**SE 4050 – Deep Learning**

4th Year second semester

A picture containing text, clipart, vector graphics

Description automatically generated

Assignment

M.R.A.Fadhil

IT20784720

B.Sc. (Hons) in Information Technology Specializing in Software Engineering

Submitted to

Department of Computer Science and Software Engineering

Sri Lanka Institute of Information Technology

Sri Lanka

**Table of Content**

1. Problem Introduction 03
2. Algorithm Introduction 03

2.1 ANN 03

2.2 CNN 05

2.3 RNN 06

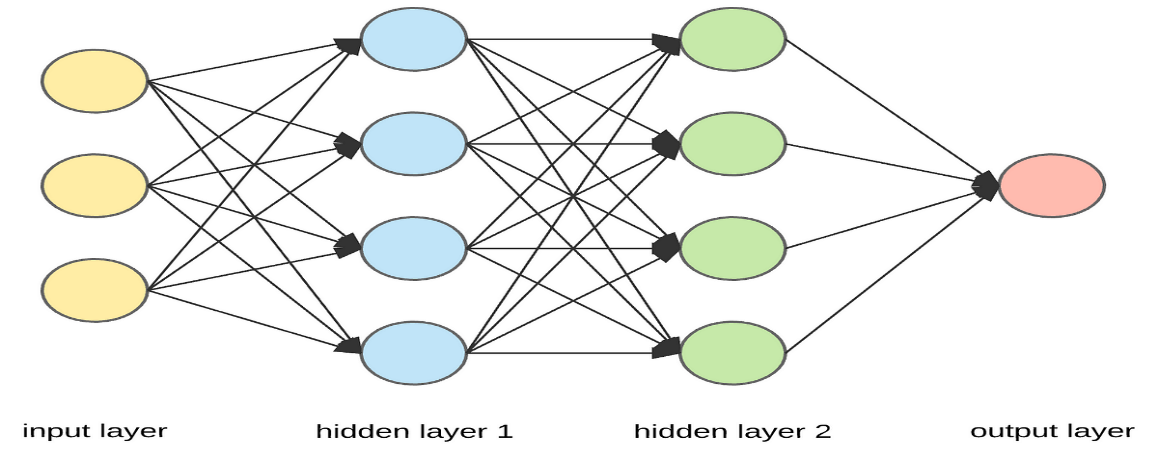
1. About Dataset 09
2. Data Analysis and Visualization 09
3. Data Preprocessing 11
4. Test Results and Analysis 13
   1. ANN 17
   2. CNN 13
   3. LSTM 17
   4. BILSTM 15
5. Conclusion 18
6. **Problem introduction**

Short Message Service (SMS) has become one of the most prevalent forms of personal and business communication. However, with its widespread use, SMS has also become a fertile ground for unwanted and often malicious messages, commonly use known as spam messages, spam messages can be widely used by cyber attackers to get particular user information by sending a spam message that will include some malicious link, once user unknowingly click the link cyber attackers have the ability to get the access of some user information. Sometimes some span messages comes with a congrats message and it says to contact a particular phone number and its calls as spam calls, so it’s important that there is a way to identify these malicious attack through sms messages, so by collecting a various amount of data of sample spam messages and also ham messages, ham messages are messages are normal messages that users receives day to day life. By collecting ham messages as well as spam messages and by feeding into a model, so model can identify the format of ‘spam’ and ‘ham’ messages.so it can help to reduce the scams that occurs through spam messages in sms.

1. **Algorithm Introduction**

This is a classification problem, so when selecting an algorithm, our initial consideration revolves around choosing a model suitable for handling classification tasks. In this particular instance, we are working with an SMS 'spam' and 'ham' classification dataset aimed at distinguishing between spam and legitimate messages. Additionally, it's essential to note that this problem falls under binary classification, meaning it only predicts whether a message is spam or ham. Consequently, we explored various deep learning algorithms to construct models for this task, including Convolutional Neural Networks (CNNs), Long Short-Term Memory networks (LSTMs), Bidirectional LSTMs (BiLSTMs), and Artificial Neural Networks (ANNs). It's worth mentioning that LSTMs and BiLSTMs are part of the Recurrent Neural Network (RNN) family, which can be particularly useful for sequential data analysis.

**2.1 ANN (Artificial Neural network)**

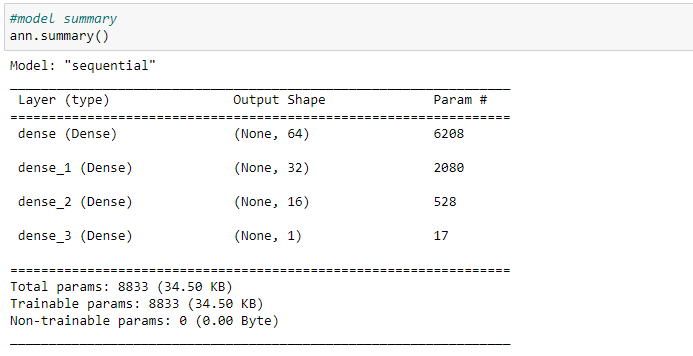
****

Artificial Neural Networks are inspired by the structure and functioning of the human brain. They consist of interconnected nodes that are organized into layers, including an input layer, one or more hidden layers, and an output layer.

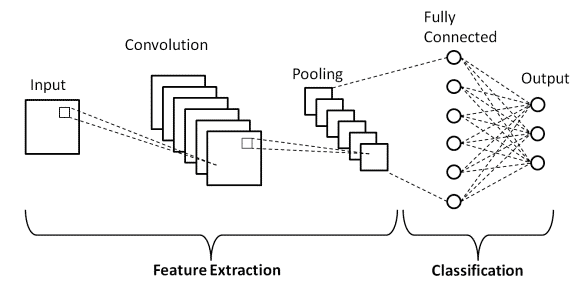
ANNs can be highly effective for text classification tasks due to their ability to capture complex patterns and relationships in textual data.

