ADA Assignment 2

Benjamin Isaac Wilson C3444086

Table of Contents

[Pivot Table 1](#_Toc503213481)

[Dashboard 6](#_Toc503213482)

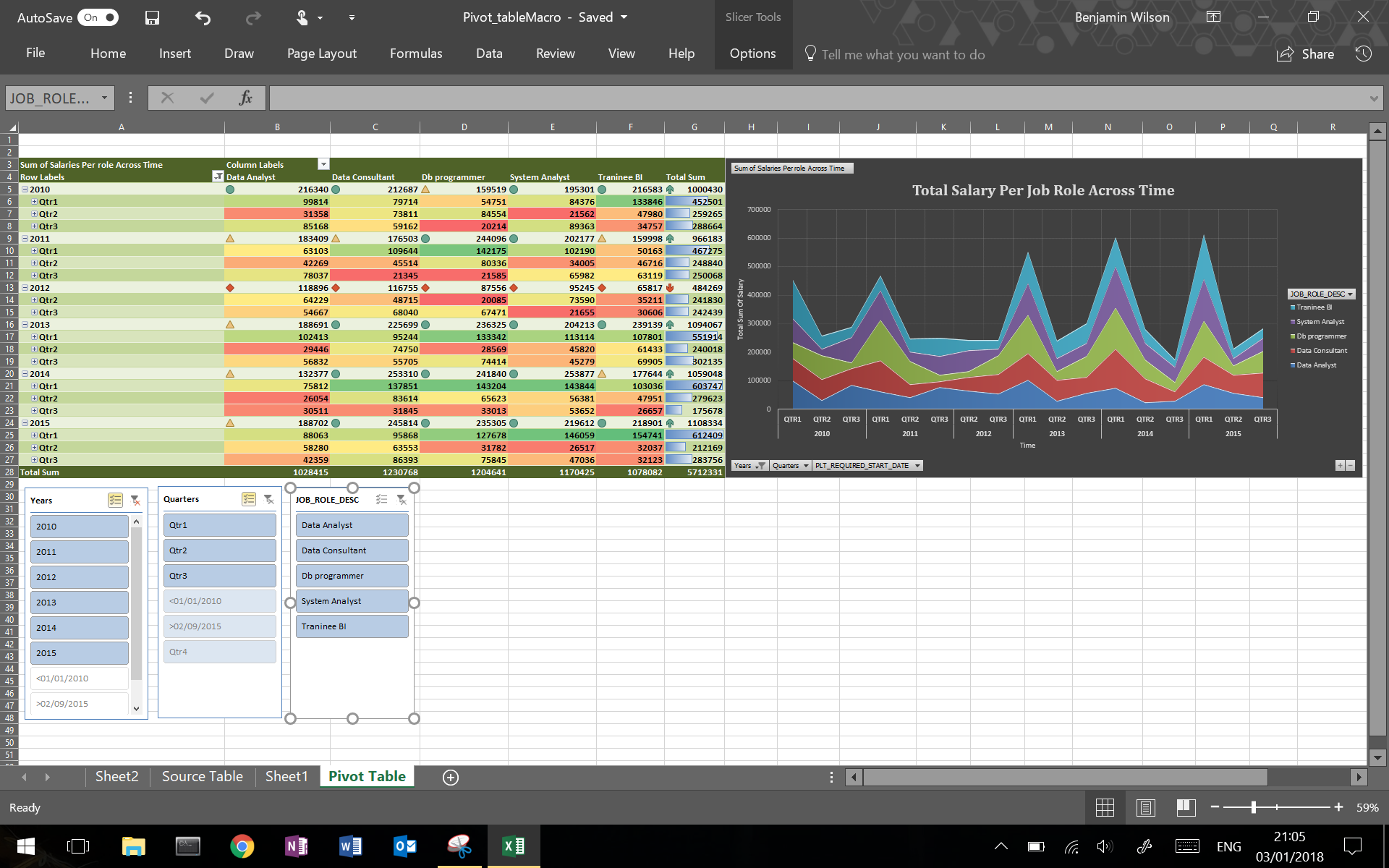
[Ethics and Security 8](#_Toc503213483)

[Practical Security Implementations and Testing 9](#_Toc503213484)

[Reflection 14](#_Toc503213485)

[Bibliography 15](#_Toc503213486)

# Pivot Table



Businesses sit on data and as time passes, they generate more. It is a core goal of a modern business to explore this data to get better insight, a difficult task if there is no obvious question to answer (K.Janert, 2011). One way to overcome this is to perform analysis of the data using visual aids. When presenting data, it is crucial to understand that the human visual system is the most powerful way convey information to an audience.

A pivot table was created to provide a report on, for example, the performance of an establishment. This could be for topics ranging from profit/loss per some category, a number of employees employed each year and/or the average amount of illnesses for a location. However, a pivot table alone can only provide a table of numbers that may be hard to assess, therefore adding conditional style formatting and symbols can help (see Figure 1).

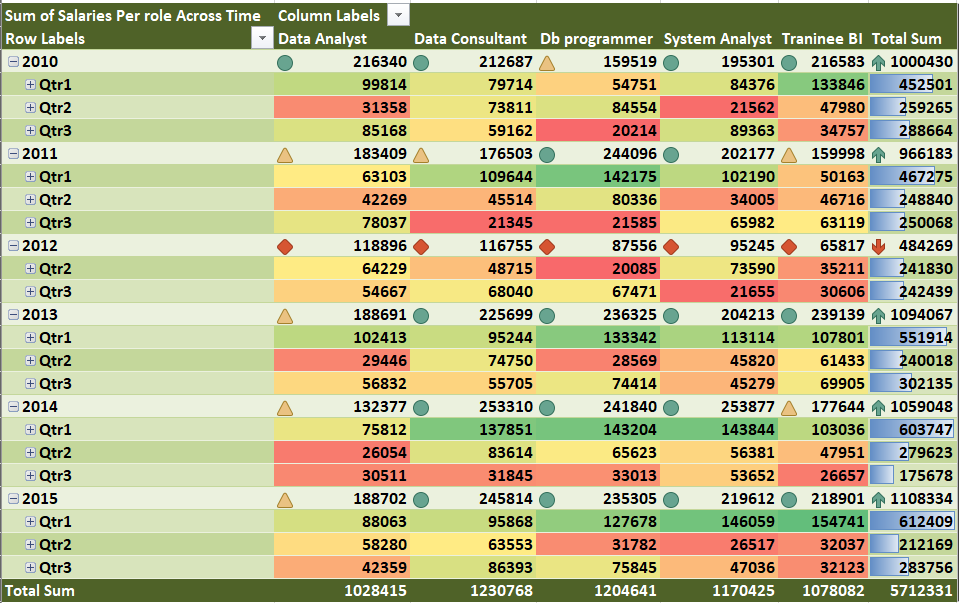


Figure Pivot Table Implementation has been decorated with conditional formatting features in excel. As seen, the formatting includes colour coded performance levels per job per quarter, symbolic performance per job per year, the growth per year represented by arrows and data bars showing highest performing quarter.

