International Journal of Computational Intelligence in Control

COMPARATIVE ANALYSIS OF MACHINE LEARNING ALGORITHMS FOR FAKE REVIEW DETECTION

Asif Raza[1]
Department of Computer Science and Information Technology.
University of Mianwali, Pakistan.
asifraza.uet@gmail.com

Faiz-ur-Rehman [2]
Department of Computer Science and Information Technology.
University of Mianwali, Pakistan.
faizii2012@gmail.com

Muhammad Bilal[3]
Department of Computer Science and Information Technology.
University of Mianwali, Pakistan.
mbilal2292@gmail.com

Muhammad Fahad Rauf [4]
Department of Computer Science and Information Technology.
University of Mianwali, Pakistan.
fahad@umw.edu.pk

Abstract- Nowadays, online buying has become a worldwide phenomenon. People frequently purchase items online, and many of e-commerce sites provide a review option for client feedback. People generally make purchasing decisions based on customer reviews that are already available. Some website owners may employ spammers to write false reviews in order to boost product sales. Many approaches have been proposed by researchers in the past to detect fraudulent reviews. However, there is a critical need to identify and analyze the best machine learning algorithm to detect fraudulent reviews. Therefore, in this study machine learning algorithms including support vector machine (SVM), Random Forest (RF), Logistic Regression (LR), Multi-layer perceptron (NN), Long Short-Term Memory (LSTM) and Decision Tree (DT) are compared. The comparison is done by comparing the results of evaluation parameters i.e. Accuracy, Precision, Recall and F1-Measure. Results of this study shows that, RF is the best algorithms for detecting fake reviews.

Keywords: Fake Reviews; Machine Learning Algorithms; Comparative Analysis; Kaggle dataset of fake reviews; Spam detection

I. INTRODUCTION

Now a days online shopping become the trend in world. People usually buy things online and these online shopping sites have review option for customer feedback. They usually decide to buy or not buy product on basis of already available reviews of customers. Some sites owners may hire the spammers for posting fake reviews to increase their sale of product [1]. For example someone want to buy laptop and the reviews are very positive but actually laptop is damaged so these are fake reviews. There is serious need to identify them and detect these fake reviews. In past many methods have suggested by researchers to detect the fake reviews. These reviews are hospitable for creating decisions about standard of products and services. Companies and traders use suggestions for making a decision for marketing structure, performance to services or product, for enhancement. Mostly companies hire the spammers or group or them for writing the reviews about products. These spammers can be professionals or non-professionals.

Automatic spam identification is an essential task, yet there is currently a dearth of study in this area. Spam on a review is significantly more difficult to detect than other sorts of spam, such as online spam or email spam. The major reason for this is that spammers can easily hide their identities. As a result, it is difficult for people to recognize, while email spam and web spam, where one can easily establish whether the latter is spam or not [1].

This problem not only misleads online shoppers while purchasing things, but it also tarnishes businesses by lowering customer happiness. As a result, developing a system that can recognize and categories text into bogus (fake) and true (truthful) evaluations is critical, as it will aid the online community in making informed purchasing decisions and quickly assessing consumer feedback. Previously, supervised machine learning (ML) and lexicon-based algorithms were employed to detect fake reviews [2, 3, 4]. To identify fraudulent and legitimate reviews submitted on social media

platforms, Asghar et al. [2] employed sentiment-based scoring algorithms. However, we are doing a comparative analysis of supervised ML technique, namely Random Forest (RF), Support vector machine (SVM), Multi-layer perceptron (NN), Logistic Regression (LR), Long Short-Term Memory (LSTM) and Decision Tree (DT), to detect real and fake (spam) text.

II. LITERATURE REVIEW

The study on Fake Review Detection focuses on ways to make ecommerce review sites more secure such that the benefits of continuing to propagate fake reviews aren't worth it [5, 6]. Owners of Online Social Networks (OSNs) have also turned to their internal resources to create procedures for detecting and restricting individuals who distribute fraudulent information: for example case studies reported by Tuenti [7], Flipkart [8], and Facebook [9]. We have not yet been able to eradicate the negative impacts of lying in review writing after years of work. This is due in large part to the lack of a "ground truth" for discriminating between honest and dishonest ideas. Even human assessors have been proven to routinely fail to discern between false and genuine evaluations [10]. It is not enough for an evaluator to look at a single review in isolation from other reviews of the same product to determine whether or not it is misleading, which makes review analysis a time-consuming and difficult process [6]. Fake review detection becoming increasingly difficult due to the progress of spamming tactics, the participation of freelancers in writing fake reviews [11], and the collaboration of spammers in groups [12]. This necessitates a full examination of regulatory advancements and machine learning algorithms used to combat the impact of review spamming.