ANN was developed as follows, first the text are included to preprocessing steps and tokenization was applied to training dataset, then when developing the model, the model contains an input layer with 96 input neuros and identifies as input shape= (96,), then there are three hidden layers which each with 64, 32 and 16 units and all three layers uses ReLU (Rectified Linear Unit) activation function. It helps the network learn complex patterns in the data. And the output layer consists of a 1 unit with a sigmoid activation function. This architecture is typical for binary classification tasks. The sigmoid activation function maps the network's output to a probability value between 0 and 1, making it suitable for binary classification to predict one of two classes.

And also model compiles with some additional configurations by using ‘binary cross entropy’ as loss function which is common for binary classification problems, then the optimizer was ‘Adam’ optimizer with a learning rate of 0.01. Adam is an optimization algorithm that helps adjust the model's weights during training to minimize the loss function. And the model was evaluated using the 'accuracy' metric.



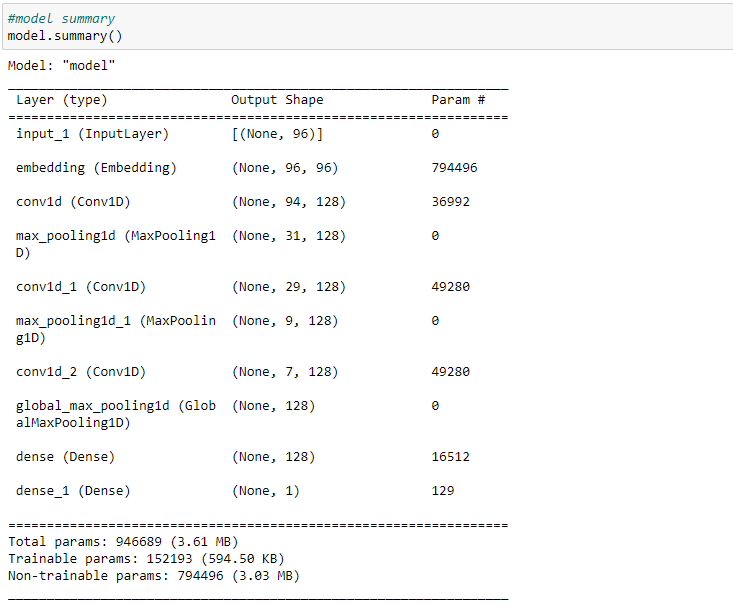
**2.2 CNN (Convolutional Neural Network)**

****

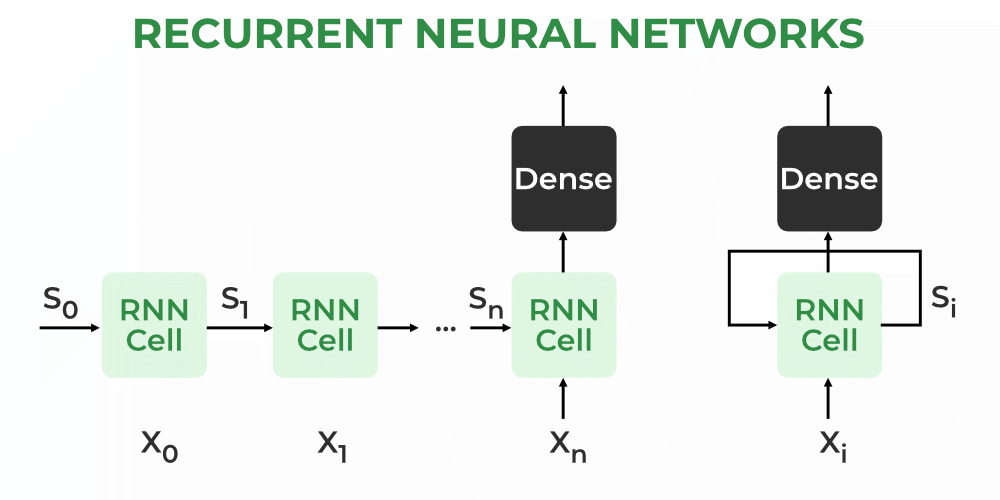
Convolutional Neural Networks (CNNs) are a type of deep learning architecture commonly used for text classification tasks, leveraging their ability to automatically extract meaningful features from text data through convolutional layers to improve classification accuracy.

CNN was developed as follows, The Input layer defines the input shape of the model. It expects sequences of a certain length (96,), then an embedding layer was used to convert categorical data into continuous vector representation, then two Conv1D layer with 128 filters, a kernel size of 3, and uses the ReLU activation function was used. It is used for feature extraction from the input and after each Conv1D layer, a MaxPooling1D layer with a pool size of 3 was added. This reduces the spatial dimensions of the output, which can help the model focus on the most important features. And then GlobalMaxPooling1D was added it extracts the most important features from the entire sequence. Then a Dense layer with 128 units and ReLU activation added after the global max-pooling layer. And the output layer consists of a 1 unit with a sigmoid activation function. This architecture is typical for binary classification tasks. The sigmoid activation function maps the network's output to a probability value between 0 and 1, making it suitable for binary classification to predict one of two classes.

And also model compiles with some additional configurations by using ‘binary cross entropy’ as loss function which is common for binary classification problems, then the optimizer was RMSprop optimizer was used. And the model was evaluated using the 'accuracy' metric.



