# Chapter 6

# Conclusion and Future Recommendation

In this chapter in section 6.1 we conclude our development system. We describe the limitations of our developed system in section 6.2. In the same section, we also provide suggestion for future improvements.

## 6.1 Conclusion

Our primary aim was to develop a system that can automatically detect conspiracy in the mail data of the employees of a company. We design and train the module that can predict the possibility of conspiracy in the user's mail data in real time and give the feedback to the governing body of that company. This system can automatically monitor the email of the users all the day continuously. We uses the conspiracy theory a totally psychological concept to implement in a machine that can automatically detect the infected mail. In this way we uses synthetic data collected from real world and train our module in different way. As it is a concept of psychology and we have used a prediction model to classify the infected mail from the true mail, we can just predict it. So we have the feature to manually monitor the mail also. Those mail are said as conspiracy that can be easily monitored by the governing body manually for further determination. If any main is detected infected and the mail is not really a conspiracy related then the governing body can easily discard the mail from the list. So it is more likely a dynamic module to be repaired manually.

## 6.2 Limitations and Suggestions for Future

As we model the system based on the data that are collected from the real field and we are analyzing the text data to predict, there are always some limitation in the works. Natural language processing is a difficult thing to process. And sentiment from natural language is likely to be more

difficult task. So accuracy is a big factor in this study. As we can say that the overall accuracy can be improved in future by learning the model more and more. By doing this the model will be accurate one day.

In the other hand, in our dataset there was some link, url that we ignored by removing them initially. But if we think properly we can say that these link could be a huge source of conspiracy related activity for a work place. So in future work this link crawling method could be developed properly for further investigation throughout the data set.

In another one is that we also removed the attachment from the email, as we only classify the text data from the dataset. But it is very much possible to have conspiracy into these attachment. And it is also possible that people can sent these related context through some hidden way like html messages and document that could be attached to this mail.

So these are the possible improvement that could be made in this project.