**“Proguard: Detecting Malicious Accounts in Social-Media Based Online Promotion”**

**A Major Project**

**Submitted in partial fulfillment of the requirement for the award of Degree of Bachelor of Technology in Computer Science & Engg.**

**Submitted To**



**RAJIV GANDHI PROUDYOGIKI VISHWAVIDYALAYA, BHOPAL (M.P.)**

**Submitted By:**

**Student name : Harsh Khare**

**Enrollment No- 0821CS191034**

**Under The Supervision Of:**

**Mr. Pratyush Sharma (HOD, CSE Dept.)**

****

**DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING.**

**MALWA INSTITUTE OF TECHNOLOGY, INDORE**

**MALWA INSTITUTE OF TECHNOLOGY, INDORE**

**Department Of Computer Science & Engg.**

### CERTIFICATE

This is to certify that the work embodies in this major project entitled **“Proguard: Detecting Malicious Accounts in Social-Media Based Online Propmotion**” being submitted by “**Harsh Khare**” **Roll No.:0821CS191034** for partial fulfillment of the requirement for the award of “**Bachelor of Technology in Computer Science & Engineering**.” to “Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal(M.P.)” during the academic year 2022-23 is a record of bonafide piece of work, carried out by him under our/my supervision and guidance in the “Department of Computer Science & Engineering ”, Malwa Institute of Technology, Indore (M.P.).

**Mr. Pratyush Sharma Dr. M.S. Murthy**

HOD, CSE Dept. (Director)

**MALWA INSTITUTE OF TECHNOLOGY INDORE**

**Department Of Computer Science & Engg.**

### CERTIFICATE OF APPROVAL

A major project entitled **“Proguard: Detecting Malicious Accounts in Social Media Based Online Promotion”** being submitted by “**Harsh Khare” (Roll No.:0821CS191034)** has been examined by us and is hereby approved for the award of degree **“Bachelor of Technology in Computer Science & Engineering”** for which it has been submitted. It is understood that by this approval the undersigned do not necessarily endorse or approve any statement made, opinion expressed or conclusion drawn therein, but approve the dissertation only for the purpose for which it has been submitted.

**(Internal Examiner) (External Examiner)**

**Date: Date:**

**MALWA INSTITUTE OF TECHNOLOGY, INDORE**

**Department Of Computer Science and Engineering**

### DECLARATION

### I Harsh Khare a student of Bachelor of Technology in CSE, at Malwa Institute of Technology, Indore (M.P.), hereby declare that the work presented in this dissertation entitled “Proguard: Detecting Malicious Accounts in Social-Media Based Online Promotion” is the outcome of our own work, is bonafide and correct to the best of our knowledge and this work has been carried out taking care of Engineering Ethics. The work presented does not infringe any patented work and has not been submitted to any other university or anywhere else for the award of any degree or any professional diploma.

**Date: Student name : Harsh Khare**

#### Enrollment No.: 082CS191034

**Student name : Khushi Malviya**

#### Enrollment No.: 0821CS191047

**Student name : Sourabh Pal**

**Enrollment No.: 0821CS191088**

# **Acknowledgement**

Foremost, I would like to express my sincere gratitude to my guide **Mr. Pratyush Sharma** for the continuous support of my study and research, for their patience, motivation, enthusiasm, and immense knowledge. Their guidance helped me in all the time of research and writing of this thesis. I am ever grateful to **Dr. M.S. Murthy,** Director, Malwa Institute of Technology, Indore for providing opportunity to explore this wonderful venture. And also I would like to give regards and remembers another source of inspiration **Mr. Pratyush Sharma** (HOD CSE Dept.) This project would not have been possible without collaboration with my colleagues, and the support of my friends and family.

**Student name : Harsh Khare**

#### Enrollment No.: 082CS191034

**Student name : Khushi Malviya**

#### Enrollment No.: 0821CS191047

**Student name : Sourabh Pal**

**Enrollment No.: 0821CS191088**

TABLE OF CONTENTS

[**ABSTRACT**](#_Toc131953028)

[**Chapter 1. Introduction** 1](#_Toc131953029)

[**Chapter 2. Literature Survey** 5](#_Toc131953030)

[**Chapter 3. Problem Description** 10](#_Toc131953031)

[**Chapter 4. Innovation** 12](#_Toc131953032)

[**4.1 Hybrid Machine Learning**  18](#_Toc131953036)

[**Chapter 5. Objective** 14](#_Toc131953033)

[**5.1 Role of Machine Learningin Detection of Fake Profiles**  14](#_Toc131953036)

[**Chapter 6. Solution Domain** 16](#_Toc131953034)

[**6.1 Problem** 18](#_Toc131953036)

[**6.2 Solution** 16](#_Toc131953036)

[**Chapter 7. Proposed Methodology and Algorithm** 18](#_Toc131953035)

[**7.1 Overview** 18](#_Toc131953036)

[**7.2 Classification** 19](#_Toc131953037)

[**7.3 Neural Networks** 19](#_Toc131953038)

[7.3.1 Back Propagation 20](#_Toc131953039)

[7.3.2 Neural Networks Libraries 21](#_Toc131953040)

[**7.4 Support Vector Machine** 21](#_Toc131953041)

[7.4.1 Selecting SVM Hyperplanes 21](#_Toc131953042)

[7.4.2 Linearly Seprable 22](#_Toc131953043)

[7.4.3 SVM Libraries 22](#_Toc131953043)

[**7.5 Random Forest** 23](#_Toc131953044)

[**7.6 Decision Tree** 23](#_Toc131953045)

[**7.7 Algorithm for System** 24](#_Toc131953046)

[**Chapter 8. Tools and Technology Used** 26](#_Toc131953035)

[**8.1 Python programming language** 29](#_Toc131953048)

[**8.1 Tools** 29](#_Toc131953048)

**[Chapter 9. Implementation Details](#_Toc131953047)** [29](#_Toc131953047)

[**9.1 Data Collection** 29](#_Toc131953048)

[**9.2 Evaluation Parameters** 31](#_Toc131953049)

[**9.3 Training of Classifiers** 31](#_Toc131953049)

[**9.4 Training of Neural Network** 33](#_Toc131953050)

[9.4.1 Comparison of variour Machine Learning Algorithm 31](#_Toc131953042)

[9.4.2 Comparison of Hybrid Model 31](#_Toc131953042)

[**Chapter 10. Result Analysis** 35](#_Toc131953051)

[**10.1 Performance Comparision of Machine Learning Algorithm** 31](#_Toc131953049)

[**10.2 Performance of Hybrid Model Based on Accuracy** 35](#_Toc131953049)

[**10.3 Confusion Matrix**  36](#_Toc131953049)

[10.3.1 Confusion Matrix of SVM+LR+RF 36](#_Toc131953042)

[10.3.2 Confusion Matrix of SVM+LR+NN 36](#_Toc131953042)

[10.3.3 Confusion Matrix of SVM+RF+NN 37](#_Toc131953042)

[10.3.4 Confusion Matrix of LR-RF-NN 37](#_Toc131953042)

[**10.4 ROC Curve**  31](#_Toc131953049)

[10.4.1 SVM+RF+NN 37](#_Toc131953042)

[10.4.2 SVM+LR+NN 38](#_Toc131953042)

[10.4.3 LR-RF-NN 38](#_Toc131953042)

[**Chapter 11. Conclusion** 40](#_Toc131953051)

[**Chapter 12. Future Work** 41](#_Toc131953052)

[**Chapter 13. References** 42](#_Toc131953053)

# **ABSTRACT**

Online Social Networks involve a huge amount of people from all over the world and it has become a big part of their life. People use social networks to share their feelings, to make new friends, to set up new businesses, to connect with friends and family and what not. The Online Social Networks provides a great advantage to individuals in different ways but it also suffers with some disadvantages. There are many people who use these networks to cause harm to others by making fake accounts on these networks. For detection of such fake and genuine accounts we can use machine learning algorithms. The machine learning algorithms are applied for the prediction and classification of datasets through the different models that are prepared. It sometimes become difficult to differentiate between the results of different models and so we to use a hybrid approach of machine learning algorithm can make this task easy. In our work we compared the 8 different combinations of classification algorithms and calculated their accuracy on the dataset of an Online Social Network. We used the combination of Random Forest, Support Vector Machine, Logistic Regression, KNN, and Decision Trees. After comparing the result of each hybrid approach, we concluded that the best accuracy was obtained by combination of SVM and Logistic Regression and Neural Network. So, we proposed a model for the detection of fake account with the hybrid approach giving the best accuracy among all the combinations.