**2.3 RNN (Recurrent Neural Network)**

****

Recurrent Neural Networks (RNNs) are particularly well-suited for tasks such as natural language processing, speech recognition, and time series analysis. They excel at modeling dependencies and relationships within sequential data. However, traditional RNNs have limitations in capturing long-term dependencies due to the vanishing gradient problem. To overcome this challenge, more advanced RNN variants like Long Short-Term Memory (LSTM), Gated Recurrent Unit (GRU), and Bidirectional Long Short-Term Memory (BiLSTM) have been developed. These variants are proven to be more effective at learning and retaining information over longer sequences.

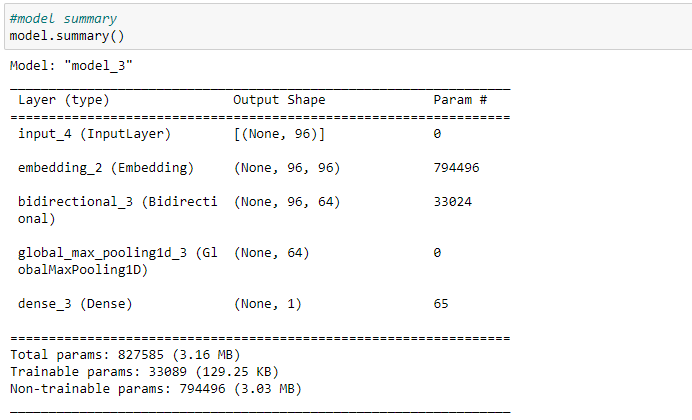
**2.3.1 LSTM and BiLSTM**

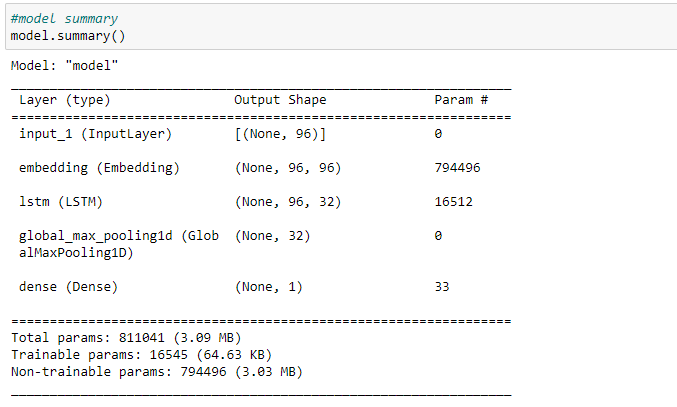
Long Short-Term Memory (LSTM) and Bidirectional Long Short-Term Memory (BiLSTM) are specialized recurrent neural network (RNN) architectures designed to efficiently handle sequential data. These models are particularly useful in text classification tasks due to their ability to capture dependencies and relationships within text data over long sequences.

LSTMs have the ability to effectively model long-range dependencies in text data. BiLSTMs, on the other hand, take the concept of LSTMs a step further by processing the input sequence in both forward and backward directions simultaneously. In text classification, the need for LSTM and BiLSTM models arises from the complexity and variability of natural language. Textual data often contains nuanced relationships, long-range dependencies, and context-specific meanings that traditional models struggle to capture effectively.

Bilstm and lstm both developed as follows, The Input layer defines the input shape of the model. It expects sequences of a certain length (96,), then an embedding layer was used to convert categorical data into continuous vector representation, then for the Bilstm an Bidirectional LSTM layer with 32 hidden units and sets return sequences=True to ensure that it returns the sequences instead of just the final output. The Bidirectional layer processes the input sequence in both forward and backward directions, which can capture bidirectional dependencies in the data. This layer takes the output from the embedding layer as input. then for the lstm an Bidirectional LSTM layer with 32 hidden units and sets return sequences=True to ensure that it returns the sequences instead of just the final output, which means it will produce output sequences of the same length as the input sequences. Then uses an global max-pooling over the sequence data. It extracts the maximum value from each feature across the entire sequence, reducing the sequence length to a fixed size. And the output layer consists of a 1 unit with a sigmoid activation function. This architecture is typical for binary classification tasks. The sigmoid activation function maps the network's output to a probability value between 0 and 1, making it suitable for binary classification to predict one of two classes.

And also model compiles with some additional configurations by using ‘binary cross entropy’ as loss function which is common for binary classification problems, then the optimizer was ‘Adam’ optimizer with a learning rate of 0.01. Adam is an optimization algorithm that helps adjust the model's weights during training to minimize the loss function. And the model was evaluated using the 'accuracy' metric.





1. **About Dataset**

The SMS spam collection data set is a kaggle dataset, the spam messages are collected from Grumble text website and the ham messages are collected through a collection of dataset collected for research at the department of computer science at the national university of Singapore.

The dataset mainly contains two main columns one classify whether the message is ‘spam’ or ‘ham’ and other column is contain the spam or ham message.

Resource URL:

<https://www.kaggle.com/datasets/uciml/sms-spam-collection-dataset>

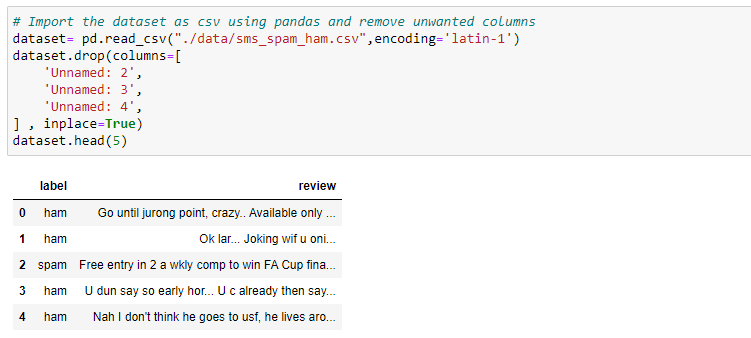
Download url:

<https://www.kaggle.com/datasets/uciml/sms-spam-collection-dataset/download?datasetVersionNumber=1>

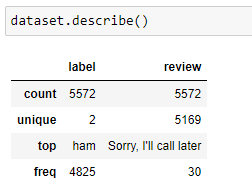
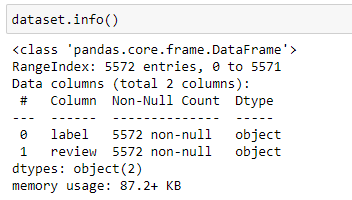
The dataset contains collection of 5574 datasets, with classified as ham or spam.

