

# Visvesvaraya Technological University

Jnana Sangama, Belagavi - 590018



A Project Work Phase-I (17CSP78)

Report on

## **“Detection of Fake and Clone Accounts on Twitter”**

*Project Report submitted in partial fulfilment of the requirement for the*

*award of the degree of*

**BACHELOR OF ENGINEERING**

IN

**COMPUTER SCIENCE AND ENGINEERING**

**Submitted by**

KAVITHA S	1KS17CS034
RAJASHREE SHIVAKUMAR	1KS17CS060
SHARANYA H	1KS17CS074
KRUTHIKA B M	1KS18CS401

Under the guidance of

**Dr. Deepa S R**

Associate Professor

Department of Computer Science & Engineering

K.S.I.T, Bengaluru-560109



**KSIT**  
K. S. INSTITUTE OF TECHNOLOGY

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

**K. S. Institute of Technology**

#14, Raghuvanahalli, Kanakapura Road, Bengaluru - 560109

2020 - 2021

# K. S. Institute of Technology

#14, Raghuvanahalli, Kanakapura Road, Bengaluru - 560109

## Department of Computer Science & Engineering



Certified that the Project Work Phase-I (17CSP78) entitled “**Detection of Fake and Clone Accounts on Twitter**” is a bonafide work carried out by:

<b>KAVITHA S</b>	<b>1KS17CS034</b>
<b>RAJASHREE SHIVAKUMAR</b>	<b>1KS17CS060</b>
<b>SHARANYA H</b>	<b>1KS17CS074</b>
<b>KRUTHIKA B M</b>	<b>1KS18CS401</b>

in partial fulfilment for VII semester B.E., Project Work in the branch of Computer Science and Engineering prescribed by **Visvesvaraya Technological University, Belagavi** during the period of September 2020 to January 2021. It is certified that all the corrections and suggestions indicated for internal assessment have been incorporated. The Project Work Phase-I Report has been approved as it satisfies the academic requirements in report of project work prescribed for the Bachelor of Engineering degree.

.....  
**Signature of the Guide**

[Dr. Deepa S R]

.....  
**Signature of the HOD**

[Dr. Rekha B. Venkatapur]

.....  
**Signature of the Principal &  
CEO**

[Dr. K.V.A. Balaji]

## DECLARATION

We, the undersigned students of 7th semester, Computer Science & Engineering, KSIT, declare that our Project Work Phase-I entitled “**Detection of Fake and Clone Accounts on Twitter**”, is a bonafide work of ours. Our project is neither a copy nor by means a modification of any other engineering project.

We also declare that this project was not entitled for submission to any other university in the past and shall remain the only submission made and will not be submitted by us to any other university in the future.

Place:

Date:

**Name and USN**

**Signature**

**KAVITHA S (1KS17CS034)**

.....

**RAJASHREE SHIVAKUMAR (1KS17CS060)**

.....

**SHARANYA H (1KS17CS074)**

.....

**KRUTHIKA B M (1KS17CS401)**

.....

## ACKNOWLEDGEMENT

The satisfaction and euphoria that accompany the successful completion of any task will be incomplete without the mention of the individuals, we are greatly indebted to, who through guidance and providing facilities have served as a beacon of light and crowned our efforts with success.

First and foremost, our sincere prayer goes to almighty, whose grace made us realize our objective and conceive this project. We take pleasure in expressing our profound sense of gratitude to our parents for helping us complete our Project Work Phase-I successfully.

We take this opportunity to express our sincere gratitude to our college **K.S. Institute of Technology**, Bengaluru for providing the environment to work on our project.

We would like to express our gratitude to our **MANAGEMENT**, K.S. Institute of Technology, Bengaluru, for providing a very good infrastructure and all the kindness forwarded to us in carrying out this project work in college.

We would like to express our gratitude to **Dr. K.V.A Balaji**, Principal & CEO, K.S. Institute of Technology, Bengaluru, for his valuable guidance.

We like to extend our gratitude to **Dr. Rekha.B.Venkatapur**, Professor and Head, Department of Computer Science & Engineering, for providing a very good facilities and all the support forwarded to us in carrying out this Project Work Phase-I successfully.

