JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

DETECTION OF FAKE PROFILE ON ONLINE SOCIAL MEDIA

Ishant Kundra

ABSTRACT:

Nowadays, online social media dominates the world in a variety of ways. The main benefits of online social media are that we can easily connect with people and communicate with them more effectively. This opened up a new avenue for potential attacks such as impersonation, false information, and so on. As per a recent survey, the number of accounts on social media is far greater than the number of users. This suggests that the number of fake accounts has increased in recent years. Due to the need for identifying these fake accounts on social media, we developed an innovative method to identify fake accounts in this paper. We used the gradient boosting algorithm in conjunction with a decision tree, as well as machine learning techniques such as neural networks and SVM.

Keywords: ***social media, machine learning, fake profile detection, Naïve bayes, Decision tree, Support vector machine (SVM), Artificial Neural Network.***

I. INTRODUCTIONS

The Online Social Networks such as Facebook, Twitter and LinkedIn, have been more popular over the past several years. People use OSNs to remain in contact with other other's, exchange news, arrange events, and even start their own e-business. Facebook community continues to expand with more than 2.2 billion monthly active users and 1.4 billion daily active users, with a growth of 11 percent on a year-over-year basis. For the goal to identify fraudulent accounts on the social media platforms the dataset collected was pre-processed and bogus accounts were identified using machine learning algorithms. The new models produced employed diverse tactics such automated posting or comments, distributing bogus information or spam with adverts to detect fake accounts. Due to the surge in the creation of the bogus accounts numerous algorithms with different qualities are use. Previously usage techniques like Naïve bayes, support vector machine, random forest has become ineffective in discovering the bogus accounts.

A. Anamoly Detection

"An anomaly is defined as "an event (or item) that deviates from some standard or reference event by more than some threshold in accordance with some similarity or distance metric on the event." The goal of anomaly detection systems is to determine whether a behavior is unusual enough to raise the possibility of an intrusion. A fundamental premise of anomaly detection is that assaults deviate from normal behavior.

1. *Naive Bayes:*

The Naive Bayes classification algorithm is a type of probabilistic classifier. It is based on probability models that amalgamate strong independence assumptions. The independence assumptions have negligible impact on reality. Thus, it is considered as naive. The feature matrix is composed of all the vectors (rows) in the dataset, each vector containing the value of dependent characteristics. The features in the preceding dataset are 'Outlook', 'Temperature', 'Humidity', and 'Windy'. For each row of the feature matrix, the response vector includes the value of the class variable (prediction or output). In above dataset, the class variable name is ‘Play golf’. It is referred to as Nave because it presupposes that the presence of a certain characteristic is unrelated to the occurrence of other traits. For instance, if the fruit is defined by its colour, shape, and flavour, a red, spherical, and sweet fruit is classified as an apple.

$$Gain(D|B) = H(D) - \sum_{v \in Values_B} \frac{|D_v|}{|D|}$$

A Naive Bayes model comprises of a large pyramid that includes the following dimensions:

- Input field name.
- Input field value for disjunct fields or input field value range for remembrance of fields.
- Consistent field value.

2. *Decision Tree:*

A decision tree is a distinctive type of probability tree that enables you to make a decision about some kind of drill. Decision Tree is a Supervised learning approach that can be used for both classification and Regression issues, however generally it is favoured for addressing Classification problems. It is a graphical depiction used to get all feasible answers to a problem/decision under certain parameters. It is named a decision tree because, like a tree, it begins with the root node and grows via additional branches to form a tree-like structure.

3. *Support Vector Machine*

The SVM is a linear model for classification and regression problems. It can solve linear and non-linear problems and work splendidly for many practical problems. Support -vector machines (SVMs, also support - vector networks) are the supervised learning models with associated learning algorithms that analyse data used for classification and regression analysis. For the given labelled training data (supervised learning), the algorithm outputs an optimal hyper plane which categorises new examples.