III. METHODOLOGY

In this research, we have applied systematic approach. First of all, a dataset having fake and truthful review has been gathered. Then different classification algorithms are applied on it. Figure 1, exhibits the methodology which is employed to conduct this research.

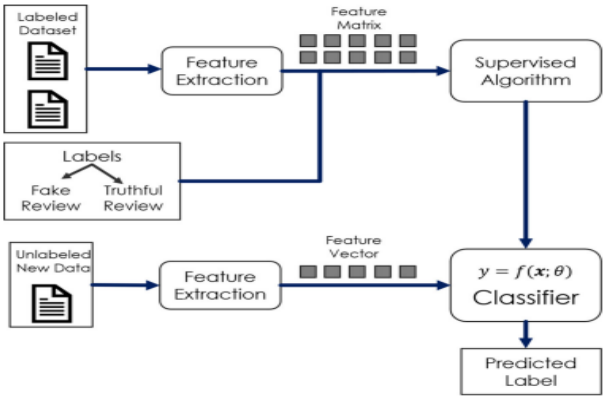

Figure 1: Methodology to apply ML algorithms

A. *Dataset*

A kaggle dataset is used in this study. The dataset is available on a sub-link of (https://www.kaggle.com/general/243411). It provided me with a good measure of attributes to work with, so we chose to give it a go. In includes, Verified Purchase, Product Title, Review Title, Rating, Review Text, and its class that is fake or real. We explored dataset to know the trends in database. The dataset have 10 attributed / features and have 21000 instances. Dataset is balanced as it has 10500 fake reviews and the same are real reviews. The data was then converted into numbers as the most of machine learning algorithms only works on integers.

B. *Classification Algorithms*

Various supervised learning classification algorithms including LR, DT, RF, NN and SVM are applied to detect the fake reviews.

- Logistic Regression: When the dependent variable is dichotomous, this model is utilised (binary). The results of the study gleaned from this model are typically regarded as predictive. Logistic regression is used to examine the connection between a nominal, intervals, ordinal, or ration-level independent variable and a binary dependent variable [13].
- Decision Tree: One of the most often used approaches for digital mapping is decision trees. This approach allows the researcher to carry out the mapping operation utilising a regression tree. This approach is predictive in nature. This method's main formula is to simply break up datasets into discrete blocks of a tree, which improves data growth in an efficient and accurate manner [14].

- Random Forest: The random forest, as the name suggests, is made up of a large number of individual decision trees that work together as an ensemble. Each individual tree in the random forest produces a class prediction, and the class with the most votes becomes the prediction of our model. The wisdom of crowds is a simple yet powerful principle at the heart of random forest [15].
- Support Vector Machine: Catanzaro created this supervised learning model. Data is utilised in SVM for regression analysis and categorization. It is the most resilient prediction model and is built on a statistical learning framework. It categorises the data into one or more groups. It categorises all new data that is provided in a previously specified category.
- Multilayer Perceptron (NN): Multilayer Perceptron is a Neural Network technique that learns linear and non-linear data correlations [16]. In the realm of deep learning, a multi-layered perceptron (MLP) is one of the most prevalent neural network models.
- LTSM: Learning and Teaching Support Material (LTSM) is a broad word that refers to a wide range of resources that instructors and students utilize in the context of teaching and learning [17].

IV. Results and Analysis

In this section, we have discussed and compared the results of each machine learning algorithm. Four different evaluation parameters were used for the comparison of algorithms which are precision, recall, accuracy and F1-Score.

