Integration of Artificial Intelligence in the Advancement of
Science and Engineering
July 2024

"MACHINE LEARNING TECHNIQUE FOR SOCIAL MEDIA FAKE PROFILE DETECTION"

Abhimanyu Nayak (abhin.rs.cse19@bitsindri.ac.in)
PhD Scholar B.I.T Sindri Dhanbad-828123
GUID-Prof.(Dr) D.K.Singh(dksingh.bits@gmail.com)
V.C.J.U.T Ranchi Jharkhand 834010

Abstract

Fake profiles, which propagate misinformation, swindle, and manipulate public opinion, have become a major issue on social media. In addition to phishing and identity theft, they propagate gossip. The creator of this research will discuss a machine learning detection algorithm that uses data such as the number of followers and friends, status updates, and other metrics to identify Twitter accounts that engage in phone-based advertising. The following categories were used to classify Twitter accounts: TFP, E13, INT, TWT, and FSF. Brain networks, Long Short-Term Memory, XG Boost, and Random Forest are all explored by the writer. Key characteristics are found in order to assess the authenticity of social media profiles. Architecture and hyperparameters are covered. Finally, model training yields outcomes. Thus, authentic profiles output 0 and bogus profiles 1 respectively. Fake profiles can be deactivated or deleted to prevent cyber security issues. For implementation, NumPy, Pandas, and Sklearn are used with Python. The author will reason that XG Lift is the best machine learning strategy for locating telephone pay profiles based on this investigation. N An extensive collection of social media profiles demonstrates that the recommended approach can accurately and consistently identify phone pay accounts with high recall and precision. The findings show that machine learning can improve social media security and integrity, making the internet safer.

Keywords: *Machine Learning, Social Media, Fake Profile, Detection*

1. INTRODUCTION

Social media has revolutionized global communication, enabling unparalleled connectivity and information exchange. Facebook, Twitter, and Instagram influence public conversation and social dynamics in personal, professional, and political domains. Despite these benefits, social media has also brought new issues, particularly false profiles. Misinformation, fraud, public opinion

manipulation, and cyber harassment are common uses of these fake accounts. Fake profiles damage social media trust, making their discovery and eradication essential. Manual verification and heuristic-based approaches to detecting false profiles cannot keep up with the expanding scope and sophistication of these fraudulent operations. Heuristic-based solutions, which use established rules and patterns, are routinely bypassed by increasingly sophisticated phone pay profile building tools, and manual verification is laborious and impracticable for large-scale applications. This highlights the need for more advanced and scalable solutions, driving the use of machine learning to detect bogus social media profiles.

Machine learning, a branch of AI, can find complicated patterns and anomalies in vast datasets. This permits programmed discovery of small signs that recognize counterfeit profiles from genuine ones. Choice trees, support vector machines, and brain organizations can be prepared on named datasets with phony and genuine profiles. Fake profiles include irregular posting patterns, unusual user interactions, and suspect network connections, which these models learn to identify. However, unsupervised learning can reveal hidden patterns in unlabeled data, revealing phone pay accounts' structural and behavioral irregularities. This research investigates machine learning methods for social media false profile detection. Using supervised and unsupervised learning models, we test various techniques for detecting bogus accounts. This approach relies on feature extraction to identify crucial traits that indicate fraudulent profiles. These variables may include post frequency and timeliness, user-generated content sentiment analysis, network structure, and user interactions. The suggested system seeks to detect and respond in real time and be robust and scalable.

2. REVIEW OF LITREEATURE

Ahmad et al. (2020) investigate machine learning ensemble approaches for fake news identification. Their research emphasises the need of integrating algorithms to increase detection system accuracy and robustness. Ensemble learning uses decision trees, support vector machines, and neural networks to combine their strengths and mitigate their faults. This thorough strategy improves the system's ability to recognise bogus news, improving precision and recall. Ahmad et al. found that ensemble algorithms can handle fake news detection complexity, providing a scalable solution for real-time social media applications.

Ali et al. (2022) present a broad overview of social media fake news detection methods. Their review divides methodologies into content-based, context-based, and hybrid. Content-based methods use NLP to identify fraudulent news stories based on their text and language. However, context-based approaches evaluate source credibility and social network news transmission. The survey also emphasises hybrid content-context analysis methods that boost detection accuracy. Current solutions are limited by the dynamic nature of fake news and malevolent actors' evasion attempts, according to Ali et al. They illuminate the state of false news identification and suggest further research.

