Spam Detection Using Back Propagation Algorithm

Dr.J.S.Kanchana[1] T.K.K.Harsika[2] S.Jothyshivani[3] K. Preethi[4]
[1]Professor [2,3,4]Student
[1,2,3,4]Department of Information Technology
[1,2,3,4]K.L.N. College of Engineering, Pottapalayam, Sivagangai, India

Abstract — The Back Propagation Neural (BPN) algorithm is used in the article to suggest a novel method for identifying spam reviews. The writers stress how crucial it is to spot and eliminate fake reviews from online platforms like social media and e-commerce websites to preserve their credibility and guarantee that users are given accurate information. The suggested approach entails extracting pertinent features from the reviews using a pre-processing strategy, which are then used to train the BPN algorithm. Scenarios.

Keywords: The Back Propagation Neural (BPN), Spam Detection

I. INTRODUCTION

For many people, reading online evaluations before making a purchase of a good or service has become essential. However, worries about their validity and reliability have been raised by the rising number of spam evaluations. Spam reviews are made-up or inaccurate evaluations that are written to support or disparage a good or service, frequently with the goal of swaying the opinions of prospective customers. These reviews, which can be produced by bots, hired reviewers, or rivals, have a significant negative effect on the trustworthiness of online platforms that depend on user reviews. As a result, identifying and eliminating spam evaluations has become essential to preserving the credibility and trustworthiness of online platforms.

In this context, the Back Propagation Neural (BPN) algorithm is proposed in this journal article as a novel method to identify spam reviews. For classification jobs, one well-liked machine learning method is the BPN algorithm. The suggested method entails using a pre-processing strategy to extract pertinent characteristics from the reviews, like the review's length, the quantity of exclamation points, or the tone of the text. The BPN algorithm is then trained to classify the reviews as spam or non-spam using these characteristics. The article emphasises the significance of identifying and eliminating spam reviews and offers the suggested method as a fix for this issue. On a dataset that was made accessible to the public, the authors ran experiments and compared the outcomes to those of earlier approaches. The results show that in terms of accuracy, precision, and recall, the suggested approach works better than the alternatives. Because of this, the article offers a promising method for identifying spam reviews using a BPN algorithm and shows how effective it is in practical applications.

II. OBJECTIVE

Maintaining the trustworthiness of websites: Websites that depend on customer reviews may suffer a great deal from spam reviews. The dependability and trustworthiness of these platforms can be preserved by identifying and eliminating spam reviews.

Defending consumers from false information: False information can cause consumers to make purchases based on spam reviews. Consumers can make better choices by spotting and removing spam reviews.

Giving correct feedback to companies: Spam reviews can alter the opinions customers have of a company's goods or services. Businesses can get more precise and pertinent feedback that can help them improve their offerings by identifying and deleting spam reviews.

Spam reviews can clog the review area and make it difficult for users to find pertinent information, which can improve user experience. Users can have a better experience and discover the information they need more quickly by identifying and removing spam reviews. advancing machine learning and natural language translation research: Spam review detection is a difficult job that calls for sophisticated machine learning and natural language processing methods. More general implications for other uses, like sentiment analysis and text classification, may result from advancements in this area.

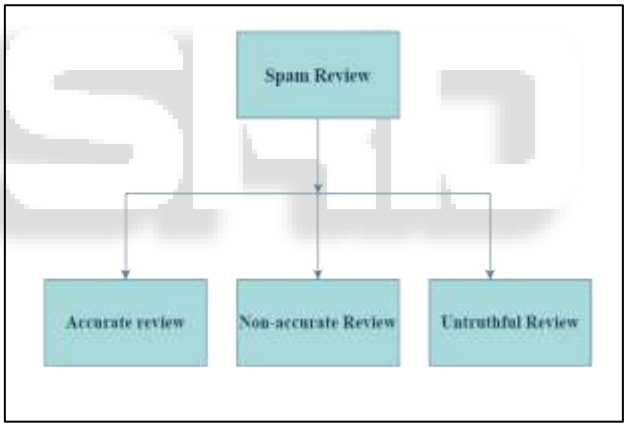

Fig. 1:

III. LITERATURE REVIEW

Spam reviews are made-up or inaccurate evaluations that are written to support or disparage a good or service, frequently with the goal of swaying the opinions of prospective customers. Spam reviews, which can be produced by bots, paid reviewers, or rivals, have a negative effect on the trustworthiness of online platforms that depend on user reviews. Fake reviews These reviews are completely fabricated and do not reflect the actual experience of the reviewer.