4. *Artificial Neural Network*

The Artificial Neural Networks (ANNs) are optimized data-driven modelling tools widely used for nonlinear systems dynamic modelling and Recognition. The features in the preceding dataset are 'Outlook', 'Temperature', 'Humidity', and 'Windy'. For each row of the feature matrix, the response vector includes the value of the class variable (prediction or output). In the above dataset, the class variable name is 'Play golf'.

5. *Random forest*

A supervised classification algorithm is the random forest algorithm. This algorithm, as the name implies, creates a forest out of a number of trees. The more trees there are in the forest, the more robust it appears. Similarly, in the random forest classifier, the greater the number of trees in the forest, the higher the accuracy results.

B. Few signs of a fake profile:

- One of the primary signals that you are confronting a phoney account or bot is the profile picture. This is frequently a part of the user’s profile: a logo, their business picture or the person themself.
- It was created lately – within the past year or two, until the person may be very younger, most people opened our fb accounts in 2006-2007. Look for the indication of long-term use of the account.
- Little or no contacts in common. When the user profile has nothing in common with you such as friends or even a professional interest, and they are continuously trying to add you, it’s likely for malicious reasons.
- When a profile adds you but once you accept them there’s no greater interplay with that user. This shows that the profile is fake and person behind the fake profile/identity just got what he/she wanted and will avoid chatting with you in the hopes you lose sight about it.

II. LITERATURE REVIEW OF RELATED WORK

The dataset generated was pre-processed in order to detect fake accounts on social media platforms, and fake accounts were determined using machine learning algorithms. For the detection of fake accounts, the classification performances of the algorithms Random Forest, Neural Network, and Support Vector Machines are used. The accuracy rates of detecting fake accounts using the algorithms mentioned are compared, and the algorithm with the highest accuracy rate is noted.

In 2018, Y. Cheng et.al, have presented Fake Buster: A Robust fake Account detection by Activity Analysis. They proposed an innovative method to detect fake account in OSNs (Online Social Networks). It is developed for accurately detecting fake account among social network users, based on various activity collection and analysis. In this research they have use Random Forest, along with C$.5 and Adaptive Boosting, with decision stump as a second classifier that created behind it to focus on the instance in the training data, in case the accuracy of the first classifier is less effective. After finish training, a cluster of features for each testing account will input into models and output a prediction with rank score indicating the likelihood of being fake account.

In 2019, F. Masood et.al, have presented in their work Spammer detection and fake user identification on social network. A look at the methods used to detect spammers on Twitter. Spammers can be identified using the following criteria: (i) fake content, (ii) URL-based spam detection, (iii) spam detection in trending topics, and (iv) fake user identification. The proposed spammer detection taxonomy on Twitter is divided into four major classes: I fake content, (ii) URL-based spam detection, (iii) detecting spam in trending topics, and (iv) fake user identification.

M. Ibrahim et.al, have presented in their work Malicious Account Detection on Twitter based on Tweet Account features using Machine Learning. In this research, build a malicious account detection that can distinguish genuine accounts from malicious accounts using only tweet features of the accounts. Also managed to build a multi-class classification for the two types of malicious accounts, fake followers and spam bots using only tweet features. Lastly, found the best combination of algorithms, features, and data transformation scenario that suits best of our problem.

Ferrara et al. proposed a method for detecting bot users on Twitter based on highly shared characteristics that distinguish them from legitimate users. They used a machine learning technique and behavioral patterns between legitimate and bot accounts in their proposed method to classify accounts as bot or legitimate.

B. Anand et al. created a new system to detect fake users on the Twitter platform by employing a graph-based semi-supervised learning algorithm (EGSLA) and analyzing and collecting behavioral and user-generated content (UGC) data. The model gathered information from users, analyzed it to extract useful features, then classified these features and made decisions. In terms of classification accuracy, the experimental results show that the EGSLA algorithm outperformed other algorithms such as decision trees, KNN, SVM, and game theory-based methods.

III. PROBLEM STATEMENT & OBJECTIVES

There are many of difficulties on social networking sites; one of the problems is bogus accounts in social networking sites which lead to numerous troubles. It impacts the users on social networking sites in different ways. Online social network suffers from many bogus accounts. There are extremely less approaches to discover the fake accounts on the Facebook. Even established techniques do not contain extremely good precision. This suggested approach combines the weighted feature set with machine learning strategies to acquire the greatest outcomes.