Furthermore, an Online analytical processing(OLAP) tool such as the pivot table is a handy way to navigate multidimensional and hierarchical data (AlexBerson & J.Smith, 1997). Users can drill up and down details of the data, say, from quarters up to years to get a simpler view over the wider time scales (see Figure 2).

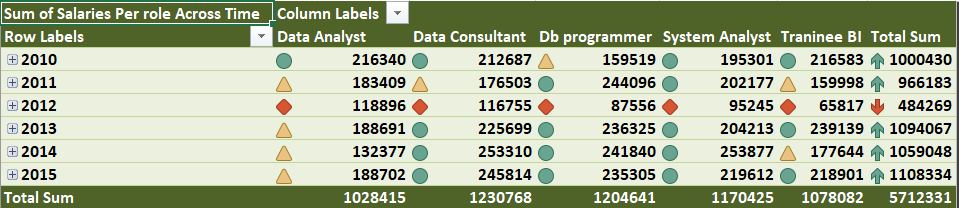


Figure A Pivot table that has drilled up into a less detailed overview across years. This was done by using the detail buttons (represented by +/-) on the left of the years.

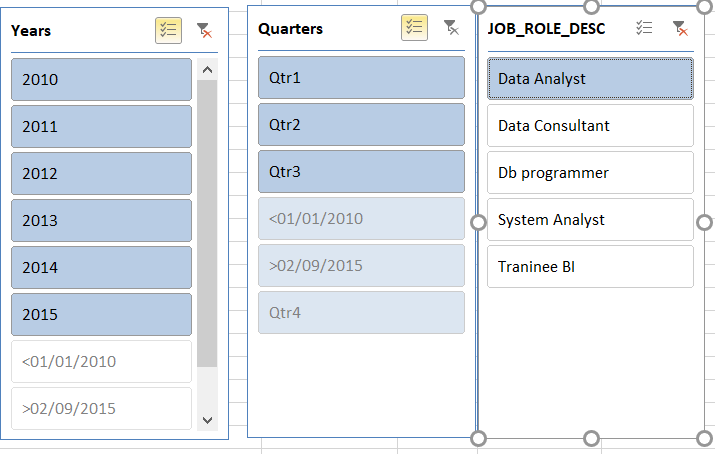


Figure Slicer functionality in Excel specifying Data Analyst only.

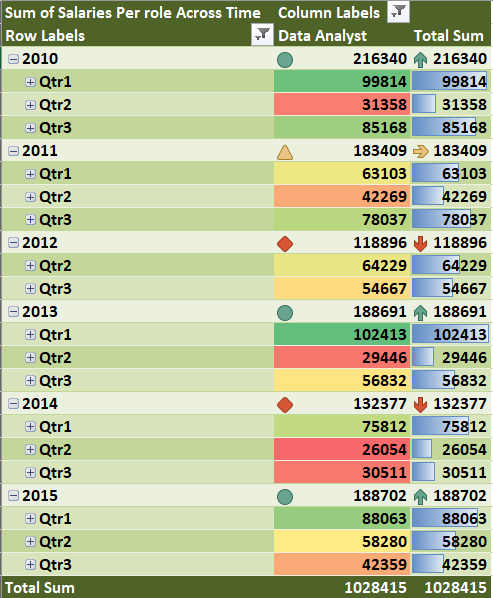


Figure The pivot table has been sliced into showing only the performance of the Data Analyst Role.

Combining a pivot table with a chart can provide even better insight. One such chart could be a stacked area line chart that can break the total measure into its sub-measures (see figure 3). Though this may be harder to view the performance of the sub-measures because whatever areas are affected by what is below them (Choudhury, 2013).

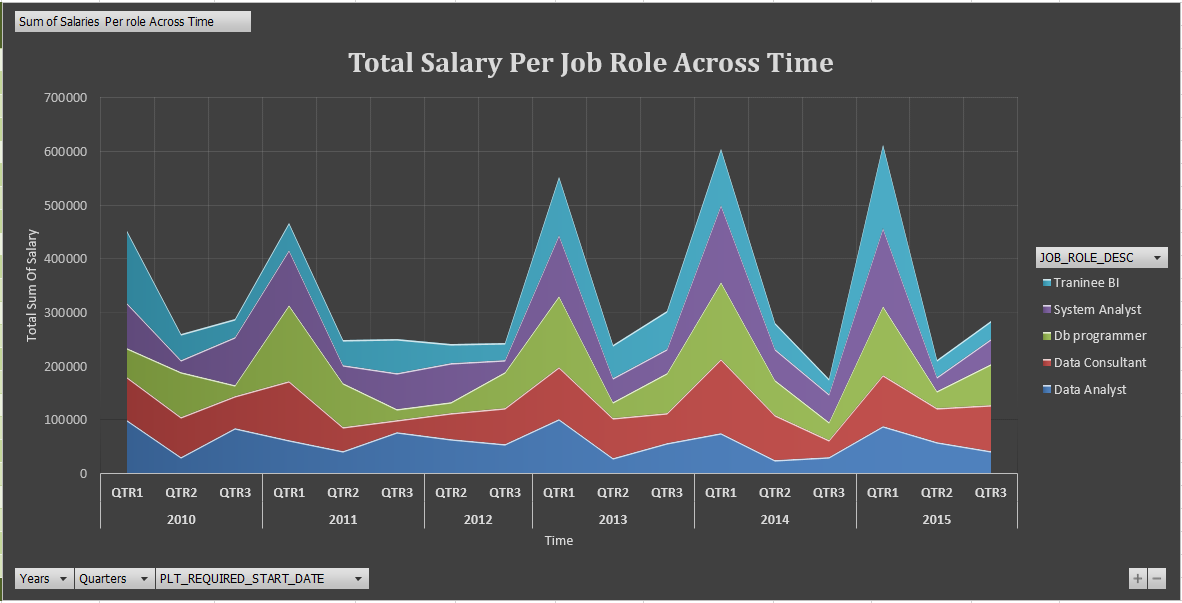


Figure A stacked area line chart that reveals performance over time per job. It can also give insight into the overall performance because it stacks each job role over each other adding them up for a total sum visualisation.

A similar option could be the line chart. This is more effective at looking at the value of each measure (see figure 5).



Figure A line chart providing a view of where individual job roles are performing in their total salary.

A chart can have pivot functionality. This can give a view of a macro or micro detail. When a chart is built via a pivot table in Excel, it inherits the functionality. This could be drilling up or down detail, slicing and representing selected measures (see figure 7 and 8).

