International Journal of Engineering Trends and Technology
ISSN: 2231 – 5381 /doi:10.14445/22315381/IJETT-V69I10P230
Volume 69 Issue 10, 235-243, October, 2021

Boosting credibility of a Recommender System using Deep Learning Techniques - An Empirical Study

R. SujithraKanmani[1], B. Surendiran[2]

[1,2]*Department of Computer Science and Engineering, National Institute of Technology Puducherry, Karaikal-609609, India*

[1]sujithrakanmani@gmail.com, [2]surendiran@nitpy.ac.in

Abstract *- The recommendation system provides the user with their needed item or service by analyzing their preference history. In recent times the location-based recommendation has played a significant role in our everyday life. User interaction towards the internet is based on the social relationships comprising User Generated Content (UGC) like online reviews. A collaborative filtering approach is a popular recommendation framework for making recommendations to a new user based on comparable user content. However, it is vulnerable to Shilling attacks, in which shills put any unethical data into the ratings or comments database in order to modify the recommendations. As a lacking of trust format, the risk of misinformation becomes a research and evaluation concern. This paper proposes a trustworthy recommendation framework using the content features of the Deceptive opinion spam corpus dataset by employing the various deep learning algorithms in predicting the truthfulness of the reviews. Among the inspired models, the proposed hybrid combination of CNN-LSTM involving content feature excels in accuracy and prediction, thereby improving the performance and stability of the recommendation system.*

Keywords — *User Generated Content (UGC), Shilling attack, Long Short-term Memory (LSTM), Gated Recurrent Unit (GRU), Convolutional Neural Network (CNN), Bidirectional Long Short Term Memory (Bi-LSTM).*

I. INTRODUCTION

The user's requirements are suggested by the recommender system based on their preferences and interests. It has several uses, including e-commerce, e-learning, and tourism. etc[1].The recent trend of recommendation is the Location-based recommender systems which provide needed services related to the physical location of the user with the help of their mobile devices. A location-based recommendation system uses the unique properties of locations having granularity in different levels. With the usage of Location-Based Social Networks (LBSN), three types of graphs can be built[2] as given in Fig.1.

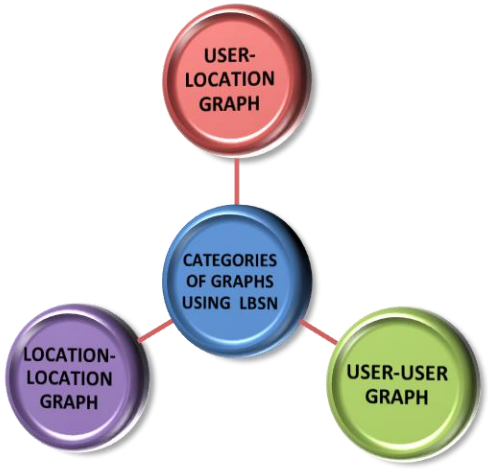

Fig.1.Categories of Graph built using LBSN

The user-location graph consists of users and their locations as entities. It is made up of user check-ins and the number of visits estimated based on the user's check-in histories. The location-location graph consists of the consecutive visit of a location by the user and their generated contents. The user-user graph depicts the nature of the relationship between both users in an online community. Thus with the usage of LBSN, the user can be given recommendations with the application of the Collaborative Filtering technique[3]. The collaborative filtering approach compares users or objects using ratings or other preference profiles based on relevance and makes a suggestion to the user. It is the most common technique used for recommendation[4][22].

It provides the recommendation based on relevance, and it is open in nature. As there is huge User-generated content is available now in the social network without any trust format, the collaborative filtering technique suffers from providing the promising recommendation to the user with the full impact of trust[5]. Thus the collaborative filtering technique is more prone to shilling or profile injection attacks[6][21].

In a shilling attack, the shillers inject unscrupulous shilling profiles into the rating or review description database, and therefore the system's recommendation gets altered, and inappropriate items are being recommended[7]. The two specific intents of shilling attacks are given in Fig.2. In the Push attack, the items are being promoted so that the item becomes more likely by the user. In the Nuke attack, the Shiller inserts bogus data to demote the opponent's item to become a less likely one to the user. The effort needed to mount the attack is the minimum knowledge required about the system.

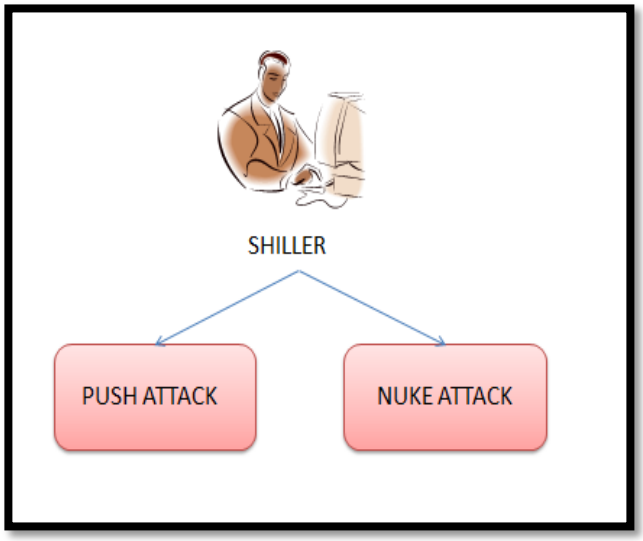

Fig.2. Attack intents of Shiller

Thus this paper provides the contribution in tackling the shilling attack with the credibility assessment on content feature involving user reviews. Deep Learning models are now widely used in recommender system as it has its variety of applications in feature engineering[8]. Thus, this proposed work analyses the deep learning model in assessing the credibility of the recommendation system with the consideration of content features involving review text and compound score. This Provides the prediction of trust in reviews. The body of the article is arranged as follows: Materials and techniques are discussed in section 2, Evaluation Metrics are discussed in section 3, Results and Discussion are discussed in section 4, and Future Work is discussed in section 5.