1. **Data analysis and visualization**

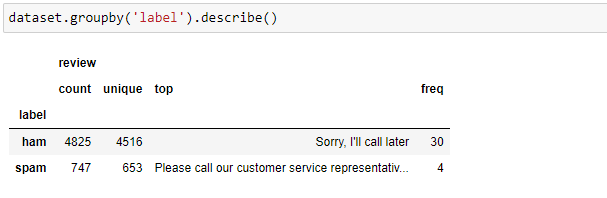
At the beginning we need to load the dataset as csv and display the dataset, for that we displayed top 20 head datasets. Then if there are unwanted columns available we can remove those columns.



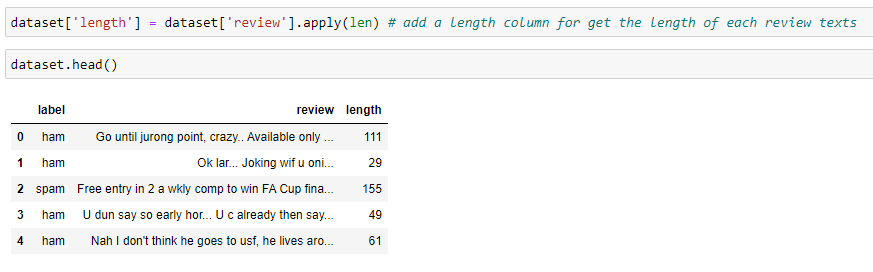
There are mainly 2 columns , first one is the Label column which classified as spam and ham , if the message spam the column value will be span and if the message is ham the column value will be ham. The other column will display the spam or ham message.



When grouping the dataset according to the ‘Label’, it shows there are 4825 ham messages and 747 spam messages, and also we can observe that there are 4516 unique ham messages and 653 unique spam messages that need to consider when doing the preprocessing to identify the duplicate values and remove from the dataset.

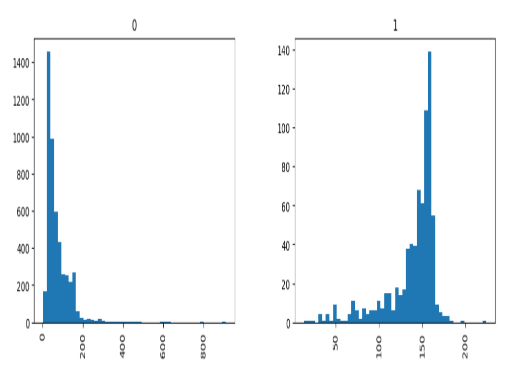
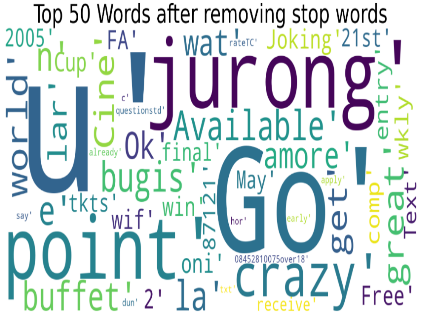
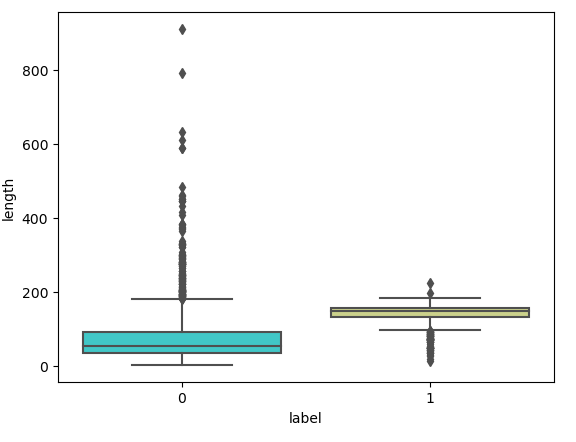


To identify the message lengths of each message, we also added a new column containing the length of each message, and we can observe that the top message contains length of 910.



We use the visualization according to the message length base off the label type (spam or ham), for the visualization we use count plot of number of occurrence for each type of label, boxplot of text length for each label type.

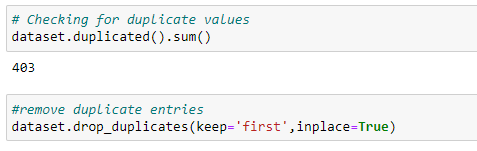
One of the main goal is to, tokenize each message and then apply preprocessing to remove unwanted punctuations and stop words and then apply lemmatization. and then apply all the changes to training data , so those steps will be handled in the preprocessing steps , once all stop words removed we can display the common words that are used in the datasets.

