International Journal of Management, IT & Engineering
Vol. 9 Issue 4, April 2019,
ISSN: 2249-0558 Impact Factor: 7.119
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

Fake Identities in Online Social Media- A Comprehensive Survey

Usha Rani [1], Anoop Sharma [2]
[1]Research Scholar, Dept. of Computer Science, Singhania University, Pacheri Bari,Jhunjhunu, Rajasthan.
[2]Dean of Computer Science and IT, Dept. of Computer Science, Singhania University, Pacheri Bari,Jhunjhunu, Rajasthan
[1] gc.ushadahiya@gmail.com, [2] sharmaanoop001@gmail.com

Abstract

In the present era, online Social Networks (OSNs) are the most popular and rapid information propagation applications on the internet. Some are authentic users but some are illegitimate users. These illegitimate users are involved in fraudulent activities against social network users. Among these activities are fake accounts or profiles are created using a fake identity. Traditional methods cannot distinguish between real and fake accounts efficiently. With the advancement of time, the new models, techniques, or methods are being created considering different approaches such as automatic posts or comments, spreading false information, or spam with advertisements to identify fake accounts. There is also a scenario of detecting fake accounts in online social networks automatically. Different classifiers which are based on machine learning approaches are used. Different classifiers are based on different algorithms like Naïve Bayes, Support Vector Machine, Random Forest, Neural Network, Gradient Boosting, Decision Tree, etc. This paper includes a comprehensive survey on fake identities and approaches that deal with these fake identities (account or profile).

Keywords: Online Social Media, Fake Account Detection, Machine learning, Support Vector Machine, Decision tree, Naïve Bayes Classification Method

I. Introduction

The widespread use of social media has become both a boon and a bane for the society. **Internet identity**, also **online identity**, or **internet persona** is a social identity that an Internet user establishes in online communities and websites. It can also be considered as an actively constructed presentation of oneself [1]. Although some people choose to use their real names online, some of the Internet users prefer to be anonymous, identifying themselves through pseudonyms, which reveal varying amounts of personally identifiable information. An online identity may even be determined by a user's relationship to a certain social group. Some can even be deceptive about their identity. Using Social media for online fraud and spreading false information is increasing at a rapid pace.

In today's modern society, social media plays a vital role in everyone's life. The general purpose of social media is to keep in touch with friends, sharing news, etc. Although, social media is one of the preferred means of communication it has become a target for spammers and scammers alike. The number of users in social media is increasing exponentially. Identity d**e**ception on big data platforms like social media is an increasing problem, due to continued growth and exponential evolvement of these platforms.

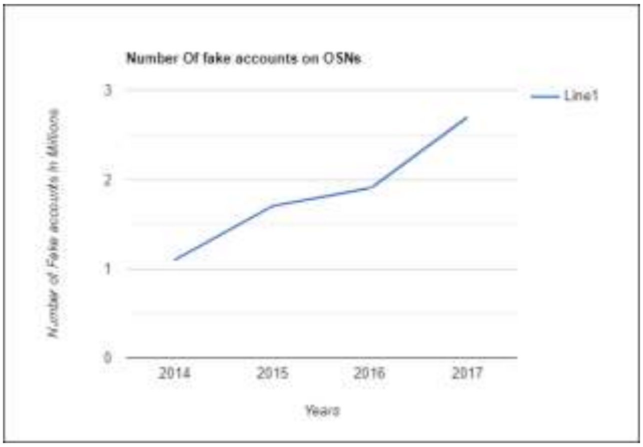

Fig 1.1 Graph Showing increase in the number of Fake accounts over the years

Fake accounts can be either human-generated, computer-generated (also referred to as "bots"), or cyborgs. A cyborg is a half-human, half-bot account. Such an account is manually opened by a human, but from then onwards the actions are automated by a bot. Variations exist between bots and human accounts. Bots are known as "Sybil" accounts when the accounts are fake and not stolen from legitimate users. On the other hand, fake human accounts are known as "trolls" when their purpose is to defame the character of another person [2][3].

