LSTM-RNN Based Identification of Fake Profile in social media

Abirami S[1, *], Abinaya S[1], Divya Sruthi R[1], Gurupriyadharshini R[1].

[1]Department of Computer Science & Engineering, PSNA college Of Engineering & Technology, Dindigul-624001, India

[1,*]email: abiramilingam2018@gmail.com, Tel. :9361900490

ABSTRACT

The increasing prevalence of fake profiles in social media has become a major concern for users and platform operators alike. In this work, we propose an LSTM-RNN based system for fake profile identification in social media. Our model is trained on a large dataset of real and fake profiles, allowing it to learn the patterns and characteristics that distinguish between them. The performance of our model was evaluated on a validation dataset and found to be highly accurate.

Keywords - LSTM-RNN, Online Identity, Social Network Analysis, User Authentication, User Behavior, User Profiling, User Verification.

1. INTRODUCTION

The widespread use of social media platforms has led to an increase in the number of fake profiles created for various reasons, such as social engineering attacks, identity theft, and cyberbullying. Recent advances in deep learning, particularly in the area of recurrent neural networks (RNNs), have provided a promising solution for fake profile identification. Long short-term memory (LSTM) is a type of RNN that has been shown to effectively model sequential data and capture long-term dependencies. In this paper, we propose an LSTM RNN-based approach for fake profile identification. We train our model on a large dataset of social media profiles and use it to classify profiles as either genuine or fake. Our approach takes into account various features such as profile information, user behavior, and network structure. We conduct experiments to evaluate the performance of our model and compare it with state-of-the-art methods for fake profile identification. The proposed LSTM RNN-based approach offers several advantages over traditional methods, including its ability to handle complex and variable-length input data, capture temporal dependencies, and adapt to new data. The results of our experiments demonstrate the effectiveness of our approach and its potential for use in real-world applications. Overall, this paper provides a novel and effective approach for fake profile identification using LSTM RNNs, which can significantly improve the security and reliability of social media platforms.

2. LITERATURE SURVEY

In this paper, Aayush Sunil Chamria, Abhishek Dinesh Mane, Prithvi Vadiraj Dambal, Smita Bharne [1] has proposed a system for detecting Fake Profile in Online Social Networks using Ensem Stack Classification Algorithm. These platforms are referred to as dynamic because their user bases are growing daily. The key advantage of online social networking is the ability to interact more effectively and interact with others. On OSN platforms like Facebook, Instagram, LinkedIn, and Twitter, users are sharing data, photographs, and private information. Criminals employ OSN platforms for cutting-edge attack strategies like phoney identities, misinformation, and many others. The proposed model, it is based on Ensem Stack's categorization mode, has the potential to more accurately determine if an OSN account is authentic or false. So, our algorithm uses the input from an Instagram user account to extract all the necessary information to determine if the account is real or fraudulent. The main goal of the proposed method is to use machine learning to conclusively prove the existence of these bogus profiles in these OSNs. The malpractices can be stopped by removing these false profiles.

Latha P, Sumitra V, Sasikala V J. Arunarasi [2] has proposed a Fake Profile Identification in Social Network using Machine Learning and NLP. These social networking sites are seeing a sharp rise in the number of users, and many of them are connecting with one another wherever they are and at any time. These social media platforms offer security issues for our information as well as positives and cons. We need to categorize these social networking accounts into real accounts and fraudulent accounts in order to investigate who is posing threats on these networking sites. In the past, we have used various categorization techniques to identify phoney social media profiles. Therefore, we must improve our ability to spot phoney accounts on these websites. In order to improve the accuracy rate of identifying bogus accounts, use machine learning technologies and natural language processing (NLP) in our study and choose Random Forest tree classifier algorithm. The main use of machine learning technologies and natural language is to improve, accelerate, and automate the underlying text analytics functions and NLP features that turn unstructured text into usable data and insights.