II. MATERIALS AND METHODS

A. Problem Formulation

With wide available user-generated content, the possibility of misinformation becomes a research problem, and evaluating the content's credibility is a key motivation of this research. The objective is to overcome the shilling attack by providing trustworthy recommendations with the exploration of credibility features in a Location-based recommender system. Thus a typical deep learning model involving the hybrid combination of CNN and LSTM exploring content feature is presented, which enhances the performance of the recommender system for detecting the deceptive review and compared with the other inspiring models.

B. Dataset

The suggested model is evaluated using the Kaggle Deceptive Opinion dataset. The dataset, which is in CSV format, contains five attributes: deceptive, polarity, source, hotel, and text. There are 1600 records in the collection. It is a corpus of 20 Chicago hotel reviews that are both true and misleading. The corpus comprises 400 honest, positive TripAdvisor reviews, 400 deceptive positive Mechanical Turk reviews, 400 truthful and bad Expedia, Hotels.com, Orbitz, Priceline, TripAdvisor, Yelp reviews, and 400 deceptive negative Mechanical Turk reviews.

C. Models Involved

The following models were employed in this paper: LSTM, Bidirectional Long Short-Term Memory (Bi-LSTM), CNN-LSTM, CNN-BiLSTM, CNN-GRU, and DenseNet. LSTM models are effective for grouping and categorizing data based on time series and text[9]. Over the last decade, LSTM models have been recognized as effective models that can learn from sequence data. The ability of LSTM is to capture long-term relationships and learn quickly from sequences of varying lengths and their value. LSTM models have also been investigated for detecting fraudulent card transactions[10]. Fig.3. depicts the LSTM working model used in this study.

The LSTM model attempts to detect whether the given review content is legitimate or fraudulent by training a many to one RNN. It feeds the pre-trained content features from the reviews, including the compound score, into the dense layer for classification using the softmax activation function, as indicated in Equation 1. The dropout is being added to avoid overfitting.

Bi-LSTM is a kind of Recurrent Neural Network as well (RNN). Because it employs two hidden layers, it can process data in both directions[11]. This is the main source of disagreement with LSTM. Bi-LSTM has demonstrated promising results in natural language processing[12][13]. After passing through forward and backward LSTM networks, the gathered attributes from each review are input into the dense layer for classification using the softmax activation function. Dropout is used before the softmax layer to prevent overfitting. Fig.4 depicts the working model of the Bidirectional-LSTM.

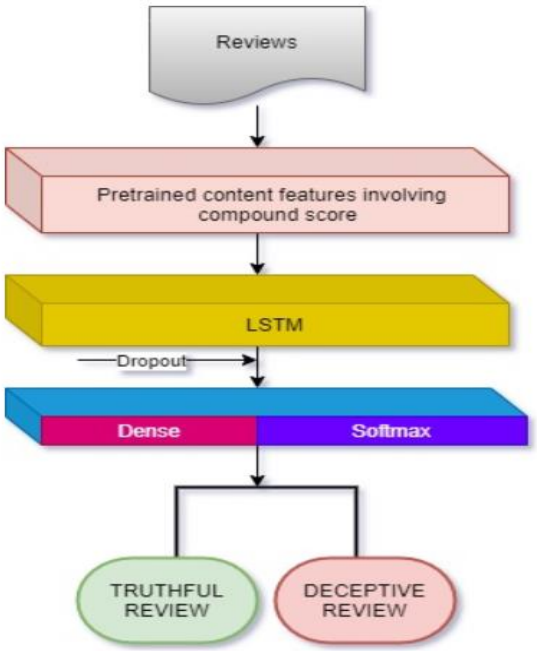

Fig.3.Working model of LSTM involving content feature

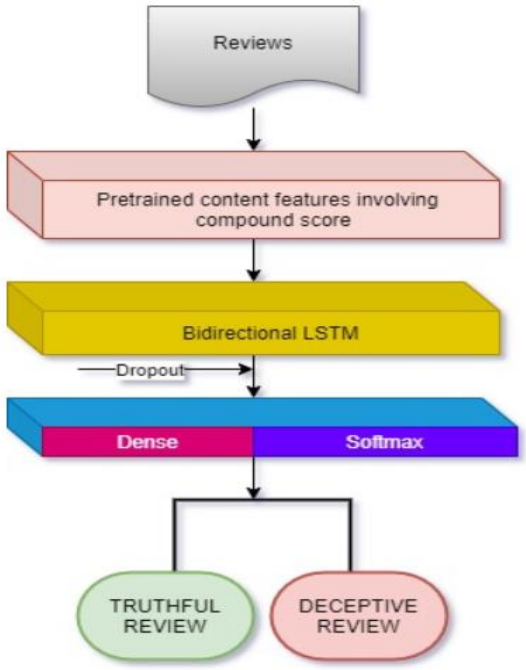

Fig.4. Working model of Bidirectional LSTM involving content feature

Several tests over the last five years have demonstrated that combining CNN with LSTM generates a more stable model than either CNN or LSTM alone. The CNN-LSTM model works by first processing the input data with CNN. An LSTM classifier is then applied to the CNN output. The excellent performance of the CNN-LSTM model is due to the combination of CNN's capacity to capture short-term feature interactions and LSTM's ability to capture long-term feature relations[14][15]. The model's first layer is the review representations. The convolution layer extracts characteristics, which are then multiplied element-by-element by the corresponding filter. The number of pools in the pooling layer is reduced when features are multiplied in the maximum pooling method. The LSTM layer learns from the information obtained after convolution and pooling and predicts whether a given review is true or false. Use a dropout of 0.3 before the convolutional layer and after the LSTM layer to avoid overfitting, as illustrated in Fig.5.