We also like to thank our Project Coordinators, **Mr. K Venkata Rao**, Associate Professor, **Mrs. Vaneeta M**, Associate Professor, **Mr. Raghavendrachar S**, Asst. Professor, **Mr. Aditya Pai H**, Asst. Professor, and **Mrs. Sneha K**, Asst. Professor, Department of Computer Science & Engineering for their help and support provided to carry out the Project Work Phase-I successfully.

Also, we are thankful to **Dr. Deepa S R**, Associate Professor, for being our Project Guide, under whose able guidance we have been able to carry out this Project Work Phase-I successfully.

We are also thankful to the teaching and non-teaching staff of Computer Science & Engineering, KSIT for helping us in completing the Project Work Phase-I successfully.

**KAVITHA S**  
**RAJASHREE SHIVAKUMAR**  
**SHARANYA H**  
**KRUTHIKA B M**

## ABSTRACT

Online Social Network (OSN) is a network hub where people with similar interests or real world relationships interact. As the popularity of OSN is increasing, the security and privacy issues related to it are also rising. Fake and Clone user profiles are creating dangerous security problems to the genuine users. Twitter is one such social networking service which is popular amongst social network users but also has fake and clone profiles which is a threat to the users. Cloning of user profiles is one serious threat, where already existing user's details are stolen to create duplicate profiles and then it is misused for damaging the identity of original profile owner. They can even launch threats like phishing, stalking, spamming etc. Fake profile is the creation of profile in the name of a person or a company which does not really exist on social media, to carry out malicious activities. In this paper, using Supervised Machine Learning Algorithms a detection method is proposed which would detect Fake and Clone profiles on Twitter.

*Keywords - Online Social Network, OSN, Clone Profile, Fake Account, Twitter, Detection, Supervised ML Algorithm.*

## TABLE OF CONTENTS

<b>Chapter No.</b>	<b>Title</b>	<b>Page No.</b>
<b>1.</b>	<b>INTRODUCTION</b>	<b>1-2</b>
1.1	Overview	1
1.2	Purpose of the Project	1
1.3	Definitions	2
<b>2.</b>	<b>LITERATURE SURVEY</b>	<b>3-4</b>
<b>3.</b>	<b>PROBLEM IDENTIFICATION</b>	<b>5</b>
3.1	Problem Statement	5
3.2	Project Scope	5
<b>4.</b>	<b>GOALS AND OBJECTIVES</b>	<b>6</b>
4.1	Project Goals	6
4.2	Project Objectives	6
<b>5.</b>	<b>SYSTEM REQUIREMENT SPECIFICATION</b>	<b>7</b>
5.1	Software Requirements	7
5.2	Hardware Requirements	7
<b>6.</b>	<b>METHODOLOGY</b>	<b>8</b>
<b>7.</b>	<b>APPLICATIONS</b>	<b>9</b>
<b>8.</b>	<b>CONTRIBUTION TO SOCIETY AND ENVIRONMENT</b>	<b>10</b>
	<b>REFERENCES</b>	<b>11</b>
	<b>APPENDIX - I CSI PUBLISHED PAPER COPY</b>	<b>12</b>
	<b>APPENDIX - II CERTIFICATES OF PAPER PRESENTED</b>	<b>13</b>

## LIST OF FIGURES

<b>Fig. No.</b>	<b>Figure Name</b>	<b>Page No.</b>
6.1	Methodology Flowchart	8

## Chapter 1

# INTRODUCTION

### 1.1 Overview

Social networking phenomenon has grown extremely since the last twenty years. Online Social Networks are used by billions of users all around the world to build network connections. The ease and accessibility of social networks have created a new era of networking. During this rise, online social networks have created many online activities which instantly attract the interests of large number of users. On the other hand, they also suffer from the increase in the number of fake and clone accounts.

Online Social Network (OSN) users share a lot of information in the network like photos, videos, personal details, career details etc. This information if put into the hands of attackers, the after effects are very severe. Most of the OSN users are unaware of the security threats that exist in the social networks and easily fall prey to these attacks. Twitter is one such social networking service, which is popular among the social network users but also has fake and clone accounts which is a threat to the users.

Fake account creation is the creation of an account in the name of a person or a company which does not really exist on social media, to carry out malicious activities. Cloning of user profiles is where the duplicate profiles of already existing users are created and then is misused for damaging the identity of the original profile owner.

