A MULTI-PERSPECTIVE APPROACH UTILIZING SUPERVISED MACHINE LEARNING ALGORITHMS FOR EFFECTIVE SOCIAL MEDIA BOT DETECTION

BY

Abu Saleh Muin Talukder
ID: 201-15-3054

FINAL YEAR DESIGN PROJECT REPORT

This Report Presented in Partial Fulfillment of the Requirements for the Degree of Bachelor of Science in Computer Science and Engineering

Supervised By

Dr. Md. Fokhray Hossain
Professor
Department of CSE
Daffodil International University

DAFFODIL INTERNATIONAL UNIVERSITY

DHAKA, BANGLADESH

JULY 2024

APPROVAL

This Project titled "A Multi-Perspective Approach Utilizing Supervised Machine Learning Algorithms for Effective Social Media Bot Detection", submitted by Abu Saleho Muin Talukder to the Department of Computer Science and Engineering, Daffodil International University, has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of B.Sc. in Computer Science and Engineering and approved as to its style and contents. The presentation has held on 15-07-2024

BOARD OF EXAMINERS

Dr. Md. Taimur Ahad (MTA) — **Chairman**
Associate Professor & Associate Head
Department of CSE, DIU
Faculty of Science & Information Technology
Daffodil International University

Shayla Sharmin

Ms. Shayla Sharmin (SS) — **Internal Examiner 1**
Sr. Lecturer
Department of CSE, DIU
Faculty of Science & Information Technology
Daffodil International University

Mr. Mayen Uddin Mojumdar (MUM) — **Internal Examiner 2**
Sr. Lecturer
Department of CSE, DIU
Faculty of Science & Information Technology
Daffodil International University

Dr. Md. Manowarul Islam — **External Examiner**
Associate Professor
Department of Computer Science and Engineering
Jagannath University

©Daffodil International University, Bangladesh i

DECLARATION

We hereby declare that, this project has been done by us under the supervision of **Dr. Md. Fokhray Hossain, Professor, Department of CSE** Daffodil International University. We further affirm that neither this project nor any part of this project has been submitted anywhere for the provision of any degree.

Supervised by:

Hossain

Dr. Md. Fokhray Hossain
Professor
Department of CSE
Daffodil International University

Submitted by:

Abu Saleho Muin Talukder

Abu Saleho Muin Talukder
ID: 201-15-3054
Department of CSE
Daffodil International University

©Daffodil International University, Bangladesh ii

ACKNOWLEDGEMENT

First we express our heartiest thanks and gratefulness to almighty **Allah** for His divine blessing makes us possible to complete the final year project successfully.

I really grateful and wish our profound our indebtedness to **Dr. Md. Fokhray Hossain**, **Professor**, Department of CSE Daffodil International University, Dhaka. Deep Knowledge & keen interest of our supervisor in the field of "*Supervised Machine Learning*" to carry out this project. His endless patience ,scholarly guidance ,continual encouragement , constant and energetic supervision, constructive criticism , valuable advice ,reading many inferior draft and correcting them at all stage have made it possible to complete this project.

I would like to express our heartiest gratitude to **Dr. Sheak Rashed Haider Noori, Professor and Head of the Department of CSE,** for his kind help to finish our project and also to other faculty member and the staff of CSE department of Daffodil International University.

I would like to thank our entire course mate in Daffodil International University, who took part in this discuss while completing the course work.

Finally, I must acknowledge with due respect the constant support and patients of our parents.

ABSTRACT

This research presents a comprehensive exploration of social media bot detection, focusing on Instagram, Twitter, and TikTok platforms. Social bots are autonomous machines that create for social media platforms. In this work present supervised machine learning algorithms, including models Random Forest, XGBoost, KNN, Decision Tree, and Neural Network, I am conducted an extensive analysis of bot behavior. Collect all public available datasets of labeled human and bot accounts. And through this study we have analyzed the behavioral activities of different bots accounts. The study aimed to understand the impact of multiple bot accounts, enhance accuracy through multi-account analysis, and deploy supervised machine learning technologies for improved platform security. In this research evaluated algorithms performance using key metrics such as accuracy, precision, recall, and F1-score, considering platform-specific challenges. Random Forest and XGBoost three-type accounts are consistently robust performers. Random Forest Instagram accuracy is 95%, Twitter accuracy is 91%, and TikTok accuracy is 97%, with the highest prediction accuracy. XGBoost Instagram accuracy is 95%, Twitter accuracy is 90%, and TikTok accuracy is 97%. All models achieve high accuracy, emphasizing the effectiveness of bot detection algorithms on the TikTok social media platform. The Neural Network maintains stable results with a balanced precision-recall trade-off, showing flexibility. Overall, the study provides valuable knowledge about social media bot detection, highlighting Random Forest and XGBoost as reliable choices. It gives strong user privacy and data security and opens the way for future research, inspiring exploration into ensemble approaches and advanced techniques.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF FIGURES

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS

ML	Machine Learning
SL	Supervised Learning
API	Application Programming Interface
GPU	Graphics Processing Unit
KNN	K-Nearest Neighbors
RF	Random Forest
DT	Decision Tree
NN	Neural Network
XGBoost	eXtreme Gradient Boosting
SQL	Structured Query Language
SSL	Secure Sockets Layer
TPU	Tensor Processing Unit

CHAPTER 1

Introduction

1.1 Overview

In today's digital age, social media has seamlessly integrated into our daily lives, providing users with the opportunity to connect with new people, stay in touch with friends, and network professionally. Platforms like Instagram, TikTok, and Twitter serve distinct purposes, catering to various user segments with unique value propositions. Twitter, as a prominent microblogging platform, excels in delivering rapid updates and breaking news. Instagram, on the other hand, is predominantly utilized by celebrities and businesses for effective marketing, while TikTok fosters creativity and engagement through short-form videos set to music. The pervasive influence of social media in the contemporary digital era has made communication, information dissemination, and societal connectivity more accessible. However, this field work influence not without challenges. The rise of automated accounts, commonly known as bots, has cast a shadow on the authenticity and reliability of these platforms. This research aims to address this issue by delving into the detection and analysis of bots and human users across major social media platforms—Twitter, TikTok, and Instagram using supervised machine learning techniques. Our exploration hinges on a comprehensive database that has undergone a meticulous supervised labeling process to differentiate between bots and non-bots based on specific criteria. This labeled data forms the foundation for training and testing machine learning models, ensuring a high level of accuracy in subsequent analyses. The study employs five distinct machine learning algorithms, tailored to the unique challenges posed by social media bot detection. The primary goal of this research is to develop an automated system capable of identifying and eliminating bots on social media networks. This involves leveraging supervised machine learning technology and a bot detection method to enhance platform security and protect users. Despite advancements, the existing solution faces challenges, including difficulties in verifying account information and the inadvertent removal of legitimate account holders in large numbers, compromising the precision and authenticity of information reaching users. This multiple-account data analysis detection can be Social network helpful for various purposes.

1.2 Background and Present State

In recent years, the landscape of social media has evolved dramatically, with platforms like Instagram, TikTok, and Twitter playing pivotal roles in global communication and digital marketing strategies. Each platform caters to diverse user demographics and offers unique engagement opportunities, from real-time updates on Twitter to creative video content on TikTok and visual storytelling on Instagram. However, alongside these opportunities, the proliferation of automated accounts, commonly known as bots, has presented significant challenges. Bots can manipulate engagement metrics, spread misinformation, and compromise the authenticity of user interactions. This phenomenon has underscored the urgent need for robust bot detection mechanisms across social media platforms. Our research focuses on analyzing current trends in bot detection methodologies, particularly through the lens of supervised machine learning techniques. We have curated a comprehensive dataset meticulously labeled to differentiate between bots and genuine users based on specific behavioral patterns and account characteristics. Using this dataset, we have implemented and evaluated several machine learning algorithms tailored for bot detection across major platforms. Our approach not only aims to enhance the accuracy of identifying bots but also to address the complexities associated with distinguishing between legitimate and malicious automated accounts. Despite significant advancements, challenges persist. Verifying account information accurately and minimizing the inadvertent removal of legitimate users remain critical areas of concern. These challenges highlight the ongoing need for refining detection strategies and developing adaptive solutions that can keep pace with evolving bot tactics. By contributing to the refinement of bot detection technologies, our research aims to bolster the security and integrity of social media platforms. We seek to empower platform administrators with tools capable of effectively mitigating bot-driven threats, thereby preserving user trust and fostering a more authentic digital environment.

1.3 Problem Statement

The research aim is to address the increasing challenges that have been created by the spread of bot activity on popular social media sites like Instagram, TikTok, and Twitter. Detecting and mitigating the impact of bots is a critical challenge for social media platforms. This is because bots often mimic human behavior, making them difficult to identify. The problem of limited access to info. Large organizations that control social networks have almost limitless data access.