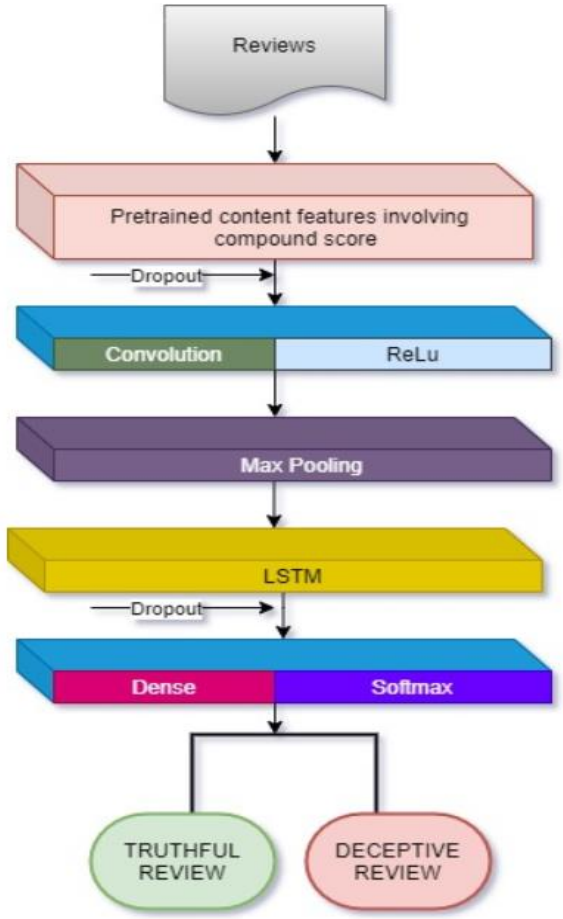

Fig.5.Working of CNN-LSTM Model involving content feature

The CNN-BiLSTM model produces results over long texts because it makes use of the CNN's capacity to extract features and the Bi-ability LSTM's to learn long-term bidirectional text dependencies[16][17]. The CNN-BiLSTM working model in our study is illustrated in Fig.6.

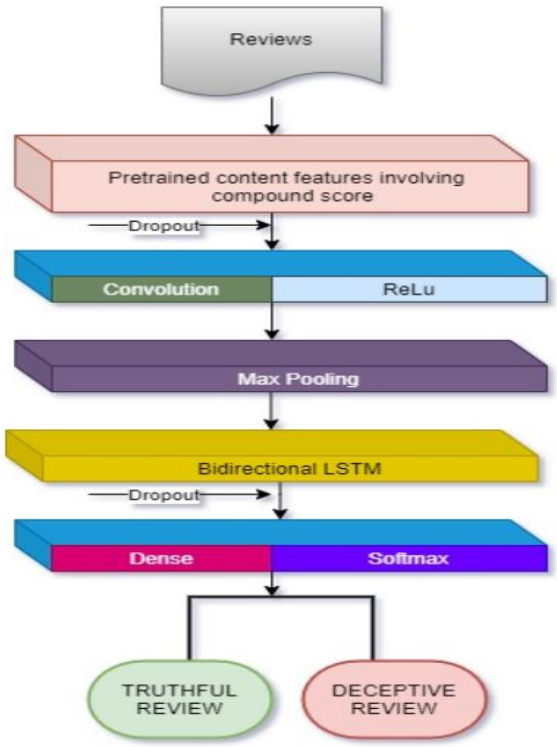

Fig.6. Working of CNN-BiLSTM Model involving content feature

Text classification may be accomplished using a model that employs a convolutional neural network, a Highway network, and a gated recurrent unit to effectively infer both global and local textual semantics. The Gate Recurrent Network offers a wide range of applications in evaluating the surfing histories of users[18]. Furthermore, totally convolutional layers are added to minimize the huge number of parameters provided by the initial fully convolutional layers. The model's convergence rate can therefore be deliberately accelerated[19]. Fig.7 depicts the CNN-GRU operational model.

Each layer in DenseNet receives extra input from all preceding levels and passes on its own feature maps to all future layers. Concatenation is employed. Each layer receives "collective knowledge" from all previous levels. Because each layer gets feature maps from all preceding layers, the network can be thinner and more compact, resulting in fewer channels. The increased number of channels for each layer is represented by the growth rate k. As a result, it has greater computational and memory efficiency[23][25]. The transition layers between two contiguous dense blocks are 1×1 Conv followed by 2×2 average pooling. The feature map sizes are the same inside the dense block, allowing them to be readily concatenated together. A global average pooling is done at the conclusion of the last dense block, and then a softmax classifier is added in this work, as shown in Fig.8.

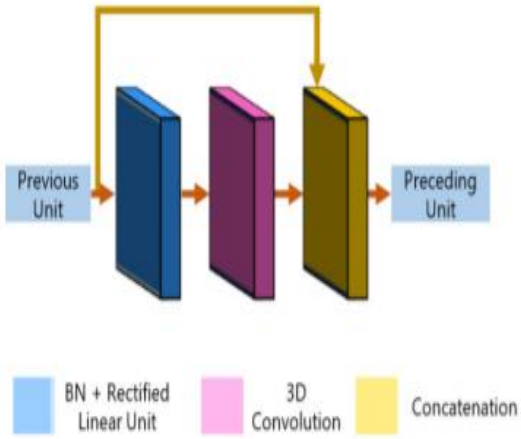

Fig.8. Working of DenseNetModel[24]