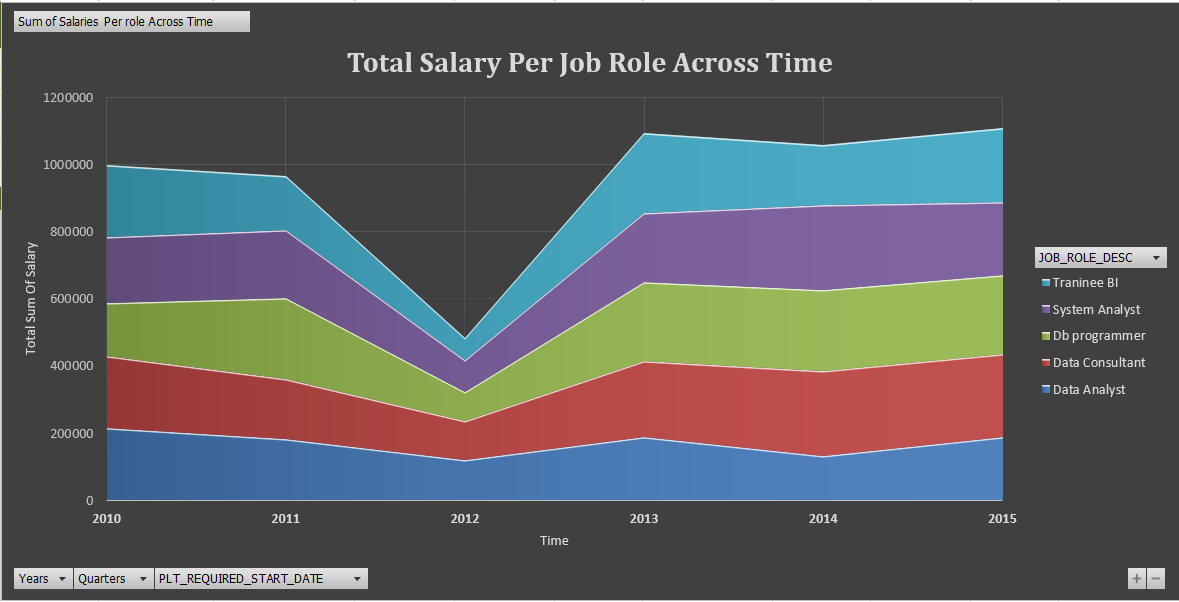


Figure A pivot chart that shows only yearly details.

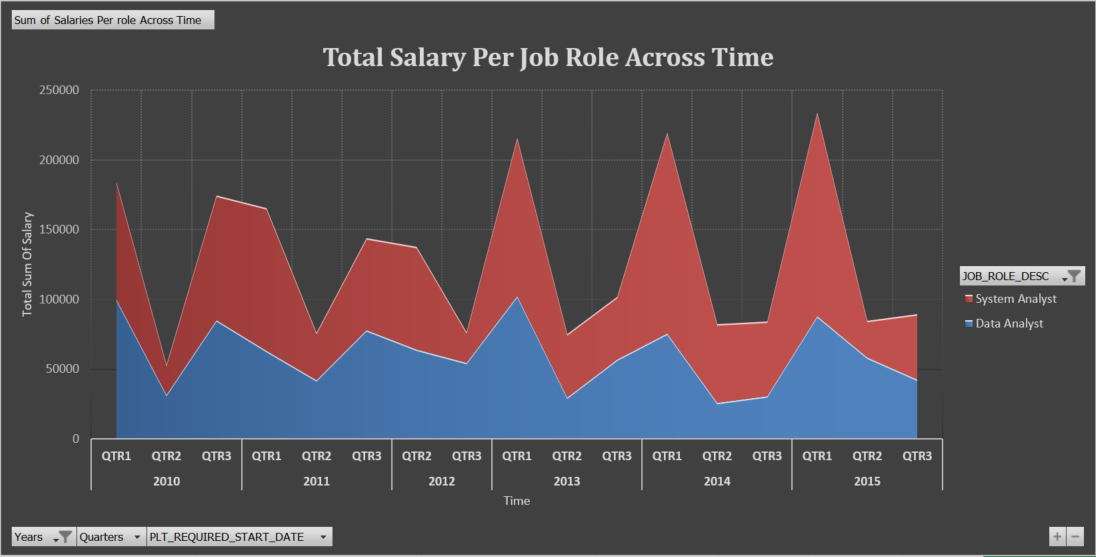
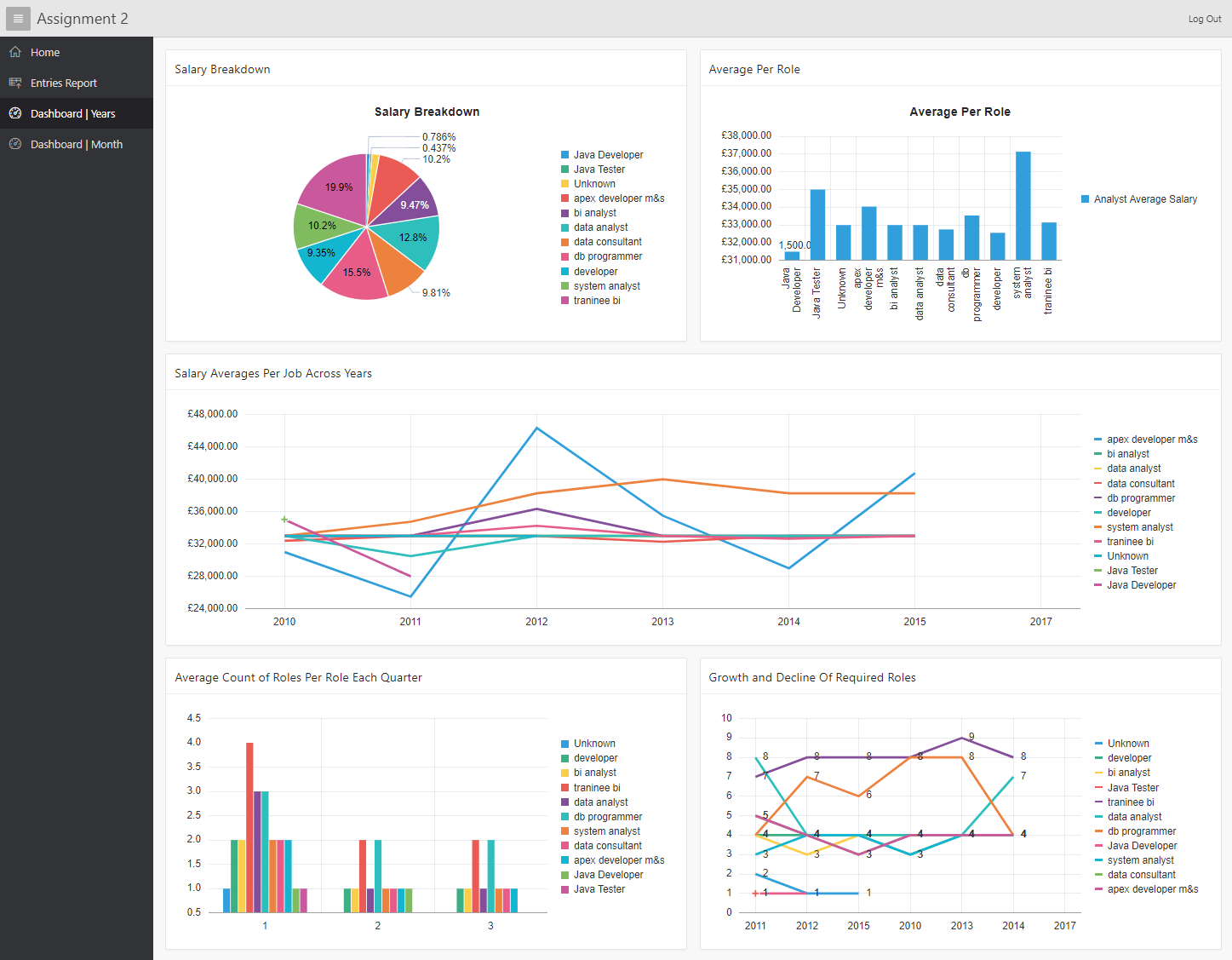