Aslam et al. (2021) introduce "Fake Detect," a deep learning ensemble model for fake news identification. Their model uses CNNs and RNNs to capture news content's geographical and temporal properties. The ensemble model uses CNNs' hierarchical structure to extract high-level textual features and RNNs' sequential nature to grasp context and flow. This dual strategy helps the model recognise bogus news better than typical machine learning. Aslam et al. evaluate their model using large datasets and show its efficacy in real-world circumstances, suggesting its use in social media monitoring systems.

Balaji et al. (2021) review social media analysis machine learning algorithms, covering their methods and uses. They explore supervised, unsupervised, and reinforcement learning techniques for sentiment analysis, trend prediction, and anomaly detection. Machine learning can analyse social media data and address issues like phoney profiles and fake news, according to the report. Balaji et al. stress the need for algorithm development innovation to keep up with social media.

3. OBJECTIVES

- To Develop a machine learning model using LSTM, XG Lift, Random Backwoods, and Neural Organizations to recognize false Twitter accounts through devotee/companion numbers and status updates.
- To Identify key elements of authentic social media profiles, including interaction patterns and follower metrics.
- To Optimize machine learning algorithm architecture and hyperparameters for enhanced detection accuracy.

- To Train the model on actual and false profiles, evaluate its performance, and find XG Boost the most effective strategy for detecting phone pay profiles.

4. METHDOLOGY

In this model, XG Boost, a random forest and profile-focused multi-layered neural network features were applied. CSV files with extracted characteristics are simply read by the model. Finally, model training, testing, and analysis conclude whether a profile is real. Because Google Colab offers free GPU access, researchers picked it to develop models. The 12-GB Google Colab NVIDIA Tesla K80 GPU runs for 12 hours. This technique identifies fraudulent profiles well. This model may be more accurate after training than comparable research. Beautiful frameworks are also emphasised in this design.

4.1 Dataset Collection

Author utilized MIB dataset. The data collection had 3474 real and 3351 fake profiles. For legitimate accounts, the dataset utilised E13 and TFP, while for fraudulent ones, it utilised TWT, INT, and FSF. For machine extraction, CSV files are utilised.

See Figure 2's indicator x-axis for false profile recognition qualities. Selection occurred during preprocessing. Y-axis shows number of entries for each dataset feature**.**

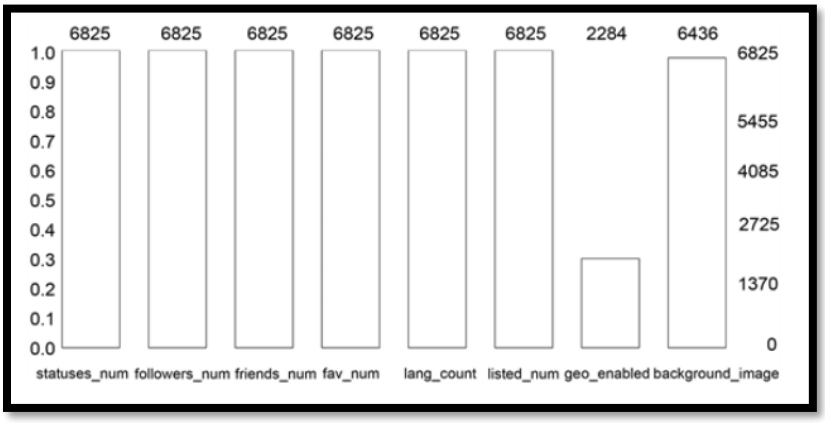

Figure 1: Dataset

4.2 Model Development

This section covered the author's method for identifying phoney accounts by concentrating on their traits. The adjacency matrix of the social network graph was first computed. Next, depending on their network friends, nodes (members of social networks) were compared to see how similar they were. Then, for every metric—common friends, Jaccard, cosine, and any other pertinent measurements—similarity matrices were made. The similarity of the nodes was displayed by several matrices.

Normalcy was applied to the data due to its unequal distribution and the fact that 98-99% of it corresponds to the majority class (ordinary users). The accuracy of classification and the minority class (false subscribers) are both made more difficult to understand by this. This difficulty was solved by using the SMOTE to balance the statistics.

4.3 Proposed Methodology

The author identified fake Twitter profiles using several supervised algorithms with varied degrees of accuracy. Each model may detect a bogus profile using visible features. Each supervised model's accuracy and loss graphs use the same data. Several model accuracy comparison graphs are also shown. Model training utilizes appropriate optimization strategies, misfortune capabilities, and logical operations. This list describes the models used.