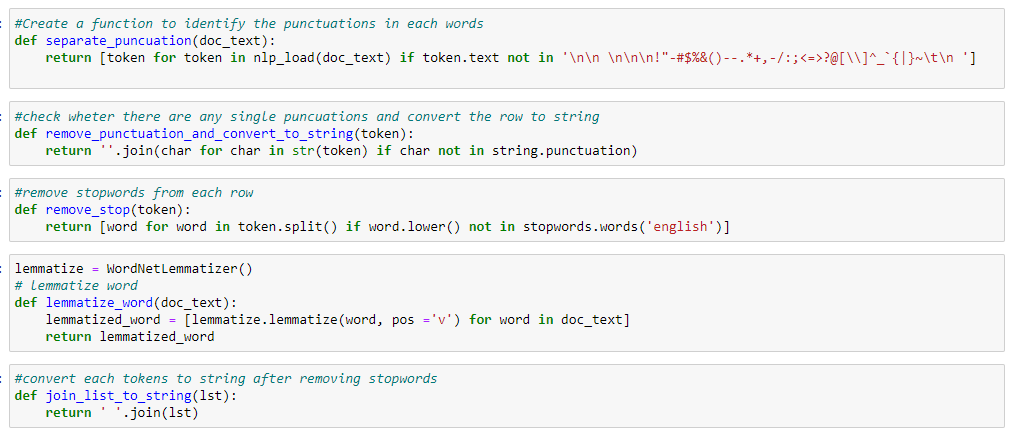
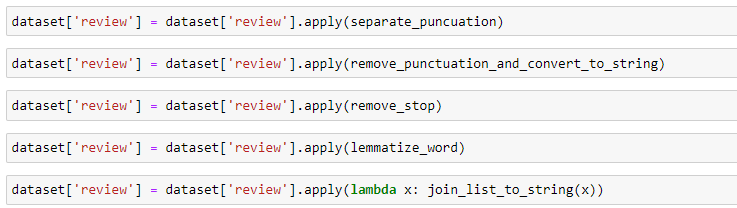


1. **Data preprocessing**

The data preprocessing is really important to get a great accuracy, in nlp there are many steps need to follow in order to complete the preprocessing, when it comes to our sms spam and ham dataset, the following preprocessing methods are performed,

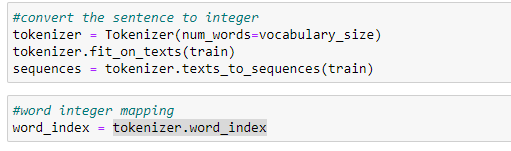
1. Identify the null values from the dataset and remove from the dataset
2. Identify the duplicate values or entries from the dataset and remove from the dataset
3. Apply label encoder on the target column to convert the values to 0 and 1
4. Break in to tokens each row of message and identify if there ant word of punctuations.
5. Check each words single letter to identify if there are any punctuations was attached with the word.
6. Stop words are frequently occurred words since we can remove stop words because it doesn’t contribute in our problem
7. After removing the stop words again join each words as string
8. Apply lemmatization , lemmatization convert a word to its root form
9. Tokenizing to convert the words to integer





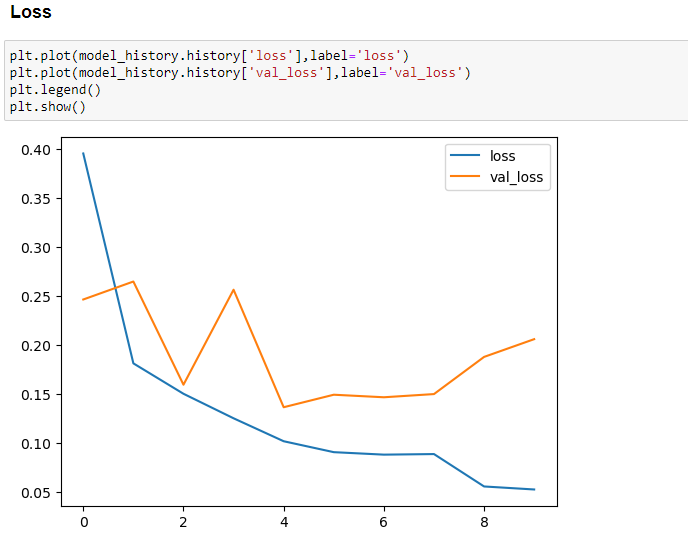
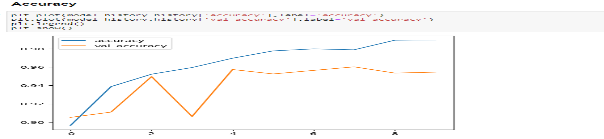
When cleaning the data removing the stop words and then applying lemmatization was are important steps need to be done in order to clean the text in the dataset.

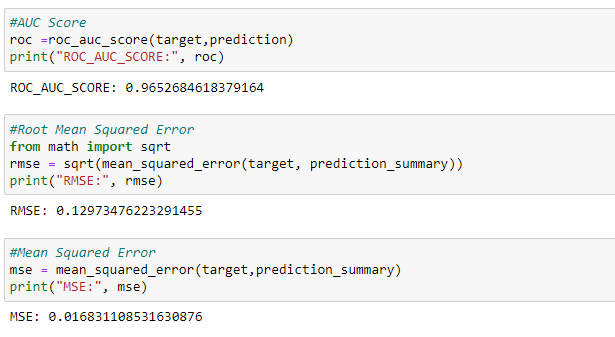
We use Tokenizer method to break the string into word and then convert each word in to integer value that can be used for word embedding. Once each word is convert to integer by using ‘tokenizer.word\_index’ method we can map each integer to the appropriate word.

