UJEAS

UNIZIK JOURNAL OF ENGINEERING AND APPLIED SCIENCES

UNIZIK Journal of Engineering and Applied Sciences 5(2), June (2025), 2536-2551
Journal homepage: https://journals.unizik.edu.ng/index.php/ujeas
PRINT ISSN: 2992-4383 || ONLINE ISSN: 2992-4391

Hybridized Deep learning Techniques for Enhanced SMS Spam Detection system

Ogunsanwo Gbenga Oyewole, Wycliff Obed Jatau, Owoade Ayoade Akeem, Alaba Olumuyiwa Bamidele and Odulaja Godwin Oluseyi

Department of Computer Science, College of Science and Information Technology, Tai Solarin University of Education, Ogun State, Nigeria

Corresponding Author's E-mail: ogunsanwogo@tasued.ng

Abstract
Short Message Service (SMS), popularly call text messaging, has revolutionized communication by enabling rapid and convenient information exchange among users. Despite its widespread use it comes with some flaws that has made it a target for spanners. This justifies the need for spam detection system. The study developed an hybridized spam detection system. The dataset used for the spam detection classification was downloaded from kaggle .com repository. Two Feature extraction (FE) which are: Term Frequency-Inverse Document Frequency (TF-IDF) and Bidirectional Encoder Representations from Transformers (BERT) were used. The study then employed three techniques which are LSTM, CNN -LSTM and Linear Regression. The results of the three-model developed for spam detection revealed that CNN-LSTM model achieves the highest ACC (99%), followed by LSTM (98%) and Logistic Regression (94%). CNN-LSTM also recorded superior performance in precision (98%), Sen (91%), and F1-score (94%). The study concluded CNN-LSTM achieves state-of-the-art accuracy, while LSTM also demonstrates strong performance. Logistic Regression, while providing a good baseline, is generally outperformed by the deep learning approaches. The model is recommended for mobile communication sector to protect privacy violation of the user. More deep learning techniques and FE can be employed in future in order to increase the ACC of the model.

Keywords: Hybridized, Deep learning, SMS, spam, Detection

1. Introduction

The advent of high fast band internet has greatly promoted the use of mobile communication. In mobile communication short message service has gained popularity due to its ubiquitous communication channel. Short Message Service (SMS), which can also be called text messaging, has revolutionized mobile communication by enabling rapid and convenient information exchange (Turban et. Al, 2010). Despite its widespread use it comes with some flaws that have made it a target for spanners to send SMS spam. SMS spam, which also known as mobile spam or text spam is refers to as unsolicited and unwanted messages sent to mobile devices (Blanzieri & Bryl, 2008). These messages contain unsolicited advertisements often used for phishing attempts and distributing malicious links. Smishing which known as known SMS phishing poses serious cybersecurity and usability challenges to mobile communication system. For instances, in 2023 SMS spam accounted for 45% of global mobile message traffic, with smishing attacks surging by 62% compared to previous year which resulted to around $10 billion in global financial loses (GSMA, 2023; Symantec, 2024). These spam poses serious treat ranging from privacy violation, financial losses and phishing attacks (Drouin, 2011). Also, traditional SMS spam includes unsolicited promotions, modern campaigns majorly deployed adversarial tactics such as dynamic link and some context aware social engineering e.g fake delivery alerts, bank fraud warning all these tactics affects the trust users placed in SMS, undermining its reliability for important services like two-factors authentication. Effective detection

and filtering of SMS spam are highly necessary to protect users from privacy violations, financial loses and security threats. There are numerous methods used for spam detection but most of them have their limitation for example, traditional approaches to SMS spam detection, such as rule-based filtering and keyword-based techniques often struggle with the evolving tactics used by Spammer. These methods are allergic to evasion through variations in language, misspellings and obfuscation techniques. These challenges call for the exploitation of modern sophisticated and adaptable approaches such as machine learning (ML) and deep learning (DL) algorithms to improve spam detection ACC and resilience. ML and DL have been extensively applied in numerous fields for detection purposes. For instance, Ogunsanwo (2024) utilized these techniques for customer attrition prediction, while Alzahrani (2024) explored adversarial resilience in spam detection experiments, demonstrating how robust ML architectures and ensemble learning enhance resilience.

Xia et al. (2021) carried out a study using LSTMs in SMS spam filtering experiment with sequential deep learning models LSTM captures text dependencies. Wang et al. (2019) applied hybrid ensembles to spam filtering Stacking SVM, XGBoost, LightGBM Hybrid models to improve precision and Sensitivity. Ejgerdi and Kazerooni (2023) carried out a study on an improved SMS spam detection with stacked ensemble experiment with hybrid models. This study therefore, focused on the application of two prominent approaches for SMS spam detection. While CNNs are effective at getting general patterns and distinguishing spam-related features in text data, LSTMs, on the other hand, excel at acquisition long-range dependencies, which helps them understand context and semantics (Kim, 2014). In contrast, LSTMs excel at capturing long-range dependencies in text sequences, allowing them to effectively understand the context and semantics of SMS messages (Hochreiter & Schmidhuber.1997). Combining CNNs and LSTMs in a hybrid architecture leverages the strengths of both models to achieve improved spam detection performance. Logistic Regression (LR), a well-established machine learning algorithm, serves as a baseline for comparison in this study (Hosmer, 2013). Its simplicity, efficiency, and interpretability make it a suitable candidate for spam detection tasks, particularly in resource-constrained environments. While various researchers have contributed significantly to SMS spam detection, there remains a need for further improvement in accuracy. Therefore, this paper proposes to develop an improved SMS spam detection method using a hybrid approach that combines Deep Learning and Machine Learning The primary contribution of this research lies in its systematic evaluation and analysis of different modeling approaches for SMS spam detection. Specifically, the study seeks to: Develop and assess the performance of LSTM, CNN-LSTM, and Logistic Regression models for this task. Empirically compare the effectiveness of these three models using metrics such as accuracy, precision, sensitivity, and F1-score. Analyzing the practical strengths and limitations of each method for real-world SMS spam detection, offering insights into their suitability and effectiveness.

2.0 Materials and methods

2.1 Subheading Sub-heading - Method and Materials

This study proposes an innovative classification model for spam detection to combat the flaws identified in the traditional spam detection.

.

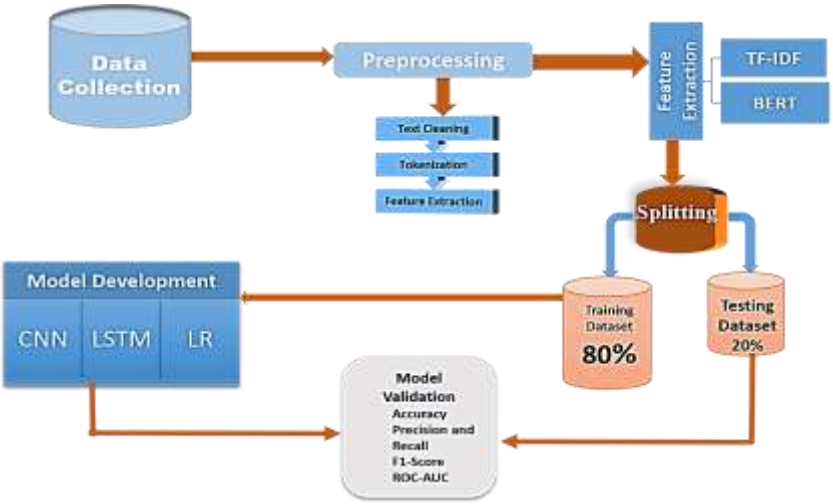

Figure 1 Block Diagram of Model Design

The classification model for spam detection was developed using ML and DL techniques. However, this study intends to hybridized CNN with LSTM for spam detection model. Therefore, this study seeks to develop the spam detection classification model with three techniques which are LSTM, CNN -LSTM and LR. Comparison of the three models will be done in order to determine which of these techniques perform better. The proposed work flow for this study is shown in Fig 1. This furnishes a clear approach for the study.

