FAKE PROFILE DETECTION IN SOCIAL MEDIA USING MACHINE LEARNING AND NLP

DIVYA A N
PG Student
Dept. of MCA
The Oxford College of Engineering,
Bommanahalli,Bengaluru-560068.
divyaanmca2024@gmail.com

DHARAMVIR
Associate Professor
Dept. of MCA
The Oxford College of Engineering,
Bommanahalli,Bengaluru-560068.
dhiruniit@gmail.com

ABSTRACT

Social networking has become a ubiquitous activity on the internet, attracting millions of users who collectively spend millions of hours on these platforms. These online social networks (OSNs) range from interaction-based platforms such as Facebook and MySpace to information-centric platforms such as Twitter and Google Buzz. Despite their popularity, security and privacy issues are still a big problem. Users often share a lot of personal information, making them targets of attacks such as identity theft (the fraudulent use of personal information). Victims of identity theft can face serious consequences, including financial loss, legal issues, and reputational damage. Most dating sites do not trust users and have weak privacy policies,making them prime targets for fraud and abuse. Users must also provide accurate information to create an account that could be used maliciously if leaked. Social media profiles contain dynamic information (generated by user behavior) or static Information (provided during registration). The data used in this study are both dynamic and static. To identify fake profiles, many dating sites usually display static profiles while dynamic profiles remain hidden. Issues such as privacy breaches, cyber bullying, and torture are often associated with the use of fake credentials to create fake documents to engage in malicious activities. Platforms like Facebook have security features like the Facebook Immune System (FIS) to protect user data, but these systems are not very effective at detecting fraudulent data. Various methods have been proposed to detect false signals and malicious content, each with its own advantages and disadvantages

Keywords: Privacy issues, Security issues, Scams, Abuse, Dating, Fake profiles, Detection, Negative content.

1. INTRODUCTION

Social media has become an online game that attracts many users who spend millions of minutes on these platforms every year. Various social networking (OSN) products include engagement generation platforms (such as MySpace), information-focused platforms (such as Google+ and Twitter), and social media capabilities (such as Flickr) that enable personal integration into modern systems. However, increasing concerns about security and protection of OSN's personal data are still seen as major challenges and goals. One would be losing money or time, be sent to reformatory, have their reputation harmed, or suffer connections to friends and family.

Nowadays, the great majority of SNs have very vulnerable privatization and safety measures and conduct longer verify the debts of regular users.

In actuality, the majority of SN applications have low privacy settings by default, which has made SNs an ideal venue for fraud and abuse. Social networks have made fraud or impersonator attempts easier for both skilled and unsuspecting offenders. To exacerbate matters, users must provide accurate information to be able to create an account on social media sites. Simple oversight of what users post online might result in disastrous losses, never mind if these bills were compromised. Online platforms will also have either passive or active profile data. Stationary understanding mentions to the data that the manipulator may supply when creating their profile, whereas active learning denotes to the fine print that is narrated by the network's architecture. One's realtime behaviours and location within a community are specimens of dynamical skills, whereas personal information and inclinations about the individual make up static info.

Most research conducted nowadays relies on both passive and active data. This isn't applicable to severalpublic media outlets, though, as only a small percentage of static pages are viewed and updated pages are typically hidden from the human chain. Many processes social networking issues, including those related to privacy, cyberbullying, abuse, slander, and a lot more. are several occasions where fraudulent personas on messaging platforms are used. False pictures are those that lack specificity, meaning they're descriptions of people who pose as someone with a false degree. False posts on Facebook frequently engage in harmful and undesired behaviour, which disrupts users of social media networks. False profiles are made by influence individuals through online platforms

2. LITERATURE REVIEW

TITLE: Fake The profiles Finding in Machine Learning for Social Media Platforms and NLP.

AUTHORS: P.SrinivasRao,

Dr. JayadevGyani, Dr. G. Narsimha The existing research upon fake profile verification in social networking sites employing device learning and natural language processing, or NLP, reveals a broad variety of strategies and techniques focused on tackling the challenges of privacy and security faced by malicious individuals. This has been emphasized in a number of studies.