4.4.1 Pre-Processing

Before modelling, the author performs one more preprocessing step. Before being fed to a model, data is preprocessed. The appearance of a profile is used to verify its authenticity. All specifics are set. Only numerical data remains after categorical elimination. The author selects the following traits.

friends	status count	fav num	geo enable	listed count	followers	lang count

A Boolean variable called “isFake” is added to each profile of accurate and inaccurate users. The Y variable stores profile X answer. Finally, zeros replace blanks and NANs.

4.4.2 Artificial Neural Network

Deep learning neural network systems aim to reproduce brain activity by simulating individual neurons. Neuralinks are present in each and every layer of neural networks. Keras was used consecutively by the author. Aside from the input and output layers, the model also has three hidden layers. Any one of them can turn on independently of the output layer. The sigmoid function activates the output layer. When building the model, we consulted the Binary Merge Loss Function and the Adam Optimizer. This model's architecture makes use of ANN. Finally, the sigmoid function predicts if a profile is phone pay or real and returns a value between 0 and 1.

Hyper parameters

Piecewise linear factors indicate corrected activation functions. ReLU is generally the primary neural network learning algorithm since it is easy to train and performs well.

4.4.3 Random Forest

Random forest (or random-decision forest) ensemble learning is a component of this technique. It is used in machine learning because it is simple to apply to regression and classification. Each decision tree's forecasts are used by the random woodland, which predicts the outcome based on the majority of estimates. Notwithstanding, random-timberland produces far additional decision trees than the decision tree strategy, and the final result appears to be the average of nearly all of them. For profile identification, the author used random woods. Meaningful disclosures are generated by the model after data handling. To fit the data, the bootstrap aggregating system is used with the X=x1,x2,⋯,xn and Y=y1,y2,⋯,yn reaction trees (fb). At foreordained intervals (B times), a random sample is picked. The accompanying approach is used to choose the sample(x') results after training:

4.4.4 Extreme Gradient Boost

XG Boost is another regression ensemble learning method. This algorithm subsamples Stochastic Gradient boosting parameters.

Random forest has the limitation of only functioning well with complete inputs or without any missing data. To get around this, the author employs gradient boosting.

The boosting technique initialises F0(x).

$$f_0(x) = \arg\min_\gamma \sum_{i=1}^{n} L(y_i, \gamma)$$

Later, the loss function gradient is determined iteratively.

$$\gamma_{im} = -\alpha \left[\frac{\delta L(y_i, F(x_i))}{F(x_i)} \right]$$

Lastly, it defines the boosted model Fm(X).

$$F_m(x) = F_{m-1}(x) + \gamma_m h_m(x)$$

The learning rate is α.

The multiplicative factor is γn.

4.4.5 Long Short-Term Memory

In order to determine if a profile is genuine, the author came up with an LSTM-based approach that uses tweets. Using this website and tweets to train an LSTM, the author oversaw the filter that removes tweet IDs.

Letters are written in lowercase on all tokens.

Tweets cannot contain stop words anymore.

The author proceeded to vectorize the sentences of these blockchain-enabled tweets by applying an embedding layer. The output is generated by advancing the 32-dimensional vector output of the LSTM through sigmoid-triggered layers.

5. EXPERIMENTAL RESULTS AND DISCUSSION

The training and testing results for each model are listed below. We present model accuracy comparisons, misfortune against eras graphs, stochastic woodland, XG help, and other ROC bends, as well as model comparisons for the LSTM neural organization.

5.1 Neural Network

The trained neural network's accuracy and loss graphs are shown in both Figures 2 and 3

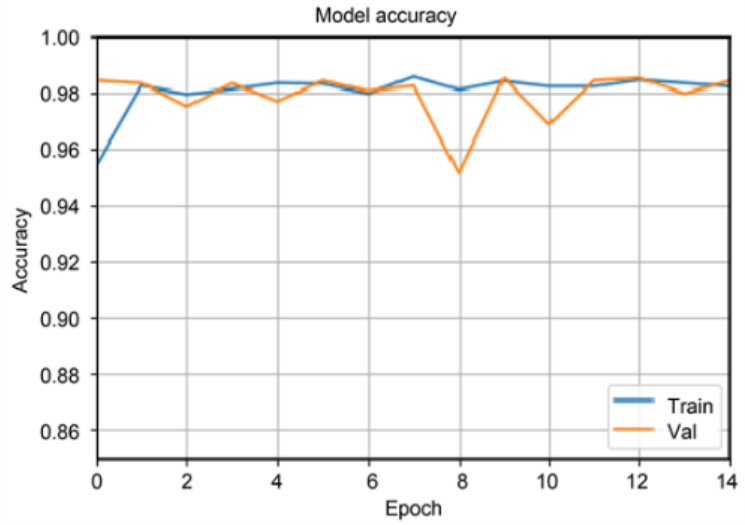

Figure 2: Model precision.