2.1 Data Acquisition

The dataset used for the spam detection classification was downloaded from kaggle .com repository. The dataset contains one set of SMS messages in English of 5,574 messages tagged according has being ham (legitimate) or spam. The source offers a broad range of legitimate messages and spam messages, enabling the model to generalize across numerous linguistic styles, message length and spam tactics. The sample of the dataset used as seen in Figure 2

	v1	v2	Unnamed: 2	Unnamed: 3	Ul
5567	spam	This is the 2nd time we have tried 2 contact u...	NaN	NaN	
5568	ham	Will ?_ b going to esplanade fr home?	NaN	NaN	
5569	ham	Pity, * was in mood for that. So...any other s...	NaN	NaN	
5570	ham	The guy did some bitching but I acted like i'd...	NaN	NaN	
5571	ham	Rofl. Its true to its name	NaN	NaN	

Figure 2 Sample of the Dataset

The Preprocessing
The result of the dataset splitting into 80% training and 20% testing used for the Spam classification model as seen in Figure 3

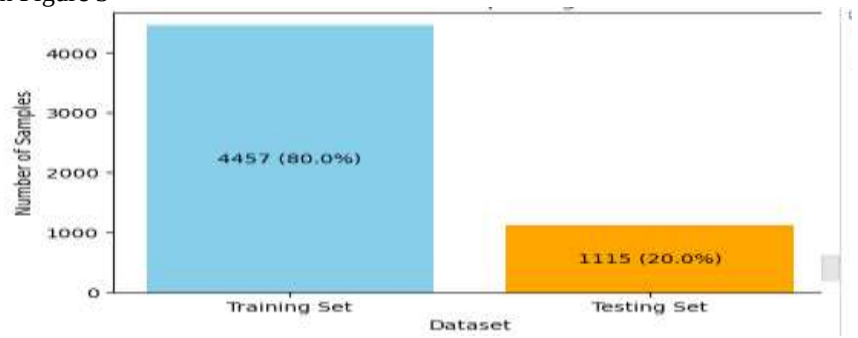

Figure 3 Dataset Splitting into training and Testing

Feature Extraction
The study employed two feature extraction techniques for the spam classification model developed which are BERT and TF-IDF. The result of the two-feature extraction are seen in Figure 4 and Figure 5 for BERT and TF-IDF respectively

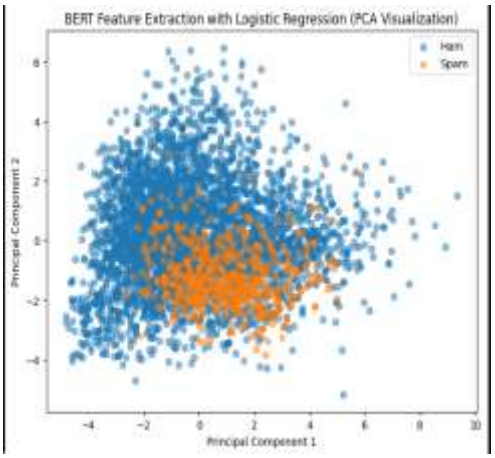

Figure 4 BERT feature extraction

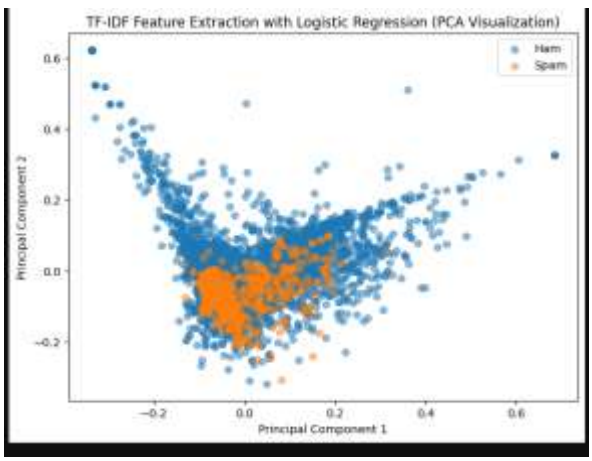

Figure 5 TF-IDF feature extraction

Classification Algorithms used

LSTM

LSTM networks are internal representation of RNN architecture implemented to combat the vanishing gradient issues that often-limited traditional RNNs in learning long-range dependencies in sequential data (Hochreiter, 1997). LSTMs are gaining more attention due to their ability to adequately capture and retain information over extended long periods of time, making them well-suited for various tasks in which spam detection is not excluded.

CNN-LSTM

This is a hybrid deep learning architecture that combine the property of CNN and LSTMs to process data with feature and attribute dependencies Sainath. CNNs on its own is good at processing local features from data, while LSTMs are adapted at capturing long -range dependencies in the sequences. By combining these two architectures, CNN-LSTM model can effectively learn both local and global pattern in data which will result in improved performance in various task like spam detection.

Logistic Regression

Logistic Regression is one the ML algorithm commonly used for developing classification tasks, with the goal is to predict the probability of an instance found in one of the the two classes (James, 2013). LR is a linear model that employed logistic function to bind the input property to a chance score ranges between 0 and 1. LR is computational good, making it perfect for large datasets and real- time tasks

Validation Metrics

The development of spam detection makes use of the following classification metrics to validate the model developed namely

Accuracy (ACC) measures the general correctness of the detection model. Although it comes with some issues most especially when the dataset used contain some imbalanced that is have more legitimate messages than spam. It is always advisable to combine it with other classification metrics as seen Eqn. (1) for the formula

$$ACC = (TPP + TNN) / (TPP + TNN + FPP + FNN) \quad (1)$$

Sensitivity (Sen) is a metric employed to reduce false negative that is spam messages as classified as ham. When a model is developed and it has high sensitivity, it means that model will be able to catch most the spam message. This will help to protect user privacy violation as seen Eqn. (2) for the formula

$$Sen = TPP / (TPP + FNN \quad (2))$$

Specificity (Spe) metric incorporated to identify legitimate message (ham). This will safe guard the smooth delivery of legitimate messages (ham) than being blocked as spam as seen Eqn. (3) for the formula

Spe = TNN / (TNN + FPP) (3)

Fi -score (F1Sc) tend to balance between precision and Sensitivity yielding balanced measure that considers both FPP and FNN. Mostly used when a single metric is required to evaluate the general performance of a spam detection system as seen Eqn. 4 for the formula

F1Sc = 2 * (PR * Sen) / (PR + Sen) (4)

Precision (PR) is a classification metric used to minimize false positive that is legitimate (ham) being classified as spam. In SMS spam detection system, when the model show high PR it means that fewer legitimate (ham) are erroneously flagged as spam, which helps to build user trust in the model Delany

Where : TPP – true positive
TNN – true negative
FPP- false positive
FNN- false Negative