Governments, other private enterprises, and regular users, on the other hand, are constrained by the quantity of API calls made by social networks. As a result, they are unable to employ massive amounts of data required for bot identification. Problem with low-quality training datasets. Datasets for training and testing bot detection tools are often created by a subjective expert using analytical methodologies. Thus, the created bot detection methods share the opinion of the bot tagging from datasets. Bot activity can sway public opinion during elections, artificially inflate the popularity of products or candidates, and disrupt financial markets. Other Literature Review To understand so many problems with this platform, like how to improve accuracy and multiple accounts, etc., do something more in social media platform. Bot creators constantly develop new techniques to evade detection, so machine learning five models can use better understanding and be improved. challenges to solving Accuracy vs. false-positives Achieving high accuracy in bot detection is crucial; minimizing the risk of mistakenly identifying legitimate users as bots is equally important.

My research can compare and assess the effectiveness of seven different algorithms, identifying their strengths and weaknesses, and potentially leading to the development of a more accurate and robust model. Examining the challenges faced by other researchers can help address them in my work and contribute to the overall advancement of bot detection solutions. Identifying and resolving issues with the constraints of the current solutions, Difficulties authenticating account information and the unintentional removal of authorized users.

1.4 Objectives

- I will be conducting an extensive test of the impact of multiple bot accounts on Twitter, TikTok, and Instagram.
- To create a robust bot detection system, despite the wide variety of user behaviors.
- The implementation of machine learning and advanced bot detection techniques will enhance (Social media) platform security and user safety.

1.5 Scope and Limitations

The research aims to analyze and mitigate the impact of bot activity on Twitter, TikTok, and Instagram by developing and evaluating five supervised machine learning models for bot detection. The scope includes conducting extensive tests to assess the influence of multiple bot accounts on platform dynamics and user interactions, implementing and evaluating five supervised machine learning algorithms to identify and classify bots based on behavioral patterns and account characteristics, contributing to the development of a robust bot detection system, and addressing challenges such as improving accuracy in bot detection while minimizing false positives. However, the research faces several limitations, including data access constraints, the quality of training data, the dynamic nature of bot tactics, generalizability, and ethical considerations. Access to comprehensive datasets for training and testing is limited due to privacy concerns and social media platform restrictions. The findings and methodologies may vary across different platforms and may require adaptation for specific contexts or emerging bot behaviors. By acknowledging these limitations and addressing them transparently, the research aims to contribute responsibly to the field of bot detection on social media platforms, striving for advancements that enhance platform security and user trust.

1.6 Report Organization

Presenting an easy way to focus show information and more.

- Chapter 1: This section introduces the topic, provides background information, defines the problem, states objectives, and outlines the report's structure, scope, and key points.
- Chapter 2: Summarizes existing research, highlights differences and gaps, identifies unresolved questions, and summarizes key takeaways.
- Chapter 3: Describes research methods, lists necessary components, discusses project timeline and finances, and summarizes key methodology aspects.
- Chapter 4: Focuses on the plan's execution, details model training, explains system testing and evaluation, and summarizes key findings.
- Chapter 5: Presents experimental results, analyzes performance, compares findings to objectives, and summarizes key results and their significance.
- Chapter 6: Discusses project impacts on life, society, and the environment, addresses ethical considerations, outlines sustainable practices, and summarizes broader impacts.
- Chapter 7: Restates main findings, acknowledges study limitations, suggests areas for further research, and summarizes key conclusions.

1.7 Summary

By identifying social media bots, my research has charted a path toward increased platform security and user trust across major platforms—Twitter, TikTok, and Instagram. I began this journey with a nuanced examination of the challenges posed by automated accounts, or bots that disrupt the authenticity of online interactions. Overarching goal is to develop an automated system that uses advanced machine learning techniques to detect and eliminate bots, contributing to a more secure and genuine online environment.

CHAPTER 2

Literature Review

2.1 Overview

In this study of bots on social media platforms like Twitter, Instagram, and TikTok has raised concerns about user experience, security, and information dissemination. This research project aims to address these challenges using supervised machine learning algorithms. By other research paper experiment supervised ML detection bot impact on diverse platforms, the project aims to understand the nuances and variations in bot behavior, addressing the growing concern about the potential adverse effects on user safety, platform integrity, and public discourse.

2.2 Literature review

Mohammad, S., Khan, M. U.*et al*. This paper on bot detection is basically neural network-based work and identifies accounts. Detection methodologies utilize the features of the accounts to label them as either bots or humans. This work in convolutional neural networks (CNN) and artificial neural networks (ANN) best compares results. For this study, the accuracy of this model when compared base-two is good. Data account features profile posting the tweets social media are the input to the model. But this combined model performs better, but not on multiple platforms. Instead of using only a single social media post, the future requires more multiple preprocessing as compared to the best output [1].

Gannarapu, S., Dawoud, A.*et al*. This paper is about improving detection and accuracy. The main purpose of this paper is to introduce an automatic mechanism for the detection and removal of bots that exist on social media platforms. Just remove related information and non-genuine account data that are posted on social media. This research uses a bot detection technique based on machine learning algorithms. Data collection and web development facilitate bot detection in social media networks and data-supervised classification and one-class classifiers. The study distinguishes validation, evaluates model accuracy, and confirms system precision. This study enhances prediction quality, eliminates undesired data, and speeds bot detection [2].

Singh, A. P.*et el*. This research-force spam detection system on social sites is designed to detect spammers by using a machine learning approach. Data collected from the H-Spam 14 site and different pre-processing schemes convert the research base. Data values were extracted to create the feature set Artificial Bee Colony (ABC) and this optimization algorithm. Then, the classification process performed using an Artificial neural network (ANN) distinguishes between spam and non-spam data and ends with a Naïve Bayes and SVM performance comparison. But this work can be extended by using other social media datasets [3].

Ümmü, T. U. N. Ç.*et al*. This aim classify Instagram user profiles into fake, bot, and real accounts with classification algorithms. Datasets on some site publicly available data accounts detection on Instagram and collection online circle of friend and other account websites and mobile applications. But not collection web scraping. There are seven classifiers that train models profile detection, and data labeled to train machine learning algorithms that accurately predict base outcomes. This study, there is a limitation that should be addressed. But only one site works in the study, Complete Instagram, not work multiple accounts on social media [4].

Alzahrani, S., Gore, C.*et al*. In this paper, Develop and experiment with network-based, behavioral and automatic identification, temporal and spatial characteristics in accounts, and identify features useful in detecting organizational accounts. Data is collected from different types of microblogs and labeled individuals accounts. Different types Features experimented with using linear and non-linear classifiers and using content and language-independent. But this research paper not multiple social media accounts use and only a single social media account is analyzed, and no other algorithms are used for automatic identification [5].

Loyola-González, O., Monroy, R.*et al*. In this context, achieving high detection accuracy is not the sole desired attribute. The research has certain limitations, such as the bots being confined to specific sets of patterns, and the investigation focusing solely on one type of events. The amount of data used for training, as well as the effectiveness of data classification and the practical implementation of machine learning, pose significant challenges. Addressing the accuracy of the dataset is also a noteworthy limitation that requires resolution. The analysis involves motive detection and network visualization of features. Uses a group of regular bot accounts and examines differences in the gathered characteristics to explore methods for creating automated responses [6].

Yang, K. C., Varol, O.*et al*. This paper introduces a framework that utilizes minimal account metadata to efficiently analyze the complete flow of public tweets. To ensure the accuracy of the model, we create a diverse set of labeled datasets for training and validation. Rather than training exhaustively on all available data, focusing on specific training data enhances model accuracy and generalization. Bot detection methods, employing various models that incorporate metadata, aim to accurately identify different types of bots. However, limited access to social media data hinders the recognition of bots, leaving individuals susceptible to manipulation. The analysis of streaming data, including computing resources and behaviors like retweeting, can only identify specific bot types. It is essential to note that this paper specifically focuses on the analysis of one type of social media data and does not cover various account types on social media. The study highlights the potential of data selection as a promising approach to address issues related to noisy training data [7].

Davis, C. A.*et al*. The article addresses the widespread problem of social bots on digital platforms and their ability to imitate human behavior for a variety of objectives, such as disseminating false information and radical propaganda. Researchers have developed a publicly accessible tool called BotOrNot to address this issue. It analyzes Twitter accounts for bot-like activity by utilizing more than a thousand variables. Over a million inquiries have been handled by BotOrNot since its 2014 start. The company offers a free evaluation service with the goal of facilitating social media research. Users may get reports on individual accounts via the website or using the API for numerous accounts, with the service removing the requirement for users to set up their own classifiers. The researchers provide prospective uses for BotOrNot in the social media community, such as browser extensions [8].