X. Jose, S. Kumar and P. Chandran [3] have proposed a characterization, classification and Detection of Fake News in Online Social Media Network. Admittedly, this has resulted in the widespread dissemination of fake news, or purposefully inaccurate or deceptive information. Fake news is an urgent problem since it has detrimental effects on both individual users and society as a whole. The OSM networks have a quick distribution of news content, thus identification systems should anticipate news items as soon as possible to prevent the spread of misleading information. Detecting fraudulent news on social media networks is therefore very important and technically difficult. In this article, we've covered the various traits and variants of fake news and have placed a practical approach to spotting it on OSM networks. The primary two factors of the solution are the stance detection model and the faked content classifier. The synthetic content classifier's accuracy with bi-directional LSTM was 93.46%, while the stance detection model's accuracy with logistic regression was 90.37%.

De Oliveira, Nicollas R., Pedro S. Pisa, Martin Andreoni Lopez, Dianne Scherly V. de Medeiros, and Diogo M. F. Mattos [4] has proposed a identifying Fake News on Social Networks Based on Natural Language Processing. In order to guarantee the preciseness of the information, we offer in this study the key algorithms and methodologies that aid in the linguistic definition and detection of false news on social networks. The study analyses the phenomenon's characteristics looks into how it spreads on social media, and offers tools and algorithms for spotting fake news. The dominant issue that influences the propagation of false news is how simple it is to generate it online as opposed to through more established media venues like newspapers or television. Thus, even if journalists can identify fake news manually, we emphasis on automatic identification using computational tools in our study. The user does not have access to models for how content is distributed or for how users are regarded. The quality criteria employed in the knowledge extraction process are also presented in the study. The main contributions of this paper are: the definition of fake news in contrast to correlated false-content pieces of information, the classification of the traditional processes of fake news identification, eliciting the primary dataset and used features to characterize the fake news, the discussion of the main vectorization schemes for converting natural language data into mathematically operable data; and the listing of research opportunities and future directions.

V. Kulkarni, D. Aashritha Reddy, P. Sreevani and R. N. Teja [5] has proposed a fake profile identification using ANN. Innovative problems have evolved, such as cybercriminals, fake profiles, and online impersonation. There are no practical solutions to these problems. In this study, we employ an artificial neural network to effectively and recognize human false profiles. We assess the likelihood that a private message on Facebook is legitimate or not. Online social networks that have hundreds of profiles that can't be manually checked can make use of this. Artificial Neural Networks (ANN) are typically employed in bogus profile identification to establish if a particular account is real or false. An established set of guidelines serve to train ANN algorithms so they can identify between authentic and false profiles. To determine yet if the provided test data contains genuine or real data, the algorithm applies the training set to new test data. In machine learning, ANN is used to evaluate if a friend request is real or not.

P. K. Roy and S. Chahar [6] has proposed A comprehensive review. This article seeks to provide a summary of current developments in the methodology for identifying phoney accounts on social networking sites. Social networking websites have captured an array of users' interest during the preceding ten years from all around the world. Popular websites like Facebook, Twitter, LinkedIn, Instagram, and others experienced an unanticipated increase in the number of unique visitors as a result. But, according to analysts, not all trading accounts are genuine; many of them are false and were made for particular goals. The main goal of fake accounts on the site is to disseminate spam, hoaxes, and other false information. So, it is necessary to screen out the bogus accounts, but doing so presents numerous difficulties. Researchers have used a variety of cutting-edge innovations in recent years to spot fictitious accounts. They provide a summary of the most recent progress in deepfakes sensing technologies in the survey which is provided in this article. We provide a brief discussion of the drawbacks and shortcomings of the current models.

Islam, M.R., Liu, S., Wang, X. et al [7] has proposed deep learning for misinformation detection on online social networks. Using social media sites like Facebook, Twitter, and Sina Weibo has recently ingrained itself into every aspect of our everyday life. Users can conveniently communicate private messages, images, and videos on this site. Because many people like online communities, there are many dishonest activities like fake news or gossip that might cause users to believe false information. A further problem is the vast volume of false information that is being distributed online. As a consequence, misinformation detection (MID) in online communities has drawn a lot of attention and is now thought to be an emerging topic of research. We discover that a variety of MID-related studies have been examined using fresh research questions and methodologies. Although crucial, it can be challenging to achieve since a sophisticated model is needed to determine how nearly or possibly related integrated report is to actual information. A thorough analysis of automated misinformation detection on erroneous information, hoaxes, spam, fake news, and disinformation has been presented. We present a state-of-the-art assessment on MID where deep learning (DL) is used to automatically process data and develop patterns to make decisions in order not just extract global features but also to get superior results. The results further demonstrate that DL is a practical and scalable method for cutting-edge MID. Finally, they outline a number of unresolved problems that currently hinder real world usage & indicated the possible future developments in this area.