First, the social networks graph's adjacency matrix will be computed. The measures of network friend likenesses between nodes (social network users) will then be computed. The similarity matrix was then computed for each of the defined measures, such as common friends' similarity, Jaccard similarity, cosine similarity, and others. At the end of this step, various matrices representing node similarity were displayed. Key attributes to look far and monitor continuous NLP, matrix, graph, ANN with the help of all this we will be able to look far as well Artificial Neural Network so that it will be updated according to the upcoming fake accounts. If government ID's, facial recognition and voice recognition will be applied to our model then it will make our work easy.

A. proposed Idea/Objectives

The aim of paper is to identify the fake profile on social media platform. Protect security and privacy threats when someone wants to attack on personal and professional life. Identity theft, terrorist propaganda, graphic violence, adult nudity, terrorist propaganda and sexual activity.

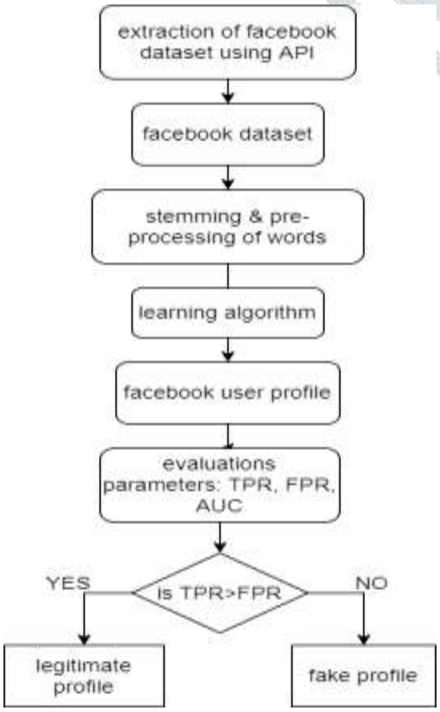
extraction of facebook dataset using API
facebook dataset
stemming & pre-processing of words
learning algorithm
facebook user profile
evaluations parameters: TPR, FPR, AUC
YES
is TPR>FPR
NO
legitimate profile
fake profile

Fig1: Process flow chart of detection of anomalies in social media

B. Methods

1. Data collection

Like maximum social media platforms, the public Instagram developer API handiest offers the public statistics of customers. It isn't viable to access some users' activities and login facts, especially while a person already has set that account to non-public mode. This hassle is taken into consideration as an obstacle to the system of information series. To resolve the troubles and crawl users' statistics, we've got evolved a selected records crawler and characteristic series tool defined inside the following steps.

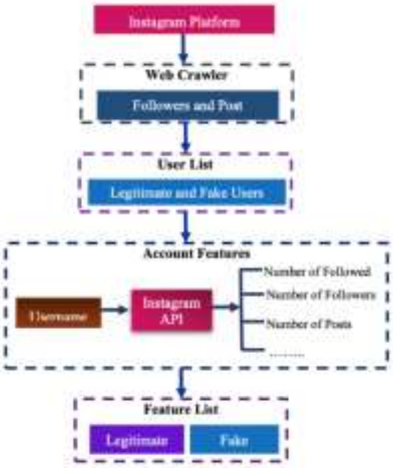

Fig4: Data Collection

With the help of four of the essential features which are:

1. The distribution of accounts with a profile picture in the dataset, and it indicates most accounts that have not set profile pictures to their accounts belong to the fake category.
2. Most fake accounts followed more people than their followers. Most fake users created only to increase the number of followers of regular users and that is because many Instagram regular users try to buy fame using increase the number of their account's followers.
3. Most fake accounts do not contain many posts or mostly have zero or one post because many of these accounts only aim at following other users or advertising, so their creator consumes a brief time at the increasing number in their post or design appearance of them.