A. Logistic Regression

LR exhibits the high accuracy and recall for dataset even though dataset was divided in such a way that test is 40% and 60% is the training set. Figure 2 exhibits the outcomes for LR. It exhibits that LR has achieved 79% of accuracy, 76.38% of precision, 79.74% of F1 score and 83.46% recall.

	precision	recall	f1-score	support
0	0.82	0.75	0.78	4239
1	0.76	0.83	0.80	4161
accuracy			0.79	8400
macro avg	0.79	0.79	0.79	8400
weighted avg	0.79	0.79	0.79	8400

```
Accuracy 0.79
Precision 0.7634644976918004
Recall 0.8346551309781303
F1_sCORE 0.7974741676234214
```

Figure 2: Results by using LR

B. Decision Tree

DT achieved an accuracy of 74.67%, 74.09% of precision, 75.15% of recall and 74.621% of F1 score. The results of decision are illustrated by figure 3.

	precision	recall	f1-score	support
0	0.75	0.74	0.75	4239
1	0.74	0.75	0.75	4161
accuracy			0.75	8400
macro avg	0.75	0.75	0.75	8400
weighted avg	0.75	0.75	0.75	8400

```
Accuracy 0.7467857142857143
Precision 0.7409952606635071
Recall 0.7515020427781783
F1_Score 0.7462116692518792
```

Figure 3: Results by using decision tree

C. Random Forest

The performance of Random forest is very well for detection of fake reviews. If shows 83.27% of accuracy, 85.64% of precision, 79.57% of recall and 82.49% of F1 score. Figure 4 exhibits the results of RF.

	precision	recall	f1-score	support
0	0.81	0.87	0.84	4239
1	0.86	0.80	0.82	4161
accuracy			0.83	8400
macro avg	0.83	0.83	0.83	8400
weighted avg	0.83	0.83	0.83	8400

Accuracy 0.8327380952380953
Precision 0.8564407656492499
Recall 0.7957221821677481
F1_Score 0.8249657406253894

Figure 4: Results by using Random Forest classifier

D. Multilayer Perceptron Neural Networks (NN)

NN has not performed well for this problem. It may be due to the size of dataset. We have used Keras library for NN model. Relu is used as activation function. 12 hidden layers and 15 epochs are used as initial parameters. NN shows 50% of accuracy and 25% of F1 score. Figure 5 exhibits the results of MPNN.

```
132/132 [==============================] - 0s 3ms/step
```

	precision	recall	f1-score	support
0	0.50	1.00	0.67	4239
1	0.00	0.00	0.00	4161
accuracy			0.50	8400
macro avg	0.25	0.50	0.34	8400
weighted avg	0.25	0.50	0.34	8400

Figure 5: Results by MPNN

E. Support Vector Machines (SVM)

SVM has also shown good results when applied to a fictitious review dataset. However, when compared to the other classifiers utilized in this study, SVM performs poorly. Figure 5 depicts the SVM findings. SVM attained 64.89% of accuracy, 61.20% of precision, 79.52% of recall and 69.17% of F1 score.

	precision	recall	f1-score	support
0	0.72	0.51	0.59	4239
1	0.61	0.80	0.69	4161
accuracy			0.65	8400
macro avg	0.66	0.65	0.64	8400
weighted avg	0.66	0.65	0.64	8400

Accuracy 0.6489285714285714
Precision 0.6120976692563818
Recall 0.7952415284787311
F1_Score 0.6917529005957981

Figure 6: Results by using SVM

F. LSTM

LSTM has also performed like multilayer perceptron neural network. It has also achieved a test accuracy of 50%. However, its training accuracy is 75.60% in 20th epochs. Figures show its training and testing accuracy.

LSTM was just not trained on enough epochs. 26,000 samples need more than 50 epochs. Another reason behind the low accuracy of LSTM network is that it is too simple and basic/default functions were used in it.

The accuracy can be improved by adding more LSTM layers and increase no of epochs or batch size. Further I can add regularizes and/or dropout to decrease the learning capacity of LSTM model.

	precision	recall	f1-score	support
0	0.50	1.00	0.67	4239
1	0.00	0.00	0.00	4161
accuracy			0.50	8400
macro avg	0.25	0.50	0.34	8400
weighted avg	0.25	0.50	0.34	8400

Figure 7: Results by LSTM

V. COMPARATIVE ANALYSIS OF RESULTS BY ML ALGORITHMS

All of the ML algorithms utilized in this investigation produced acceptable results. As a result, a comparison of all evaluation parameters attained by ML algorithms was performed. Table 1 provides a quick comparison of all algorithms in terms of assessment parameters.