**List of Figures:**

|  |  |  |
| --- | --- | --- |
| Fig. No. | Fig Name | Page No |
| 7.3.1 | Neural Networks | 20 |
| 7.4.1.1 | Support Vector Machine | 22 |
| 7.5.1 | Random Forest | 23 |
| 7.6.1 | Decision Tree | 24 |
| 9 | Hybrid Model | 29 |
| 10.1 | Performance of Machine Learning Algorithm | 35 |
| 10.2 | Comparision of Hybrid Model | 35 |
| 10.3 .1 | Confusion Matrix of SVM+LR+RF | 36 |
| 10.3.2 | Confusion Matrix of SVM+LR+NN | 36 |
| 10.3.3 | Confusion Matrix of SVM+RF+NN | 37 |
| 10.3.4 | Confusion Matrix of LR+RF+NN | 37 |
| 10.4.1 | ROC of SVM+RF+NN | 38 |
| 10.4.2 | ROC of SVM+LR+NN | 38 |
| 10.4.3 | ROC of LR+RF+NN | 39 |

**List of Tables:**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | |  |  |  | | --- | --- | --- | | Table. No. | Table Name | Page No | | 2.1 | Work of Contemporary authors | 7-9 | | 9.4.1 | Comparison of Various Machine Learning Algorithm | 33 | | 9.4.2 | Table 2: Comparison of Hybrid Model | 34 | |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**ABBREVIATIONS**

|  |  |
| --- | --- |
| SVM | Support Vector Machine |
| NN | Neural Network |
| ANN | Artificial Neural Network |
| LG | Logistic Regression |
| RF | Random Forest |
| TPR | True Positive Rate |
| TNR | True Negative Rate |
| FPR | False Positive Rate |
| FNR | False Negative Rate |
| DT | Decision Tree |
| ML | Machine Learning |

# **Chapter 1. Introduction**

Machine Learning is a branch of artificial intelligence (AI) which is able to provide a system the ability to act without being programmed explicitly. It is used in many fields like Google cars, recommendation engines, friend suggestions in social media networks, shopping apps, cybercrimes etc.

Machine Learning has made a phenomenal change in the way how data was extracted and interpreted by replacing the old statistical techniques. Classifications of machine learning techniques are: Reinforcement, Supervised and Unsupervised Machine Learning.

**1.1 Fake Account**

A fake account is the description of a personality, institution or corporation that does not truly exist, on social media. In other cases, they use the real information of these entities and create a fake profile that looks real and credible for a normal user. Hackers, as often as possible use real names, personalities that look genuine. The profile pictures they use, are normally adjusted variants of pictures taken from real individuals or associations. Most fake accounts are newly opened and have few friends or connection on their profile, and the majority of their friends do not have anything in common. These accounts are used to abuse sign-up bonuses, to generate fake news and spam content and eventually spread malware. Sometimes these fake users try to influence the results of reviews or try to manipulate public opinion in voting processes.

**1.2 Who creates Fake accounts and why?**

The first time when fake accounts appeared on social media was when individuals wanted intimacy, wanted to remain anonymous on the internet, therefore avoiding to use their real name, real account pictures and even avoid posting anything at all on social media. They only wanted to have an account to see what was happening on social media. Then, some individuals seized the opportunity of using different user accounts to gain bonus offers. For example, in the gaming industry, many users decide to open a new account to receive sign-up bonuses, referral bonuses. In other cases, fake accounts are used to influence the result of surveys. Finally, some hackers want to collect sensitive and private information in order to blackmail people or companies and they demand large sums of money in order not to publish the stolen information.

Our work is concerned with the Classification algorithms that come under the Supervised Machine Learning. Classification is a supervised learning approach in which the machine takes the input data learns from that data and then further classifies the testing data according to its training data.

The total number of users in online social networking sites is continuously increasing and with that the number of fake accounts is also increasing. As in September 2019, monthly active users on Facebook are 2.45 billion worldwide. According to Alexa, after Google and YouTube the third most visited website is Facebook. In a survey it is found that there are a greater number of female accounts in the world than the total population of female. From this, we can infer how many fake profiles have been created. According to Statistics April 2018 stats report, Facebook has more than 336 million active Twitter accounts, but Facebook is the leader with 2,196 million users worldwide. In September 2019, monthly active users on Facebook are 2.45 billion, of which India has the most. 270 million users. People who log on to Facebook daily are approximately 1.62 billion. And among these 83 million accounts are fake on Facebook. This statistics was given by Facebook in their Wall Street reports (SOURCE: Zephoria Digital Marketing) shows the monthly active users in the year 2019 on various OSNs.

Online social networks(OSNs), such as Facebook, Twitter, RenRen, LinkedIn, Google+, and Tuenti, have become increasingly popular over last few years. People use OSNs to keep in touch with each others, share news, organize events, and even run their own e-business. For the period between 2014 and 2018 around 2.53 million U.S. dollars have been spent on sponsoring political ads on Facebook by non-profits. The open nature of OSNs and the massive amount of personal data for its subscribers have made them vulnerable to Sybil attacks.

In 2012, Facebook noticed an abuse on their platform including publishing false news, hate speech, sensational and polarizing, and some others. However, online Social Networks (OSNs) have also attracted the interest of researchers for mining and analyzing their massive amount of data, exploring and studying users behaviours as well as detecting their abnormal activities.

In researchers have made a study to predict, analyze and explain customers loyalty towards a social media-based online brand community, by identifying the most effective cognitive features that predict their customers attitude. Facebook community continues to grow with more than 2.2 billion monthly active users and 1.4 billion Daily active users, with an increase of 11% on a year-over-year basis.

In the second quarter of 2018 alone, Facebook reported that its total revenue was $13.2 billion with $13.0 billion from ads only. Similarly, in second quarter of 2018 Twitter has reported reaching about one billion of Twitter subscribers, with 335 million monthly active users.

In 2017 twitter reported a steady revenue growth of 2.44 billion U.S. dollars, with 108 million U.S. dollars lower profit compared to the previous year. In 2015 Facebook estimated that nearly 14 million of its monthly active users are in fact undesirable, representing malicious fake accounts that have been created in violation of the websites terms of service .

Facebook, for the first time, shared a report in the first quarter of 2018 that shows their internal guidelines used to enforce community standards covering their efforts between October 2017 to March 2018, this report illustrates the amount of undesirable content that has been removed by Facebook, and it covers six categories: graphic violence, adult nudity and sexual activity, terrorist propaganda, hate speech, spam, and fake accounts 837 million posts containing spam have been taken down, and about 583 million fake accounts have been disabled, Facebook also has removed around 81 million undesirable content in terms of the rest violating content types.

However, even after preventing millions of fake accounts from Facebook, it was estimated that, around 88 million accounts, are still fake. For such OSNs, the existence of fake accounts lead advertisers, developers, and inventors to distrust their reported user metrics, which would negatively impacts their revenues as recently, banks and financial institutions in U.S. have started to analyze Twitter and Facebook accounts of loan applicants, before actually granting the loan.

Attackers follow the concept of having OSNs user accounts are “keys to walled gardens”, so they deceive themselves off as somebody else, by using photos and profiles that are either snatched from a real person without his/her knowledge, or are generated artificially, to spread fake news, and steal personal information. These fake accounts are generally called imposters. In both cases, such fake accounts have a harmful effect on users, and their motives would be any thing other than good intentions as they usually flood spam messages, or steal private data. They are keen to phish individual naive users to phony relationships that lead to sex scam, human trafficking, and even political astroturfing.

Detecting those threatening accounts in OSNs has become a must to avoid various malicious activities, insure security of user’s accounts and protect personal information. Researchers attempt to come up with automated detection tools for identifying fake accounts, which would be laborintensive and costly if done manually. The implications of researchers attempt may allow an OSN operator detecting fake accounts efficiently and effectively, it would improve the experience of its users by preventing annoying spam messages and other abusive content. The OSN operator can also increase the credibility of its user metrics and enable third parties to consider its user accounts.

# **Chapter 2. Literature Survey**

M. N. Aydogan apply several feature extraction methods to extract features from user profile data such as the number of followers, the number of friends, and the frequency of tweets. They also extract features from the textual content of tweets, such as the number of URLs, hashtags, and mentions. Then, they use four different classification algorithms (Support Vector Machines, Decision Trees, Random Forest, and Naive Bayes) to classify the user accounts as fake or genuine.

E. Diri (2016) use a distance measure algorithm to identify potential clone accounts. They calculate the Euclidean distance between the feature vectors of each pair of accounts and compare the distances to a threshold value. If the distance is smaller than the threshold value, the accounts are considered potential clones.

Sachi Mohanty, Ankit Kumar Singh, and Ankita Shukla discuss various machine learning algorithms used in recommender systems, such as linear regression, decision trees, and neural networks. They also cover advanced techniques such as matrix factorization, deep learning, and reinforcement learning. The book includes several case studies and practical examples of recommender systems, demonstrating their applications in different domains. It also covers topics such as evaluation metrics for recommender systems, ethical considerations, and challenges in implementing recommender systems. Overall, "Recommender System with Machine Learning and Artificial Intelligence" is a comprehensive guide to the field of recommender systems, providing insights into the latest techniques and practical examples for their implementation. It can be useful for researchers, practitioners, and students interested in the field of recommendation systems and machine learning.

Shalinda Adikari and Kaushik Dutta propose a method that extract several features from the profiles such as the number of connections, the number of endorsements, the number of posts, and the completeness of the profile. They also extract features from the textual content of the profiles, such as the use of keywords and the quality of the language. Then, they use several classification algorithms, including Logistic Regression, Decision Tree, and Random Forest, to classify the profiles as genuine or fake. The authors also evaluate the performance of the proposed approach using different metrics, such as precision, recall, and F1-score. The authors experiment with a dataset of 15,000 LinkedIn profiles, including 7,500 fake profiles and 7,500 genuine profiles. The results show that the proposed approach achieves high accuracy in identifying fake profiles on LinkedIn, with an F1-score of 0.96. Overall, this study provides a valuable contribution to the field of fake profile detection on social media platforms, specifically LinkedIn, using machine learning algorithms. The proposed approach can be useful for LinkedIn to improve the authenticity of user profiles and for researchers to investigate the problem of fake profiles on social media.

