have all options to show and receive payments of their customers and payment gateway provider who will be instrumental in facilitating the payment by interacting with the various payment processors like Master [25], Visa [24], Amex, and ACH etc. Every payer needs to login into the merchant website using his login credentials, select the bill to be paid, select the payment mode like Credit card or Debit card or online bank account. The payment gateway provider performs the task of collecting the payment credentials, sends it to the payment processors, checks the validity of the card, credit limit validity, requests for making payment to payment processors, gets the result of either success or failure of payment with detailed error code and returns it back to the merchant website which initiated the process along with transaction id. If the details are valid and the customer has credit limit to make payment, if the settlement is immediate, amounts will be credited and debited to respective accounts in real time. If the settlement is not immediate, amount will be blocked in customer's card credit limit
Fig 3.1: Existing Typical Online Payment Processing System
and credit request will be given to vendor bank account. On the settlement period, the actual transaction takes place accordingly to credit or debit the respective accounts. In case of Net banking (debit card or bank account), the amount will be deducted immediately in the debtor account and will be credited to the creditor account in case transactions happen in the different branches of the same bank and in the event of creditor and debtor having their A/cs in different banks, the amount will be credited in the next cycle of bank processing of the inter bank transfer request. The reflection of the transactions on account statement happens at the preset frequency, when the card issuing bank account queries the payment processors and fetches information to show to its clients which will be generally a couple of times in a day at a predefined interval if the transaction happens through credit card. Even though it may take a while for the transaction to get reflected in the online account, which will happen from customer account at the predefined interval of each day, but the limit will be blocked immediately as soon as the transaction happens. The result code and result message conveys the transaction status to the merchant site with detailed information on error code, if any, along with the transaction id. The transaction id is returned along with the information sent for making payment and these will be stored in the merchant database and will be presented as the report to the customer to provide the complete information about the transaction happened. Each payment will be processed based on merchant settings on settlement time on that day and merchant may receive payment in a couple of days based on arrangement he has made with payment gateway providers. A successful transaction can be cancelled (made void) before settlement by merchant himself and if it is to be cancelled after the settlement, refund can be made by requesting payment processor with another API with required parameters. More information in detail about an OPPS can be seen in the patent given in reference [12].

3.2 SYSTEM LEVEL ARCHITECTURE DIAGRAM

The Proposed OPPS is designed using a bunch of solid subsystems which are devised keeping the scalability of the system to cater to millions of users. Each sub system performs a well defined functionality. Each sub system follows the 3 tier architecture and is deployed in a distributed system so that performance can always be enhanced by adding more servers or machines for each tier.
Refer the figure 3.2. The proposed OPPS comprises of Web Server, application Server, Database Server, Application Server and Notification Server.

Web Server is the entry point which presents the UI interface with screens and forms through which user can login, do the transactions and view information. This server takes care of all client side validations and Application server can be only connected through this Web server. Web server has high security protection like SSL and encrypting data while transmitting. Web server communicates with application server component which is a windows service type application.

Application Server houses the business logic and further connects to the Database server. Application server is designed in such a way that only our Web server alone can connect it to Application Server and this can not be connected or accessed from outside from any other system. The Application server alone can connect it to the Database Server of our application. Application server component is a windows service type application developed using .Net Remoting with TCP Channel and binary mode. This will act as the bridge between web server and Database server. As we have very clearly defined Application Server, any future enhancements of business logic or new features in coding can be implemented just by updating specific portion of the Application Server without affecting Web Server or Database Server.

Database Server manages the Database of the application. We can connect or change any database without this affecting other servers. It can be connected through this Application Server and cannot be accessed from outside applications. Enhancements to the Database Server can be implemented just by modifying this Database Server portion itself without disturbing the rest of the application.

Notification Server manages the Reporting services, notification of alerts or messages through SMS or Email. As the Notification Server works independently, this can facilitate huge report or bulk notification without presenting much load to the Web Server or App Server. This helps in the good performance of the overall application. Separation of this load will help to reduce a very significant amount of load if the transactions are huge and report generation occupies more processing time of CPUs.
3.3 **TOOLS & TECHNOLOGIES**

- MS-Visual Studio2008
- .Net Framework3.5
- VB.NET
- AJAX
- MS-SQL Server2008
- Stored Procedures
- IIS7

3.4. **KEY SECURITY FEATURES**

Security is critical to any OPPS. Every OPPS needs to undergo rigorous tests and qualify the stipulated certifications like PCI – DSS compliances before getting launched into the market [46]. People will trust the system and will use it only if they see all these security measures being implemented and arrangements for some
insurance cover being made for the business which will come in handy if some hacking happens or any other problem which results in monetary loss to the customers. Following are the key security features implemented in the Proposed OPPS:

- PCI-DSS Compliance System
- Distributed Application
- Tokenization Features

### 3.4.1 PCI-DSS Compliance

The entire process of payment may take a few seconds to a minute in a secured way using various protocols and systems. Since security is the main concern, the industry follows the standard, called “Payment Card Industry Data Security Standards - PCI-DSS” which is the well-defined standard adopted in payment processing systems around the world [51]. In 2006, five noted payment brands, VISA, MasterCard, Amex, JCB, International and Discover Financial Services, formed a council of security standards called the Payment Card Industry Data Security Standard (PCI DSS). PCI DSS is an open global forum that works on developing, managing, spreading awareness and educating merchants and customers about PCI Security Standards. It provides a baseline of technical and operational requirements designed to protect cardholder data. It applies to all entities involved in payment card processing – including merchants, processors, acquirers, issuers and service providers, as well as all other entities that store, process or transmits cardholder data. It also works on Payment Application Data Security Standard (PA-DSS) and Pin Transaction Security (PTS) requirements. Online merchants who use these five payment brands for payment in their websites are required to follow the PCI DSS policies. Violation of the policies may result in revoking a merchant’s right to sell [67]. Furthermore, violation of a policy is usually tracked when it is reported by someone or a breach is identified with a merchant.

PCI DSS comprises a minimum set of requirements for protecting cardholder data, and may be enhanced by additional controls and practices to further mitigate risks. Below is given a high-level overview of the 12 PCI DSS requirements:
3.4.1.1 PCI Data Security Standards – An Overview [51]

- **BUILD AND MAINTAIN A SECURE NETWORK**
  1. Install and maintain a firewall configuration to protect cardholder data.
  2. Do not use vendor supplied default system passwords and other security parameters.

- **PROTECT CARDHOLDER DATA**
  1. Protect stored cardholder data.
  2. Encrypt transmission of cardholder data across open and public networks.

- **MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM**
  1. Use and regularly update antivirus software and programs.
  2. Develop and maintain secure systems and applications.

- **IMPLEMENT STRONG ACCESS CONTROL MEASURES**
  1. Restrict access to cardholder data by the business need to know.
  2. Assign a unique ID to each person with computer access.
  3. Restrict physical access to cardholder data.

- **REGULARLY MONITOR AND TEST NETWORKS**
  1. Track and monitor access to all network resources and cardholder data.
  2. Regularly test security systems & processes

- **MAINTAIN AN INFORMATION SECURITY POLICY**
  1. Maintain a policy that addresses the information security for all personnel.

  The entire process of payment may take a few seconds to a minute in a secured way using various protocols and systems. The heart of any Ecommerce system is the OPPS.

3.4.2. Distributed Application

Application is developed using a 3-tier distributed architecture which is organized into three major disjunctive tiers with each tier deployed in physically
distinct machines so that at any point of time, the application can be scalable by adding more servers and load balancing system as the volume of business increases. Refer figure 3.3.

These tiers are

1. Data Tier (Backend)
2. Logical Tier (Middleware)
3. Presentation Tier (Front end)

3.4.2.1 Data Tier

This Tier is responsible for retrieving, storing and updating information and therefore this tier can be ideally represented through a commercial database. Here the stored procedures are considered as a part of the Data Tier. Usage of stored procedures increases the performance and code transparency of an application.

3.4.2.2 Logical Tier

This is the brain of the 3-Tier Application. We can separate Logical Tier into Business Tier and Data Access Tier. Some of the advantages are code transparency increase, Supports changes in Data Layer. We can change or alter database without touching the Business Layer and this would be a very minimum touch up.

3.4.2.2.1 Business Tier

This sub tier contains classes to calculate aggregated values such as total revenue, cash flow and debit and this tier doesn’t know about any GUI controls and how to access databases. The classes of Data Access Tier will supply the needy information from the databases to this sub tier.

3.4.2.2.2 Data Access Tier

This tier acts as an interface to Data Tier. This tier knows how to (from which database) retrieve and store information.

3.4.2.3 Presentation Tier

This Tier is responsible for communication with the users and web service consumers and it will use objects from Business Layer to response GUI raised events.
3.4.3 TOKENIZATION

Tokenization is the process of replacing sensitive data with unique identification symbols that retain all the essential information about the data without compromising its security. Tokenization, which seeks to minimize the amount of data a business needs to keep on hand, has become a popular way for small and mid-sized businesses to bolster the security of credit card and e-commerce transactions while minimizing the cost and complexity of compliance with industry standards and government regulations.

