The issue in this case of Enron is that its email details and private files were made public in 2002 where emails could be seen by non Enron workers and it was manipulated too. The whole email section of Enron was jammed when it was made public where frauds happened with the use of the leaked data available everywhere and very well accessible.

The problem had a severe impact on one of USA’S largest company Enron as it made the company go bankrupt when financial data were leaked outside the company many outsider workers of other firms including workers of Enron manipulated the data gathered to make the company drown as illustrated in the question sheet the data of employees of Enron in collab. It shows how email were shared at a fast pace since data was outside. The issue was so severe that the company a big firm went bankrupt just because of a leak of information.

IT occurred as in Enron Company there was no proper software security and when employees were sending emails they tend to cover up data to be able to leak many other important details of the company even status and identity of workers who sent the email appeared like “N/A” which means unknown emails in collab couldn’t be read as it was encrypted and covered up not to be doubtful about malicious activities taking place. This issue happened because mainly of lack of transparency in work by the employees of Enron and lack of software to detect abnormal data being sent in email as it is visible in extract of email structure that was being sent.

To prevent such thing to happen again good software must be used to detect malicious emails activities. Password can be used for only restricted person can get access to these important data being transferred. Proper training must be given to employees. More severe laws must be implemented at Enron to avoid data leak all electronic commands executed at the company must be watched closely by using antivirus and anti phishing application to control emails sent from the company’s account and to receive clear data on the receiver of these email to be able to track the accused persons next time if a fraud like this happens again.

Plan to fix this issue is that we must analyse the python data and graphs using colab to get as much data possible to be able to fine the root of the fraud who is the real fraud and by building a business report it will help to get a historical overview of the company and also financial data which will help a lot in getting to the root of the problem of email database leak.