These research efforts have highlighted the importance ofidentifying profiles of individuals into real and fake categories in instruction to reduce risks like identity theft, on the internet imitation, and the banquet of unlawful information. To discern between genuine and fraudulent profiles, one method—demonstrated by Chai et al.—focuses on machine learning approaches as interaction with users patterns. To enhance the user interface and pinpointing precision, their research highlights the reputation of integrating standard menu-driven algorithms using straightforward dialog-based navigational. The example of LinkedIn, as examined by Shalinda Adikari and Avinash Dutta, highlights the challenge of detecting fraudulent profiles unpaid to the scarcity of publicly accessible profile data plus the strict privacy regulations in place.

They suggested making use of a small amount of profile data and suitable Using data mining methods, professionals communities' bogus profile detecting can be improved.
Z. Halim et al. have conducted a separate investigation that uses latent semantic evaluation and spatio-temporal mining to identify the circles of harmful participants in social networking sites.

Their outcomes show that spatio-temporal co-occurrence can closely mimic real-world internet connections, and that identifying dangerous information and behaviour requires carefully selecting certain criteria. Furthermore, a study on spam & harmful communications in social networking sites by Saeed Abu-Nimeh et al. highlights the use of behavioural and a content-based assessment for ruling out undesired acts, emphasizing the need for robust detection systems.

Predictive algorithms like Support Vector Machines (SVM) and Bayes naïve, when combined with natural language processing (NLP) techniques, generally show promise for improving.

3. Existing System

Chai et al. The welcome reception of their letters is a testament to their thoughtfulness and wisdom. Although it uses the best methods in natural language processing and human-to-human interaction, the results of user testing of the technology are important. By comparing this simple model with a full menu, they found that users (mostly new users) preferred the conversational approach.

They also realized that contact management capabilities in the online sales environment must be tailored to meet each individual's unique needs. They have successfully developed a new concept that provides significant improvements in information processing, leadership and language distribution.
They believe free puzzles provide a powerful, customizable alternative to menus or searchable web layouts.People with real jobs prefer LinkedIn to other platforms. Due to the rapid development of social media, people can misuse social media for unfair and illegal activities.
Creating a fake profile can cause controversy. It can be difficult to detect without research. The social aspects of people's emotions in society are the main subject of modern realistic and theoretically developed answers to resolve this conflict. However, due to privacy requirements, such behavioural analyzes are strictly limited to information regarding users' public LinkedIn accounts.
Due to the limited number of biometric data available on the web, it is not possible to detect fake data using existing methods. Kaushik Dutta and Shalinda Adikari conducted research to identify the minimum profile information required to identify fake information on LinkedIn and clarify the process of searching for the right profile for jobs.
Halim Z. et al. It is recommended to use latent semantic analysis and spatiotemporal mining of conversations to find the customer business affected by the negative events. These results are potentially very encouraging because the real relationships and relations resulting from the spatiotemporal integration are similar. After determining the threshold

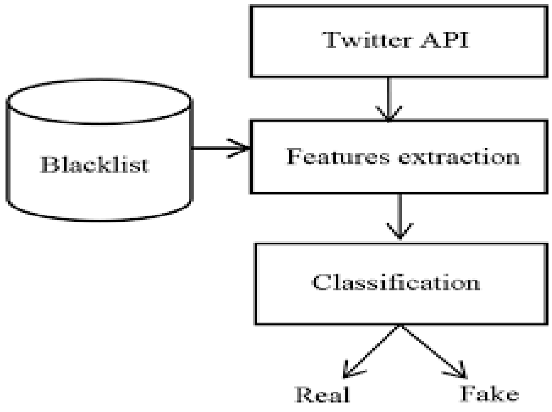


Fig 1: Flow chart

4. PROPOSED SYSTEM

In this article, we propose a method to detect fake social media profiles by combining natural language processing and machine learning.