Table 1: Comparative analysis against evaluation parameters

	SVM	Decision Tree	Logistic Regression	Random Forest (RF)	NN	LSTM
Accuracy	0.648	0.749	0.79	0.831	0.50	0.50
F1-Score	0.691	0.748	0.797	0.824	0.34	0.34
Precision	0.6120	0.744	0.763	0.854	0.25	0.25
Recall	0.795	0.752	0.834	0.795	0.50	0.50

Table 1 shows the results in terms of F1-score, precision, accuracy, and recall, against each classifier used in this research. It indicates that when classification algorithms are used, Random Forest outperforms all the algorithms. However, Logistic Regression have a high recall then random forest. RF shows an accuracy of 83.16%. The second best classifier of fake review detection is LR with 79% of accuracy. In terms of recall the second best classifier for our dataset is RF which shows 79.5% which is lesser then LR i.e. 83.4%. Support Vector Machine shows 64.8% of accuracy, 79.5% recall, 61.20% of precision and 69.1% of F1-score. The least but not the worst results against every parameter was shown by neural networks i.e. LSTM and multispectral. Both have achieved and accuracy of 50%. Figure 8, 9, 10 and 11 shows the comparative analysis of all the evaluation parameters for all ML algorithms in graphical form

.

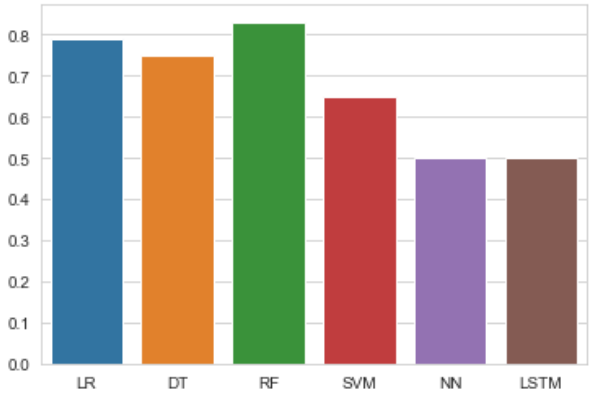

Figure 8: Accuracy comparison of ML algorithms

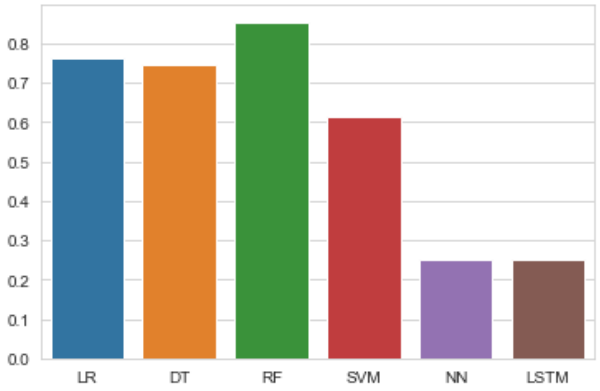

Figure 9: Precision comparison of ML algorithms

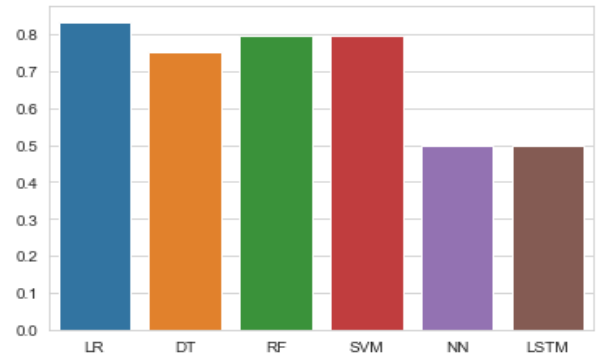

Figure 10: Recall comparison of ML algorithms

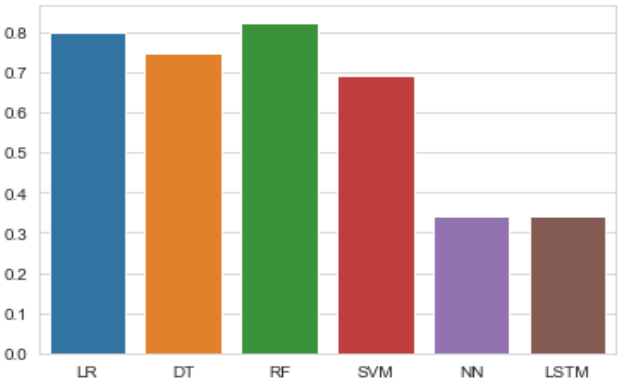

Figure 11: F1_Score comparison of ML algorithms

VI. DISCUSSION

The findings of this study shows that machine learning algorithms can successfully address the issue of fake review identification. All of the algorithms used, produce results that are more than excellent. As RF is a mixture of trees, it produces the greatest results. This is due to the nature and design of the algorithms. A single decision tree has an accuracy of 74.9%, whereas a combination of trees, such as RF, has an accuracy of 83.1%.

NN is well-suited to classification problems, and it performs best on two-class datasets. NN, on the other hand, did not fare well in this research. It has an accuracy of just 50%, which is much behind that of RF. The key reason for the poor performance of NNs is the large amount of data. For tiny datasets, NNs do not perform well. Another possible explanation is that we have converted some features into numbers, which may be the source of some noise.

References

[1] A. Heydari, M. Tavakoli and Z. Heydari, "Detection of review spam: A survey," *Expert Systmem and Applications*, pp. 3634-3642, 2015.