According to the importance of the effect of social media to the society, this project aims at detecting the fake and clone accounts on Twitter to prevent the problems caused by these accounts to the genuine users. In this paper, a detection method is proposed which would detect Fake and Clone accounts on Twitter.

### 1.2 Purpose of the project

In the recent years, Fake and Clone accounts have become a very serious issue in online social networks. So, a detection method is very much necessary in order to overcome the problems caused by the frauds that create these fake and clone accounts which is also a threat to the genuine users.



## 1.3 Definitions

### ➤ **Anaconda**

Anaconda is a free and open source distribution of the Python and R programming languages for data science and machine learning related applications (large-scale data processing, predictive analytics, scientific computing), that aims to simplify package management and deployment. Package versions are managed by the package management system *conda*. The Anaconda distribution is used by over 6 million users and it includes more than 250 popular data science packages suitable for Windows, Linux and MacOS.

### ➤ **Python**

Python is an interpreter, object-oriented, high-level programming language with dynamic semantics, created by Guido van Rossum and first released in 1991. Python features a dynamic type system and automatic memory management and supports multiple programming paradigms, including object-oriented, imperative, functional programming and procedural styles. It has an expansive and extensive standard library its abnormal state worked in information structures, joined with dynamic writing makes it extremely alluring for Rapid Application Development.

### ➤ **Machine Learning**

Machine learning (ML) is a type of artificial intelligence (AI) that allows software applications to become more accurate at predicting outcomes without being explicitly programmed to do so. ML is the study of computer algorithms that improve automatically through experience.

### ➤ **Supervised Machine Learning**

Supervised learning is the machine learning task of learning a function that maps an input to an output based on example input-output pairs. It infers a function from labeled training data consisting of a set of training examples. In supervised machine learning, the algorithm learns on a labeled dataset, providing an answer key that the algorithm can use to evaluate its accuracy on training data.

## Chapter 2

### LITERATURE SURVEY

Piotr Brodka, Mateusz Sobas and Henric Johnson [1] have proposed two novel methods for detecting cloned profiles. The first method is based on the similarity of attribute values from original and cloned profiles and the second method is based on the network relationships. A person who doubts that his profile has been cloned will be chosen as a victim. Then treating name as primary key, a search is made for profiles with the same name as that of victim, using query search. Potential clone (Pc) and the Victim profile (Pv) are compared and similarity  $S$  is calculated. If  $S(Pc, Pv) > \text{Threshold}$ , then profile is suspected to be a clone. In the verification step, the user does it manually as he knows which one is the original profile and which is the duplicate one.

Supraja Gurajala, Joshua S. White, Brian Hudson and Jeanna N. Matthews [2] have proposed a system: Using a crawler, a large Twitter user profile database of 62 million user accounts was obtained and analyzed to understand the characteristics of fake account creation. A highly reliable 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. A subset of the accounts identified as fake by our algorithm were manually inspected and verified as all being fake (based on their Tweet activity).

Ahmed El Azab, Amira M Idrees, Mahmoud A Mahmoud, Hesham Hefny [3] have proposed a classification method for detecting fake accounts on Twitter. They have collected some effective features for the detection process from different research and have filtered and weighted them in first stage. Various experiments are conducted to get minimum set of attributes which gives accurate results. From 22 attributes, only seven attributes were selected which can effectively detect fake accounts and have applied these factors on classification techniques. A comparison of the classification techniques based on results is made and the one which provides most accurate result is selected.

Arpitha D, Shrilakshmi Prasad, Prakruthi S and Raghuram A S.[4] In the proposed work they have used different algorithms for different attributes like name, age, address and email. By making use of these algorithms duplicate profiles can be easily identified. All the algorithms give more probability to identify the correct match.

Sowmya P and Madhumita Chatterjee [5] have proposed a system where, for fake detection, a set of rules were used which when applied can classify fake and genuine profiles. Clone detection was carried out using Similarity Measures and C4.5 algorithm and a comparison was made to check the performance. Clone detection using Similarity Measures worked better than C4.5 and was able to detect most of the clones which were fed into the system. In this work they have considered only the profile attributes for fake and clone detection.

