Fraud Detection and Loss Prevention System with Secure Data Transmission

Submitted By

Meet Hadvani

16MCEI07

तमसो मा ज्योतिर्गमय

NIRMA UNIVERSITY

INSTITUTE OF TECHNOLOGY

NAAC ACCREDITED ‘A’ GRADE

DEPARTMENT OF COMPUTER ENGINEERING

INSTITUTE OF TECHNOLOGY

NIRMA UNIVERSITY

AHMEDABAD-382481

May 2018

Fraud Detection and Loss Prevention System with Secure Data Transmission

Major Project

Submitted in partial fulfillment of the requirements

for the degree of

Master of Technology in Computer Engineering (Information & Network Security)

Submitted By

Meet Hadvani

(16MCEI07)

Guided By

Prof.Pooja Shah

तमसो मा ज्योतिर्गमय

NIRMA
UNIVERSITY

INSTITUTE OF TECHNOLOGY

NAAC ACCREDITED ‘A’ GRADE

DEPARTMENT OF COMPUTER ENGINEERING

INSTITUTE OF TECHNOLOGY

NIRMA UNIVERSITY

AHMEDABAD-382481

May 2018

Certificate

This is to certify that the major project entitled **”Fraud Detection and Loss Prevention System with Secure Data Transmission”** submitted by **Meet Hadvani (16MCEI07)**, towards the partial fulfillment of the requirements for the award of degree of Master of Technology in Computer Engineering ((Information & Network Security) of Nirma University, Ahmedabad, is the record of work carried out by him under my supervision and guidance. In my opinion, the submitted work has reached a level required for being accepted for examination. The results embodied in this major project, to the best of my knowledge, haven't been submitted to any other university or institution for award of any degree or diploma.

Prof.Pooja Shah
Guide & Assistant Professor,
CE / IT Department,
Institute of Technology,
Nirma University, Ahmedabad.

Dr.Sharda Valiveti
Associate Professor,
Coordinator M.Tech - CSE (INS)
Institute of Technology,
Nirma University, Ahmedabad

Dr. Sanjay Garg
Professor and Head,
CE Department,
Institute of Technology,
Nirma University, Ahmedabad.

Dr Alka Mahajan
Director,
Institute of Technology,
Nirma University, Ahmedabad

Statement of Originality

I, **Meet Hadvani**, **16MCEI07**, give undertaking that the Major Project entitled "**Fraud Detection and Loss Prevention System with Secure Data Transmission**" submitted by me, towards the partial fulfillment of the requirements for the degree of Master of Technology in **Computer Engineering (Information & Network Security)** of Institute of Technology, Nirma University, Ahmedabad, contains no material that has been awarded for any degree or diploma in any university or school in any territory to the best of my knowledge. It is the original work carried out by me and I give assurance that no attempt of plagiarism has been made.It contains no material that is previously published or written, except where reference has been made. I understand that in the event of any similarity found subsequently with any published work or any dissertation work elsewhere; it will result in severe disciplinary action.

Signature of Student

Date:

Place: Nirma University,Ahmedabad.

Endorsed by

Prof.Pooja Shah

(Signature of Guide)

Acknowledgements

It gives me immense pleasure in expressing thanks and profound gratitude to **Prof. Pooja Shah**, Assistant Professor, Computer Engineering Department, Institute of Technology, Nirma University, Ahmedabad for her valuable guidance and continual encouragement throughout this work. The appreciation and continual support she has imparted has been a great motivation to me in reaching a higher goal. Her guidance has triggered and nourished my intellectual maturity that I will benefit from, for a long time to come.

I heartily thank our internal project guide, **Atul Gupta**, Sr. Software Developer at Oracle India Pvt Ltd for his guidance and suggestions during this project work.

It gives me an immense pleasure to thank **Dr. Sharda Valiveti**, Hon'ble Coordinator M.Tech - CSE (INS) Institute of Technology, Nirma University, Ahmedabad for her kind support and providing basic infrastructure and healthy research environment.

It gives me an immense pleasure to thank **Dr. Sanjay Garg**, Hon'ble Head of Computer Engineering Department, Institute of Technology, Nirma University, Ahmedabad for his kind support and providing basic infrastructure and healthy research environment.

I would also thank the Institution, all faculty members of Computer Engineering Department, Nirma University, Ahmedabad for their special attention and suggestions towards the project work.

- Meet Hadvani
16MCEI07

Abstract

The project aims at providing a customer friendly solution for POS (point of sale) application. This integration helps accumulate data from POS application at different locations under one centralized cloud system. This way the service providers can target different categories of loss and frauds that can emerge in retails. It also helps in providing business analysis. In this project, integration consists of two major modules i.e. loss prevention and fraud detection application with any POS (point of sale) or online customer retail application. This integration helps the two applications to communicate where one application uses the data from the other .The UI framework has been designed using the OJET (Oracle Java Extension Toolkit). This helps in displaying the generated reports which provide data analysis. This data analysis helps in the decision making process and to increase the profits. The business analysis module is used to give an insight into the data pattern and then formulate policies and decisions accordingly.

Abbreviations

POS	Point of Sale
CCTV	Closed-Circuit Television.
DBS	Data Base System.
LP	Loss Prevention
VI	Visual Insight
SID	Session ID
ELT	Extract Load Transform
JWT	Json Web Token
JWS	Json Web Signature
JWE	Json Web Encryption
HTTP	HyperText Transfer Protocol
XSS	Cross Site Scripting
JSON	JavaScript Object Notation
HTTP	Hypertext Transfer Protocol
REST	Representational State Transfer
MVC	Model-View-Controller

–

Contents

List of Figures

Chapter 1

Introduction

1.1 Overview

There are a number of POS applications present at various stores which provide a huge amount of customer data that needs to be handled. Also, there are different categories of customers which leads to return and refunds for the products which he purchased. Returns and refunds also handled at POS application but which return and refund is honest that we need to consolidate and figure out. Hence, here the Loss prevention and Fraud detection come into the picture. Loss Prevention and Fraud Detection System is the most widely used for loss prevention and point of sale (POS) data analysis tool. It mainly contains two different modules:

1. The Loss Prevention module is an intuitive, intelligent and global analytical reporting solution that is designed to quickly identify suspicious trends, transactions, and other data anomalies. The Loss Prevention module allows easy user access, dynamic functionality, and forensic analysis to make more-informed decisions with timely, data-driven answers to business questions and to protect the bottom line.

2. Sales & Productivity module offers robust and highly configurable reporting across all levels of the retail organization hierarchy (Salesperson, Store, District, Region, and so on), merchandise hierarchy (item, class, dept., and so on), and/or by geographic attributes. Through a comprehensive set of grid and graph reports, documents and interactive dashboards, users can compare same store sales to past performance and custom goals, measure sales members productivity, and evaluate the impact of merchandise characteristics on productivity.

1.1.1 Data Flow of Application

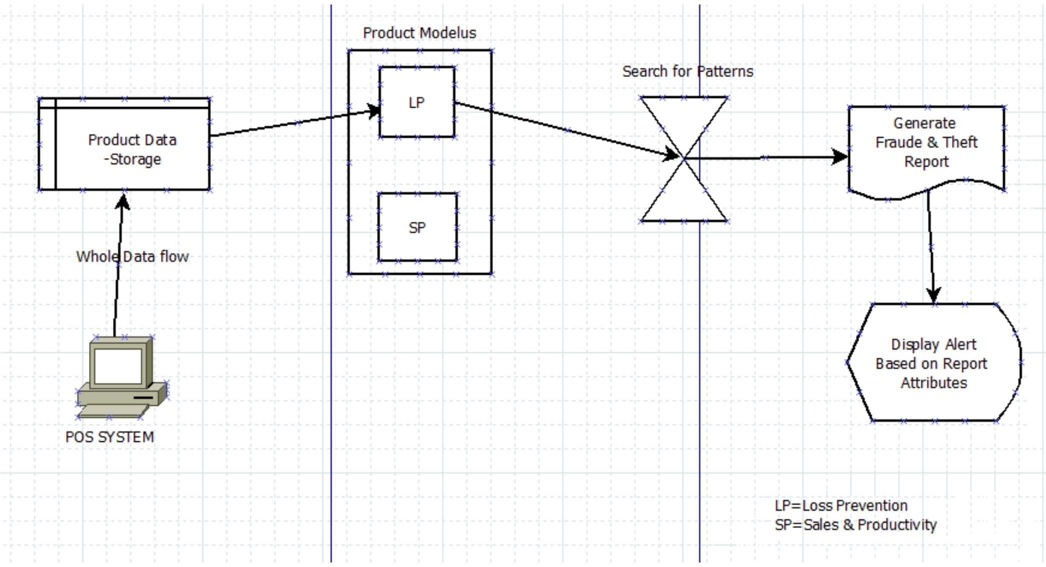


Figure 1.1: Loss Prevention Data Flow

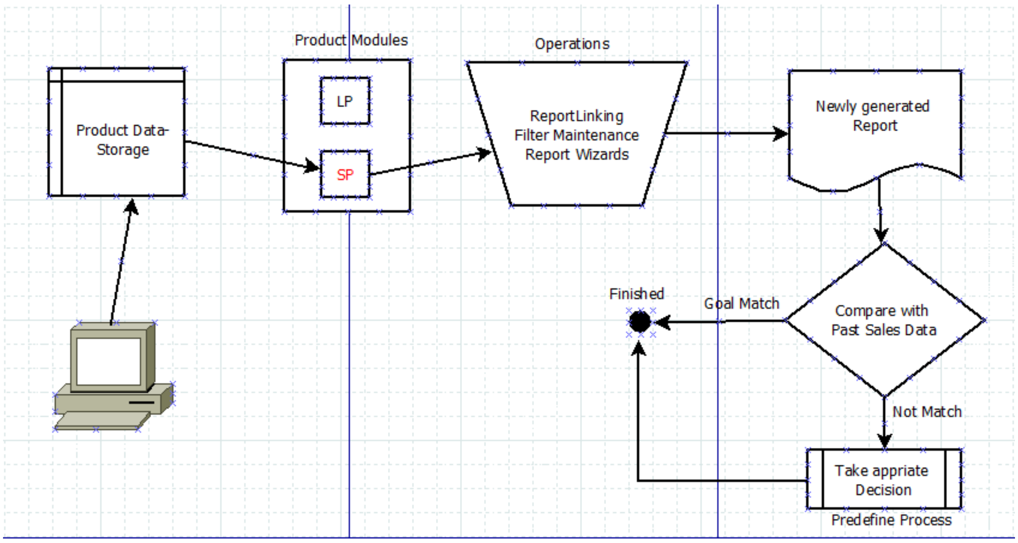


Figure 1.2: Sales & Productivity Data Flow

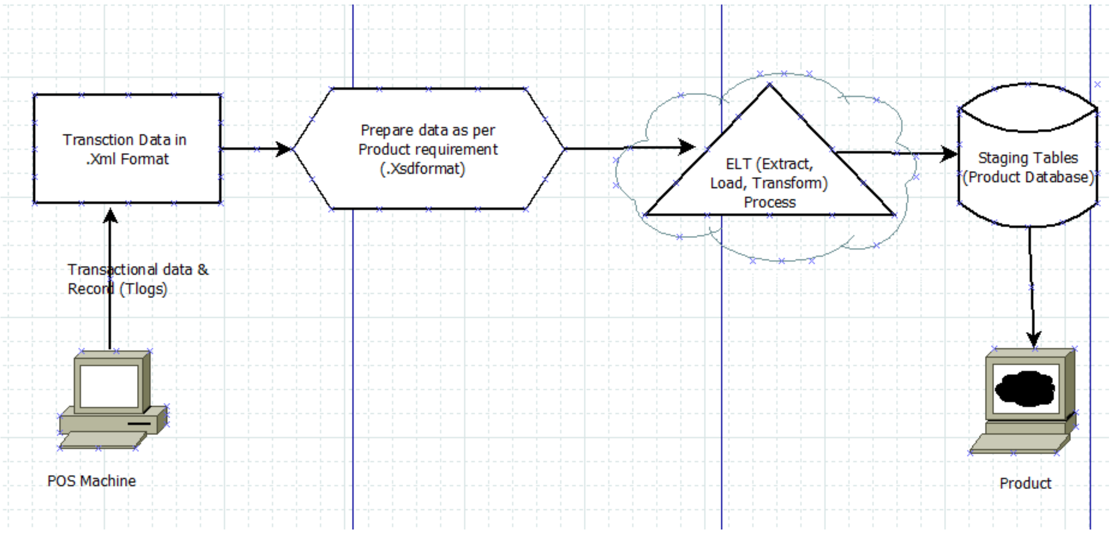

Transction Data in .Xml Format
Prepare data as per Product requirement (.Xsdformat)
ELT (Extract, Load, Transform) Process
Staging Tables (Product Database)
Transactional data & Record (Tlogs)
POS Machine
Product

Figure 1.3: POS to Application Data Flow

1.2 Objectives

- To reduce merchandise shrinkage.
- To ensure effective use of CCTV camera, Alarms and other security instruments.
- To increase the sales & productivity by creating report/dashboard from previous data
- Identification of policy violations and training issues to resolve operational problems.
- To provide security against theft exceptions in retail store
- Reduce operational costs through efficient auto-distributed alerts and reports
- Securely data transfer between two parties.