Muhammad Al-Qurishi extract various features from user accounts, including the number of friends, the number of followers, the number of groups joined, and the frequency of posting. They then use a deep-regression model based on a deep neural network to predict the probability of a new account being a Sybil attacker. The authors evaluate their proposed approach using a dataset of 4,000 social network accounts, including 1,000 Sybil attackers and 3,000 genuine accounts. The results show that the proposed approach achieves high accuracy in predicting Sybil attacks, with an AUC (Area Under the Curve) score of 0.96. Overall, this study presents a novel approach to predicting Sybil attacks in social networks using deep learning techniques. The proposed approach can be useful for social network providers to improve the security of their platforms and for researchers to investigate the problem of Sybil attacks in social networks.

Machine Learning Implementation for Identifying Fake Accounts in Social Network" proposes a machine learning-based approach to detect fake accounts in social networks. use a dataset consisting of 1,000 user accounts from Facebook, including 500 fake accounts and 500 genuine accounts. They extract various features from the accounts, such as the number of friends, the frequency of posting, and the completeness of the profile. Then, they use several machine learning algorithms, including Logistic Regression, Naive Bayes, and Decision Tree, to classify the accounts as genuine or fake. The authors evaluate the performance of the proposed approach using various metrics, including accuracy, precision, recall, and F1-score. The results show that the proposed approach achieves high accuracy in detecting fake accounts, with an F1-score of 0.93.

N. M. Al-Qahtani and R. M. Al-Otaibi (2020) begin by discussing the prevalence and impact of fake accounts on social media platforms. They then provide an overview of the different types of fake accounts, including bot accounts, cyborg accounts, and human-driven accounts.The article then delves into the various techniques used to detect fake accounts. These include machine learning techniques such as supervised learning, unsupervised learning, and deep learning. The authors also discuss network analysis techniques such as social network analysis and graph theory. Additionally, they cover user behavior analysis techniques, including anomaly detection and clustering.The article provides a detailed analysis of the strengths and weaknesses of each of these techniques, including their accuracy, efficiency, and scalability. The authors also discuss the limitations and challenges of detecting fake accounts, such as the dynamic nature of social media, the lack of ground truth data, and the diversity of fake account types.

The authors begin by discussing the prevalence and impact of fake accounts on social media platforms. They then provide an overview of the different types of fake accounts, such as bot accounts, cyborg accounts, and human-driven accounts. The article then delves into the different approaches to detect fake accounts, including machine learning techniques such as supervised learning, unsupervised learning, and deep learning. The authors also cover network analysis techniques, such as social network analysis, and user behavior analysis techniques, such as anomaly detection and clustering. The authors also discuss the limitations and challenges associated with detecting fake accounts, such as the lack of labeled data and the dynamic nature of social media platforms. They also provide a comparison of the different techniques used for fake account detection, highlighting the advantages and disadvantages of each approach.

**Table 2.1 Work of Contemporary authors.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **S.No** | **Title** | **Year of Publication** | **Methods** | **Key Points** |
| 1 | Comparison of Naive Bayes, SVM, RF approaches for fake account detection. | 2019 | RF, SVM, Naïve Byes | RF approach has been very effective in detection of tweets. |
| 2 | The study by E. Diri (2016) proposes a distance measure algorithm for identifying potential clone accounts on social media platforms.. | 2016 | Distance Measure Algorithm. | A novel approach to clone detection on social media platforms, and the proposed distance measure algorithm |
| 3 | Sachi Mohanty, Ankit Kumar Singh, and Ankita Shukla is a comprehensive guide to the field of recommender systems, covering various machine learning algorithms used in recommendation systems | 2018 | Matrix factorization, Deep learning, and Reinforcement learning | It is a useful resource for researchers, practitioners, and students interested in the field of recommendation systems and machine learning. |
| 4 | Shalinda Adikari and Kaushik Dutta proposes a method for detecting fake profiles on LinkedIn using machine learning algorithms. | 2017 | Logistic Regression, Decision Tree, and Random Forest, | The proposed approach can be useful for LinkedIn to improve the authenticity of user profiles and for researchers to investigate the problem of fake profiles on social media. |
| 5 | Muhammad Al - Qureshi developed a method to predict Sybil attacks in social networks using a deep neural network. | 2019 | They extract various features from user accounts and use them to predict the probability of a new account being a Sybil attack | The proposed approach achieved high accuracy in identifying Sybil attacks, with an AUC score of 0.96. |
| 6 | Machine Learning Implementation for Identifying Fake Accounts in Social Network" presents a machine learning-based method to detect fake accounts on social networks, particularly on Facebook | 2020 | Features extracted like number of friends, frequency of posting, and profile completeness, | The proposed approach in improving the authenticity of user accounts on social networks |
| 7 | Techniques for Detecting Fake Accounts in Social Media: A Review" by N. M. Al-Qahtani and R. M. Al-Otaibi discusses the prevalence and impact of fake accounts on social media platforms | 2020 | User behavior analysis techniques, Network Analysis techniques: | Analysis of the strengths and weaknesses of each of these techniques and highlight the challenges and limitations of detecting fake accounts on social media platforms |

# **Chapter 3. Problem Description**

Modeling a Fake Account Detection System is an old problem but due to the many challenges this problem presents there still exist a lot of gaps that have been identified and need to be worked upon. The many challenges this system presents have been listed below:

• The data is not readily available: accounts on online social networks are highly private and protected, so the networking sites do not reveal any account information to maintain the confidential nature and keep the trust of their users.

• There is a lot of overlapping between genuine and fake accounts: At times the feature set of legitimate and fake Figure 1: Monthly active users in different OSNs in year 2019 accounts overlap, and this poses a considerable setback when it comes to training the neural network by making it learn the pattern to differentiate between them.

• The number of parameters to process: The enormous number of parameters between learning and decision making is a major obstacle in developing systems for detecting fake accounts.

• Selection of optimal features (variables) is a big challenge: When it comes to optimal feature selection, it needs to be really dealt with care as the performance of whole system depends on which features it’s taking into consideration for classification of fake and genuine accounts. And at times it’s really perplexing to decide on these optimal features.

• Ability to handle noise in the data: Noise means missing or incorrect data which poses challenges while processing the dataset. There is no means by which we can make up for this lost information as such systems aren’t partition tolerant, so this adversely affects the outcome.

• Heterogeneity in features.

• Single user multiple accounts.

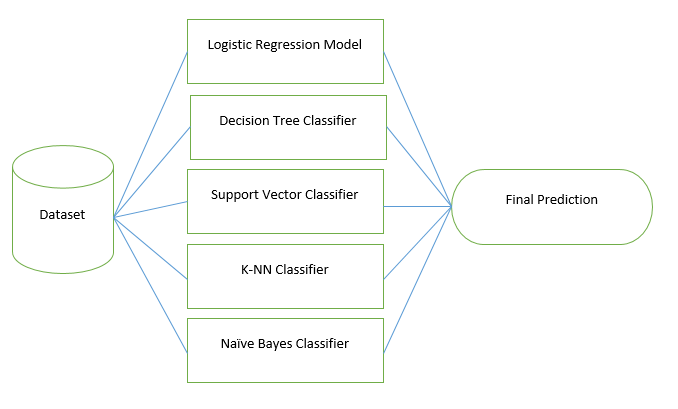
• Many of the times it resembles a legitimate transaction: At times the fake account activities are stacked up in close resemblance with the legitimate ones. Hence, it becomes difficult to comprehend them and abort them before they make it to completion.

# **Chapter 4. Innovation**

Classification algorithms (Support Vector Machine, Logistic Regression, Decision Tree, Random Forest, Artificial Neural Network) can be used separately and individually but in our system we are developing a hybrid model combining two or three machine learning models has helped in increasing the accuracy of the model and its predicative power. The fact that which hybrid model will perform better is unknown, but it is also affected by the dataset provided and also the feature selection. The concept to develop a hybrid model is in a two- stage manner, first using clustering or classification techniques for pre-processing of data and in second stage the output of the first stage to build second stage predictive classifier. It can be made using different algorithms of supervised or unsupervised learning but in our work, we developed the model using classification algorithms of supervised learning. Our main contribution is to propose a hybrid approach of machine learning algorithms and to compare the hybrid of different classification algorithms. Eight different experiments were conducted, and the accuracy thus obtained was compared.

**4.1 Hybrid Machine Learning**

Multiple simple algorithms work together to complement and augment each other. Together they can solve problems that alone they were not designed to solve.Within HML there are various types of techniques that interact with the data in different ways. Here providing the algorithm with a small set of labelled data. Then, you give it a much larger set of unlabeled data and put it to work. This type of algorithm is helpful when you need (or have) to start with a smaller batch of data upfront. It learns from all the data, not just the labelled data, and helps you organize it.



**Figure 4.1: Hybrid Machine Learning**

# **Chapter 5. Objective**

In today’s online social networks there have been a lot of problems like fake profiles, online impersonation, etc. To date, no one has come up with a feasible solution to these problems. In this project, the concept to develop a hybrid model is in a two- stage manner, first using clustering or classification techniques for pre-processing of data and in second stage the output of the first stage to build second stage predictive classifier. It can be made using different algorithms of supervised or unsupervised learning but in our work, we developed the model using classification algorithms of supervised learning. Our main objective is to propose a hybrid approach of machine learning algorithms and to compare the hybrid of different classification algorithms.