Figure A sliced chart showing only System and Data Analyst roles.

# Dashboard



A Dashboard, more specifically a KPI dashboard should provide insight into how a company is performing much like how a vehicle dashboard. A dashboard allows people to make quick decisions based on easy to digest view of key performance indicators. A good dashboard should be used to:

* **Make comparisons**
* **See trends over time**
* **See distribution**
* **See relationships between parts of our process/organisation**

As well as letting the user know:

* **Things are OK**
* **Things are looking bad**
* **Things are looking good**

**When designing a layout, there are no strict rules to follow, but making sure the charts are clear is key. One such suggestion is to make line charts wide and vertical bar charts square** (Briggs, 2014)**. Secondly, avoiding too much information on one page as to not generate information overload** (Bawden & Robinson, 2009)**.**

**In the following figures, the KPI is monitoring the demands of the companies. More specifically, looking at the number of placements and salary reports.**

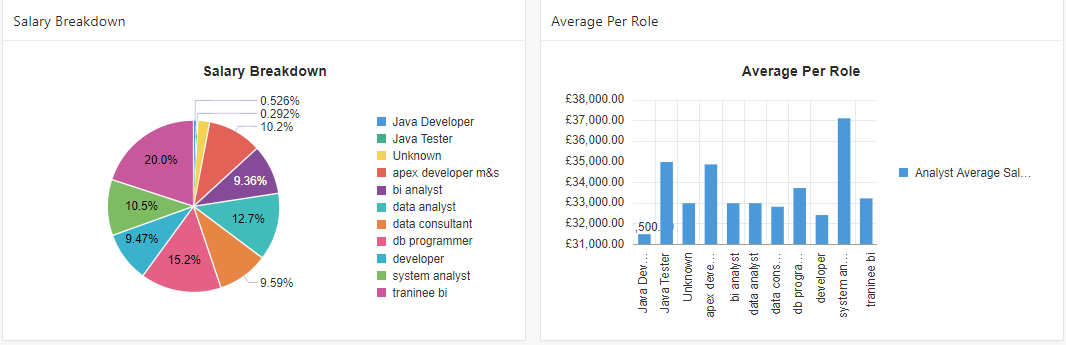


Figure A pie chart breakdown of what jobs are bringing in the most value and a salary average for each job.

|  |  |
| --- | --- |
| SELECT job\_role, SUM(actual\_salary) FROM ss\_temp\_clean GROUP BY job\_role; | SELECT job\_role, ROUND(AVG(actual\_salary), 0) AS Average  FROM ss\_temp\_clean  GROUP BY job\_role; |

As mentioned in the pivot table section, line charts are a good way to plot across time (see figure 10).

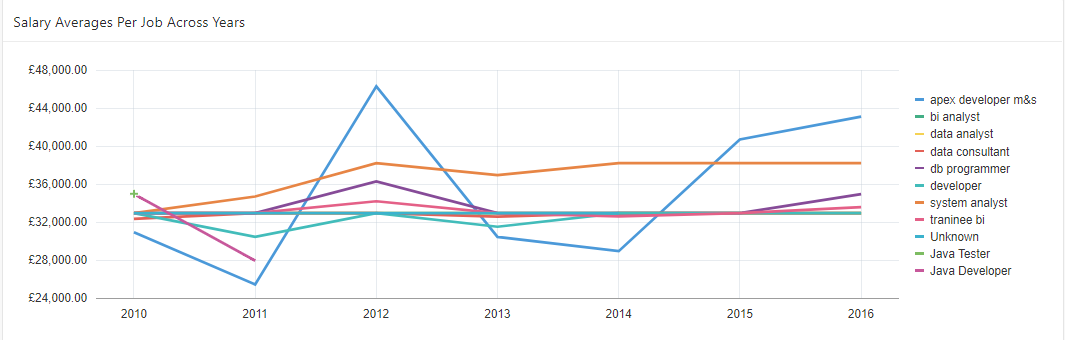


Figure Plotting the performance of roles across time.

|  |
| --- |
| SELECT year, job\_role ,ROUND(AVG(actual\_salary), 0)  FROM ss\_temp\_clean  GROUP BY year, job\_role  ORDER BY YEAR; |

Sometimes splitting the chart into two is clearer. For example, perhaps you want to show the detail of each quarter per year. This may be too cluttered, so a good option is to have a chart describe the typical quarterly performance in one chart and then the yearly performance across another (see figure 11) (Briggs, 2014).

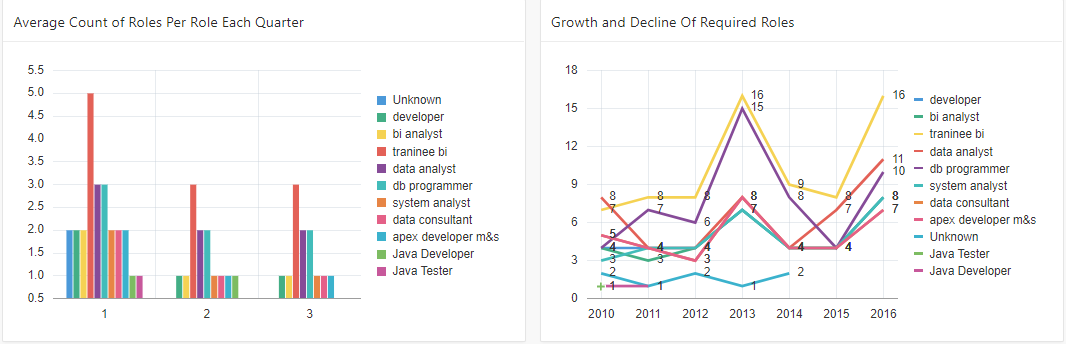


Figure Two charts that work together to describe the requirement for each quarter and then the number of roles per year.

|  |  |
| --- | --- |
| SELECT job\_role, ROUND(AVG(count\_per\_year\_per\_quarter),0) as Average ,quarter FROM (  SELECT job\_role,COUNT(job\_role) AS count\_per\_year\_per\_quarter, year, quarter FROM ss\_temp\_clean GROUP BY job\_role,year,quarter ORDER BY year  ) GROUP BY quarter,job\_role; | SELECT job\_role,year, COUNT(job\_role) FROM ss\_temp\_clean GROUP BY year,job\_role; |

# Ethics and Security

A data warehouse is used to provide analytical information to help decision making and predictions. Because of this, data may be extracted from various sources might contain sensitive information such as healthcare data or company ­­data. A data warehouse may also contain information that helps an establishment compete in markets or streamlining health services.