Cai, M.*et al*.In the context of social media, the literature investigates how bot users affect the spread of public opinion, especially in times of public health emergency. The research aims to better understand the behavioral traits and dissemination processes that differentiate bot users from human users. Classification algorithms, social network analysis, and deep learning techniques (Top2Vec and BERT) are used in this study to examine the variations in user behavior and information sharing with the focus on public health situations. The findings are intended to improve online order maintenance and emergency management by directing public attention, highlighting subject changing, and encouraging good feelings in social networks [9].

Varol, O.*et al*. The research looks into the rise of social bots on Twitter and proposes a rigorous methodology for detecting them. The study achieves excellent accuracy in identifying different sorts of bots by utilizing over a thousand factors, such as tweet content, user data, and network behaviors. It's estimated that between 9% and 15% of Twitter accounts that are currently active are automated. The study delves into interaction patterns, content flows, and account subclasses, offering light on the various behaviors displayed by both human and bot users. The study acknowledges how simple it is for accounts managed by automated or hybrid techniques to post content and communicate on social media. The main goal is to recognize and categorize these bots, which will lay the groundwork for comprehending the communication patterns across various social media entities [10].

Madahali, L.*et al*. Benford's Law is a statistical theory that reveals the non-uniform distribution of initial digits in natural systems. It has applications in forensic accounting, the stock market, survey data analysis, and natural sciences. The law's application entails spotting variations in the distribution of digits that might indicate possible fraudulent activity. This study examines if Benford's Law applies to information operations (IO) and bots. The study's findings suggest that bots don't follow the normal distribution, which might make them a useful tool for identifying fraudulent internet identities. Inconsistencies in IO operations' adherence to the law, however, highlight the necessity of closely examining both typical and unusual online activity in order to stop the spread of harmful information on social media [11].

Shen, F.*er al*. This study looks at Twitter conversations around the Russia-Ukraine conflict, focusing on the differences between bot and non-bot accounts. Using the Twitter API and the phrases "Russia" and "Ukraine," the researchers gathered a sizable dataset between February 17 and March 18. The collection had about 3.7 million tweets from nearly one million different users. The investigation, which was performed on 1% of the data using interval sampling for bot identification, indicated that 13.4% of the accounts were social media bots, accounting for 16.7% of the tweets. Using account analysis, textual analysis, and interaction analysis, the study investigated differences between bots and non-bots in the context of the Russia-Ukraine War. According to the results, there were bots on both sides; Russian bots communicated more effectively, while Ukrainian bots were louder. Although the discrepancies seemed to be less pronounced than in prior studies, the study did find parallels and variances in the behavior of online interactions [12].

Steel, B., Parker, S.*et al*. This paper gives a complete dataset from TikTok that includes video descriptions, comments, and user statistics, with a focus on the 2022 invasion of Ukraine. This incident exposed previously unrecognized political processes and behaviors on TikTok, propelling the platform into the geopolitical arena. Researchers studying language and interpersonal processes associated with these occurrences will find great value in the dataset, the authors stress. An assessment of bot identification on TikTok is presented in conjunction with an early investigation of language dynamics and social interactions. To encourage more study, both the collection library and the dataset are publicly available [13].

Yang, K. C. The supervised machine-learning strategy for detecting bots on social media platforms is investigated in the literature review. Using automated techniques like acquiring fictitious follower accounts or using honeypot accounts, the approach entails gathering labeled samples of accounts. For machine learning algorithms, the features of these samples, such as profile information, interaction patterns, content variety, temporal patterns, and network topologies, are measured. To distinguish between bot and human behavior, a variety of models are used, ranging from well-known ones like Random Forest to cutting-edge neural networks and natural language processing approaches. The paper also discusses the rise of social bots, how they could affect online discussions, and how useful detection tools are [14].

Xiao, C., Freeman, D.*et al*. The research investigates the frequency of false accounts in online social networks as well as the difficulties involved with recognizing and minimizing them. Fake accounts are widely employed by evil users for spam, scams, and other nefarious activities. The paper emphasizes the need for a quick and scalable method to identify and take action against these accounts to protect genuine network members and keep overall trustworthiness. The proposed approach includes a guided machine learning process meant to classify groups of fake accounts made by the same person. Key features for classification include data on user-generated text areas such as name, email address, and connections. The research applies this methodology to LinkedIn account data, demonstrating high performance in detecting fraudulent accounts and effectively identifying over 250,000 such accounts in production [15].

Boser, B. E., Guyon, I.*et al*. The literature provides a training technique aimed at optimizing the margin between training patterns and the decision border, which is applicable to a wide range of classification functions, including Perceptrons, polynomials, and Radial Basis Functions. The method adapts the effective number of parameters dynamically to meet the issue complexity, describing the answer as a linear combination of supporting patterns—those nearest to the decision boundary. We provide generalization performance limits using the leave-one-out approach and the VC-dimension. When compared to other learning methods, experimental findings on optical character recognition indicate excellent generalization [16].

Kalameyets, M..*et al*. This research presents novel machine learning algorithms for detecting and identifying dangerous bots in social networks. The key change lies in leveraging only the interaction patterns of friends linked with the studied accounts as the main data source for bot identification. The suggested methodologies provide various benefits, including the capacity to identify hidden bots behind privacy settings, detect camouflaged bots imitating actual users, identify bot groups, and assess the quality and price of a bot. The process entails building a social graph using a hierarchical social network model, extracting characteristics with statistical methods and graph algorithms, and applying decision-making models like random forests or neural networks. The paper confirms these algorithms via trials focusing on bot identification in the VKontakte social network, displaying remarkable efficiency and robustness against diverse forms of bots [17].

Aljabri, M., Zagrouba, R.*et al*. Online social networks provide a wealth of knowledge and an open atmosphere in the digital age. However, fraudsters use bots to imitate human behavior because of this openness. These bots are very dangerous to privacy because they do things like spamming, making fake profiles, sharing content, and more. The fact that these bots are always changing makes it hard for technologies to find them. This review of the literature gathers and analyzes contemporary Machine Learning (ML)-based algorithms for identifying and categorizing bots on key social media platforms (Facebook, Instagram, LinkedIn, Twitter, and Weibo). It goes into depth about datasets and feature groups for supervised, semi-supervised, and unstructured methods. The study also talks about problems, chances, and possible future research paths in the area [18].

Zhang, W., & Sun, H.*et al.* According to the research being looked at, the problem of spam and ads flooding Instagram, one of the top 15 social networks online, is getting worse. The widespread fame of Instagram has led to a pressing need for the development of an effective spam detection model to curb the growth of unwanted posts. The suggested method uses a feature-based approach and supervised learning techniques to successfully spot trash on Instagram. The authors utilize K-fold cross-validation to find the best pair of supervised learning models and related parameters. The stated precision of the best model stands at an amazing 96.27%. Additionally, the study presents a unique two-pass clustering method involving Minhash clustering and K-medoids clustering to group near-duplicate posts, marking them as either spam or normal. The feature extraction approach incorporates not just statistical data of user profiles and postings, but also information encoded in photographs, distinguishing it from past studies. The recovered feature vectors consist of four person biography features, one Colour Difference Histogram feature, and 23 media post features. [19].

Purba, K. R.*et al.* In the continually changing Instagram ecosystem, follower count is a vital measure that shapes the success story for influencers. However, the growth in follower-selling services has given rise to a widespread challenge – the invasion of fake follows. This surge not only affects the authenticity of influencers but also presents a significant financial risk for companies acting in brand endorsements. Recognizing the significance of distinguishing between real and false followers, this study makes use of supervised machine learning models. The dataset comprises fake users gathered from various sources and genuine users, combining 17 traits covering statistics, media information, activity, media tags, and media resemblance. Through thorough testing of five machine learning algorithms, the Random Forest algorithm appears as a top worker, getting an amazing accuracy rate of up to 91.76%. Crucially, the study finds five information factors, including post count and friend numbers, as crucial drivers for user classification. Descriptive data further underscore clear differences between fake and real users. This study carries clear consequences for company owners navigating the influencer marketing realm on Instagram, a site defined by its extensive media-sharing capabilities and crucial role in brand promotion. Looking forward, prospective additions include merging text, relation graph, and picture analysis to reinforce the identification of bogus users, given the platform's dynamic nature [20].

Rao, S., Verma, A.*et al*. The literature review covers the dynamic environment of Online Social Networks (OSNs) and addresses the widespread challenges posed by social spam, covering issues such as dividing emotions, degradation of information quality, and the impact on network resources. With the rise of planned automatic accounts and the emergence of Deepfakes driven by artificial intelligence, the study stresses the importance of understanding and fighting these threats. The study presents a detailed assessment of current improvements in social spam detection, encompassing dimensionality reduction methods, features employed, and a spectrum of machine learning and deep learning methodologies. Additionally, it dives into the world of Deepfake trash in text, picture, and video forms. The thorough study finds difficulties in detection systems, scaling, real-time datasets, and tactics employed by trolls, giving lessons for future research in the context of changing cyber dangers. This offers difficulties such as class mismatch, hostile strikes, and model scaling [21].