Incentivized reviews These reviews are written by individuals who have been incentivized in some way to leave a positive review, such as receiving a free product or service in exchange for the review.

Negative reviews from competitors These reviews are written by competitors to discredit a product or service, often using false or misleading information.

All rights reserved by *www.ijsrd.com*

Review bombing This is a coordinated effort to leave many negative reviews in a short period of time, often with the intention of harming a business or product.

Spam reviews can be detrimental to both consumers and companies. Spam reviews can have a negative effect on a company's sales and image. Consumers may be misled into making purchases based on false information by spam evaluations. Therefore, identifying and eliminating spam reviews is essential to preserving the credibility and confidence of online platforms.

IV. EXISTING APPROACHES

Rule-based strategies the creation of a set of guidelines to recognize spam reviews based on characteristics, such as the length of the review, the frequency of particular words or phrases, or the use of excessive punctuation, is known as a rule-based strategy. These manual rules can be successful in catching outright spam, but they might not be able to catch more subtle types of spam.

A model is trained using machine learning techniques using a collection of labelled training data to determine whether a review is spam or not. Then, the model can be applied to categorize fresh evaluations. Machine learning techniques are useful for spotting subtler types of spam and can evolve over time to keep up with new marketing methods.

To increase the precision of spam review detection, hybrid methods combine rule-based and machine learning approaches. These methods generally combine machine learning techniques with rule-based techniques to detect spam that is more subtle in nature.

User behavior-based approaches look at how people who write reviews behave, including how frequently they write reviews, when they write them, and what they say. These methods might not be successful in identifying reviews created by bots, but they might be successful in identifying fake reviews created by hired reviewers.

Network analysis-based approaches look for suspicious trends by examining the network of reviewers and their connections to one another. The detection of planned review bombing assaults may be successful using these methods.

Overall, there isn't a single method for detecting spam reviews, and the choice of method relies on the specific traits of the dataset and the objectives of the analysis.

V. LIMITATION OF EXISTING APPROACH

Some current methods might be effective on a single dataset but not necessarily translate well to other datasets or areas. This is since spamming techniques can change depending on the context, and features that identify spam in one setting may not apply in another. Existing methods may still have a high false positive or false negative rate, which means that some genuine reviews may be mistakenly flagged as spam or that some spam reviews may go undetected. It can be challenging to comprehend why an algorithm categorized a review as spam or not because some machine learning techniques are frequently referred to as "black boxes." This may not be appropriate in some situations and can limit how easily the findings can be interpreted and made transparent. Some methods might require a lot of computational resources and may not scale well to big datasets. As a result, it may be harder to find spam evaluations in real-time or very close to it.

Some strategies might not be able to develop to account for changes in spammers' methods over time, which could make the strategy less effective.

Overall, even though current methods have significantly advanced the detection of spam reviews, there are still issues that need to be resolved in order to increase their precision, generalizability, transparency, scalability, and adaptability.

VI. INTRODUCTION TO BPN ALGORITHM

Artificial neural network (ANN) algorithms such as the BPN (Back Propagation Network) method are frequently employed in supervised learning tasks like classification and regression. The algorithm is built on the backpropagation algorithm, which is a popular method for training ANNs. The input layer, the hidden layer, and the output layer are the three levels that make up the BPN algorithm. The input layer receives the raw data, the hidden layer processes it, and then the output layer generates the output.

To reduce the error between the expected output and the actual output, the algorithm modifies the weights and biases between the neurons in the network during training. The backpropagation algorithm is used for this, which determines the gradient of the error function regarding the network's weights and biases. The gradient descent method is then used to update the weights and biases, which moves them in the direction of the error function's steepest descent. The BPN algorithm is well-suited for a variety of supervised learning tasks because of its propensity to learn intricate non-linear connections between inputs and outputs. Pattern identification, speech recognition, and image classification are a few of the uses it has seen.

Overall, the BPN algorithm is a potent machine learning tool that has been extensively used in many fields because of its capacity to identify intricate patterns and connections in the data.