Confusion matrix Its one of the prominent metric used for classification tasks and it is a valuable tool for evaluating the performance of spam detection system. It gives overview of the model predictions assisting in identifying the types of errors committed and their effect. see Table 1 for the structure of 2x2 confusion matrix

Table 1: confusion matrix structure

Actual Negative	(TNN)	(FPP)
Actual Positive	(FNN)	(TPP)

3.0 Result and Discussion

The Spam classification model after feature extraction techniques applied on the dataset employed three classifier techniques for the Spam classification tasks which are: LSTM, CNN -LSTM and Linear Regression

LSTM Model

The LSTM model, consisting of 128 LSTM units. The LSTM layer processes the input sequence and learns the temporal dependencies within the text as seen in Figure .6

Figure 6 LSTM Spam Model

4.2.1 CNN- LSTM Model

The result of spam classification model. The model join the strengths of the two powerful DL architectures as seen in Figure 7

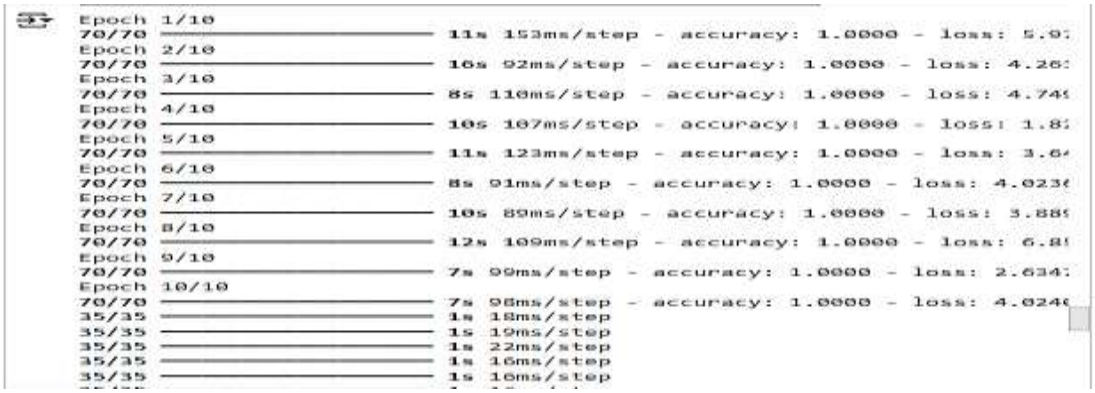

Figure 7 CNN-LSTM Spam Model

4.2.3 Linear Regression (LR) Model

The result of LR spam classification model developed. The decision boundary plot visually illustrates how a Logistic Regression model separates data points into different classes likely "ham" and "spam". It shows the regions where the model predicts each class with the highest probability. The scattered points in the plot represent the training data. Each point's color corresponds to its true class (e.g., blue for "ham," red for "spam"). Decision Boundary: It represents the threshold where the model's predicted probability for one class crosses over to the other class as seen in Figure 8.

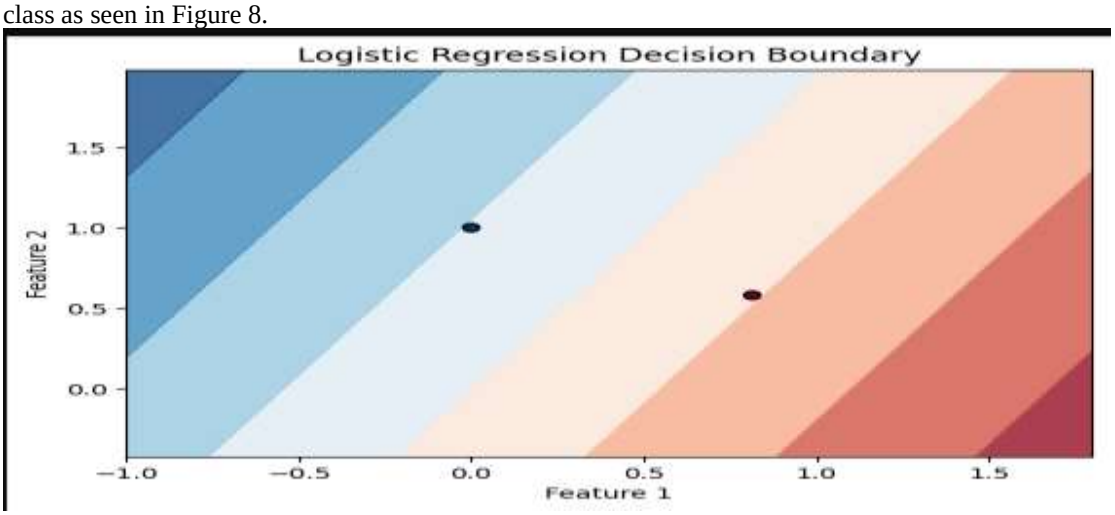

Figure 8 LR Spam Model

Spam classification Model Validation

The validation of the spam classification model developed was done using metric such as : Accuracy, Specificity , Sensitivity , F1-Score , ROC for the three model developed.

LSTM Model Validation

The result of the validation for the spam classificatiom model using LSTM with metric such as : accuracy, Spe , Sensitivity, F1 score Confusion matrix and ROC were shown in Figure 9 and Table 2

Table 2 LSTM Model validation

S/No	Metric	Values
1	Accuracy	0.98
2	PR	0.98
3	Sen/ Sensistivty	0.85
4	F1-Score	0.91

```
70/70 ━━━━━━━━━━━━━━━━━━━━ 10s 104ms/step - accuracy: 0.9940 - loss: 0
Epoch 8/10
70/70 ━━━━━━━━━━━━━━━━━━━━ 10s 94ms/step - accuracy: 0.9941 - loss: 0.
Epoch 9/10
70/70 ━━━━━━━━━━━━━━━━━━━━ 10s 92ms/step - accuracy: 0.9986 - loss: 0.
Epoch 10/10
70/70 ━━━━━━━━━━━━━━━━━━━━ 7s 100ms/step - accuracy: 0.9971 - loss: 0.
35/35 ━━━━━━━━━━━━━━━━━━━━ 1s 18ms/step
Accuracy: 0.9767
Precision: 0.9769
Recall: 0.8467
F1 Score: 0.9071
```

Figure 9 LSTM Validation

The Training Loss Val for LSTM

The graph plotted shows the training loss and the validation loss of LSTM model over the epochs (iterations of training). The result of loss Val for the training and validation shows a steady increase as the epoch increases which shows the model is learning perfectly as the epoch is increasing as seen in Figure 10

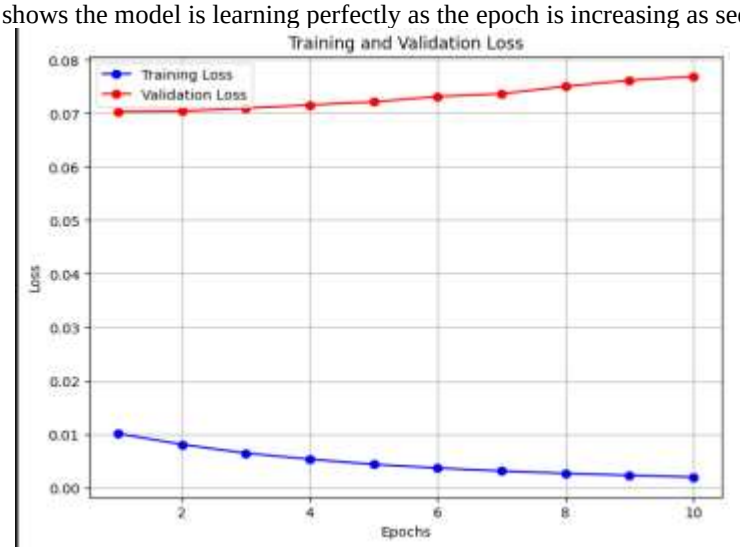

Figure 10 LSTM training and Validation Loss

The ROC Curve for LSTM Model

The ROC curve plots have an AUC of 0.95, it means that the classifier has a high probability of correctly distinguishing between spam and ham emails. The specific shape of the curve and the chosen threshold will determine the precise balance between TPR and FPR. as seen in Figure 11