1.2 Classification

Classification is a data mining technique that allocates objects in a group to target categories or classes. The goal of classification is to perfectly calculate the target class for every case in the data. Data is classified based on the class label given to the data. Classification is a two-step process. The first step is learning in which classification algorithm analyzes the training data. The second step in classification is in which test data is used to calculate the accuracy of data. Classification predicts the result based on the specified input. Item is belonged to which class is calculated by classification algorithms based on the training dataset. Neural Networks and SVM is the most successful technique for classification. The machine learning (ML) approach works on individual fake accounts as well as on clusters of fake accounts created by the same agent. The approach used mainly with these classifiers is a feature-based classification approach [4] and used in different fake user scenarios.

Case 1: Individual Fake Accounts

Humans, in general, behave differently from fake or bot accounts. If this difference in behavior can be captured in numerical or categorical attributes, then machine learning techniques can be applied to detect real from fake. This is the essence of feature-based classification approaches to detect malicious accounts. The ML process to detect real or fake status at the account level has three components:

- **Feature Design:** Individual users and groups of users in a network can be described using two categories of features. Depending on the time-sensitivity of detecting fake users, features engineered can come from one or both of the categories. First is the attributes present at or around registration time i.e. Profile Features while second is attributes that develop over time i.e. connections with other users in the network, activity, or behavior patterns.
- **Feature Selection:** In an OSN (Online Social Network), there may be a large number of attributes associated with an account. Using all the features may become computationally expensive. There may be redundancy in some of the features or some may not be good predictors of user status. Feature selection addresses some of these concerns. Wrapper and Filter methods are commonly used to include the best predictors. A weight is assigned to each attribute and the ones selected are those with weights above a certain threshold.
- **Model Training and Evaluation:** Several machine learning methods are used for model training as well as to evaluate the models**.** Some supervised machine learning algorithms like Random Forest, Decision Tree, Support Vector Machine, Naive Bayes, and Neural Network are used to detect fake accounts. These algorithms perform well in classification tasks. Weighted attributes determined from the feature selection step can be applied to these algorithms. Metrics commonly used here are Precision, Recall, and F-score.

Case 2: Clusters of fake accounts created by the same agent

In a large scale OSN, a bad actor can create dozens to thousands of malicious accounts. Predicting each account, as most fake user detection techniques do, may not be scalable or efficient. In such a situation, Cluster level detection is desirable here.

Legitimate user clusters display variation in patterns of profiles while groups of fake accounts generated by a single actor show the similar distribution and attribute frequencies. Hence, engineering features to identify the entire cluster allow the identification of fake account clusters.

The key difference between methods that predict the status of each user and the status of a community is the level of features i.e. individual or cluster. Cluster Detection Machine Learning Pipeline is the tool employed to identify these instances. To be run on clusters it operates on three major components which are:

- **Cluster Builder:** This component takes the raw list of accounts and builds clusters of accounts along with their raw features. There are 3 user-specified parameters fed to this module
  a) minimum and maximum cluster size
  b) period of accounts registered (e.g. last 24 hours), and
  c) Clustering criteria (e.g. registration IP address).

The output of this component is a table of accounts, where each row represents one account and contains features like the user's name, organization, education, and cluster identifier unique to the account's cluster. The cluster builder also uses the fake or real status of individual accounts to label clusters as fake or real. A threshold 'x' decides cluster labels — fewer than x percent fake accounts in the cluster, then it is a real cluster.

- **Profile Featurizer:** This second module converts raw data for each cluster into a single numerical vector representing the cluster. It is implemented as a set of functions that extract information from the raw features. The features could be:
  a) **Basic distribution features** — these are the statistical measures for each column. Like mean or quartiles for numerical features, the number of unique values for categorical features.
  b) **Pattern features** — Mapping of user-generated text to a categorical space (e.g. patterns in email addresses).
  c) **Frequency features** — Frequency of overall individual accounts and their distribution over these frequencies of each feature value are considered. Legitimate account clusters have some high-frequency and some low-frequency data, but malicious account clusters do display less variation in their data frequencies.
- **Account Scorer:** This third component is to train the models and evaluate their performance on previously unseen data. The module is either executed in the *training mode* or *evaluation mode*. The output is either a model description and evaluation metrics (training mode) or a cluster score (evaluation mode) which is the likelihood of the cluster composed of fake accounts.