O. Ajao, D. Bhowmik and S. Zargari [8] has proposed a sentiment Aware Fake News Detection on online social network. Social networking website messages have recently generated controversy since they are used to fabricate stories or false information. For computerized false news and scuttlebutt detection, this effort tries to comprehend and assess the traits of fake news, particularly with regard to sentiments. We put up the theory that there's a causal connection between completely bogus messages or falsehoods and the emotion of the texts posted online based on empirical proof. By contrasting our findings to splitting baseline text-only false news detection techniques that do not take sentiments into account, we are able to confirm our theory. Our tests on the common Twitter fake news dataset demonstrate significant gains in the ability to identify rumors or false news items.

W. Han and V. Mehta [9] has proposed a Fake News Detection in Social Networks Using Machine Learning and Deep Learning. Fake news issues are escalating quickly, which distorts perceptions of some information. Social media platforms are among the quickest means of disseminating information and have a tremendous impact on information manipulations by affecting readers in both positive and unfavorable ways. This study attempts to compare and contrast diverse methods that are used to tackle this issue, including some well-known deep learning techniques such hybridized CNN and RNN as well as some standard machine learning techniques like Naive Bayes. Comparisons are made between conventional and deep learning methods as well as conventional and unconventional techniques. The basis for choosing a machine learning or deep learning approach to a problem requiring striking a balance between accuracy, light weightiness and precision is laid forth in this work.

Sk. Shama, K. Siva Nandini, P. Bhavya Anjali [10] used to detect a fake profile identification in Online Social Networks. This technology is linked to online social networks, which are now a vital component of life and make it easier for people to make and stay friends and discover common interests. However, the rise in networking sites has brought up a number of issues, such as people creating false profiles and the rise in online impersonation. When surfing, users are fed more pointless information that is provided by bogus individuals. 20% to 40% of the profiles in online networks such as Facebook are false, according to studies. Frameworks are used as a result of both the bogus profile detection in online social networks. It contains a way to categorize an object into a certain group in accordance with the training data set which was utilized to develop the classifier. They provide a data set to the decoder so it's possible to train it to accurately recognize entities and relationships. An algorithm for classification is a classifier. They have employed neural networks and support vector machines as classifiers in this project, comparing the effectiveness of each. The findings relate to determining if an account is false or real leveraging manufactured features and machine learning models like neural networks and random forests that have been trained. Predictions show that the neural network algorithm generated 93% accuracy. When Facebook rolls out new features, it will be simple to spot bogus accounts.

N. Singh, T. Sharma, A. Thakral and T. Choudhury [11] used to detection of Fake Profile in Online Social Networks Using Machine Learning. Those of us who use social media platforms for nefarious purposes are using them in larger numbers. Although machine adapting techniques have satisfactorily treated unfairly created accounts in a range of situations, human-made counterfeit characters have received very little research attention. The ML models employed a variety of features to evaluate an account's number of followers to buddies on social media networks in order to identify bots. No account's rights are infringed, and the profiles of all accounts make the number of friends and followers readily available. They create a fabricated human account throughout order to successfully detect, identify, and remove the fraudulent accounts.

Rao, P. S. J. Gyani, and G. Narsimha [12] has propose a fake profiles identification in online social networks using machine learning and NLP. In addition to offering users perks, social networking sites also pose a security risk to them and their personal data. We must analyze user profiles on social media outlets in order to identify who is promoting dangers there. We can determine the real profiles on social networks and the fraudulent profiles from the classification. For classifying fraudulent profiles on social networks, we traditionally use a variety of techniques. Therefore, we must increase the social network's phony profile detection's rate of accuracy. They suggest machine learning and natural language processing (NLP) techniques in this paper to increase the efficacy of bogus profile detection. Support Vector Machine (SVM) and Naive Bayes can be used.