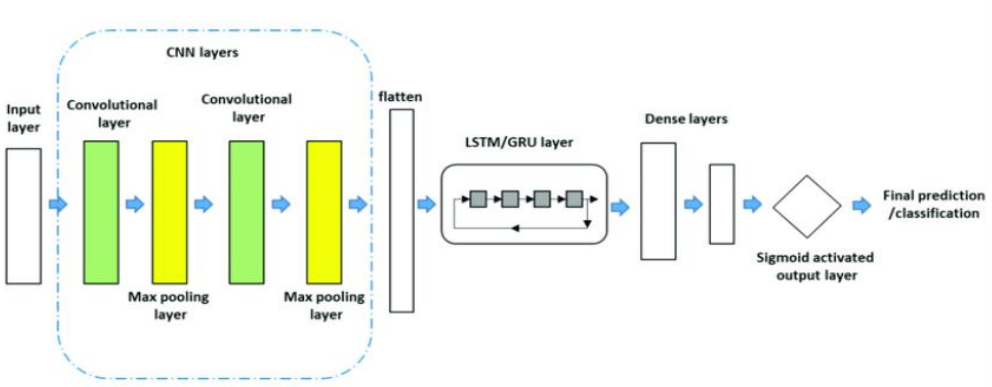

Fig.7.Working of CNN-GRU Model involving contentfeature[5]

D. Proposed System

The proposed system provides recommendations by concentrating on the user's review text and sentiment, including its truthfulness. The proposed system architecture is shown in Fig.9. as given below; for detecting and predicting the deceptive reviews, the hybrid combinational model of CNN and LSTM along with compound score is being utilized. The main challenge of a recommender system lies in the trustworthy providence of user's choices and needs.

Following data preparation, the real data is split into training and testing sets. Reviews are classified and input into deep learning models based on the derived compound score. The polarity feature is used with the VADER library, and its emotion is categorized as positive, negative, or neutral.

The compound score is computed by taking each word in the lexicon and adding their valence scores, then normalizing it to be between (most severe negative) and +1. (most extreme positive).

Eq.1. shows how to compute the compound score.

$$Compound\ score,\ c = \frac{s}{\sqrt{s^2+\beta}} \qquad (1)$$

Where c is the compound score calculated, s is the sum of polarity scores of all words, and β is the constant and default set to the value 15. The classification of positive, negative, and neutral sentiment is made by satisfying the following compound range conditions as given in Eq.2, below

$$c = \begin{cases} Positive, & c > 0.5 \\ Negative, & c < -0.5 \\ Neutral, & (c < -0.5 \ and \ c > 0.5) \end{cases} \qquad (2)$$

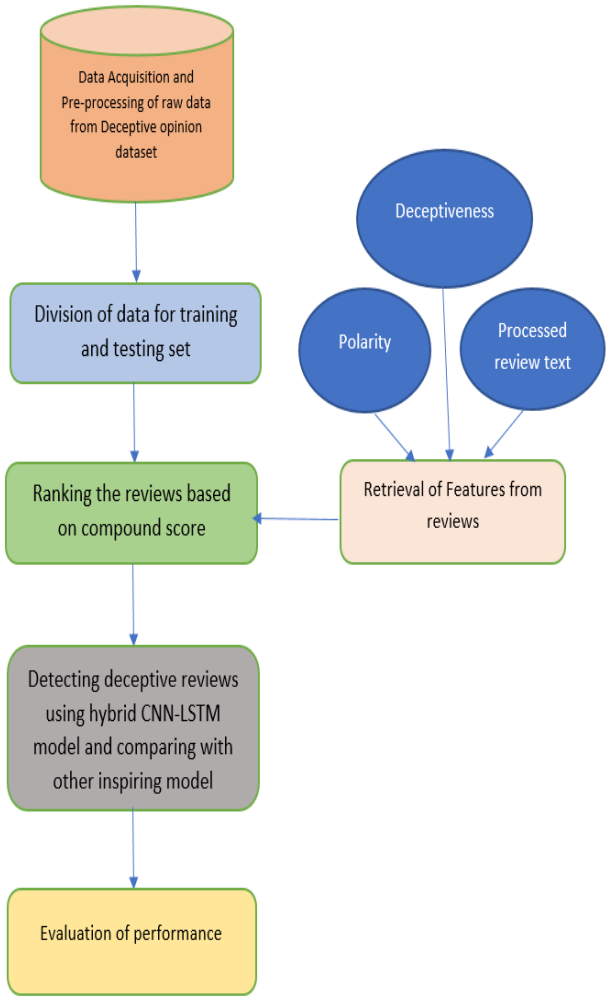

Fig.9. Proposed System Architecture

The estimated sentiment intensity levels are depicted in the figures below.Fig.10 states the scattering view of positive reviews over the Polarity as the compound value will be greater than 0.5 and towards 1 stating the positive reviews, Fig.11 states the scattering view of neutral reviews over the Polarity and it can be found between c < - 0.5 & c > 0.5 and Fig.12 states the scattering view of negative reviews over the Polarity as the compound value will be lesser than -0.5.

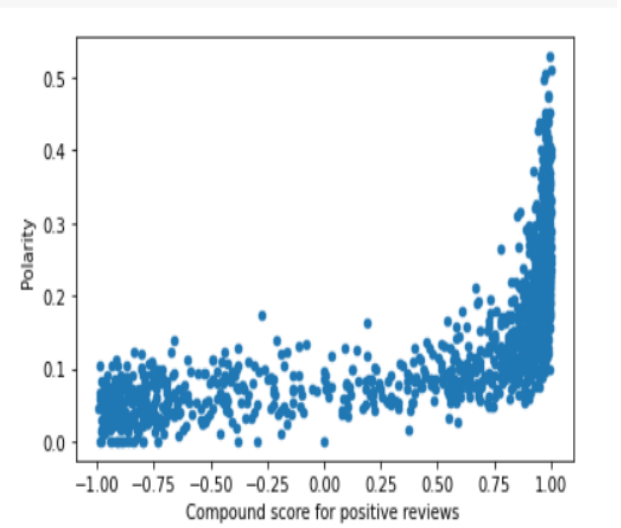

Fig.10.Compound Score plotted over polarity in Deceptive opinion spam Corpus Scattered towards +1 stating positive reviews