[2] M. Z. Asghar, A. Ullah, S. Ahmad and A. Khan, "Opinion spam detection framework using hybrid classification scheme," *Soft Computing*, p. 3475–3498, 2020.

[3] E. M.Bahgat, S. Rady, W. Gad and I. F.Moawad, "Efficient email classification approach based on semantic methods," *Ain Shams Engineering Journal*, pp. 3259-3269, 2018.

[4] G. Jain, M. Sharma and B. Agarwal, "Optimizing semantic LSTM for spam detection," *International Journal of Information Technology*, pp. 239-250, 2019.

[5] N. Jindal and B. Liu, "Opinion spam and analysis Proceedings of 2008 international conference on," *Proceedings of 2008 international conference on web search and data mining*, pp. 219-229, 2008.

[6] E. Lim, V. Nguyen, N. Jindal, B. Liu and H. Lauw, "Detecting product review spammers using rating behaviours," *Proceedings of 19th ACM international conference on information and knowledge managment* , 2010.

[7] Q. Cao, M. Sirivianos, X. Yang and T. Pregueiro, "Aiding the detection of fake accounts in large scale social online services," in *Proceedings of ACM conference on computer and communications security*, 2014.

[8] S. Kumar, B. Hooi, D. Makhija and M. Kumar, "FairJudge: trustworthy user prediction in rating platforms," *arXiv preprint arXiv:1703.10545*, 2018.

[9] A. Beutel, W. Xu, V. Guruswami and C. Palow, " Copycatch: stopping group attacks by spotting lockstep behavior in social networks," *Proceedings of 22nd international conference on World Wide Web*, pp. 119-130, 2013.

[10] M. Crawford, T. Khoshgoftaar and J. Prusa, "Survey of review spam detection using machine learning techniques.," *J Big Data*, 2015.

[11] A. Fayazi, K. Lee and J. Caverlee, "Uncovering crowdsourced manipulation of online reviews," *Proceedings of 38th international ACM SIGIR conference on research and development in information retrieval*, 2015.

[12] S. Mukherjee, S. Dutta and G. Weikum, "Credible review detection with limited information using consisteny features," *Proceedings of Joint European conference on machine learning and knowledge discovery in databases*, 2016.

[13] E. Dumitrescu, S. Hué, C. Hurlin and S. Tokpavi, "Machine learning for credit scoring: Improving logistic regression with non-linear decision-tree effects," *European Journal of Operational Research*, pp. 1178-1192, 2022.

[14] S. Souto-Miranda, A. Machado, A. Oliveira, C. Jácome, J. Cruz, V. Enes and V. Afreixo, "COPD profiles and treatable traits using minimal resources: identification, decision tree and stability over time," *Respiratory Research volume* , 2022.

[15] J. Bai, Y. Li and J. Li, "Multinomial random forest," *Pattern Recognition*, 2022.