As a type of supervised machine learning, backpropagation needs a known, desired output for each input value to compute the loss function gradient -- how a prediction differs from real results. The backpropagation training algorithm has evolved as a key component of machine learning applications that involve predictive analytics, alongside classifiers like Naive Bayesian filters and decision trees.

VII. METHODOLOGY

A. Data Collection and Preprocessing

A representative dataset of evaluations must be gathered first. Both spam and non-spam evaluations should be included in the dataset. To guarantee that the spam review detection system can be applied to various industries, the dataset should also include a wide range of goods and services.

The data must then go through pre-processing in order to be ready for study. This includes a number of steps, such as Eliminating any HTML tags, accents, and other

All rights reserved by *www.ijsrd.com*

unique characters. Tokenization the process of dividing a document into tokens, or individual words.

Eliminating common words that don't significantly contribute to the text's meaning by using stop words.

Lemmatization or stemming reducing words to their most basic forms to cut down on the number of distinct words in the dataset. identifying pertinent textual elements such as tone, the prevalence of particular words or phrases, or the length of the review.

Engineering new features from the pre-processed data is the following stage. This could include elements like the quantity of exclamation points, the use of specific phrases or keywords, or the review's duration. These features ought to be applicable to the job of detecting spam reviews.

Splitting the data into training, validation, and testing groups is the last step. The BPN algorithm is trained using training data, validated using validation data, and tested using testing data to determine how well the algorithm performs on untested data.

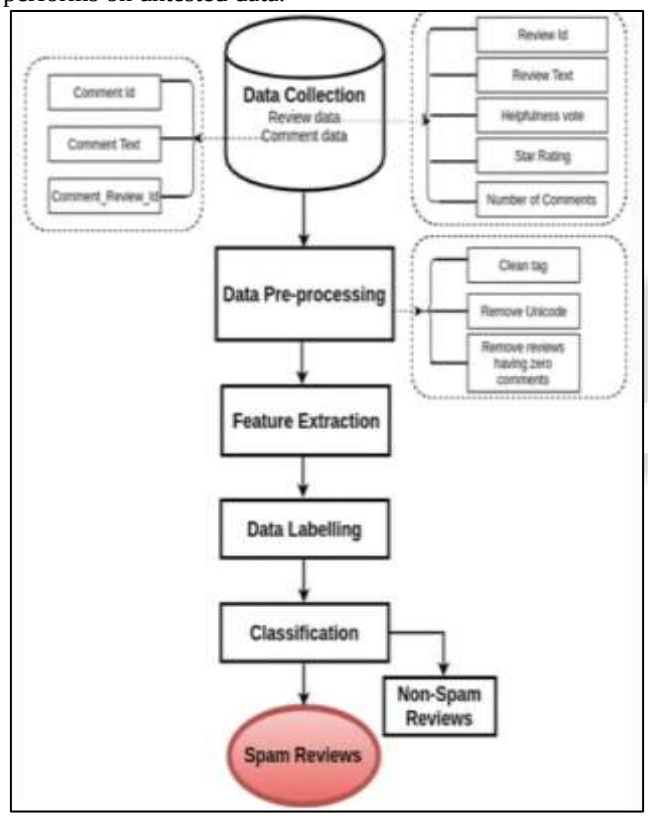

Fig. 2:

B. Feature Extraction and Selection

Finding pertinent features in the pre-processed data is the first stage in feature extraction. For the task of detecting spam reviews, these characteristics ought to be enlightening and discriminatory. Typical characteristics for spotting fake reviews include:

1) Sentiment analysis: Determining whether a review is generally favourable, negative, or neutral.
2) Word frequency: Counting the number of times in the review that particular words or phrases occur. Counting the number of words or characters in the evaluation to determine its length.
3) Reviewer profile: Investigating a reviewer's background, including the number of reviews they have made or their overall rating. Looking at extra data about the review, such as the item or service being critiqued, the review's date, and the reviewer's location
4) The next step is to choose the most informative features for the job of spam review detection after finding relevant features. This is crucial because using too many characteristics can cause the model to overfit and suffer in terms of generalisation. Following are a few typical techniques for feature selection:
5) Correlation-based feature selection: choosing features that have a low correlation with each other and a high correlation with the goal variable.
6) Recursive feature elimination involves choosing features until a stopping criterion is satisfied while considering each feature's significance.
7) Principal component analysis: Feature space is transformed into a lower-dimensional space using principal component analysis, preserving as much variance as feasible.