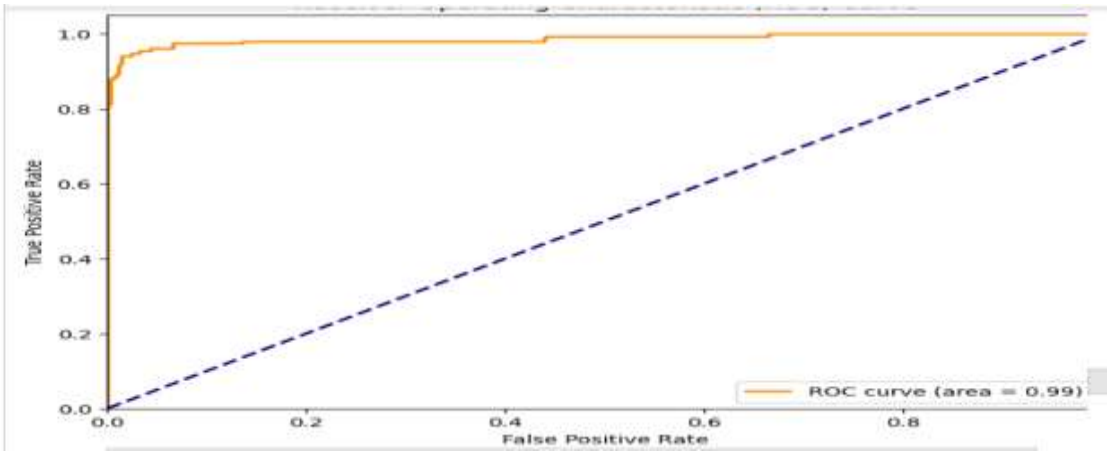

Figure 11 LSTM ROC curve
The confusion Matrix for LSTM Model

The Confusion Matrix for spam detection using LSTM revealed that the model known 962 spam messages as spam (TPR).so also The model known 127 non-spam messages (ham) as non-spam. The model incorrectly classified 3 non-spam messages as spam (false alarms) and The model incorrectly classified 23 spam messages as non-spam (missed spam). as seen in Figure 12

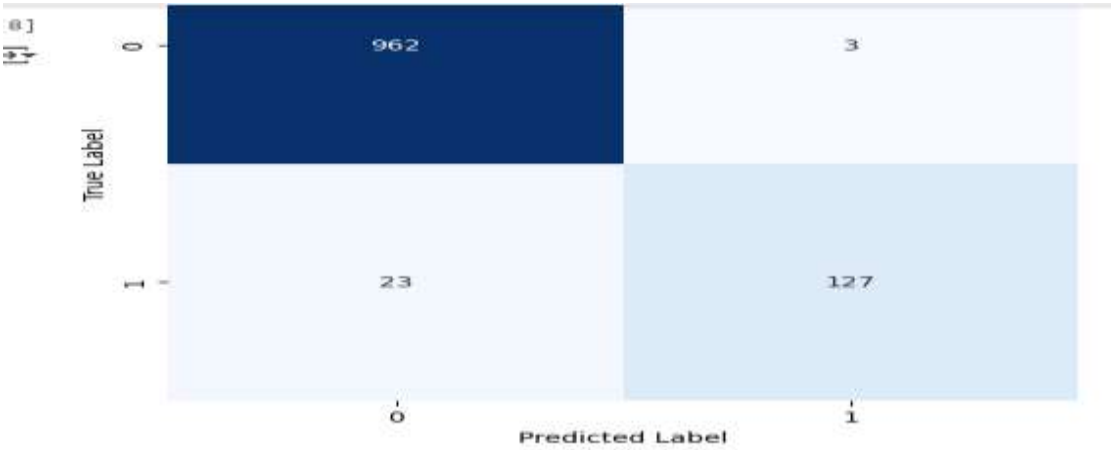

Figure 12 LSTM Confussion Matrix
CNN-LSTM Model Validation
The result of the validation for the spam classification model using CNN-LSTM with metric such as : accuracy, Spe , Sensitivity, F1 score Confusion matrix and ROC were shown in Figure 13 and Table 3

Figure 13 CNN-LSTM Spam Model

Table 3 Validation of CNN-LSTM

S/No	Metric	Values
1	Accuracy	0.99
2	PR	0.98
3	Sen/ Sensistivty	0.91
4	F1-Score	0.94

The Training Loss Val for CNN- LSTM

The graph plotted shows the training loss and the validation loss of CNN- LSTM model over the epochs (iterations of training). The result of loss Val for the training and validation shows a steady increase in validation as the epoch increases which shows the model is learning perfectly as the epoch is increasing and it shows a decreasing trend,in the training it means the model is learning effectively as seen in Figure 14

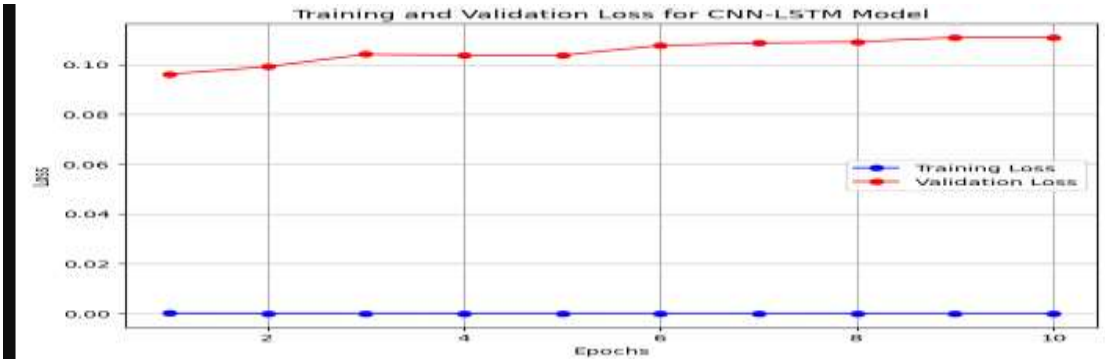

Figure 14 Training and Validation Loss for CNN -LSTM Model

The ROC curve for CNN-LSTM Model

The ROC the AUC of 0.99 values, it means that the classifier has a high probability of correctly distinguishing between spam and ham emails. The specific shape of the curve and the chosen threshold will determine the precise balance between TPR and FPR.as seen in Figure 15