V.Tiwari [13] used to analysis and detection of fake profile over social network. They have presented that more than 10 million likes and shares are sent. Other social media platforms like Twitter, Instagram, Pinterest, LinkedIn, and others are rapidly expanding. The expansion of social networks has led to an extremely high number of fraudulent user profiles being created for nefarious purposes. Other names for fake profiles include Sybils and social Bots. Several of these profiles attempt to become friends with both the good users in order to eventually acquire confidential information. Any online social network's main threat source is psychological manipulation (OSN). The several techniques to identify fraudulent profiles and associated online social bots are reviewed in this research. Online social networks from such a multi-agent perspective have also been investigated. Additionally, it covers the machine learning techniques that can be used to create and analyze profiles.

J. Jia, B. Wang and N. Z. Gong [14] has proposed a random walk based fake account detection in online social networks. In this study, we offer SybilWalk, a brand-new Sybil planned based on random walks. By keeping the desirable characteristics of existing randomized walk-based approaches, SybilWalk overcomes their flaws. In order to compare SybilWalk with earlier random walk-based techniques, we engage both theoretical and empirical reviews. Theoretically, SybilWalk has a tighter asymptotical restriction on the number of Sybils that are fraudulently accepted into the social network than any known random track approaches for online social networks only with fast-mixing property. Using social networks containing synthetic Sybils and a sizable Twitter database with genuine Sybils, we empirically assess SybilWalk with prior random walk-based approaches. Our research indicates that SybilWalk is significantly more precise than current randomness.

M. Torky, A. Meligy and H. Ibrahim [15] has proposed a recognizing fake identity in online social networks based on a finite automation approach. In this research, they proposed the Fake Profiles Recognizer (FPR), a detection mechanism for recognizing and detecting fake profiles in OSNs. The Regular Expression and Deterministic Finite Automaton (DFA) techniques for identifying profiles serve as the foundation for the detection process in FPR. On three well-known categories of online social networks, including Facebook, Google+, and Twitter, they tested our identification technique. The findings examined the high sensitivity, accuracy, and reduced FPR procedure in identifying the identities of Fake Profiles. In addition, their suggested detection mechanism outperformed other detection systems in the literature with significant competitive results.

3. PROPOSED SYSTEM

There have been several studies on using LSTM-RNN for fake profile identification. These studies typically focus on using LSTM-RNN to analyze various characteristics of a profile such as the text in the profile description, the behavior patterns of the profile, and the relationships between different profiles. The main aim is to identify patterns that are indicative of fake profiles, and to develop models that can accurately classify profiles as either fake or real. The results of these studies have shown promising results, with LSTM-RNN achieving high accuracy in detecting fake profiles. However, there is still room for improvement, and ongoing research is aimed at making these models even more accurate and robust. Some of the proposed methods have also leveraged natural language processing techniques to analyze the text content posted by users, such as posts and comments, to improve the accuracy of fake profile detection. Some recent studies have proposed using multi-modal learning techniques to combine both visual and textual information for fake profile detection. This can improve the robustness of the model and increase its ability to distinguish between real and fake profiles, as well as profile impersonation. In summary, proposed system works on LSTM-RNN based identification of fake profiles in social media have mainly focused on using user metadata and text content posted by users to train models, and there have been recent attempts to incorporate visual information into the models.

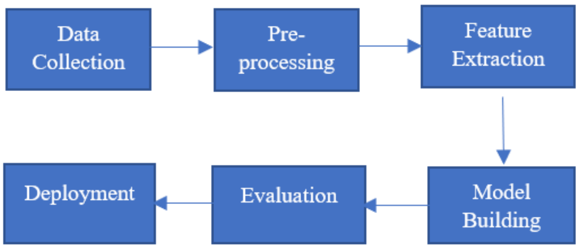

Fig. 1.1 Flow Diagram to detect fake profile

Fig. 1.1 Describes the steps involved in the methodology for LSTM-RNN based identification of fake profiles in social media using machine learning (ML) and natural language processing (NLP):

- Data Collection: The first step is to collect the data of real and fake profiles from social media platforms. This data can be used to train and test the machine learning model.

