

Social Networking Sites Fake Profiles Detection Using Machine Learning Techniques

Ajaykumar Dharmireddy¹, Monika Devi Gottipalli²

¹ Department of Electronics and Communication Engineering, ²Department of Computer Science Engineering,

^{1,2}Sir C.R.Reddy College of Engineering,

Eluru-534007 Andhra Pradesh, INDIA

¹ajaybabuji@gmail.com, ²monikadevi.g@gmail.com

Abstract— In the present paper, we offer a model that might be applied to identify if an account is real or false. It is unnecessary to manually examine each account because our model, which uses a support vector machine as a classification technique, can simultaneously process an extensive accounts dataset. We are concerned with the community of fake accounts, and our issue is classification and clustering. We employ artificial neural networks (ANN) and machine learning (ML) to assess the likelihood that a Facebook friend request is genuine or not. The existence of bots and phoney profiles is another risk factor for personal data being collected for illicit purposes. Bots are computer programmers that can compile data about users without their knowledge. Web scraping is the term for this activity. The fact that this behaviour is legal makes it worse. Bots can be disguised or appear as false friend requests to access private information on a social networking site. Still, there is a 7% false positive rate in which our system fails to identify a fake profile correctly.

Index Terms— Artificial neural networks (ANN), Machine Learning (ML), Big Data set, Phoney Profile, Fake Profile Detection.

I. INTRODUCTION

Online social media is taking over the world these days in several ways. The amount of people utilizing social media is rapidly rising every day. The primary benefit of social media on the internet is the ease with which we can connect with others and improve our communication with them. This provided a new way of a potential attack, such as fake identity, false information, etc... A recent survey suggests that the number of accounts present on social media is far more expansive than the number of people who utilize it. Facebook is the most widely used form of social media, with 2.46 billion users worldwide as of 2017. Social networking sites are platforms to generate income from user-provided data. The typical user must know their rights are forfeited when using a Social networking site. Businesses that use social media have a lot to gain at the expense of users. Facebook generates income from advertisements and data each time a user publishes a new location or new images, expresses their likes and dislikes, and tags other users in anything they post. The average American user generates roughly \$26.76 per quarter. With millions of users, that sum grows quite quickly. In the current digital media, the growing reliance on computer technology has made the average person more susceptible to crimes like data breaches and potential identity theft. These attacks are

frequently carried out without warning or informing the individuals whose data was compromised.

Social networking sites like Facebook, Instagram, and Twitter are frequently the targets of these hacks. In the current generation, everyone's social life is now entwined with online social networking sites. Adding new friends and staying in touch with them and their updates has become a time pass. Social networking sites impact various fields, including science, education, community activism, employment, and business. Instructors may quickly reach their students using this, creating a welcoming environment for them to learn. Teachers are becoming more familiar with these sites and using them to provide online classroom pages and assignments, hold conversations, and perform other activities that greatly enhance learning. Employers can utilize these social networking sites to find brilliant candidates who are enthusiastic about their jobs and whose backgrounds can be easily checked.

Each social networking site user has a profile and can communicate with friends, share updates, and connect with people. Social networking services are expanding quickly and altering how individuals communicate. Online groups bring people with similar interests together, making it more straightforward for users to establish new connections. Over the past few years, online social networking sites like Facebook, Instagram, Twitter, and LinkedIn have grown in popularity.

With more than 2.2 billion monthly active users and 1.4 active users, the community is up 11% from the previous year, as shown in Figure 1. After pre-processing the generated data, machine learning techniques were used to identify and detect phoney accounts on social media sites. The classification results of the algorithms Support Vector, Random Forest, and Neural Network: Fake account detection is done by machines. The described algorithms' accuracy rates for identifying bogus accounts are compared, and the algorithm with the highest accuracy rate is noted. Our study focuses on finding phoney profiles and clever BOTS on a social media site like Twitter. Because they are automated and may be used without a human, phone-profile bots are employed increasingly frequently.

As technology advances, AI is now used in every field of work and is replacing humans, making it more challenging to detect human-made fake profiles. Bots and fake profiles created for stalling personal data of users on social networking



sites like Facebook, Instagram and Twitter are for spreading fake news and rumours.