Merchants accommodate common post-transaction processes such as refunds, returns and additional purchases by storing cardholder data for future access. Storage of in-the-clear cardholder data, however, can incur considerable commitments of time and resources for those who attempt to comply as the system should be PCI compliance [2]. Further, storing important information as clear text can pose a security risk, regardless of protective measures taken.
Tokenization is the alternative option to avoid any risk of storing data in the clear form. After a payment transaction takes place, tokenization allows cardholder data to be replaced by an identifying text string, known as a "token", for storage. This process can be performed by a hardware security module (HSM), ensuring that no data is stored in the clear format. To retrieve cardholder data for the purposes of charge backs, returns, data analysis, and other processes, the relevant token is sent to the HSM, which will then return the requested data in a secure manner.

By implementing tokenization and eliminating in-the-clear storage of data, merchants enjoy a considerable reduction of PCI scope and cost. In turn, merchants need not devote significant resources to maintaining compliance, and the risk of security breach is lessened substantially.

3.5 KEY FEATURES OF A TYPICAL ONLINE PAYMENT PROCESSING SYSTEM

There are many features available in most of the OPPS to allow customers to make payments to merchants. Though the main aim of OPPS is to facilitate a smooth transaction so that customer can make payment comfortably to any utility services or bills of merchants, the features are built around this core feature to provide flexibility, choices and comfort to the customers.

➤ MULTIPLE PAYMENT OPTIONS

Allows customers to make payment to multiple bills from same vendors at a time.

➤ SINGLE SIGN ON (SSO)

Allows customers to make utility payments without logging into any third party website. This gives the extra comfort of not having to create and use multiple user login credentials.

➤ TIERED CONVENIENCE FEE OPTION

Payment application will have configurable option to set any fee that can be allowed to the client like processing fee, tax, etc. The client or Merchant will have option either to levy the same from the customers or can make it free which is again configurable from his screen. So the rules can be set with total flexibility at all levels.
CUSTOMER DATA IMPORT AND BILL DATA IMPORT

Customer data like profile info, login info and other things can be seamlessly integrated to the payment application and utility bill data can be imported so that client can key in bill data again for getting payment from customers. This saves a lot of time, money and encourages clients to use the system.

IVR PROCESS

Interactive Voice Response (IVR) system for its clients make the bill payment available for their customers even without computer and internet – just by using communication devices like phone or mobile. The IVR is dynamic enough to meet the needs of multiple clients offering a broad range of payment options and customer validation options.

IVR exposes the necessary information from payment application system using Web Services that accept POST values and return the proper XML-formatted response.

A caller will enter information into IVR system via his/her telephone/mobile; based on already-built logic in the IVR system, Web Service calls the Payment system which will interface with the billing system to return the required data back to IVR system, and ultimately to the caller.

ACH PROCESS (AUTOMATED CLEARING HOUSE NETWORK)

The ACH Network is a highly reliable and efficient nationwide batch-oriented electronic funds transfer system which provides for the interbank clearing of electronic payments for participating depository financial institutions.

ACH payments include but not limited to:

Direct Deposit of payroll, Social Security and other government benefits, and tax refunds;

Direct Payment of consumer bills such as mortgages, loans, utility bills and insurance premiums;
Business-to-business payments;
E-checks;
E-commerce payments;
Central, state and local tax payments.

When E-Check payments are made, the payments are not physically sent to the Payment API Engine. Instead, these payments are stored in the data base and processed by an ACH process when EOD is run.

Electronic check payments need an effective duration of 2 business days past the actual payment date in which the payment is processed by the application to complete all processes.

This process will read all the electronic check transactions and build a formatted ACH file. The ACH Payment file will debit customers accounts and credit a designated client Account. The ACH process will have to query to see what account is being utilized for the file being created.

A Daily ACH Settlement file will also be created. The clients designated account will be credited 2 non-holiday business days after the customer’s payment has been made. This file will contain the credit to the Client account and a debit to the designated customer account.

A Daily ACH Returns file can also be created. This file will contain a debit to the Client account and a credit to the payment portal Account for the return item.

➤ API PAYMENT PROCESS

The API Payments Process system allows clients the ability to process and manage payment activity directly through an API Gateway. This can be accomplished by passing credit card, debit card, checking or savings account information directly to the API gateway to process the payment request.

Most of the Payment portals, in addition to processing and managing payment activity directly to the API interface for processing, also provide the ability to store customer payment information thus allowing clients the ability to avoid the cost (PCI) associated with capturing and storing credit card information. These systems can support many different payment accounts per customer.
CSR PAYMENT OPTIONS

This option allows customers to make payment using the help of Customer Care Representative. By establishing and identifying identity, customers can make payment with the help of CSR by following a set of well defined steps.