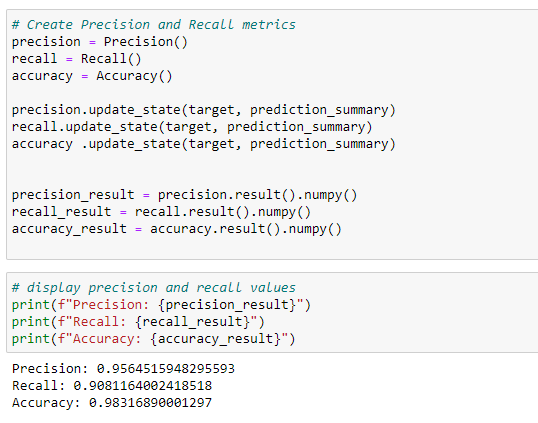
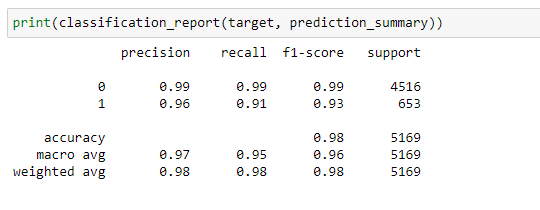


1. **Test result and analysis**

**6.1 CNN (Convolutional Neural Network)**

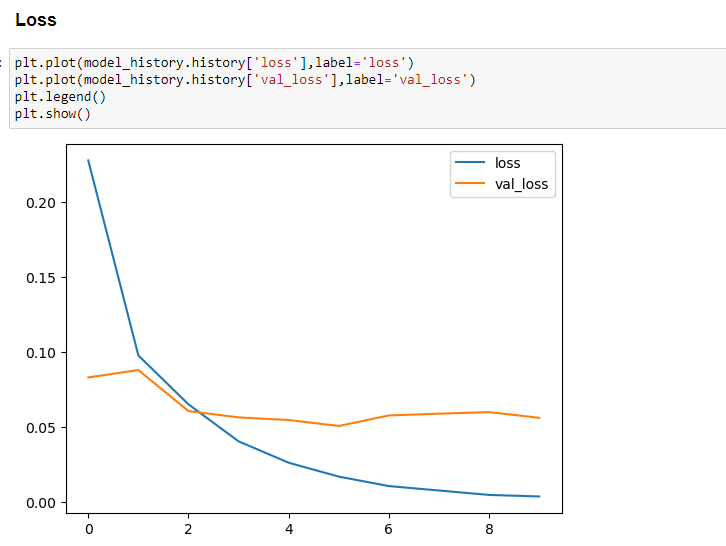
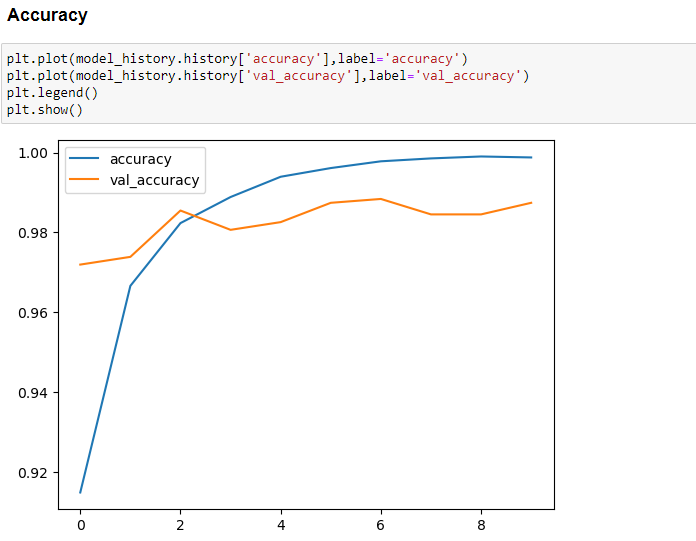


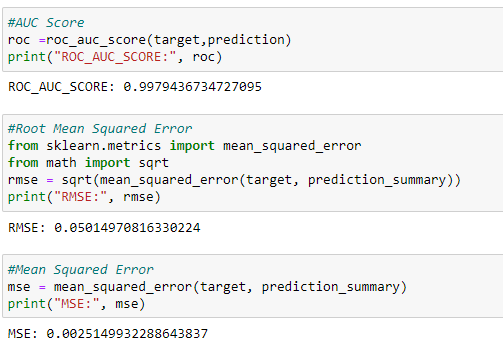


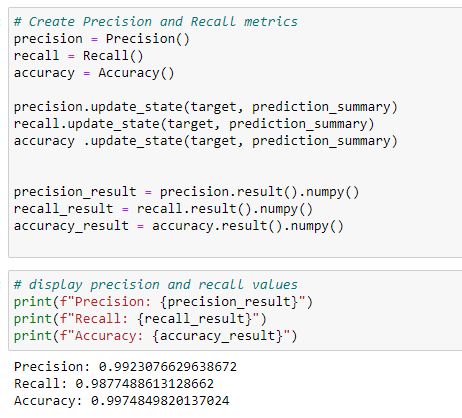


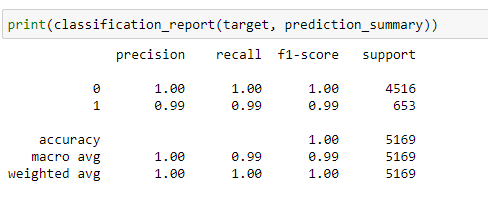
The CNN model having an ROC AUC (Receiver Operating Characteristic Area Under the Curve) score of 0.9652, it demonstrates a high ability to distinguish between positive and negative classes, indicating strong discriminatory power. The low RMSE (Root Mean Square Error) value of 0.1297 suggests that the model's predictions closely align with the actual values in a regression context, implying good predictive accuracy. Additionally, the precision score of 0.95645 indicates that the model has a high proportion of true positive predictions among its positive class predictions, minimizing false positives. The recall of 0.9081 showcases the model's ability to correctly identify a substantial portion of actual positive cases. Lastly, the high accuracy of 0.9831 underscores the model's overall correctness in classifying instances, making it a robust and reliable tool for the given task.

