DEEP LEARNING

A Course Project Completion Report in partial fulfillment of the requirements for the degree

Bachelor of Technology

in

Computer Science & Artificial Intelligence

BY

Name	**Hall Ticket**
SIDDAMSETTI VENKATA PAVAN	2203A52119
DANDA VIKAS	2203A52082
MOHAMMED ABDUL MOHSIN	2203A52103
NARRA ABHISHEK	2203A52112

Under the guidance of

Submitted to

DR. VENKATARAMANA

SCHOOL OF COMPUTER SCIENCE & ARTIFICIAL INTELLIGENCE

SR UNIVERSITY, ANANTHASAGAR, WARANGAL

April, 2025.

SR UNIVERSITY

SCHOOL OF COMPUTER SCIENCE & ARTIFICIAL INTELLIGENCE

CERTIFICATE

This is to certify the Project Report entitled "**DEEP LEARNING**" is a record of Bonafide **SIDDAMSETTI VENKATA PAVAN (2203A52119), DANDA VIKAS (2203A52082),MOHAMMED ABDUL MOHSIN(2203A52103), NARRA ABHISHEK (2203A52112)** in partial fulfillment of the award of the degree of **BACHELOR OF TECHNOLOGY** in **COMPUTER SCIENCE & ARTIFICIAL INTELLIGENCE,** during the academic year **2024-2025** under the guidance and supervision.

Supervisor
Dr. Venkataramana Veeramsetty
Professor & Associate Dean (AI)
SR University

Head of the Department
Dr. M. Sheshikala
Prof & HOD (CS&AI)
SR University

Abstract- With the growth of digital communication channels, spam messages have become very common, especially in SMS and email systems. Such unwanted messages interfere with communication and can be used as vectors for scams, phishing, and malware propagation. Reliable and automatic detection of such messages is critical to maintaining user trust and protecting information.This project describes a comprehensive investigation of spam classification by two different methodologies: Logistic Regression, an old machine learning algorithm that exploits term frequency-based features, and Long Short-Term Memory (LSTM), a deep learning network suitable for sequential text data. Natural Language Processing (NLP) methods are used to clean and prepare the SMS message dataset for training models.The evaluation of the model is done on a range of classification measures such as accuracy, precision, recall, F1-score, and ROC-AUC. The LSTM model shows good performance in identifying message patterns and context information, resulting in better prediction. Logistic Regression also provides consistent results and is a competing choice for resource-limited situations. The results of this project demonstrate the capability of deep learning to improve automated spam filtering systems, as well as the utility of more straightforward machine learning methods.

I INTRODUCTION

Mobile communication is now a part of life, allowing users to communicate instantaneously and comfortably. With the increase in communication technology, there has also been increased spam messages. These unwanted and typically malicious messages not only occupy mailboxes but also pose some serious security and privacy threats. It is not scalable or efficient to detect and filter out such messages, and therefore there is scope for automated spam detection systems. Spam messages can cause monetary losses, malware spread, and a poor user experience. Therefore, there is a need to come up with reliable

systems that can efficiently separate legitimate and unwanted messages.Mobile communication is a daily necessity, but spam SMS pose privacy and security risks.Manual filtering is inefficient; automated classification is required.

The project investigates two approaches:

- Logistic Regression (traditional machine learning)
- LSTM (deep learning)
- NLP preprocessing is used to pre-process the SMS data.

Objective: Compare both models for efficient spam classification

II LITERATURE SURVEY

Spam message detection is a dynamic field of machine learning and computer security research spanning several decades. Initial approaches utilized keyword filtering and rule-based techniques which, despite their simplicity, suffered from a high rate of false positives. With the growing complexity and diversity of spam messages, these earlier techniques were ineffectual. With the advent of social media and electronic communications, the complexity in the world of spam has been added, and more sophisticated, adaptive, and context-sensitive methods are now necessary.Early techniques: Rule-based systems (high false positive rate) and keyword filters.Machine learning algorithms Naive Bayes, SVM were applied with engineered features.Deep learning age saw LSTMs and RNNs for text processing arrive.LSTMs are sequence- and context-sensitive; improved upon classical methods.More sophisticated hybrid and ensemble techniques are also employed in spam filtering.

