International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 09 | September - 2023 SJIF Rating: 8.176 ISSN: 2582-3930

A STUDY COMPARING MACHINE LEARNING AND DEEP LEARNING METHODS FOR THE DISCOVERY OF FAKE NEWS IN HEALTH SECTOR USING DIFFERENT DEEP AND SHALLOW METHODS

Prof. Sandeep Rao[1], Prof. Vivek Patel[2], Prof. Rajendra Arakh[3]

[1] Assistant Professor, Department of Computer Science & Engineering, Shri Ram Institute of Technology, Jabalpur, MP.

[2] Assistant Professor, Department of Computer Science & Engineering, Shri Ram Institute of Technology, Jabalpur, MP.

[3] Assistant Professor, Department of Computer Science & Engineering, Shri Ram Institute of Technology, Jabalpur, MP.

ABSTRACT

The problem of fake news, which existed even before Internet prevalence, has been made worse by the internet's growth and adoption. If the news is concerning your health, this becomes more urgent. This study suggests Content Based Models (CBM) and Feature Based Models (FBM) as solutions to this problem. The supplied input is what distinguishes the two models. The FBM also takes two readability features as input in addition to the content, whereas the CBM simply accepts news content as an input. Under each category, the effectiveness of two hybrid deep learning approaches, namely CNN-LSTM and CNN-BiLSTM, is compared with five classic machine learning techniques: Decision Tree, Random Forest, Support Vector Machine, AdaBoost-Decision Tree, and AdaBoost-Random Forest.

The study used the Fake News Healthcare dataset, which included 9581 stories. This extremely unbalanced dataset is balanced using a simple data augmentation technique. The experimental findings show that Feature Based Models outperform Content Based Models in terms of performance. AdaBoost-Random Forest had an F1 Score of 98.9%, while the Hybrid CNN-LSTM model had an F1 Score of 97.09% among the proposed FBM. The best-performing model for classifying fake news is Adaboost-Random Forest under FBM.

INTRODUCTION:

The way we access and distribute information has been completely transformed by the Internet. Although the Internet has had many advantages, it has also made it possible for false information and fake news to proliferate quickly. In this day and age, the phrase "fake news" has gained more and more currency. It is nothing more than twisted information that is false and cannot be independently confirmed.

LITERATURE REVIEW:

It is ‘‘news that is intentionally and verifiable false’’ [1] and is disseminated with the goal to deceive people.

Fake news has been around for a while. The ‘‘Great Moon Hoax’’ was one of a number of articles concerning the finding of life on the moon in 1835 that were published in the New York Sun. [2].

However, massive information transmission from several sources, including online newspapers, blogs, social media, magazines, and numerous forums has been facilitated by high internet penetration, making it challenging to assess the veracity of news that has been published. [3].

For instance, fake news became popular after the 2016 U.S. presidential elections. [4].

According to an Ipsos survey by the Centre for International Governance Innovation (CIGI) in over 25 countries, 86% of users acknowledged having come across false information but had at first accepted it as fact. [5].

According to a Microsoft survey, 60% of Indians have come across bogus news online, compared to 57% globally [6]. Fake news is most prevalent in the political realm, but it has since moved to a number of other fields. For instance, a lot of false information was shared about an Australian bushfire in January 2020 as a result of press coverage of the incident. [7].

The COVID-19 pandemic fuelled the fire of false information being shared about the virus's genesis, transmission, symptoms, and treatments. Managing the propagation of fake news while treating the illness proved to be exceedingly challenging for medical personnel. The World Health Organization (WHO) warned of an "infodemic" in addition to the global pandemic because a lot of erroneous information regarding the virus's origin, transmission, treatment, and prevention was being distributed. [8].

For instance, after taking medication, a US citizen who had heard that chloroquine could be able to treat COVID died. [9].

In addition to a newly discovered virus or bacteria, existing diseases like the causes and treatments for cancer, autism, dementia, and urological disorders are also spreadable. [9], [10], [11], [12], [13].