Any data breach poses loss of value or can become very costly to the victim, whether it be profit or life. In 2017 the NHS suffered a wave of malware called WannaCry that held encrypted data to ransom. This had disrupted the service in areas such as emergency respondents, patient operations and clinical appointments (Grierson & Gibbs, 2017). Furthermore, information leaks can also be a massive legal risk. Morrisons, a British supermarket suffered a data leak when a former employee had leaked the data of approximately 100,000 staff (Chapman, 2017). This lead to a legal battle that suggested Morrisons give compensation to the employees as the data contained personal information. This included information on bank accounts and addresses that could have led to them being victims of fraud or identity theft. During 2014 a study about Data Breach Preparedness, 43% of 33 company respondents reported data breaches. It was also revealed that data breaches are frequently caused by employee mistakes and lack of training (Ponemon Institute LLC, 2014).

Individuals working with sensitive data should keep in mind that the scenario with the WannaCry ransomware had a devastating effect, therefore the right measures should be taken to protect the best interests of their establishment. To combat data breaches, allocating resources to further develop technical security measures such as segmenting a system into clearance levels or access levels at the client level can provide much-needed security. This allows administrators to control access to areas of the system by restricting access for different user types. This can provide better control over who sees what, reducing the risk of a potential data breach (Flair, 2013). Secondly, monitoring activity is an effective measure against a security catastrophe. Detecting abnormal behaviour at the data level early on can provide much needed time to respond to potential threats and risks. One such practice is using a Data Activity Monitor(DAM) architecture. DAMs monitor access and transactions on a database system in real time. This is normally done by logging in a database system audit table. From this, qualified personnel can code various automated measures and triggers to detect IP addresses that are perhaps located in an unauthorised location or checking that users are not entering parts of the system without the right credentials (Wah, 2015). Thirdly, encryption at the data level can reduce the risk of data being read by anyone without access to the key. Encryption of Data at Rest is promoted to secure against direct copying of the database (Inmon, 2005). Finally, the General Data Protection Regulation(GDPR), in effect as of 25th May 2018 attempts to create better data protection measures. The Information Commissioners Office has created a guideline for a new regulation called the Following these guidelines will help prepare for this change (Infomation Commissioner's Office).

It is recommended that anyone who might be responsible for data be active in keeping up with the security and ethics. The suggestions here are only some potential measures that should be taken.

*Word Count: 548*

# Practical Security Implementations and Testing

With regards to a practical security implementation, access control is a common feature used among database driven applications. For example, In an apex application that incorporates access control, an administrator has full access to all features and data. This allows for manipulation and viewing of critical/sensitive information, such as user details, activity logs and administration functions like managing users. On the contrary, normal end users should not be allowed (generally speaking) to view any critical data. Normal Users are permitted to use the application features without being able to access administration features. But if different kinds of users should or could have different access restrictions or requirements to parts of the application data. For example, managers may need to view dashboards on KPIs, but a user only needs to use the application for data input to the data warehouse.

Here is a practical implementation and test of how access control is used:

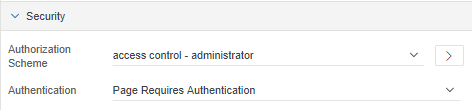


Figure Setting the access control for each page. In this case, only administrators may access this page.