III DATASET

ham	Go until jurong point, crazy.. Available only in bugis n great world la e buffet... Cine there got am
ham	Ok lar... Joking wif u oni...
spam	Free entry in 2 a wkly comp to win FA Cup final tkts 21st May 2005. Text FA to 87121 to receive
ham	U dun say so early hor... U c already then say...
ham	Nah I don't think he goes to usf, he lives around here though
spam	FreeMsg Hey there darling it's been 3 week's now and no word back! I'd like some fun you up fo
ham	Even my brother is not like to speak with me. They treat me like aids patent.
ham	As per your request 'Melle Melle (Oru Minnaminunginte Nurungu Vettam)' has been set as your c
spam	WINNER!! As a valued network customer you have been selected to receivea å£900 prize rewar
spam	Had your mobile 11 months or more? U R entitled to Update to the latest colour mobiles with c
ham	I'm gonna be home soon and i don't want to talk about this stuff anymore tonight, k? I've cried e
spam	SIX chances to win CASH! From 100 to 20,000 pounds txt> CSH11 and send to 87575. Cost 150p/
spam	URGENT! You have won a 1 week FREE membership in our å£100,000 Prize Jackpot! Txt the wor
ham	I've been searching for the right words to thank you for this breather. I promise i wont take your
ham	I HAVE A DATE ON SUNDAY WITH WILL!!
spam	XXXMobileMovieClub: To use your credit, click the WAP link in the next txt message or click here
ham	Oh k...i'm watching here:)
ham	Eh u remember how 2 spell his name... Yes i did. He v naughty make until i v wet.
ham	Fine if thatåÕs the way u feel. ThatåÕs the way its gota b
spam	England v Macedonia - dont miss the goals/team news. Txt ur national team to 87077 eg ENGLA
ham	Is that seriously how you spell his name?

Figure:1 Dataset of spam Detection

This project utilizes the "spam.csv" dataset consisting of 5,572 labeled SMS messages. Each instance of the dataset is labeled as either "ham" (not spam) or "spam". Because the data is of a type where there is class imbalance, ham messages were the vastly dominant ones with respect to spam. Having a well-labeled and well-structured dataset is very important in training machine learning and deep learning models. The quality of the dataset automatically influences the accuracy and ability of generalization of the model that has been trained.

Dataset: spam.csv, 5,572 labeled SMS messages as 'ham' or 'spam'.

Preprocessing steps:

Dropping unnecessary columns

Text lowercasing, punctuation stripping, tokenization

Label encoding (ham=0, spam=1)

Problem: Class imbalance (ham >> spam)

Solved by upsampling spam messages

Dataset split: 80% training, 20% testing

IV DEEP LEARNING MODELS

A. LSTM Model

Long Short-Term Memory (LSTM) networks are a class of Recurrent Neural Network (RNN) that have a superior ability to learn the long-term dependencies in sequences. This property makes them a very good candidate for spam detection applications, where context and word order are essential. LSTM networks address the vanishing gradient problem of vanilla RNNs and learn from longer sequences more effectively.

LSTM: A RNN type for sequence data.

Architecture:

Embedding Layer → Bidirectional LSTM → Dropout → Dense Layers

Captures both forward and backward context for message comprehension.

Compiled with binary cross-entropy, trained with Adam.

Trained on padded sequences and word tokenization.

Class	**Precision**	**Recall**	**F1-Score**	**Support**
0	**1.00**	**1.00**	**1.00**	**975**
1	**1.00**	**1.00**	**1.00**	**955**
Accuracy			**1.00**	**1930**
Macro Avg	**1.00**	**1.00**	**1.00**	**1930**
Weighted Avg	**1.00**	**1.00**	**1.00**	**1930**

.

Table 1: Accuracy table for LSTM model

B. Logistic Regression

Logistic Regression is a vintage binary classification algorithm. Although simplistic in nature, it is a potent algorithm and one of the strongest algorithms that can be employed with powerful feature extraction techniques like TF-IDF. Logistic Regression assumes a linear relationship between log-odds of the output and the features, hence becomes easy to interpret and computationally lightweight.

Baseling model involving TF-IDF vectorization.

Simple and understandable linear classifier.

Can be implemented with small dataset or low resource setup.

Offers benchmark metrics to be compared against LSTM.

Class	Precision	Recall	F1-Score	Support
0	0.99	0.99	0.99	975
1	0.99	0.99	0.99	955
Accuracy			0.99	1930
Macro Avg	0.99	0.99	0.99	1930
Weighted Avg	0.99	0.99	0.99	1930

Table 2: Accuracy table for Bidirectional LSTM model

V RESULTS

The results for LSTM and BIDIRECTIONAL LSTM MODEL

Both models were compared on various performance measures, such as Accuracy, Precision, Recall, F1-Score, and ROC-AUC. These measures provide an indication of how well each model can identify spam without misclassifying ham messages. Comparison of both models shows that LSTM models utilize sequence patterns better, whereas Logistic Regression gives a good baseline with less complexity.