Over 70% of adults use the Internet to look for healthcare-related information, albeit this may not necessarily yield accurate information due to the very high Internet penetration. As it affects human life, the effects of fake news in the health sector may be more detrimental than in other fields. The propagation of false information may have unfavourable effects on patients, healthcare professionals, and the cost of care, among other things. A thorough analysis revealed that false and deceptive health-related information results in people suffering from mental, social, political, and/or economic difficulties. As an illustration, a single piece of false medical information caused at least 800 fatalities and 5,800 hospital admissions. [14].

Thus, the focus of this study is on recognizing false information in the healthcare industry. Two model categories—Content Based Models (CBM) and Feature Based Models (FBM)—have been presented as solutions to this problem. In contrast to FBM, which also takes into account two readability factors along with content, CBM employs the textual content of the articles as its input. For greater accuracy, the two proposed hybrid deep learning models (CNN-LSTM and CNN-BiLSTM) were compared against the performance of different machine learning models for each category.

The remainder of this essay is divided into the following sections. The literature review is in Section II, and the methodology is in Section III. Model construction is covered in Section IV, while model evaluation metrics is covered in Section V. Section VI presents the findings and Section VII presents the analysis of the models created. In Section VIII, the conclusion is delivered.

BACKGROUND STUDY:

The three most researched fields for the classification of fake news are politics, tourism, and marketing, whereas the least researched field is health care. [15].

Due to its importance, spotting fake news in the healthcare industry is more important than in any other field, hence this research concentrates on it and presents the relevant literature. For the purpose of classifying fake news, research in this field can be divided into two categories based on the methods employed: classical machine learning and deep learning.

The performance of multiple machine learning models was compared with the BERT Model using the Health Lies dataset, which contains real and misleading information on a number of diseases like AIDS, cancer,

the Zika virus, cancer, and covid. The findings showed that BERT performed better than all other conventional models. [16].

A Random Forest Classifier with an F1 score of 85% was used to create a classifier to identify bogus news for autism. [17].

The effectiveness of four Deep Learning approaches: CNN, RNN, GRU, and RNN was compared with that of classic machine learning algorithms including Naive Bayes, Nearest Neighbour, Random Forest, Logistics Regression, Adaboost, and Neural Network. The outcomes demonstrate that for the COVID 19 dataset, deep learning methods outperform conventional machine learning algorithms [18].

Cross-SEAN was put forth and evaluated against seven state-of-the-art methods for fake news identification. Cross-SEAN uses semi-supervised models for text categorization and learns from significant external information. With a 0.95 F1 Score on CTF, a significant-scale test, the results revealed that it performed 9% better than the best baseline. Twitter COVID-19 dataset [19].

In [20], in order to distinguish fake news, the effectiveness of conventional machine learning methods such as Multinomial Naive Bayes, Support Vector Machine, Logistic Regression, and Random Forest was compared. For the Covid-19 dataset, conventional and Deep Learning techniques were contrasted to identify bogus news.

The findings demonstrated that deep learning-based algorithms are more effective at identifying bogus news. [21].

After combining linguistic and sentiment characteristics, a classifier was created for COVID-19 that uses Random Forest to identify bogus news. [22].

Using feature selection and a Random tree-based classifier with an F1 score of 94.5%, fraudulent tweets about the Zika virus were identified. [23].

Compared to the healthcare industry, other industries have seen somewhat higher development.

For example, in [24], Word embedding over linguistic characteristics is used in a two-phase method termed WELFake by researchers to identify bogus news using supervised machine learning models. Linguistic traits were used in the initial step to validate the veracity of news information. Voting categorization was carried out in the second stage when word embedding and linguistic feature sets were joined.

The greatest accuracy of the CNN and BERT models for articles in the political area were 92.48% and 93.79%, respectively. The WELFake model's accuracy of 96.73% was greater. The performance of deep learning models (CNN, LSTM) was compared to those of classic machine learning models (Binomial Linear Regression, Naive Bayes Classifier), and a deep learning model achieved an accuracy and F1 score of about 94% and 98%, respectively. [25].

A thorough analysis of the methods currently used to identify fake news was undertaken, along with a comparison of traditional methods (Naive Bayes and Random Forest) with Deep Learning-based techniques like Passive Aggressive and LSTM.