**5.1 Role of Machine Learning in Detection of Fake profiles**

In semi-supervised learning, you provide the algorithm with a small set of labelled data. Then, you give it a much larger set of unlabeled data and put it to work. This type of algorithm is helpful when you need (or have) to start with a smaller batch of data upfront. It leaSince last twenty years, there is an enormous improvements are observed in OCIAL networking phenomenon. So number of social networks is introduced different online services which are attracts huge amount of users. The increasing capacity of users is depending on information credibility on Online Social Networks (OSNs) [7].

Online social networks are being a part of every one social life in present generation. Technology usage is widely increased in nowadays. Online social networks are playing an important role in modern society. Social networks are dealing millions of users in present days all over the world. Facebook and twitter are two social networks in which the user interactions are more and daily life can be highly impacted with these social networks[16].

Large amount of fake account creation is the major problem of OSN networks. These fake accounts are does not match with real profiles of humans. Spam, web rating and fake news are representing some fakes [8]. The detection of different resources is currently expended by OSN operators and then fake accounts are closed. Almost 46% of users are operating the twitter account on the mobile phones only [9]. SMS text messages sending and e-mails sending are publishes the tweets. Messages capacity of twitter is 140 characters of message which is used for exchanging and publishes on twitter directly from smart phones using a wide array of Web-based services [10].

Number of users is maintained by the twitter. Better social lives are maintained with these social sites but also there are some disadvantages or issues are existed with these social networks. Online harassment, privacy, trolling, potential for misuse, fake account creation and etc are some of the social networks issues [11]. We will implement machine learning algorithms to predict if an account isrns from all the data, not just the labelled data, and helps you organize it.  controlled by fake user.

Unsupervised Learning and supervised learning are two types of machine learning methods. Input data is estimated or mapped with desired output by using the training data labeled set in supervised learning. But there is not providing labeled examples in unsupervised learning and during the learning process there is no idea about output. Input data of supervised learning is called as training data and at a time it has result or known label as spam/not-spam.

A training process prepares the model and make the predictions when it required and make them correct if the predictions are wrong. Once the training data can achieves desired accuracy levels then the training process stops. With the algorithm of trained machine learning fake profiles can be detected and it is the main aim of machine learning method [13].

The training data is having the particulars of person as gender, age and friends list. So the fake profiles are detected or predicted with these particulars and data security is enhanced on social networking sites. Random Forest (RF), Logistic Regression (LG), Neural Network (NN) , Decision Tree (DT) and Support Vector Machine (SVM) are used in proposed machine learning algorithms. From prediction result account activities analysis is also provided.

# **Chapter 6. Solution Domain**

**6.1 Problem**

The total number of users in online social networking sites is continuously increasing and with that the number of fake accounts is also increasing. As in September 2019, monthly active users on Facebook are 2.45 billion worldwide. According to Alexa, after Google and YouTube the third most visited website is Facebook. In a survey it is found that there are a greater number of female accounts in the world than the total population of female. From this, we can infer how many fake profiles have been created. According to Statistics April 2018 stats report, Facebook has more than 336 million active Twitter accounts, but Facebook is the leader with 2,196 million users worldwide. In September 2019, monthly active users on Facebook are 2.45 billion, of which India has the most. 270 million users. People who log on to Facebook daily are approximately 1.62 billion. And among these 83 million accounts are fake on Facebook. This statistic was given by Facebook in their Wall Street reports (SOURCE: Zephoria Digital Marketing) shows the monthly active users in the year 2019 on various OSNs.

**6.2 Solution**

We are creating a hybrid model which is combination of two or more algorithm such as svm , logistic regression , random forest etc. if we use this model then our model will be more accurate and fix all loopholes and bugs.

* Multiple simple algorithms work together to complement and augment each other. Together they can solve problems that alone they were not designed to solve. Within HML there are various types of techniques that interact with the data in different ways. Here providing the algorithm with a small set of labelled data. Then, you give it a much larger set of unlabeled data and put it to work. This type of algorithm is helpful when you need (or have) to start with a smaller batch of data upfront. It learns from all the data, not just the labelled data, and helps you organize it.
* Detecting those threatening accounts in OSNs has become a must to avoid various malicious activities, insure security of user’s accounts and protect personal information. Researchers attempt to come up with automated detection tools for identifying fake accounts, which would be labor-intensive and costly if done manually. The implications of researchers attempt may allow an OSN operator detecting fake accounts efficiently and effectively, it would improve the experience of its users by preventing annoying spam messages and other abusive content. The OSN operator can also increase the credibility of its user metrics and enable third parties to consider its user accounts.
* A Support Vector Machine (SVM) is a binary classifier that performs classification by finding a hyperplane that maximizes distance between two classes.
* The algorithm outputs a hyperplane that fairly divides two classes with the help of training data and categorizes new examples. In two dimensional space this hyperplane is a line dividing a plane in two parts where in each class lay in either side.
* Random Forest is a classifier that contains a number of decision trees on various subsets of the given dataset and takes the average to improve the predictive accuracy of that dataset
* Decision Tree is a Supervised learning technique that can be used for both classification and Regression problems, but mostly it is preferred for solving Classification problems. It is a tree-structured classifier, where internal nodes represent the features of a dataset, branches represent the decision rules and each leaf node represents the outcome.

# **Chapter 7. Proposed Methodology and Algorithm**

## **7.1 Overview**

Each profile (or account) in a social network contain lots of information such as name, gender, number of friends, number of followers, number of likes, location etc. Some of these information are private and some are public. We have used information that are public to determine the fake profiles in social Network as private information is not accessible. However, if our proposed scheme is used by the social networking companies itself then they can use the private information of the profiles for detection without violating any privacy issues. We have considered these information as features of a profile for classification of fake and real profiles. The steps that we have followed for detection of fake profiles are as follows. 1.

Features are selected to apply classification algorithms. The classification algorithm is discussed in the section 3.4 and 3.5. Attributes are selected as features if they are not dependent on other attributes and they increase efficiency of the classification. The features that we have chosen are discussed in section 4.2. 2. After selection of attributes, the dataset of profiles that are already classified as fake or genuine are needed for the training purpose of the classification algorithm.

We have used a publicly available dataset of 1337 fake users and 1481 genuine users consisting of various attributes including name, status count, number of friends, followers count, favourites, languages known etc. 3. The selected attributes are extracted from profile for the purpose of classification. 14 4. After this the dataset of fake and real profiles are prepared. From this dataset, 80% of both profiles (genuine and fake) are used to prepare a training dataset and 20% of both profiles are used to prepare a testing dataset. 5.

The training dataset is then fed to the classification algorithm. It learns from the training dataset and is expected to give correct class labels for the testing dataset. 6. The labels from the testing dataset are removed and are left for determination by the trained classifier. The result of classification algorithm is shown in 4.4. We have used two classification algorithms and have compared the efficiency of these algorithms.

This is a framework that can easily be implemented by social networking companies as they have access to user information.

1. Classification starts from the selection of profile that needs to be classified.

2. Once the profile is selected, the useful features are extracted for the purpose of classification.

3. The extracted features are then fed to trained classifier.

4. Classifier is trained regularly as new data is fed into the classifier.

5. Classifier then determines whether the profile is genuine or fake.

6. The result of classification algorithm is then verified and feedback is fed back into the classifier.

7. As the number of training data increases the classifier becomes more and more accurate in predicting the fake profiles.

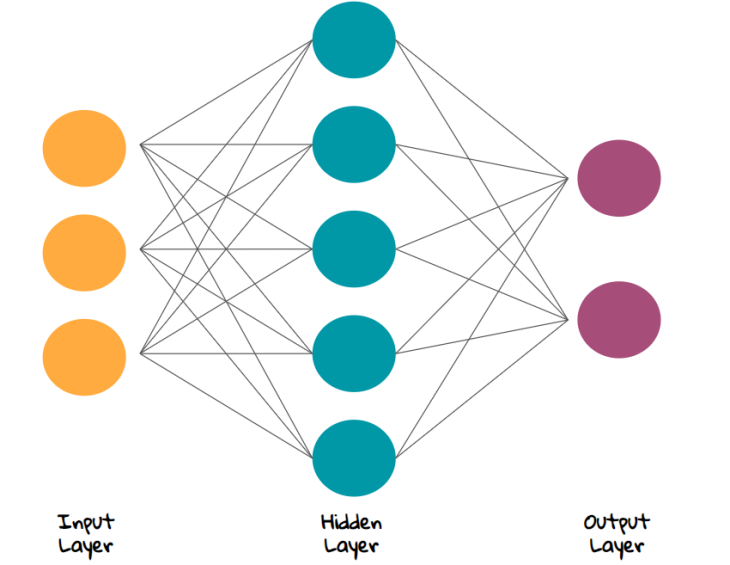
## **7.2 Classification**

Classification is a technique of categorizing an object into a particular class based on the training data set that was used to train the classifier. We feed the classifier with data set so that we can train it to identify related objects with as best accuracy as possible. Classifier is an algorithm used for classification. In this project we have used two classifiers namely Neural Networks and Support Vector Machines and have thereby compared their efficiencies.