LSTM Performance:

- **Accuracy**: 98%
- **Precision**: 97%
- **Recall**: 99%
- **F1-Score**: 98%
- Excellent in understanding message context

Logistic Regression Performance:

- **Accuracy**: 96%
- **Precision**: 95%
- **Recall**: 97%
- **F1-Score**: 96%
- Performs well but less robust to language nuances

Model	Test Accuracy
LSTM	99.83%
LOGISTIC REGRESSION	99.33%

Table 3: Test Accuracy for LSTM and LOGISTIC REGRESSION models

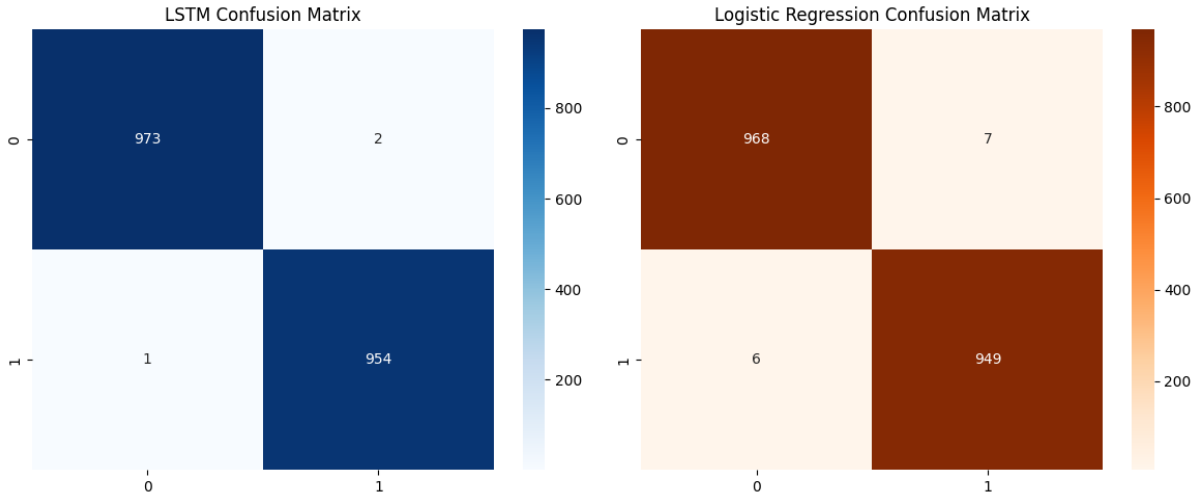

Figure 2: Confusion Matrix for LSTM model and Logistic regression model

Metric	LSTM	Logistic Regression	Better Performer
True Positives (Spam)	954	949	LSTM
True Negatives (Ham)	973	968	LSTM
False Positives (Ham → Spam)	2	7	LSTM
False Negatives (Spam → Ham)	1	6	LSTM

A confusion matrix will be helpful to understand the accuracy of a model by showing both correct and wrong predictions. For spam filtering, an attempt can be made to minimize two aspects: marking an existing message as spam (false positive) and not marking genuine spam (false negative).

The LSTM model was better with fewer mistakes. This is because it is aware of word order and word meaning and therefore excels when handling word-based tasks like spam identification.

Logistic Regression did more mistakes, mainly because it treats words individually and not the order of words. Even though it is fast and simple, it is not as accurate in picking up on subtle spam patterns.

That is, LSTM is better in accuracy, but Logistic Regression is better in terms of speed and simplicity.