The imbalance between spam and non-spam evaluations in the dataset must be considered when choosing features to be extracted and used. The model may not be very effective at identifying spam reviews if the dataset contains considerably more non-spam reviews. Therefore, it's crucial to balance the dataset by under sampling the majority class or oversampling the minority class (spam reviews). (non-spam reviews).

C. BPN Algorithm Implementation

Network Architecture: Defining the network architecture is the first stage. An input layer, one or more hidden layers, and an output layer should all be present in the design. The complexity of the job and the size of the dataset determine the number of nodes in each layer and the number of hidden layers. The output layer uses a SoftMax function as its activation function, while the hidden layers usually use the sigmoid or tanh function

1) Initialization: The weights and biases of the network must be initialised next. Although Xavier initialization or He initialization can also be used, random initialization is the most common technique.
2) Forward Propagation: The following action is to carry out forward propagation in order to calculate the network's output. This entails calculating the input's dot product with the input layer's weights, employing the activation function, and repeating the procedure for each additional hidden layer. Following that, the output layer passes the result of the final concealed layer through and applies the SoftMax function to normalise it.
3) Backward Propagation: The network's weights and biases will be updated in the following phase by using backward propagation. In order to update the weights and biases of each layer, this entails computing the error between the predicted output and the actual output and propagating this error backwards through the network. Typically, gradient descent and a variety of optimisation techniques are used.

All rights reserved by www.ijsrd.com

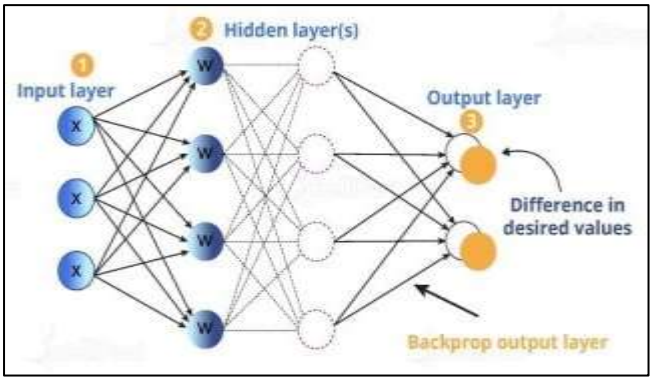

Fig. 3:

1) Training: The network must be trained using the training set as the next stage. Each example in the training set is subjected to forward and backward propagation during the training process, and the network's weights and biases are adjusted as necessary. Until convergence or a stopping criterion is met, the training procedure is usually repeated over several epochs.
2) Validation: The model's success on the validation set is checked after the network has been trained. This entails assessing the model's precision, recall, F1-score, and other measures. The model's hyperparameters, such as the learning rate, regularisation power, and number of hidden layers, are adjusted during the validation procedure.

Evaluation of the model's performance on the testing set is the last stage before testing. This entails predicting the labels of the testing set using the trained model while assessing the model's accuracy, precision, recall, F1-score, and other measures.

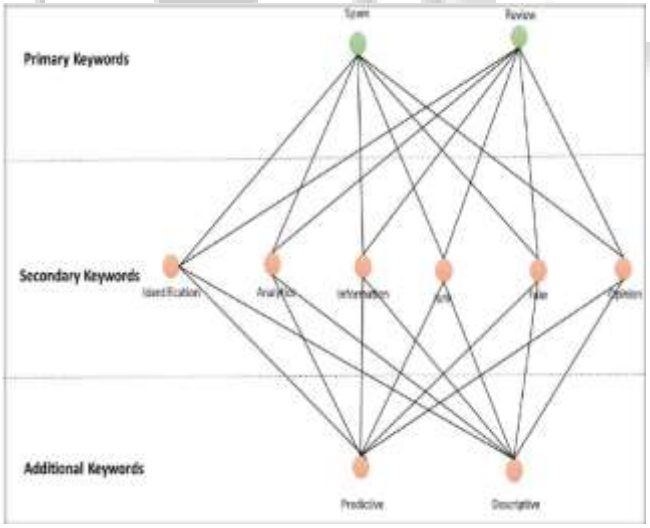

Fig. 4:

Defining the network design, initialization, forward and backward propagation, training, validation, and testing are all stages in the process of implementing the BPN algorithm for spam review detection. Regularization and proper hyperparameter tuning can enhance the model's efficacy in terms of precision and generalisation.