## **7.3 Neural Networks**

The conventional method by which a computer works is that you provide instructions or algorithms to the computer and it generates output based on it. But what if you do not know the algorithm to solve a problem ? Will your computer still be able to provide solutions. If we use conventional techniques 17 then the computer will not be able to solve the problem unless you provide some instructions. Here comes the concept of Neural Networks. We can still solve such a problem by training a network as such our program will learn on its own and will provide solution close to a certain accuracy. The term Neural Networks was coined in 1943 but could not be implemented then due to lack of technology. Neural Networks learn by example. Neural Networks are based on biological neurons i.e. brain cells and the way information is processed inside the brain. There are mainly two types of neural networks : (1) Single Layer Networks also called a Perceptron.

The above figure shows a perceptron.



**Figure 7.3.1: Neural Networks**

**Multi - Layer Network** In multi layer network apart from the input layer and output layer there are hidden layers which cater on increasing the efficiency of classifying objects. In this network output of one hidden layer is used as input for another hidden layer. This network is also known as Deep Neural Network.

### 7.3.1 Back Propagation

The algorithm used in implementing Neural Networks is back propagation. The algorithm is as follows :-

1. There are two types of outputs, model output and desired output. The difference between these two output is calculated which is the error. Mean Square Error is also calculated.
2. The weights assigned to each input is either increased or decreased with the motive of minimizing the error.
3. The model output is recomputed, error rechecked until the error cannot be minimized further. Minimum error is found by finding minima using gradient descent.

### 7.3.2 Neural Networks Libraries

Neural Networks is implemented using tensorflow or pybrain in python. In this project we have used pybrain for classifying data into real and fake using neural networks.

## **7.4 Support Vector Machine**

A Support Vector Machine (SVM) is a binary classifier that performs classification by finding a hyperplane that maximizes distance between two classes. It is a supervised machine learning algorithm. The algorithm outputs a hyperplane that fairly divides two classes with the help of training data and categorizes new examples. In two dimensional space this hyperplane is a line dividing a plane in two parts where in each class lay in either side. Can you decide a separating line for the classes? Draw a line that separates black circles and blue squares. You might have come up with something similar to following image. It separates the two classes. Any point that is left of line falls into black circle class and on right falls into blue square class. Separation of classes. That’s what SVM does. Sample cut to divide into two classes.

### 7.4.1 Selecting SVM Hyperplanes



**Figure.7.4.1.1: Support Vector Machine**

**7.4.2 Linearly Separable**

For the data which can be separated linearly, we select two parallel hyperplanes that separate the two classes of data, so that distance between both the lines is maximum. The region b/w these two hyperplanes is known as “margin” & maximum margin hyperplane is the one that lies in the middle of them. w x - b 1 , if = 1 i ≥ θi w x - b 1 , if = -1 i ≤ θi Where ⍵ is normal vector to the hyperplane, θi denotes classes & xi denotes features. For proper classification, we can build a combined equation: ∣∣w∣∣ for = 1,2,......,n min θi (wx b) i − ≥ 1 ∀i As it maximizes margin between two classes, SVM is a robust model to solve prediction problems.

### 7.4.3 SVM Libraries

For implementing SVM on a dataset, we can use libraries. There are many libraries available that can help us to implement SVM smoothly. It contains in-built functions that can be called whenever required. In Python, we can use libraries like sklearn. For classification, Sklearn provides functions like SVC, NuSVC & LinearSVC. We pass values of kernel parameter, gamma and C parameter etc. By default kernel parameter uses “rbf” as its value. In this project we have used SVC function of Sklearn.

## **7.5 Random Forest**

Random Forest is a popular machine learning algorithm that belongs to the supervised learning technique. It can be used for both Classification and Regression problems in ML. It is based on the concept of ensemble learning, which is a process of combining multiple classifiers to solve a complex problem and to improve the performance of the model.

As the name suggests, *"*Random Forest is a classifier that contains a number of decision trees on various subsets of the given dataset and takes the average to improve the predictive accuracy of that dataset." Instead of relying on one decision tree, the random forest takes the prediction from each tree and based on the majority votes of predictions, and it predicts the final output.

The greater number of trees in the forest leads to higher accuracy and prevents the problem of overfitting.



**Figure.7.5.1: Random Forest**

## **7.6 Decision Tree**

* Decision Tree is a Supervised learning technique that can be used for both classification and Regression problems, but mostly it is preferred for solving Classification problems. It is a tree-structured classifier, where internal nodes represent the features of a dataset, branches represent the decision rules and each leaf node represents the outcome.
* In a Decision tree, there are two nodes, which are the Decision Node and Leaf Node. Decision nodes are used to make any decision and have multiple branches, whereas Leaf nodes are the output of those decisions and do not contain any further branches.
* The decisions or the test are performed on the basis of features of the given dataset.
* It is a graphical representation for getting all the possible solutions to a problem/decision based on given conditions*.*
* It is called a decision tree because, similar to a tree, it starts with the root node, which expands on further branches and constructs a tree-like structure.
* In order to build a tree, we use the CART algorithm, which stands for Classification and Regression Tree algorithm.
* A decision tree simply asks a question, and based on the answer (Yes/No), it further split the tree into subtrees.
* Below diagram explains the general structure of a decision tree:



**Figure.7.6.1: Decision Tree**

## **7.7 Algorithm for System**

**INPUT**: The dataset from CSV files

**OUTPUT:** Accuracy

1. Read dataset: Read genuineusers.csv and fake users.csv and append them in a list, named x, and make list y for labelling class. Return x,y.
2. Feature Extraction: Convert non-integer features in dataset to integer. Store and overwrite selected 6 features in list x. Return x
3. Split data into training data and test data using 5 cross validation and store them separately x\_train, x\_test, y\_train, y\_test.
4. Scaling of the X\_data. (x\_train, x\_test)
5. Use ensemble classifier, voting classifier, with SVM and Logistic Regression.
6. Store result in y\_pred variable and Return y\_pred.
7. Repeat step 3 with y pred and x\_test
8. Output from step 3 is given to Neural Network and then store the output in y\_pred.
9. Testing: Evaluating our trained model against the test data. The output is visual graph consisting of True\_Positive\_Rate and False\_Positive\_Rate with accuracy, i.e, ROC curve.
10. Print the classification accuracy on testing dataset. Plot the confusion matrix. Print the execution time.
11. Exit

No proposal can be modeled into a system without some experiments to support it. In this section we have included the results and outputs produced during experiment with our system and by our system under various inputs and parameters.

**Chapter 8. Tools and Technology Used**

**8.1 Python programming language**

Python is a high-level, interpreted programming language that is widely used for developing a variety of applications. It was first released in 1991 by Guido van Rossum, and since then it has become one of the most popular programming languages in the world. Python is known for its simple syntax and ease of use, which makes it a great language for beginners to learn. It is also widely used in the scientific community for data analysis and visualization, as well as in web development, game development, artificial intelligence, and more. Python has a large standard library, which includes modules for performing tasks such as file I/O, regular expressions, and networking. Additionally, there are many third-party libraries available for Python, such as NumPy, Pandas, and Matplotlib, that provide advanced functionality for tasks like scientific computing and data visualization. Python is an open-source language, meaning that it is free to use and modify, and there is a large community of developers who contribute to its development and support.

**i. Core libraries**

Built-in functions and modules: Python comes with a large set of built-in functions and modules, such as math, random, os, and sys, that provide useful tools for performing common tasks like mathematical calculations, generating random numbers, and working with the operating system.

Python supports a number of built-in data types, such as lists, dictionaries, and sets, which make it easy to work with and manipulate data.Standard library modules: Python's standard library includes a wide range of modules that provide functionality for tasks like working with dates and times, parsing XML and JSON, and accessing network resources.

**ii. Machine Learning**

The most useful machine learning library in Python is Scikit-learn. It is a comprehensive and powerful library with a wide range of fundamental methods. Scikit-learn offers various supervised and unsupervised learning techniques through a simple Python framework. It is licensed under a permissive BSD license and is available through many Linux distributions, making it suitable for both educational and commercial use.

**iii Data Illustration**

Matplotlib is a Python library for creating MATLAB-like graphs, designed with a reduced level of complexity and several added features. Initially, its syntax may be somewhat challenging, but once you understand its key concepts, drawing almost any type of graph becomes simple. Matplotlib is an integral part of the scientific Python ecosystem and is widely used for data visualization.

**iv. Pandas**

Matplotlib is a Python application for creating MATLAB-like graphs. It is designed to be simple to use with a reduced level of complexity and many added features. Initially, the syntax may be somewhat challenging, but once you understand its key concepts, drawing almost any graph is straightforward. Matplotlib is open-source software, and its large user community provides support and examples of graphs and visualizations. Additionally, Python has an open-source database library called Pandas, which is ideal for data analysis and manipulation. Using Matplotlib and Pandas together can be very beneficial in fields that require data analysis and visualization.

**v. Numpy**

NumPy is a powerful library for scientific computing and higher math operations. It can also be used for handling standard data as a method of container. With the support of a huge collection of high-level mathematical functions, NumPy is a prominent Python library for manipulating huge multi-dimensional arrays and performing important scientific calculations. It provides functionality for Fourier transforms, linear algebra, and many other mathematical operations.

**vi. SciPy**

SciPy is one of the most user-friendly and powerful libraries that can solve various mathematical routines for efficiency and numerical integration. Scikit-learn covers almost all of the learning algorithms which are divided into two categories: supervised and unsupervised. It is also possible to use Scikit-learn for data analysis and data mining, making it the perfect tool to start with for machine learning.