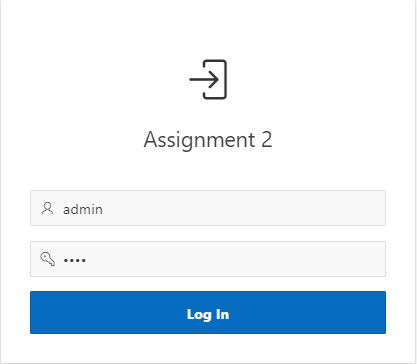


Figure Login in as Admin

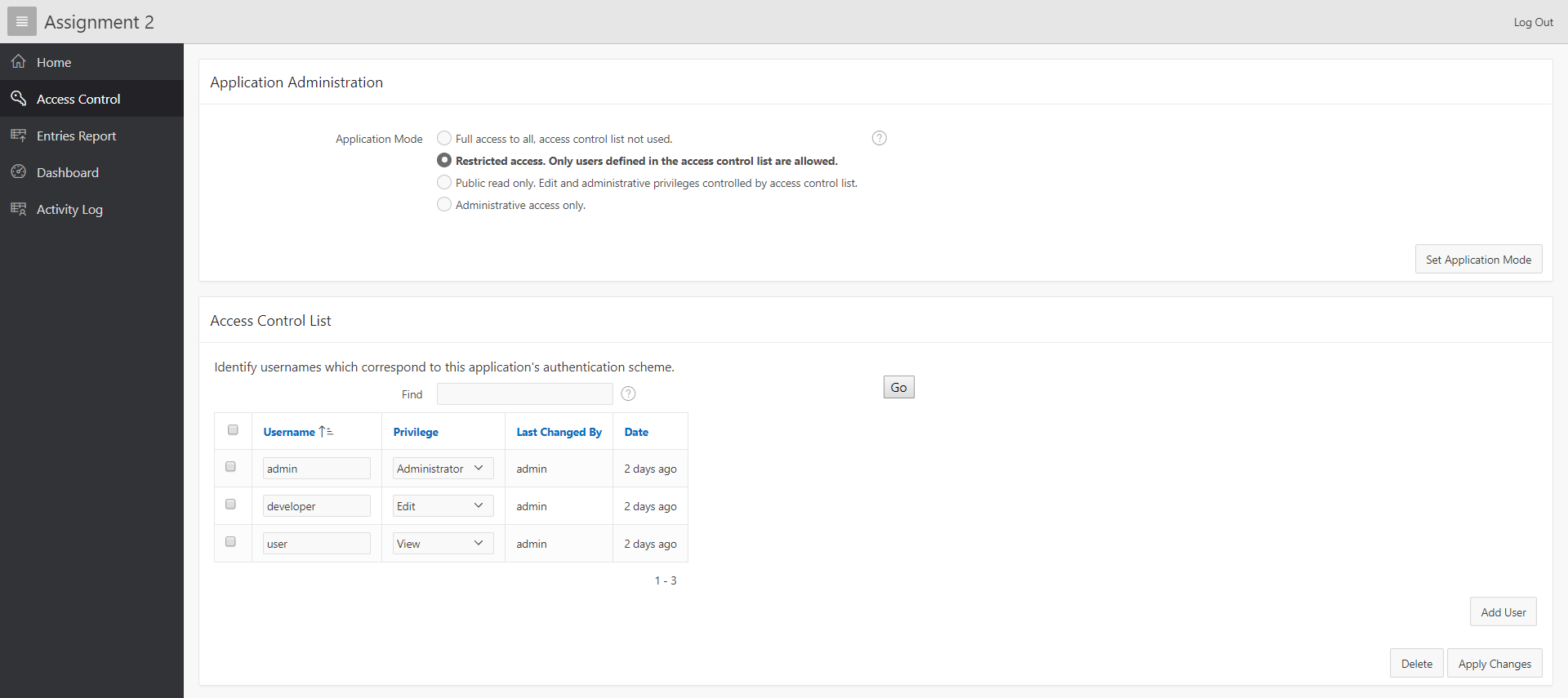


Figure The application features an access control page that allows only administrators to see and change levels of access privilege per each user. As seen, the navigation menu shows all pages of the application to the administrator in the left navigation menu.

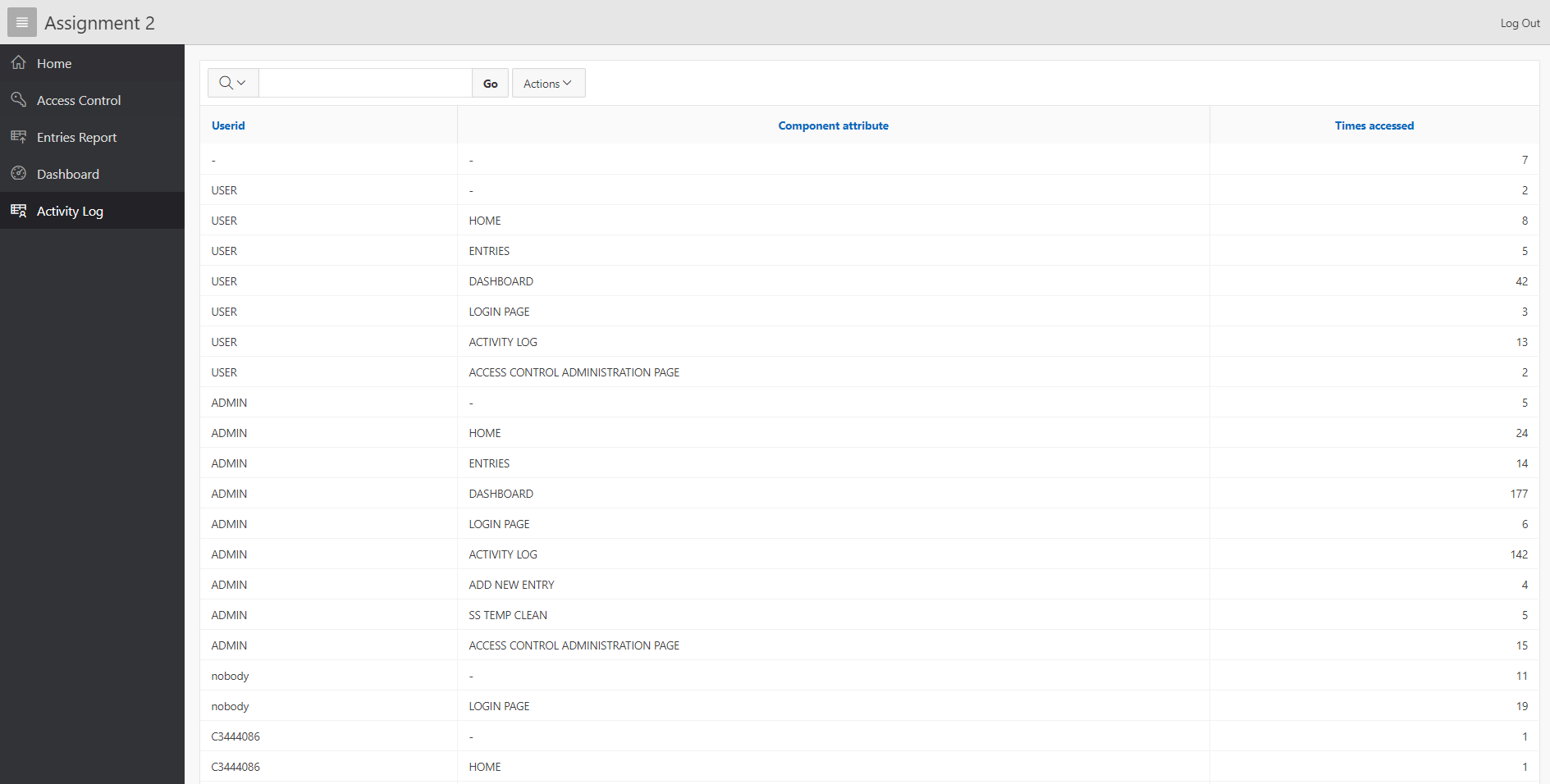


Figure Only Administrators may view the activity to make sure that users are not doing anything out of the ordinary. In this example case, one user has somehow accessed the activity log and access control page which means that they have incorrect privileges. This may pose a security risk. Administrators may now further inquire into the issue.

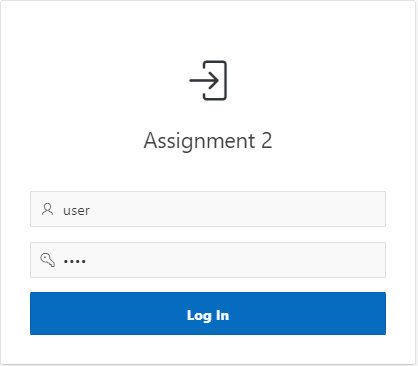


Figure Login as a normal user.