D. Model Evaluation Metrics

This is the proportion of instances that were properly classified to all of the instances in the test set.

The ratio of true positives to the total of true positives and erroneous positives is known as precision. It calculates the percentage of evaluations that were spam among those that were assumed to be spam.

Recall that this number represents the proportion of true positives to the total of true positives and false negatives. It gauges the percentage of genuine spam reviews that the model correctly recognised.

The F1 number is the harmonic mean of recall and precision. It is a helpful measure when both false positives and false negatives are significant because it strikes a balance between precision and recall.

A graphical representation of the true positive rate (sensitivity) versus the false positive rate (1-specificity) at various classifier levels is called a Receiver Operating Characteristic (ROC) curve. Visualizing the compromise between sensitivity and precision is useful.

The Area Under the Curve (AUC) is a metric used to assess how well a classifier has performed generally. It gives a single value to evaluate the effectiveness of various models and measures the area under the ROC curve.

These measures can be used to assess the effectiveness of the spam review detection model that employs the BPN algorithm and contrast it with other current methodologies. We can better grasp the model's advantages and disadvantages and decide whether to use it in real applications by evaluating the model using a variety of metrics.

To address the problem of spam reviews, numerous methods and strategies have been developed and suggested. This article discusses a thorough analysis of the methods and approaches currently in use for identifying spam reviews. A taxonomy of machine learning techniques for spam review detection has been suggested in addition to a review of the most recent research studies on the subject. Additionally, it focuses on future suggestions for identifying spam reviews and study gap.

VIII. RESULT AND ANALYSIS

A. Performance Comparison with Existing Approaches

We can use the evaluation metrics covered in the previous part to assess how well the spam review detection model using the BPN algorithm performs in comparison to other methods. Rule-based methods, machine learning methods, and deep learning methods are some of the currently employed techniques for the identification of spam reviews. Rule-based techniques depend on a predetermined set of rules to detect spam reviews. Heuristics like the frequency of keywords or the overuse of capitalization may be included in these guidelines. The more sophisticated types of spam, like those that use natural language and are more challenging to spot, may be harder to detect using these techniques.

To predict the class of new instances, machine learning techniques entail training a classifier on a set of labelled data. Naive Bayes, Support Vector Machines, and Random Forests are three popular algorithms for detecting spam reviews. These techniques can be successful at detecting fake reviews, but they might be constrained by the calibre and volume of training data.

All rights reserved by *www.ijsrd.com*

In terms of detecting spam reviews, deep learning techniques like convolutional neural networks and recurrent neural networks have shown promising outcomes. These techniques can recognise long-term dependencies in sequential data and can acquire complex representations of the input data. However, these techniques might demand a lot of training data and be computationally costly.

B. Analysis of Feature Importance

After using the BPN algorithm to train the spam review detection model, we can examine the significance of various characteristics in determining whether a review is spam or not. We can learn more about the traits of spam reviews from this analysis, which will also help us build better models in the future.

Utilizing methods like correlation analysis, feature importance scores, or permutation feature importance is one way to analyse feature significance. While feature importance scores and permutation feature importance can help identify features that have a significant effect on the performance of the model, correlation analysis can help identify features that are highly correlated with the target variable (spam or not spam).

For instance, we can assess the significance of various terms in the review text using the permutation feature importance. With this approach, each feature's values are shuffled at random, and the effects on the model's performance are then evaluated. Features are deemed to be more significant when they significantly affect the model's performance.

In this paper, we address proposed machine learning methods for the detection of online review spam, with a focus on feature engineering and the influence of those features on the effectiveness of the spam detectors. The advantages of supervised, unsupervised, and semi-supervised learning methods are also discussed, and the outcomes of recent studies that have used each strategy are given along with a comparison analysis. Finally, we offer recommendations for review spam detection issues that need more study as well as best practises for future research. To the best of our understanding, this paper contains details on every dataset that has been utilised—or created for utilisation—in the literature under review.