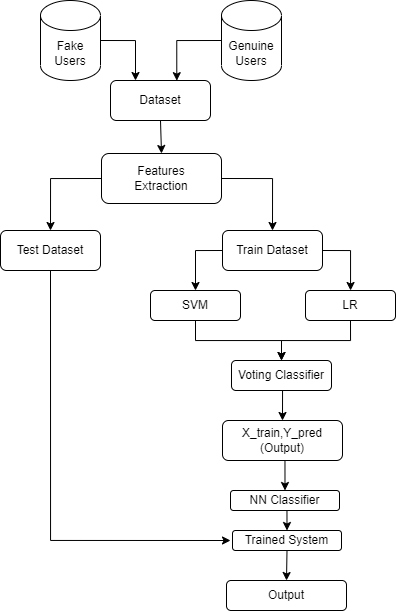
**8.2 Tools**

Tools of machine learning refer to the software and programming languages used to develop, test, and deploy machine learning models. Some common tools of machine learning include:

1. Programming languages: Python and R are the most popular programming languages for machine learning.
2. Libraries and frameworks: Libraries such as NumPy, Pandas, Scikit-learn, TensorFlow, PyTorch, Keras, and many others provide a wide range of functionality for data preprocessing, model building, training, and evaluation.
3. Visualization tools: Visualization tools such as Matplotlib and Seaborn are used for data exploration, model interpretation, and presentation of results.
4. Cloud platforms: Cloud platforms such as AWS, Google Cloud, and Microsoft Azure provide infrastructure for deploying and scaling machine learning models.
5. Data storage and processing: Databases such as MySQL, PostgreSQL, and MongoDB are used for storing and processing large datasets.
6. Development environments: Integrated development environments (IDEs) such as Jupyter Notebook, PyCharm, and Spyder provide a convenient interface for developing and testing machine learning models.

# **Chapter 9. Implementation Details**

Each phase of our proposed system is briefly described in this section along with description, results at each stage are also provided.



**Fig. 9 Hybrid Model**

## **9.1 Data Collection**

For the model to work upon, there is a need for data collection. The dataset can be collected from various online platforms and can also be created by using Crawler. We have collected two datasets through online from well-known websites Kaggle and GitHub. But we worked on the dataset which is collected by Kaggle and in that we are using two CSV files corresponding to fake and genuine users. Figure 5 shows the sample of csv file. And the code for reading both the files are:

genuineusers=pd.read\_csv("users.csv")

fakeusers= pd.read\_csv(“fusers.csv")

Data pre-processing is used to achieve the better result from any machine learning model and data processing is used to clean the data from raw data we import the useful libraries which will rescale or clean our data and the libraries we import are numpy, panda, scikit-learn and from sklearn we import preprocessing to clean our data. Now in the next part for data preprocessing we use feature extraction technique first we try the principal component analysis technique and then we use the genetic algorithm and then after we select the features manually and we compare the result obtained from three ways and we get better result from the manually selection of features and the features we select manually are:

* statuses\_count
* followers\_count
* friends\_count
* favourites\_count
* listed\_count
* lang\_code

The language code feature is of string type we convert it into integer. After calling extract feature function it prints the extracted feature name and describes the entire extracted feature in summarized by printing mean, quartile, count, std, min, max etc.

Figure 4 shows the data distribution in each column or feature in terms of count, mean, standard deviation, minimum and maximum values, and average of 25%, 50% and 75% of the data points when taken in ascending order.

**9.2 Evaluation Parameters**

**Efficiency/Accuracy** = Number of correct predictions/ total number of predictions

**Percent Error** = (1-Accuracy)\*100

**Confusion Matrix** - Confusion Matrix is a technique for summarizing the performance of a classification algorithm. Calculating a confusion matrix can give you a better idea of what your classification model is getting right and what types of errors it is making.

**TPR**- True Positive Rate TPR=TP/(TP+FN)

**FPR**- False Positive Rate FPR=FP/(FP+TN)

**TNR**- True Negative Rate TNR=TN/(FP+TN)

**FNR**- False Negative Rate FNR=1-TPR

**Recall**- How many of the true positives were recalled (found), i.e. how many of the correct hits were also found.

**Recall** = TP / (TP+FN) Precision- Precision is how many of the returned hits were true positive i.e. how many of the found were correct hits.

**Precision** = TP / (TP + FP) F1 score- F1 score is a measure of a test's accuracy. It considers both the precision p and the recall r of the test to compute the score. ROC

**Curve**- The Receiver Operating Characteristic is the plot of TPR versus FPR. ROC can be used to compare the performances of different classifiers

**F1 score**- F1 score is a measure of a test's accuracy. It considers both the precision p and the recall r of the test to compute the score.

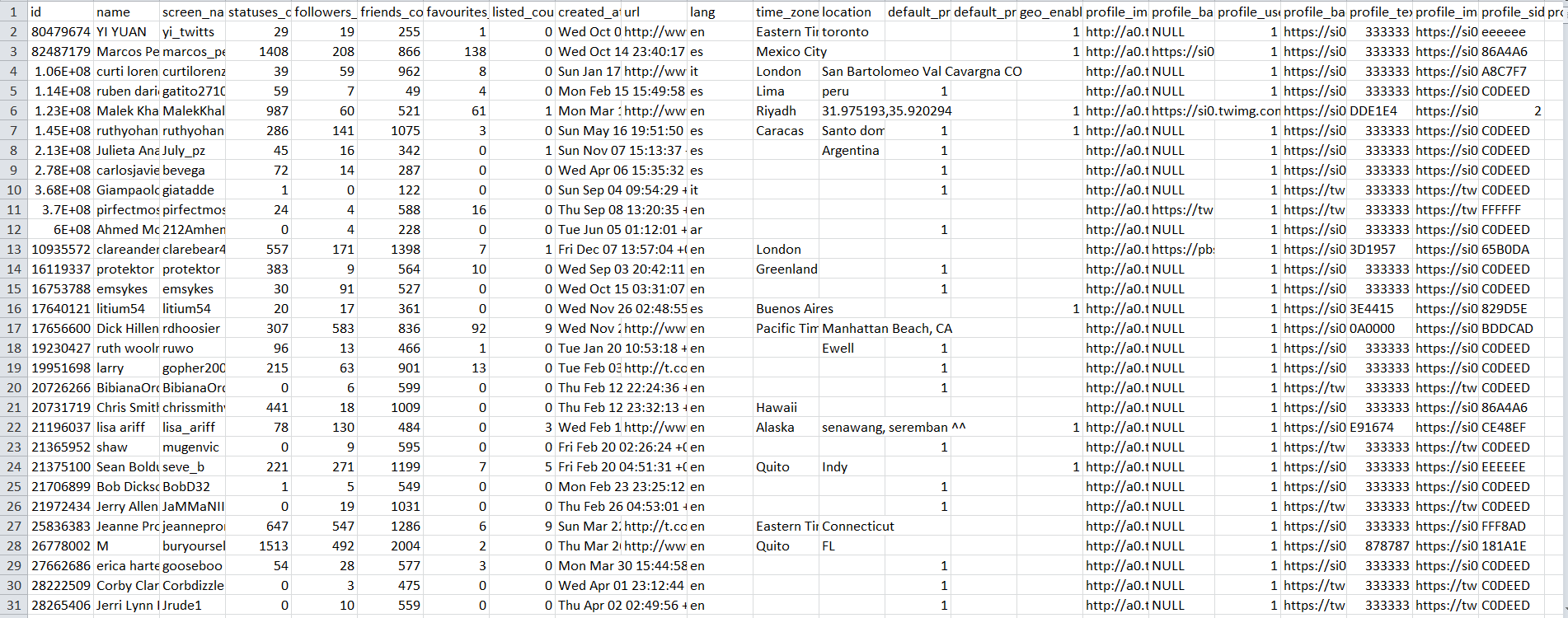
**ROC Curve**- The Receiver Operating Characteristic is the plot of TPR versus FPR. ROC can be used to compare the performances of different classifiers.

## **9.3 Training of Classifiers**

As we are using the hybrid approach of the techniques in our proposed system, so we have done experiments with five techniques i.e. SVM, RF, LR, DTC, NN and finalize the techniques that gives the best result and they are Support Vector Machine, Logistic Regression and Neural Network.

First we train our data using support vector machine independently and then we train our data on Logistic Regression independently and after analyzing the result of both the classification techniques we merge both the techniques to check the accuracy of both of them together and hybrid approach of both the techniques gives us the best result and after training the data from both the voting classifier is used to get the best result from both and then passing value for any one of them and then we use 5 fold cross validation technique to avoid the situation of overfitting as in k-fold cross validation technique dataset in divided into k folds where 1 fold is used for validation or testing while others are used for training and in these way we can avoid the situation of overfitting.

After getting the score of each fold final estimated score is printed and in these we got 0.91 and the accuracy on testing dataset is 99.56.and after that the confusion matrix is plotted which will gives us the 261 true positive value and 7 false negative value and 29 false positive and 267 true negative value and then we plot the normalized confusion matrix which gives us all the four (TP,TN,FP,FN) values in percentage form along with precision, recall, f1 score and support and all these are evaluation criteria. For fake recall we got is 0.98 and for genuine it is 1.00 and f1 score for both is 0.99 and overall accuracy is0.99. called epoch.