Chapter 2

Literature Survey

2.1 Survey of Retail Industries Losses

Now a day most of the transactions are happening through electronic payment, like credit card, debit card,e-wallet etc. Main focus of any retailer is to increase the profit in their business through increasing sales of item/goods.There is other side to increase the profit by reducing loophole in existing system. As per my Survey retail industries facing losses against internal theft, Shoplifting, fraud in the system, paperwork error etc[1].

Below chart show the theft and fraud in Retail industries.

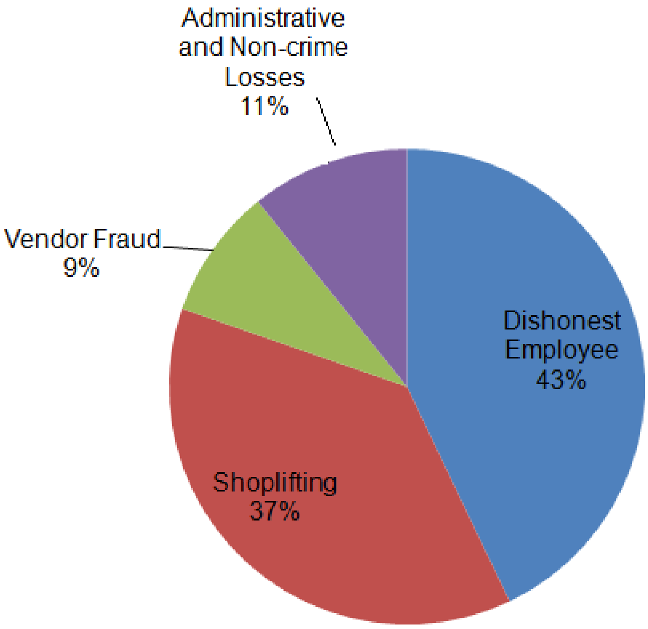


Figure 2.1: Chart-daigram of Retail losses

To handle this much amount of data, system should have flexibility and scalability.Cloud give that functionality so this project will design in such a way so it can move to cloud and serve the need of customers dynamically.

2.1.1 Traditional Authorization method

Before Json web Token introduce in the market, Industries uses tradition session approach to identify the user. In session approch server needs to mianten session for each and every user and store into its memory or Database system. Step to authorize the user using Session/cookies approach[2]:

- User request for the resources by sending Username and Password
- Server verify the login information.
- Server create session and store it into DB
- Server return Session Id (SID) to particular client and store into client cookies
- Client request next Resource with SID
- Server check Session ID is valid or not (by searching into DB)
- Check the user role for authorization of requested resources
- Finally User receive requested Resource.

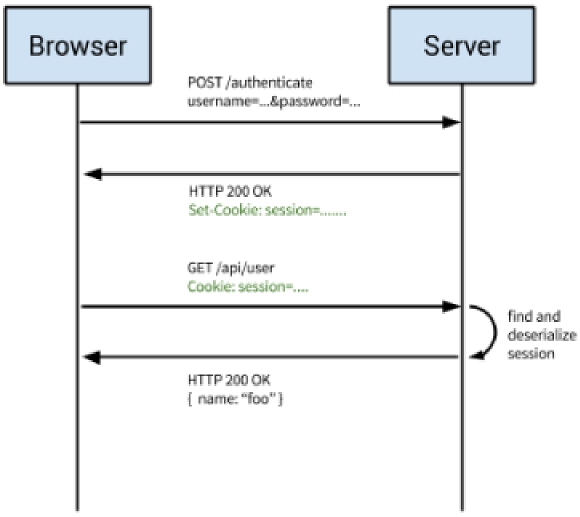


Figure 2.2: Cookies/Session based Authentication/Authorization

Chapter 3

Functionality and Features

3.1 Functionality of the System

There are several functionality of system which helps to achieve retailer goal. some of the functionality are mention below :

1. Dashboard - Exception Analysis :

   This dashboard was designed to summarize controls and exceptions in order to provide Loss Prevention (LP) leadership with information on what exceptions are occurring, how they are being addressed, and who may be handling them[3]. The dashboard has a selection of date ranges to summarize on exceptions; looking at total generated, break down by status, type, where they are occurring, and who is assigned to investigate them.

2. New Administration - Project Defaults Screen:

   New Administration is basically meant for different access rights at various user-levels. Here are some of instances of it:

   (a) Day Parts :

   This new Project Defaults screen lets users customize the day parts, or defined intra-day time periods (for example, Morning, Lunch, Afternoon, Evening) that are used in the Sales Flow by Period Dashboard and Sales Flow by Period reporting.

   (b) Discount Details :

   This report now includes the ability to display items. The discounts were not being associated with the item to which the discount was applied or against which it was prorated. [1]

3. Reporting :

   Reporting provide the facilities to create different types of report based on previous data. It's also vary from module to module. Some of the Report types are mention below:

   - Cash Refund Summery Report
   - Discounts and Price Overrides Summary Report
   - Refund and Exchange Summery Report
   - Transaction Discount Report
   - Employee Discount Report
   - Coupon Transaction Report

4. Look and Feel to Visual Insights (VI) Module [4]:

   There is a new look-and-feel that modernizes the appearance of Visual Insights to provide an improved user experience.

   (a) Dynamic Links:

   User can create dynamic links to external content in a Grid visualization.

   (b) Graph Value Options:

   User can now specify values outside the minimum and maximum value range to maintain a consistent scale over time, even if the data is republished and the minimum and maximum values change.

   (c) Attribute Thresholds:

   User can add thresholds to attributes in visualizations, allowing you to apply conditional formatting across headers. When applying a threshold to a parent attribute, the conditional formatting is applied at level of the visualization.

3.2 Features

3.2.1 Features of Fraud Detection and Loss Prevention Module

1. Video Linking :

   The Video Linking module provides lessons that show you how to link to a video clip of activity filmed during a specific POS transaction and how to archive video links, manage IP addresses for camera locations, and upload video files to the database System[3].

   The video link feature allows you to retrieve the digital video that corresponds to one or more transactions. You can execute a video link from any header/detail level report, or document that includes the Trans attribute. From the Video Queue page, you can modify the camera, start time, and end time before launching the video. After viewing the video clip, you can send the link to the Video Archive, where you can view the video again, make changes if needed, and upload it to the database for later retrieval.

2. Exception Control :

   You can add thresholds to attributes in visualizations, allowing you to apply conditional formatting across headers. When applying a threshold to a parent attribute, the conditional formatting is applied at level of the visualization.

   A users data security filter must be incorporated into the application of the alert filter. The security filter should be applied first before the alert filter or any report filter. For example, if a user is restricted to one store and an alert filter is used showing the top five cashiers for revenue, the report will include the top five cashiers in the store to which the user has access. Security filters restricting a user to their organization in a multi-tenant environment should be applied first as well.

3. Watch Status :

   Use the Watch List functionality to assign a watch status to stores or cashiers displaying questionable activities.

   The Watch List detail screen contains the complete history of a specific cashier or store on the watch list as well as the tools used to change the status or add information regarding the status.

Cashier Watch List information includes :

(a) Cashier or Store information

(b) History : watch status history appears in chronological order, with the most recent information at the top of the list. Information within the History section cannot be changed or deleted.

(c) Watch Status selection menu

(d) Watch Notes - In the Watch Note field to enter comments regarding this watch status, the cashier, or any other information that may help track the item.

4. Real Time Processing : It provides real-time processing to support intraday flash sales reporting for the new Sales and Productivity module. This is accomplished by processing data in specified time increments throughout the day rather than once at the end of day. Additional business logic supports the inclusion of post voids, clock in, clock out, and adjustments to normal business.

   Additional Loss Prevention analysis followed by no sale and no match transactions will be updated through the end of day process. Here the implementation of Real Time Processing:

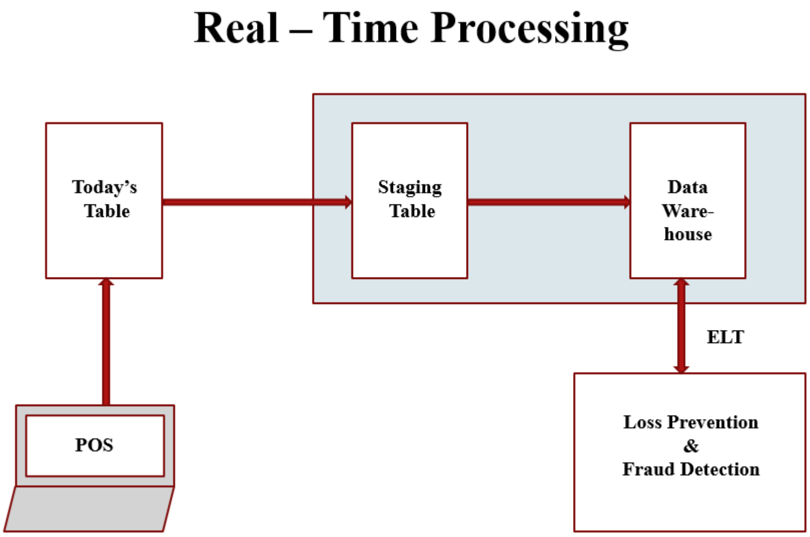


Figure 3.1: Real-Time-Processing

3.2.2 Featurs of Sales and Productivity Module

1. Report / Dashboard Linking :

   Ability to link from one report to multiple reports that assist the end users with analysis or investigating the data. The linking functionality allows for reports to be link to the same report or different, allowing focus on a key field or set of fields while allowing expansion of the date range. The reports also need to link to and from dashboards that may contain one or multiple datasets. Dashboards also need to be able to link from one to other dashboards.