## **Chapter 3**

# **PROBLEM IDENTIFICATION**

### **3.1 Problem Statement**

Today, Online Social Network (OSN) has become an integral part of many people's lives. Many activities such as communication, promotion, advertisement, news, agenda creation are done through online social networks. But, some malicious accounts on social networking sites are creating dangerous security problems to the genuine users. Twitter is one such social networking service which is popular among the social network users but also has fake and clone accounts which is a threat to the users. In most of the fake and clone accounts, people lie on their ages for instance, mostly people set the age as 18-19 so that they make their account eligible for creation, people also lie about their gender, the images are also mostly downloaded from internet and some accounts have image of a character of different gender as set in their gender section by them.

### **3.2 Project Scope**

Since, it is not possible to distinguish between fake and genuine accounts just by looking at the profiles a detection method is proposed which would detect fake and clone accounts on Twitter. Existing datasets will be used for the experiments. User information will be extracted from the user profiles through the API's provided in the dataset. Later based on the tweets, number of followers and other activities of the users the fake and clone accounts will be detected using the supervised machine learning algorithms.

## **Chapter 4**

# **GOALS AND OBJECTIVES**

### **4.1 Project Goals**

The goals of our project are

- Detection of Fake accounts on Twitter.
- Classification of Clone and Real accounts on Twitter.

### **4.2 Project Objectives**

To achieve the goals of a project, it is very much necessary to be able to achieve the objectives of the project. The objectives of this project are to detect the Fake and Clone Twitter accounts. Using a detection system fake accounts are detected and to classify clone and real accounts, firstly Twitter accounts with cloned profiles have to be identified and only after this is done, classifying clone and real accounts is possible.

## Chapter 5

# SYSTEM REQUIREMENT SPECIFICATION

A software requirements specification (SRS) is a comprehensive description of the intended purpose and environment for software under development. The SRS fully describes what the software will do and how it will be expected to perform. Software requirements specification permits a rigorous assessment of requirements before design can begin and reduces later redesign. It should also provide a realistic basis for estimating product costs, risks, and schedules.

The software requirements specification document enlists enough and necessary requirements that are required for the project development. To derive the requirements we need to have clear and thorough understanding of the products to be developed or being developed. This is achieved and refined with detailed and continuous communications with the project team and customer till the completion of the software.

### 5.1 Hardware Requirements

- Processor: Intel i3 / i5 2.5GHz
- RAM : 4GB / 8GB
- Hard Disk : 50GB

### 5.2 Software Requirements

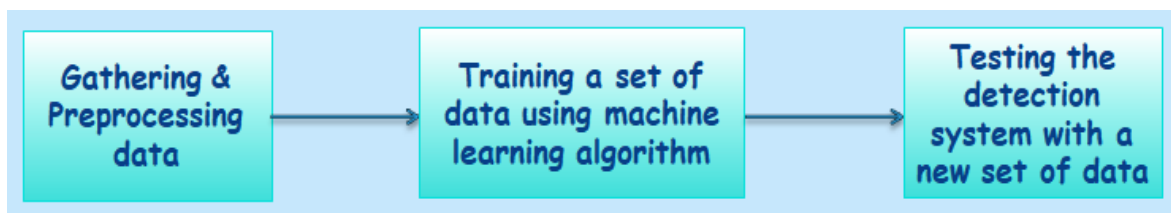
- Operating system : Windows 7/Windows 10
- Coding Language : Python
- IDE : Anaconda Navigator

## Chapter 6

### METHODOLOGY

Firstly the data will be gathered and analyzed. Then, data pre-processing will be done, which means if any data is missing, then statistical methods such mean, median and mode will be used for filling up the missing data. The data will be split into test data and train data. Train data is 75% of the data, which will be used for training the machine. Test data is the remaining 25% of the data, which will be used for testing the already trained machine. Then, a Supervised Machine Learning Algorithm is used for training a set of data. Finally, the detection system is tested with a new set of data which is not used for training to detect Fake and Clone accounts.

#### 6.1 Flowchart



*Fig.6.1: Methodology Flowchart*

Fig 6.1: Describes the Methodology.

## Chapter 7

### APPLICATIONS

The applications of this project are:

- Detection of Fake Twitter accounts.
- Identification of Twitter accounts with Cloned profiles.
- Classification Clone and Real profiles on Twitter.