SVM classifier and unknown Bayesian engine are also added to improve the accuracy of image error detection. Separate those that fall into other categories. The surface of the largest line connecting two groups is best for the SVM technique.

SVM uses an arbitrary plane to classify objects, separating all elements of a given group from the remaining elements of the group. Data points near and far from the hyperplane are auxiliary vectors.

The Naive Bayes method determines the probability that a particular item belongs to a person or group. In short, it is a classifier that uses random events. The model used by Naive Bayes is called "naive" because it assumes the existence of unusual features that are not affected by their frequency or otherwise. For example, let's say we want to detect false information using the time, current, language, and domain in which it was published or posted.

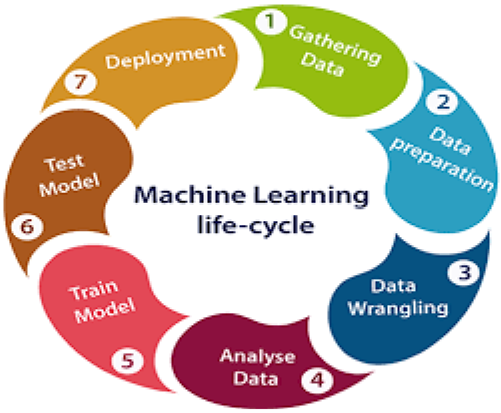


Fig 2: Machine Learning

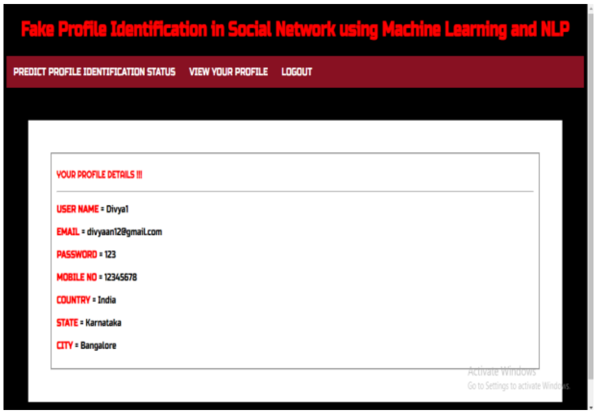
5. MODULE DESCRIPTION

IMPLEMENTATION

Service Provider: In order to access the module in question, the solution source must enter a valid username along with a password. Upon login successfully, he can perform several tasks like testing and training information sets, Get the ratio of the reviewed detect type, download the anticipated information sets, view the results of the review detected ratio, examine all external users, & assess the precision of the lessons learned and certified sets in a graphic form.

View and Authorize Users: The administrator can see a list of each user who are enrolled in that module. This permits the admin to examine user information such identity, email contact information, and satisfy, and it also allows the administration to grant access to users.

Remote User: A entire of a specified number of users that utilize this particular section. Prior to beginning first of the operations, the user must sign up. Following the login process, The user can do a quantity of tasks, like as view my characteristics, predict Reviews TYPE, and Registration and Registration.


Fake Profile Identification in Social Network using Machine Learning and NLP
PREDICT PROFILE IDENTIFICATION STATUS
VIEW YOUR PROFILE
LOGOUT
Activate Windows
Go to Settings to activate Windows.

YOUR PROFILE DETAILS !!!

USER NAME = Divya1

EMAIL = divyaan12@gmail.com

PASSWORD = 123

MOBILE NO = 12345678

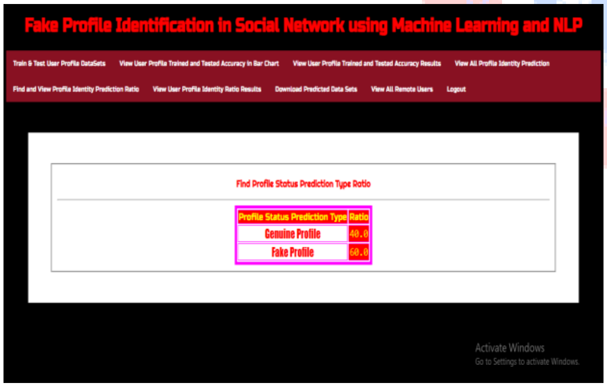
COUNTRY = India

STATE = Karnataka

CITY = Bangalore

Fig 3. Profile page

Shows how to identify fake profiles using machine learning and NLP to view user profiles containing personal details.