Van Der Walt, E.*et al*. The study focuses on identifying fraudulent identities on social media platforms, specifically those created by people for malevolent reasons. Using supervised machine learning models, the research aims to measure the transferability of traits from bot-focused studies to human-generated fake accounts. The study finds that previous features for bot identification perform sub optimally in predicting fake human accounts, highlighting the challenge of spotting sparse cases of human-generated fake accounts compared to common bot-generated ones. Future research should consider adding elements from social sciences, particularly psychology, to improve detection capabilities. [22].

Shao, C.*et al*. The research under review examines the widespread problem of digital misinformation, noting it as a major threat to political processes. In reaction to this challenge, scientists from various fields are studying the multiple reasons behind the rapid spread of lies, while online platforms are starting defenses. Despite this, the literature points out a lack of structured, data-driven proof to lead these efforts. The study addresses this gap by studying a vast collection of 14 million messages spreading 400 thousand stories on Twitter over ten months in 2016 and 2017. The main focus is on the role played by social bots in boosting and spreading material from low-credibility sources. The results suggest that handling social bots could be a promising approach to counter the spread of online lies, with possible implications for the wider field of social media platform security [23].

2.3 Comparison between existing works

The author utilizes research from various scholars and sources to combat social media bots, enhancing our understanding of bot detection across various platforms.

TABLE 2.3.1: COMPARATIVE ANALYSIS TABLE

SL No	Author Name	Used Algorithm	Best Accuracy with Algorithm
1.	Mohammad, S.et al [1]	ANN,Naïve Bayes,SVM	ANN = 99.14%
2.	Alzahrani, S. et al. [5]	Random forest, KNN, MLP, NB, SVM, DT	Random forest = 90.2%
3.	Aljabri, M. et al. [18]	KNN, RF, DT, NB, SVM	KNN = 89.23%,
4.	Varol, O.et al. [10]	Random Forest,Logistic Regression,k-NN	Random Forest = 92.00%
5.	Xiao, C.et al. [15]	Gradient Boosting,SVM,Neural Networks	Neural Networks = 95.00%
6.	Madahali, L.et al.[11]	Naive Bayes, Decision Tree, K-Nearest	Decision Tree = 79.23%
7.	Purba, K. R.et al.[20]	Logistic Regression,Naive Bayes,SVM,Random Forest	Logistic Regression = 91.76%
8.	Aljabri, M., Zagrouba, R.et al.[18]	Decision Tree, ANN, CNN, SVM	SVM = 89.81%
9.	Kalameyets, M.et al.[17]	Random Forest, Naive Bayes, Decision Tree	Decision Tree = 90.01%
10.	Rao, S., Verma, A.et al. [21]	Naive Bayes, Logistic Regression, XGboost, SVM	XGboost = 93.32%

2.4 Open Issues

The open issues of my research project encompasses examination of the challenges posed by social media bots on platforms such as Twitter, TikTok, and Instagram. By adjust insights from various research papers, we aim to address the multifaceted dimensions of the bot detection problem. Let's highlight the scope with references to the literature review:

The research acknowledges the rise of social bots on Twitter and proposes a rigorous methodology for detecting them. My project extends this scope by including platforms like TikTok and Instagram, recognizing the unique challenges posed by diverse social media ecosystems [10]. The study experiments with different classifiers, including linear and non-linear ones, to detect organizational accounts. My scope expands on this by incorporating five distinct machine learning algorithms (KNN, Random Forest, Decision Tree, XGBoost, Neural Network) for a comprehensive evaluation of their effectiveness across various platforms [5]. My project aligns with this scope by ensuring that datasets encompass a range of user behaviors, facilitating the training of robust machine learning models capable of capturing various bot manifestations [3]. The literature emphasizes the importance of implementing advanced bot detection techniques to improve platform security and user safety. My research project aligns with this scope by aiming to contribute to the development of more effective and accurate bot detection technologies, addressing the security concerns associated with the presence of bots [2]. The project aims to identify limitations in current solutions, similar to the study highlighting issues such as the bots being confined to specific sets of patterns. By recognizing and addressing these limitations, my research seeks to advance the understanding and applicability of bot detection models across a broader spectrum of user interactions [7].

2.5 Summary

A study on social media bot detection has identified various methodologies and models, including K-Nearest Neighbors (KNN), Random Forest, Decision Tree, XGBoost, and Neural Network, across Twitter, TikTok, and Instagram. The researchers acknowledge the challenges posed by social media bots and aim to develop a unified framework adaptable to diverse bot behaviors. The study also highlights the need for enriched feature sets and confined bot patterns, as well as sparse data for human-generated bots accounts. The study emphasizes the dynamic nature of the field and the ongoing commitment to advancing accuracy, efficiency, and ethical considerations in bot detection.

CHAPTER 3

Research Methodology

3.1 Overview

In this research project, we aim to address the pervasive issue of social media bot presence by proposing a comprehensive and innovative bot detection system. Focusing on Twitter, TikTok, and Instagram, our approach leverages a multi-perspective methodology and supervised machine learning algorithms to enhance accuracy. Multiple Account behavioral patterns, content characteristics, and network structures - research aim to build a highly accurate and robust bot detection system. The process of using supervised machine learning for social media bot detection involves several key steps, dataset is collected, and encompassing both bot and non-bot accounts of 2,797 Twitter users, 2,799 Instagram users, and 2,864 TikTok users. Data preprocessing is a crucial step in machine learning tasks, ensuring consistency and handling missing values. It includes normalizing data, encoding categorical variables, and removing duplicates. The data is divided into training and testing sets for effective evaluation. This research uses five different supervised machine learning methods for bot detection on social media platforms, each chosen for its strengths and applicability. The model's performance is tested on the testing dataset using measures including confusion matrix, accuracy, precision, recall, and F1 score. If needed, hyperparameters are changed or different methods are looked into to make the model more accurate. Divide into training, validation, and testing sets (20 split). Ensure stratification for class balance (ratio of bots to humans). Performance evaluation involves assessing accuracy, precision, recall, F1-score, and confusion matrix metrics, and comparing each model to identify strengths and weaknesses in bot detection algorithms. This process involves cleaning data, creating a function to check classifier performance, identifying attributes determining bot or non-bot accounts, creating a bot identification criteria, and randomly classifying the dataset into train and test sets. Different classification methods are applied, and the accuracy of each method is compared. The most relevant method is then selected for testing, and the best classifier is chosen for the final accuracy comparison. Acknowledging limits in existing solutions, such as difficulties in checking account information and mistaken removal of valid users, my study will fill these gaps.

3.2 Proposed Methodology

Specify social media platforms (Instagram, TikTok, Twitter, or others). Using Supervised Machine Learning (ML) methods to make a system for finding social media bots has several important steps, so I am Specify the social media and research based platforms collect data (Instagram, TikTok, Twitter, or others). Now, let's look context for a comprehensive exploration of the proposed Methodology, guiding subsequent sections that will delve into the intricacies of the model's workflow and methodologies and here below Process:

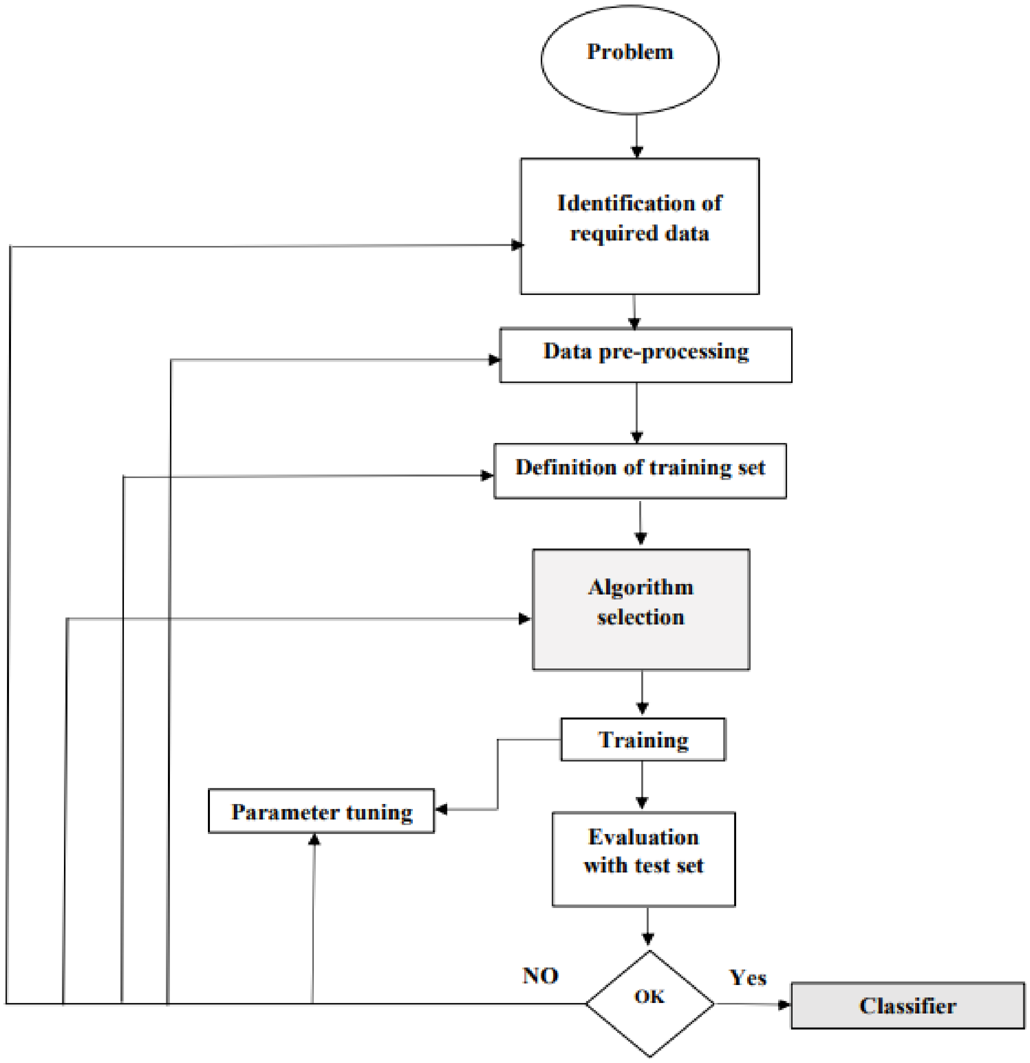

Figure 3.2.1: Propose of Methodology.

K-Nearest Neighbor (KNN):

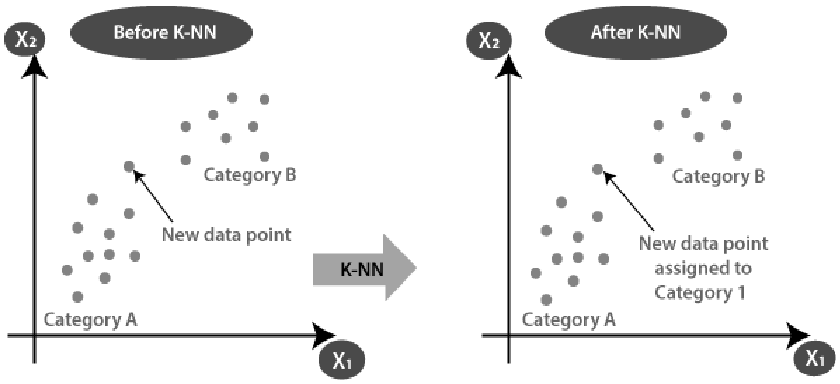

Figure 3.2.2: K-Nearest Neighbor (KNN) Schematic representation (Source-Google)

The K-Nearest Neighbor (KNN) algorithm plays a vital role in the proposed social media bot detection system. Here's a condensed overview: KNN is a supervised machine learning algorithm known for its simplicity and adaptability, making it suitable for social media bot detection. KNN is compatible with diverse data types and effectively learns from labeled datasets, considering relevant attributes for bot identification. The algorithm's simplicity, adaptability, and interpretability are advantageous, but challenges include computational intensity for large datasets and sensitivity to irrelevant features. Key metrics assess model effectiveness, and KNN integrates seamlessly into workflow.The integration of KNN brings simplicity, adaptability, and interpretability to the bot detection system, addressing the unique challenges posed by social media platforms. Subsequent design considerations will enhance the algorithm's implementation for optimal performance in identifying and mitigating social media bots.

Random Forest:

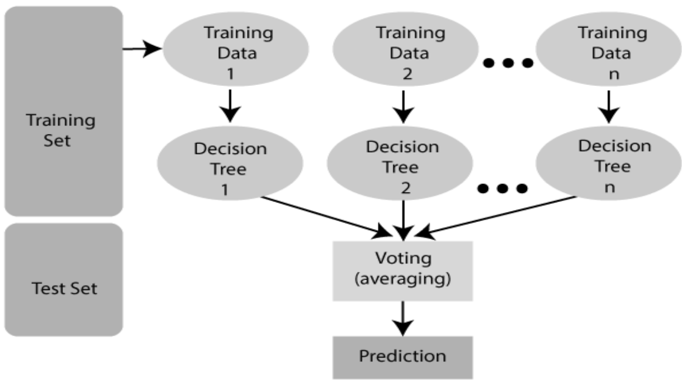

Figure 3.2.3: Random Forest classifier Schematic representation (Source-Google)

The Random Forest algorithm is a robust ensemble learning technique used for social media bot detection. It combines the power of multiple decision trees to enhance accuracy and resilience. The model is built using recursively splitting the dataset based on feature attributes, introducing randomness and diversity. Bootstrapping is used to train each decision tree, introducing diversity among individual trees. During the prediction phase, each decision tree "votes" for the class, and the final prediction is determined by the majority vote.

Random Forest provides a measure of feature importance based on how frequently a feature is used to split the data across all trees, which helps understand. The model is integrated into the bot detection workflow through data preprocessing, training, and performance evaluation. Performance metrics such as accuracy, precision, recall, F1-score, and model's ability to handle imbalanced datasets. Hyperparameter tuning is employed to optimize performance, with cross-validation techniques employed to find the most effective combination of hyperparameters. The Random Forest model offers interpretability through feature importance scores, aiding in model interpretability. System integration considerations include scalability, real-time prediction, and model maintenance. Scalability ensures efficient processing of large datasets and implementations, while real-time prediction speed is reasonable for many applications. Regular retraining and automation of model updates based on new data patterns and emerging trends are considered for long-term efficacy.

Decision Tree:

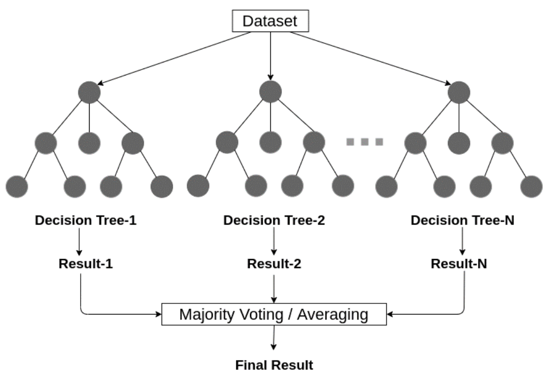

Figure 3.2.4: Decision Tree classifier Schematic representation (Source-Google)

The Decision Tree algorithm is a supervised machine learning algorithm used for both classification and regression applications. It resembles the structure of a tree and makes judgments based on feature values. In the area of social media bot detection, the Decision Tree model is selected for its interpretability, simplicity of implementation, and ability to handle non-linear correlations in data. Clean the dataset by addressing missing values, duplicates, and useless information. Select relevant criteria for bot detection based on traits that separate bot and non-bot accounts. Randomly partition the dataset into training and testing sets. Model train Implement the Decision Tree algorithm for training on the provided dataset. The system learns the decision criteria based on attributes to categorize accounts as bots or non-bots. Utilize techniques like as trimming to minimize overfitting. Performance Evaluation Decision Tree model employing measures such as accuracy, precision, recall, and F1-score. Analyze the confusion matrix to understand the true positives, true negatives, false positives, and false negatives. Assess the model's capacity to generalize to unseen dataIdentify any areas of improvement or possible biases in the model's decision-making Implement the Decision Tree model in a production setting for real-time bot detection. Implement security mechanisms to safeguard the Decision Tree model from possible assaults or hostile inputs. Challenges skewed Data Decision Trees could be sensitive to skewed datasets. Implement techniques such as oversampling, undersampling, or applying proper class weights to overcome this problem. Overfitting Decision Trees are prone to overfitting, particularly on noisy data. Implementing pruning techniques and reducing tree depth helps reduce this problem.