## Chapter 8

# CONTRIBUTION TO THE SOCIETY AND ENVIRONMENT

Fake and clone accounts have become a very serious threat to online social network users. So, a detection method has been proposed in this project which can detect both Fake and Clone Twitter accounts.

This project helps the people to distinguish between clone and real profiles and also helps in identifying fake accounts on Twitter by detecting them.

By detecting these malicious Twitter accounts, the threats being caused to the Online Social Network (OSN) users can be prevented. The harm being caused to the identity of the genuine users by the creation of clone profiles can also be prevented by detecting them.

## REFERENCES

- [1] Piotr Bródka, Mateusz Sobas and Henric Johnson, “Profile Cloning Detection in Social Networks”, European Network Intelligence Conference, 2014.
- [2] Supraja Gurajala, Joshua S. White, Brian Hudson and Jeanna N. Matthews “Fake twitter accounts: profile characteristics obtained using an activity-based pattern detection approach”, International Conference on Social Media & Society, ACM 2015.
- [3] Ahmed El Azab, Amira M Idrees, Mahmoud A Mahmoud, Hesham Hefny, “Fake Account Detection in Twitter Based on Minimum Weighted Feature set”, World Academy of Science, Engineering and Technology, International Journal of Computer and Information Engineering Vol:10, 2016.
- [4] Arpitha D, Shrilakshmi Prasad, Prakruthi S, Raghuram A S, “PYTHON BASED MACHINE LEARNING FOR PROFILE MATCHING”, International Research Journal of Engineering and Technology (IRJET), Volume: 05 Issue: 03, 2018.
- [5] Sowmya P and Madhumita Chatterjee, “Detection of Fake and Clone accounts in Twitter using Classification and Distance Measure Algorithms”, International Conference on Communication and Signal Processing (India), 2020.

## **APPENDIX-I**

### **CSI PUBLISHED PAPER COPY**

<https://mail.google.com/mail/u/1/?tab=wm&ogbl#sent/QgrcJHsNjBgzRHFCRBVqgDxjtIVMrtjCkRl?projector=1&messagePartId=0.1>

The CSI Published Paper Copy is attached behind.

# Detection of Fake and Clone Accounts on Twitter

Kavitha S  
Computer Science  
(of Affiliation)  
K S Institute of Technology  
(of Affiliation)  
Bangalore, India  
[svdkavitha99@gmail.com](mailto:svdkavitha99@gmail.com)

Rajashree Shivakumar  
Computer Science  
(of Affiliation)  
K S Institute of Technology  
(of Affiliation)  
Bangalore, India  
[rajashreesgowda1001@gmail.com](mailto:rajashreesgowda1001@gmail.com)

Sharanya H  
Computer Science  
(of Affiliation)  
K S Institute of Technology  
(of Affiliation)  
Bangalore, India  
[sharanya.harish@gmail.com](mailto:sharanya.harish@gmail.com)

Kruthika B M  
Computer Science  
(of Affiliation)  
K S Institute of Technology  
(of Affiliation)  
Bangalore, India  
[kruthikruthikabm@gmail.com](mailto:kruthikruthikabm@gmail.com)

Dr. Deepa S R  
Computer Science  
(of Affiliation)  
K S Institute of Technology  
(of Affiliation)  
Bangalore, India  
[deepasr@ksit.edu.in](mailto:deepasr@ksit.edu.in)

**Abstract**— Today, Online Social Network (OSN) has become an integral part of many people's lives. Many activities such as communication, promotion, advertisement, news, agenda creation are done through online social networks. But, some malicious accounts on social networking sites are creating dangerous security problems to the genuine users. Twitter is one such social networking service which is popular among the social network users but also has fake and clone accounts which is a threat to the users. Cloning of user profiles is one serious threat, where duplicate profiles of already existing users are created and then is misused for damaging the identity of the original profile owner. Fake account creation is the creation of an account in the name of a person or a company which does not really exist on social media, to carry out malicious activities. Therefore detection of such malicious accounts is very much necessary.

**Keywords**—component, formatting, style, styling, insert (key words)

## I. INTRODUCTION

Social networking phenomenon has grown extremely since the last twenty years. During this rise, online social networks like Facebook, Twitter, Instagram, LinkedIn, etc., have created many online activities which instantly attract the interests of large number of users. On the other hand, they also suffer from the increase in the number of fake and clone accounts.