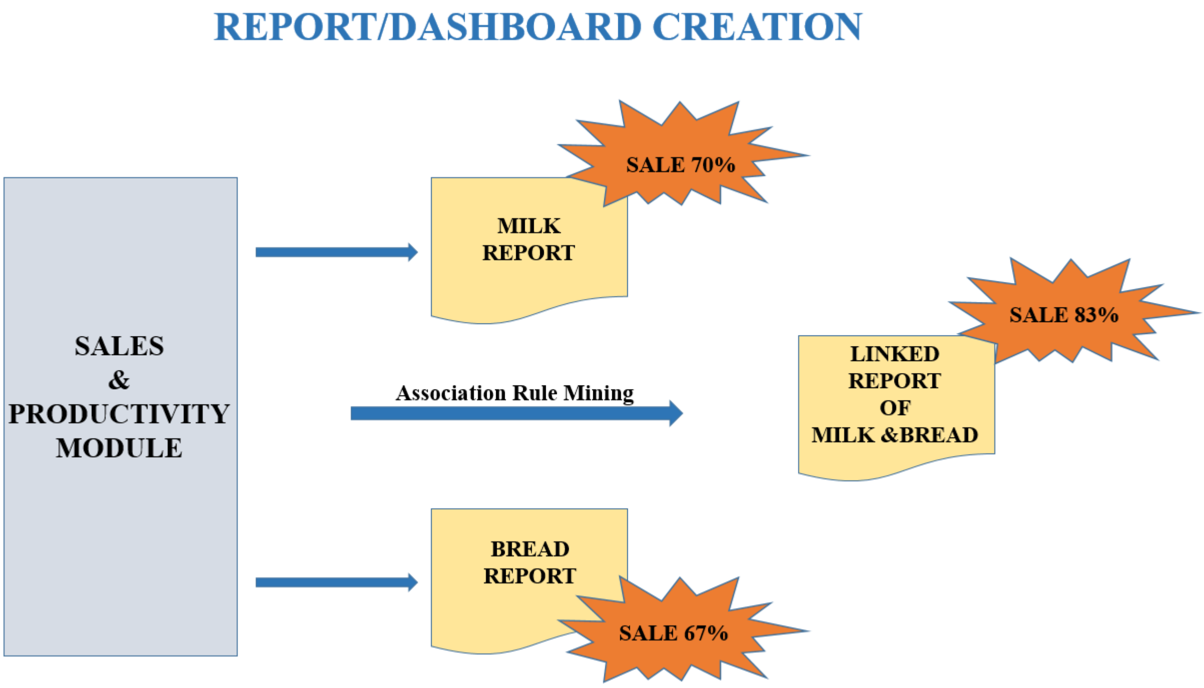


Figure 3.2: ReportLinking Process

2. User Security Administration - Functionality Access :

   User Roles are defined to allow different levels of access application for functionality depending on the need of the users. In addition, the extended features can be controlled through the administrative interface.

3. Lookup Conversion :

   Ability to have lookup tables that convert raw data to display descriptions that are more meaningful to the end users.The ability to have summarization of metrics at different levels for analysis or comparison based on master table hierarchies. The end user may want to compare the employee to the store, district and/or regional level as an average.

4. Report Wizards :

   The reports wizards are designed for the end user to build new reports with a limited access to what fields and metrics can be put on the report based on the tables and joins. This provides a step by step process for the end user to reduce possible confusion.

   This report wizards will designed to summarize controls and exceptions in order to provide leadership with information on what exceptions are occurring, how they are being addressed, and who may be handling them. The dashboard has a selection of date ranges to summarize on exceptions; looking at total generated, break down by status, type, where they are occurring, and who is assigned to investigate them[5].

Chapter 4

Architecture and Workflow

4.1 Application Architecture

This Application follows a layered architecture and the user requests going from layer to layer. The architecture given below depicts the working of the projects in brief and how the data travel from user system to the database and how the reports get generated and communicated back to the desired results. The below architecture is used in the project and depicts the request and response from the user end. Also, it depicts the layered architecture as discussed above.[5]

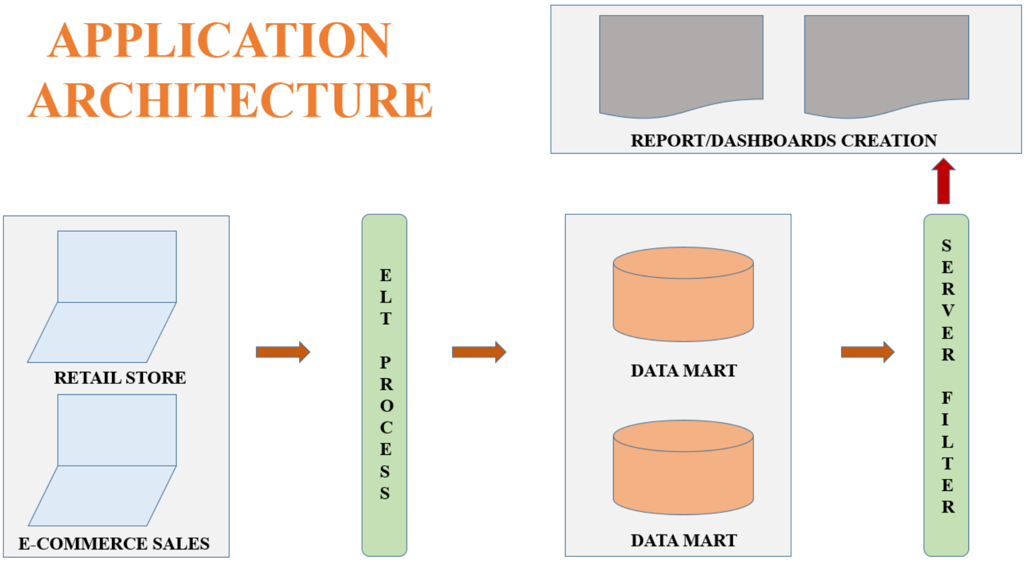


Figure 4.1: Architecture

4.2 Application Workflow

The following points outline how the application data retrieval is done in the project and shows the workflow of the application.[6]

1. All the customer transaction starts from bottom to up to convert in valuable report.

2. On the application architecture, the customer transaction can generated at Any Retails Store and E-commerce Inventory Sales.

3. All customer related transaction are transferred to the local database of our system through via path of cloud storage and with the process of ELT.

4. Transaction that stored into data mart and all related data (data about data) will store into Application Meta Data.

5. Then, all the data will transferred to Intelligence Server which leads to take inputs from Data Mart and Application Meta Data.

6. Now, all structure getting stored into Schema Object and all values stored into Metrics and then Intelligence Server apply some kind of Filters on data so that valuable information get collected.

7. Filtered information then leads to generate reports/dashboards on the basis of given previous data. Dashboard also implemented here as it is nothing, it just collection of various reports.

8. Then, generated reports and dashboards are available to display at various devices i.e. Mobile and Web.

4.3 ELT Dataflow

ELT is an alternate method for taking a information at the device way. Rather than changing the information before it's composed, ELT use the objective framework to do the change. The information is copied to the objective and after that changed set up.ELT performed well when the end system is a high-perrfomance data engine, like a cloud installation, data appliance and Hadoop cluster ELT Data flow take major 4 steps for completion:

1. In first step, it will extract all the data from the customer transaction
2. Then, it will lead to deliver data on Cloud through a protocol called SFTP
3. Data available on cloud loaded into local database of system.
4. Loaded data now transformed to a valuable format.

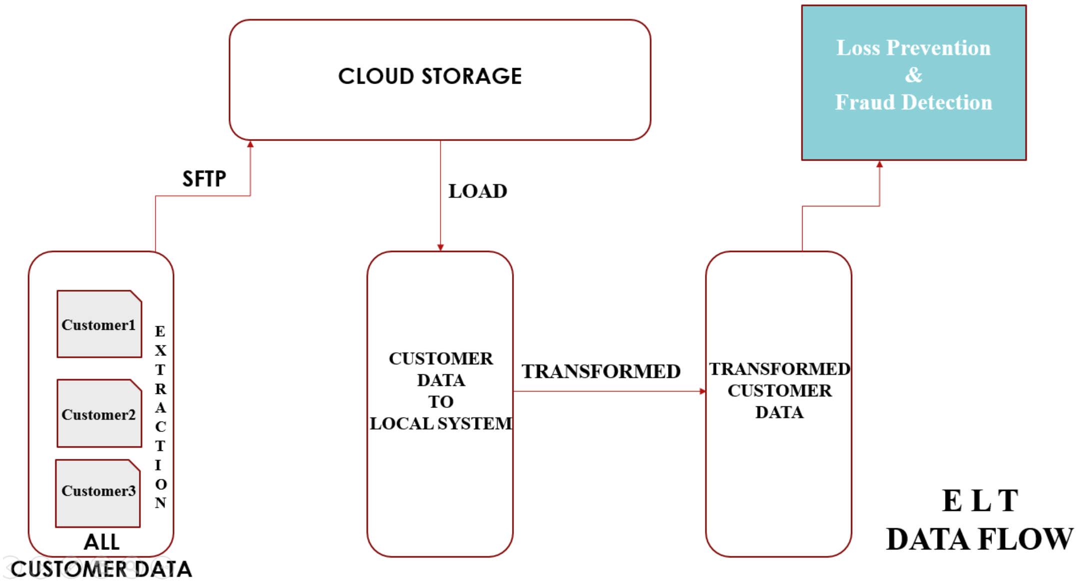


Figure 4.2: ELT Data Flow

Chapter 5

Authorization and Data Transfer with JWT(Json Web Token)

5.1 Introduction of JWT

JWT stands for Json Web Token which is highly use in industrial product.It is an open standard define in RFC-7519.It is a means of transmitting data between two parties (Client and Server) in a compact, verifiable form. In our case, It transfer data between POS and Loss prevention and fraud Detection system.The purpose of JWT is NOT to encrypt the information in any way. The reason why JWT are used is to prove that the data which is sent to server is not tempered, its sent by a legal sources. Basically its give integrity to the information which is transfer.[7]

The byte of information encoded in the payload of a JWT are called claims. The expanded form of the JWT is in a JSON format, so each claim is a key in the JSON object. This adds a powerful layer of verifiability to the user of JWTs. The receiver has a high degree of confidence that the JWT has not been tampered with by verifying the signature.JWT is just a representation of data. It does not provide encryption to the data so its not safe to add sensitive data to JWT. [8]

Some times JWT has lots of claim to transfer, some browser does not support that much data in a get URL so we need to compress the JWT payload at that time JWT compression mechanism can be use to compress the JWT payload. JWT is mainly used in Web application and services

5.2 Structure of JWT

JWT looks like a long String but it is divided into three part with the "." operator only if its signed JWt otherwise its contain only two parts Header and Payload only. All parts are encoded with base64 encoding. [9]

1. **Header** : Every JWT carries a Header witch contain type of Header so server can identify received token is JWT.
   alg : It shows which type of algorithm is used to sign jwt so it can be verify on server side. It is a mandatory filed to add in JWT Header.
   cty : It indicate type of content in whole JWT.
   Header looks like below while decode JWT
   {
   typ : JWT, (Optional)
   alg : HS256 (mandatory)
   }

2. **Payload** : It contains all the information as per user and application. like:

   - iss: Issuer of the token
   - sub: Subject of the token
   - aud: Audience of the token
   - exp: Expiration time, which time it should expire.
   - iat: Issued at time at which the token was issued by sever
   - ti: JWT ID contain unique identity for the JWT

   We can also add some custom into payload as per our need. It is in a Json object like as Header. It does not contain any mandatory data to add, its totally depend on us.[9]
   {
   "sub" : "INS",
   "name": "Meet Hadvani",
   "admin": true

”jti” : ”12345678”

}

3. **Signature** : It is a heart of token because its generate the signature which is used to verify the token at end system. without signature JWT is not secure its called unsecured JWT.This element appears after the last dot (.) in the compact serialization form. It can be use SHA256 algorithm , HMAC256 algorithm ,RSASSA algorithm. It is also called as JWS(Json Web Signature)[10]
Generate Signature:
Assume, S = Header + dot(.) + Payload
Signature = HashAlgHS265(S , secret key)
So, JWT = S + dot(.) + base64Encode(Signature).

5.3 Json Web Token Creation

JWT can be create in two form secure JWT and Unsecure JWT. Secure JWT contain signature within it while Unsecure can not contain signature[9]. To create compact and secure form of JWT follow the below steps :

- Create header as byte array and in UTF-8 representation
- Encode that array using Base64-URL algorithm
- Take Payload data as byte array and represent in UTF8 format
- Encode the byte array using the Base64-URL algorithm
- Generate signature by applying algorithm on Header and Payload
- Combine Header,Payload and signature with dot(.) sign.