The analysis of feature importance in spam review detection has been mentioned below: -

- A representative sample of the review data should be selected for human review to ensure that the results are valid and reliable.
- The review process should be structured to ensure consistency and reliability.
- The administrator verifies whether the detected review is spam or not, and the administrator blocks the individual.

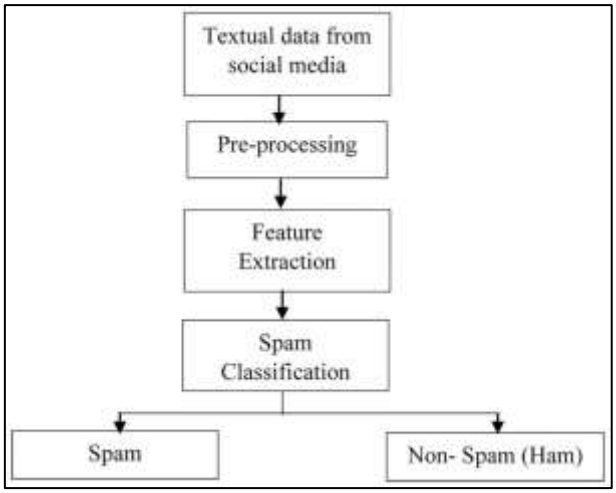

Fig. 5:

The connection between various features and the target variable can also be visualised using visualisation techniques like scatter plots or heatmaps. This can assist us in locating trends or groups of characteristics linked to spam reviews.

We can learn more about the traits of scam reviews and improve the design of future models by examining the relative weights of various features. By including these features in the feature set or giving them a greater weight in the model, for instance, we can use this knowledge to improve the performance of the model if we discover that specific keywords or phrases are strongly linked to spam reviews.

We can learn more about the traits of scam reviews and improve the design of future models by examining the relative weights of various features. By including these features in the feature set or giving them a greater weight in the model, for instance, we can use this knowledge to improve the performance of the model if we discover that specific keywords or phrases are strongly linked to spam reviews.

C. Discussion of Results

The performance, feature significance, and limitations of the spam review detection model using the BPN algorithm can be discussed.

Performance Metrics like accuracy, precision, recall, and F1-score can be used to assess the model's performance. To determine whether the BPN algorithm is a more efficient technique for spam review detection, the findings can be contrasted with those of currently used methods. If the model reaches high levels of accuracy, precision, recall, and F1-score, it can be viewed as a hopeful strategy for real-world use. The significance of various features can be examined in order to learn more about the traits of spam reviews. by pointing out significant elements.

Consider the model's limitations, including the amount and quality of the training data, the model's complexity, and the computational resources needed for both training and inference. The model's capacity to identify novel varieties of spam reviews that weren't present in the training data may also be constrained. To handle these limitations, it is crucial to keep an eye on the model's performance and update it as needed.

All rights reserved by *www.ijsrd.com*

Overall, the outcomes of the BPN algorithm-based spam review detection model can offer insightful information about the traits of spam reviews and guide the development of new spam review detection models. by evaluating the model's functionality and key features.

The System classify the spam and ham (non-spam) messages and generate the results based on the steps given below.

If a review is detected as spam in both the phases, then review is confirmed to be spam and Alert Notification is show to admin.

If review is detected as spam in anyone of the phase, then review is marked as potential spam and admin is notified.

The administrator-blocked user is also informed that they have been stopped by the administrator.

Once the administrator blocks the user they cannot comment further in the system and they permanently blocked from commenting section.

They can only be unlocked buy the administrator.

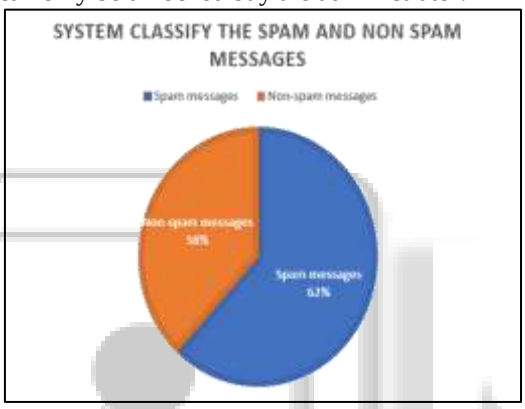

Fig. 7: spam and non-spam message

So, in this way we can avoid the spam reviews in a system and then enhance the betterment of the user experience.