Online Social Network (OSN) users share a lot of information in the network like photos, videos, personal details, career details etc. This information if put into the hands of attackers, the after effects are very severe. Most of the OSN users are unaware of the security threats that exist in the social networks and easily fall prey to these attacks.

Fake account creation is the creation of an account in the name of a person or a company which does not really exist on social media, to carry out malicious activities. In fake accounts people usually lie about their age, gender and also use profile pictures taken from the internet in order to hide their identity. Fake accounts can present fake news, misleading web rating and spam. They act in a prohibited manner such as attempting to deceive or mislead people by

posting harmful links and aggressive following behaviors can also be found in such accounts like mass following etc.

Cloning of user profiles is one serious threat, where duplicate profiles of already existing users are created and then is misused for damaging the identity of the original profile owner. There are two types of Profile Cloning namely - Same Site and Cross Site Profile Cloning. If user credentials are taken from one Network to create a clone profile in same Network then it is called Same Site profile cloning. In Cross Site profile cloning, attacker takes the user information from one Network to create a duplicate profile in other Network in which the user is not having any account.

As the registration process in social networks has become very simple in order to attract more and more users, the creation of fake and clone accounts are also increasing in an alarming rate. In most of the fake and clone accounts, people lie on their age, gender, which place they belong to, current location etc.

According to the importance of the effect of social media to the society, this project aims at detecting the fake and clone profile accounts on Twitter to prevent the problems caused by these accounts to the genuine users. In this paper, a detection method will be proposed which can detect Fake and Clone accounts on Twitter.

## II. LITERATURE SURVEY

Nowadays, Fake and Clone accounts have become a very serious issue in online social networks. So, a detection method is very much necessary in order to overcome the problems caused by the frauds that create these fake and clone accounts which is also a threat to the genuine users. Many authors have worked in this area and have proposed various methods to identify these types of profiles in social networks. Some of these methods are discussed below.

Georgios Kontaxis, Iasonas Polakis, Sotiris Ioannidis and Evangelos P Markatos have proposed a prototype to check whether the users have become victim to cloning attack or not. Information is extracted from user profile and a search is made in OSN to find profiles which match to that of user

profile and a similarity score is calculated based on commonality of attribute values. If the similarity score is above the threshold value then the particular profile is termed as clone.

Piotr Brodka, Mateusz Sobas and Henric Johnson in their paper have proposed two novel methods for detecting cloned profiles. The first method is based on the similarity of attribute values from original and cloned profiles and the second method is based on the network relationships. A person who doubts that his profile has been cloned will be chosen as a victim. Then treating name as primary key, a search is made for profiles with the same name as that of victim, using query search. Potential clone (Pc) and the Victim profile (Pv) are compared and similarity  $S$  is calculated. If  $S(Pc, Pv) > \text{Threshold}$ , then profile is suspected to be a clone. In the verification step, the user does it manually as he knows which one is the original profile and which is the duplicate one.

Stephano Cresci, Di Pietro R, Petrocchi M, Spognardi A, Tesconi M, in their paper have reviewed some of the most relevant existing features and rules (proposed by Academia and Media) for fake Twitter accounts detection. They have used these rules and features to train a set of machine learning classifiers. Then they have come up with Class A classifier which can effectively classify original and fake accounts.

Ahmed El Azab, Amira M Idrees, Mahmoud A Mahmoud, Hesham Hefny, have proposed a classification method for detecting fake accounts on Twitter. They have collected some effective features for the detection process from different research and have filtered and weighted them in first stage. Various experiments are conducted to get minimum set of attributes which gives accurate results. From 22 attributes, only seven attributes were selected which can effectively detect fake accounts and have applied these factors on classification techniques. A comparison of the classification techniques based on results is made and the one which provides most accurate result is selected.

### III. METHODOLOGY

First, all the previous data, which was collected to find fake accounts created by bots or cyborg accounts will be cleared in order to find those accounts which are created by humans. It is found that almost all fake, clone and real accounts have their profile pictures and names in their profile.

In most of the fake and clone accounts, people lie on their ages for instance, mostly people set the age as 18-19 so that they make their account eligible for creation, people also lie about their gender, the images are also mostly downloaded from internet and some accounts have image of a character of different gender as set in their gender section by them. Hence, it is not possible to distinguish between fake and genuine accounts just by looking at the profiles.