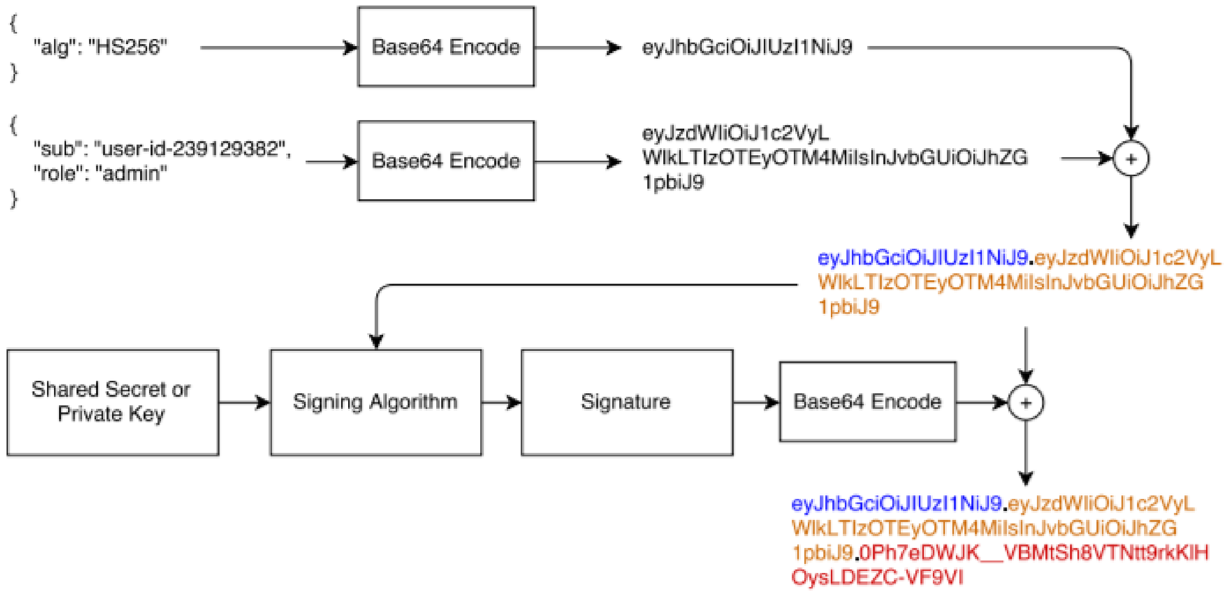

{
"alg": "HS256"
}
Base64 Encode
eyJhbGciOiJIUzI1NiJ9
{
"sub": "user-id-239129382",
"role": "admin"
}
Base64 Encode
eyJzdWIiOiJ1c2VyL
WlkLTIzOTEyOTM4MilsInJvbGUiOiJhZG
1pbiJ9
+
eyJhbGciOiJIUzI1NiJ9.eyJzdWIiOiJ1c2VyL
WlkLTIzOTEyOTM4MilsInJvbGUiOiJhZG
1pbiJ9
Shared Secret or
Private Key
Signing Algorithm
Signature
Base64 Encode
+
eyJhbGciOiJIUzI1NiJ9.eyJzdWIiOiJ1c2VyL
WlkLTIzOTEyOTM4MilsInJvbGUiOiJhZG
1pbiJ9.0Ph7eDWJK__VBMtSh8VTNtt9rkKIH
OysLDEZC-VF9VI

Figure 5.1: Compact JWT Creation

5.4 JWT Work Flow

As we know Http is a stateless protocol so it can not remeber previous user's request. So for that we create JWT on the first request at the server side and send back to requested user. Below are the step to transfer Json web Token.[11]

1. User Send User name and Password to server for authentication.
2. Server Verify the User authentication.
3. Server Create Json Web Token based on User
4. Send JWT to respected client
5. Client Receive JWT and store it.
6. Client send Jwt for next subsequent requests
7. Server verify JWT and send response according to the request

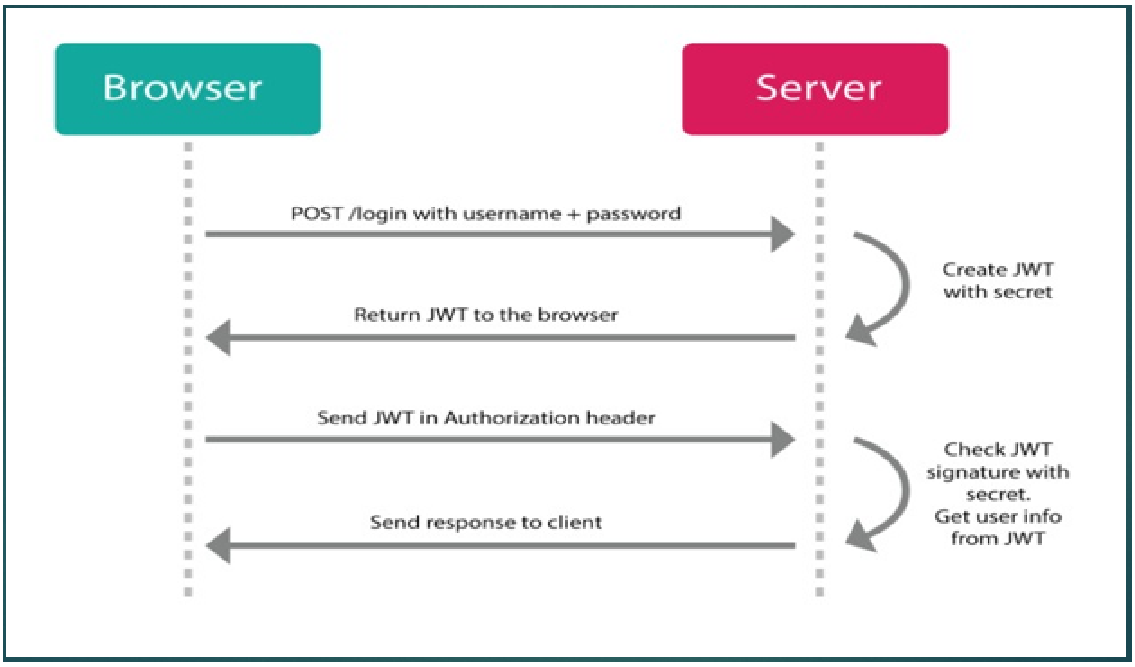
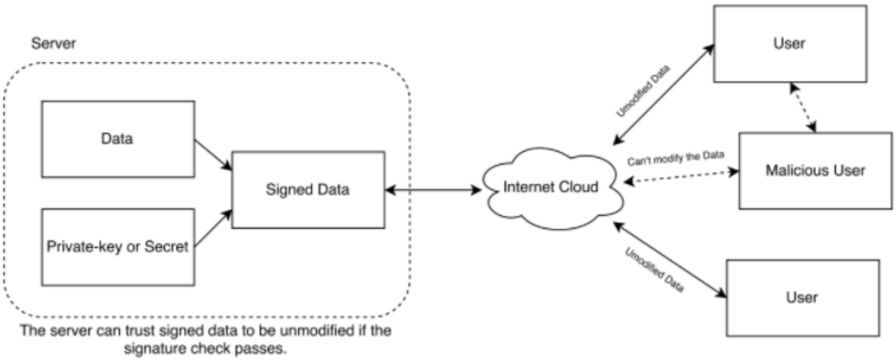

Browser
Server
POST /login with username + password
Create JWT with secret
Return JWT to the browser
Send JWT in Authorization header
Check JWT signature with secret. Get user info from JWT
Send response to client

Figure 5.2: JWT Exchange Flow

We just encode the JWT, it is not encrypted so any malicious user can read the data as a plain text[10]. If we want to hide the data from third party then we need to encrypt the JWT its called Json Web Encryption(JWE). It provide various type of encryption algorithm to secure data. So we can say that JWS is useful to validate the data against tampering. JWE is useful to protect the data against malicious user.[9]



The server can trust signed data to be unmodified if the signature check passes.

5.5 JWT Storage and Security

In aspect of the token storage, we need to store the token in client side so token can be send with each request.[2]

5.5.1 Attack on Cookies

Generally token was stored in browsers cookies. But in that case we need to care of Cross Site Scripting (XSS) and Cross-Site Request Forgery (XSRF or CSRF) attacks.

This type of attacks, exploit browser cookies and expose the data from the cookies. It is very vulnerable for the public website where user can give the input to website(like comment box) as a exploit code then server execute that code and it give cookies data to attacker.

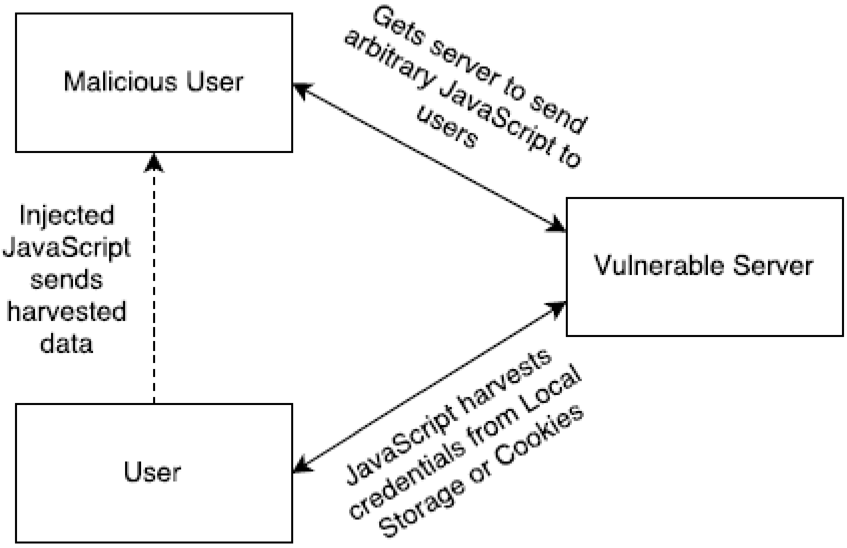

Malicious User
Gets server to send arbitrary JavaScript to users
Injected JavaScript sends harvested data
Vulnerable Server
User
JavaScript harvests credentials from Local Storage or Cookies

Figure 5.3: Cross site Scripting

5.5.2 Cookies Storage and Local Storage

Browser cookies can be exploit via attack Cross site Scripting (XSS). For protecting cookies we need to store cookies in only HTTP secure flag and also transfer via secure channel.[8] Limitation of the cookies:

- Cookies can not store more than 4KB data
- Cookies are open to across the domain

- Behaviour of cookies is different from browser to browser(at time of implementation we also needs to consider browser)
- cookies are sent with every HTTP request (Data overheating)

While Local storage has some more benefit than Cookies.It can only read the data at client side. It can not deal with server side So server side exploit can be eliminate by Using local storage.If we add more payload to JWT then its size become an issue for cookies.

- Support by most modern browsers
- Its not send with every HTTP request
- Its give 5Mb Storage to store the data.
- Data are Persistent that is stored directly in the browser

At the bottom line,To secure our JWT. We need to store it into Local storage of Browser rather than cookies[2].

5.6 Advantages of Json Web Token

There is more number of benefit to use JWT for authentication and data transfer as compare to tradition approaches like Http session Below are the some Advantages[9] :

- No Session to Manage (stateless): The token has everything you need to identify users, and the rest of your app's state can be stored in local storage on the client side. No requirement for a session object stored on the server.
- Portable/Homogenous: A single token can be utilized with various backends, even on various services.
- No Cookies Required: You can store the token anyway we need: e.g., in localStorage, indexDB, or some local store (or and cookies, if you really want)
- Mobile Friendly: Developing local applications (iOS, Android, Windows 8, and so on.) is hard with treats (e.g., you need to manage treat compartments), however receiving a token-based approach incredibly rearranges this.

- Built-in Expiration: JWT has standard claims that can be set in the payload when another token is made. Nothing more should be finished.

- Don't Need to Logout: Just discard the token when you're finished with it, it will lapse without anyone else. You as a rule need to give a short termination time, however in the event that you truly need to, you can monitor a "blacklist" of tokens that are set apart as "invalid" on the server which could be added to from an explicit logout, or from a administrator denoting certain tokens as invalid.

Chapter 6

Remote access of system's logs

6.1 Introduction

This application is running in distributed environment. Basically each system is connected to different server. It is very difficult to access the remote system. In this system, while executing report or run any other functionality of application it might get some error, exception or generate the log for the particular module.
So Loss prevention and fraud detection system provide the one unique functionality called log maintenance to access the different system's log remotely. [1].

6.2 Log Maintenance

It is a functionality to maintain, view and download the logs/error of the different machine where the application is running. It will provide the remote access of the log file/table to the admin user only. In this application logs are store in two ways:

- File Logs : File logs contains logs information in readable mode with the dot (.) log extension.
- Table Logs : Table logs contain logs information in the tabular manner like: time of log, Log description, Log location etc. it will show the log size in number of rows in the table.

Application will deploy on Cloud so different instance of the application will created according to the number of user. It is very difficult to go (login) into each machine and show the log/error, so this functionality give User interface to the admin user to access the logs/errors of different machine in a single screen.

6.3 Log Maintenance Functionality

To control over the system's log, It provides major four functionality:

- Add log References: Add reference to the log not actual log file. log References: Edit added references
- Delete log References: Delete the log reference, actual log file is still there
- View/Download: It shows the actual log file contents base on Added reference. It also allow user to download the actual log file

Below diagram can give the more realistic view of the functionality.

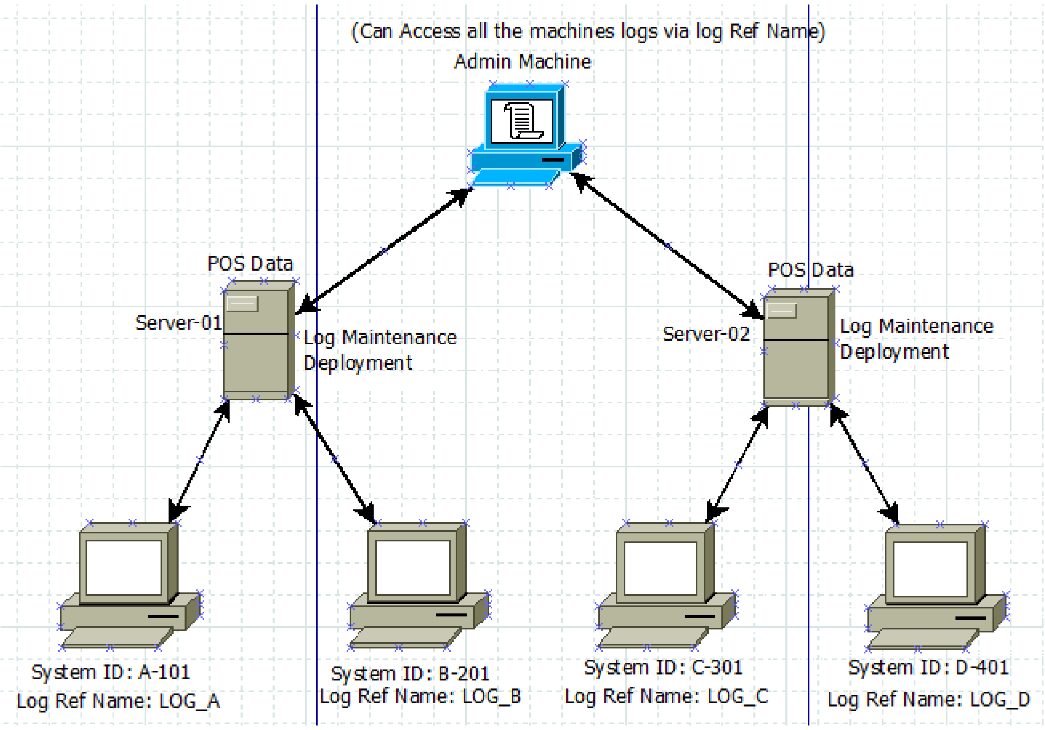


Figure 6.1: Log Maintenance Data Flow

Example: If we want to access machines A logs (where the application is running.)

1. First we need to add the one reference to the machines A log file (If machine A store its log in location C:/log folder and we add the Reference to that location as LOG-A.
2. By using the log view functionality we can access that log by just giving log reference (LOG-A). Now it will show list of log which is in C:/log folder.

3. Same as add, we can edit the log reference from LOG-A to some other name.

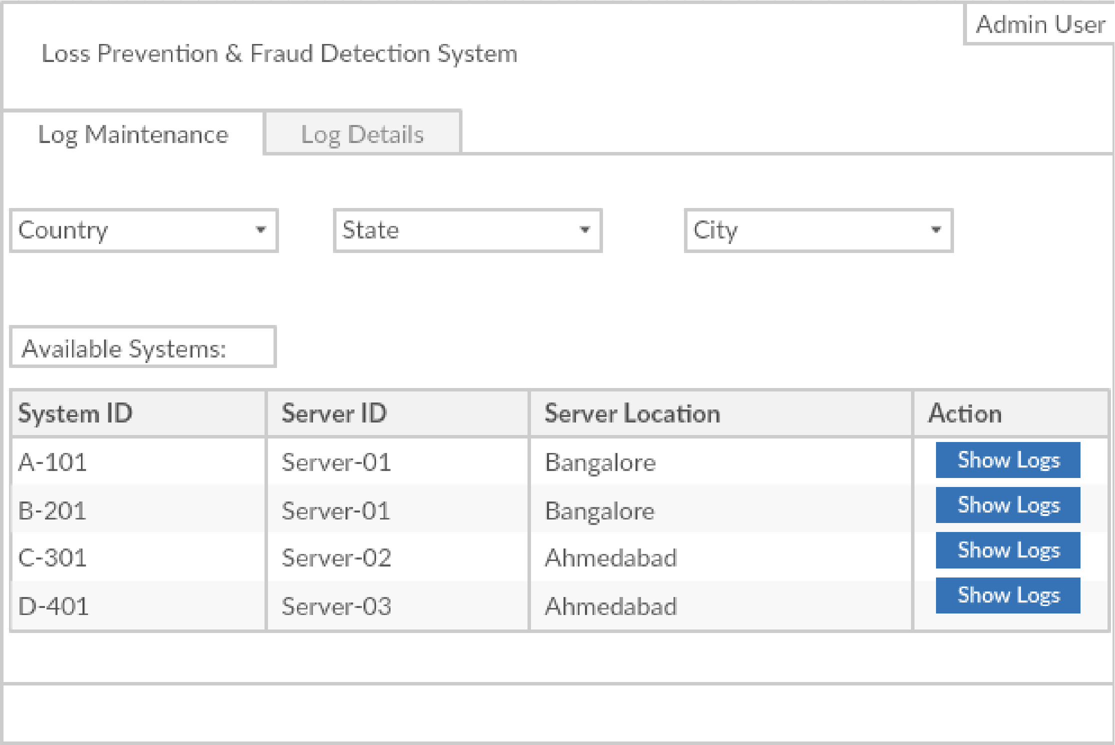
4. While we delete the log reference (LOG-A) it just remove the reference which is pointing to C:/log folder but not an actual file, actual file is still in C:/log folder.

To handle this much amount of data, system should have flexibility and scalability.Cloud give that functionality so this project will design in such a way so it can move to cloud and serve the need of customers dynamically.

6.3.1 Viewing the active systems

It will help user to view the connected system to the particular server. We can filter out the connected system by using three parameters.

- Country
- State
- City



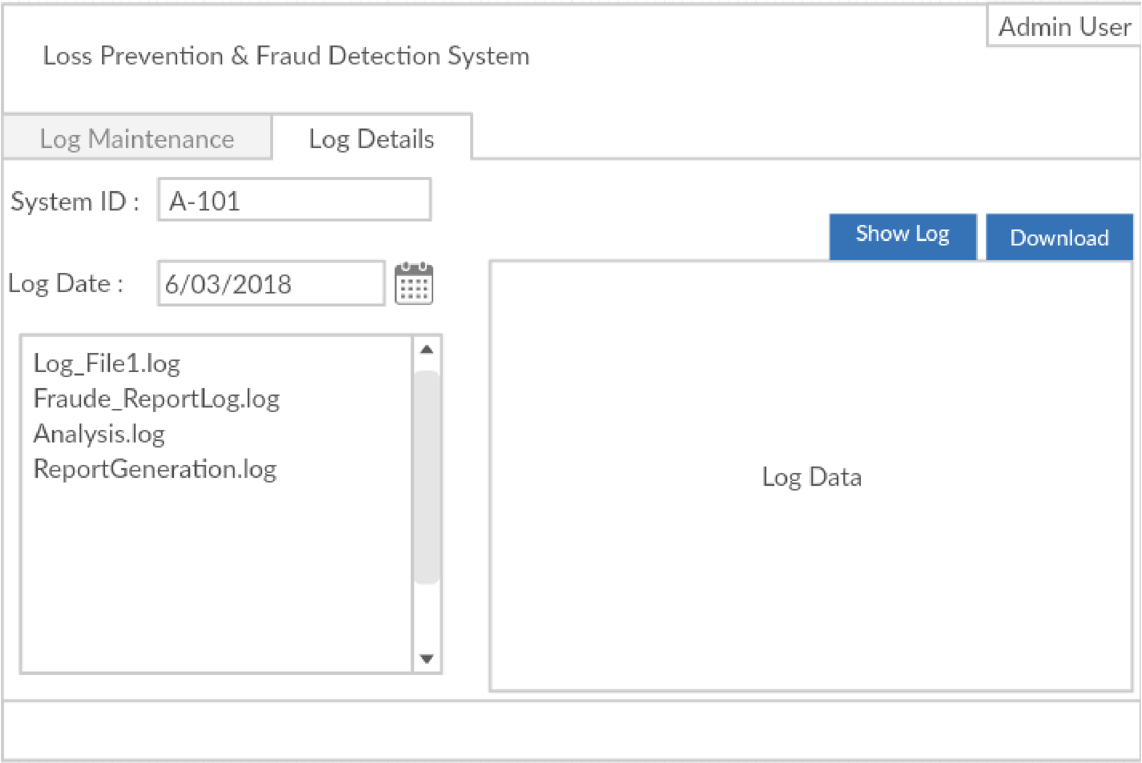
System ID	Server ID	Server Location	Action
A-101	Server-01	Bangalore	Show Logs
B-201	Server-01	Bangalore	Show Logs
C-301	Server-02	Ahmedabad	Show Logs
D-401	Server-03	Ahmedabad	Show Logs

Figure 6.2: Viewing Remote System

After selecting appropriate location filter, It will show SystemID, Connected server to that system (ServerID) and physical Location of server. It will contain show log action which will help to display logs of different server.

6.3.2 View/Download Systems Logs

This functionality will provide access to the remote machine's log. it is very easy for the user to view the log of different machine (Server) by using show log action from the given panel. It will display log detail of selected system according to the date filter.



System ID : A-101

Log Date : 6/03/2018

Log_File1.log
Fraude_ReportLog.log
Analysis.log
ReportGeneration.log

Figure 6.3: View/Download system's logs

This screen has major two functionality

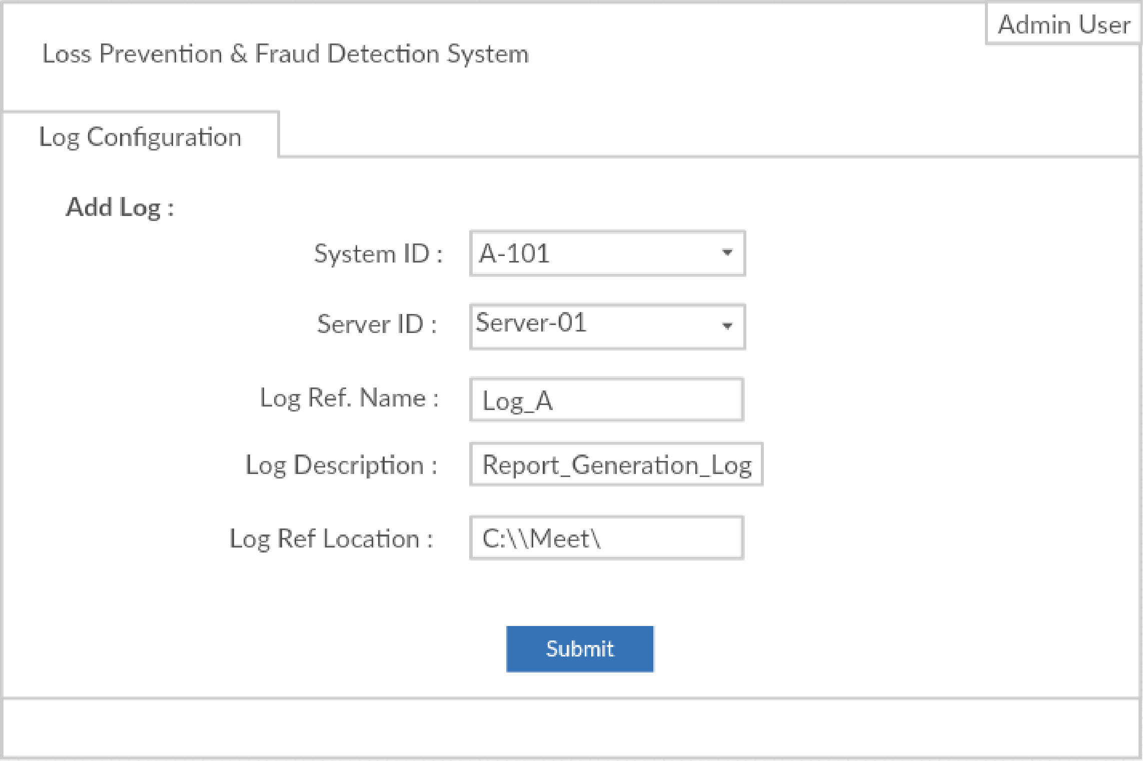
- Show Log : It will show the log within the application UI
- Download Log : It will download the log to local system

While executing show/download action , request will send to server and it will search log according to the given filter (Date) and display that log in view area. We can also download the file log and table log by using the download action.

6.3.3 Log Configuration

This functionality is available for admin user only to create/add or Edit log reference to specific system. By providing SystemID, ServerID, and Log location,User can add log reference which will reflected to viewing remote system screen.

Log Configuration Screen :



Add Log :

System ID : A-101

Server ID : Server-01

Log Ref. Name : Log_A

Log Description : Report_Generation_Log

Log Ref Location : C:\\Meet\

Figure 6.4: Add/Edit Log Configuration

Here user just add the log reference to particular server not the actual log file. Log file will generated by server its self according to the error or exception scenario.

Chapter 7

Application Auditing

7.1 Audit Framework

Application provide the interface between Users and sensitive data therefor application proper control on information flow are on top priority. To protect those data from user or keep eye on their action we require a frame work in such a way so it can monitor all required action from user. Purpose of the data auditing is used to capture the event or operation on the application data, it involves profiling of user data. Some data of the application are very sensitive and restricted to the admin users only. It is very useful in future to track the modification and access of sensitive data[12]. Auditing in application can be done via two ways:

1. Store the data in flat file
2. Store the data in database table

In this application audit data are store in database rather than flat file. There are several parameters needs to be define in database to store the auditing data. Parameters are mention below:

- User id :- Id of user who is accessing the data
- User role :- role of user (ex: Admin, Super User)
- Data and Time of auditing :- Exact date and time of accessing data in predefined format

- Performed action: - It store the user action on while accessing particular data, Action can be Create, Read, Update (modification of data) or Delete.
- Severity of action : It indicate severity of user action. it will be like high, low, medium
- Actual audit data: this data will be in Json format which contain all the accessed data. Like in case of adding new record in system it will track of that record along with user details.

Below is the pictorial representation of flow and different parameters of audit data.

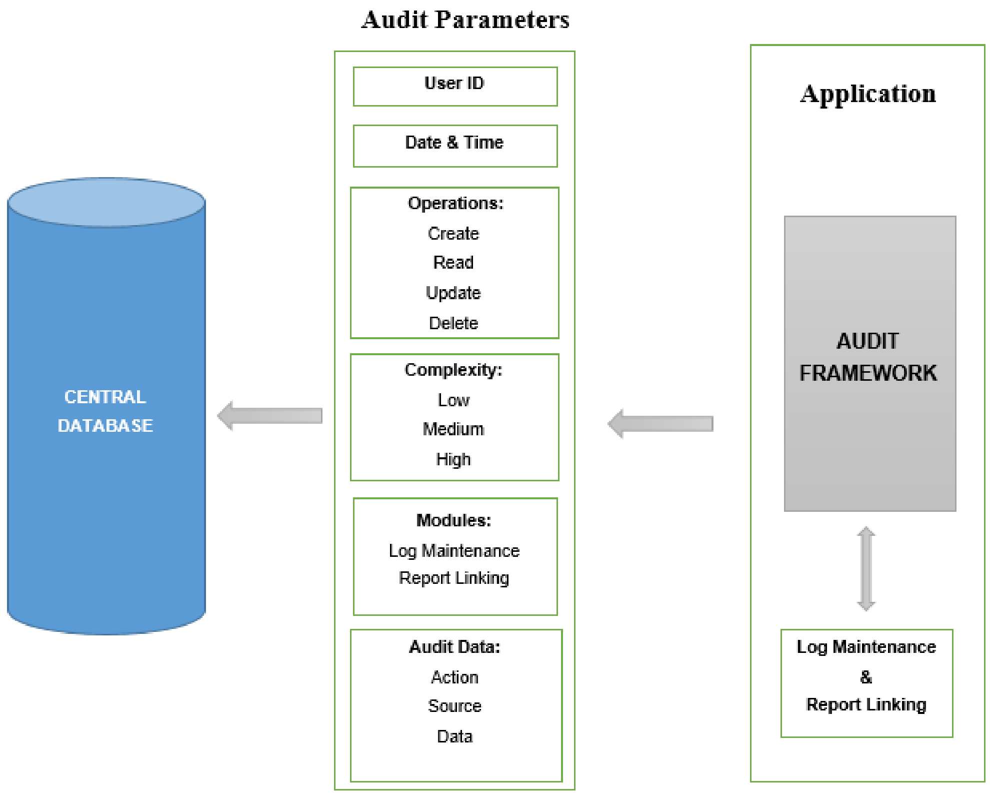


Figure 7.1: Audit Parameters

7.2 Data Auditing

In loss prevention and fraud detection system, we have different module to access the various functionality of application like report linking, Log maintenance, filter maintenance etc. Here I designed a frame work in such a way so any module can use this audit frame work to make auditing happen in various module. Here is the explanation of how audit framework implemented in log maintenance features. There are several request will be initiate while serving output or result of requested module[13].

- Choose one module and execute from System UI
- Request will initiate for accessed module
- set required parameter to initiated request and REST call will execute to the server
- Before serving output to System UI , It will call the audit framework to store the audit data in database
- After successful auditing of data, output will displayed to User for a requested module

Flow diagram of audit data framework:

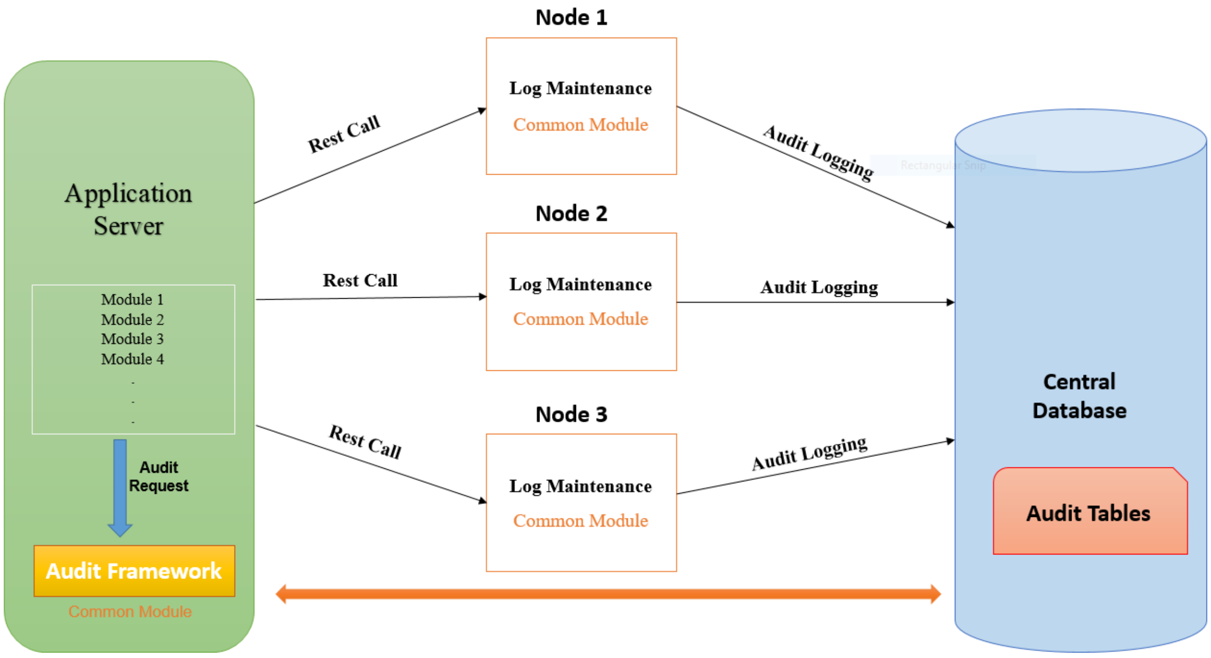
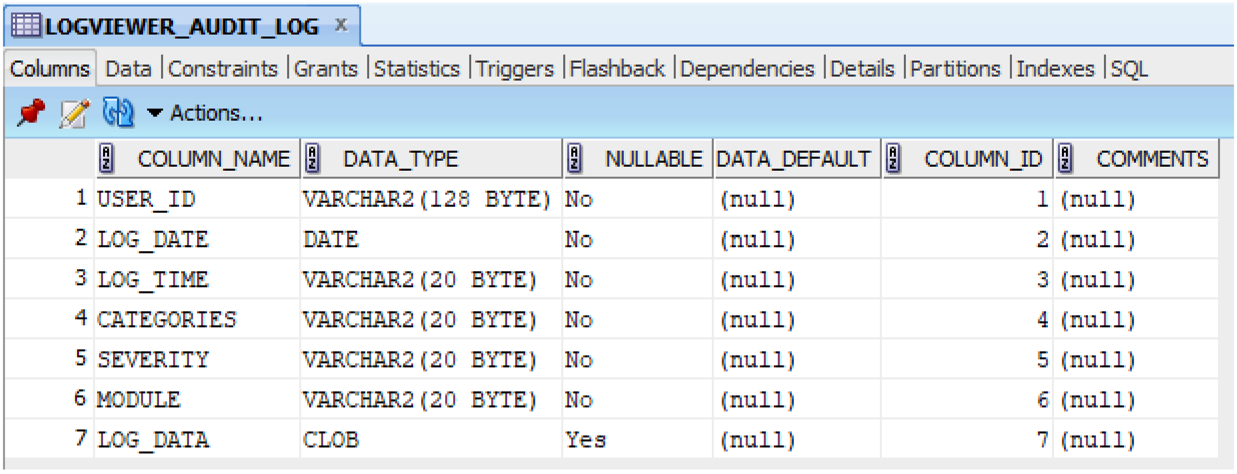


Figure 7.2: Audit Data-Flow

7.2.1 Audit Database

Here the screen shots for LOGVIEWER-AUDIT-TABLE:

As here all the columns which are present in table are defined with their data type, with nullable property (whether it will be null or not), Default data that will be present, COLUMN-ID assigned to each column of table and their respective comments[14].


LOGVIEWER_AUDIT_LOG
Columns | Data | Constraints | Grants | Statistics | Triggers | Flashback | Dependencies | Details | Partitions | Indexes | SQL
Actions...

	COLUMN_NAME	DATA_TYPE	NULLABLE	DATA_DEFAULT	COLUMN_ID	COMMENTS
1	USER_ID	VARCHAR2(128 BYTE)	No	(null)	1	(null)
2	LOG_DATE	DATE	No	(null)	2	(null)
3	LOG_TIME	VARCHAR2(20 BYTE)	No	(null)	3	(null)
4	CATEGORIES	VARCHAR2(20 BYTE)	No	(null)	4	(null)
5	SEVERITY	VARCHAR2(20 BYTE)	No	(null)	5	(null)
6	MODULE	VARCHAR2(20 BYTE)	No	(null)	6	(null)
7	LOG_DATA	CLOB	Yes	(null)	7	(null)

Figure 7.3: Audit Table

Properties are defined for various attributes of audit table due to certain assumptions/reasons[15].

- USER-ID: Its data type should be varchar of 128 bytes as the name of person can be too long. It cannot be null as it must contains user name on audit.

- LOG-DATE: Log date data type must be of DATE type which defined for storing dates in DATABASE. It also cannot be null as it take system date.

- LOG-TIME: It is stored in data type that is varchar. It takes system time and hence it must be in fixed format which leads to store in fixed size that is less than to 20bytes.

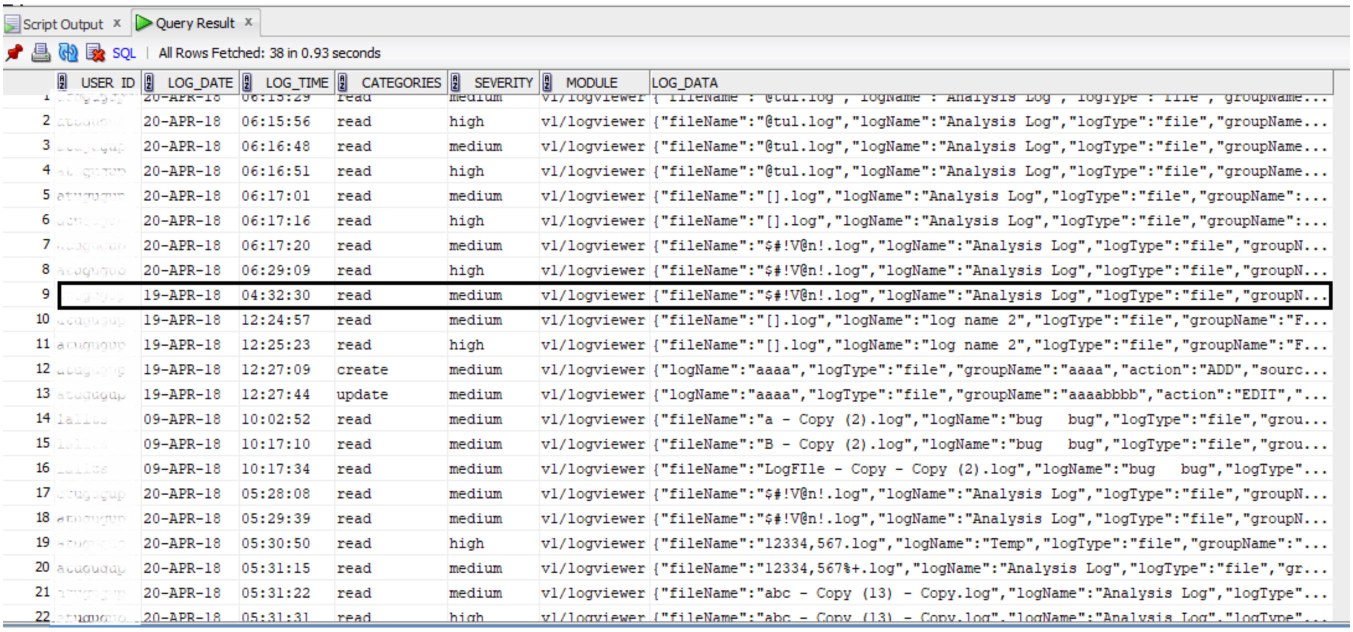
- CATEGORIES/OPERATIONS: It defines CRUD operations which are fixed in length and of string type. Hence, VARCHAR2 of 20 bytes is suitable data type for it. It also cannot be null.

- SEVERITY/COMPLEXITY: It tell about complexity whether it can be HIGH,MEDIUM,LOW and it will also be of string type with length than 20 bytes, hence VARCHAR2 of 20 bytes is suitable for it.

- MODULE: It tell about user accessing the module. None module in application have name length more than 20 bytes.

- LOG-DATA/AUDIT-DATA: It stores JSON object as its data. Hence it leads to store as in the format of CLOB. In this field data can be null if user just trying to access module but not trying to access sensitive data.

Column id are by default generated at the time of adding fields to table.
User who can access database can put comment for description against each column of table.
Screenshot displays how the data of an audit log stored into database:
Audit log 9th entry contains some user name, 19-APR-18 as date, 04:32:30 as time, read as operation, medium as complexity, log viewer as module name and JSON of filename, log name, logotype etc. as Audit data.
Audit Logs:



	USER ID	LOG_DATE	LOG_TIME	CATEGORIES	SEVERITY	MODULE	LOG_DATA
1	[redacted]	20-APR-18	06:15:29	read	medium	vl/logviewer	{"fileName":"@tul.log","logName":"Analysis Log","logType":"file","groupName...
2	[redacted]	20-APR-18	06:15:56	read	high	vl/logviewer	{"fileName":"@tul.log","logName":"Analysis Log","logType":"file","groupName...
3	[redacted]	20-APR-18	06:16:48	read	medium	vl/logviewer	{"fileName":"@tul.log","logName":"Analysis Log","logType":"file","groupName...
4	[redacted]	20-APR-18	06:16:51	read	high	vl/logviewer	{"fileName":"@tul.log","logName":"Analysis Log","logType":"file","groupName...
5	[redacted]	20-APR-18	06:17:01	read	medium	vl/logviewer	{"fileName":"[].log","logName":"Analysis Log","logType":"file","groupName":...
6	[redacted]	20-APR-18	06:17:16	read	high	vl/logviewer	{"fileName":"[].log","logName":"Analysis Log","logType":"file","groupName":...
7	[redacted]	20-APR-18	06:17:20	read	medium	vl/logviewer	{"fileName":"$#!V@n!.log","logName":"Analysis Log","logType":"file","groupN...
8	[redacted]	20-APR-18	06:29:09	read	high	vl/logviewer	{"fileName":"$#!V@n!.log","logName":"Analysis Log","logType":"file","groupN...
9	[redacted]	19-APR-18	04:32:30	read	medium	vl/logviewer	{"fileName":"$#!V@n!.log","logName":"Analysis Log","logType":"file","groupN...
10	[redacted]	19-APR-18	12:24:57	read	medium	vl/logviewer	{"fileName":"[].log","logName":"log name 2","logType":"file","groupName":"F...
11	[redacted]	19-APR-18	12:25:23	read	high	vl/logviewer	{"fileName":"[].log","logName":"log name 2","logType":"file","groupName":"F...
12	[redacted]	19-APR-18	12:27:09	create	medium	vl/logviewer	{"logName":"aaaa","logType":"file","groupName":"aaaa","action":"ADD","sourc...
13	[redacted]	19-APR-18	12:27:44	update	medium	vl/logviewer	{"logName":"aaaa","logType":"file","groupName":"aaaabbbb","action":"EDIT","...
14	[redacted]	09-APR-18	10:02:52	read	medium	vl/logviewer	{"fileName":"a - Copy (2).log","logName":"bug bug","logType":"file","grou...
15	[redacted]	09-APR-18	10:17:10	read	medium	vl/logviewer	{"fileName":"B - Copy (2).log","logName":"bug bug","logType":"file","grou...
16	[redacted]	09-APR-18	10:17:34	read	medium	vl/logviewer	{"fileName":"LogFIle - Copy - Copy (2).log","logName":"bug bug","logType"...
17	[redacted]	20-APR-18	05:28:08	read	medium	vl/logviewer	{"fileName":"$#!V@n!.log","logName":"Analysis Log","logType":"file","groupN...
18	[redacted]	20-APR-18	05:29:39	read	medium	vl/logviewer	{"fileName":"$#!V@n!.log","logName":"Analysis Log","logType":"file","groupN...
19	[redacted]	20-APR-18	05:30:50	read	high	vl/logviewer	{"fileName":"12334,567.log","logName":"Temp","logType":"file","groupName":"...
20	[redacted]	20-APR-18	05:31:15	read	medium	vl/logviewer	{"fileName":"12334,567%+.log","logName":"Analysis Log","logType":"file","gr...
21	[redacted]	20-APR-18	05:31:22	read	medium	vl/logviewer	{"fileName":"abc - Copy (13) - Copy.log","logName":"Analysis Log","logType"...
22	[redacted]	20-APR-18	05:31:31	read	high	vl/logviewer	{"fileName":"abc - Copy (13) - Copy.log","logName":"Analysis Log","logType"...

Chapter 8

Application Security Scan

8.1 Application Scanning

Loss prevention and fraud detection system is a web application(web Project). It is frequently transferred data over the network.
Path manipulation errors occur when the following two conditions are met:

- An attacker can specify a path used in an operation on the file system.
- By specifying the resource, the attacker gains a capability that would not otherwise be permitted.

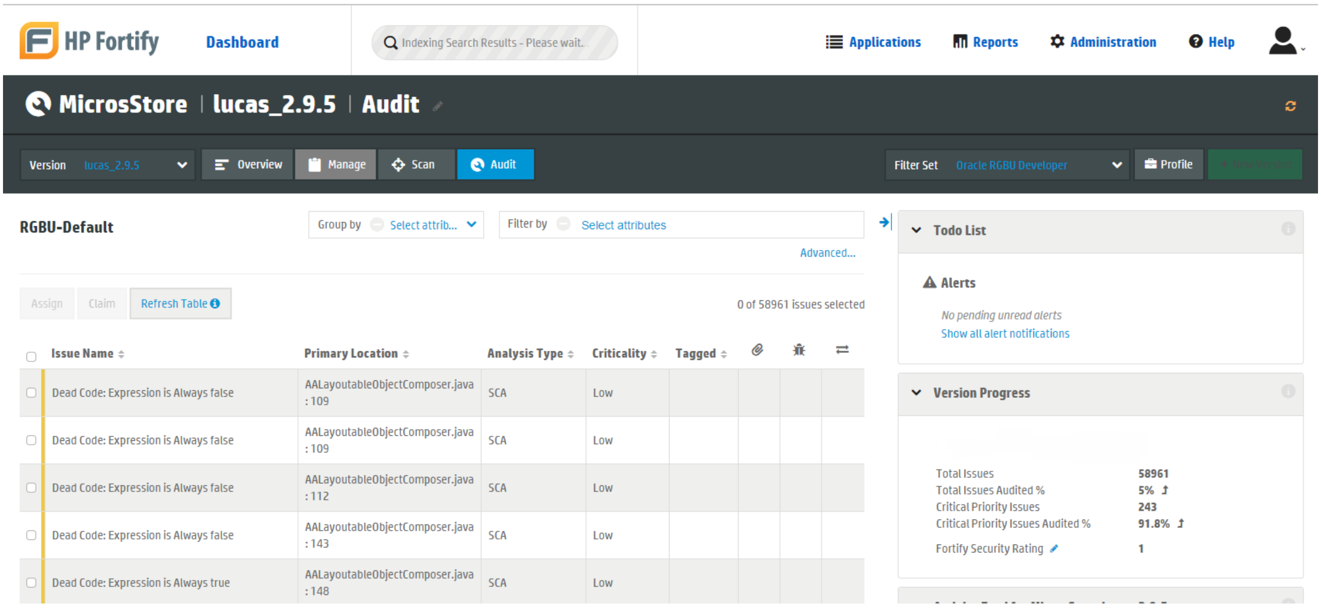
For example, the program may give the attacker the ability to overwrite the specified file or run with a configuration controlled by the attacker[14]. In this case, the attacker can specify the value that enters the program at particular field in and this value is used to access a file-system resource.
There are the several well known vulnerability which could be found at a time of security scanning. Like:

- Resource data-flow Vulnerability
- Path manipulation Vulnerability
- Application information leak vulnerability
- Unreleased resource vulnerability

8.2 Fortify Scan

It is a tool for checking security vulnerability in the application. It prioritizes vulnerability by severity and importance. It helps to find the root cause of security issues. It will pinpoint to exact location/ line where attacker can expose the system. It has a capability to analyze the static codes in different language and also support various IDEs integration (ex: Eclipse, NetBeans). We can also build our custom rule for security scanning of application[13].

It categories security issues by it's severity. It may be high, medium, low or by severity number(1,2,3). It will highlight primary location, Issue name, Analysis type etc on dashboard. Below is the dashboard of fortify tool:



MicrosStore | lucas_2.9.5 | Audit

Version lucas_2.9.5

Filter Set Oracle RGBU Developer

RGBU-Default

Group by Select attrib...

Filter by Select attributes

0 of 58961 issues selected

Issue Name	Primary Location	Analysis Type	Criticality	Tagged
Dead Code: Expression is Always false	AALayoutableObjectComposer.java : 109	SCA	Low	
Dead Code: Expression is Always false	AALayoutableObjectComposer.java : 109	SCA	Low	
Dead Code: Expression is Always false	AALayoutableObjectComposer.java : 112	SCA	Low	
Dead Code: Expression is Always false	AALayoutableObjectComposer.java : 143	SCA	Low	
Dead Code: Expression is Always true	AALayoutableObjectComposer.java : 148	SCA	Low	

Alerts

No pending unread alerts

Show all alert notifications

Total Issues	58961
Total Issues Audited %	5%
Critical Priority Issues	243
Critical Priority Issues Audited %	91.8%
Fortify Security Rating	1

Figure 8.1: Fortify Dashboard

As standard by the industries, If scanning results have severity issues which is belong to high or medium category then application can not be release to production environment but severity low category issues are fine for them and it will gradually evolve as application enhance. Most of the type low category issues occur due to bad coding practice.

8.2.1 Analyze & Prevent Vulnerability

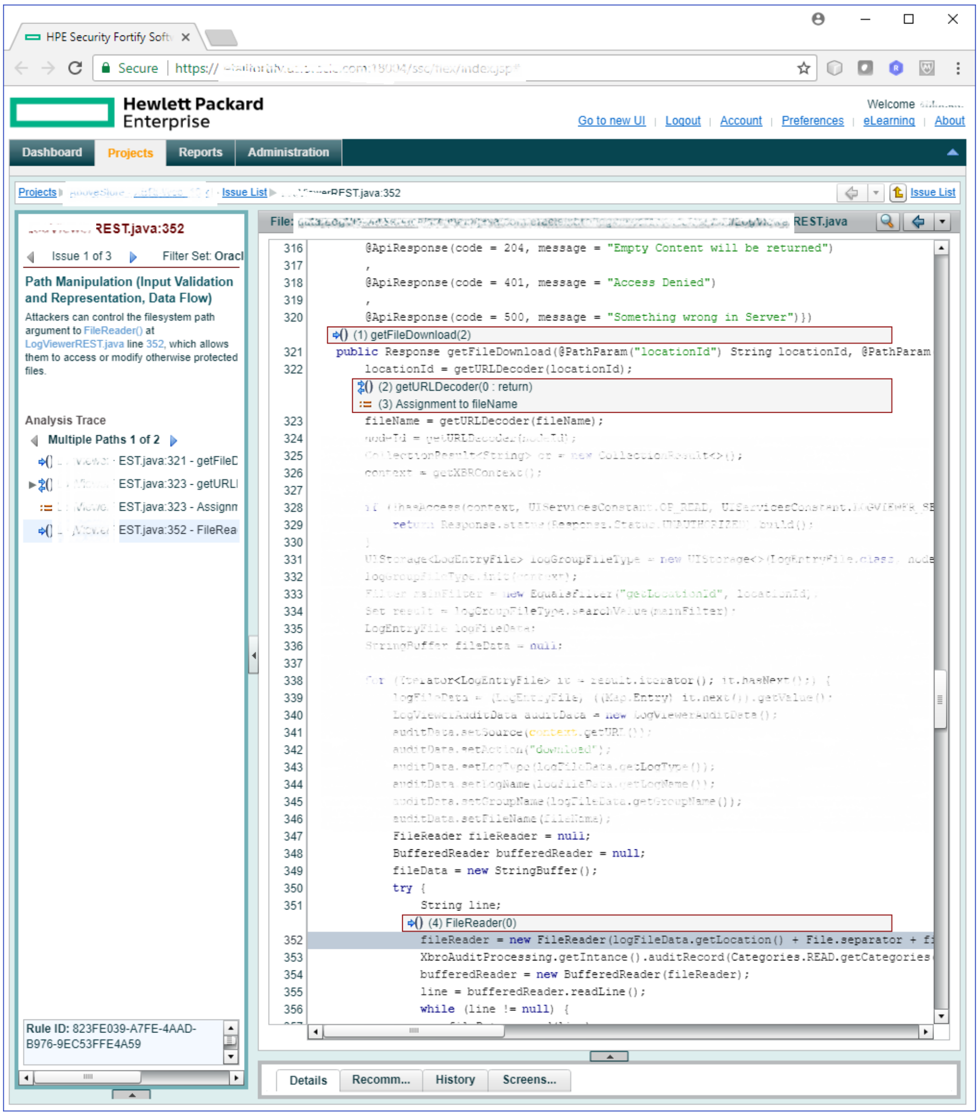
The best way to prevent path manipulation is with a level of indirection. create a list of legitimate resource names that a user is allowed to specify, and only allow the user to select from the list. With this approach the input provided by the user is never used directly to specify the resource name. In some situations this approach is impractical because the set of legitimate resource names is too large or too hard to keep track of. Programmers often resort to blacklisting in these situations. Blacklisting selectively rejects or escapes potentially dangerous characters before using the input[12]. However, any such list of unsafe characters is likely to be incomplete and will almost certainly become out of date. A better approach is to create a whitelist of characters that are allowed to appear in the resource name and accept input composed exclusively of characters in the approved set. There are some way to Prevent Vulnerability:

1. If the program is performing input validation, satisfy yourself that the validation is correct, and use the HPE Security Fortify Custom Rules Editor to create a cleanse rule for the validation routine.

2. Implementation of an effective blacklist is notoriously difficult. One should be skeptical if validation logic requires blacklisting. Consider different types of input encoding and different sets of meta-characters that might have special meaning when interpreted by different operating systems, databases, or other resources. Determine whether or not the blacklist can be updated easily, correctly, and completely if these requirements ever change.

3. A number of modern web frameworks provide mechanisms for performing validation of user input. Struts and Spring MVC are among them. To highlight the unvalidated sources of input, the HPE Security Fortify Secure Coding Rulepacks dynamically re-prioritize the issues reported by HPE Security Fortify Static Code Analyzer by lowering their probability of exploit and providing pointers to the supporting evidence whenever the framework validation mechanism is in use.

Below is the screen shot of how fortify can detect the security loop holes in the application.



HPE Security Fortify Soft
Secure | https:// [redacted]
Hewlett Packard Enterprise
Welcome [redacted]
Go to new UI | Logout | Account | Preferences | eLearning | About
Dashboard
Projects
Reports
Administration
Projects ▸ [redacted] ▸ Issue List ▸ [redacted]REST.java:352
Issue List
File: [redacted] REST.java
Details
Recomm...
History
Screens...

[redacted]REST.java:352

Issue 1 of 3 Filter Set: Oracl

Path Manipulation (Input Validation and Representation, Data Flow)

Attackers can control the filesystem path argument to FileReader() at LogViewerREST.java line 352, which allows them to access or modify otherwise protected files.

Analysis Trace

Multiple Paths 1 of 2

- [redacted] EST.java:321 - getFileD
- [redacted] EST.java:323 - getURLI
- [redacted] EST.java:323 - Assignm
- [redacted] EST.java:352 - FileRea

Rule ID: 823FE039-A7FE-4AAD-B976-9EC53FFE4A59

```
    @ApiResponse(code = 204, message = "Empty Content will be returned")
    ,
    @ApiResponse(code = 401, message = "Access Denied")
    ,
    @ApiResponse(code = 500, message = "Something wrong in Server")})
  (1) getFileDownload(2)
public Response getFileDownload(@PathParam("locationId") String locationId, @PathParam
    locationId = getURLDecoder(locationId);
    (2) getURLDecoder(0 : return)
    (3) Assignment to fileName
    fileName = getURLDecoder(fileName);
    [redacted]
        FileReader fileReader = null;
        BufferedReader bufferedReader = null;
        fileData = new StringBuffer();
        try {
            String line;
          (4) FileReader(0)
            fileReader = new FileReader(logFileData.getLocation() + File.separator + fi
            XbroAuditProcessing.getIntance().auditRecord(Categories.READ.getCategories
            bufferedReader = new BufferedReader(fileReader);
            line = bufferedReader.readLine();
            while (line != null) {
```

Figure 8.2: Fortify Scan Result

8.2.2 Benefit of Fortify

- It will reduce the development cost by finding vulnerability issues in early development phase[15].
- It will enable to secure coding for the application.
- It will help in remediation of security vulnerability
- It provides correlation and priorities the results

Bibliography

[1] J. Hillmer, R. Jones, C. Gessner, C. Johnston, K. Lewis, and S. Deshpande, "System and method for detecting fraudulent transactions," Mar. 30 2004. US Patent 6,714,918.

[2] A. Kukic, "Cookies vs. tokens: The definitive guide," 2016.

[3] J. Shapland, "Preventing retail-sector crimes," *Crime and Justice*, vol. 19, pp. 263–342, 1995.

[4] B. Goodman, "Loss prevention and sales productivity cloud services," 2017.

[5] C. Welch, J. Rozmus, J. Whiteman, M. Negin, and W. Herd, "System and methods for preventing fraud in retail environments, including the detection of empty and non-empty shopping carts," Mar. 16 1999. US Patent 5,883,968.

[6] K. Cook, "Method and system for the detection, management and prevention of losses in retail and other environments," Apr. 20 1999. US Patent 5,895,453.

[7] M. Haekal and Eliyani, "Token-based authentication using json web token on sikasir restful web service," in *2016 International Conference on Informatics and Computing (ICIC)*, pp. 175–179, Oct 2016.

[8] P. Otemuyiwa, "Json web tokens vs. session cookies: In practice," 2016.

[9] S. Peyrott, *JWT Handbook*.

[10] P. Solapurkar, "Building secure healthcare services using oauth 2.0 and json web token in iot cloud scenario," in *2016 2nd International Conference on Contemporary Computing and Informatics (IC3I)*, pp. 99–104, Dec 2016.

[11] R. Damphousse, "Build secure user interfaces using json web tokens (jwts)," 2015.

[12] L. K. Shar and H. B. K. Tan, “Auditing the xss defence features implemented in web application programs,” *IET Software*, vol. 6, pp. 377–390, August 2012.

[13] S. Hiremath and S. Kunte, “A novel data auditing approach to achieve data privacy and data integrity in cloud computing,” in *2017 International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT)*, pp. 306–310, Dec 2017.

[14] S. Sasmal and I. Pan, “Mutual auditing framework for service level security auditing in cloud,” in *2017 Third International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN)*, pp. 297–302, Nov 2017.

[15] L. K. Shar and H. B. K. Tan, “Auditing the xss defence features implemented in web application programs,” *IET Software*, vol. 6, pp. 377–390, August 2012.