According to the study's findings, LSTM has the highest accuracy (92%; 26). It was suggested to use a content-based transfer learning approach to identify bogus news, and it had a 92% accuracy rate.

Only a little amount of research has been done on creating hybrid models. For instance, a hybrid model for recognizing bogus news was proposed using LSTM and CNN. [28], [29].

Although more models have been developed for other areas, it has been found that there have been few research using limited methodologies in the healthcare sector for fake news identification. Therefore, this research fills in this vacuum by creating a highly accurate fake news classifier tailored exclusively for the healthcare industry.

METHODOLOGY:

Building Content Based and Proposed Feature Based models utilizing machine learning and Deep Learning techniques is the proposed study methodology shown in Fig. 1. In the first scenario, only the content (i.e., fake news) is utilized to create the models; however, for feature-based models, extra readability features are

supplied as input along with the content to create models, and their performance is compared.

1. Data Collection

Open datasets are widely available for the research of fake news in the political sphere, but they are incredibly rare and sparse in the healthcare sphere. The HealthLIES dataset is a well-known example of a publicly accessible dataset. It consists of 12,267 phrases that are classified as true or false depending on whether they contain accurate health information or incorrect information about health.

Sentences from diverse online sources, such as social media, news stories, and health-related websites, were collected to construct the HealthLIES dataset [30].

Additionally, the Fake News Healthcare (FNH) dataset, which focuses on false information in the healthcare sector, has been assembled [31].

This dataset consists of 9581 labelled news articles, of which 7765 are authentic and 1816 are fraudulent. The dataset also contains further details like the URL, article title, and word count. The FNH dataset contains samples of both fake and real news, which were gathered from reliable websites including theonion.com and PolitiFact for fake news samples and CNN, BBC News, and The Atlantic for real news samples. The FNH dataset was chosen for this study due to the additional data that is accessible and will be used to create models.

2. Data Augmentation

The FNH has two classes: True and Fake, and is a severely unbalanced dataset. The data was split between true news (76.4%) and false news (23.6%). The ratio of imbalance for the FNH dataset was 4:1 when comparing the number of documents that contain actual news to those that do not.

The accuracy of the results is impacted by this kind of dataset imbalance, making it impossible to create reliable models.

To solve this issue and create a balanced and useful dataset, data augmentation techniques must be used to randomly duplicate samples from the minority class. By creating synthetic data from the existent data, data augmentation is used to balance the dataset [32].

This approach is common in computer vision, but it is more challenging in natural language processing (NLP) because it requires comprehension of the text's grammatical structure [33]. One of the most popular augmentation techniques for textual data is the Easy Data Augmentation (EDA) method [34].

Using WordNet, "n' words—other than stop words—are chosen from the phrase and substituted with random synonyms. In this study, EDA was used to supplement the data. The final dataset after augmentation had 7765 authentic articles and 7625 fraudulent ones.

3. Data Pre-Processing

Obtaining a proper set of tokens for each article came after the dataset had been balanced. The numbers and other special characters were eliminated to achieve this. Stop words and punctuation are left in place since they add context to the text and help with feature extraction by incorporating word embedding. Lemmatization was finally used to extract the root words. Using this preprocessing, a list of legitimate tokens was produced.

4. Feature Extraction

In conventional machine learning and deep learning models, feature extraction is carried out using Term Frequency- Inverse Document Frequency (tf-idf) and GloVe Word Embeddings, respectively. For FBM, readability features were extracted.

PROPOSED MODEL

The creation of classifier models is suggested in this part under two headings: content-based models and feature-based models, as shown in Fig 1. To find the best classifier for identifying fake news, the

effectiveness of conventional machine learning algorithms is compared with the suggested deep learning methods for both categories. We may examine the performance of both the CBM and FBM categories using conventional machine learning models including Decision Tree, Random Forest, Support Vector Machine, and AdaBoost Decision tree and AdaBoost Random Forest models were developed.

1) DECISION TREE-

Using a hierarchical tree structure, decision trees are a modelling tool that may be used to create regression or classification models. While building a decision tree, it repeatedly divides a dataset into progressively smaller sections. The decision and leaf nodes, each of which represents a categorization or choice, are included in the final tree. The decision tree's root node, which stands for the best predictor, is located at the top. Information Gain is the term used to describe the process of splitting data by entropy.