Existing datasets will be used for the experiments. User information will be extracted from the user profiles through the API's provided in the dataset. Later based on the tweets,

number of followers and other activities of the users the fake and clone accounts will be detected.

Using the extracted user information, fake accounts will be detected based on a set of rules. Fake and genuine accounts will be classified using Naïve Bayes algorithm.

For clone account detection, profiles which are similar to that of the other user profiles will be searched and information will be extracted. Later, using Random Forest algorithm, the accounts will be classified into clone or normal accounts.

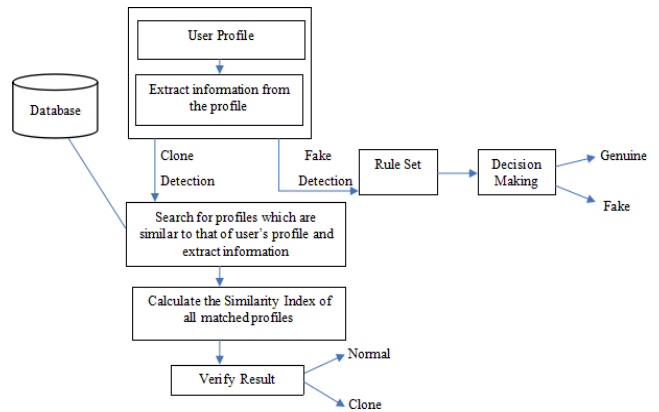


Fig 1: Workflow

### IV. CONCLUSION

Fake and clone accounts have become a very serious threat to online social network users. So, a detection method has been proposed which can find both fake and clone Twitter accounts.

In the previously carried out experiments, for fake account detection, a set of rules were used along with a set of machine learning classifiers which when applied would classify fake and genuine profiles. Clone account detection was carried out using Similarity Measures and C4.5 algorithm and a comparison was made to check the performance. Clone detection using Similarity Measures worked more efficiently than C4.5 algorithm and was able to detect most of the clones which were fed into the system.

In the previous work only the profile attributes were considered for fake and clone accounts detection. In future, this work can be extended by taking tweets and also other activities into consideration in order to increase the accuracy of the detection system.

### V. REFERENCES

- [1] Mauro Conti, Radha Poovendran and Marco Secchiero, "FakeBook: Detecting Fake Profiles in On-line Social Networks", 2012 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining.
- [2] Georgios Kontaxis, Iasonas Polakis, Sotiris Ioannidis and Evangelos P. Markatos, "Detecting Social Network Profile Cloning", 2013

- [3] Piotr Bródka, Mateusz Sobas and Henric Johnson, "Profile Cloning Detection in Social Networks", 2014 European Network Intelligence Conference.
- [4] B. Hudson, "Fake twitter accounts: profile characteristics obtained using an activity-based pattern detection approach", International Conference on Social Media & Society, ACM 2015.
- [5] Ahmed El Azab, Amira M Idrees, Mahmoud A Mahmoud, Hesham Hefny, "Fake Account Detection in Twitter Based on Minimum Weighted Feature set", World Academy of Science, Engineering and Technology, International Journal of Computer and Information Engineering Vol:10, 2016.
- [6] Buket Erşahin, Ozlem Aktaş, Deniz Kiliç, Ceyhan Akyol, "Twitter fake account detection", 2017 International Conference on Computer Science and Engineering (UBMK).
- [7] Sowmya P and Madhumita Chatterjee, "Detection of Fake and Cloned Profiles in Online Social Networks", Proceedings 2019: Conference on Technologies for Future Cities (CTFC).

## **APPENDIX-II**

### **CERTIFICATES OF PAPER PRESENTED**

The Certificates of Paper Presentation is attached behind.



Department of Computer Science and Engineering

## 34<sup>TH</sup> CSI KARNATAKA STATE STUDENT CONVENTION

THEME: SELF-RELIANCE AND AUTOMATION

## CERTIFICATE OF PARTICIPATION

This is to certify that Mr./Ms.

**Kavitha S**

from K S Institute of Technology college


has participated and presented a paper entitled

**Detection of Fake and Clone Accounts on Twitter**

in the domain Android and Web Technologies and Security Systems

in 34<sup>th</sup> CSI Karnataka State Student Convention

Jointly organized by Computer Society of India, Region V,  
Bangalore Chapter and Department of Computer Science and Engineering  
at K. S. Institute of Technology, Bangalore on 22<sup>nd</sup> and 23<sup>rd</sup> December, 2020.



