LITERATURE SURVEY

1.Detection of Fake Twitter accounts with Machine Learning Algorithm

This research investigates how fake messages are used on Twitter during the Dutch election of 2012. It researches the performance of 8 supervised Machine Learning classifiers on a Twitter dataset. We provide that the Decision Tree algorithm perform best on the used dataset, with an F-Score of 88%. In total, 613.033 tweets were classified, of which 328.897 were classified as true, and 284.136 tweets were classified as false. Through a qualitative content analysis of false tweets sent during the election, distinctive features and characteristics of false content have been found and grouped into six different categories.

2. Detection of fake profile in online social networks using Machine Learning

In today's world, the social media platforms are being used on daily basis and has become an important part of our lives. The number of peoples on social media platforms are incrementing at a greater level for malicious use. There are numerous cases where produced accounts have been effectively distinguished utilizing machine adapting techniques however the amount of research work is very low to recognize counterfeit characters made by people. For bots the ML models used various features to calculate the no. of followers to the no. of friends that an account has on social media platforms (SOCIAL MEDIA PLATFORMSs). The no. of friends to the no. of followers of any account are easily available in the account profiles and no rights are violated of any accounts. In order to accomplish the task of detecting, identifying and eliminate the fake accounts we establish a forged human account.

3. Detecting Fake accounts on Social Media

In the present generation, on-Line social networks (OSNs) have become increasingly popular, people's social lives have become more associated with these sites. They use on-Line social networks (OSNs) to keep in touch with each others, share news, organize events, and even run their own e-business. The rapid growth of OSNs and the massive amount of personal data of its subscribers have attracted attackers, and imposters to steal personal data, share false news, and spread malicious activities. On the other hand, researchers have started to investigate efficient techniques to detect abnormal activities and fake accounts relying on accounts features, and classification algorithms. However, some of the account's exploited features have negative contribution in the final results or have no impact, also using standalone classification algorithms does not always achieve satisfactory results. In this paper, a new algorithm, SVM-NN, is proposed to provide efficient detection for fake Twitter accounts and bots, feature selection and dimension reduction techniques were applied. Machine learning classification algorithms were used to decide the target accounts identity real or fake, those algorithms were support vector machine (SVM), neural Network (NN), and our newly developed algorithm, SVM-NN. The proposed algorithm (SVM-NN) uses less number of features, while still being able to correctly classify about 98% of the accounts of our training dataset.

4. Twitter fake account detection

Nowadays, Twitter has become one of the fastest-growing Online Social Networks (OSNs) for data sharing frameworks and microblogging. It attracts millions of users worldwide where subscribers communicate with each through posts and messages known as "tweets". The open structure and behaviour of Twitter cause it to be vulnerable to attacks from fake accounts and a large number of automated software, known as 'bots'. Bots are regarded to be malicious as they send spam to users of social networks over the internet. Data security and privacy are among the most critical issues of social network users, as the protection and fulfilment of these requirements strengthen the network's interest and, ultimately, its credibility. To overcome these issues, we need to build an efficient model to detect and classify fake twitter accounts. This paper presents a new approach with dual functions, namely to identify and classify the twitter bots based on ontological engineering and Semantic Web Rule Language (SWRL) rules. Web Ontology Language (OWL), Semantic Web Rule Language (SWRL) rules, and reasoners are deployed to inductively learn the rules that distinguish a fake account (bot) from a real one, as well as to classify fake accounts into fake followers or spam bot. Our approach could properly identify the false account with an accuracy of (97%) in the first stage, after which these fake accounts were classified into spam or fake follower bots with an accuracy rate of (94.9%). Furthermore, it has been found that he ontology classifier is a more interpretable model that offers straightforward and human-interpretable decision rules, as compared to other machine learning classifiers.