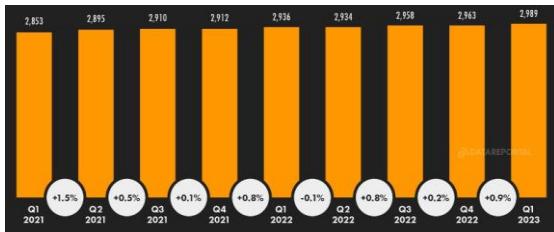


Fig. 1. Facebook monthly active users (QOQ) in Millions: May 2023

II. LITERATURE SURVAY

Y. Y.Boshmaf et al.,[7] Online social network (OSN) administrators and users are protected from harmful actions when false accounts in OSNs are detected. By examining user-level behaviours or graph-level structures, most detection systems aim to categorize user accounts as genuine (i.e., harmless, honest) or fraudulent (i.e., evil, Sybil). Unfortunately, adversarial assaults that employ phoney accounts to masquerade as legitimate ones are brutal for these systems to withstand.

This article demonstrates that victims, who are actual accounts whose users have accepted friend requests issued by scammers, constitute a separate category that may be used to develop effective detection systems. Íntegro, a solid and extensible defence mechanism, is specifically introduced here. It uses victim categorization to prioritize actual accounts over fraudulent ones, allowing OSN operators to punish low-ranking false ones. Íntegro begins by using supervised machine learning to detect possible victims based on user-level actions. Then, it annotates the graph by making edges that may be victims less significant. Ultimately, Íntegro sorts user accounts according to the landing probability of a brief random walk that begins with a verified actual account. The reason Íntegro gets the rating it wants is because this stroll isn't going to land on fakes and cross low-weight edges quickly.

We leveraged popular open-source distributed computing platforms to deploy Íntegro, and it grew almost linearly from there. Íntegro was tested using real-world datasets and a large-scale deployment at Tuenti, the biggest OSN in Spain with over 15 million active users, compared to SybilRank, the leading solution for detecting false accounts. Given that the victim classifier used must be better than random, we demonstrate that Íntegro surpasses SybilRank regarding user rating quality. Additionally, compared to SybilRank, the accuracy of detecting bogus accounts was up to a factor of ten greater when Íntegro was implemented at Tuenti.

P. Kondeti et al.,[8] The use of digital technology has been growing exponentially recently. Concurrently, the number of evil users has been on the rise. Across the world, millions of individuals use social media websites such as Twitter and Facebook. One of the many problems arising from people's increased engagement with online networking is the potential for disseminating harmful information via bogus accounts. Spam, fraud, and abuse on social media platforms may easily be perpetrated via fake accounts. These issues must be addressed to provide users with a trustworthy online social

network. Some of the machine learning methods used in this research include support vector machines (SVMs), logistic regression (LRs), random forests (RFs), and K-nearest neighbours (KNNs). Z-Score and Min-Max are two normalization methods used in conjunction with these algorithms to enhance accuracy. It can identify bots and bogus Twitter accounts, so we implement it. Random Forest and KNN obtained high precision and true positives with our approach.

M. Conti et al.,[9] People's professional, personal, and political lives are becoming increasingly shaped by online social networks (OSNs). Malicious actors seek to take advantage of the holes and vulnerabilities of OSNs, just like they do in cyberspace on the Internet. Security experts are attempting to find ways to protect individual users from the growing number of complaints about security and privacy vulnerabilities in OSNs. A significant issue in identifying and preventing assaults on individual user privacy is the large number of users (tens or hundreds of millions) on many OSNs, generating billions of potentially exploitable personal data. Most recent studies have focused on methods for preserving the anonymity of an already-established profile inside a certain OSN. Rather, we point out that not having a profile in the most recent trendy social network is a possibility! An attacker might pose a threat by creating a phoney profile to fool OSN users into thinking they are someone else. To obtain personal information from victims of identity theft, the perpetrators may use the bogus profile to establish online relationships with their friends. This work details our research into a potential solution to this issue. Along the way, we made a note of being the pioneers in the field of privacy threat analysis of social network graphs from a dynamic perspective.

M. M. Swe et al.,[10] Twitter, Facebook, Weibo, and other social media platforms have become ubiquitous in people's daily lives. Additionally, most bad actors use these platforms to trick good people into advertising their goods or services, clicking on their spam links, slandering others, etc. Faux accounts on these sites have become a big problem due to the ever-increasing user base on these social media platforms. This study proposes a new method for detecting bogus accounts—a blocklist—rather than the more conventional spam word list. A topic modelling and keyword extraction strategy is used to generate the blocklist. In addition to the 1KS–10KN dataset, we use the Social Honey Pot dataset in our assessment experiment. We compare our blacklist-based method to the conventional spam word list-based method in terms of accuracy. Decorate, a meta-learner classifier, distinguishes between real and phoney Twitter accounts. Our practice has a positive rate of 0.95 and an accuracy of 95.4%.