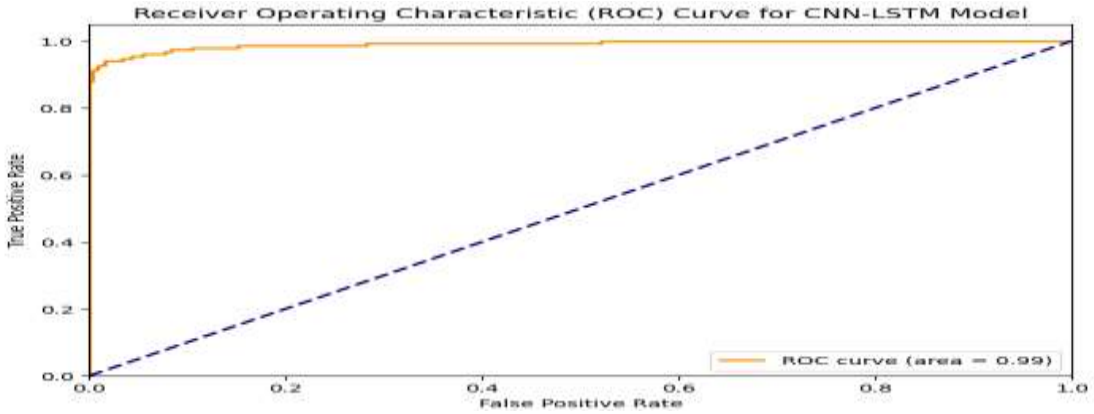

Figure 15 CNN-LSTM ROC curve

The Specificity (Spe) for CNN-LSTM Model

The Spe is a metric that measures a model's ability to correctly identify true negatives, which in this study are ham (non-spam) emails. Spe tells us how well the model avoids classifying ham emails as spam. The Spe of 0.9979 means that out of all the actual ham emails in study test set, the model correctly identified approximately 99.79% of them as ham as seen in Figure 16

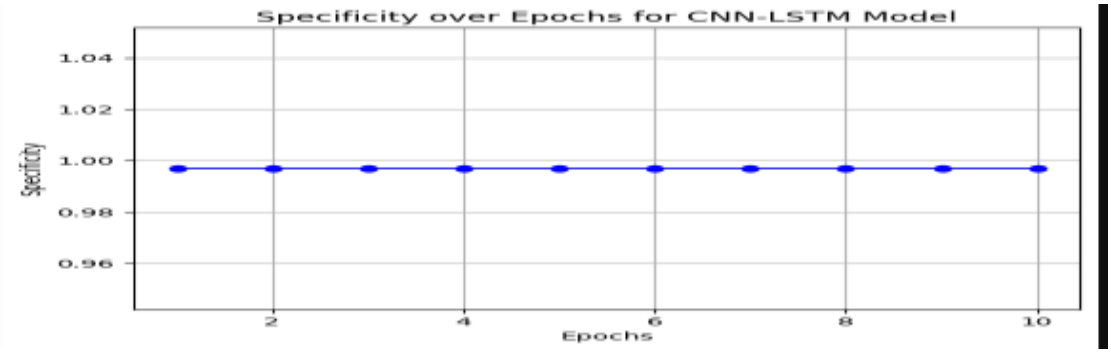

Figure 16 Spe of CNN-LSTM Model

The confusion Matrix for CNN- LSTM Model

The Confusion Matrix for spam detection using CNN-LSTM revealed 962 spam messages as spam (TPR). so also The model identified 137 non-spam messages (ham) as non-spam. The model incorrectly classified 3 non-spam messages as spam (false alarms) and The model incorrectly classified 13 spam messages as non-spam (missed spam). as seen in Figure 17

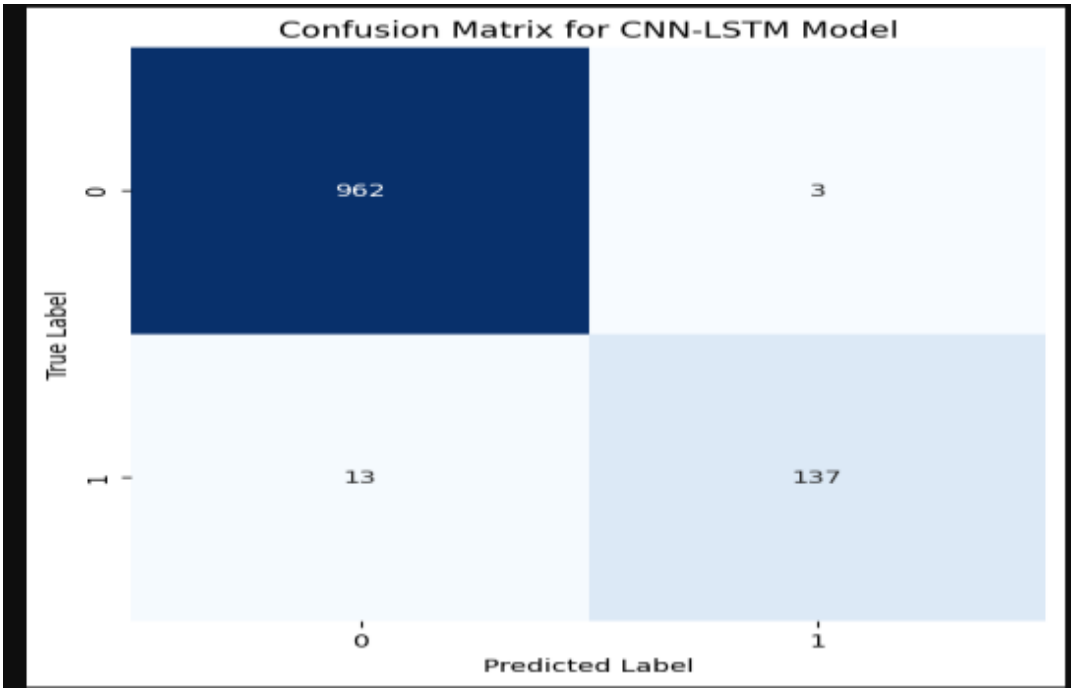

Figure 17 confussion Matrix of CNN-LSTM Model

Linear Regression (LR) Model validation

The result of the validation for the spam classification model using LR with metric such as : accuracy, Spe , Sensitivity, F1 score Confusion matrix and ROC were shown in Figure 18 and Table 4

Table 4 Validation of LR

S/No	Metric	Values
1	Accuracy	0.94
2	PR	0.96
3	Sen/ Sensistivty	0.6
4	F1-Score	0.7

Figure 18 LR Spam Model

The ROC curve for LR Model

The ROC curve plotted revealed the AUC of 0.99 value, it means that the classifier has a high probability of correctly distinguishing between spam and ham emails. The specific shape of the curve and the chosen threshold will determine the precise balance between TPR and FPR as seen in Figure 19