**6.2 BiLstm (Bidirectional Long Short Term Memory)**



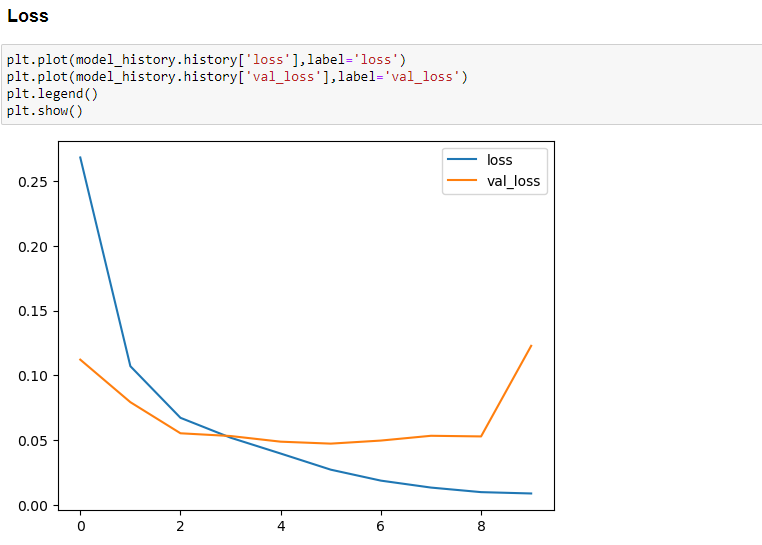
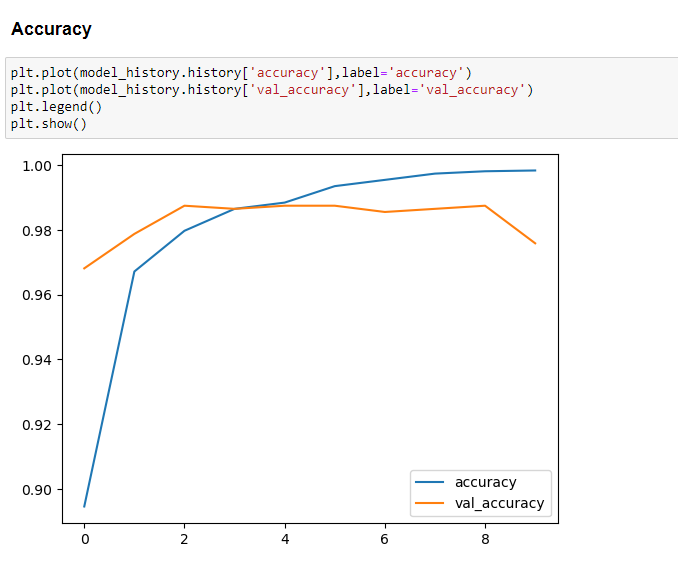


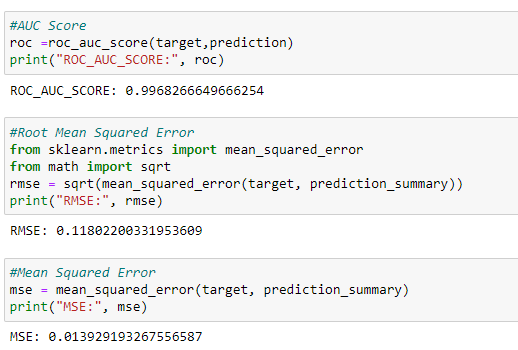
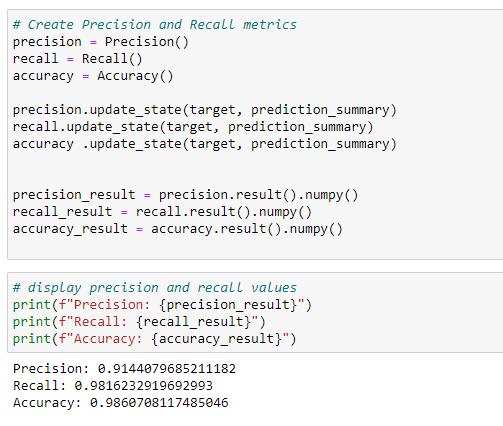


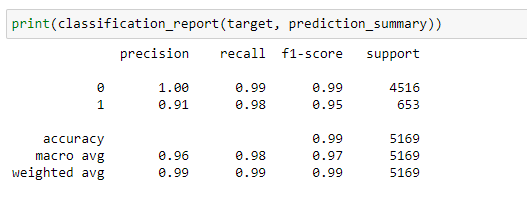


The Bilstm model having an ROC AUC (Receiver Operating Characteristic Area Under the Curve) score of 0.997, it demonstrates outstanding discriminative power in distinguishing between positive and negative cases, suggesting that it's highly effective at classification tasks. The low RMSE (Root Mean Square Error) of 0.050 indicates that the model's predictions are very close to the actual values, highlighting its accuracy in regression tasks. Moreover, the model achieves a precision of 0.992307 and recall of 0.9877488, demonstrating its ability to not only make accurate positive predictions but also effectively identify a large proportion of actual positives. This combination of high precision and recall suggests a well-balanced trade-off between minimizing false positives and false negatives. Finally, the accuracy of 0.997 indicates that the model correctly classifies the majority of the instances in the dataset, further underscoring its overall excellence in predictive performance. Overall, this model showcases exceptional performance across various metrics.