Since decision trees are non-parametric and can process both numerical and categorical data, they can successfully manage huge and complex datasets without imposing a sophisticated parametric framework.

2) RANDOM FOREST-

The supervised learning method Random Forest builds an ensemble of decision trees using the "bagging" method. This approach uses various learning models to enhance the final result. A third of the samples, referred to as out-of-bag samples, are used to test the model after replacing the samples used to sample the data.

The Gini index can be used to determine the dataset's impurity, with the root node chosen as the feature. For each decision tree, Scikit-learn calculates the Gini Importance of each node under the assumption that the tree is binary and has only two child nodes.

3) SUPPORT VECTOR MACHINE-

A Support Vector Machine (SVM) is a classification method that looks for a hyperplane that divides the data points into various categories in an N-dimensional space.

The goal is to create an ideal decision border or line for the precise classification of new data points, and the size is dictated by the number of features. The "hyperplane" is the name of the best choice boundary.

The linear kernel performs exceptionally well in cases when there are many features, such as in text classification tasks.

The majority of alternative kernel functions are slower than the linear kernel functions. The decision boundary of the SVM is defined by this equation.

4) ADABOOST-

AdaBoost is an ensemble learning technique that combines different classifiers to increase the accuracy of classifiers.

By combining numerous weak classifiers, the AdaBoost classifier creates a strong and robust classifier that is extremely accurate and dependable. AdaBoost's main idea is to train data samples and build classifier weights in order to make accurate predictions for unusual observations. A basic classifier in AdaBoost can be any machine learning technique that accepts training set weights.

5) CNN-LSTM MODEL-

This paper proposes a hybrid model that combines both CNN and LSTM, as seen in Fig 2. The embedding layer comes first, then a one-dimensional CNN layer (Conv1D). Using 64 filters and a kernel size of 5, this layer extracts local features using the ReLU activation function. Large feature vectors are produced as a result, and these feature vectors are used as input by the MaxPooling 1D layer with a four-window size. The feature vectors' dimension can be reduced as a result.

The pooled feature maps are fed into two LSTM layers, which output the input feature maps' long-term dependent features while conserving memory.

Each LSTM layer has a linear activation function and has 20 neurons with a 20-by-20 output dimension. With the help of a dense layer that reduces the output space dimension to one and uses the sigmoid activation function to indicate the classification label (fake or not fake), the learned feature vectors are ultimately classified. Cross entropy is used as the loss function and the Adam optimizer is used to train the model.

6) HYBRID CNN-BILSTM MODEL

The architecture of the model is the same as that of the hybrid CNN-LSTM model. The only change is the Bi-directional LSTM layer being used in place of the LSTM layers, as shown in Fig 3. It uses a variety of layers, beginning with the word-embedding layer and continuing with the CNN layer, max pooling layer, bi-directional LSTM layer, and dense layer, to achieve classification. The input for a bi-directional LSTM moves in both directions and contains both historical and current data. The production can then be more significant as a result.

MODEL EVALUATION METRICS

Accuracy, Precision, Recall, and F1 Score were the four metrics that were used to assess the model's performance.

Four estimation parameters were used to assess the model: True Positive (TP), True Negative (TN), False Positive (FP), and False Negative (FN). genuine positive results happen when the model successfully predicts the positive class, while genuine negative results happen when the model appropriately describes the negative class. A false positive result happens when the model estimates the positive class wrong, and a false negative result happens when the model predicts the negative class incorrectly.