IV. ANOMALY DETECTION BASED ON GRAPH STRUCTURE

A. To detect anomalies by applying graph-based techniques

A graph of a social network can be clarified as G= {V, E} in which V is the nodes set depicting end-users while E is the edges set representing the links between users. A Graph representing social network data is normally categorised into undirected or directed based on the threshold route, unweighted or weighted primarily based on weights of edge and unattributed, or attributed based on the availability of attributes on nodes and/or edge attributes. Anomaly detection primarily based on Graph method is typically used to locate: unusual graph substructures. Absence of usual edges or nodes.

Presence of unusual edges or nodes. Changes in features of edges or nodes.

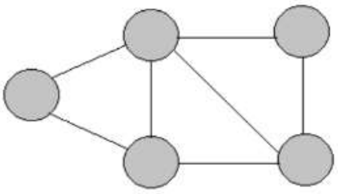

Fig1: Aspects of anomalies in graph on social networks.

A Graph depicting social network data is often classed into undirected or directed based on the edge direction, unweighted or weighted based on weights of edge and unattributed. There are various troubles for which developing a scalable approach for anomaly detection on graph data is difficult. These problems are:

Traditional approaches to detecting anomalies do not apply to graphs. Anomaly in graph-based data typically depends on the application. High time and space complexities due to full graph traversal for finding anomalies.

B. Why to use graph

A social network is usually shaped as a Graph in which nodes represent the users, and edges represent the links amid the users. Approaches for graph mining to detect anomalies in social networks are a growing field because it is tough for attackers to fake it as long as the vitality of the graph is maintained. How the users are grouped and interact with each other in social networks has a strong basis in Anomaly detection. A social network is described as a "group of internet-based applications that are built on the ideological and technological basis of the web and enable the creation and exchange of user-generated content." Understanding such a network provides us with useful insights into how social communities are formed and how they interact with one another. As a result, in order to understand the network, a graphical view must be generated, making future refinement or analysis easier.

The structure that shows the relationships between individuals and organizations is known as a social network. It denotes the various social familiarities that connect them, ranging from casual acquaintance to close familiar bonds. A social network can be depicted by an undirected graph G (V, E), where V is the set of vertices expressing users and E is the set of edges representing social ties such as friendship, kinship, and so on. Graphs are utilized to represent communication networks or social networks, and studying some of their basic properties can help in the evaluation and improvement of networking solutions.

The purpose of using a graphical model in a social network is to more elaborately and systematically describe the network. Using a graphical model allows us to elaborately and precisely describe the properties of a network. The relationship between individuals can be mapped graphically, and how one can access the resource(s) of another user(s) can be described. Because social networks contain a large amount of sensitive data, privacy is a major concern when using them. A more detailed graph theoretical model of a social network can help to improve the ease of use of social networks and keep user information secure within the social network community and beyond.

C. Aspects of social network anomaly detection

Input network's structure is an essential characteristic of approaches to detect anomalies. There are two main categories in which methods to detect anomalies are categorized as:

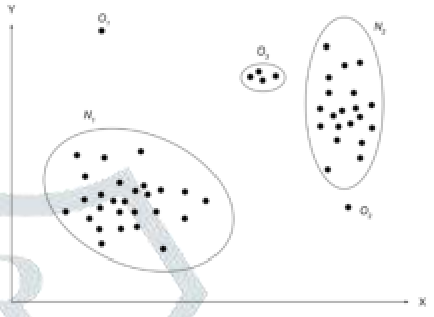

Fig2: simple anomaly detections in 2-D spaces.

Point Anomalies: - If one thing may be viewed against other objects as anomaly, it is a point anomaly. This is the simplest anomaly category and a lot of study incorporate them. Taking into mind example shown in Figure 1 points O_1 and O_2 are point anomalies

***Collective Anomalies:* -** If certain related things may be detected against other objects as abnormality. Individual thing can't be anomalous in this scenario, only group of objects.