**6.3 LSTM (Long Short Term Memory)**

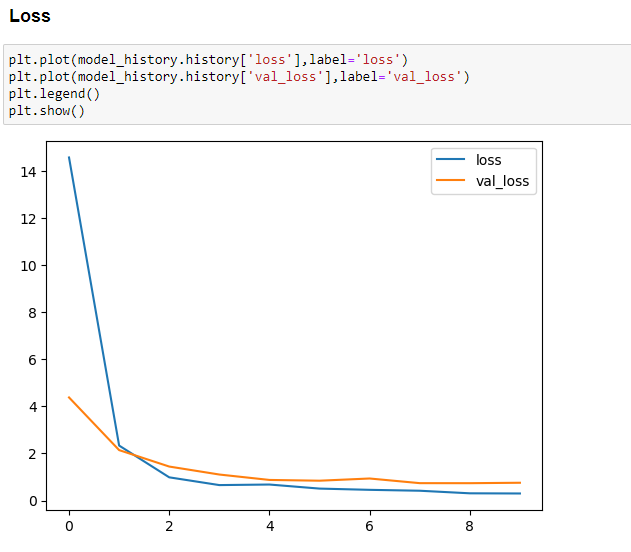
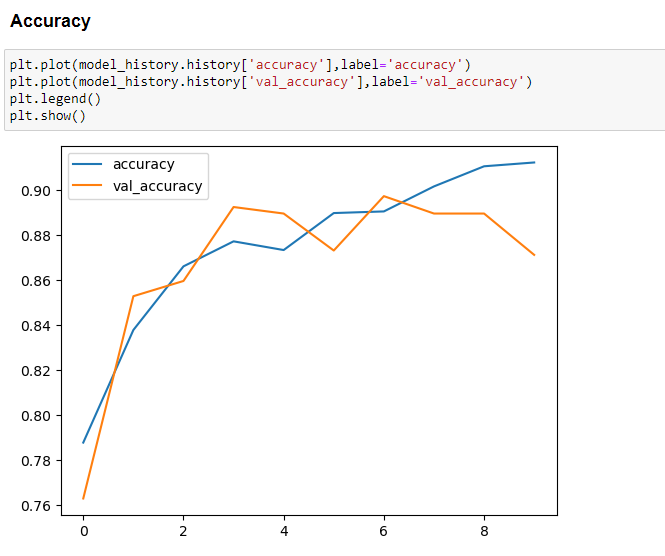


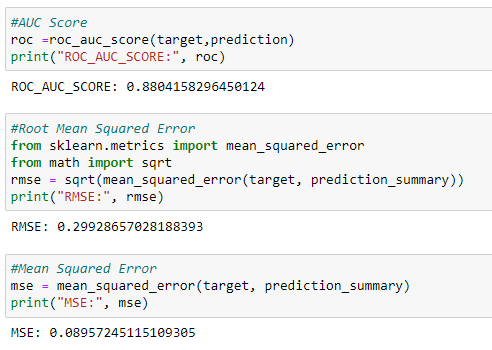
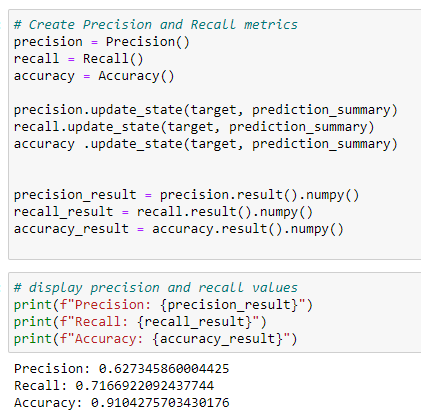


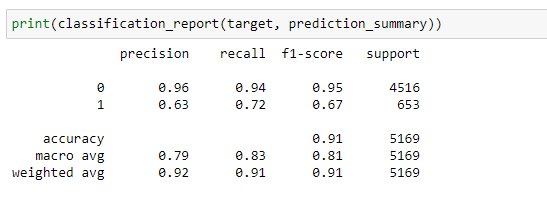


The Lstm model having an ROC AUC score of 0.996 suggests that the model has a high ability to distinguish between positive and negative classes, making it well-suited for binary classification tasks. The low RMSE (Root Mean Square Error) value of 0.1180 indicates that the model's predictions are very close to the actual values, which is particularly relevant for regression tasks. Furthermore, the precision of 0.914407 and recall of 0.981623 signify that the model strikes a strong balance between minimizing false positives and false negatives, essential for scenarios where precision and recall are critical. Lastly, an accuracy of 0.9860 demonstrates that the model correctly classifies a large majority of the samples, further highlighting its overall robustness and competence in handling the given task.

**6.4 ANN (Artificial Neural Network)**







The ANN model having an ROC AUC (Receiver Operating Characteristic Area Under the Curve) score of 0.8804, it demonstrates a strong ability to discriminate between positive and negative classes in binary classification tasks. A lower RMSE (Root Mean Square Error) value of 0.2992 suggests that the model is accurate in predicting continuous numerical values, indicating good regression performance. Additionally, a precision of 0.6273 indicates that the model has a relatively low rate of false positives, which is important in applications where minimizing Type I errors is critical. A recall of 0.7166 shows that the model captures a substantial portion of the true positive cases, and an accuracy of 0.9104 indicates that it is overall quite accurate in its predictions.

1. **Conclusion**

Based on the evaluation of four different models, The BiLSTM model stands out with an outstanding ROC AUC score of 0.997, indicating exceptional discriminative power in binary classification tasks. Its low RMSE of 0.050 demonstrates high accuracy in regression tasks, and it achieves an impressive precision of 0.992307 and recall of 0.9877488, striking a well-balanced trade-off between false positives and false negatives. The high accuracy of 0.997 further solidifies its overall excellence. In conclusion, the BiLSTM model appears to be the top-performing model in overall.