- Pre-processing: The collected data is pre-processed to remove irrelevant information and clean it up for further use. This includes removing special characters, punctuation, stop words, etc.

- Feature Engineering: In this step, features are extracted from the pre-processed data. These features can be the profile information, user behavior, network analysis, etc.

- Model Building: In this step, the LSTM-RNN model is built using the extracted features. The model is trained on the collected data and is used to classify the real and fake profiles.

- Evaluation: The trained model is evaluated using various evaluation metrics such as accuracy, precision, recall, F1 score, etc. This helps in determining the performance of the model.

- Deployment: Finally, the trained and evaluated model is deployed in a real-world scenario to identify fake profiles in social media.

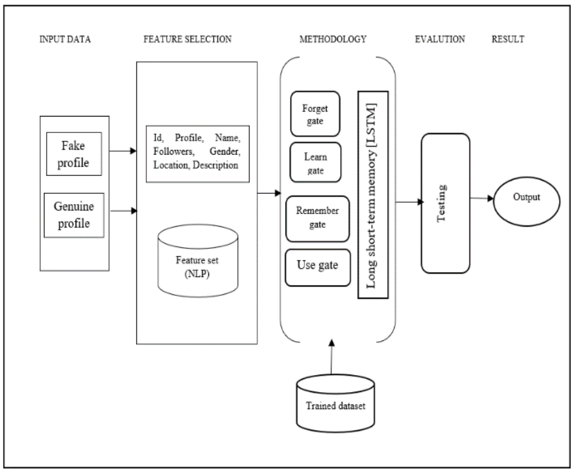

Fig. 1.2. Architecture Diagram of Fake Profile

In this approach, methodology used which removes data normalization on dataset before analyzing them. This technique has been applied to the field of Deep Learning. It is a variety of recurrent neural network (RNNs) that are capable of learning long-term dependency, especially in sequence prediction problems. In this paper the trained model using supervised machine algorithm, although technically, they are trained using supervised learning methods, referred as self-supervised independent for both data set such as fake and genuine. Ensemble methodology have been used for the prediction more accurately with both long-Term memory (LTM) and short-term memory (STM) and for making calculation simple and effective it uses the concept of gates fig 1.2. Based on research analysis, the effective functions of LSTM gate like (i)Forget Gate-LTM goes to forget gate and it forget the information that is not useful (ii) Learn Gate-event (current input) and STM are combined together so that necessary learned from STM can be applied to current input. (iii) Remember gate-information that we haven't forget STM & event are combined in remember gate which work as updated LTM. (iv) Use gate-predict the output of current event which work as an updated STM.

Now in the end, we conclude the work are to be done to identify or detect fake profile created by false users. Training LSTMs remove the problem vanishing gradient, it can be easily done using python frameworks and libraries like NLTK (NLP), NumPy, Math plot, Kernal, etc. And finally catches the same as RNN, we would need GPU for training deeper LSTM network

4. CONCLUSION & FUTURE

The conclusion of a study on the use of Long-Short Term Memory Recurrent Neural Network (LSTM-RNN) for fake profile identification in social media would depend on the specific findings of the study. However, in general, an LSTM-RNN model can be an effective tool for detecting fake profiles in social media due to its ability to analyses sequential data and capture long-term dependencies. The success of the model would depend on the quality of the training data and the specific architecture used in the study. However, it's important to note that the challenge of fake profile identification is constantly evolving, and LSTM-RNN based approaches may not be able to fully address all the challenges involved.

The future work for LSTM-RNN based identification of fake profiles in social media using ML & NLP can include several research areas. Some of these are:

- Improving the accuracy of the model.

- Incorporating additional features such as image analysis and sentiment analysis, to enhance the performance of the model.

- Applying deep learning models such as Convolutional Neural Networks (CNNs), to enhance the performance of the LSTM-RNN model.

- Real-time fake profile detection to develop a real-time fake profile detection system, which can automatically identify fake profiles as soon as they are created.

- Integration with social media platforms to make it more widely available and useful to the users.