XGBoost:

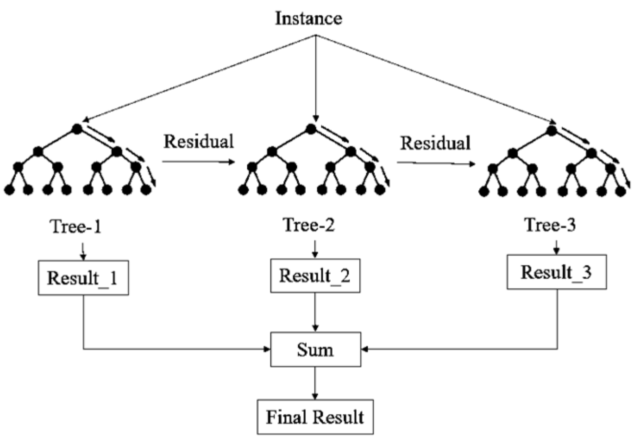

Figure 3.2.5: XGBoost Schematic representation (Source-Google)

XGBoost is the primary machine learning algorithm for social media bot detection due to its effectiveness in handling complex, non-linear relationships within datasets. This optimized gradient boosting algorithm excels in classification tasks, making it well-suited for the binary nature of bot detection. Its ability to handle missing data, feature selection, and regularization further enhances its applicability to the challenges posed by social media bot detection. XGBoost uses decision trees as base learners, allowing it to capture complex relationships and interactions within the data. The algorithm optimizes performance by adding weak learners and adjusting for errors made by previous models. It incorporates L1 (LASSO) and L2 (Ridge) regularization terms to prevent overfitting and enhance the model's generalization capability. XGBoost can effectively handle missing data, reducing the need for extensive data preprocessing. The algorithm provides insights into feature importance, aiding in the interpretation of the model's decision-making process. It is designed for efficiency and speed, supporting parallel and distributed computing for large datasets. XGBoost's performance evaluation outputs probability scores, making it compatible with various evaluation metrics such as accuracy, precision, recall, F1-score, and AUC-ROC curve. However, it may still require significant computational resources, particularly for large datasets.

Neural Networks:

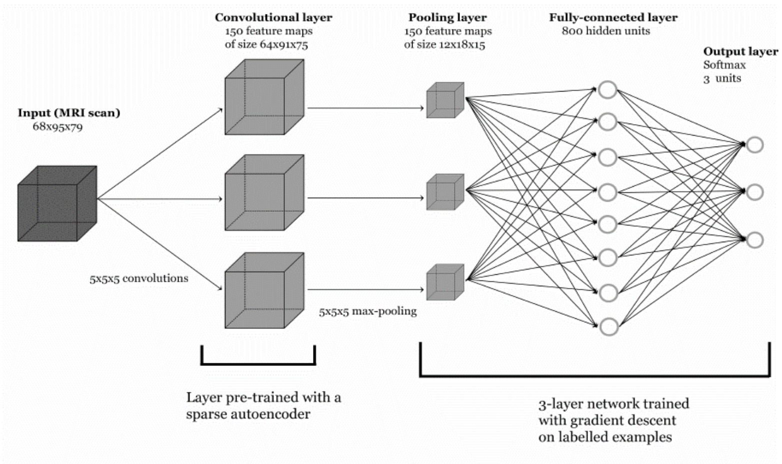

Figure 3.2.6: Neural Networks Schematic representation (Source-Google)

The proposed neural network model for social media bot detection is a sophisticated approach that utilizes deep learning architectures to detect intricate patterns in data. It aims to enhance pattern recognition, improve accuracy, adaptability, streamline training, and generalize well on diverse social media platforms. The model consists of an input layer with nodes representing features from social media data, hidden layers for learning hierarchical representations, an output layer with a single node representing binary classification output, loss functions, an optimizer for gradient descent, regularization techniques, a training process using labeled examples, batch training, monitoring loss and validation metrics, and evaluation metrics like accuracy, precision, recall, F1-score, and curves. Data considerations include a diverse dataset, preprocessing, feature engineering, scalability, and security and ethical considerations.The model's design ensures high accuracy, adaptability, and efficiency in identifying bots across diverse social media platforms through effective system analysis. The model will be refined and implemented in subsequent stages of system design and implementation to further refine its capabilities.

3.3 Hardware/ Software Requirement

- **Hardware Requirements:**
    - GPU and TPU free acceleration provided by Google Colab for faster model training.
    - Memory and storage within the Colab environment for datasets.
    - Use a stable internet connection as Colab operates online.
    - Integrate with Google Drive for additional storage and seamless data management.
    - Document Colab notebooks for reproducibility and collaboration.
- **Software Requirements:**

    Programming Language:-

    - Python3
    - pandas
    - matplotlib
    - sklearn
    - numpy
    - seaborn
    - sys
    - warnings

  Machine Learning Libraries:-

  Scikit-learn: Algorithms Supported, KNN, Random Forest, Decision Tree, Neural network.

  XGBoost: Algorithm Supported, Gradient Boosted Decision Trees (XGBoost)

  Google Colab Notebooks:-

  Description: Useful for work implementation and data investigation.

3.4 Project Management and Financial Analysis

Project Management

- **Project Objectives:**
  - A. To conduct extensive testing of the impact of multiple bot accounts on Twitter, TikTok, and Instagram.
  - B. To create a robust bot detection system capable of handling a wide variety of user behaviors.
  - C. To implement machine learning and advanced bot detection techniques to enhance social media platform security and user safety.
- **Project Timeline:**
  - A. Phase 1: Project Planning and Research (4-6 weeks)
  - B. Phase 2: Data Collection and Preparation (6-8 weeks)
  - C. Phase 3: Model Development (8-10 weeks)
  - D. Phase 4: Model Testing and Validation (6-8 weeks)
  - E. Phase 5: System Integration and Deployment (4-6 weeks)
  - F. Phase 6: Evaluation and Optimization (4-6 weeks)
  - G. Phase 7: Documentation and Reporting (2-4 weeks)
- **Resource Planning:**

  A. **Equipment and Tools:**

  - High-performance computers for the development team.
  - GPU and TPU acceleration provided by Google Colab.
  - Stable internet connection and integration with Google Drive.

  B. **Software and Technologies:**

  - Programming Languages: Python3.
  - Data Analysis Libraries: pandas, matplotlib, seaborn, numpy.
  - Machine Learning Libraries: Scikit-learn (KNN, Random Forest, Decision Tree, Neural Network), XGBoost.
  - Development Environment: Google Colab Notebooks.

C. **Data and Content:**

- Labeled datasets from Twitter, TikTok, and Instagram.
- Behavioral patterns and account characteristics data for model training.
- Documentation of all processes and findings.

D. **Training and Skill Development:**

- Ensure the development is proficient in Python and machine learning.
- Provide additional training on specific machine learning algorithms and data analysis techniques as needed.
- Continuous learning opportunities to stay updated with the latest advancements in bot detection.

- **Risk Management:**

  A SWOT analysis helps assess the strengths, weaknesses, opportunities, and threats of our project:

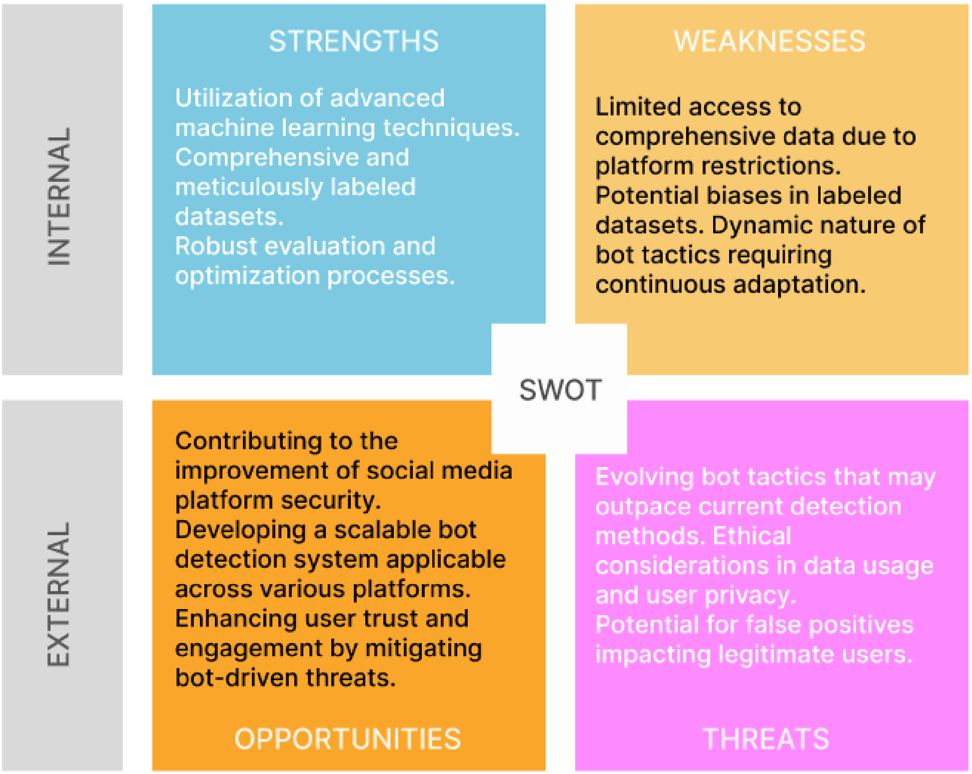

Figure 3.4.1: SWOT analysis

- **Financial Analysis**

  Below is the estimated cost for the machine learning-based project focused on bot detection in social media platforms. The costs are represented in BDT and are approximations that may vary based on actual project requirements.

Table 3.4.1: Estimated Cost for Machine Learning-based Project

SN	Components	Estimated cost (BDT)
1	SSD	4500-6000
2	Google Collab Pro	2000-3000
3	Data Collection and Processing	0
4	Documentation And Report Writing	500-1000
5	Miscellaneous	500-1000
6	Contingency	850-1100
	Total Estimated cost	8350-12000

The total estimated cost for the project ranges between 8350 BDT and 12000 BDT. This estimation ensures that all necessary components for successful project completion are covered, providing a comprehensive financial plan to manage resources efficiently.

3.5 Summary

In conclusion, the study project discussed the difficulties of social media bot identification through a multi-perspective method. By leveraging supervised machine learning algorithms and considering the unique challenges faced by different platforms, the created bot identification system adds to better platform security and user safety. The suggested approach and execution requirements serve as a basis for future improvements in social media bot identification. As social media platforms change, ongoing study and creative thinking will be important to stay ahead of new bot tricks and ensure an accurate online environment.

CHAPTER 4
Implementation

4.1 Overview

The implementation phase is a crucial stage in the development of a social media bot detection system. It involves coding the algorithms, integrating them into a cohesive system, and rigorously testing the system's performance. Various supervised machine learning algorithms, such as K-Nearest Neighbors (KNN), Random Forest, Decision Tree, XGBoost, and Neural Network, are carefully considered and applied to achieve optimal performance in detecting social media bots. The process involves developing and implementing the algorithms using Python and relevant libraries like Scikit-learn and XGBoost. The system is integrated into a unified system capable of processing data and identifying bots across multiple social media platforms. System testing is employed to evaluate the model's performance, including assessing metrics like accuracy, precision, recall, and F1-score. The system is also designed to adapt to new data and the evolving nature of social media bot behaviors through continuous learning and updates. The success of this phase is crucial for enhancing security and user safety on social media platforms.

4.2 Train Model

Training the model is a pivotal component in the development of our social media bot detection system. My Total data TikTok row 2864, column 35 and Twitter row 2797, column 20, Instragram row 2799, column 13 and Total Data: 8,460 .This phase involves preparing the data, selecting appropriate machine learning algorithms, and training these models to accurately identify and differentiate between bots and genuine users. The following steps outline our process of training the model:

Data Preparation

Step 1: First, import libraries and check performances imports, which are required for
Performance will result.

Step 2: Clean the Data and prepare to Classification. Make a function to check
Performance of the classifiers.

Step 3: Now I am consider attributes which determine a multiple account to be a bot or non bot.

Step 4: Create a bot identification criteria based on attributes and classify the dataset randomly Into train and test dataset.

Step 5: Apply my five classification method and find accuracy of each method.

Step 6: After the classification is completed Compare Accuracy of my five methods and find The most relevant one.

Step 7: Work on test data and find my five algorithms. Result by the best and found classifier, And all algorithms accuracy methods have been compared to show results.

Model Selection for Training:

KNN, Random Forest, Decision Tree, Neural network, XGBoost

Model Training:

I have divided the dataset into training and testing sets to evaluate the model's performance accurately. Typically, a split of 80% training data and 20% testing data was used.Training Algorithms data was fed into the selected my 5 model machine learning algorithms to build models. Each algorithm learned the patterns and relationships in the data to classify multiple accounts as bots or non-bots. Sometime Hyperparameter Tuning I adjusted the parameters of the algorithms to optimize their performance. Techniques such as grid search or random search were used to find the best combination of hyperparameters.

4.3 System Testing/ Model Evaluation

4.3.1 Instagram Bot detection System Testing and Model Evaluation:

- **Here Instagram DataFrame:**

	Id	Followers	Followings	Bio length	Fullname	Private	Post count	Average number of media likes	Media count	Last month media count	Consecutive characters in username	Number of digits in username	Account_type
0	0	134	241	19	True	True	2	NaN	NaN	NaN	4	0	0
1	1	129	427	0	True	True	0	NaN	NaN	NaN	2	4	0
2	2	168	790	120	True	True	6	NaN	NaN	NaN	2	2	0
3	3	66	110	37	True	True	8	NaN	NaN	NaN	0	4	0

Figure 4.3.1: Shape of the Data Frame row 2799, colume13 (Instagram).

- **Here is Distribution of Account Types bot and non-bot :**

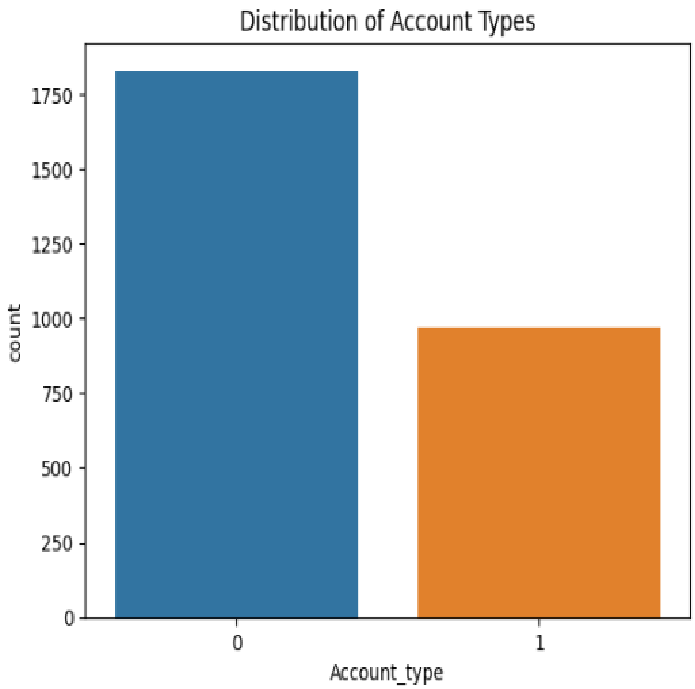

Figure 4.3.2: Class Counts of bot and non-bot (Instagram).

- **Side-by-side scatter plots comparing the relationship between the number of followers and followings for two groups: Bots and Non-Bots:**

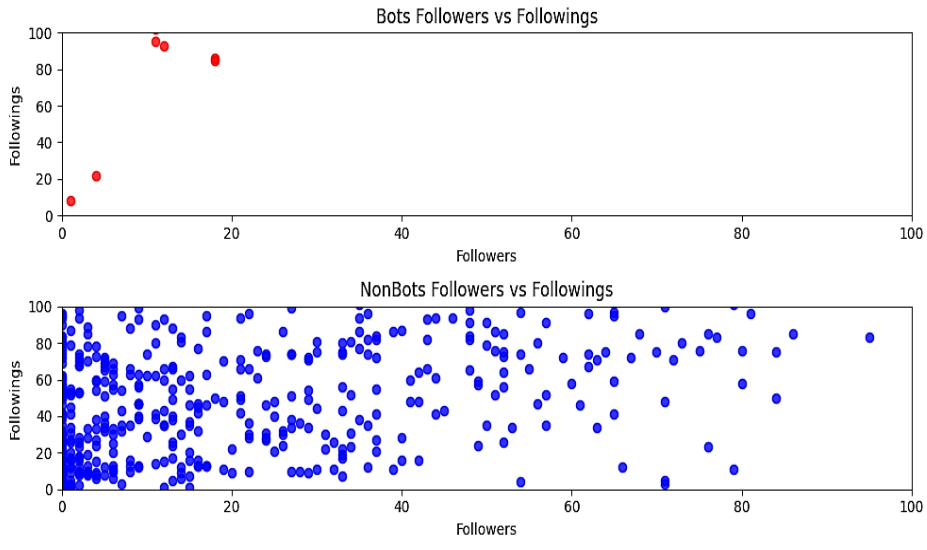

Figure 4.3.3: Comparing between number followers and followings Bot and Non-Bots (Instagram).