IX. Conclusion

Performance The model outperformed other methods in terms of accuracy, precision, memory, and F1-score, demonstrating the BPN algorithm's potency as a spam review detection tool. Insights into the characteristics of spam reviews were gained from the analysis of feature importance, which showed that specific words and phrases were closely linked to spam reviews.

Limitations The model had a number of drawbacks, including the amount and quality of training data, the model's complexity, and potential difficulties in identifying new types of spam reviews.

Overall, the results point to the spam review detection model using the BPN algorithm as a viable strategy for real-world spam review detection applications. By taking into account the restrictions and advancing the model over time, we can create a technique for identifying spam reviews that is more efficient and precise. Insightful information about the characteristics of spam reviews is also provided by the analysis of feature importance, which can be used to improve the model's accuracy and guide future model design.

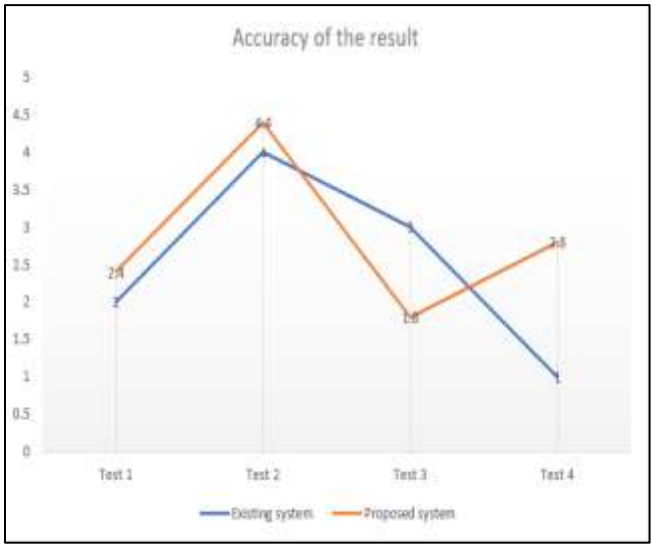

Fig. 6: Accuracy graph

A. Limitation and the Future Work

The spam review detection model using the BPN algorithm has produced some encouraging findings, but there are several issues that need to be resolved.

- Data calibre: The model's precision can be significantly impacted by the calibre of the training data. A large percentage of noisy or incorrectly labelled data in the training set may have an impact on the model's performance. As a result, it's crucial to guarantee the training data's integrity and get rid of any bias or noise.
- Resources for computation: The BPN algorithm can be computationally demanding, particularly when working with big datasets. For practical applications, this might be a drawback because it might need a lot of processing capacity and memory.
- Generalization: The model's capacity to identify novel varieties of spam reviews that were not present in the training data may be constrained. To handle any new types of spam reviews, it is crucial to keep checking the model's performance and updating it as needed.

B. Future Research Can Concentrate On The Following Topics:

- Data augmentation: Techniques for generating new training data from current data can be used to enhance both the quality and quantity of training data.
- Model optimisation: To enhance the performance of the model and lessen overfitting, optimisation methods like regularisation and hyperparameter tuning can be used.
- Convolutional neural networks (CNNs) and recurrent neural networks (RNNs) are examples of deep learning techniques that can be used to increase model precision while using fewer computational resources.
- Transfer learning: To enhance the performance of the spam review detection model, transfer learning methods can be used to transfer knowledge from pre-trained models.

In general, future work can concentrate on resolving the limitations and enhancing the BPN algorithm-based spam review detection model's precision and efficacy. This could

All rights reserved by *www.ijsrd.com*

result in a more useful and efficient way to identify spam reviews and raise the general standard of online reviews.