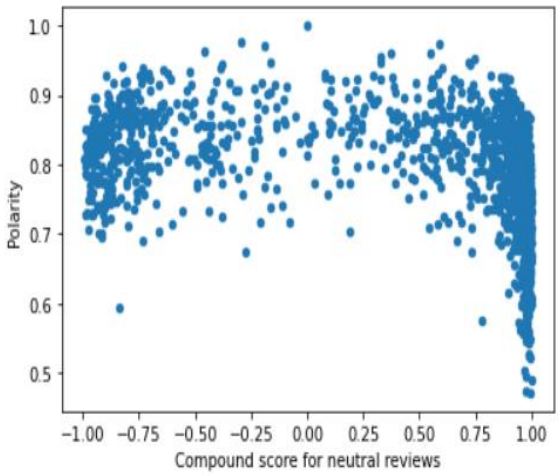

Fig.11. Compound Score plotted over polarity in Deceptive opinion spam Corpus Scattered towards +1 and -1 stating neutral reviews

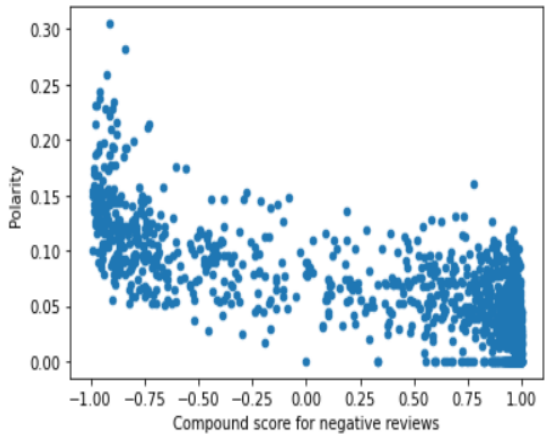

Fig.12. Compound Score plotted over polarity in Deceptive opinion spam Corpus Scattered -1 stating negative reviews

After preprocessing, the content features such as deceptive, polarity, and text are chosen, and the reviews are ordered and fed into various deep learning models such as LSTM, Bidirectional Long Short-Term Memory (Bi-LSTM), CNN-LSTM, CNN-BiLSTM, and CNN-GRU, and the CNN-LSTM combination performs well on detecting and predicting deceptive reviews. The accuracy and loss in training and validation demonstrate that the above models suit well for the identification of misleading data. The models' performance is being assessed using accuracy and loss calculation. Thus, fraudulent reviews are discovered and ignored. The proposed system delivers the suggestion of the top ten truthful reviews having the highest compound score providing the user with a trustworthy recommendation.

III. EVALUATION METRICS

The proposed model is being evaluated by the following measures

Accuracy is an instinctive performance measure. It is the ratio of correctly predicted items, and It is given by the following Eq. 3.

$$Accuracy = \frac{(TP + TN)}{(TP + FN + FP + TN)} \quad (3)$$

Loss is calculated by running the network forward over inputs Xi and comparing the network outputs $\hat{Y}_i$ With the ground, truth values Yi using a loss function. It is given by the below Eq.4.

$$J = \frac{1}{N}\sum_{i=1}^{N} L(\hat{Y}_i, Yi) \quad (4)$$

IV. RESULTS AND DISCUSSIONS

A. Performance Evaluation

The experiment was conducted on the Deceptive opinion dataset. The results of the proposed combinational recommended model CNN and LSTM with sentiment intensity value are finer than traditional models such as LSTM, BI-LSTM, CNN+Bi-LSTM, and CNN+GRU method. In addition, the outcomes of this hybrid method are improved than the model based on the sentiment intensity values. The accuracy value of the proposed hybrid (CNN-LSTM) model is better than other models. The proposed model is assessed as far as the performance metric, and the loss function stood out from different models. The correlation accuracy estimations of different models for deceptive opinion dataset is provided in the below Fig.13-18.Fig.13 illustrates the LSTM model with an accuracy value of 80.5%. Fig.14 shows the Bi-LSTM model with an accuracy of 82.5%. Fig.15 shows the CNN-BiLSTM model with an accuracy of 49%. This combination has the least accuracy percentage on the deceptive opinion dataset. Fig.16. shows the CNN-GRU model with an accuracy of 42%.Fig.17 shows the DenseNet model with an accuracy of 79%. The proposed combinational model of CNN-LSTM is shown in Fig.18, which excels inaccuracy with 83.7% when compared with the existing models. The first fifty review sentence from the testing set is being given as an input, and it is predicted for its deceptiveness using this proposed model. Then it is compared with the various inspired deep learning models for its accuracy. The accuracy percentage and deceptiveness prediction percentage are being tabulated for the Deceptive opinion dataset for 200 epochs, as shown below in Table 1.

TABLE I

DECEPTIVENESS PREDICTION PERCENTAGE AND ACCURACY OF THE PROPOSED AND INSPIRED DEEPLEARNING MODELS

Deep Learning Model	Prediction Percentage forDeceptiveness (%)	Accuracy percentage(%)
LSTM	96	80.5
Bi-LSTM	97	82.5
CNN+ Bi-LSTM	56	49
CNN+GRU	49	42
DenseNet	43	79
Proposed (CNN+LSTM involving Sentiment Intensity)	99	83.7

A. Recommendation Results

The top 10 truthful reviews with higher positive values are being recommended to the user thus providing trustworthy recommendation resolving the shilling attack and overcomes the limitation of coverage by providing the user with effective recommendation as shown in Table. 2.