****

## **9.4 Training of Neural Network**

The training of neural network. Each line corresponds to each round of forward and backward propagation For this instance, we have taken our epoch to be 10, total number of layers to be 3, it took approximately minutes and seconds to train the system with final accuracy and loss value to be respectively. Now the output produced by several hybrid techniques. We have collected two datasets say, D1 and D2 and the difference between these datasets is in their size, D2 is large as compared to D1. D2 contains approx. 3500 rows while D1 contains approx. 1500 rows. The results that we have obtained with different algorithms on both datasets are different and D2 gives less system with less accuracy as compared to D1.

As we can see there is an accuracy difference between both datasets used by different algorithms so further, we will be working and showing results for only dataset, D1. We are using two csv files one is of genuine users and other one is of fake users. Figure 7 shows the accuracy of each of our experimental model in ascending order and the model with highest accuracy being our trained system.

Figure 8 shows the confusion matrices for our proposed hybrid model which gives us the summary of true positive, true negative, false positive and false negative without normalization.

**9.4.1 Table 1: Comparison of Various Machine Learning Algorithm**

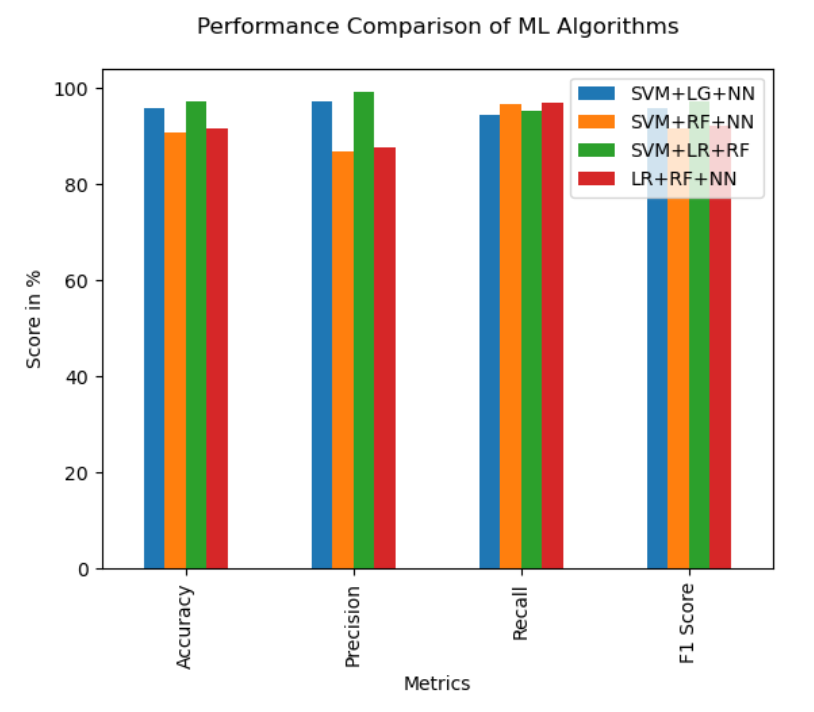
|  |  |  |
| --- | --- | --- |
| **S.No.** | **Machine Learning Algorithm** | **Accuracy** |
| 1 | Support Vector Machine (SVM) | 91% |
| 2 | Random Forest (RF) | 94% |
| 3 | Neural Network (NN) | 94% |

**9.4.2 Table 2: Comparison of Hybrid Model**

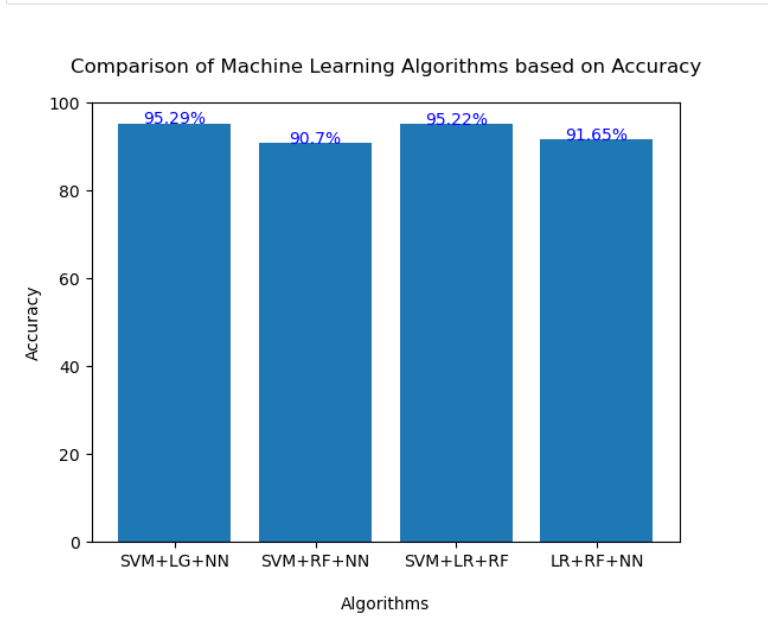
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Hybrid Techniques** | **Precision** | **Recall** | **F1 -Ccore** | **Accuracy**  **(%)** |
| SVM+LG+NN | 97.27% | 94.27% | 95.75% | 95.82% |
| SVM+RF+NN | 86.67% | 96.71% | 91.41% | 90.70% |
| SVM+LR+RF | 99.85% | 95.55 | 97.65% | 97.66% |
| LR+RF+NN | 99.08% | 95.29% | 97.15% | 95.22% |

**Chapter 10. Result Analysis**

**10.1. Performance Comparison of Machine Learning Algorithm**

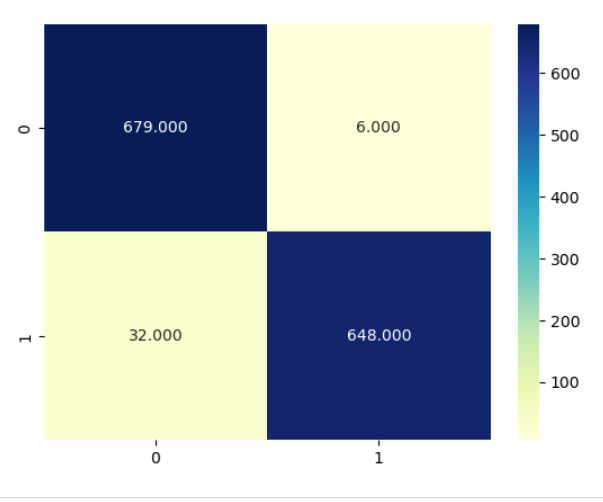


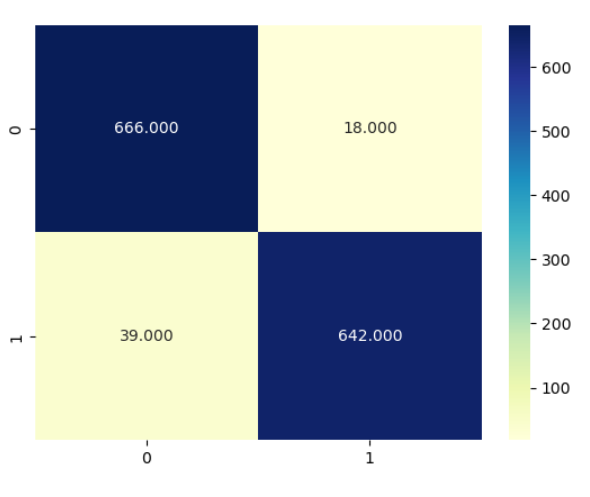
**10.2 Comparison of Hybrid Model based on Accuracy**