1.2.1 Principal Component Analysis

The principal component analysis is the feature selection technique. It is used to reduce the dimensions of data and also reduce the computational complexity. The principal component analysis is a ranking based technique. It calculates the eigenvectors and eigenvalues. Based on eigenvalues, principal component analysis arranges the variables of features from ascending to descending order. The PCA is one of the seven Techniques for Data Dimensionality Reduction. The rest are Missing Values Ratio, Low Variance Filter, High Correlation Filter, Random Forests / Ensemble Trees, Backward Feature Elimination, Forward Feature Construction. Dimensionality reduction is the process of reducing the number of random variables or attributes under consideration. If a dataset with hundreds of features (columns in the database), then these features of attributes of data can be reduced by combining or merging them in such a way that it will not loose much of the significant characteristics of the original dataset. Principal component analysis reduces the data dimensions having a large number of variables and also increases the accuracy. With the least number of variables, it is easy to calculate the results with lesser time and high accuracy. It means principal component analysis also helps to increase the computational speed of the algorithm. The Principal component analysis also finds the related variable and provides the ranking to a related set of variables. [5]

1.3 Machine Learning Methods

There is a range of machine learning techniques that have been developed to detect fake accounts in social networking sites. The machine learning methods can be supervised as well as unsupervised.

- **Supervised learning methods**

Some of the supervised learning techniques are Neural Network, Naive Bayes, Markov Model, and Bayesian Network. In recent researches, it has been found that these techniques make available enhanced results to detect fake accounts. Neural Network consists of many interconnected processing elements. It takes decisions just like a human brain. SVM is supervised machine learning techniques used for classification. It finds the hyperplane to classify the data. Neural networks and SVM can accept a large amount of random data and suitable to detect fake accounts on social networking sites based on various characteristics of accounts. Naive Bayes classifier is based on Bayes' theorem. It predicts the probability that a given variable belongs to a particular class. Moreover, Natural language processing (NLP) techniques can be implemented to detect fake accounts more accurately. Brief description of some supervised machine learning methods is as follows:

- **Neural Networks**

The basic idea of Neural Network is to simulate lots of densely interconnected brain cells inside a computer to make decisions like humans. We don't have to program it to learn explicitly, it learns by itself just like a brain.

- **Support Vector Machine (SVM)**

SVM (support vector machine) is a supervised machine learning technique used to classify the data. SVM provides higher accuracy than the other classification techniques. The basic idea behind SVM is to maximize the margin of data by discovering the best possible separating hyperplane. Multiple hyperplanes separate the data but the best one is chosen. After that to get the margin, the difference between the hyperplane and the closest data point is computed and this value is doubled but choosing the best hyper plane among many hyper planes helps to classify the data accurately. SVM provides higher accuracy than the other classification techniques. There are two types of SVM:-

a) **Linear SVM**: - In linear SVM the plane is linear. In it, there is one hyperplane separating the data. One side of data belongs to one class and other side data belongs to another class. In linear SVM data is simply separable. There is no complexity while the separation of data into classes like nonlinear SVM. Therefore it used only for simple classification of data.

b) **Non-Linear SVM**:- In the non-linear SVM plane is not linear. In this, the kernel function is used for the transformation of input space into high dimensional space

- **Naïve Bayes Algorithm**

Naive Bayes algorithm is the algorithm that learns the chance of an object with designated features belonging to a unique crew/category. In brief, it's a probabilistic classifier. The

Naive Bayes algorithm is called "naive" on account that it makes the belief that the occurrence of a distinct feature is independent of the prevalence of other aspects. In a case of determining false profiles based on its time, date of publication or posts, language, and geo-position, even if these points depend upon every different or on the presence of the other facets, all of these properties contribute to the probability that the false profile.

- **Random Forest Algorithm**

This algorithm identifies the fake account. It is efficient when it has the correct inputs and when it has all the inputs. When some of the inputs are missing it becomes difficult for the algorithm to produce the output. The disadvantage of the Random Forest Algorithm is that this algorithm has few downsides such as inefficiency to handle the categorical variables which have a different number of levels.

- **Gradient Boosting Algorithm**

The gradient boosting algorithm is like a random forest algorithm that uses decision trees as its main component. This algorithm gives us an output even if some inputs are missing. This is the major reason for choosing this algorithm. Due to the use of this algorithm we were able to get highly accurate results. Moreover, Gradient boosting is the most effective algorithm for classification problems. The basic principle of gradient boosting is that it forms a strong rule from multiple weak learners. The main advantage of this algorithm is that it predicts perfectly in the absence of any one of the used factors. The decision trees formed are combined and predicted value is found.

1.3.2 Unsupervised Machine Learning

The most commonly used unsupervised machine learning technique is Clustering. It is the process of grouping a set of physical or abstract objects into classes of related objects. A cluster is a collection of data objects that are related to one another within a similar cluster and are unrelated to the objects in other clusters. Clustering is used to discover the pattern information. In clustering, the class label is not known. There are various clustering techniques, but K-medoids is a commonly used technique. This algorithm similarly works as a K-mean algorithm with a slight difference. K-mean algorithm calculates the mean of data items as a centroid whereas K-Mediod randomly selects the data points called medoids. Median refers to data items having less average dissimilarity with other data items in the cluster. K-Medoid algorithm is better than K-mean algorithm because it is vigorous to outliers.K-medoid algorithm minimizes R squared error.

II. Literature Survey

Many studies have been done regarding different machine learning methods which are used as classifiers to differentiate between fake and real accounts as well as detecting fake accounts. Below is the summary showing different studies done on it.

Table 1.1 : Different studies done on detecting fake accounts using machine learning classifiers

Author	**Year**	**Classifier**	**Processing method**
S.Kiruthiga et al.	2014	Naive Bayes	Cosine similarity
M.Alsaleh et al.	2014	Decision tree, random forest, Naive Bayes, multilayer neural networks	Feature set
Y.Shen et al.	2014	SVM	Feature set
M.Egele et al.	2015	COMPA	Behavioral profiles
D. Freeman et al.	2015	SVM, Random forest	Registration IP address
Yazan Boshmaf	2015	Random forest, SVM, Naive Bayes	Feature set
Sazzadur Rahman et al.	2015	FRAppE	Feature set
A.Azab et al.	2016	SVM, Neural Networks, Random Forest, Decision Tree, Naive Bayes	Feature set
Estee Van Der Walt	2018	Random Forest, Boosting Technique, SVM	Feature Set
Rohit Raturi	2018	NLP, CNB	Text Classification
Sumit Milind Kulkarni	2018	SVM, Naïve Bayes, Decision Tree	Feature Set
M. Mohammadreza	2018	Medium Gaussian SVM	Similarity measures like cosine, Jaccard, L1-Measure & Weight Similarity
P. Srinivas Rao	2018	SVM, NLP, Naïve Bayes	Feature Set

.

III. A Survey on major Online Social Networks - Facebook & Twitter

There are several online Social Networks like Instagram, LinkedIn, Pinterest, Twitter, Facebook, etc. In this paper the authors have reviewed the two platforms namely facebook and Twitter. Both of these OSNs have become a popular means for creating and sharing personal profiles, text, pictures, audios, and videos, and for finding and making friends, thereby facilitating the users to interact with people across the globe. In the following sections the details of these major OSNs along with studies done are discussed.

Case 1: Facebook OSN (Online Social Network)

With 1.44 billion monthly active users 1 (MAUs) and a potentially rich source of information, Facebook is one of the largest OSNs in the world. This popularity has also given rise to the growth of a black-market industry that leverages the trust relationship inherent between the users in these OSNs to offer illegal services like buying Facebook likes, comments, and shares. All these malicious activities involve the mass creation of fake accounts for effectively carrying out online attacks on the OSNs. Fake accounts are categorized into what Facebook calls as duplicate accounts and false accounts . A duplicate account refers to an account maintained by a user in addition to his/her principal account. False accounts are further broken down into two categories user-misclassified accounts and undesirable accounts User-misclassified accounts represent the personal profiles created by users for a business, organization, or nonhuman entity such as a pet (Facebook terms of service permits such entities as a Page rather than a personal profile). On the other hand, undesirable accounts are the user profiles that are intended to be used for purposes that violate Facebook terms of service, such as spamming. [10]

.

False profiles are the profiles that are not specific i.e. they are the profiles of men and women with false credentials. The false Facebook profiles more commonly are indulged in malicious and undesirable activities causing problems to the social community, customers. Individuals create fake profiles for social engineering, online impersonation to defame, a man or woman, promoting and campaigning for a character, or a crowd of individuals. Facebook has its security system to guard person credentials against spamming, phishing, and so on. This security system is called the Facebook immune system (FIS). This FIS is unable to observe fake profiles created on Facebook via customers to a bigger extent.

As per the research article "How Facebook uses machine learning to detect fake accounts" Facebook took down on average close to two billion fake accounts per quarter. Fraudsters used these fake accounts to spread spam, phishing links, or malware. It's a lucrative business that can be devastating for any innocent users that it snares. The machine learning system of Facebook distinguishes between two types of fake accounts. First, there are "user-misclassified accounts," personal profiles for businesses or pets that are meant to be Pages. These are relatively straightforward to deal with—they just get converted to Pages. "Violating accounts," on the other hand, are more serious. These are personal profiles that engage in scamming and spamming or otherwise violate the platform's terms of service. Violating accounts need to be removed as quickly as possible without casting too wide a net and snagging real accounts as well.

To do this, Facebook uses hand-coded rules and machine learning to block a fake account either before it is created or before it becomes active. In other words, before it can harm real users. The final stage is after a fake account has gone live. This is when detection gets a lot trickier and where the new machine-learning system, known as Deep Entity Classification (DEC), comes in. DEC learns to differentiate fake and real users by their connection patterns across the network. It calls these "deep features," and they include things like the average age or gender distribution of the user's friends. Facebook uses over 20,000 deep features to characterize each account, providing a snapshot of how each profile behaves to make it difficult for attackers to gain the system by changing tactics.

Different studies done in consonance with Facebook OSN are:

- **A Hybrid Scheme for Detecting Fake Accounts on Facebook**

The author proposed a hybrid model to detect the existence of fake accounts based on machine learning and skin detection algorithms. The experimentation process used dataset collected using the Facebook API graph and also other fields that were collected from our neighborhood because of strict privacy concerns. After a long period of observance and interaction with various account holders on Facebook, the accounts were identified as fake or legitimate manually.

Supervised machine learning algorithms like KNN algorithm, Support Vector Machine, Naïve Bayes' Algorithm, Decision tree, and Random Forest are implemented on the collected data set. The images collected from the manually identified fake accounts were fed into the skin detection algorithm and the percentage of skin present in each image was calculated. With the combined approach of the skin detection, this study evaluates that using old features of Facebook, decision tree gives 80% accuracy but other classifiers give 60-80% accuracy with 20% error but with new features, Random Forest, Naive Bayes, and decision tree give 80% accuracy but SVM gives 60% accuracy.

- **Towards Detecting Fake User Accounts in Facebook**

This work focuses on detecting fake accounts on a very popular online social network, Facebook. Key contributions include the collection of data related to real and fake accounts, use of user-feed information to understand user profile activity and identifying an extensive set of 17 features to discriminate fake users with real users, identifying the key machine learning-based classifiers using these features and identifying activities (like comment, tagging, sharing, etc) contribute the most in fake user detection on Facebook. Results exhibit a classification accuracy of 79% among the best performing classifiers [10].

- **Fake Accounts Detection In Facebook Using Machine Learning Techniques (2017)**

The author discussed machine learning techniques such as Neural Networks and SVM for detecting fake accounts on Facebook. Weka tool has been used for the simulation of the algorithm Neural network and SVM are used collectively in a hybrid fashion. K-medoid clustering is also used to improve accuracy and reduce the time complexity of the algorithm. Then the randomization technique is used for data filtration. The clustering technique detects multiple fake accounts at a time. The clustering technique not only improves the accuracy to classify the data but also reduces that time complexity. The principal component analysis is used to provide the ranking on a feature set. The Precision of proposed work with the neural network is 99.4% and SVM is 99.2%. [11]

- **Fake Identities in Social Media: A Case Study on the Sustainability of the Facebook Business Model (2012)**

This research evaluates the implications of fake user profiles on Facebook. For this, a business model is proposed having comprehensive data harvesting attack, the social engineering experiment, and analyzed the interactions between fake profiles and regular users. Furthermore, privacy considerations are analyzed using focus groups. Awareness of users is engineered via determining factors that contribute to the successful integration of a fake profile into an existing friendship network on Facebook. Moreover, the correlation between the number of registered profiles and the correctness of the user data and its impacts on the Facebook business model is also discussed [12].

Case 2: Twitter OSN (Online Social Network)

The issue of the black market is addressed in Twitter by Aggarwal et al.; who have analyzed the anatomy of purchased Twitter followers accounts based on the significant difference in their profile attributes, interaction, and content sharing patterns compared to legitimate Twitter users [10]. Twitter also provides many solutions for fake account detection. Studies done on Twitter OSN are:

- **The Detection of Fake Messages using Machine Learning (2018)**

This research is an investigation of the usage of fake messages on Twitter during the Dutch election of 2012. It presented the performance of 8 supervised Machine Learning classifiers on a Twitter dataset. The Decision Tree algorithm performs best on the used dataset, with an F-Score of 88%. A total of 613,033 tweets were collected. Undoubtedly, this dataset was a collection of true and false tweets. After testing, 328.897 were found to be true tweets while 284.136 tweets were categorized as false tweets. Through a qualitative content analysis of false tweets sent during the election, distinguishing characteristics and features of false content were identified and grouped into six separate categories [14].

- **Identifying Fake News and Fake Users on Twitter (2018)**

The proposed work in this research is service-oriented architecture. This architecture is developed by collaborating with different modules. These modules enhance the efficiency of response by interacting. The whole content is categorized into tweets and users. The application requests it and then proceeds to work on other useful tasks instead of stalling as it is waiting for an answer. If the requested function is completed, the application is told of the results through a callback or a commitment or Observable. This allows for the execution of large numbers of operations in parallel which is important for scaling applications. It returns a set of statistics about the veracity of the message, based on the text of the message and the user of the tweet [15].

- **Detecting Fake Followers in Twitter: A Machine Learning Approach (2017)**

This approach is efficient enough to detect fake followers on Twitter via Machine learning techniques. Detection is done via using characteristics that distinguish fake and genuine followers. These characteristics are set as attributes to the machine learning algorithm for user classification as fake or genuine. Different machine learning algorithms have different detection accuracy i.e. either low or high. These attributes are the number of followers, number of followees, number of favored

Tweets, number of lists a user is a member of, number of tweets the user has posted, and number of followers per followers. On behalf of these attributes, a large sample of fake and genuine followers are tested manually as well as via machine learning algorithms. There is a gain of high detection accuracy using machine learning algorithms. [16]

- **Profile characteristics of fake Twitter accounts (2016)**

This research article includes the analysis of 62 million publicly available Twitter user profiles and a strategy to identify automatically generated fake profiles. Using a combination of a pattern-matching algorithm on screen-names and an analysis of update times, a reasonable number of highly reliable fake user accounts were identified. An analysis of the temporal evolution of accounts over 2 years showed that the friends-to-followers ratio increased over time for fake profiles while they decreased for ground truth users. This study suggests that a profile-based approach can be used for identifying a core set of fake online social network users in a time-efficient manner. A highly reliable clustered fake profile set was generated by grouping user accounts based on matched multiple- profile-attributes; patterns in their screen names; and an update-time distribution filter [17].

- **Fame for sale: Efficient detection of fake Twitter followers (2015)**

The proposed Feature Renovation approach explains the efficient detection of fake Twitter followers by different dimensions. It starts with the study of most relevant existing features and rules (proposed by Academia and Media) for anomalous Twitter accounts detection. Then, a baseline dataset of verified human and fake follower accounts is created and machine learning classifiers are built using the reviewed rules and features. Classifiers are tested over baseline dataset shows better performance by rules of Academia than those of Media. Different machine learning techniques used are SVM, Random Forest Algorithm, ANNs, etc. [18]

IV Conclusion

Social media is growing incredibly fast these days, which is important for marketing campaigns for making product awareness to users and celebrities for their publicity. But fake identities like accounts as well as the profile can create negative effects regarding product advertisement as well can damage the reputation of celebrities. Many online social networks are in tune these days. Among them are Facebook, Twitter, Instagram, LinkedIn, Pinterest, are the prominent ones.

This paper puts the limelight on different works done by a number of researchers in concern with fake identities, fake accounts, fake profiles, various detection techniques as well as classification methods like SVM, Naïve Bayes algorithm, etc to detect fake identities. This paper also includes a literature survey of two major online social network platforms i.e Facebook and Twitter to cover the advanced aspects which explain the difficulties in the handling of billions of users as well as detection/security tactics used by these OSNs.

Future work involves proposing a mechanism to detect these fake profiles successfully and efficiently.

References

[1] C. Xiao, D. M. Freeman, and T. Hwa, "Detecting clusters of fake accounts in online social networks," *AISec 2015 - Proc. 8th ACM Work. Artif. Intell. Secur. co-located with CCS 2015*, pp. 91–102, 2015.

[2] E. Van Der Walt and J. Eloff, "Using Machine Learning to Detect Fake Identities: Bots vs Humans," *IEEE* ,

2169-3536, vol. 6, pp. 6540–6549, 2018.

[3] V. Tiwari, "Analysis and detection of fake profile over social network," *Proceeding - IEEE Int. Conf. Comput. Commun. Autom. ICCCA 2017, IEEE 978-1-5090-6471*, vol. 7, pp. 175–179, 2017.

[4] "Detecting-suspicious-accounts-in-online-social-networks-48eabf4c75b6 @ towardsdatascience.com." .

[5] P. Srinivas Rao and J. Gyani, "Fake Profiles Identification in Online Social Networks Using Machine Learning and NLP," *Int. J. Appl. Eng. Res. ISSN 0973-4562*, vol. 13, no. 6, pp. 4133–4136, 2018.

[6] A. Romanov, A. Semenov, O. Mazhelis, and J. Veijalainen, "Detection of fake profiles in social media: Literature review," *WEBIST 2017 - Proc. 13th Int. Conf. Web Inf. Syst. Technol.*, no. Webist, pp. 363–369, 2017.

[7] R. Raturi, "Machine Learning Implementation for Identifying Fake Accounts in Social Network," vol. 118, no. 20, pp. 4785–4797, 2018.

[8] S. M. Kulkarni and V. Dhamdhere, "Automatic Detection of Fake Profiles in Online Social Networks," *OAIJSE, ISO- 32972007*, vol. 3, no. special issue 1, pp. 70–73, 2018.

[9] M. Mohammadrezaei, M. E. Shiri, and A. M. Rahmani, "Identifying Fake Accounts on Social Networks Based on Graph Analysis and Classification Algorithms," *Secur. Commun. Networks*, vol. 2018, 2018.

[10] A. Gupta and R. Kaushal, "Towards detecting fake user accounts in facebook," *ISEA Asia Secur. Priv. Conf. 2017, ISEASP 2017*, no. February, 2017.

[11] P. Virdi, "Fake Accounts Detection in Facebook Using Machine Learning Techniques," 2017.

[12] K. Krombholz, D. Merkl, and E. Weippl, "Fake identities in social media: A case study on the sustainability of the Facebook business model," *J. Serv. Sci. Res.*, vol. 4, no. 2, pp. 175–212, 2012.

[13] M. M. Swe and N. Nyein Myo, "Fake Accounts Detection on Twitter Using Blacklist," *Proc. - 17th IEEE/ACIS Int. Conf. Comput. Inf. Sci. ICIS 2018, 978-1-5386-5892-5/18 IEEE, https//www.researchgate.net/publication/327820843*, no. June, pp. 562–566, 2018.

[14] M. S. Looijenga, "The Detection of Fake Messages using Machine Learning," 2018.

[15] C. S. Atodiresei, A. Tănăselea, and A. Iftene, "Identifying Fake News and Fake Users on Twitter," *Procedia Comput. Sci. Sci. 126 451–461, 222.elsevier.com/locate/procedia*, vol. 126, pp. 451–461, 2018.

[16] A. Khalil, H. Hajjdiab, and N. Al-Qirim, "Detecting fake followers in twitter: A machine learning approach," *Int. J. Mach. Learn. Comput.*, vol. 7, no. 6, pp. 198–202, 2017.

[17] S. Gurajala, J. S. White, B. Hudson, B. R. Voter, and J. N. Matthews, "Profile characteristics of fake Twitter accounts," *Big Data Soc.*, vol. 3, no. 2, 2016.

[18] S. Cresci, R. Di Pietro, M. Petrocchi, A. Spognardi, and M. Tesconi, "Fame for sale: Efficient detection of fake Twitter followers," *Decis. Support Syst. , www.elsevier.com/locate/dss. 0167-9236*, vol. 80, no. August, pp. 56–71, 2015.