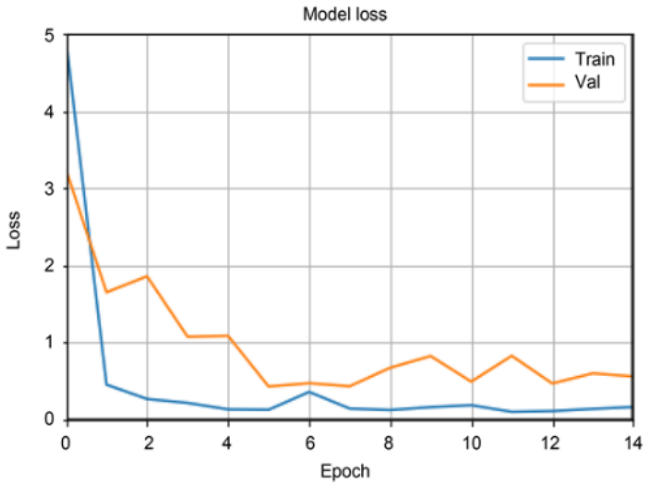

Figure 3: Model loss.

The aforementioned loss and accuracy graphs represent the end product of fifteen operational epochs. While it starts at 0.97, accuracy peaks at 0.98 and fluctuates throughout. After showing a local minimum of less than 0.5, the loss graph starts at 1 for the test dataset and 4 for validation. Loss is calculated using binary cross-entropy. Before weighting each characteristic, the machine gives random weights.

5.2 Random Forest and Other Approaches

The accuracy of decision trees, boost, random forests, and ada boosts are contrasted in Figure 4. The highest precision is produced with XG boost (0.996). Random forests and decision trees both have 0.99 accuracy. At last, the writer secures assistance from the ADA.

Figure 4 shows the accuracy comparison, while Figures 5 and 6 provide the ROC curve graphics.

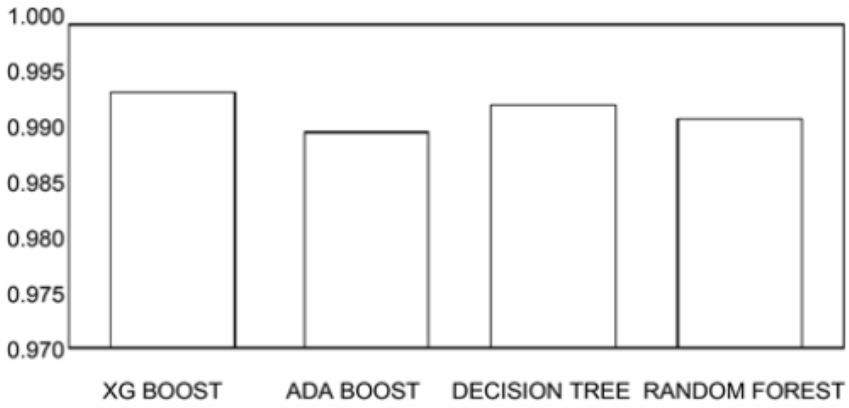

Figure 4: Accuracy of different models.

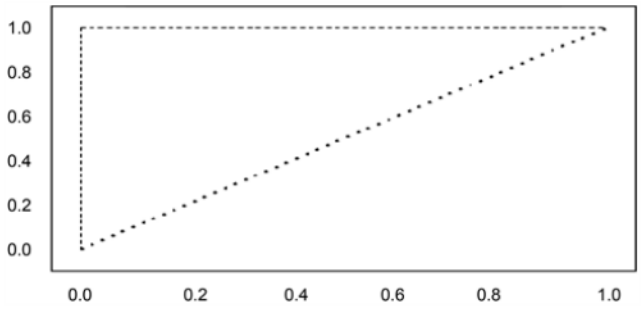

Figure 5: XG boost ROC curve.