REFERENCES

- Staudemeyer R.C., Voyiatzis A.G., Moldovan G., Suppan S.R., Lioumpas A., Calvo D. *Human-Computer Interaction and Cybersecurity Handbook.* CRC Press; Boca Raton, FL, USA: 2018. Smart cities under attack.
- Podgorelec B., Turkanović M., Karakatič S. A machine learning-based method for automated blockchain transaction signing including personalized anomaly detection. *Sensors.* 2020;**20**:147.
- Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008.
- Farrugia S., Ellul J., Azzopardi G. Detection of illicit accounts over the Ethereum blockchain. *Expert Syst. Appl.* 2020;**150**:113318.
- Ostapowicz M., Żbikowski K. Detecting fraudulent accounts on blockchain: A supervised approach; Proceedings of the International Conference on Web Information Systems Engineering; Hong Kong, China. 19–22 January 2020; Cham, Switzerland: Springer; 2020. pp. 18–31
- Aziz A.S.A., Hassanien A.E., Azar A.T., Hanafy S.E. Genetic Algorithm with Different Feature Selection Techniques for Anomaly Detectors Generation; Proceedings of the 2013 Federated Conference on Computer Science and Information Systems (FedCSIS); Kraków, Poland. 8–11 September 2013
- Hassanien A.E., Tolba M., Azar A.T. *Communications in Computer and Information Science.* Volume 488. Springer; Berlin/Heidelberg, Germany: 2014. Advanced Machine Learning Technologies and Applications: Second International Conference, AMLTA 2014, Cairo, Egypt, 28–30 November 2014.
- Khan H., Asghar M.U., Asghar M.Z., Srivastava G., Maddikunta P.K.R., Gadekallu T.R. Fake review classification using

supervised machine learning; Proceedings of the International Conference on Pattern Recognition; Virtual Event. 10–15 January 2021; Cham, Switzerland: Springer; 2021. pp. 269–288.

- Shahbazi Z., Hazra D.P., Park S., Byun Y.C. Toward Improving the Prediction Accuracy of Product Recommendation System Using Extreme Gradient Boosting and Encoding Approaches. *Symmetry.* 2020;**12**:1566.
- Pesantez-Narvaez J., Guillen M., Alcañiz M. Predicting motor insurance claims using telematics data—XGBoost versus logistic regression. *Risks.* 2019;**7**:70.
- Li J., Gu C., Wei F., Chen X. A Survey on Blockchain Anomaly Detection Using Data Mining Techniques; Proceedings of the International Conference on Blockchain and Trustworthy Systems; Guangzhou, China. 7–8 December 2019; Singapore: Springer; 2019.
- Reid F., Harrigan M. *Security and Privacy in Social Networks.* Springer; New York, NY, USA: 2013. An analysis of anonymity in the bitcoin system; pp. 197–223
- Ngai E.W.T., Hu Y., Wong Y.H., Chen Y., Sun X. The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. *Decis. Support Syst.* 2011;**50**:559–569.
- Saia R., Carta S. Evaluating Credit Card Transactions in the Frequency Domain for a Proactive Fraud Detection Approach; Proceedings of the 14th International Conference on Security and Cryptography (SECRYPT 2017); Madrid, Spain. 26–28 July 2017; pp. 335–342
- Sánchez D., Vila M.A., Cerda L., Serrano J.M. Association rules applied to credit card fraud detection. *Expert Syst. Appl.* 2009;**36**:3630–3640.
- Gyamfi N.K., Abdulai J.D. Bank fraud detection using support vector machine; Proceedings of the 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON); Vancouver, BC, Canada. 1–3 November 2018; pp. 37–41
- Panigrahi S., Kundu A., Sural S., Majumdar A.K. Credit card fraud detection: A fusion approach using Dempster–Shafer theory and Bayesian learning. *Inf. Fusion.* 2009;**10**:354–363.
- Shi F.B., Sun X.Q., Gao J.H., Xu L., Shen H.W., Cheng X.Q. Anomaly detection in Bitcoin market via price return analysis. *PLoS ONE.* 2019;**14**:e0218341.
- Kumar P., Gupta G.P., Tripathi R. TP2SF: A Trustworthy Privacy-Preserving Secured Framework for sustainable smart cities by leveraging blockchain and machine learning. *J. Syst. Archit.* 2021;**115**:101954.
- Zhao Y., Tarus S.K., Yang L.T., Sun J., Ge Y., Wang J. Privacy-preserving clustering for big data in cyber-physical-social systems: Survey and perspectives. *Inf. Sci.* 2020;**515**:132–155
- Alkadi O., Moustafa N., Turnbull B., Choo K.K.R. A deep blockchain framework-enabled collaborative intrusion detection for protecting IoT and cloud networks. *IEEE Internet Things J.* 2020;**8**:9463–9472.
- AlKadi O., Moustafa N., Turnbull B., Choo K.K.R. Mixture localization-based outliers models for securing data migration in cloud centers. *IEEE Access.* 2019;**7**:114607–114618.
- Keshk M., Sitnikova E., Moustafa N., Hu J., Khalil I. An integrated framework for privacy-preserving based anomaly detection for cyber-physical systems. *IEEE Trans. Sustain. Comput.* 2019;**6**:66–79.
- Kurakin A., Goodfellow I., Bengio S. Adversarial machine learning at scale. *arXiv.* 20161611.01236
- Biggio B., Roli F. Wild patterns: Ten years after the rise of adversarial machine learning. *Pattern Recognit.* 2018;**84**:317–331.