**Dr. Nalini N**  
Chairperson  
CSI-BC



**Mrs. Anitha Venkatesh**  
State Student Coordinator  
CSI



**Prof. K. Venkata Rao**  
Event Convener  
Dept. of CSE



**Dr. Rekha B Venkatapur**  
Head of the Department  
Dept. of CSE



**Dr. K. V. A. Balaji**  
Principal/CEO  
K. S. I. T

Sponsored by:





Department of Computer Science and Engineering

**34<sup>TH</sup> CSI KARNATAKA STATE STUDENT CONVENTION**

**THEME: SELF-RELIANCE AND AUTOMATION**

**CERTIFICATE OF PARTICIPATION**

This is to certify that Mr./Ms.

**Rajashree Shivakumar**

from K S Institute of Technology college


has participated and presented a paper entitled

**Detection of Fake and Clone Accounts on Twitter**

in the domain Android and Web Technologies and Security Systems

in 34<sup>th</sup> CSI Karnataka State Student Convention

Jointly organized by Computer Society of India, Region V,  
Bangalore Chapter and Department of Computer Science and Engineering  
at K. S. Institute of Technology, Bangalore on 22<sup>nd</sup> and 23<sup>rd</sup> December, 2020.



**Dr. Nalini N**  
Chairperson  
CSI-BC



**Mrs. Anitha Venkatesh**  
State Student Coordinator  
CSI



**Prof. K. Venkata Rao**  
Event Convener  
Dept. of CSE



**Dr. Rekha B Venkatapur**  
Head of the Department  
Dept. of CSE



**Dr. K. V. A. Balaji**  
Principal/CEO  
K. S. I. T

Sponsored by:



Department of Computer Science and Engineering

## 34<sup>TH</sup> CSI KARNATAKA STATE STUDENT CONVENTION

THEME: SELF-RELIANCE AND AUTOMATION

## CERTIFICATE OF PARTICIPATION

This is to certify that Mr./Ms.

**Sharanya H**

from K S Institute of Technology college

has participated and presented a paper entitled

***Detection of Fake and Clone Accounts on Twitter***

in the domain Android and Web Technologies and Security Systems

in 34<sup>th</sup> CSI Karnataka State Student Convention

Jointly organized by Computer Society of India, Region V,  
Bangalore Chapter and Department of Computer Science and Engineering  
at K. S. Institute of Technology, Bangalore on 22<sup>nd</sup> and 23<sup>rd</sup> December, 2020.



Dr. Nalini N  
Chairperson  
CSI-BC



Mrs. Anitha Venkatesh  
State Student Coordinator  
CSI



Prof. K. Venkata Rao  
Event Convener  
Dept. of CSE



Dr. Rekha B Venkatapur  
Head of the Department  
Dept. of CSE



Dr. K. V. A. Balaji  
Principal/CEO  
K. S. I. T

Sponsored by:





Department of Computer Science and Engineering

## 34<sup>TH</sup> CSI KARNATAKA STATE STUDENT CONVENTION

THEME: SELF-RELIANCE AND AUTOMATION

## CERTIFICATE OF PARTICIPATION

This is to certify that Mr./Ms.

**Kruthika B M**

from K S Institute of Technology college


has participated and presented a paper entitled

***Detection of Fake and Clone Accounts on Twitter***

in the domain Android and Web Technologies and Security Systems

in 34<sup>th</sup> CSI Karnataka State Student Convention

Jointly organized by Computer Society of India, Region V,  
Bangalore Chapter and Department of Computer Science and Engineering  
at K. S. Institute of Technology, Bangalore on 22<sup>nd</sup> and 23<sup>rd</sup> December, 2020.



Dr. Nalini N  
Chairperson  
CSI-BC



Mrs. Anitha Venkatesh  
State Student Coordinator  
CSI



Prof. K. Venkata Rao  
Event Convener  
Dept. of CSE



Dr. Rekha B Venkatapur  
Head of the Department  
Dept. of CSE



Dr. K. V. A. Balaji  
Principal/CEO  
K. S. I. T

Sponsored by:

