INDEX

Sr. no.	Practical	Date	Signature
1	Creating Data Model using Cassandra		
2	Organising Data in Cassandra		
3	Retrieving Data in Cassandra		
4	Conversion from different format to HOURS model		
5	Describe and Expand, Drop/Delete for assessing data		
6	Data processing in rstudio		
7	Data transformation or Cleaning		
8	Data visualization using powerBI		
9	Auditing and utilities in PowerBI		
10	Generating reports in PowerBI		
11	Review Paper		

Practical No. 1

Aim:- Creating Data Model using Cassandra.

Steps:

Create keyspace

```
CREATE KEYSPACE student_information
 WITH REPLICATION = {
  'class' : 'SimpleStrategy',
  'replication_factor' : 1
 };
```

Use keyspace

```
use  student_information;
```

Similarly create another key space and access it.

Eg emp_info

Sign:_________________

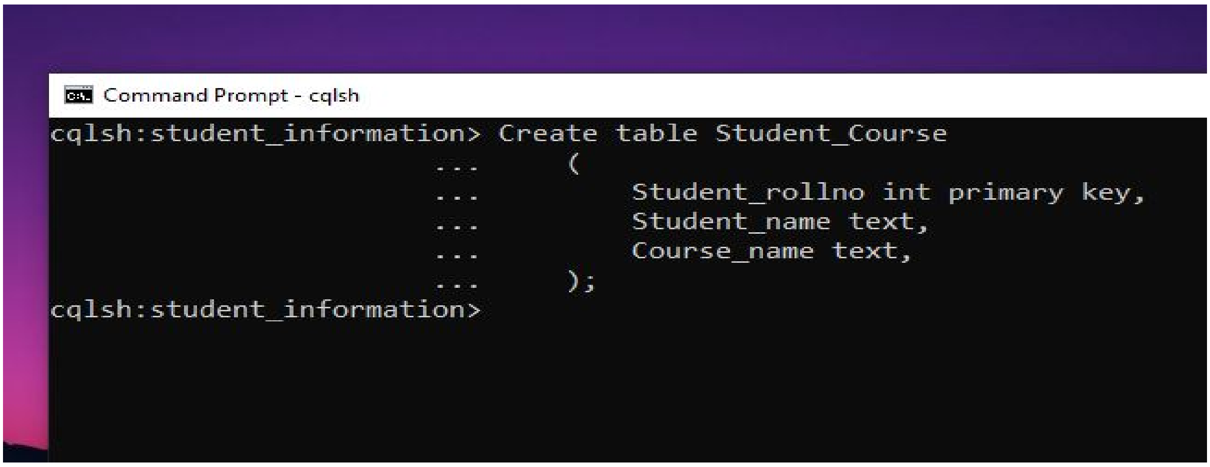
Practical No.2

Aim:- Organising the Data in Cassandra.

Steps

Create table

```
Create table Student_Course
   (
      Student_rollno int primary key,
      Student_name text,
      Course_name text,
   );
```



```
cqlsh:student_information> Create table Student_Course
                       ...     (
                       ...         Student_rollno int primary key,
                       ...         Student_name text,
                       ...         Course_name text,
                       ...     );
cqlsh:student_information>
```

Insert values in Student_Course

```
Insert into student_information.Student_course(Student_rollno,
Student_name, Course_name) values
(1, ‘abcd’,’data-science’);

Insert into student_information.Student_course(Student_rollno,
Student_name, Course_name) values
(2, ‘xyz’,’cloud-computing’);
```

Sign:________________

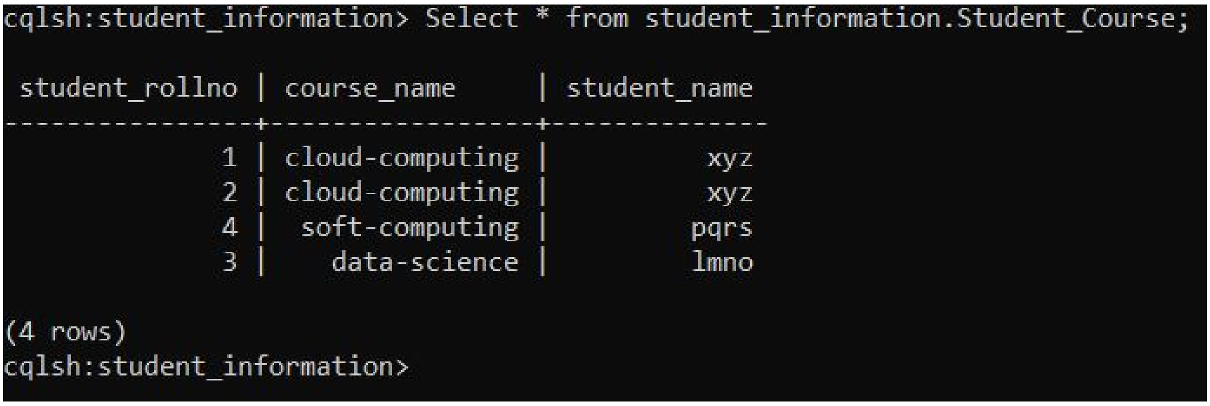
Practical No.3

Aim:- Retrieving Data in Cassandra

Steps:-

Displaying values

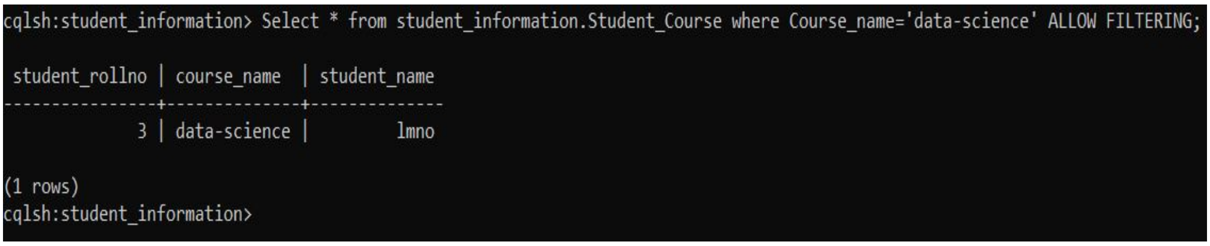
```
Select * from student_infromation.Student_Course;
```



```
cqlsh:student_information> Select * from student_information.Student_Course;

 student_rollno | course_name     | student_name
----------------+-----------------+--------------
              1 | cloud-computing |          xyz
              2 | cloud-computing |          xyz
              4 |  soft-computing |         pqrs
              3 |    data-science |         lmno

(4 rows)
cqlsh:student_information>
```

Displaying filtered with values

```
Select * from student_information.Student_Course where
Course_name='data-science' ALLOW FILTERING;
```



```
cqlsh:student_information> Select * from student_information.Student_Course where Course_name='data-science' ALLOW FILTERING;

 student_rollno | course_name  | student_name
----------------+--------------+--------------
              3 | data-science |         lmno

(1 rows)
cqlsh:student_information>
```

Sign:__________________

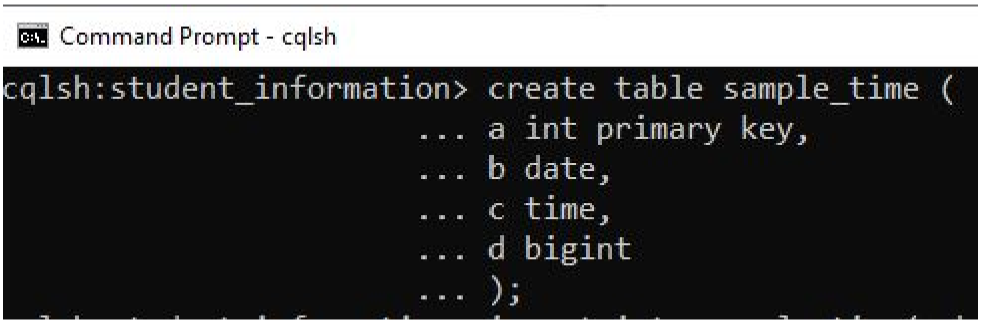
Practical no. 4

Aim:- Conversion from different format of HOURS Model.

Steps

1. Create table with int *(primary key)*, date, time and bigint datatype.

```
Create table sample_time(a int primary key, b date, c time,
d bigint);
```



```
cqlsh:student_information> create table sample_time (
                       ... a int primary key,
                       ... b date,
                       ... c time,
                       ... d bigint
                       ... );
```

2. We will store timestamp value in big int and then convert the value to date type.

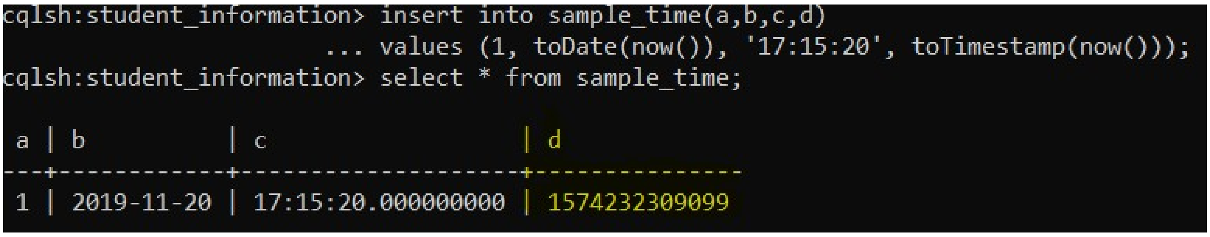
3. Insert values in the table.

```
Insert into sample_time (a,b,c,d) values (1,
toDate(now()), ’17:15:20’, toTimestamp(now()));
```

now() is use to get current time.

4. Displaying the table values

```
Select * from sample_time;
```

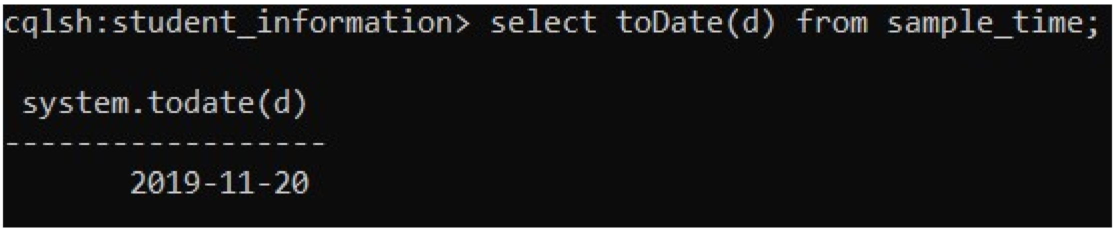


```
cqlsh:student_information> insert into sample_time(a,b,c,d)
                       ... values (1, toDate(now()), '17:15:20', toTimestamp(now()));
cqlsh:student_information> select * from sample_time;

 a | b          | c                  | d
---+------------+--------------------+---------------
 1 | 2019-11-20 | 17:15:20.000000000 | 1574232309099
```

As we can see the value in d column is in the bigint format. We need to convert this value to date format.

5. Converting to date format

```
Select toDate(d) from sample_time;
```



```
cqlsh:student_information> select toDate(d) from sample_time;

 system.todate(d)
------------------
       2019-11-20
```

Sign:__________________

Practical No. 5

Aim:- Describe and Expand, Drop/Delete for assessing data

Describe

This command describes the current cluster of Cassandra and its objects. The variants of this command are explained below.

Describe cluster − This command provides information about the cluster.

```
cqlsh:tutorialspoint> describe cluster;

Cluster: Test Cluster
Partitioner: Murmur3Partitioner

Range ownership:
                  -658380912249644557 [127.0.0.1]
                  -2833890865268921414 [127.0.0.1]
                  -6792159006375935836 [127.0.0.1]
```

Describe Keyspaces − This command lists all the keyspaces in a cluster. Given below is the usage of this command.

```
cqlsh:tutorialspoint> describe keyspaces;

system_traces system tp tutorialspoint
```

Describe tables − This command lists all the tables in a keyspace. Given below is the usage of this command.

```
cqlsh:tutorialspoint> describe tables;
emp
```

Describe table − This command provides the description of a table. Given below is the usage of this command.

```
cqlsh:tutorialspoint> describe table emp;
```

Describe Type

This command is used to describe a user-defined data type. Given below is the usage of this command.

```
cqlsh:tutorialspoint> describe type card_details;

CREATE TYPE tutorialspoint.card_details (
   num int,
   pin int,
   name text,
   cvv int,
   phone set<int>,
   mail text
);
```

Describe Types

This command lists all the user-defined data types. Given below is the usage of this command. Assume there are two user-defined data types: **card** and **card_details**.

```
cqlsh:tutorialspoint> DESCRIBE TYPES;

card_details card
```

Expand

This command is used to expand the output. Before using this command, you have to turn the expand command on. Given below is the usage of this command.

```
cqlsh:tutorialspoint> expand on;
cqlsh:tutorialspoint> select * from emp;

@ Row 1
-----------+------------
    emp_id | 1
  emp_city | Hyderabad
  emp_name | ram
 emp_phone | 9848022338
   emp_sal | 50000

@ Row 2
-----------+------------
    emp_id | 2
  emp_city | Delhi
  emp_name | robin
 emp_phone | 9848022339
   emp_sal | 50000
```

Dropping a Table

You can drop a table using the command **Drop Table**. Its syntax is as follows −

Syntax

```
DROP TABLE <tablename>
```

Example

The following code drops an existing table from a KeySpace.

```
cqlsh:tutorialspoint> DROP TABLE emp;
```

Sign:__________________

Practical No. 6

Data processing in rstudio

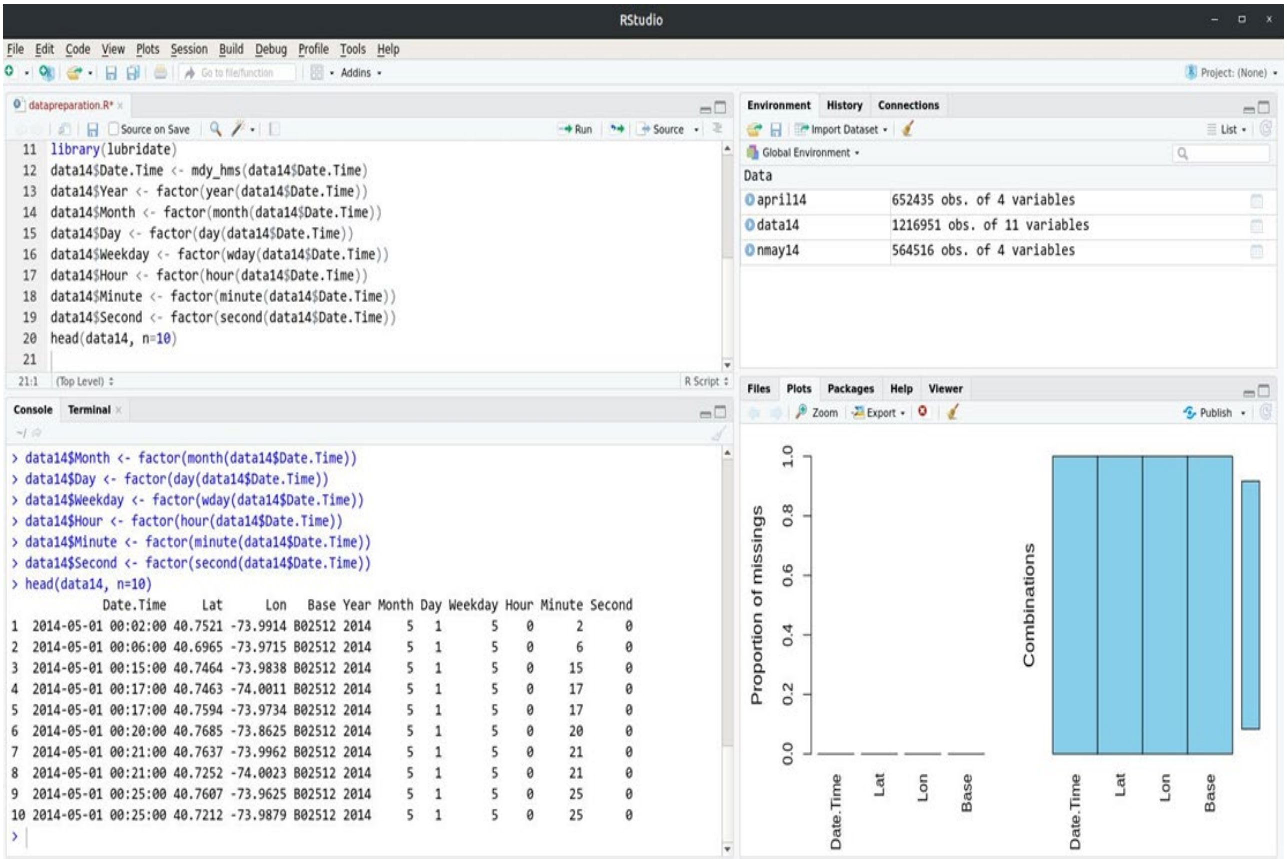
Aim: To perform Data processing and extraction from given dataset in R-Studio

Data Preparation takes most of the time in data science projects. Dataset with clean data and

simpler model is most likely to outperform dataset with ambiguous data and complicated model.

Code:

```
install.packages("dplyr")

install.packages("VIM")

install.packages("lubridate")

april14<-read.csv("https://goo.gl/cHtDVX")

nmay14 <- read.csv("https://goo.gl/vD21bs")

library(dplyr)

data14<-bind_rows(april14,nmay14)

summary(data14)

library(VIM)

aggr(data14)

library(lubridate)

data14$Date.Time <- mdy_hms(data14$Date.Time)

data14$Year <- factor(year(data14$Date.Time))

data14$Month <- factor(month(data14$Date.Time))

data14$Day <- factor(day(data14$Date.Time))

data14$Weekday <- factor(wday(data14$Date.Time))

data14$Hour <- factor(hour(data14$Date.Time))

data14$Minute <- factor(minute(data14$Date.Time))

data14$Second <- factor(second(data14$Date.Time))

head(data14, n=10)
```



```
library(lubridate)
data14$Date.Time <- mdy_hms(data14$Date.Time)
data14$Year <- factor(year(data14$Date.Time))
data14$Month <- factor(month(data14$Date.Time))
data14$Day <- factor(day(data14$Date.Time))
data14$Weekday <- factor(wday(data14$Date.Time))
data14$Hour <- factor(hour(data14$Date.Time))
data14$Minute <- factor(minute(data14$Date.Time))
data14$Second <- factor(second(data14$Date.Time))
head(data14, n=10)
```

```
> data14$Month <- factor(month(data14$Date.Time))
> data14$Day <- factor(day(data14$Date.Time))
> data14$Weekday <- factor(wday(data14$Date.Time))
> data14$Hour <- factor(hour(data14$Date.Time))
> data14$Minute <- factor(minute(data14$Date.Time))
> data14$Second <- factor(second(data14$Date.Time))
> head(data14, n=10)
             Date.Time     Lat      Lon   Base Year Month Day Weekday Hour Minute Second
1  2014-05-01 00:02:00 40.7521 -73.9914 B02512 2014     5   1       5    0      2      0
2  2014-05-01 00:06:00 40.6965 -73.9715 B02512 2014     5   1       5    0      6      0
3  2014-05-01 00:15:00 40.7464 -73.9838 B02512 2014     5   1       5    0     15      0
4  2014-05-01 00:17:00 40.7463 -74.0011 B02512 2014     5   1       5    0     17      0
5  2014-05-01 00:17:00 40.7594 -73.9734 B02512 2014     5   1       5    0     17      0
6  2014-05-01 00:20:00 40.7685 -73.8625 B02512 2014     5   1       5    0     20      0
7  2014-05-01 00:21:00 40.7637 -73.9962 B02512 2014     5   1       5    0     21      0
8  2014-05-01 00:21:00 40.7252 -74.0023 B02512 2014     5   1       5    0     21      0
9  2014-05-01 00:25:00 40.7607 -73.9625 B02512 2014     5   1       5    0     25      0
10 2014-05-01 00:25:00 40.7212 -73.9879 B02512 2014     5   1       5    0     25      0
> 
```

Data

april14	652435 obs. of 4 variables
data14	1216951 obs. of 11 variables
nmay14	564516 obs. of 4 variables

Sign:__________________

Practical No. 7

Data transformation or Cleaning

Aim: To perform data cleaning by replacing missing values in R-Studio

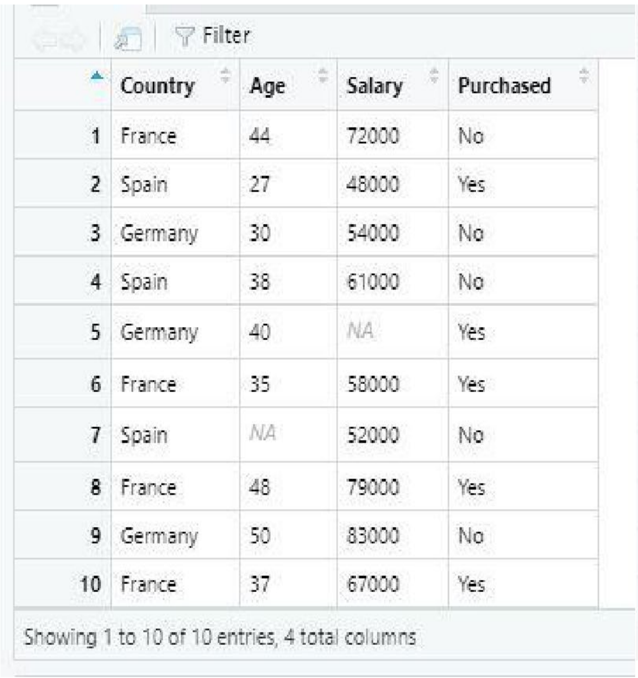
Data cleaning is a process of detecting and removing inaccurate data from the dataset. In data cleaning we identify incomplete, inaccurate, incorrect, irrelevant part of data and replace, modify of delete the data. In our dataset missing values are replaced with the average value of that column.

Code:

```
install.packages('VIM')

library(VIM)

#import data.csv from excel file

library(readr)

Data <- read_csv("E:/ds/prac2/Data.csv")

View(Data)# 'aggr' plots the amount of missing/imputed values in each column

dataset<-Data

aggr(dataset)

# Taking care of missing data

# is.na is function to check if value is null. na.rm will omit values to

calculate mean if null

dataset$Age = ifelse(is.na(dataset$Age),

 ave(dataset$Age, FUN = function(x) mean(x, na.rm = TRUE)),

dataset$Age)

dataset$Salary = ifelse(is.na(dataset$Salary),

 ave(dataset$Salary, FUN = function(x) mean(x, na.rm =

TRUE)),

 dataset$Salary)

aggr(dataset)

head(dataset,n=10)
```

OUTPUT:-

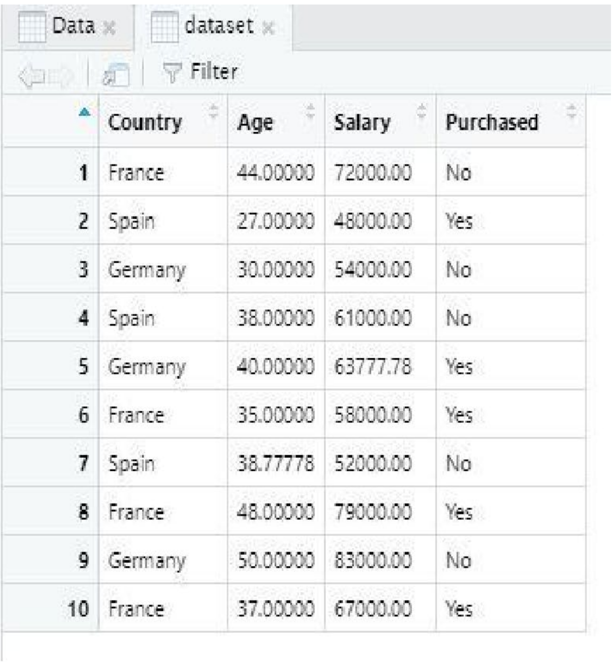
Data Before Cleaning



	Country	Age	Salary	Purchased
1	France	44	72000	No
2	Spain	27	48000	Yes
3	Germany	30	54000	No
4	Spain	38	61000	No
5	Germany	40	NA	Yes
6	France	35	58000	Yes
7	Spain	NA	52000	No
8	France	48	79000	Yes
9	Germany	50	83000	No
10	France	37	67000	Yes

Showing 1 to 10 of 10 entries, 4 total columns

Data After Cleaning



	Country	Age	Salary	Purchased
1	France	44.00000	72000.00	No
2	Spain	27.00000	48000.00	Yes
3	Germany	30.00000	54000.00	No
4	Spain	38.00000	61000.00	No
5	Germany	40.00000	63777.78	Yes
6	France	35.00000	58000.00	Yes
7	Spain	38.77778	52000.00	No
8	France	48.00000	79000.00	Yes
9	Germany	50.00000	83000.00	No
10	France	37.00000	67000.00	Yes

Sign:________________

Practical No. 8

Aim:- Data visualization using powerBI

Get data from Excel or dataset and convert into graphs or statistical models and evaluate functions.

Steps:

Create a data set in excel.

Student Name	Marks	Grade	Status	Year
Ram	45	D	Pass	2019
Sham	65	C	Pass	2019
Rohan	37	D	Fail	2019
Geet	47	D	Pass	2019
Roshan	87	A	Pass	2019
Shiv	45	D	Pass	2019

Export the data in Power Bi

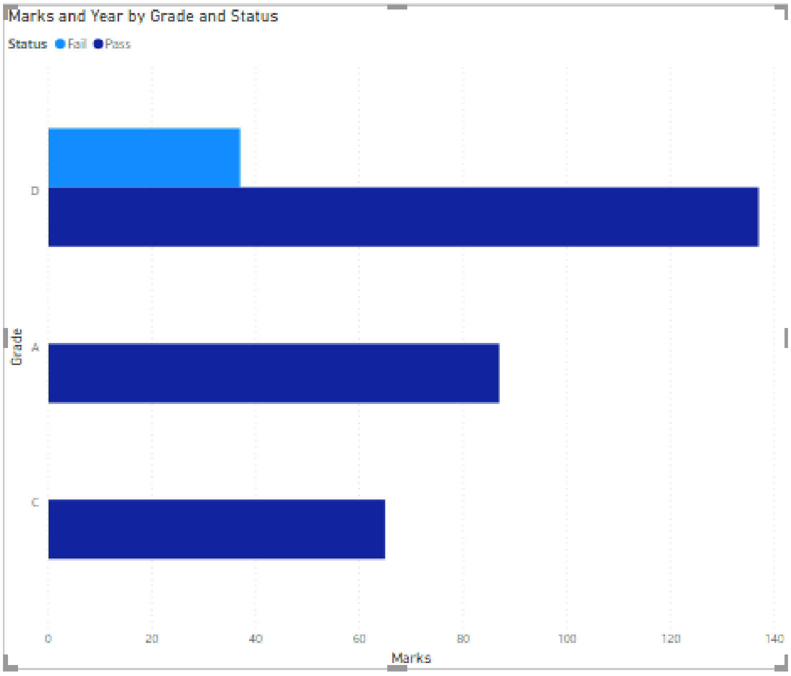
View=> Get Data=> Excel=> Select file Location.

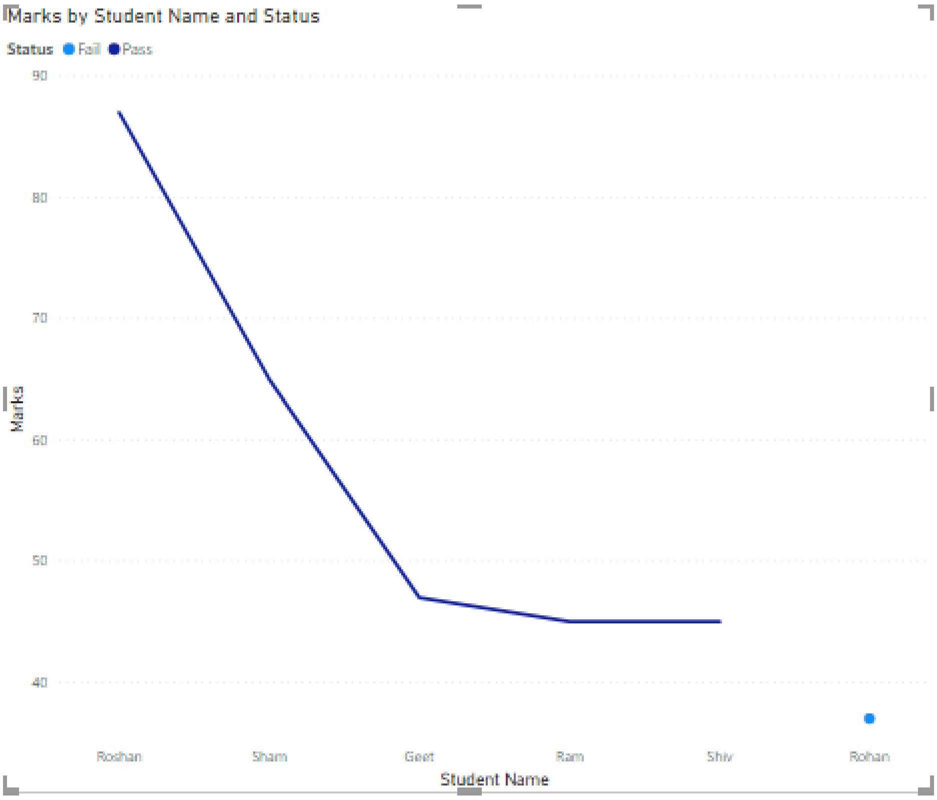
Click on the file and select ok.

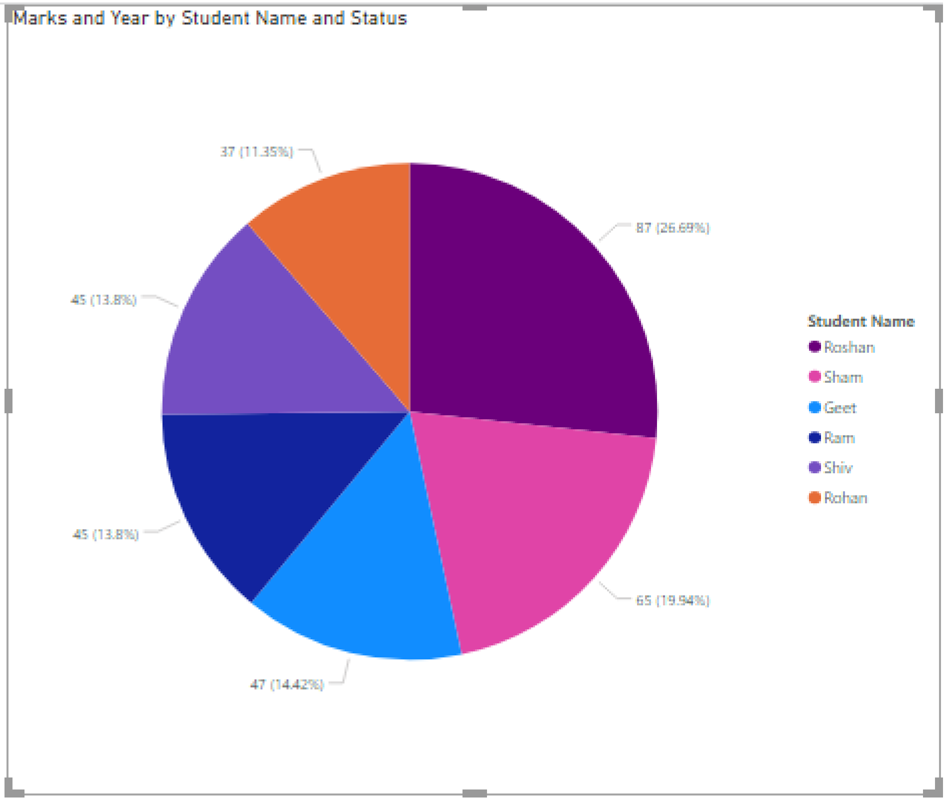
Navigator will display.

Tick on sheet 1=> Load

Graphs:-


Marks and Year by Grade and Status
Status ● Fail ● Pass
Grade
D
A
C
0
20
40
60
80
100
120
140
Marks


Marks by Student Name and Status
Status ● Fail ● Pass
90
80
70
60
50
40
Marks
Roshan
Sham
Geet
Ram
Shiv
Rohan
Student Name


Marks and Year by Student Name and Status
37 (11.35%)
87 (26.69%)
45 (13.8%)
45 (13.8%)
65 (19.94%)
47 (14.42%)
Student Name
● Roshan
● Sham
● Geet
● Ram
● Shiv
● Rohan

Sign:_________________

Practical No.9

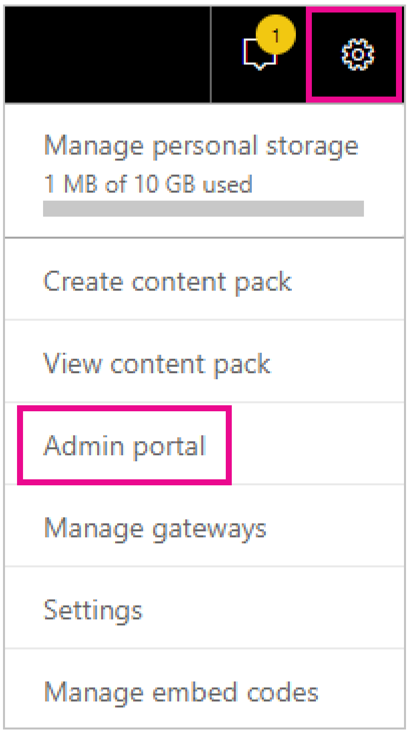
Aim:- Auditing and Utilities in power bi

Access your audit logs

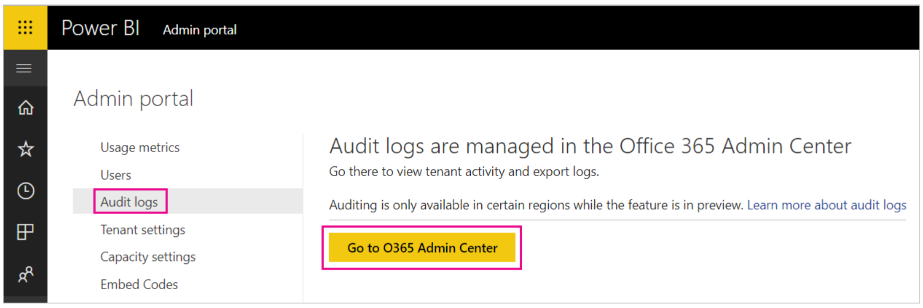
To access logs, first make sure to enable logging in Power BI. For more information, see Audit logs in the admin portal documentation. There can be up to a 48 hour delay between the time you enable auditing and when you can view audit data. If you don't see data immediately, check the audit logs later. There can be a similar delay between getting permission to view audit logs and being able to access the logs.

The Power BI audit logs are available directly through the Office 365 Security & Compliance Center. There's also a link from the Power BI admin portal:

1. In Power BI, select the **gear icon** in the upper-right corner, then select **Admin portal**.



2. Select **Audit logs**.
3. Select **Go to O365 Admin Center**.


Power BI Admin portal

Admin portal

Audit logs are managed in the Office 365 Admin Center

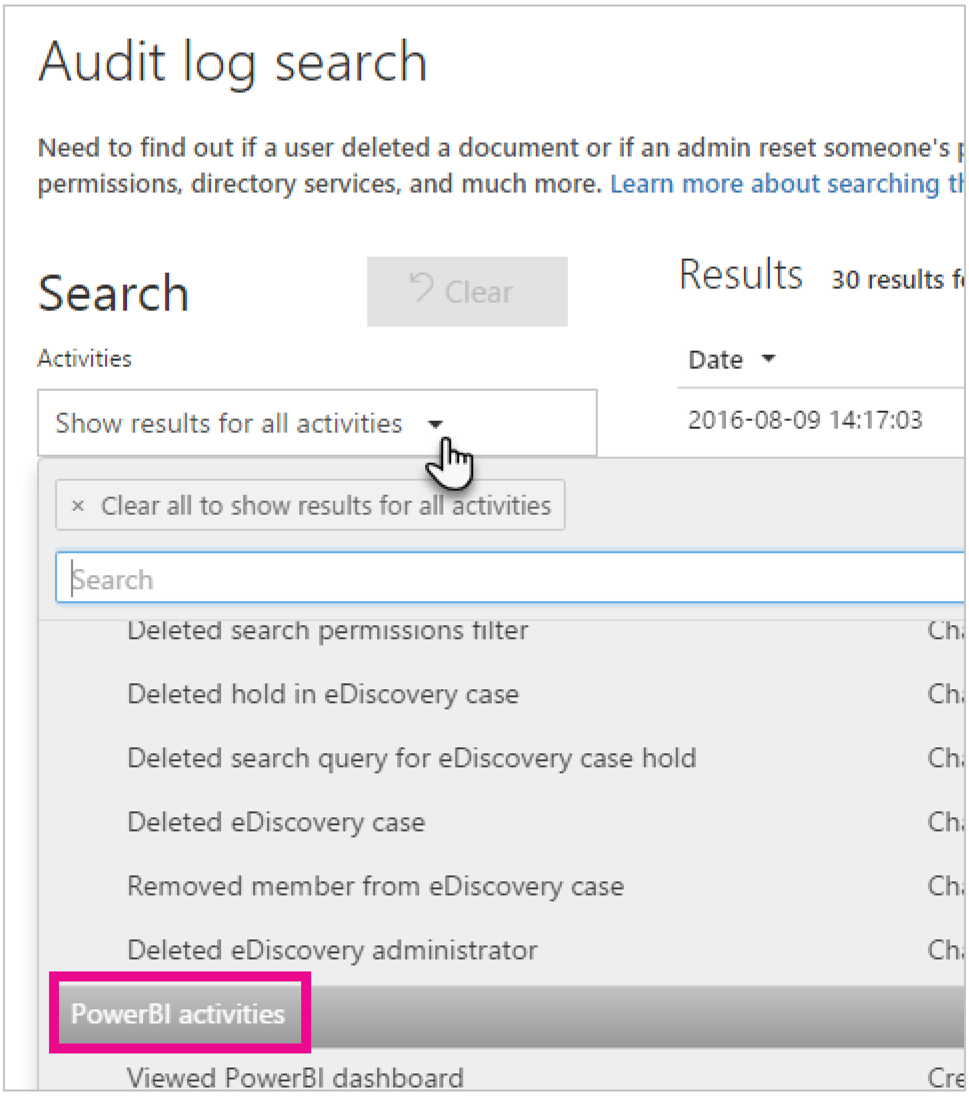
Go there to view tenant activity and export logs.

Auditing is only available in certain regions while the feature is in preview. Learn more about audit logs

Search only Power BI activities

Restrict results to only Power BI activities by following these steps. For a list of activities, see the list of activities audited by Power BI later in this article.

1. On the **Audit log search** page, under **Search**, select the drop-down for **Activities**.
2. Select **Power BI activities**.


Audit log search

Need to find out if a user deleted a document or if an admin reset someone's p permissions, directory services, and much more. Learn more about searching th

Search
Clear
Results
30 results f
Activities
Date
Show results for all activities
2016-08-09 14:17:03
× Clear all to show results for all activities
Search
Deleted search permissions filter
Deleted hold in eDiscovery case
Deleted search query for eDiscovery case hold
Deleted eDiscovery case
Removed member from eDiscovery case
Deleted eDiscovery administrator
PowerBI activities
Viewed PowerBI dashboard
Ch
Cre

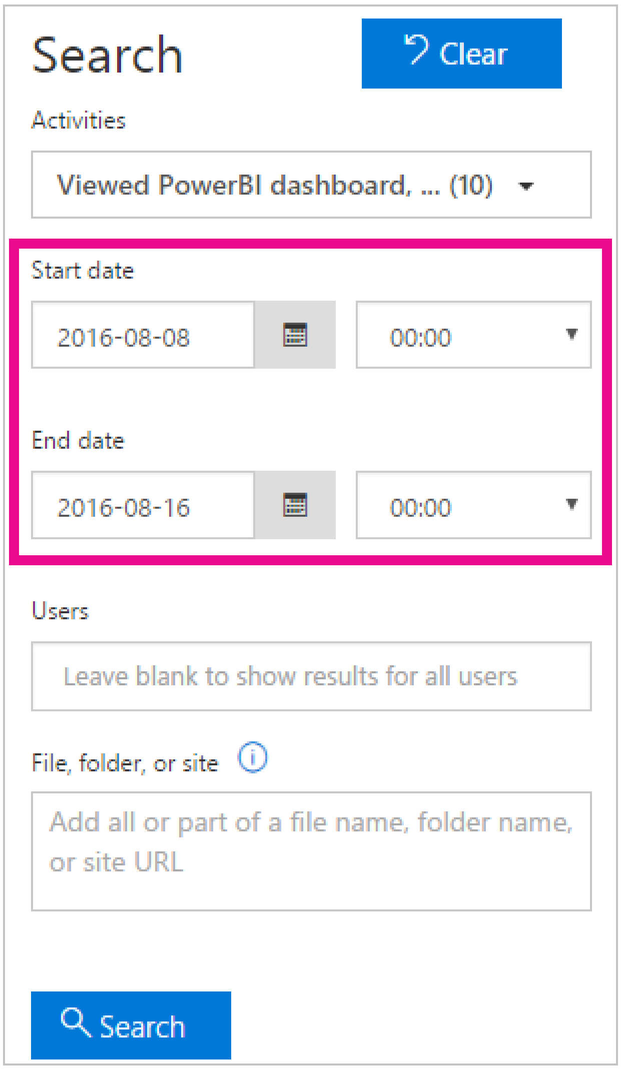
3. Select anywhere outside of the selection box to close it.

Your searches will only return Power BI activities.

Search the audit logs by date

You can search the logs by date range using the **Start date** and **End date** fields. The default selection is the past seven days. The display presents the date and time in Coordinated Universal Time (UTC) format. The maximum date range that you can specify is 90 days.

You'll receive an error if the selected date range is greater than 90 days. If you're using the maximum date range of 90 days, select the current time for **Start date**. Otherwise, you'll receive an error saying that the start date is earlier than the end date. If you've turned on auditing within the last 90 days, the date range can't start before the date that auditing was turned on.



Activities

Viewed PowerBI dashboard, ... (10)

Start date

2016-08-08 00:00

End date

2016-08-16 00:00

Users

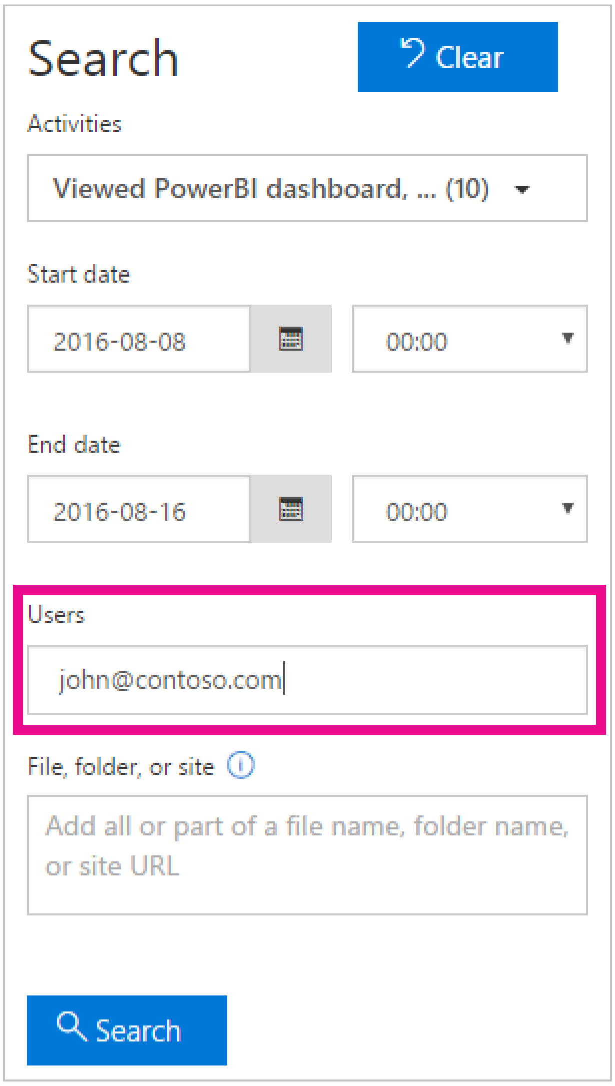
Leave blank to show results for all users

File, folder, or site

Add all or part of a file name, folder name, or site URL

Search the audit logs by users

You can search for audit log entries for activities done by specific users. Enter one or more user names in the **Users** field. The user name looks like an email address. It's the account that users log into Power BI with. Leave this box blank to return entries for all users (and service accounts) in your organization.



Activities: Viewed PowerBI dashboard, ... (10)

Start date: 2016-08-08 00:00

End date: 2016-08-16 00:00

Users: john@contoso.com

File, folder, or site: Add all or part of a file name, folder name, or site URL

View search results

After you select **Search**, the search results load. After a few moments, they display under **Results**. When the search finishes, the display shows the number of results found. **Audit log search** displays a maximum of 1000 events. If more than 1000 events meet the search criteria, the app displays the newest 1000 events.

View the main results

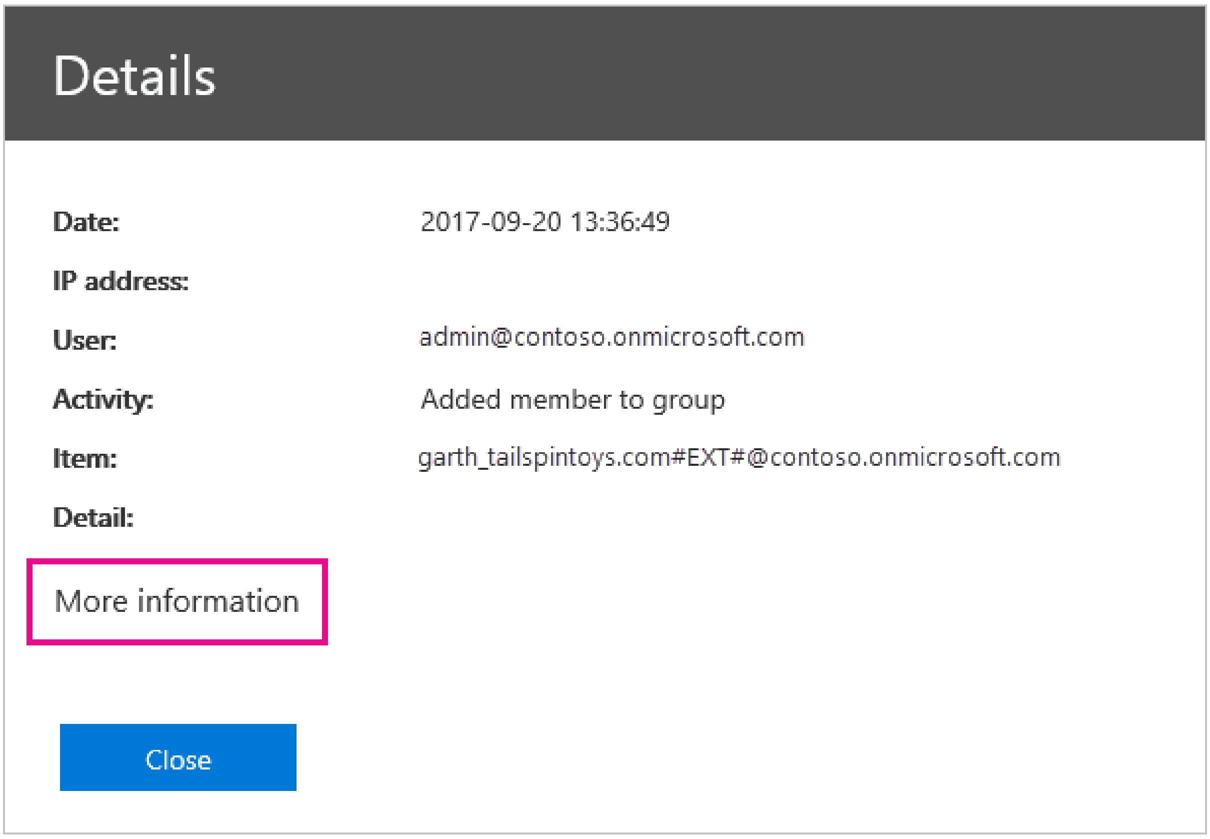
The **Results** area has the following information for each event returned by the search. Select a column header under **Results** to sort the results.

Column	Definition
Date	The date and time (in UTC format) when the event occurred.
IP address	The IP address of the device used for the logged activity. The app displays the IP address in either an IPv4 or IPv6 address format.
User	The user (or service account) who performed the action that triggered the event.
Activity	The activity performed by the user. This value corresponds to the activities that you selected in the **Activities** drop down list. For an event from the Exchange admin audit log, the value in this column is an Exchange cmdlet.
Item	The object created or modified because of the corresponding activity. For example, the viewed or modified file, or the updated user account. Not all activities have a value in this column.
Detail	Additional detail about an activity. Again, not all activities have a value.

View the details for an event

To view more details about an event, select the event record in the list of search results. A **Details** page appears that has the detailed properties from the event record. The **Details** page displays properties depending on the Office 365 service in which the event occurs.

To display these details, select **More information**. All Power BI entries have a value of 20 for the RecordType property. For information about other properties, see Detailed properties in the audit log.



Details

Date: 2017-09-20 13:36:49

IP address:

User: admin@contoso.onmicrosoft.com

Activity: Added member to group

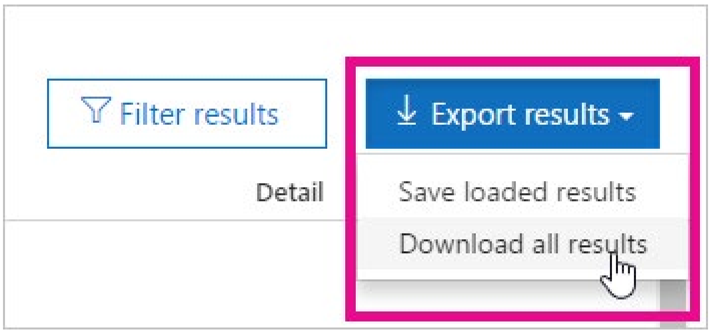
Item: garth_tailspintoys.com#EXT#@contoso.onmicrosoft.com

Detail:

Export search results

To export the Power BI audit log to a CSV file, follow these steps.

1. Select **Export results**.
2. Select either **Save loaded results** or **Download all results**.



Use PowerShell to search audit logs

You can also use PowerShell to access the audit logs based on your login. The following example shows how to connect to Exchange Online PowerShell and then use the Search-UnifiedAuditLog command to pull Power BI audit log entries. To run the script, an admin must assign you the appropriate permissions, as described in the Requirements section.

```
Set-ExecutionPolicy RemoteSigned

$UserCredential = Get-Credential

$Session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri
https://outlook.office365.com/powershell-liveid/ -Credential $UserCredential -
Authentication Basic -AllowRedirection

Import-PSSession $Session

Search-UnifiedAuditLog -StartDate 9/11/2018 -EndDate 9/15/2018 -RecordType PowerBI -
ResultSize 1000 | Format-Table | More
```

Use PowerShell to export audit logs

You can also use PowerShell to export the results of your audit logs search. The following example shows how to send from the Search-UnifiedAuditLog command, and export the results using the Export-Csv cmdlet. To run the script, an admin must assign you the appropriate permissions, as described in the Requirements section.

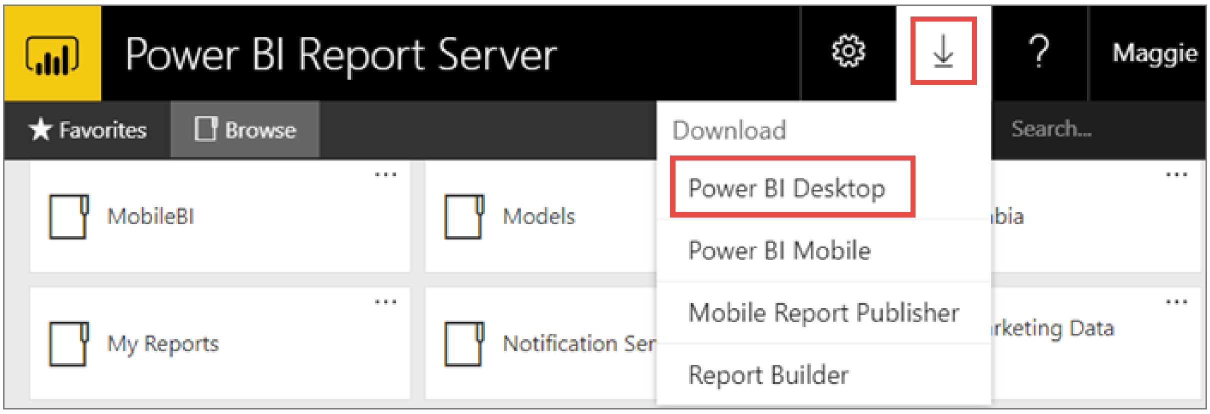
```
$UserCredential = Get-Credential

$Session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri
https://outlook.office365.com/powershell-liveid/ -Credential $UserCredential -
Authentication Basic -AllowRedirection

Import-PSSession $Session

Search-UnifiedAuditLog -StartDate 9/11/2019 -EndDate 9/15/2019 -RecordType PowerBI -
ResultSize 5000 |

Export-Csv -Path "c:\temp\PowerBIAuditLog.csv" -NoTypeInformation

Remove-PSSession $Session
```

Practical No 10

Aim:- Generating reports in Power Bi.

Step 1: Install Power BI Desktop optimized for Power BI Report Server

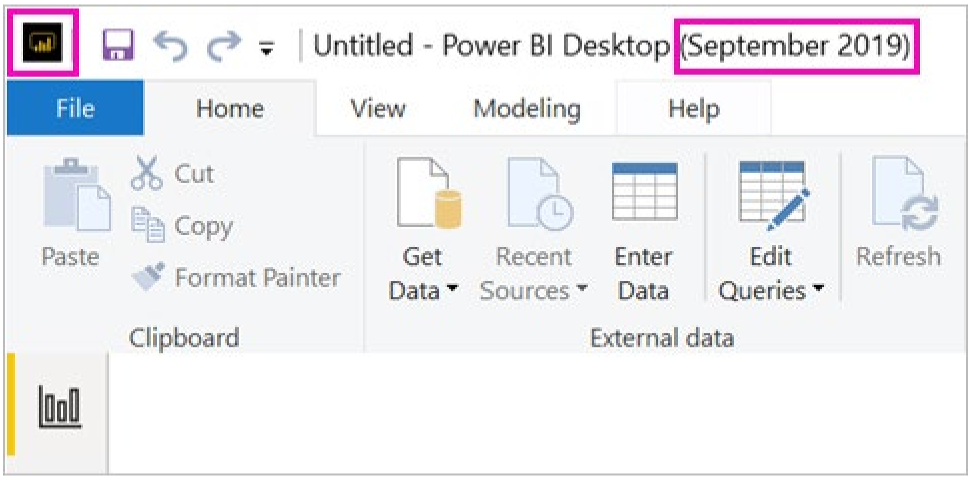
1. In the report server web portal, select the **Download** arrow > **Power BI Desktop**.

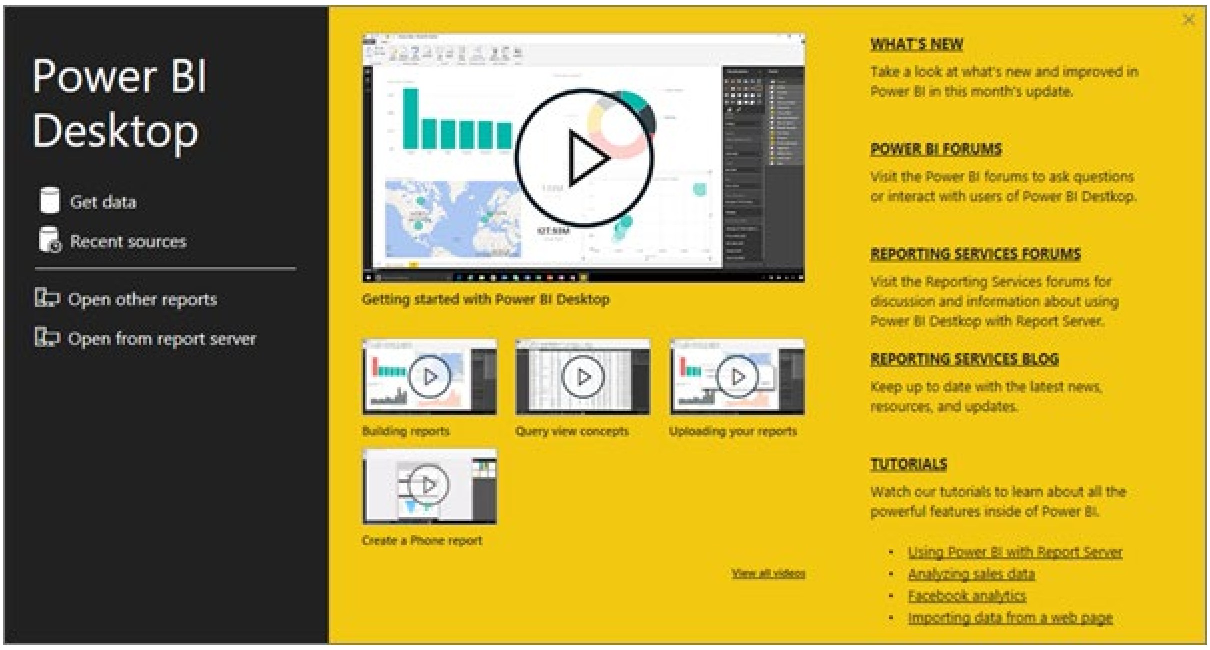
   Or go to the Power BI Report Server home page and select **Advanced download options**.

2. In the Download Center page, select **Download**.
3. Depending on your computer, select:
   - **PBIDesktopRS.msi** (the 32-bit version) or
   - **PBIDesktopRS_x64.msi** (the 64-bit version).
4. After you download the installer, run the Power BI Desktop (September 2019) Setup Wizard.
5. At the end of the installation, check **Start Power BI Desktop now**.

   It starts automatically and you're ready to go. You can tell you have the right version because **Power BI Desktop (September 2019)** is in the title bar.



6. If you're not familiar with Power BI Desktop, consider watching the videos on the welcome screen.



WHAT'S NEW

Take a look at what's new and improved in Power BI in this month's update.

POWER BI FORUMS

Visit the Power BI forums to ask questions or interact with users of Power BI Desktop.

REPORTING SERVICES FORUMS

Visit the Reporting Services forums for discussion and information about using Power BI Destkop with Report Server.

REPORTING SERVICES BLOG

Keep up to date with the latest news, resources, and updates.

TUTORIALS

Watch our tutorials to learn about all the powerful features inside of Power BI.

- Using Power BI with Report Server
- Analyzing sales data
- Facebook analytics
- Importing data from a web page

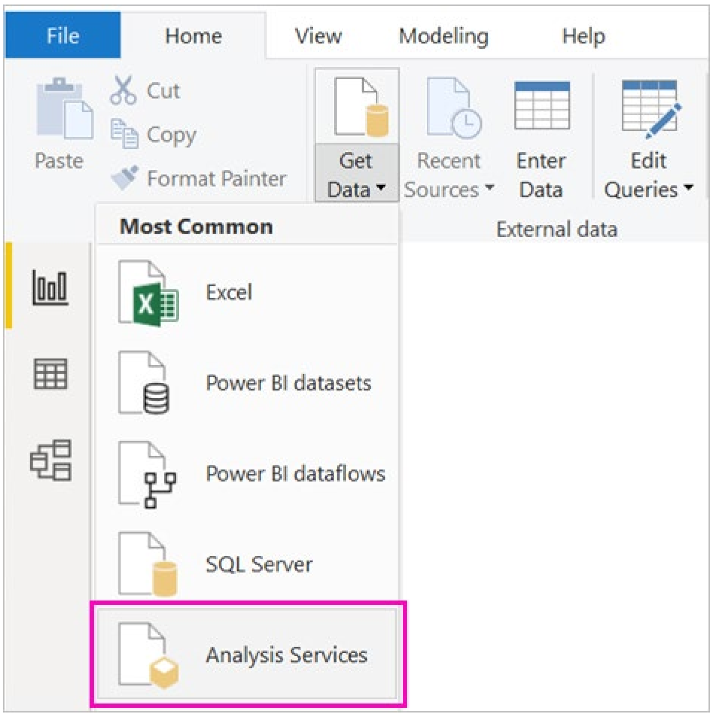
Step 2: Select a data source

You can connect to a variety of data sources. Read more about connecting to data sources.

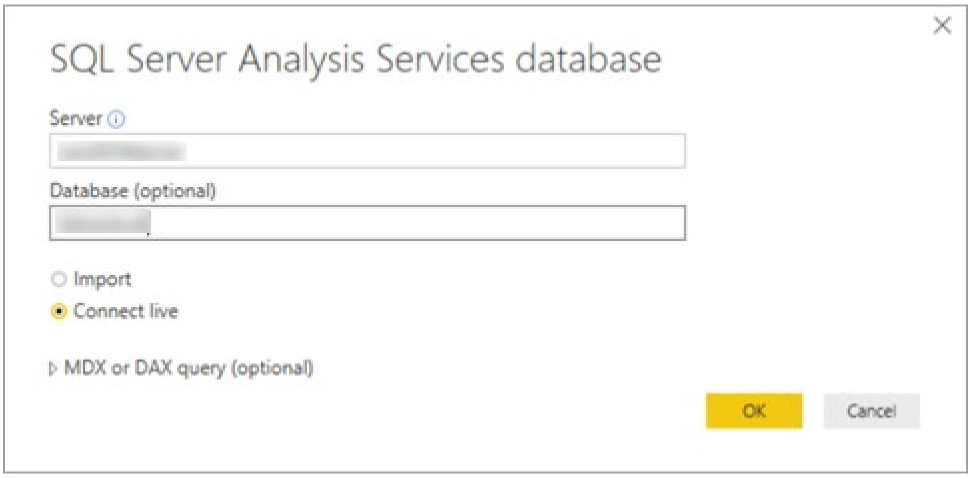
1. From the welcome screen, select **Get Data**.

   Or on the **Home** tab, select **Get Data**.

2. Select your data source -- in this example, **Analysis Services**.



3. Fill in **Server**, and optionally, **Database**. Make sure **Connect live** is selected > **OK**.



SQL Server Analysis Services database

Server ⓘ

[redacted]

Database (optional)

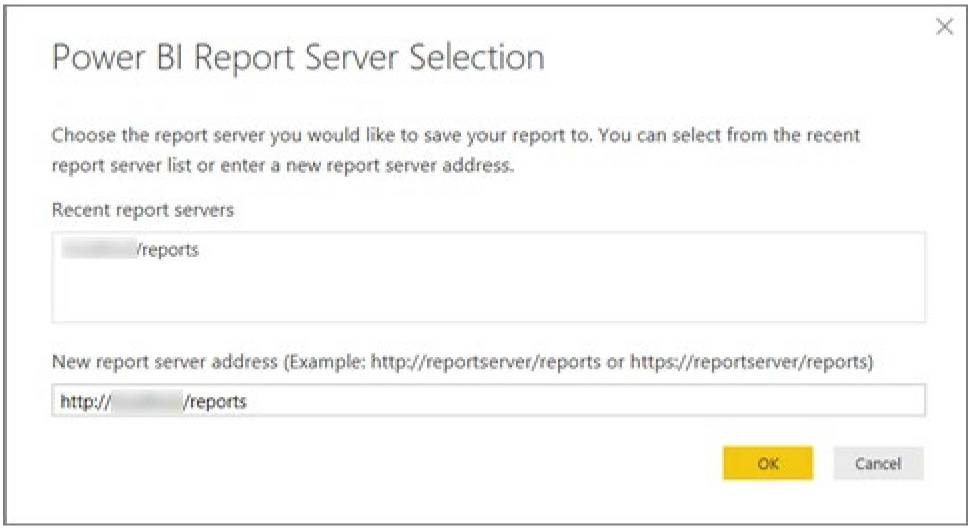
[redacted]

○ Import

● Connect live

▷ MDX or DAX query (optional)

4. Choose the report server where you'll save your reports.



Power BI Report Server Selection

Choose the report server you would like to save your report to. You can select from the recent report server list or enter a new report server address.

Recent report servers

[redacted]/reports

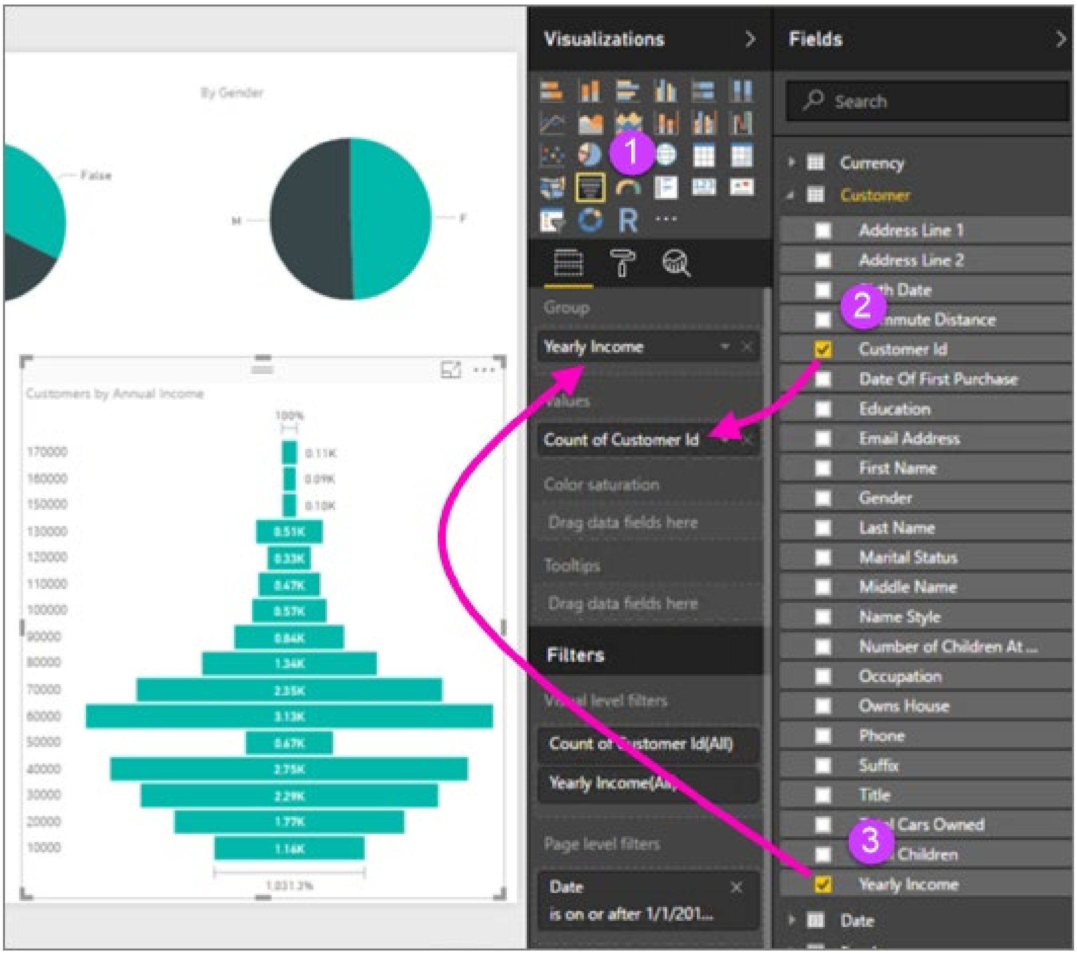
New report server address (Example: http://reportserver/reports or https://reportserver/reports)

http://[redacted]/reports

Step 3: Design your report

Here's the fun part: You get to create visuals that illustrate your data.

For example, you could create a funnel chart of customers and group values by yearly income.

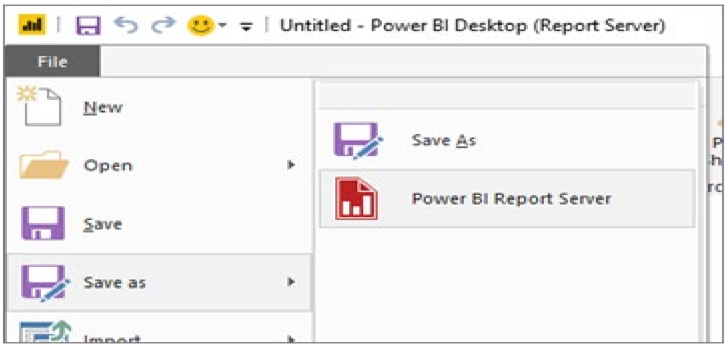


1. In **Visualizations**, select **Funnel chart**.
2. Drag the field to be counted to the **Values** well. If it's not a numeric field, Power BI Desktop automatically makes it a *Count of* the value.
3. Drag the field to group on to the **Group** well.

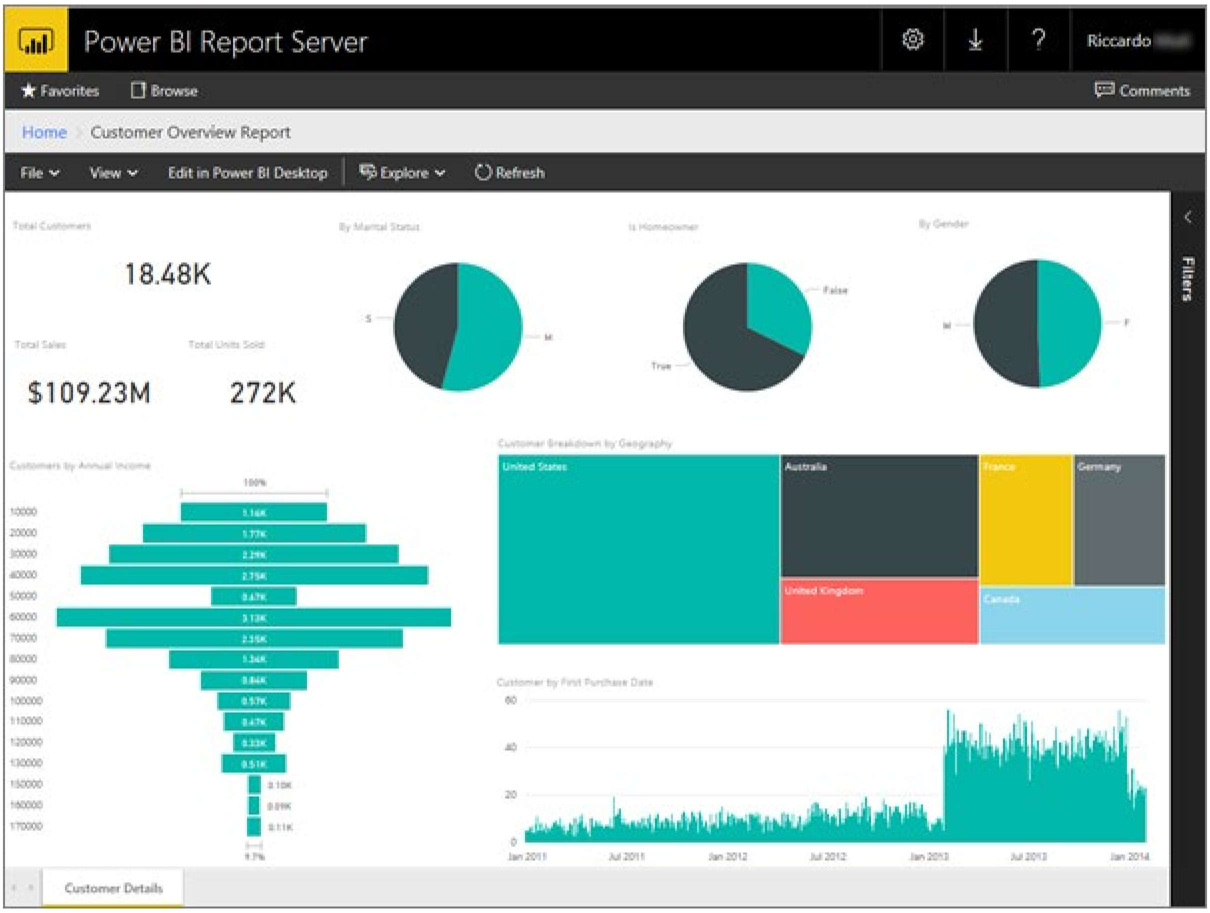
Step 4: Save your report to the report server

When your report is ready, you save it to the Power BI Report Server you chose in Step 2.

1. On the **File** menu, select **Save as** > **Power BI Report Server**.



2. Now you can view it in the web portal.


Power BI Report Server
Riccardo [redacted]
★ Favorites
Browse
Comments
Home
Customer Overview Report
File
View
Edit in Power BI Desktop
Explore
Refresh
Filters
Total Customers
18.48K
Total Sales
$109.23M
Total Units Sold
272K
By Marital Status
S
M
Is Homeowner
False
True
By Gender
M
F
Customers by Annual Income
100%
10000
1.16K
20000
1.77K
30000
2.29K
40000
2.75K
50000
0.47K
60000
3.13K
70000
2.35K
80000
1.36K
90000
0.84K
100000
0.57K
110000
0.47K
120000
0.33K
130000
0.51K
150000
0.10K
160000
0.09K
170000
0.11K
9.7%
Customer Breakdown by Geography
United States
Australia
France
Germany
United Kingdom
Canada
Customer by First Purchase Date
60
40
20
0
Jan 2011
Jul 2011
Jan 2012
Jul 2012
Jan 2013
Jul 2013
Jan 2014
Customer Details

Sign:___________

Practical No.11

Review Paper

CLOUD SECURITY: DISTORTION CONTROL AND PRECAUTION TECHNIQUE

Abstract

Cloud Computing Security allude to the security implementation, deployment, and the precaution to defend against the security threats. Cloud Security deployment of security tools such as application firewall, controlling the policies and hardening the infrastructure. Though cloud computing is offering lots of services with the flexibility, efficiency, and also find threats in cloud services which is vulnerable. It allows the access to personal and shared resources with minimal management. Perfect example for cloud computing is Amazon Elastic Cloud Compute (EC2), which is highly capable, low cost and flexible. The purpose of this paper is to provide a comprehensive overview of latest advance and existing literature covering varieties of dimensions in cloud security. The paper also includes various attacks faced on cloud services and the methods to overcome on it is also been mention in this paper.

Keywords

Cloud security, Physical Security, Cloud deployment, Tools for preventing from attacks, Deployment, IT management.

Introduction

Cloud Computing Technology is nowadays most popular, because of its ability , flexibility and mobile support. Cloud Computing allows the access to the personal and shared resources with minimal management. It often relies on the internet. But there is third party cloud solution available which saves from expanding resources and maintenance. As we know the most trending example for cloud storage is Amazon Elastic Cloud Compute (EC2), which is highly flexible and capable along with low cost.

Some of the major features of cloud computing includes:-

- Automated Management
- Virtualization
- On-demand self-service
- Rapid Elasticity
- Measured services
- Distributed Storage

Types of Cloud Computing Services:-

- Infrastructure as a service (IaaS)
- Platform as a Service (PaaS)
- Software as a Service (SaaS)

- ***Infrastructure as a Service (SaaS):-*** It is been used for accessing, managing process and monitoring. This infrastructure services (IaaS) also known as Cloud infrastructure service basically a self-service model. We can take an example like, Instead of purchasing additional hardware such as networking device, firewall, server and spending money on management, maintenance, deployment, IaaS model
offers cloud based infrastructure to deploy the remote data center. Most common and popular examples of IaaS are AMAZON (EC2), Microsoft Azure, Google Compute Engine (GCE), Cisco Metapod.

- ***Platform as a Service (PaaS):-*** It allows the users to develop, run and manage the applications. PaaS offers Development Tools, Deployment platform, Configuration management, and migrate the app to the hybrid models. It basically helps us to develop and customize applications, manages OSes, virtualization, storage and networking, etc. Examples for PaaS are Intel Mash Maker, Google app Engine, Microsoft Azure, etc.

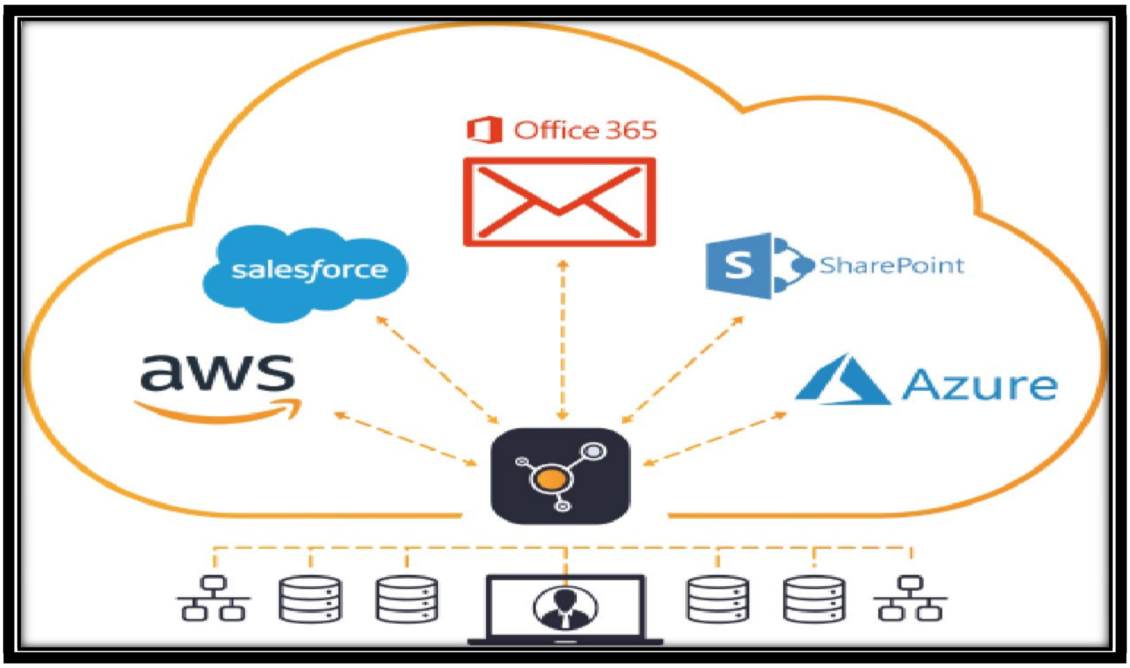
- ***Software as a Service (SaaS):-*** SaaS is the one of the most common type of cloud which is been used in cloud computing is widely than other services. On demand Software is centrally hosted accessible by user using client through browsers. An example for SaaS is office software such as office 365, Cisco WebEx, Citrix GoToMeeting, Google Apps, DBMS, ERP, CAD, HRM, messaging software, etc.

Cloud Deployment Models for Cloud Services are as follow:-

1. Public Cloud- Public Cloud are hosted by the third party which offers them different types of cloud computing services.
2. Private Cloud- Private Cloud are hosted personally & individually. Corporate companies usually have their own private clouds services due to their security policies.
3. Hybrid Cloud- Hybrid Clouds are combination of both private and public cloud respectively. Private cloud is used to enhance their sensitive and public cloud capabilities and services.
4. Community Cloud- They are accessed by the multiple parties having common goals and shared resources.

Benefits for Cloud Computing:-

- ***Increased speed-*** Cloud Computing environment has dramatically reduced the time and cost of new IT services the increase speed for the organizations to access the IT resources.
- ***Low Latency-*** In the using of cloud computing, the customers have the facility of implementing their applications with just few clicks, so they can do their task easily at minimal costs, i.e., not more time consumed as well as minimal latency is been produced.
- ***Security-*** In the terms of security, cloud computing is always been very efficient. Highly recommended advantages include less investment over security with the effective patch management and security updates. Disaster recovery, dynamically scaling defensive resources and other security services also provides with the protection against cloud computing threats.
- ***Less Economic Expense-*** This is the major advantage in cloud computing. No need to purchase any kind of external hardware for particular function. Data Centre, Networking, and other services can be easily virtualized over cloud saving the cost of purchasing any hardware, configuration and management complexity and less maintenance cost.



Working

Cloud computing consists of some activities that have been taken for the service provider end as well as the action that should be taken under the user end.

Cloud Security working under some control layers, which have been discussed below:-

✓ Application Layer:-

There are some security mechanisms, devices and the policies that provide support at different cloud security control layers. In the application layer, Web application firewall are deployed to filter the traffic and observe the behavior of the traffic. Likely, Software Development Life Cycle (SDLC), Binary Code Analysis, Transactional Security provides the security for online transactions, etc.

In cloud computing , to provide confidentiality and integrity of information that is being communicated between client and server, different policies are configured to monitor any kind of data loss. These policies includes Data Loss Prevention (DLP) and the content management framework. DLP is the feature which generally offers to prevent the leakage of information to the outside network. Traditionally this information may include company or organizations confidential data, proprietary, financial and other secret information. DLP also features ensure the enforcement of compliances with the rules and regulations using Data Loss Prevention policies to prevent the user from intentionally or unintentionally sending this confidential information.

Security of Cloud Computing regarding management is performed by different ways to approaches the Governance, Risk Management, and Compliance (Grc), Identity and Access Management (IAM), Patch and Configuration Management. These approaches helps us to control the secure access t the resources ad manage them.

✓ Network Layer:

The next generation of intrusion prevention systems, known as NGIPS, is one of the efficiently active components in integrated threat protection solutions. NIIPS provide a robust security layer with deep visibility, enhanced security intelligence, and enhanced security against emerging threats to secure the network's complex infrastructure. The CISCO NGIPS solution provides deep network visibility automation, security intelligence and next level security.

It uses the most advanced and effective intrusion prevention capabilities to reach emerging sophisticated network attacks. It continuously collects all the information regarding the network, including the operating system, files and applications information, users and device information. This information helps NGIPS to determine network maps and host profiles which lead to contextual information to make better decisions about intrusive enhancements.

✓ Trusted Computing :-

The Root of Trust (RoT) is established by validating each components of hardware and software from the end entities up to the root certificate. It makes ensure that only trusted software and hardware can used while still retaining the facilities and also retaining the flexibility.

✓ Computer and Storage:-

Computer and Storage in cloud Computing can be secured by implementing Host-Based Intrusion Detection or prevention system HIDS/HIPS. Configuring Integrity Check, File system Monitoring and log file analysis, connection analysis, Encrypting the storage, Kernel Level Detection, etc.

Host Based IPS/IDS is normally made for the protection of specific host machine, and it works closely with operating system Kernel of the host machine. It creates the filtering layer and some kind of filters which make them to purify any malicious application call to the OS.

✓ Physical Security:-

Physical Security is always been the required priority to secure anything. It also the first layer OSI model, if devices is not physically secured, any sort of security configuration will not be effective. Physical security includes protection against man-made attacks such as damage, thefts, unauthorized physical access as well as environmental impact such as dust, rain, fire, power, failure, etc.

Experiments

In clouds computing the most common attacks that are being used by an attacker to exploit or extract sensitive information such as gaining an unauthorized access. The attacks are as follow-

• Service Hijacking using Social Engineering Attacks-

As we know about the social engineering attacks. Using social engineering techniques, an attack can be attempted to guess the password. Social engineering attacks occur when unauthorized access to uncover sensitive information according to the compromised user's privilege level.

• SQL Injection Attack

SQL injection attacks allow attackers to lose identity, cause damage to existing data, and also causes counter attack. Issues such as transactions or changing balances allow full disclosure of all data on systems, destroying data or otherwise being unavailable, and becoming administrators of database servers.

• Domain Name System (DNS) Attack

Domain Name System (DNS) attack include DNS Poisoning, Cybersquatting, Domain hijacking and Domain Snipping. An attacker may attempt to spoil the DNS server or cache by poisoning it to gain internal users' credentials. Domain Hijacking mainly involves in stealing cloud services domain name. Similarly, through Phishing scams, users can be redirected to a fake website

- ### Session Hijacking using XSS Attack

By launching Cross-Site (XSS), the attacker can steal cookies by injecting malicious code into the website.

- ### Cryptanalysis

Cryptanalysis is the science of encoding and decoding codes. It is used more benignly, to find and correct weaknesses in encryption algorithms, to violate authentication schemes, and to break cryptographic protocols.

- ### Dos/DDoS Attacks

DOS / DDOS attacks are being done to create a machine or network. Temporarily unavailable and indefinitely interrupted service of host network to connect to server

- ### Session Hijacking using Session Riding-

It is been use to intend for session hijacking. An attacker may exploit it by attempting cross-site request forgery. The attacker uses currently active session and rides on it by executing the request such as modification of data, erasing data, online transactions and password change by tracking the user to click on malicious link.

- ### Service Hijacking using Network Sniffing

Using Packet Sniffing tools by placing them in the network, then attacker can capture sensitive information such as password, session ID, cookies, and another web service related information such as UDDI, SOAP, and WSDL.

Tools used to detect & prevent those attacks are as follow-

- **Core Cloud Inspect**

Core security Technologies offers “Core CloudInspect”, A cloud Security testing solutions for the Amazon Web services (AWS). This tool has been helping to make the profits from the core Impact and core Insight Technologies to offer penetration-testing as a service from Amazon Web Services for EC2 users.

- ### CloudPassage Halo

CloudPassage Halo provides a broad range of security controls. It is focused Cloud Security solution which prevents attacks and detect the indication of compromise. Cloud Passage Halo operates under ISO-27002 security standards and is audited annually against PCI level 1 and SOC 2 standards. Cloud Passage Halo is the only workload security automation platform that provides speed and scale to on-demand delivery of security control speeds across data centers, private or public cloud, virtual machines, and containers. Unlike traditionally security systems, Halo and its secure APIs integrate with popular CI / CD toolchains and processes, providing periodic feedback to fix vulnerabilities in the development life cycle. This allows DevOps teams to perform security teams by providing the validation they need. Halo integrates easily with popular infrastructure automation and orchestration platforms allowing Halo to be easily deployed to continuously monitor workload security and compliance posture.

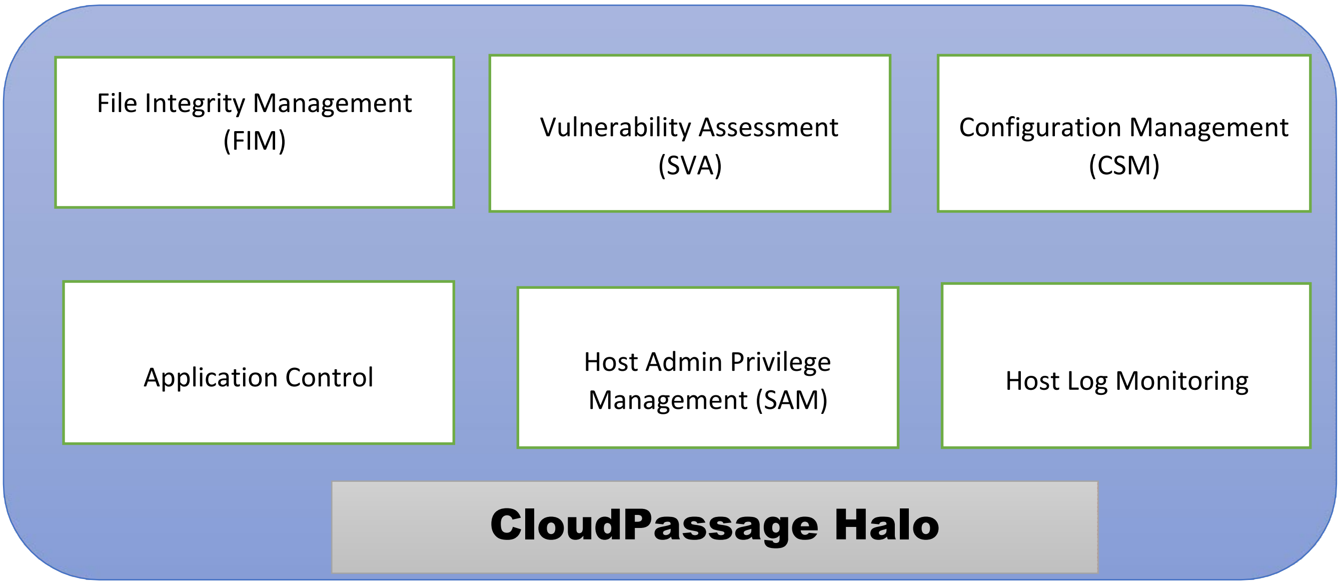

File Integrity Management (FIM)
Vulnerability Assessment (SVA)
Configuration Management (CSM)
Application Control
Host Admin Privilege Management (SAM)
Host Log Monitoring
CloudPassage Halo

Fig: CloudPassage Halo

Conclusion:-

In Research studies, there should be a bond of trust and privacy between the service provider and the client. Security must be seen as a continuous process to meet the changing needs of a highly volatile computing environment. There is a need to have a holistic view of cloud computing security methodology, which can be used in any service model in general, as long as the customer is not using the service. There should also be self-awareness from the client about self-protection. In view of these observations, this study provided a detailed review of the existing literature and offered several research areas based on existing research work where future work is required. The paper can provide an important aid for obtaining research areas where further work is required, especially for entry-level researchers. The responsibilities provided by the service provider should be consisted of web application firewall, secure web gateway, load balancer, application security and virtual private network. Cloud service clients should be aware of public key infrastructure, firewall, encryption, security development life cycle (SDLC), and others.

References:-

[1] **Cloud Computing in a general perspective.- Journal of computing and management studies- January 2019.- ISSN 2516-2047 Issue 1 – Volume 3**

[2] **A survey on Cloud Cloud Computing and Hybrid Cloud.- International Journal of Applied Engineering Research ISSN 0973-4562 Volume 14, Number 2 (2019) pp. 429-434 by M.P.Vaishnavve**

[3**] Hindwai Wireless Communication and Mobile Computing, Volume 2019, Article ID 8204394 introduces "Recent Advances in Cloud Aware Mobile Fog Computing"**

[4**] "Measuring Information Security and Cybersecurity on Private Cloud Computing." By Wendy, Wang Gunawan published on Journal of Theoretical and Applied Information Technology- January 2019 at ISSN 1992-8645**

[5**] Journal of Analysis and Computation (JAC) –ISSN 0973-2861. D.Sakthpriya an Assistant Professor Introduces "Security Issues In cloud Computing"**

[6] **The Calculus of Cloud Computing.- Research Centre of Big Analytics and Intelligent Systems (BAIS) By"Zhaohao Sun"Bias 4(11):1-6**

[7] **Study on Cloud Storage and its Issues in Cloud Computing.- International Journal of Management, Technology And Engineering ISSN 2249-7455 by Dr. K.Sharmila**

[8**] Improving Database Security in Cloud Computing.- Journal of Applied Science and Computation ISSN 1076-5131 by Mrunali Sangar Professor at B.A.Kelkar.**

Sign:______________