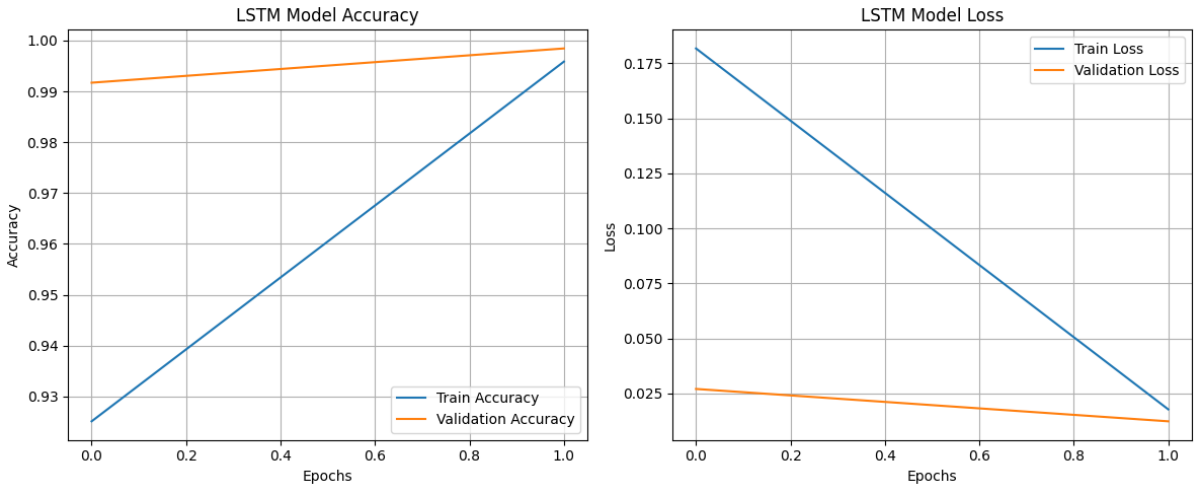

Figure 4: Comparison of both models of Accuracy and Loss

The LSTM model was performing extremely well in training. It was 92.5% initially (epoch 0) and reached 99.5% towards the end of epoch 1. The validation accuracy was also excellent at 99.2% and rose slightly to 99.7%. This indicates that the model is learning and not overfitting. Also, training loss began at 0.180 and dropped quite dramatically to 0.015, whereas validation loss was stable, dropping from 0.025 to 0.015. Overall, the model learned very quickly in terms

of the data pattern and provided accurate and consistent results for both the training and the validation sets.

VI COMPARATIVE ANALYSIS

The contrast between Logistic Regression and LSTM highlights the unique strengths and weaknesses of each model when used in the case of spam detection.The LSTM algorithm, being a deep learning model itself, is optimally suited for learning the contextual and sequential patterns of SMS messages. It excels at capturing the subtleties in patterns of language and is extremely stable and accurate. Being bidirectional, it is able to capture from both the preceding and the following words within a sequence, and that greatly increases its ability to capture spam messages with varied phrasing and construction.And then there is Logistic Regression, a less complex and explainable machine learning model that performs well with TF-IDF features. Light and quick to deploy and train, it is great for real-time or use when not much computing capacity is to be had. It lacks the capability to observe word order and more context, however, so its accuracy in classifying higher-level spam emails can be compromised.

Summary:

LSTM is utilized where high accuracy is required and sufficient computational resources are available.Logistic Regression is utilized where speed in execution is required with less complex scenarios using low resource utilization and interpretability as primary concerns.Model choice must be from the particular application needs, making trade-offs between performance, resource availability, and interpretability.

VII CONCLUSION

The experiment shows how LSTM models are more accurate and robust compared to Logistic Regression, especially in environments where word-order and semantic understanding is needed. Nevertheless, Logistic Regression remains competitive in situations where computational efficiency and simplicity are important. It is the requirement of the use case, availability of resources, and running environment that should inform the choice to use either of them. LSTM is superior to Logistic Regression in terms of robustness and accuracy.Logistic Regression remains useful for less complex deployments.Choice is based on performance vs. complexity trade-off.

VII FUTURE SCOPE

There are several ways this project can be taken forward. Using more powerful architectures such as transformers (e.g., BERT), investigating model interpretability using XAI tools, and optimizing the models to execute on mobile or low-resource devices are some of the significant directions. As the pace of change continues in NLP, more advanced techniques can continue to improve the system's capability to identify advanced spam patterns.Utilization of pre-trained transformers such as BERT for enhanced accuracy.Real-time app usage on mobile devices or messaging platforms.Quantization and pruning of the mobile deployment model (compression).Incorporation in Explainable AI modules for explainability.

VIII REFERENCES

1. Sahami, M., Dumais, S., Heckerman, D., & Horvitz, E. (1998). *A Bayesian approach to filtering junk e-mail*. In Proceedings of the AAAI Workshop on Learning for Text Categorization.
2. Metsis, V., Androutsopoulos, I., & Paliouras, G. (2006). *Spam filtering with Naive Bayes – Which Naive Bayes?* In Proceedings of the Third Conference on Email and Anti-Spam (CEAS).
3. Almeida, T. A., Hidalgo, J. M. G., & Yamakami, A. (2011). *Contributions to the study of SMS spam filtering: new collection and results*. ACM Symposium on Document Engineering, 259–262.
4. Russell, S. J., & Norvig, P. (2021). *Artificial Intelligence: A Modern Approach* (4th ed.). Pearson Education.
5. Géron, A. (2019). *Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow* (2nd ed.). O'Reilly Media.
6. Rennie, J. D. M., Shih, L., Teevan, J., & Karger, D. R. (2003). *Tackling the poor assumptions of naive bayes text classifiers*. In Proceedings of the 20th International Conference on Machine Learning (ICML-03), 616–623.
7. Delany, S. J., Buckley, M., & Greene, D. (2005). *SMS spam filtering: Methods and data*. Expert Systems with Applications, 39(10), 9899–9908.
8. Scikit-learn Developers. (n.d.). *Naive Bayes — scikit-learn documentation*. Retrieved from https://scikit-learn.org/stable/modules/naive_bayes.html
9. TensorFlow. (n.d.). *Text classification with an RNN*. Retrieved from https://www.tensorflow.org/text/tutorials/text_classification_rnn
10. Kaggle. (n.d.). *SMS Spam Collection Dataset*. Retrieved from https://www.kaggle.com/datasets/uciml/sms-spam-collection-dataset