- Xuan S., Liu G., Li Z., Zheng L., Wang S., Jiang C. Random forest for credit card fraud detection; Proceedings of the 2018 IEEE 15th International Conference on Networking, Sensing and Control (ICNSC); Zhuhai, China. 27–29 March 2018; pp. 1–6
- Liu C., Chan Y., Alam Kazmi S.H., Fu H. Financial fraud detection model: Based on random forest. *Int. J. Econ. Financ.* 2015;**7**:178–188.
- Apruzzese G., Andreolini M., Colajanni M., Marchetti M. Hardening random forest cyber detectors against adversarial attacks. *IEEE Trans. Emerg. Top. Comput. Intell.* 2020;**4**:427–439. 29. Primartha R., Tama B.A. Anomaly detection using random forest: A performance revisited; Proceedings of the 2017 International Conference on Data and Software Engineering (ICoDSE); Palembang, Indonesia. 1–2 November 2017; pp. 1–6.
- Laskov P. Practical evasion of a learning-based classifier: A case study; Proceedings of the 2014 IEEE Symposium on Security and Privacy; San Jose, CA, USA. 18–21 May 2014; pp. 197–211.
- Pham T., Lee S. Anomaly detection in bitcoin network using unsupervised learning methods. *arXiv.* 20161611.03941
- Martin K., Rahouti M., Ayyash M., Alsmadi I. Anomaly detection in blockchain using network representation and machine learning. *Secur. Priv.* 2022;**5**:e192.
- Pinzón C., Rocha C. Double-spend attack models with time advantange for bitcoin. *Electron. Notes Theor. Comput. Sci.* 2016;**329**:79–103.
- Bitcoin Network Transactional Metadata. [(accessed on 12 September 2022)].
- Shafiq O. *Master's Thesis*. Tampere University; Tampere, Finland: 2019. Anomaly Detection in Blockchain.
- Chawla N.V., Bowyer K.W., Hall L.O., Kegelmeyer W.P. SMOTE: Synthetic minority over-sampling technique. *J. Artif. Intell. Res.* 2002;**16**:321–357.
- Sadaf K., Sultana J. Intrusion detection based on autoencoder and isolation Forest in fog computing. *IEEE Access.* 2020;**8**:167059–167068.
- Eyal I., Sirer E.G. Majority is not enough: Bitcoin Mining is vulnerable; Proceedings of the International Conference on Financial Cryptography and Data Security; Christ Church, Barbados. 3–7 March 2014; Berlin/Heidelberg, Germany: Springer; 2014. pp. 436–454.
- Landa R., Griffin D., Clegg R.G., Mykoniati E., Rio M. A Sybilproof indirect reciprocity mechanism for peer-to-peer networks; Proceedings of the IEEE INFOCOM 2009, Rio De Janeiro; Brazil. 24 April 2009; pp. 343–351
- Luu L., Chu D.-H., Olickel H., Saxena P., Hobor A. Making smart contracts smarter; Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security; Vienna, Austria. 24–28 October 2016.
- Nizamuddin N., Hasan H., Salah K., Iqbal R. Blockchain-based framework for protecting author royalty of digital assets. *Arab. J. Sci. Eng.* 2019;**44**:3849–3866.
- Halo Block, Medium How To Use Oyente, a Smart Contract Security Analyzer—Solidity Tutorial. 2020.