REFERENCE

[1] Aayush Sunil Chamria, Abhishek Dinesh Mane, Prithvi Vadiraj Dambal, Smita Bharne, "*Detecting Fake Profile in Online Social Networks using EnsemStack Categorization mode"* International Conference on Computing, Communication, Control and Automation (ICCUBEA) Issue: 26 | August 2022 https://ieeexplore.ieee.org/,e-ISSN: 2771-1358, p-ISSN: 2771-134X.

[2] Latha P, Sumitra V, Sasikala V J. Arunarasi "*Fake Profile Identification in Social Network using Machine Learning and NLP*", 2022 International Conference on Communication, Computing and Internet of Things (IC3IoT), doi:10.1109/IC3IOT53935.2022.9767958.

[3] X. Jose, S. D. M. Kumar and P. Chandran, "*Characterization, Classification and Detection of Fake News in Online Social Media Networks*," 2021 IEEE Mysore Sub Section International Conference (MysuruCon), Hassan, India, 2021, doi:10.1109/MysuruCon 52639.2021.9641517.

[4] De Oliveira, Nicollas R., Pedro S. Pisa, Martin Andreoni Lopez, Dianne Scherly V. de Medeiros, and Diogo M. F. Mattos. "*Identifying Fake News on Social Networks Based on Natural Language Processing: "Trend & Challenges*"2021,https://doi.org/10.3390/info12010038.

[5] V. Kulkarni, D. Aashritha Reddy, P. Sreevani and R.N. Teja, "*Fake profile identification using ANN,*" 4th Smart Cities Symposium (SCS 2021), Online Conference, Bahrain, 2021, pp. 375-380, doi: 10.1049/icp.2022.0372.

[6] P. K. Roy and S. Chahar, "*Fake Profile Detection on social networking websites: A comprehensive Review*," in IEEE Transactions on Artificial Intelligence, vol. 1, no. 3, pp. 271-285 Dec. 2020, doi: 10.1109/TAI.2021.3064901.

[7] Islam, M.R., Liu, S., Wang, X. et al. *Deep learning for misinformation detection on online social networks: a survey and new perspectives Social Network* Anal. Min. 10, 82 (2020). https://doi.org/10.1007/s13278-020-00696-x.

[8] O. Ajao, D. Bhowmik and S. Zargari, "*Sentiment Aware Fake News Detection on Online Social Networks*," ICASSP 2019 - 2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Brighton, UK, 2019, pp. doi: 10.1109/ICASSP.2019.8683170.

[9] W. Han and V. Mehta, "*Fake News Detection in Social Networks Using Machine Learning and Deep Learning: Performance Evaluation*," 2019 IEEE International Conference on Industrial Internet (ICII), Orlando, FL, USA, 2019, pp. 375-380, doi: 10.1109/ICII.2019.00070.

[10] S.k. Shama, K. Siva Nandini, P. Bhavya Anjali, K. Devi Manaswi, Sk. Wasim Akram *Fake Profile Identification in Online Social Networks* International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878 (Online), Volume-8 Issue-4, November 2019.

[11] N. Singh, T. Sharma, A. Thakral and T. Choudhury, "*Detection of Fake Profile in Online Social Networks*

Using Machine Learning," 2018 International Conference on Advances in Computing and Communication Engineering (ICACCE), Paris, France, 2018, pp. 231-234, doi: 10.1109/ICACCE.2018.8441713.

[12] Rao, P. S., J. Gyani, and G. Narsimha. "*Fake profiles identification in online social networks using machine learning and NLP*." Int. J. Appl. Eng. Res 13.6 (2018): 973-4562.

[13] V.Tiwari, "*Analysis and detection of fake profile over social network*," 2017 International Conference on Computing, Communication and Automation (ICCCA), Greater Noida, India, 2017, pp. 175-179, doi: 10.1109/CCAA.2017.8229795.

[14] J. Jia, B. Wang and N. Z. Gong, "*Random Walk Based Fake Account Detection in Online Social Networks*," 2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), Denver, CO, USA, 2017, pp. 273-284, doi: 10.1109/DSN.2017.55.

[15] M. Torky, A. Meligy and H. Ibrahim, "*Recognizing Fake identities in Online Social Networks based on a Finite Automaton approach*," 2016 12th International Computer Engineering Conference (ICENCO), Cairo, Egypt, 2016, doi: 10.1109/ICENCO.2016.7856436.