****

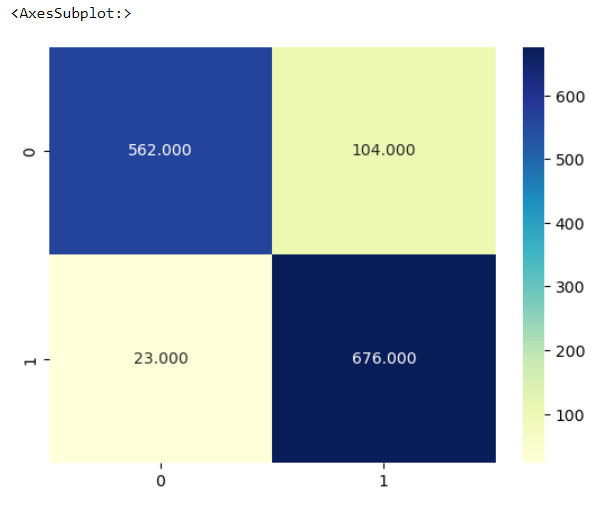
**10.3 Confusion Matrix**

**10.3.1 Confusion Matrix of SVM+LR+RF**

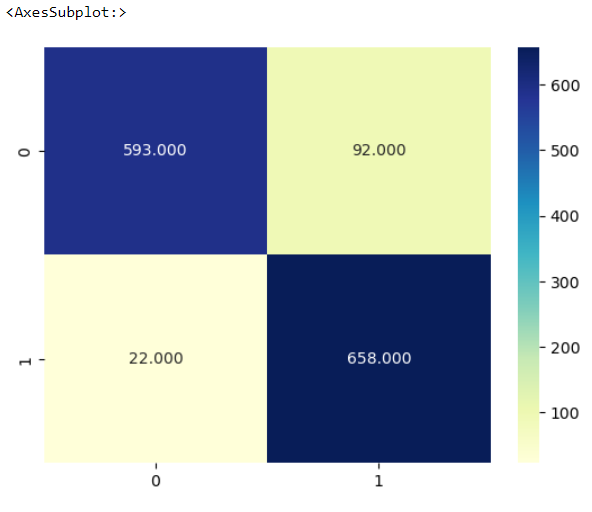
****

**10.3.2 Confusion Matrix of SVM+LR+NN**

**10.3.3 Confusion Matrix of SVM-RF-NN**

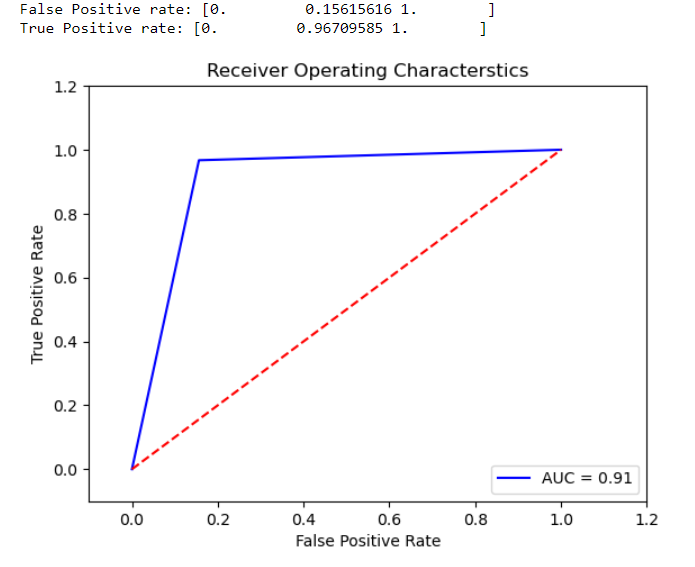
****

**10.3.4 Confusion Matrix of LR+RF+NN**

****

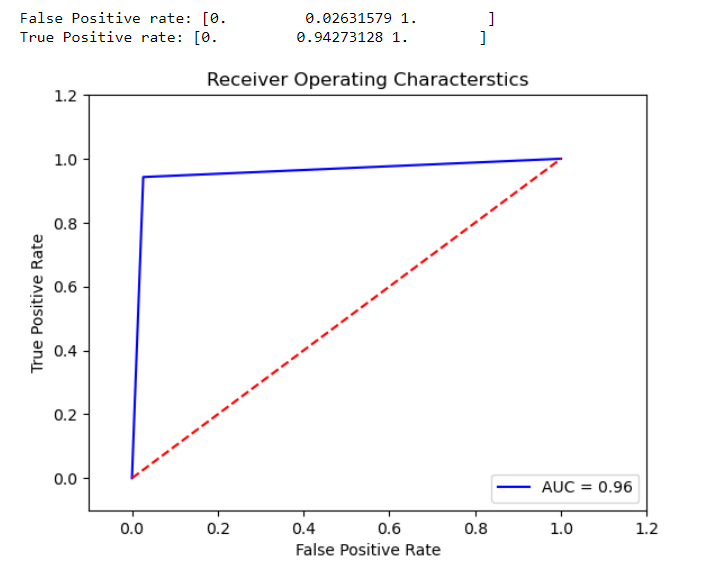
**10.4. ROC Curve**

**10.4.1. SVM+RF+NN**

****

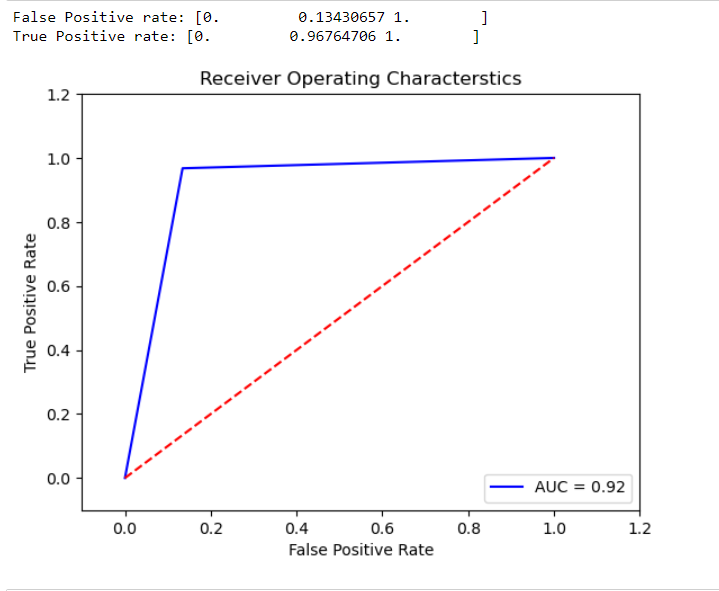
Accuracy with SVM RF NN is 91%

**10.4.2. SVM+LR+NN**

****

Accuracy with SVM LR NN is 96%

**10.4.3. LR+RF+NN**

****

Accuracy with LR RF NN is 92%

# **Chapter 11. Conclusion**

The use of Online Social Networks has become a big part of people's lives, but it also poses a risk due to the presence of fake accounts. To detect such accounts, machine learning algorithms can be applied to predict and classify datasets. In this work, a hybrid approach was used to compare eight different combinations of classification algorithms on the dataset of an Online Social Network. The best accuracy was obtained by combining SVM and Logistic Regression and Neural Network (96%), which led to the proposal of a model for the detection of fake accounts. This approach can be useful in improving the safety and security of Online Social Networks by identifying and removing fake accounts.

# **Chapter 12. Future Work**

1. **Improving the accuracy of the hybrid model** : Although the proposed hybrid approach has the best accuracy, there may be room for further improvement. Researchers could experiment with different combinations of machine learning algorithms and adjust their parameters to optimize the model's performance.
2. **Incorporating new features:** Currently, the proposed model uses a limited set of features to classify accounts as fake or genuine. Future work could involve exploring new features that could improve the accuracy of the model, such as the user's activity patterns, posting frequency, or the network structure of their connections.
3. **Evaluating the model on different datasets:** The proposed model was evaluated on a specific dataset of an online social network. Future work could involve evaluating the model on different datasets from various social networks to test its generalizability and robustness.
4. **Developing real-time detection:** The proposed model was applied to a pre-existing dataset, but future work could involve developing a real-time system that can detect fake accounts as soon as they are created. This would require integrating the model with the social network's platform and monitoring new account creations in real-time.
5. **Addressing ethical concerns:** Machine learning algorithms for fake account detection raise ethical concerns, such as privacy issues and potential biases in the classification process. Future work could involve developing approaches to mitigate these concerns, such as ensuring transparency in the classification process and obtaining user consent for data collection and analysis.

# **Chapter 13. References**

1. Joshi, Shruti, et al. "Identifying Fake Profile in Online Social Network: An Overview and Survey." International Conference on Machine Learning, Image Processing, Network Security and Data Sciences. Springer, Singapore, 2020. Available at: <https://link.springer.com/chapter/10.1007/978-981-15-6315-7_2>
2. Mohanty, Sachi, et al. Recommender System with Machine Learning and Artificial Intelligence. Wiley-Scrivener, 2020. Available at <https://www.researchgate.net/publication/342970511_Recommender_System_with_Machine_Learning_and_Artificial_Intelligence>
3. Balaanand, Muthu, et al. "An enhanced graph-based semi-supervised learning algorithm to detect fake users on Twitter." The Journal of Supercomputing 75.9 (2019): 6085-6105. Available at: <https://link.springer.com/article/10.1007/s11227-019-02948-w#:~:text=The%20proposed%20strategy%20is%20an,processed%20to%20extract%20the%20features.>
4. Boshmaf, Yazan, et al. "Integro: Leveraging Victim Prediction for Robust Fake Account Detection in OSNs." NDSS. Vol. 15. 2015.
5. Erşahin, Buket, et al. "Twitter fake account detection." 2017 International Conference on Computer Science and Engineering (UBMK). IEEE, 2017
6. Mateen, Malik, et al. "A hybrid approach for spam detection for Twitter." 2017 14th International Bhurban Conference on Applied Sciences and Technology (IBCAST). IEEE, 2017.
7. Al-Qurishi, Muhammad, et al. "A prediction system of Sybil attack in social network using deep-regression model." Future Generation Computer Systems 87 (2018): 743-753.
8. Cresci, Stefano, et al. "Fame for sale:Efficient detection of fake Twitter followers." Decision Support Systems 80 (2015): 56-71.
9. Yang, Zhi, et al. "Uncovering social network sybils in the wild." ACM Transactions on Knowledge Discovery from Data (TKDD) 8.1 (2014): 1-29.
10. Adikari, Shalinda, and Kaushik Dutta. "Identifying fake profiles in linkedin." arXiv preprint arXiv:2006.01381 (2020).
11. ] Xiao, Cao, David Mandell Freeman, and Theodore Hwa. "Detecting clusters of fake accounts in online social networks." Proceedings of the 8th ACM Workshop on Artificial Intelligence and Security. 2015.
12. Jia, Jinyuan, Binghui Wang, and Neil Zhenqiang Gong. "Random walk based fake account detection in online social networks." 2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). IEEE, 2017.
13. Kaur, Ravneet, and Sarbjeet Singh. "A survey of data mining and social network analysis based anomaly detection techniques." Egyptian informatics journal 17.2 (2016): 199-216.
14. Sahoo, SomyaRanjan, and Brij B. Gupta. "Hybrid approach for detection of malicious profiles in twitter." Computers & Electrical Engineering 76 (2019): 65-81.