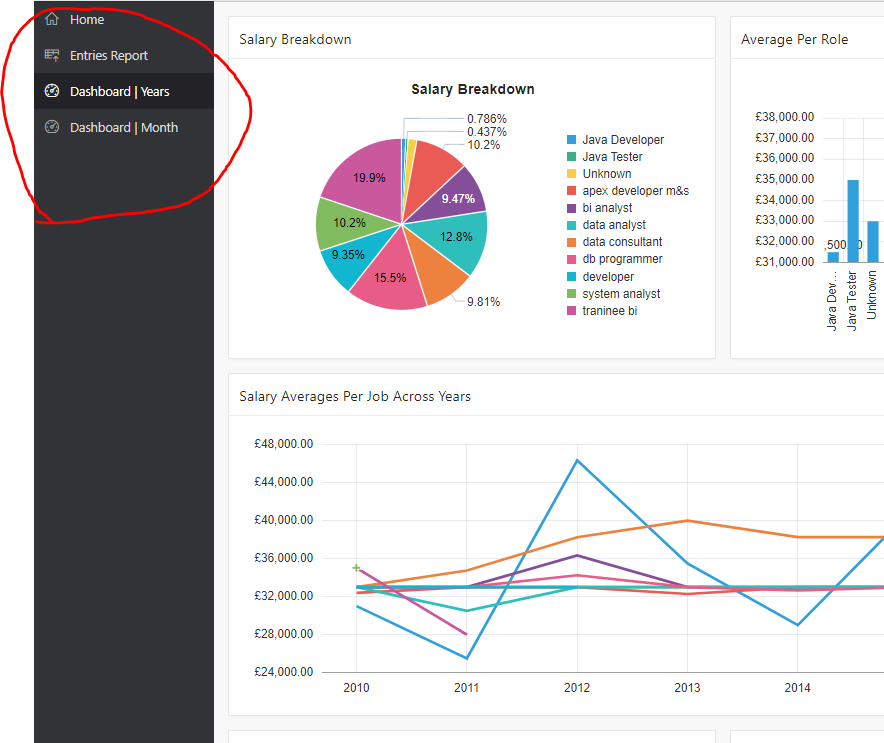


Figure The navigation bar does not show normal users any of the administration pages.

Leading on to a second security consideration, and that is monitoring of activity. Oracle DB/APEX offers SQL access to system event log that can be used to generate reports and charts that are useful for monitoring users and their activity (see figure 10 and 11). With this comes the possibility, as mentioned in the ethics and security research section, to create parameters that may possibly detect any potential threats such as unauthorised IP address login attempt.

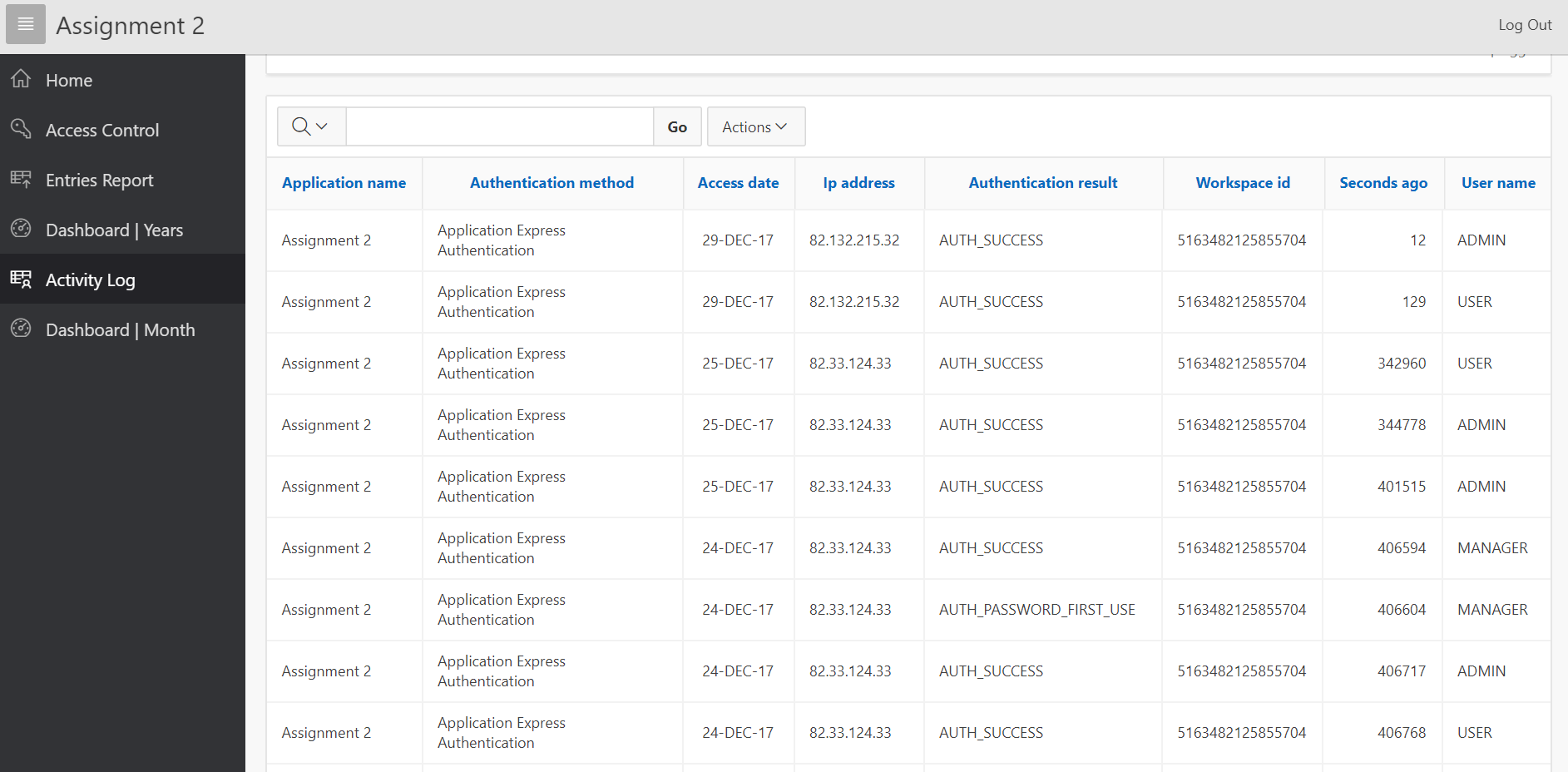


Figure This report shows the IP location, date of authentication attempt and method of authentication of each user.