Fake Profile Identification in Social Network using Machine Learning and NLP
Train & Test User Profile DataSets
View User Profile Trained and Tested Accuracy in Bar Chart
View User Profile Trained and Tested Accuracy Results
View All Profile Identity Prediction
Find and View Profile Identity Prediction Ratio
View User Profile Identity Ratio Results
Download Predicted Data Sets
View All Remote Users
Logout
Activate Windows
Go to Settings to activate Windows.

Find Profile Status Prediction Type Ratio

Profile Status Prediction Type	Ratio
Genuine Profile	40.0
Fake Profile	60.0

Fig 4. Performance Analysis

Fig: Shows the profile status estimate, which shows real profiles and fake profiles on the platform.

6. RESULTS

Leveraging results in detecting scammers on social media using machine learning and natural language processing (NLP) to achieve success. Recent research shows that combining personal characteristics, user behavior, and social patterns with advanced machine learning can improve the accuracy of search results. Supervised learning models such as support vector machine (SVM), random forests, and neural networks have been used effectively to classify data as true or false.

Additionally, the integration of NLP technology to analyze user written content improves the ability to detect misinformation. Combinations combining multiple classifications have proven to be particularly powerful, providing greater accuracy and reducing false positives. Additionally, using graph embeddings to capture relationships between social networks helps improve search performance by providing a deeper understanding of the network structure.Taken together, the use of these cutting-edge tools has created an effective and efficient reporting system that improves the security and integrity of social platforms.

Test Cases

Test id	Analyzing	Expected output	Actual output
T1	Profile with username, pictures,post	Fake Profile	Fake profile
T2	Profile, username no profile picture	Fake profile	Fake profile
T3	Profile with username, bio, profile picture, verified mail,posts	Genuine profile	Genuine profile
T4	Detect fake Profile with incomplete resume	Fake Profile	Fake Profile

Table 1. Test Cases

7. CONCLUSION

In this article, we present machine learning algorithms and natural language processing techniques. This technique can easily detect fake people on social media platforms. We use Facebook profile settings in this study to detect fake profiles. The dataset and machine learning algorithms were analyzed using NLP techniques, and support vector machines and Naive Bayes analysis were used in classification.In this research, recognizing speed is increased using these type of learning techniques.

8. REFERENCES

[1] Michael Fire et al. (2012). "Strangers intrusiondetection-detecting spammers and fake profiles in social networks based on topology anomalies." Human Journal 1(1): 26-39.Günther, F. and S. Fritsch (2010). "neuralnet: Training of neural networks." The R Journal 2(1): 30-38

[2] Dr. S. Kannan, VairaprakashGurusamy, “Preprocessing Techniques for Text Mining”, 05 March 2015.

[3] Shalinda Adikari and Kaushik Dutta, Identifying Fake Profiles in LinkedIn, PACIS 2014 Proceedings, AISeL

[4] Z. Halim, M. Gul, N. ul Hassan, R. Baig, S. Rehman, and F. Naz,“Malicious users’ circle detection in social network based on spatiotemporal co-occurrence,” in Computer Networks and Information Technology(ICCNIT),2011 International Conference on, July, pp. 35–390.

[5] Liu Y, Gummadi K, Krishnamurthy B, Mislove A,” Analyzing Facebook privacy settings: Userexpectations vs. reality”, in: Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference,ACM,pp.61–70.

[6] Mahmood S, Desmedt Y,” Poster: preliminary analysisofgoogle?’s privacy. In: Proceedings of the 18th ACMconference on computer and communications security”, ACM 2011, pp.809–812.

[7] Stein T, Chen E, Mangla K,” Facebook immunesystem. In: Proceedings of the 4th workshop on social network systems”, ACM 2011, pp