B. Erşahin et al.,[11] Millions of people all around the globe use social media every day, and how they use these sites directly impacts their daily lives. One issue arising from social media's meteoric rise to prominence is the proliferation of harmful material that may be transmitted using false accounts, which might expose users to inaccurate information. In the actual world, society may suffer tremendous harm due to this predicament. We provide a categorization strategy for identifying Twitter accounts that are not real in our investigation. We used a supervised discretization method

called Entropy Minimization Discretization (EMD) on numerical features to preprocess our dataset, and then we examined the outcomes of the Naïve Bayes algorithm.

Y. -C. Chen et al.,[12] Nowadays, it's easier to imagine contemporary life with online social networks. Not only did it revolutionize human communication, but it also opened the door to new forms of assault, including misleading information, identity theft, and more. Recently, several issues have arisen throughout online social networks (OSNs) due to phoney accounts. The large number of bogus invoices, overflooded advertisements, the distribution of fraudulent information, etc., are some of the problems that OSN providers face. There is no foolproof way to tell a legitimate account from a phoney one using conventional methods. While there has been some research on the make-up and structure of spam accounts in the past, the rapid development of these accounts has rendered this prior study either irrelevant or ineffectual. Then, we zero in on a new kind of fraudulent account that may share misinformation and spam with ads and automatically post or remark. A new approach to identifying phoney OSN accounts was suggested in this study. Using machine learning, we can determine whether an account is being managed by a fake person based on their Facebook activity patterns. In addition, we provide an analysis of the predicted account activity. New levels of accuracy in identifying fraudulent accounts may be possible due to this study.

Qiang C et al.,[13] People increasingly believe in the integrity of the content shared on OSNs. Also, the OSN providers' business models rely on this data being marketable. On the other hand, OSNs are vulnerable to misuse due to the proliferation of false accounts that do not represent actual people. Spam, manipulated online ratings, and exploiting network-extracted information are all possible outcomes of fakes. Identifying, manually verifying, and deactivating phoney accounts is a significant resource drain for OSN operators. The biggest OSN in Spain, Tuenti, spends much money and has 14 full-time workers on just one duty. The distinct differences in behaviour between actual and false OSN profiles make it challenging to automate this kind of work consistently.

We provide SybilRank, a new tool for OSN operators to use. It ranks people based on how likely it is that they are not phoney using social graph features (Sybils). Our Hadoop prototype proved that SybilRank is computationally efficient and can handle networks with hundreds of millions of nodes. We set up SybilRank in Tuenti's control room. Around 90% of the 200,000 accounts SybilRank flagged as very probable to be fraudulent needed to be suspended. However, according to Tuenti's current user-report-based method, only around 5% of the accounts examined are indeed fraudulent.

III. PROPOSED SYSTEM

Architecture of proposed design is shown in Figure 2. In our approach, we use artificial neural networks and machine learning to assess the likelihood that a friend request is genuine or not. To keep both old and new phoney data profiles, we use Microsoft Excel. The data is subsequently supported by the algorithm in a data frame. This data collection will create a training set and a testing set. To train our model, we would want a set of data from the social media platforms.

The attributes we use for the training set when determining whether a profile is false are the following: Account age, Gender, User age, Link in the description, Number of messages exchanged, Number of friend requests sent, Entered location, Location by IP. Each of these attributes is evaluated before being given a value. For the gender parameter, for instance, a matter of is assigned to the training set for gender if it can be identified whether the profile is female or male. Other parameters are subjected to the same procedure.

We also take into account a person's country of origin. Fake profiles of all kinds create negative effects that counteract the advantages of social media for businesses in advertising and marketing and pave the way for cyber bullying.

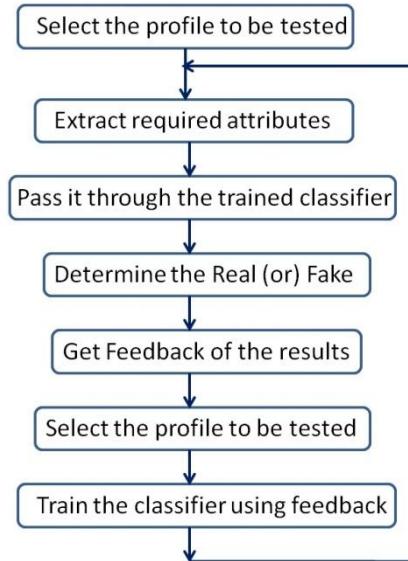


Fig. 2. Architecture of proposed design

There are many social networking sites including Twitter, Facebook, Google+, Myspace, Instagram, Tumblr, Foursquare and LinkedIn. There were 823 million people who used Facebook daily on their mobile devices, which is an increase from the 654 million such users in the previous quarter. Social networking sites such as Facebook cannot yet deliver notifications regarding fake profiles in real-time, and discriminating between real and fake profiles is difficult for non-technically savvy users. Moreover, many big data issues, including data storage, how to handle streaming data, and how to provide immediate responses to users, must be handled while simultaneously operating on large volumes of data to achieve accurate profile identification results.

IV. METHODOLOGY

Supervised Machine Learning algorithms can be broadly classified into Regression and Classification Algorithms.

A. Linear Regression

Independent and dependent variables are correlated through regression analysis. A vital task in the modern world, regression algorithms help forecast continuous variables like real estate values, economic trends, weather patterns, oil and gas prices, etc.

Linear Regression classified into two types:

- Decision Tree Regressor
- Random Forest Regressor

Linear regression is a straightforward and often used Machine Learning technique. It is a mathematical method used to do predictive analysis. Linear regression provides predictions for continuous, accurate, numeric variables such as sales, salary, age, and product price. The linear regression procedure, sometimes called linear regression, illustrates a direct relationship between a dependent variable (y) and one or more independent variables (x). Linear regression is a statistical method that may analyse the relationship between dependent and independent variables[19]. It helps identify how the value of the dependent variable varies based on the value of the independent variable. A linear regression model shows the relationship between the variables, where a straight line with a slope illustrates the link.

1) *Decision tree regressor:*

Decision tree regression is a machine learning technique that enables non-linear regression. The primary function of the decision tree regression technique is to partition the information into smaller, more manageable segments. The subsets of the dataset are used to depict the values of all data points relevant to the problem statement. This method partitions the data set into decision and leaf nodes, creating a decision tree[20]. When the data collection has yet to undergo sufficient alteration, machine learning specialists choose this model. It is important to note that even a slight change in the data may significantly affect the layout of the decision tree.

Furthermore, it is advisable to refrain from excessively pruning the decision tree regressors. Due to an insufficient number of surviving end nodes, the prognosis cannot be made [21]. To ensure a more significant number of end nodes (regression output values), it is advisable not to prune the decision tree regressors excessively. This approach employs a hierarchical structure like a tree to predict future data and provide valuable continuous output..

2) *Random forest regressor:*

Random Forest is another popular method for non-linear regression in machine learning. A random forest employs multiple decision trees to predict the outcome instead of decision tree regression (single tree). With the help of this algorithm, a decision tree is constructed using k randomly chosen data points from the provided dataset. The worth of any new data point is then predicted using several decision trees. A random forest algorithm will forecast multiple output values because of numerous decision trees. To determine the final result for a new data point, you must discover the average of all the predicted values. This occurs due to the numerous decision trees that must be mapped using this method—more processing capacity. Trees run parallel; it's a bagging method, not a boosting technique. i.e., there is no interaction between these trees as you construct trees.

B. Classification of algorithm

A classification algorithm discovers functions to categorize the dataset into groups based on different criteria. A computer program divides the data into other groups based on what it learns from the training dataset.

1) *Decision tree algorithm*

A decision tree, a supervised learning approach, is often used for solving classification and regression issues. A tree-structured classifier represents a dataset's attributes as internal nodes, the decision-making process as branches, and the classification result as each child node. The Decision Node and Leaf Node are the two components of a decision tree. Leaf nodes represent the outcomes of choices and do not contain any extra branches. On the other hand, decision nodes are used to make decisions and have several components. A decision tree is a visual tool used to discover all possible solutions or outcomes for a given choice or problem, considering established parameters. Due to its resemblance to a tree structure, it is often called a decision tree. The process begins at the root node and expands via supplementary branches, resulting in a tree-like form. The CART method, short for the Classification and Regression Tree algorithm, is used for constructing a tree. It is used for both classification and regression tasks..

2) *Random forest algorithm*

The preferred algorithm for machine learning, Random Forest, is a component of the supervised learning process. To enhance the prediction accuracy of the dataset, the Random Forest classifier employs numerous decision trees on distinct regions of the input data. This technique applies to machine learning problems that include both classification and regression. Ensemble learning is based on mixing many classifiers to tackle intricate problems and improve the performance of models. Despite the size of the dataset, it performs efficiently and accurately predicts the result with a high level of precision. Even when a substantial portion of the data is missing, it is still possible to preserve accuracy..

V. RESULTS AND DISCUSSION

To execute this application, deploy it on a DJANGO server and then access it in a web browser by entering the URL as 'http://localhost:800' to get the screen below. To access the login screen, click the "ADMIN" link above the screen and enter the admin user name and password is shown in Figure 3&4



Fig. 3. To access the login screen, click on the "ADMIN" link located screen.

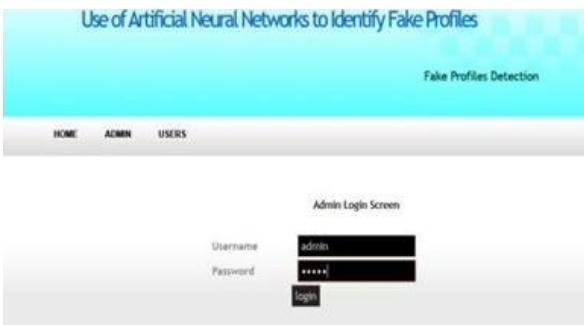


Fig. 4. Enter "admin" as the username and password in the appropriate fields on the screen.



Fig. 5. Construct ANN Train Model.

To construct a training model on the dataset, click the button labeled 'construct ANN Train Model' shown on the Figure 5. By clicking on the provided

link, you can access the server console, review the specifics of the ANN processing with precision. All ANN details are visible in the black console is shown in Figure 6.

Figure 7.illustrated in it evident that ANN achieved a remarkable accuracy of 98% in training all Facebook profiles. Please click on the 'View Ann Train Dataset' link to get all the dataset information.

```
Epoch 5/200
- 0s - loss: 2.1975 - accuracy: 0.9646
Epoch 6/200
- 0s - loss: 1.9974 - accuracy: 0.9458
Epoch 7/200
- 0s - loss: 2.2751 - accuracy: 0.9625
Epoch 8/200
- 0s - loss: 2.1176 - accuracy: 0.9667
Epoch 9/200
- 0s - loss: 2.3582 - accuracy: 0.9688
Epoch 10/200
- 0s - loss: 1.4462 - accuracy: 0.9479
Epoch 11/200
- 0s - loss: 2.6030 - accuracy: 0.9396
Epoch 12/200
- 0s - loss: 3.7952 - accuracy: 0.9667
Epoch 13/200
- 0s - loss: 1.6807 - accuracy: 0.9646
Epoch 14/200
- 0s - loss: 0.8312 - accuracy: 0.9688
Epoch 15/200
- 0s - loss: 1.8899 - accuracy: 0.9396
Epoch 16/200
- 0s - loss: 1.6779 - accuracy: 0.9684
Epoch 17/200
- 0s - loss: 1.2181 - accuracy: 0.9688
Epoch 18/200
```

Fig. 6. ANN details are visible in the black console



Fig. 7. 98% in training all Facebook profiles.

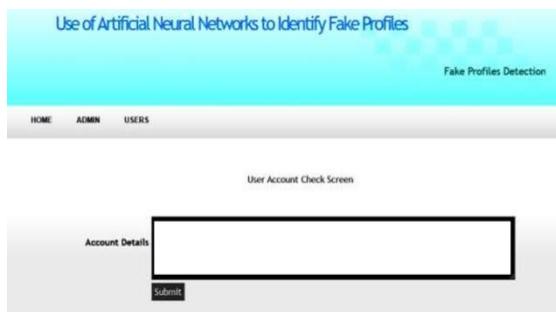


Fig. 8. Train data and examine all the records

In the shown in Figure 8, we can observe all the train data and scroll down to examine all the records. The ANN training model is now prepared and ready. You may proceed to log out and click on the 'User' link to see the next page.

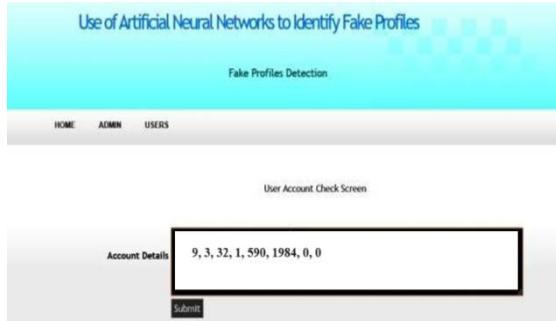


Fig. 9. Enter account details of R1.

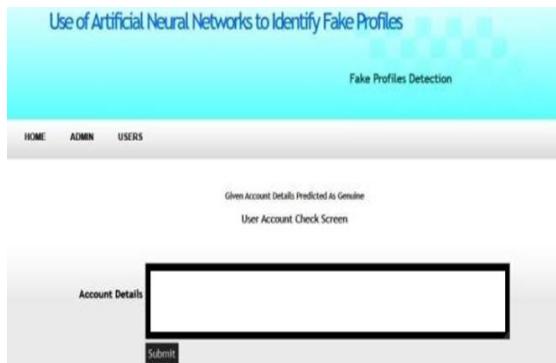


Fig. 10. Check the account of R1 from ANN.

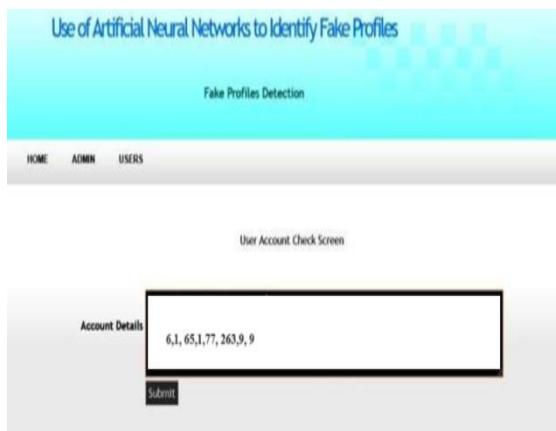


Fig. 11. Enter account details of R2

TABLE I. PREDICTION ACCOUNT FROM ANN

S. NO	Account Age	Gender	User Age	Link Description	Status Count	Profile Picture	No.of Posts	Friend Count	Location	Location IP	Profile Status
1	15	0	26	0	3578	0	0	1930	0	0	0
2	15	0	56	0	2464	0	0	712	0	0	0
3	15	0	45	0	6856	0	0	891	0	0	0
4	15	1	23	0	4675	0	0	255	0	0	0
5	15	0	51	0	11238	0	0	1178	0	0	0
6	14	1	54	0	20376	0	0	1930	0	0	0
7	14	1	56	0	4598	0	0	236	0	0	0
8	14	0	32	0	5439	0	0	760	0	0	0
9	14	1	25	0	20459	0	0	1564	0	0	0
10	13	1	31	0	10342	0	0	1234	0	0	0
11	13	1	45	0	2399	0	0	57	0	0	0
12	13	0	57	0	1174	0	0	36	0	0	0
13	13	0	34	0	10033	0	0	1100	0	0	0
14	12	1	22	0	405	0	0	78	0	0	0
15	12	0	42	0	770	0	0	90	0	0	0
16	12	0	30	0	1530	0	0	554	0	0	0
17	12	1	38	0	6778	0	0	371	0	0	0
18	12	1	20	0	9634	0	0	181	0	0	0
19	12	0	36	0	7098	0	0	305	0	0	0
20	12	1	23	0	571	0	0	916	0	0	0

To obtain predictions or identification from the Artificial Neural Network (ANN) in Table1, please enter the necessary account details in the provided input field is shown in Figure 9.

Refer to the following records

9, 3, 32, 1, 590, 1984, 0, 0 (R1)

6,1, 65,1,77, 263,9, 9 (R2)

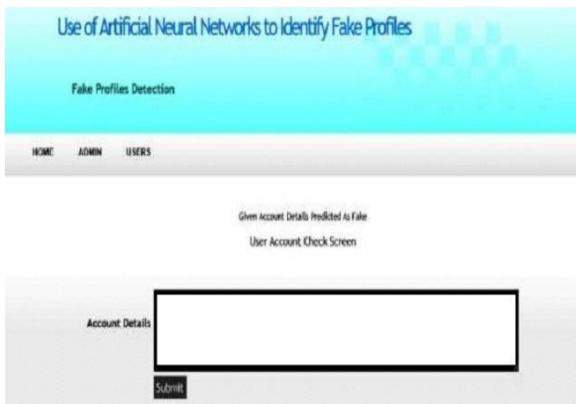


Fig. 12. Identified results from given records

The result was a real account shown in Figure 12.we got a result of a fake profiles cleared account

VI. CONCLUSION

In Social networking sites like Facebook, Instagram, and Twitter assess the authentication of a friend request; we use artificial neural networks and machine learning. Here every value is divided as neurons. Every equation is sent via a sigmoid function at every neuron. We use training data sets from Face book, Instagram, and Twitter or any other social networking sites. The proposed deep learning method may learn new patterns of behavior by minimizing the final cost function, adjusting each neuron's weights, and propagating bot activity patterns in reverse. In conjunction with the Random

Forest Classifier, we have developed a technique that enables us to detect fraudulent accounts or Fake biodata in any online social networking sites with a precision rate of up to 95%. Utilizing NLP techniques and neural networks to analyze posts and profiles in their accounts helps to improve the detection of bogus or fake profiles. In the future, we want to classify shapes by using profile photographs as a characteristic.

VII. FUTURE WORK

The primary limitations of this research are its reliance on just visible data and its lack of real-time applications. Additional tasks may be accomplished by executing a Convolution Neural Network (CNN) on the numerical, categorical, and profile picture data. Improved results may also arise from incorporating novel variables, integrating diverse models, and developing a model that operates in real-time. The regions in the model and data may be assigned different levels of prominence based on their size or unique relevance in the recognition process. It would be easier to identify regions where very intricate issues, such as those that infrequently arise, may be found using this method, for instance. Despite their complexity, these hybrid models are expected to provide superior outcomes. However, the rare combination of different strategies may not significantly impact the final result. Once that occurs, the model will be prepared to integrate with social networking sites like LinkedIn, Snap chat, We Chat, QQ, and others.

REFERENCES

- [1] S. Vidros, C. Koliас, G. Kambourakis, and L. Akoglu, "Automatic Detection of Online Recruitment Frauds: Characteristics, Methods, and a Public Dataset", Future Internet, vol.9,no.6,2017,doi:10.3390/fi9010006.
- [2] B. Alghamdi, F. Alharby, "An Intelligent Model for Online Recruitment Fraud Detection", Journal of Information Security, Vol.10,pp.155-176,2019,https://doi.org/10.4236/iis.2019.103009.
- [3] Ajaykumar Dharmireddy, Surya Manohar, G.T.Sri Hari, G. Gayatri, A. Venkateswarlu, "Detection of COVID-19 from X-RAY Images using Artificial Intelligence (AI)" 2022 International Conference on Intelligent

Technologies (CONIT), PP.1-5, 2022. DOI: 10.1109/CONIT55038.2022.9847741.

[4] P Hareesh, P Shanmugaraja, P H S T Murthy, M Narendra Kumar & Rajesh Kumar B. (2022). Detection of Volatile Organic Compounds using Micro-Electro-mechanical- Systems Micro cantilever: A Review. Computer Integrated Manufacturing Systems, 28(11), 861-882.

[5] Li, H.; Chen, Z.; Liu, B.; Wei, X.; Shao, J. Spotting fake reviews via collective positive-unlabeled learning. In Proceedings of the 2014 IEEE International Conference on Data Mining (ICDM), Shenzhen, China, 14-17 December 2014; pp. 899-904.

[6] P Hareesh, P Shanmugaraja, P H S Tejomurthy. Design of Microcantilever Based Sensor for Detection of Volatile Organic Compounds TELEMATIQUE. ISSN: 1856-4194 Volume 21 Issue 1, 2022, 7344 – 7353.

[7] Yazan Boshmaf, Dionysios Logothetis, Georgos Siganos, Jorge Lería, Jose Lorenzo, Matei Ripeanu, Konstantin Beznosov, Hassan Halawa, "Integro: Leveraging victim prediction for robust fake account detection in large scale OSNs", Computers & Security, Volume 61, 2016, Pages 142-168, ISSN 0167-4048, <https://doi.org/10.1016/j.cose.2016.05.005>.

[8] J. Mohana Prithvi, Ajaykumar Dharmireddy "Multitrack Simulator Implementation in FPGA for ESM System" International Journal of Electronics Signals and Systems, 29th Sep 2013, pp. 81-84.

[9] M. Conti, R. Poovendran and M. Secchiero, "FakeBook: Detecting Fake Profiles in On-Line Social Networks," 2012 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, Istanbul, Turkey, 2012, pp. 1071-1078, doi: 10.1109/ASONAM.2012.185

[10] M. M. Swe and N. Nyein Myo, "Fake Accounts Detection on Twitter Using Blacklist," 2018 IEEE/ACIS 17th International Conference on Computer and Information Science (ICIS), Singapore, 2018, pp. 562-566, doi: 10.1109/ICIS.2018.8466499.

[11] B. Erşahin, Ö. Aktas, D. Kılınç and C. Akyol, "Twitter fake account detection," 2017 International Conference on Computer Science and Engineering (UBMK), Antalya, Turkey, 2017, pp. 388-392, doi: 10.1109/UBMK.2017.8093420..

[12] Y. -C. Chen and S. F. Wu, "FakeBuster: A Robust Fake Account Detection by Activity Analysis," 2018 9th International Symposium on Parallel Architectures, Algorithms and Programming (PAAP), Taipei, Taiwan, 2018, pp. 108-110, doi: 10.1109/PAAP.2018.00026.

[13] Qiang C, Michael S, Xiaowei Y, and Tiago P (2012) Detecting bogus accounts in large-scale social online services. 9th USENIX conference on designing and implementing networks. pp 1-14

[14] J. Zhang, B. Dong and P. S. Yu, "FakeDetector: Effective Fake News Detection with Deep Diffusive Neural Network," 2020 IEEE 36th International Conference on Data Engineering (ICDE), Dallas, TX, USA, 2020, pp. 1826-1829, doi: 10.1109/ICDE48307.2020.00180..

[15] Wang, Peng et al. "Semantic expansion using word embedding clustering and convolutional neural network for improving short text classification." Neuro computing Vol.174, 2016, pp. 806-814.

[16] C. Li, G. Zhan, and Z. Li, "News Text Classification Based on Improved BiLSTM-CNN," in 2018 9th International Conference on Information Technology in Medicine and Education (ITME), 2018, pp. 890-893.

[17] K Shashidhar, Ajay kumar Dharmireddy, Ch Madhava Rao "Anti-Theft Fingerprint Security System for Motor Vehicles" Blockchain Technology for IoT and Wireless Communications, CRC Press, pp.89-102, 2024.

[18] Ajaykumar Dharmireddy, M. Greeshma, S. Chalasani, S. T. Sriya, S. B. Ratnam and S. Sana, "Azolla Crop Growing Through IOT by Using ARM CORTEX-M0." 2023 3rd International conference on Artificial Intelligence and Signal Processing (AISP), Vijayawada, India, 2023, pp. 1-5, doi: 10.1109/AISP57993.2023.10135032.

[19] Ajay kumar Dharmireddy, P Srinivasulu, M Greeshma, K Shashidhar "Soft Sensor-Based Remote Monitoring System for Industrial Environments" Blockchain Technology for IoT and Wireless Communications, CRC Press, pp.103-112, 2024.

[20] Ott, M.; Cardie, C.; Hancock, J. Estimating the prevalence of deception in online review communities. In Proceedings of the 21st international conference on World Wide Web, Lyon, France, 16-20 April 2012; ACM: New York, NY, USA, 2012; pp. 201-210.

[21] Nizam ani, S., Memon, N., Glasdam, M. and Nguyen, D.D. (2014) Detection of Fraudulent Emails by Employing Advanced Feature Abundance. Egyptian Informatics Journal, Vol.15, pp.169-174

Author(s') Profile(s)



Ajaykumar Dharmireddy, M.Tech, is working as a Asst. professor in ECE department, Sir C.R.Reddy College of Engineering Eluru, India. He received his master degree in Anna University, Coimbatore (India) in 2009. He published several research articles in various international journals. His research interests include Low-power VLSI Design, Device Modeling, Machine learning, Block Chain Technology. He is a life member of the IEI, ISTE and IAENG.



Monikadevi Gottipalli, M.Tech, is working as a Asst. professor in CSE department, Sir C.R.Reddy College of Engineering Eluru, India. He received his master degree in JNTU, Kakinada (India) in 2013. Her research interests include Machine learning, Block Chain Technology.