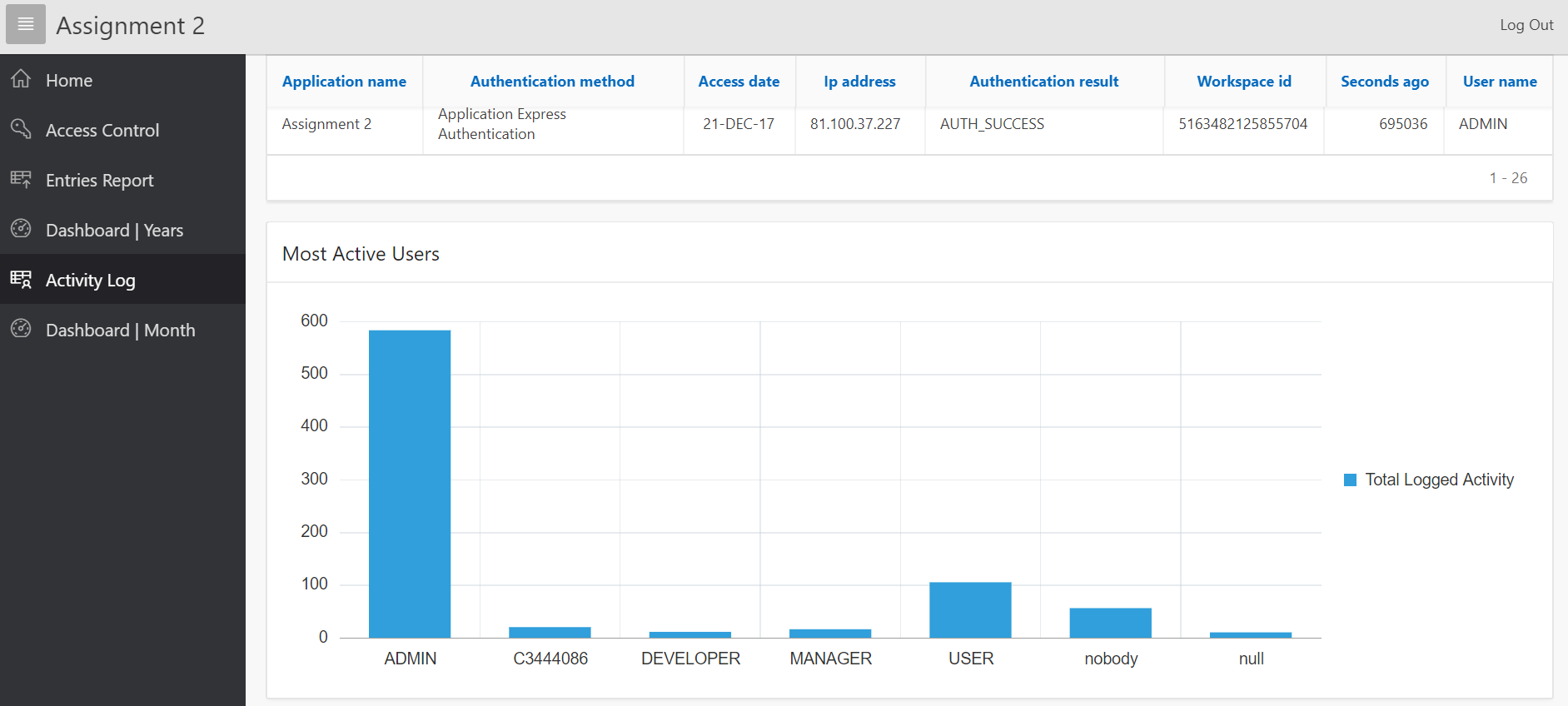


Figure Charts can be built to summarise the activity for a quicker look at the usage of the system. The chart shows the ADMIN is the most active member with USER coming second.

# Reflection

The implementation works to a basic degree. Further work may include adding some form of trigger that logs any unauthorised attempt to log in. This may be done via IP location or a specified period, say, a day where no one should have been able to access the system. Creating these triggers was not possible because of a lack of privileges to the system logs but for example could look something like:

|  |
| --- |
| CREATE TRIGGER unauth\_access\_logger  AFTER  INSERT ON APEX\_WORKSPACE\_ACCESS\_LOG  BEGIN  INSERT INTO  SS\_UNAUTHORISED\_ACCESS\_LOG(  SELECT  Access\_date, User\_name, Ip\_address  FROM  APEX\_WORKSPACE\_ACCESS\_LOG  WHERE  APPLICATION\_ID = 470  AND Access\_Date LIKE "%12/25%"  ORDER BY  access\_date DESC);  END; |

Where the date is Christmas day when people most likely will not be working if the company is closed for the holidays.

The access control had worked as expected, the user was unable to enter admin areas of the application. Administrators had control over who accessed what. As well as that, the activity log has picked up on an authorised user accessing the admin page. The admin now knows about a security risk.

# Bibliography

AlexBerson, & J.Smith, S. (1997). *Data Warehousing, Data Mining & OLAP.* McGraw-Hill.

Bawden, D., & Robinson, L. (2009). The dark side of information: overload, anxiety and other paradoxes and pathologies. *Journal of Information Science, 35*(2), 180-191.

Briggs, J. (2014, April 23). *Management Reports & Dashboard Best Practice*. Retrieved January 2018, 04, from Target Dashboard: https://www.targetdashboard.com/site/kpi-dashboard-best-practice/default.aspx#KPI-Dashboard-Design

Chapman, B. (2017, December 1). *Morrisons data leak: Thousands of staff to receive payout in landmark judgment over personal details posted online*. Retrieved December 27, 2017, from Independent: http://www.independent.co.uk/news/business/news/morrisons-data-leak-staff-payout-details-sensitive-data-personal-online-hack-a8086521.html

Choudhury, S. (2013, June 21). *Choosing the right chart type: Line charts vs Area charts*. Retrieved 01 03, 2018, from FusionCharts: https://www.fusioncharts.com/blog/line-charts-vs-area-charts/

Creative Bloq. (2013, August 08). *The science behind data visualisation*. Retrieved December 2017, 2017, from Creative Bloq: http://www.creativebloq.com/design/science-behind-data-visualisation-8135496

Flair, I. (2013). Access control. *Salem Press Encyclopedia*, 1. Retrieved December 2017, 2017

Grierson, J., & Gibbs, S. (2017, May 19). *NHS cyber-attack causing disruption one week after breach*. Retrieved 12 25, 2017, from The Guardian: https://www.theguardian.com/society/2017/may/19/nhs-cyber-attack-ransomware-disruption-breach

Infomation Commissioner's Office. (n.d.). *Prepairing for the General Data Protection Regulation(GDPR).* Retrieved January 04, 2018, from ico.org.uk: https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

Inmon, B. (2005, August 01). *Encryption at Rest*. Retrieved 01 2018, 2018, from Information Management: https://www.information-management.com/news/encryption-at-rest?regconf=1

K.Janert, P. (2011). *Data Analysis with Open Source Tools.* Sebastopol, Canada: O,Reilly.

Kahneman, D. (2011). *Thinking Fast and Thinking Slow.* Farrar, Straus and Giroux.

Ponemon Institute LLC. (2014). *Is Your Company Ready for a Big Data Breach?* Ponemon Institute LLC . Traverse City: Ponemon Institute LLC.

Wah, M. (2015, July 31). *Data Activity Monitoring and Data Loss Prevention: A Balanced Approach to Securing Your Critical Assets*. Retrieved December 27, 2017, from Security Intelligence: https://securityintelligence.com/data-activity-monitoring-and-data-loss-prevention-a-balanced-approach-to-securing-your-critical-assets/