D. Methods to Detect Anomalies

Static unattributed anomaly: Means the profile that shows no changes and have a source which is strange or outlier. Akoglu et al. [19] observed that aberrant behaviour in social networks may be characterised by both near star structure or near clique structure. In a social network, curve of power law is altered while considering the major deviation with the aid of residuals. Various characteristics of egonet have followed this approach. Hassan zadeh et al. in [20] demonstrated that typical and anomalous egonets (near stars or near cliques) are discriminated by using power-law formula. Using Signal processing methods are also a significant strategy to discover static unattributed abnormalities [21]. Signal processing application derives from the study done on community identification and graph splitting approaches. A signal embedded in a huge graph is classified as anomalous subgraphs.

Static attributed anomalies: Means the profile which don't change and cause by someone but are outlier or strange. A context may be characterised by considering node and edge qualities in addition to the network topology, in which case normal egonets may seem to be atypical [19]. On the other hand, node and edge combinations inside an egonet's context may seem to be unusual. Apart from recognising stars and cliques using unattributed characteristics, Akoglu and colleagues studied egonets in terms of attributes.

Dynamic unattributed anomalies: means the profile which changes constantly, don't have source and is outlier or strange too. Dynamic unattributed anomalies develop as a result of changes in communication patterns over time. For instance, one step's network structure is clearly different from the preceding one. Conventional techniques may be used to study the time series created when different graph features are taken into consideration. The static inquiry may also be utilised as a time series topic, with the value changing over time. The difficulty here is in choosing a handy feature that sufficiently distracts from the intriguing real-world aspect.

Dynamic attributed anomalies: means the profile which changes constantly have source or caused by someone but is outlier or strange. Dynamic attributed anomalies detection examines edge probability between two nodes is based on a linear combination of node labels, and it is an extension of the approach to analyse the signals for static unattributed anomalies.

E. Besides graph what are the other ways to detect anomaly

This work trained the behaviour classifier utilising the quicker R-CNN algorithm, the object detection algorithm for picture deep learning technique, to develop the behaviour classifier. To train the behaviour classifier, it initially specified nine behaviours.

- ***Behaviour based techniques***

Behaviour based techniques handle the behavioural properties of the users such as number and content of messages, content of the items shared, number of likes or comments on a post and duration of a conversation. The photographs were acquired using the Extreme Picture Finder System from the web to learn the nine stated characteristics. The Extreme Picture Finder System looks for photos linked to terms on the web by inputting the keyword for the examined image, and it may be downloaded with a single click. Duplicate photos may occur in image datasets retrieved using the Extreme Picture Finder System, which creates an inefficient learning process and increases the learning time. Some of the popular behaviour-based techniques are:

1. Content-based filtering
2. Structure-based filtering
3. Spectral Based techniques

Spectral anomaly detection techniques help in detecting anomalies using some spectral characteristics in the spectral space of a graph. Different complex measures such as eigenvalues or eigenvectors applicable to the adjacency matrix or the different hypergraph algorithms used for Laplacian graphs are focused in these methods. We construct the universal graph-filtering based spectral decomposition as finding an undirected, weighted and linked graph G, and two graph-based filters ($h(\lambda)$ and $\tilde{h}(\lambda)$), that answer the optimization problem.

F. What are the different analytics methods to use to analyse social networking data?

Data aggregation and mining, network propagation modeling, network modeling and sampling, user attribute and behavior analysis, community-maintained resource support, location-based interaction analysis, social sharing and filtering, recommender system development, and link prediction and entity resolution are some common network analysis applications. Even we will create few fake accounts to check whether it is working or not. Social media analysis includes three primary steps: data identification, data analysis, and information interpretation. To optimise the value gained at each stage of the process, analysts may formulate a question that has to be addressed.

Data identifications

The process of data identification entails determining which subsets of accessible data to analyse. Once understood, raw data is helpful. After analysis, data might begin to transmit a message. Information is defined as any data that sends a meaningful message.

Data analysis

It is a collection of actions that aid in the transformation of raw data into insight, resulting in a new basis of knowledge and corporate value. In other words, data analysis is the phase that takes filtered data as input and converts it to knowledge that analysts can use.

Information interpretation

The insights gained via analysis might be as diverse as the initial inquiry stated in step one. At this level, since the information is being received by non-technical business users, the manner in which the data is presented becomes critical.

V. CONCLUSION AND FUTURE RESEARCH WORK

In this paper we have long past via plenty of methods to resolve the trouble and at the end we decided to go together with NLP, Naive Bayes, Decision tree, Support Vector Machine ,Artificial Neural Network, facial recognition, voice recognition and API techniques so that our accuracy will be greater as well as sealed in phrases of safety of the user as we will be using NLP, Naive bayes, Decision tree, Support vector machine, Artificial Neural Networks with API techniques which does the equal work so this way our accuracy will be extra to detect the fake profile. In addition to it we have introduced two new approaches which is facial recognition and voice recognition for more secure for user to engage with different people and our future research work would be addition of ID proof even as making the profile so that we could end the beginning of the fake profile.

VI. References

[1] A. Gupta, and R. Kaushal, "*Towards Detecting Fake User Accounts in Facebook"*, ISEA Asia Security and Privacy (ISEASP), 2017.

[2] Estee van der Walt, J.H.P. Eloff, and J. Grobler, *"Cyber-security: Identity Deception Detection on Social Media Platforms"*, Computers & Security, June 2018.

[3] P. Krishnan, D. J. Aravindhar, and P. B. P. Reddy, "*Finite Automata for Fake Profile Identification in Online Social Networks"*, 4th International Conference on Intelligent Computing and Control Systems (ICICCS), 2020.

[4] Buket Erşahin, Özlem Aktaş, Deniz Kılınç, and Ceyhun Akyol, "*Twitter fake account detection"*, International Conference on Computer Science and Engineering (UBMK), 2017.

[5] J. Jia, B. Wang, and N. Z. Gong, *Random Walk based "Fake Account Detection in Online Social Networks"*, 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2017.

[6] B. Wang, Le Zhang, and N. Z. Gong, "*Sybilscar: Sybil detection in online social networks via local rule based propagation"*. In INFOCOM, 2017.

[7] G. Stringhini, C. Kruegel, and G. Vigna, "*Detecting spammers on social networks"*, 26th Annual Computer Security Applications Conference, ACM, 2010.

[8] A. A. Amleshwaram, N. Reddy, S. Yadav, G. Gu, and C. Yang, "*CATS: Characterizing automation of Twitter spammers"*, Communication Systems and Networks (COMSNETS), 2013 Fifth International Conference, IEEE , 2013.

[9] S. Kumar, S. Kandasamy, and Deepa K., "*On Privacy and Security in Social Media – A Comprehensive Study"*, Procedia Computer Science 78. International Conference on Information Security & Privacy, 2016.

[10] S. K. Shama, K. S. Nandini, P.Bhavya Anjali, and K. D. Manaswi, "*Fake Profile Identification in Online Social Network"s*, International Journal of Recent Technology and Engineering, November 2019.

[11] S. Deliri, and M. Albanese, "*Security and Privacy Issues in Social Networks"*, 2015.

[12] Bhume Bhumiratana, *"A Model for Automating Persistent Identity Clone in Online Social Network"*, IEEE, 2011.

[13] Z. Chu, S. Gianvecchio, H. Wang, and S. Jajodia, "*Who is tweeting on Twitter: Human, bot, or cyborg ?"*, 26th Annual Computer Security Applications Conference (ACSAC), 2010.

[14] S. Gurajala, J. S. White, B. Hudson, and J. N. Matthews, *"Fake Twitter accounts: Profile characteristics obtained using an activity-based pattern detection approach"*, International Conference on Social Media and Society, 2015.

[15] M. Conti, R. Poovendran, and M. Secchiero, "*FakeBook: Detecting fake profiles in on-line social networks"*, IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, ASONAM 2012, August 2012.

[16] S. Gurajala, J. White, B. Hudson, and J. Matthews, *Profile characteristics of fake Twitter accounts*, Big Data Society, 2016.

[17] G. Kontaxis, I. Polakis, S. Ioannidis, and E. P. Markatos, "*Detecting social network profile cloning"*, 3rd International workshop on security and social networking, USA, 2011.