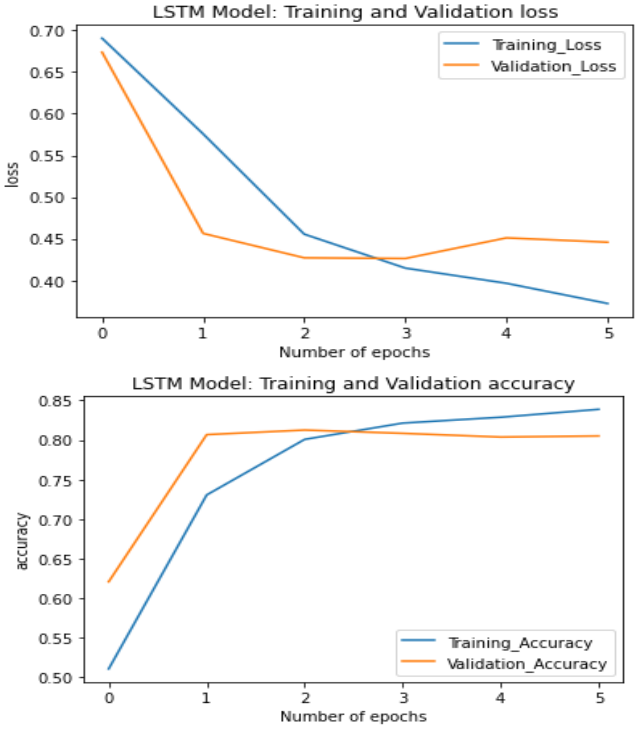

Fig.13.LSTM model involving sentiment intensity values with Loss and Accuracy curves

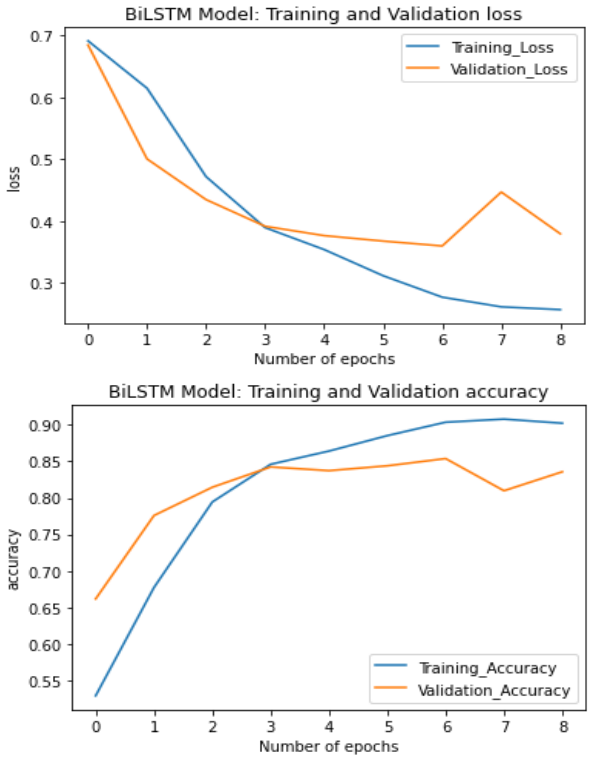

Fig.14.Bi-LSTM model involving sentiment intensity value with Loss and Accuracy curve

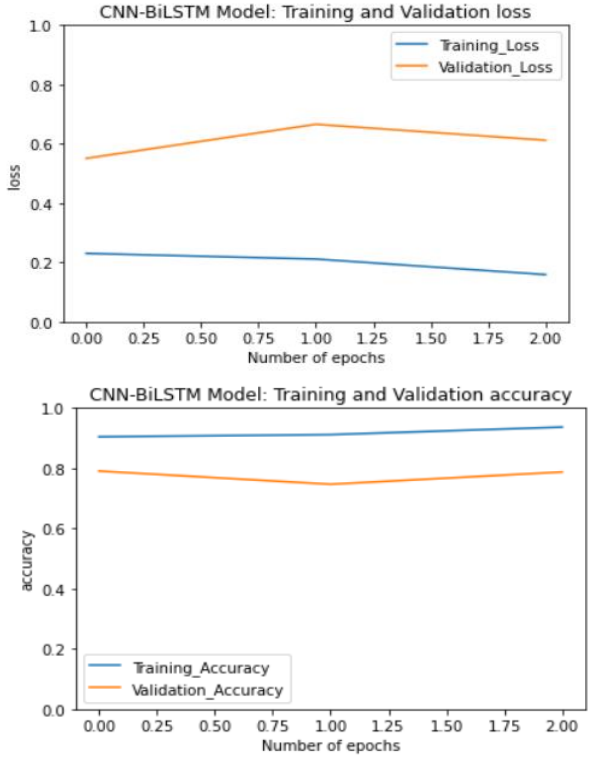

Fig.15. CNN +Bi- LSTM model involving sentiment intensity values with Loss and Accuracy curves

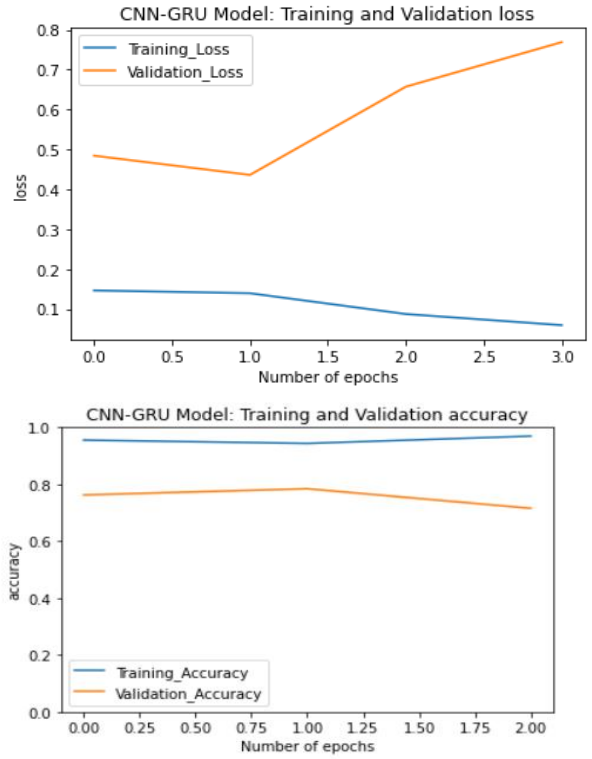

Fig.16.CNN + GRU model involving sentiment intensity values with Loss and Accuracy curves