[16] M. Gardnera and S. Dorlinga, "Artificial neural networks (the multilayer perceptron)—a review of applications in the atmospheric sciences," *Atmospheric Environment*, 1998.

[17] G. Liang and R. Ju, "LTSM: Lightweight and Time Sliced Measurement for Link State," *IEEE 26th International Conference on Network Protocols (ICNP)*, 2018.

[18] W. S. Bhaya, "Review of Data Preprocessing Techniques in Data Mining," *Journal of Engineering and Applied Sciences*, pp. 4102-4107, 2017.

[19] A. Sivakumar and R. Gunasundari, "A Survey on Data Preprocessing Techniques for Bioinformatics and Web Usage Mining," *Semantic Scholar*, 2017.

[20] Trifacta, "Trifacta," [Online]. Available: https://www.trifacta.com/data-cleansing-2/. [Accessed 20202].

[21] G. James, D. Witten and T. Hastie, An Introduction to Statistical Learning: with Applications in R (Springer Texts in Statistics), Corr. 7th printing , 2017.

[22] D. M.Allen, "The Relationship between Variable Selection and Data Agumentation and a Method for Prediction," *Technometrics*, p. 125–127, 1974.

[23] M. Kuhn and K. Johnson, Applied Predictive Modeling, New York: Springer-Verlag, 2013.

[24] S. Yeom, I. Giacomelli, M. Fredrikson and S. Jha, "Privacy Risk in Machine Learning: Analyzing the Connection to Overfitting," in *IEEE 31st Computer Security Foundations Symposium (CSF)*, Oxford, 2018.

[25] H. K. JABBAR and D. R. Z. KHAN, "METHODS TO AVOID OVER-FITTING AND UNDER-FITTING IN SUPERVISED MACHINE LEARNING (COMPARATIVE STUDY)," *Computer Science, Communication & Instrumentation Devices*, 2016.

[26] C. Bergmeir, MauroCostantini and J. M.Benítez, "On the usefulness of cross-validation for directional forecast evaluation," *Computational Statistics & Data Analysis*, pp. 132 - 143, 2014.

[27] M. Junker, R. Hoch and A. Dengel, "On the evaluation of document analysis components by recall, precision, and accuracy," in *roceedings of the Fifth International Conference on Document Analysis and Recognition*, Bangalore, India, 1999.

[28] J. LSeverens, J. Mulder, R. J.FLaheij and A. L.MVerbeek, "Precision and accuracy in measuring absence from work as a basis for calculating productivity costs in The Netherlands," *Social Science & Medicine*, pp. 243-249, 2000.

[29] K. Oksuz, B. C. Cam, E. Akbas and S. Kalkan, "Localization Recall Precision (LRP): A New Performance Metric for Object Detection," in *roceedings of the European Conference on Computer Vision (ECCV)*, 2018.

[30] D. M. W. Powers, *Evaluation: from precision, recall and F-measure to ROC, informedness, markedness and correlation*, arXiv:2010.16061 , 2020.

[31] F. Pedregosa, G. Varoquaux, A. Gramfort, V. Michel, B. Thirion, O. Grisel, M. Blondel, P. Prettenhofer, R. Weiss, V. Dubourg, J. Vanderplas, A. Passos, D. Cournapeau, M. Perrot and É. Duchesna, " Scikit-learn: Machine Learning in Python," *Journal of Machine Learning Research*, p. 2825–2830, 2011.

[32] D. Kingma, "Adam: A Method for Stochastic Optimization," *arXiv:1412.6980*, 2015.

[33] T. Hastie, R. Tibshirani and J. H. Friedman, The Elements of Statistical Learning, New York: Springer, 2009.

[34] Rosenblatt and F. x, Principles of Neurodynamics: Perceptrons and the Theory of Brain Mechanisms, Washington DC: Spartan Books, 1961.

[35] D. E. Rumelhart, G. E. Hinton and R. J. Williams, "Learning Internal Representations by Error Propagation, MIT Press, 1986.

[36] T. Dietterich, "Overfitting and undercomputing in machine learning," *ACM Computing Surveys*, 2007.

[37] Aayush, "Github," [Online]. Available: https://github.com/aayush210789/Deception-Detection-on-Amazon-reviews-dataset. [Accessed 10 12 2020].