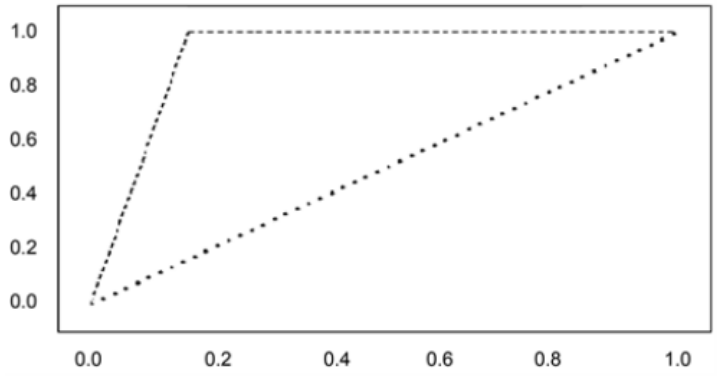

Figure 6: ROC curve for a random forest.

6. CONCLUSION

Using techniques including LSTM, XG Boost, Random Forest, and Neural Networks, this study created a strong machine learning model to identify phoney Twitter profiles, tackling the serious problem of phoney profiles that disseminate false information and influence public opinion. Finding essential components of genuine profiles, enhancing algorithm performance, and testing the models on a sizable dataset of real and fictitious profiles were among the main goals. The approach comprised profile-specific features and supervised learning techniques. SMOTE was used to preprocess and balance the data, and Google Colab's free GPU was used to train the models. According to experimental data, XG Boost fared better than other models in identifying phoney profiles, attaining the highest recall and precision rates. This demonstrates the superiority of XG Boost in detecting fake profiles and the usefulness of ensemble approaches in challenging detection tasks. By successfully detecting and disabling phoney personas, the study illustrates how machine learning may improve social media security and integrity and promote a safer online environment.

REFRENCES

1. Ahmad, I., Yousaf, M., Yousaf, S., & Ahmad, M. O. (2020). Fake news detection using machine learning ensemble methods. Complexity, 2020(1), 8885861.
2. Ali, I., Ayub, M. N. B., Shivakumara, P., & Noor, N. F. B. M. (2022). Fake news detection techniques on social media: A survey. Wireless Communications and Mobile Computing, 2022(1), 6072084.
3. Aslam, N., Ullah Khan, I., Alotaibi, F. S., Aldaej, L. A., & Aldubaikil, A. K. (2021). Fake detect: A deep learning ensemble model for fake news detection. complexity, 2021(1), 5557784.

4. Balaji, T. K., Annavarapu, C. S. R., & Bablani, A. (2021). Machine learning algorithms for social media analysis: A survey. Computer Science Review, 40, 100395.
5. Della Vedova, M. L., Tacchini, E., Moret, S., Ballarin, G., DiPierro, M., & De Alfaro, L. (2018, May). Automatic online fake news detection combining content and social signals. In 2018 22nd conference of open innovations association (FRUCT) (pp. 272-279). IEEE.
6. Kaliyar, R. K., Goswami, A., & Narang, P. (2021). FakeBERT: Fake news detection in social media with a BERT-based deep learning approach. *Multimedia tools and applications*, *80*(8), 11765-11788.
7. Mishra, S., Shukla, P., & Agarwal, R. (2022). Analyzing machine learning enabled fake news detection techniques for diversified datasets. Wireless Communications and Mobile Computing, 2022(1), 1575365.
8. Mohammadrezaei, M., Shiri, M. E., & Rahmani, A. M. (2018). Identifying fake accounts on social networks based on graph analysis and classification algorithms. Security and Communication Networks, 2018(1), 5923156.
9. Monti, F., Frasca, F., Eynard, D., Mannion, D., & Bronstein, M. M. (2019). Fake news detection on social media using geometric deep learning. arXiv preprint arXiv:1902.06673.
10. Ozbay, F. A., & Alatas, B. (2020). Fake news detection within online social media using supervised artificial intelligence algorithms. Physica A: statistical mechanics and its applications, 540, 123174.
11. Ramalingam, D., & Chinnaiah, V. (2018). Fake profile detection techniques in large-scale online social networks: A comprehensive review. Computers & Electrical Engineering, 65, 165-177.
12. Sahoo, S. R., & Gupta, B. B. (2021). Multiple features based approach for automatic fake news detection on social networks using deep learning. Applied Soft Computing, 100, 106983.
13. Shu, K., Zhou, X., Wang, S., Zafarani, R., & Liu, H. (2019, August). The role of user profiles for fake news detection. In Proceedings of the 2019 IEEE/ACM international conference on advances in social networks analysis and mining (pp. 436-439).
14. Thota, A., Tilak, P., Ahluwalia, S., & Lohia, N. (2018). Fake news detection: a deep learning approach. SMU Data Science Review, 1(3), 10.
15. Van Der Walt, E., & Eloff, J. (2018). Using machine learning to detect fake identities: bots vs humans. IEEE access, 6, 6540-6549.