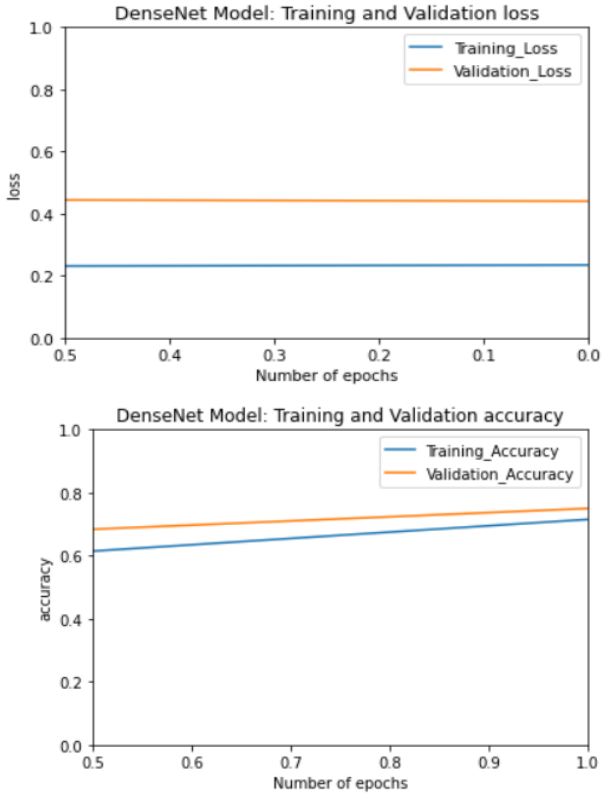

Fig.17. DenseNetmodel involving sentiment intensity values with Loss and Accuracy curves

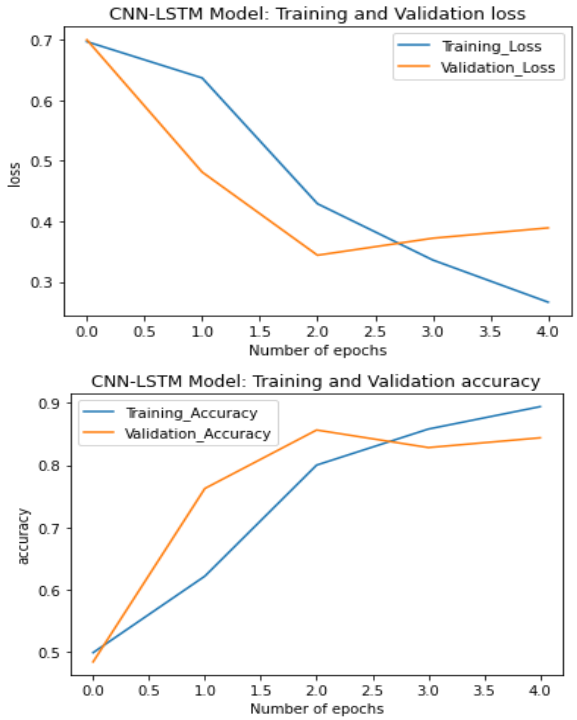

Fig.18. Proposed CNN+ LSTM model involving sentiment intensity values with Accuracy and Loss curves

TABLE II
RECOMMENDATION OF TOP 10 TRUTHFUL REVIEWS BASED ON HIGH POSITIVE VALUE

Compound range	Truthful Review Content
0.9988	We just returned from our first trip to Chicago...
0.9984	I loved this hotel - fabulous old building but...
0.9983	I love the Ambassador East, true, she's a litt...
0.9981	This is one of my favorite Sheratons/Starwood…
0.9981	My wife and I stayed at the James recently and...
0.9980	We have just returned from a week at the James...
0.9977	We recently completed our second stay at the F...
0.9974	Got a great deal through Hotwire for $70 a nig...
0.9973	I'll keep it short. My wife, daughter and I st...
0.9971	The Knickerbocker hotel is fantastic! It's an ...

V. CONCLUSION

The proposed work provides recommendations considering the credibility content feature, which involves the User Generated Content such as reviews of the user. Thus the shilling attack in the recommendation system is being sorted out with the usage of accessing credibility along with the exploration of review sentiment. This paper studied and proposed a trustworthy recommendation framework using Deceptive opinion spam corpus dataset and employing deep learning models in which the hybrid combination of CNN and LSTM with polarity feature excels in accuracy compared with other deep learning models such as LSTM, Bi-LSTM, CNN+ Bi-LSTM, DenseNetand CNN+GRU. Thus this system improves the performance and stability of the recommendation system overcoming the trust issues by avoiding deceptive reviews. The future work is to enhance the work with a huge real-time dataset as the deep learning models suffer in learning with the small labeled dataset. The generation of the synthetic dataset with negative labels and applying this on various unlabeled datasets makes us enhance the prediction accuracy.

REFERENCES

[1] Rajabpour, Neda, et al. Application domain of recommender system: a survey. International Journal of Advanced Studies in Computers, Science and Engineering, 3(2) 2014, doi: http://www.ijascse.org/.

[2] J. Bao, Y. Zheng, D. Wilkie, and M. Mokbel, Recommendations in location-based social networks : A survey Recommendations in location-based social networks : a survey, ACM Transaction on Intelligent systems and technology, July, (2015), doi: 10.1007/s10707-014-0220-8.

[3] V. W. Zheng, Y. Zheng, X. Xie, and Q. Yang, Towards mobile intelligence : Learning from GPS history data for collaborative recommendation, Artif. Intell., 184–185 (202) 17–37, doi: 10.1016/j.artint.2012.02.002.