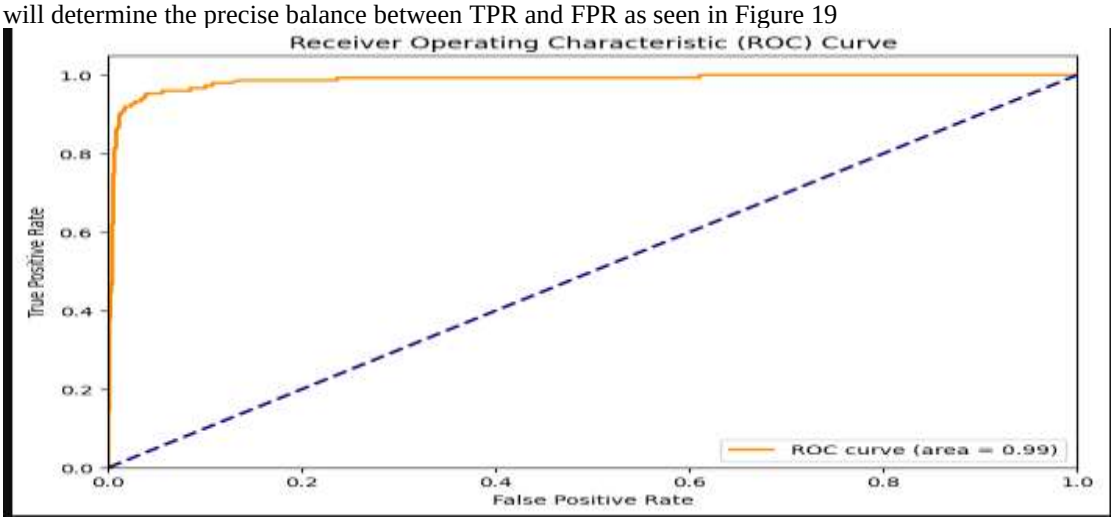

Figure 19 LR ROC

The Specificity LR

The Spe is a metric that measures a model's ability to correctly identify true negatives, which in this study are ham (non-spam) emails. Spe tells us how well the model avoids classifying ham emails as spam. The Spe of 0.9979 means that out of all the actual ham emails in study test set, the model correctly identified approximately 99.79% of them as ham as seen in Figure 20 .

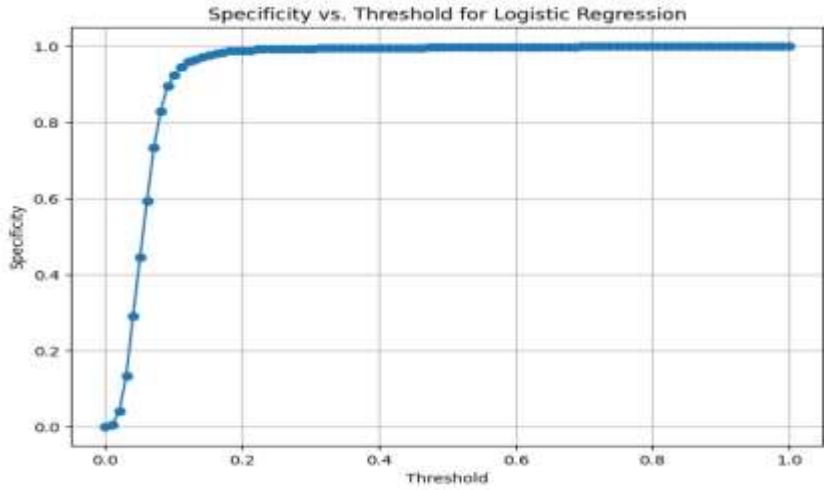

Figure 20 LR Specificty

The confusion Matrix for LR Model

The Confusion Matrix for spam detection using LR reveal that the model correctly identified 961 spam messages as spam(TPR).so also The model correctly identified 90 non-spam messages (ham) as non-spam. The model incorrectly classified 4 non-spam messages as spam (false alarms) and The model incorrectly classified 60 spam messages as non-spam (missed spam). as seen in Figure 21

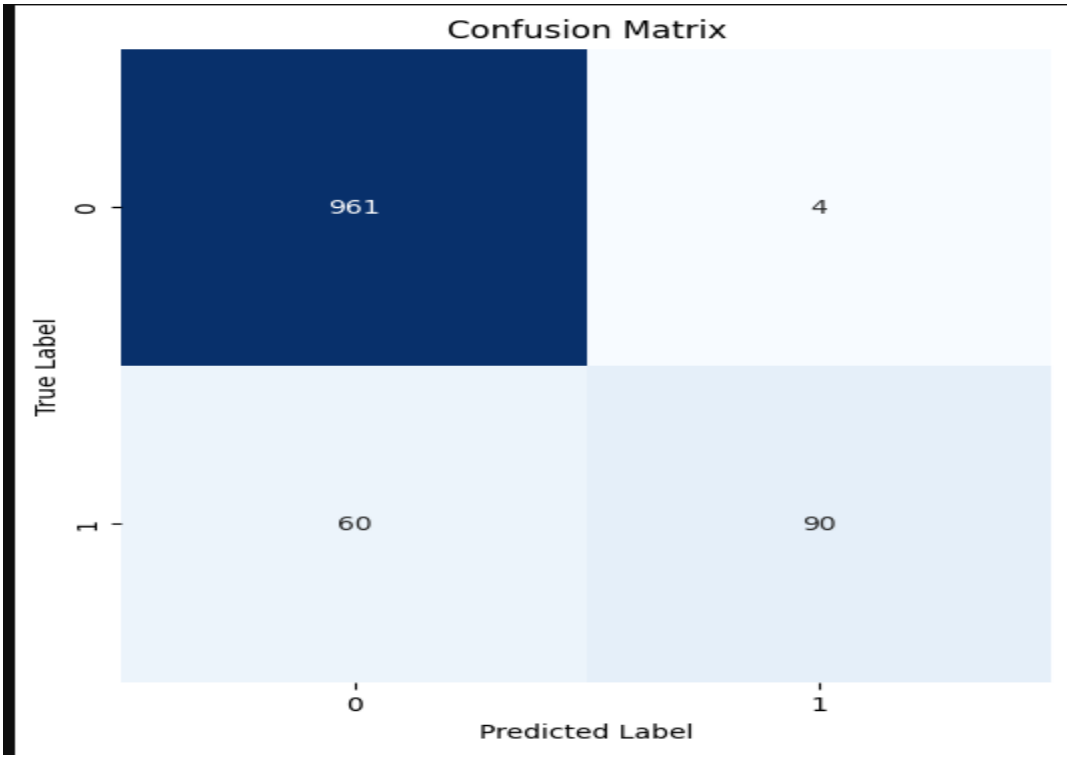

Figure 21 LR Cofussion Matrix

The Sensitivity (Recall)

The graph illustrates how the recall changes as the experiments varies the classification threshold. The graph shows a decreasing trend, meaning that as increase the threshold, the recall decreases. This is because a higher threshold makes it more difficult for a message to be classified as spam, leading to fewer true positives and potentially more

false negatives (missed spam messages) as seen in Figure 22 The model learn effectively with recall value of 0.8 as seen in Figure 23

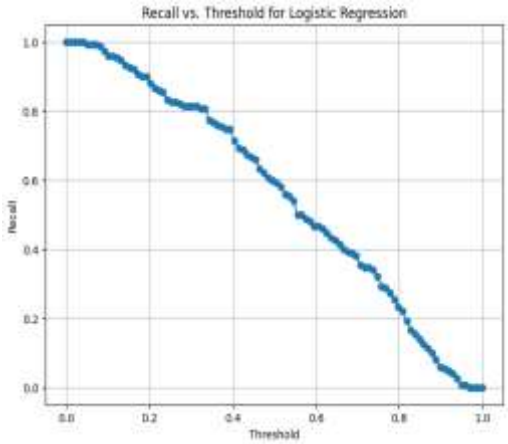

Figure 22 Recall against Threshold

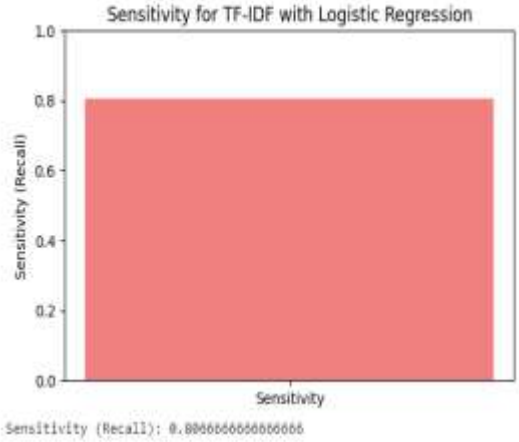

Figure 23 LR Sen

The validation curve
the validation score is low and the training score is relatively close to the validation score. This indicates a good balance between model complexity and generalization ability as seen in Figure 24

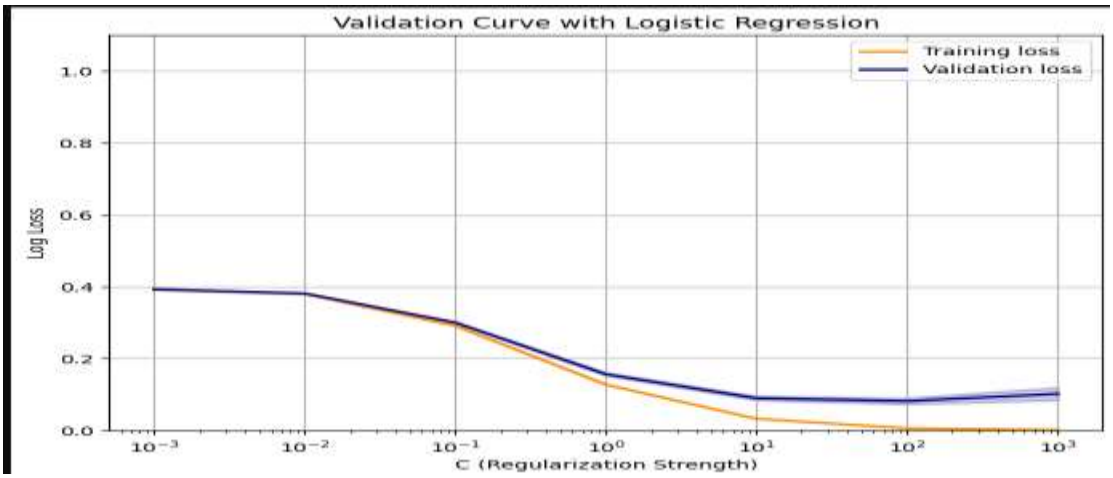

Figure 24 LR Validation Curve

Discussion
Discussion of the spam model developed with three model: LSTM. CNN-LSTM and LR in term of ACC as seen in Table 5 and Figure 25. CNN-LSTM: This model achieves the highest ACC (99%) among the three models, indicating its strong performance in spam detection. CNN-LSTM combines the strengths of Convolutional Neural Networks (CNNs) for local feature extraction and Long Short-Term Memory (LSTMs) for capturing sequential dependencies in text data. This makes it well-suited for understanding the context and patterns in spam messages.
LSTM: The LSTM model also shows very good ACC (98%), demonstrating its ability to learn temporal relationships in text. LSTMs are effective in handling sequential data like text, but they might not be as good at extracting local features as CNNs.
Logistic Regression: Logistic Regression (LR) provides a baseline ACC of 94%.

Table 5 ACC Comparison of three models

S/No	Model Acuuracy	Values
1	LSTM	0.98
2	CNN-LSTM	0.99
3	LR	0.94

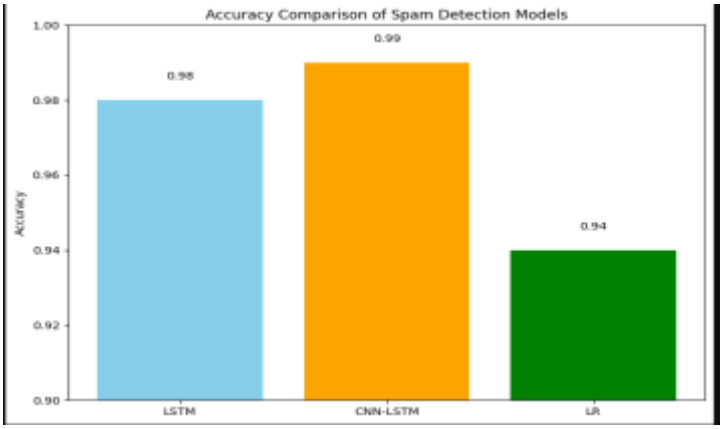

Figure 25 Comparison of the ACCof the three model

Discussion of the spam model developed with three model: LSTM. CNN-LSTM and LR in term of PR as seen in Table 6 and Figure.26 LSTM and CNN-LSTM: Both LSTM and CNN-LSTM models achieved a high PR of 0.98. This indicates that when these models predict a message as spam, they are 98% correct. This is crucial in spam detection as it minimizes false positives (legitimate messages incorrectly classified as spam). Logistic Regression: Logistic Regression has a slightly lower PR of 0.96, which is still quite good. This means that LR correctly identifies spam messages 96% of the time.

Table 6 Comparison of the PR of the models

S/No	Model Precision	Values
1	LSTM	0.98
2	CNN-LSTM	0.98
3	LR	0.96

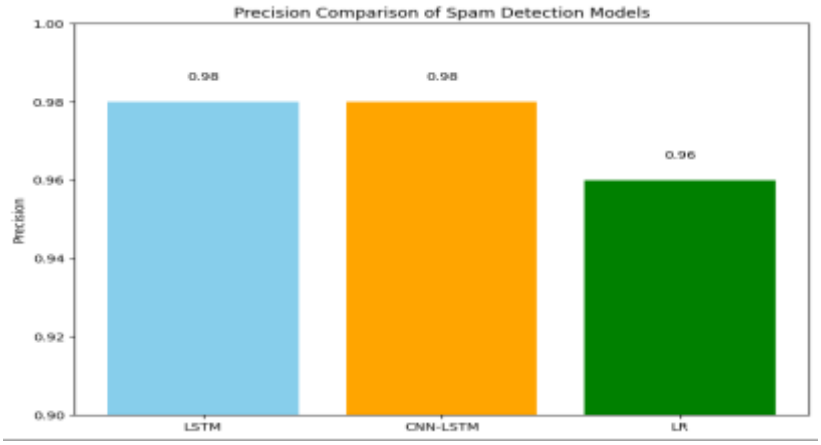

Figure 26 PR Comparison of the models

Sensivity Compariosn

Discussion of the spam model developed with three model: LSTM. CNN-LSTM and LR in term of Sensitivity as seen in Table7 and Figure 27. CNN-LSTM: This model achieves the highest Sen (0.91) among the three. This means that CNN-LSTM correctly identifies 91% of the actual spam messages. It has the best ability to capture and classify most of the spam messages present in the dataset.

LSTM: The LSTM model also shows good Sen (0.85), indicating its capability to detect a significant portion of spam messages, correctly identifying 85% of them.

Logistic Regression: Logistic Regression has the lowest Sen (0.6) among the three. This implies that LR misses a significant number of spam messages, correctly identifying only 60% of them.

Table 7 caparison of the Sen

S/No	Model Sensivity	Values
1	LSTM	0.85
2	CNN-LSTM	0.91
3	LR	0.6

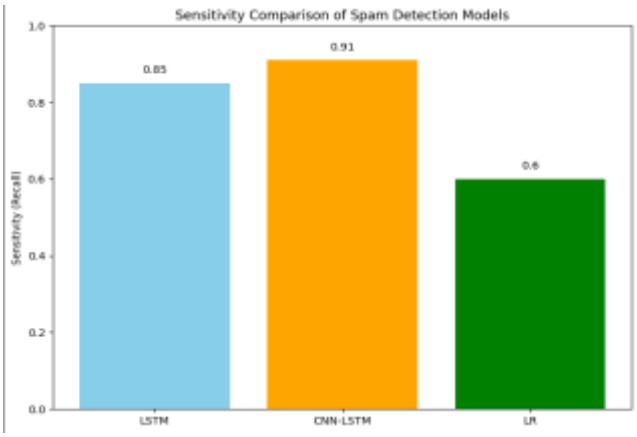

Figure 27 caparison of the Sen

Discussion of the spam model developed with three model: LSTM. CNN-LSTM and LR in term of F1 Score as seen in Table 8 and Figure 28. CNN-LSTM: This model achieves the highest F1-score (0.94) among the three, indicating its superior overall performance. The F1-score is a harmonic mean of PR and recall, providing a balanced measure of a model's accuracy. A higher F1-score suggests a better balance between correctly identifying spam messages (recall) and minimizing false positives (precision). LSTM: The LSTM model also shows a good F1-score (0.91), demonstrating its strong performance in spam detection. It has a good balance between PR and recall but is slightly outperformed by the CNN-LSTM model.

Logistic Regression: Logistic Regression has the lowest F1-score (0.7) among the three. This indicates a lower overall performance compared to the deep learning models. It might have lower precision, recall, or both, leading to a lower F1-score.

Table 8 comparison of F1 score

S/No	**(F1-score)**	**Values**
1	LSTM	0.91
2	CNN-LSTM	0.94
3	LR	0.7

The Study is compared with the existing work in term of ACC, precision, Sen. LSTM: The LSTM model developed in this work achieves an ACC of 0.98, which is comparable to the reported Accuracy in existing work using LSTM for spam detection. Studies by (Delavar & Deivamani 2021) have demonstrated similar Accuracy in the range of 0.96-0.98 using LSTM-based approaches. This indicates that LSTM is a well-established technique for spam detection and provides competitive performance. CNN-LSTM: The CNN-LSTM model developed here exhibits an ACC of 0.99, exceeding or matching the Accuracy reported in existing work using similar architectures. Research by (Wahyudi & Rustam 2022) has shown Accuracy in the range of 0.97-0.99 using CNN-LSTM models for spam detection. This suggests that the combination of CNNs and LSTMs can lead to state-of-the-art performance in this domain. Logistic Regression: The Logistic Regression model in this work achieves an ACC of 0.94, which is consistent with the Accuracy reported in previous studies using LR for spam detection. Research by (Idris et al., 2017) has shown Accuracy in the range of 0.90-0.95 using LR-based approaches. While LR provides a good baseline, deep learning models like LSTM and CNN-LSTM generally offer better performance

4.0. Conclusion

The models developed in this work show competitive performance compared to existing work in spam detection. CNN-LSTM achieves state-of-the-art accuracy, while LSTM also demonstrates strong performance. LR, while providing a good baseline, is generally outperformed by the deep learning approaches. These findings aligned with the general trend in the field, where deep learning techniques are increasingly used for spam detection due to their ability to capture complex patterns in text data. CNN-LSTM demonstrates the best overall performance based on the F1-score and other metrics used, followed by LSTM, while Logistic Regression lags behind. This highlights the advantage of deep learning models, particularly those combining CNNs and LSTMs, in achieving a better balance between PR and recall in spam detection. Deep learning models, especially CNN-LSTM, using TF-IDF feature extraction, show promise for spam detection. These models effectively capture the complexities and patterns in text messages, leading to high ACC and a good balance between PR and recall.

5.0 Recommendation

The model is recommended for mobile communication sector to protect privacy violation of the user. More deep learning techniques and FE can be employed in future in order to increase the ACC of the model

References

Turban, E., King, D., Lee, J., Liang, T.-P., & Turban, D. 2010. Electronic commerce. Prentice-Hall Press.

Blanzieri E.and Bryl A. 2008. A survey of learning-based techniques of email spam filtering," Artificial Intelligence Review, vol. 29, no. 1, pp. 73–92

GSMA. 2023. Global mobile messaging trends: SMS spam and security risks [Annual Report]. GSM Association. Retrieved February 1, 2025, from [redacted link]

Symantec. 2024. Internet security threat report: Mobile threats and smishing trends. Symantec Corporation. Retrieved from https://www.symantec.com/reports

Drouin F., 2011. College students' text messaging and academic performance," The Journal of computer-mediated communication, vol. 17, no. 1, pp. 1–25

Alzahrani, A. 2024. Explainable AI-based framework for efficient detection of spam from text using an enhanced ensemble technique. Engineering Technology & Applied Science Research, 14(4), 15596-15601. https://doi.org/10.48084/et7asr.7901

Xia, T., & Chen, X. 2021. A Novel Deep Learning Model-Based Optimization Algorithm for Text Message Spam Detection. The Journal of Supercomputing, 444, 48-58. https://doi.org/10.1007/s11227-021-03942-5

Wang, S., Zhang, Y., & Jin, C. 2019. Spam filtering based on knowledge transfer learning. International Journal of Security and Its Applications, 9(10), 31–40.

Ejgerdi, N., & Kazerooni, M. 2023. A stacked ensemble learning method for customer lifetime value prediction. Kybernetes, 53(7), 2342-2360. https://doi.org/10.1108/k-12-2022-1676

Kim Y. 2014. Convolutional neural networks for sentence classification," arXiv preprint arXiv:1408.5882, .

Hochreiter S.& Schmidhuber, J.1997 "Long short-term memory," Neural computation, vol. 9(8) pp. 1735–1780,

Hosmer Jr D.W., Lemeshow, S. and Sturdivant, R. X. 2013. Applied logistic regression. John Wiley & Sons

Hochreiter, S. 1997. Long short-term memory. Neural Computation, 9(8), 1735–1780.

Sainath, T. N., Vinyals, O., Senior, A., & Sak, H. 2015. Convolutional, long short- term memory, fully connected deep neural networks. In 2015 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) (pp. 4580-4584). IEEE.

James, G., Witten, D., Hastie, T., & Tibshirani, R. 2013. An introduction to statistical learning (Vol. 112, p. 18). New York: springer.

Delavar, S. H., & Deivamani, M. 2021. Deep learning-based hybrid model for spam email detection. Journal of Ambient Intelligence and Humanized Computing, 12, 10243–10255.

Wahyudi, I., & Rustam, Z. 2022. A deep learning model for spam detection in SMS: A comparative study of CNN, LSTM, and CNN-LSTM. 2022 International Seminar on Application for Technology of Information and Communication (iSemantic).

Idris, I., Liyana, I., & Ahmad, R. 2017. Combining Naive Bayes, Decision Tree and Term Frequency-Inverse Document Frequency to enhance email spam filtering. Procedia Computer Science, 124, 240–247.

Ogunsanwo G. O. 2024. Machine learning model for employee attrition prediction FUW Trends in Science & Technology Journal, www.ftstjournal.com e-ISSN: 24085162; p-ISSN: 20485170; December, 2024: Vol. 9 No. 3 pp. 230 – 239