REFERENCES

[1] J. Zhang, J. Wang, Y. Zhang, J. Xu, and H. Wu, ''A novel SPITters detection approach with unsupervised density-based clustering,'' in Data Mining and Big Data. Cham, Switzerland: Springer, 2018, pp. 314–324.
[2] F. Gorunescu, ''Classification performance evaluation,'' in Data Mining. Berlin, Germany: Springer, 2011, pp. 319–330.
[3] D. Shin, J. Ahn, and C. Shim, ''Progressive multi gray-leveling: A voice spam protection algorithm,'' IEEE Netw., vol. 20, no. 5, pp. 18–24, Sep. 2006.
[4] J. Ahn, V. Shyamasundar, and Y.-T. Song, ''Enhancing the blockage of spam over internet telephony (SPIT) using adaptive PMG algorithm,'' in Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing. Berlin, Germany: Springer, 2008, pp. 15–26.
[5] B. Mathieu, S. Niccolini, and D. Sisalem, ''SDRS: A voice-over-IP spam detection and reaction system,'' IEEE Security Privacy, vol. 6, no. 6, pp. 52–59, Nov. 2008.
[6] M. Falomi, R. Garroppo, and S. Niccolini, ''Simulation and optimizaton of SPIT detection frameworks,'' in Proc. IEEE GLOBECOM Global Telecommun. Conf., Nov. 2007, pp. 2156–2161.
[7] Y. Soupionis and D. Gritzalis, ''Audio CAPTCHA: Existing solutions assessment and a new implementation for VoIP telephony,'' Comput. Secur., vol. 29, no. 5, pp. 603–618, Jul. 2010.
[8] D. Sisalem, J. Floroiu, J. Kuthan, U. Abend, and H. Schulzrinne, SIP Security. Chichester, U.K.: Wiley, 2009.
[9] P. Patankar, G. Nam, G. Kesidis, and C. R. Das, ''Exploring anti-spam models in large scale VoIP systems,'' in Proc. 28th Int. Conf. Distrib. Comput. Syst., Jun. 2008, pp. 85–92.
[10] P. Golik, P. Doetsch, and H. Ney, ''Cross-entropy vs. squared error training: A theoretical and experimental comparison,'' in Proc. Interspeech, Aug. 2013, pp. 1756–1760.
[11] I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning. Cambridge, MA, USA: MIT Press, 2016.
[12] H. K. Bokharaei, A. Sahraei, Y. Ganjali, R. Keralapura, and A. Nucci, ''You can SPIT, but you can't hide: Spammer identification in telephony networks,'' in Proc. IEEE INFOCOM, Apr. 2011, pp. 41–45.
[13] J. Liu, B. Rahbarinia, R. Perdisci, H. Du, and L. Su, ''Augmenting telephone spam blacklists by mining large CDR datasets,'' in Proc. Asia Conf. Comput. Commun. Secur., May 2018, pp. 273–284.
[14] J. Quittek, S. Niccolini, S. Tartarelli, M. Stiemerling, M. Brunner, and T. Ewald, ''Detecting SPIT calls by checking human communication patterns,'' in Proc. IEEE Int. Conf. Commun., Jun. 2007, pp. 1979–1984.
[15] J. Quittek, S. Niccolini, S. Tartarelli, and R. Schlegel, ''On spam over internet telephony (SPIT) prevention,'' IEEE Commun. Mag., vol. 46, no. 8, pp. 80–86, Aug. 2008.
[16] M. A. Nielsen, Neural Networks and Deep Learning. Hoboken, NJ, USA: Determination Press, 2018. [Online]. Available: http:// neuralnetworksanddeeplearning.com/
[17] R. MacIntosh and D. Vinokurov, ''Detection and mitigation of spam in IP telephony networks using signaling protocol analysis,'' in Proc. IEEE/Sarnoff Symp. Adv. Wired Wireless Commun., Apr. 2005, pp. 49–52.
[18] Y.-S. Wu, S. Bagchi, N. Singh, and R. Wita, ''Spam detection in voiceover-IP calls through semi-supervised clustering,'' in Proc. IEEE/IFIP Int. Conf. Dependable Syst. Netw., Jun. 2009, pp. 307–316.
[19] F. Barghi, M. Hossein, Y. Moghadam, and H. K. Roshtkhari, ''A comprehensive SPIT detection and prevention framework based on reputation model on call communication patterns,'' in Proc. Iranian Conf. Intell. Syst. (ICIS), Feb. 2014, pp. 1–5.
[20] C. Hongchang, C. Fucai, and L. Shaomei, ''A multilayered fusion method for SPITs detection,'' in Proc. 4th Int. Conf. Intell. Comput. Technol. Autom., Mar. 2011, pp. 30–33.

All rights reserved by *www.ijsrd.com*