[4] R. Katarya and O. P. Verma, Effectivecollaborative movie recommender system using asymmetric user similarity and matrix factorization, 2016 Int. Conf. Comput. Commun. Autom., (2016) 71–75, doi: 10.1109/CCAA.2016.7813692.

[5] L. Guo, J. Liang, Y. Zhu, Y. Luo, L. Sun, and X. Zheng, Collaborative filtering recommendation based on trust and emotion, J. Intell. Inf. Syst., 53(1) (2019) 113–135, doi: 10.1007/s10844-018-0517-4.

[6] M. Si and Q. Li, Shilling attacks against collaborative recommender systems : a review, Artif. Intell. Rev., 53(1) (2020) 291–319, doi: 10.1007/s10462-018-9655-x.

[7] A. P. Sundar, F. Li, X. Zou, T. Gao, and E. D. Russomanno, Understanding shilling attacks and their detection traits: A comprehensive survey, IEEE Access, 8(2020) 171703–171715, doi: 10.1109/ACCESS.2020.3022962.

[8] W. Long, Z. Lu, and L. Cui, Deep learning-based feature engineering for stock price movement prediction, Knowledge-Based Syst., 164 (2019) 163–173, doi: 10.1016/j.knosys.2018.10.034.

[9] Kumar, Lokesh. Predictive Analytics of COVID-19 Pandemic: Statistical Modelling Perspective. Walailak Journal of Science and Technology (WJST), 18(16) (2021) ,doi:https://doi.org/10.48048/wjst.2021.15583.

[10] Wiese B., OmlinC. Credit Card Transactions, Fraud Detection, and Machine Learning: Modelling Time with LSTM Recurrent Neural Networks, Innovations in Neural Information Paradigms and Applications. Studies in Computational Intelligence, 247, 231–268,doi: https://doi.org/10.1007/978-3-642-04003-0_10.

[11] T. Fornaciari and L. Cagnina, Fake opinion detection : how similar are crowdsourced datasets to real data ?, Lang. Resour. Eval., (2020), doi: 10.1007/s10579-020-09486-5.

[12] M. Schuster and K. K. Paliwal, Bidirectional recurrent neural networks, IEEE Trans. Signal Process., 45(11) (1997) 2673–2681, doi: 10.1109/78.650093.

[13] V. Makarenkov, L. Rokach, and B. Shapira, Choosing the right word: Using bidirectional LSTM tagger for writing support systems, Eng. Appl. Artif. Intell., 84 (2019) 1–10, doi: 10.1016/j.engappai.2019.05.003.

[14] Y. Heryadi and H. L. H. S. Warnars, Learning temporal representation of transaction amount for fraudulent transaction recognition using CNN, Stacked LSTM, and CNN-LSTM, 2017 IEEE Int. Conf. Cybern. Comput. Intell. Cybern. 2017 - Proc., 2017(2018) 84–89, doi: 10.1109/CYBERNETICSCOM.2017.8311689.

[15] K. Vivekanandan and N. Praveena, Hybrid convolutional neural network (CNN) and long-short term memory (LSTM) based deep learning model for detecting shilling attack in the social-aware network, J. Ambient Intell. Humaniz. Comput., 12(1) (2021) 1197–1210, doi: 10.1007/s12652-020-02164-y.

[16] M. Rhanoui, M. Mikram, S. Yousfi, and S. Barzali, A CNN-BiLSTM Model for Document-Level Sentiment Analysis, Mach. Learn. Knowl. Extr., 1(3) (2019) 832–847, doi: 10.3390/make1030048.

[17] L. Zhang and F. Xiang, Relation Classi fi cation via BiLSTM-CNN, Data Mining and Big data no. 10 (2018) 373–382, doi: 10.1007/978-3-319-93803-5.

[18] Okura, Shumpei, Yukihiro Tagami, Shingo Ono, and Akira Tajima. Embedding-based news recommendation for millions of users. In Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, (2017) 1933-1942, doi: https://doi.org/10.1145/3097983.3098108

[19] B. Liu, Y. Zhou, and W. Sun, Character-level text classification via convolutional neural network and gated recurrent unit, Int. J. Mach. Learn. Cybern., 11(8) (2020) 1939–1949, doi: 10.1007/s13042-020-01084-9.

[20] S. Y. Yerima, M. K. Alzaylaee, A. Shajan, andP.Vinod, Deep learning techniques for android botnet detection, Electroics., 10(4) (2021) 1–17, doi: 10.3390/electronics10040519.

[21] Anjani KumarVerma, Veer Sain Dixit, Security Based Recommender System Against Profile Injection Attack. International Journal of Engineering Trends and Technology, 69(3) 219-228.doi: 10.14445/22315381/IJETT-V69I3P233.

[22] Kaushik, Shaivya, and Pradeep Tomar. Evaluation of Similarity Functions by using User based Collaborative Filtering approach in Recommendation Systems. IJETT, (2015) 194-200.

[23] Londt, Trevor, Xiaoying Gao, and Peter Andreae., Evolving Character-level DenseNet architectures using genetic programming. In International Conference on the Applications of Evolutionary Computation (Part of EvoStar), (2021) 665-680. Springer, Cham, doi: https://doi.org/10.1007/978-3-030-72699-7_42.

[24] Ruiz J., Mahmud M., Modasshir M., Shamim Kaiser M., Alzheimer's Disease Neuroimaging Initiative, 3D DenseNet Ensemble in 4-Way Classification of Alzheimer's Disease. In: Mahmud M., Vassanelli S., Kaiser M.S., Zhong N. (eds) Brain Informatics. BI 2020. Lecture Notes in Computer Science, 12241 (2020). Springer, Cham.doi:https://doi.org/10.1007/978-3-030-59277-6_8.

[25] Yu, Su-Gyeong, Kun Ha Suh, and EuiChul Lee. Face Spoofing Detection Using DenseNet. In International Conference on Intelligent Human Computer Interaction, (2020) 229-238, doi: https://doi.org/10.1007/978-3-030-68452-5_24.