- **Pearson Correlation Matrix**

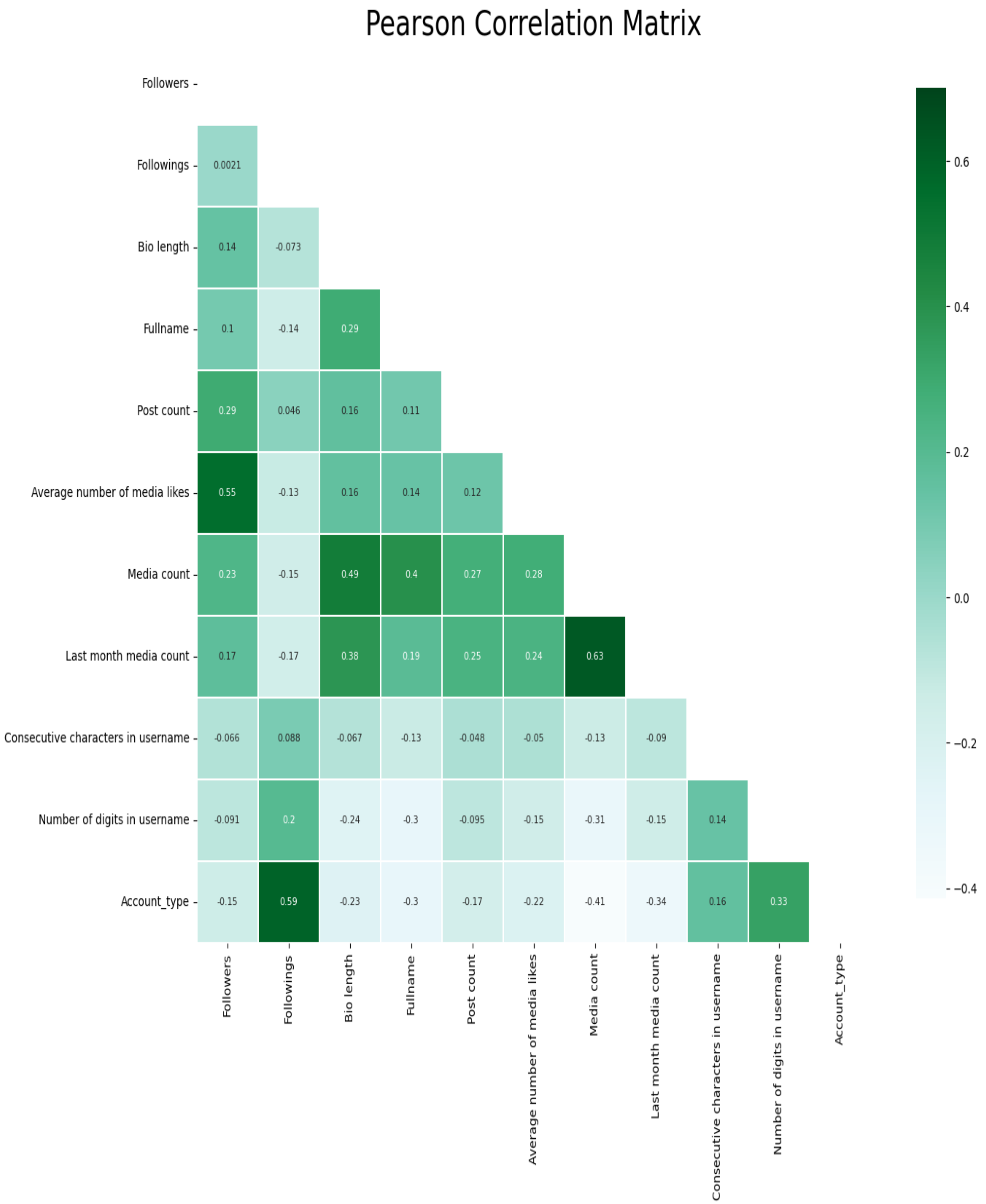

Figure 4.3.4: Pearson Correlation Matrix (Instagram).

- **Distribution of Followers and Followings by bot and non-bot:**

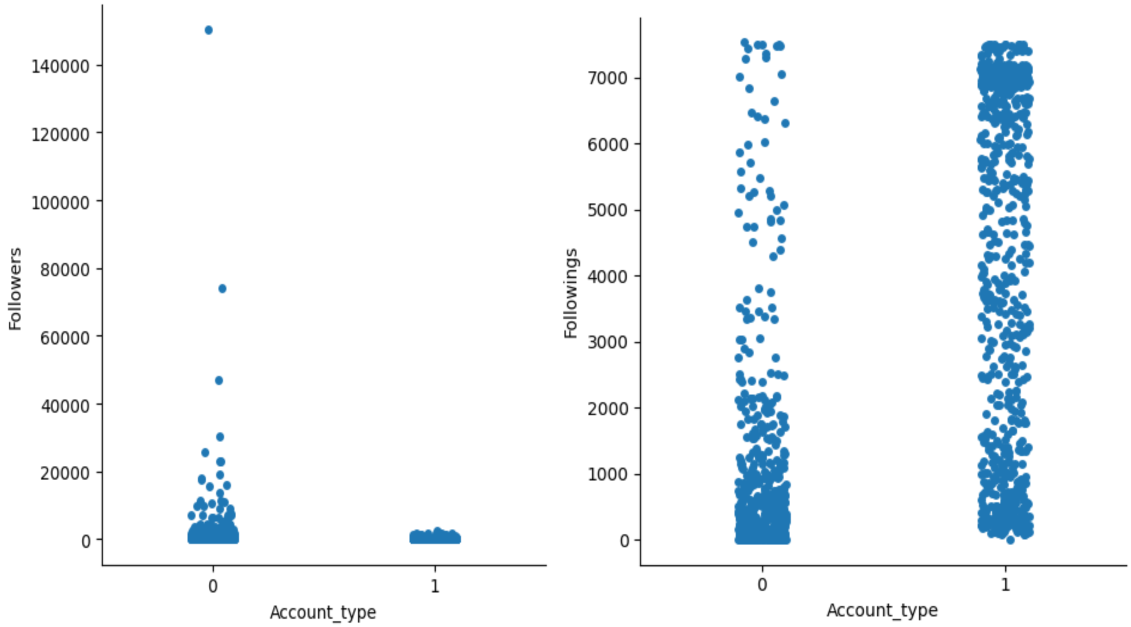

Figure 4.3.5: Visualize Followers and Followings by Account Type (Instagram).

- Distribution of Bio length, Fullname, Private, Post count by bot and non-bot:

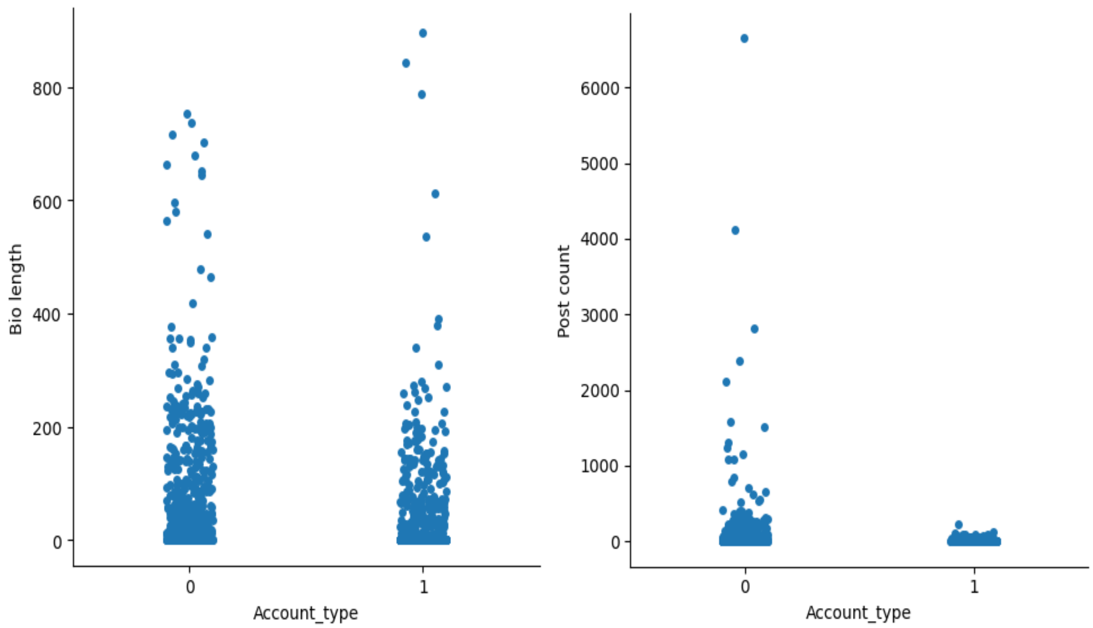

Figure 4.3.6: Visualize Bio length, Post Count by bot and non-bot (Instagram).

- **Distribution of Average number of media likes, Last month media count, Consecutive characters in username, Number of digits in username by bot and non-bot:**

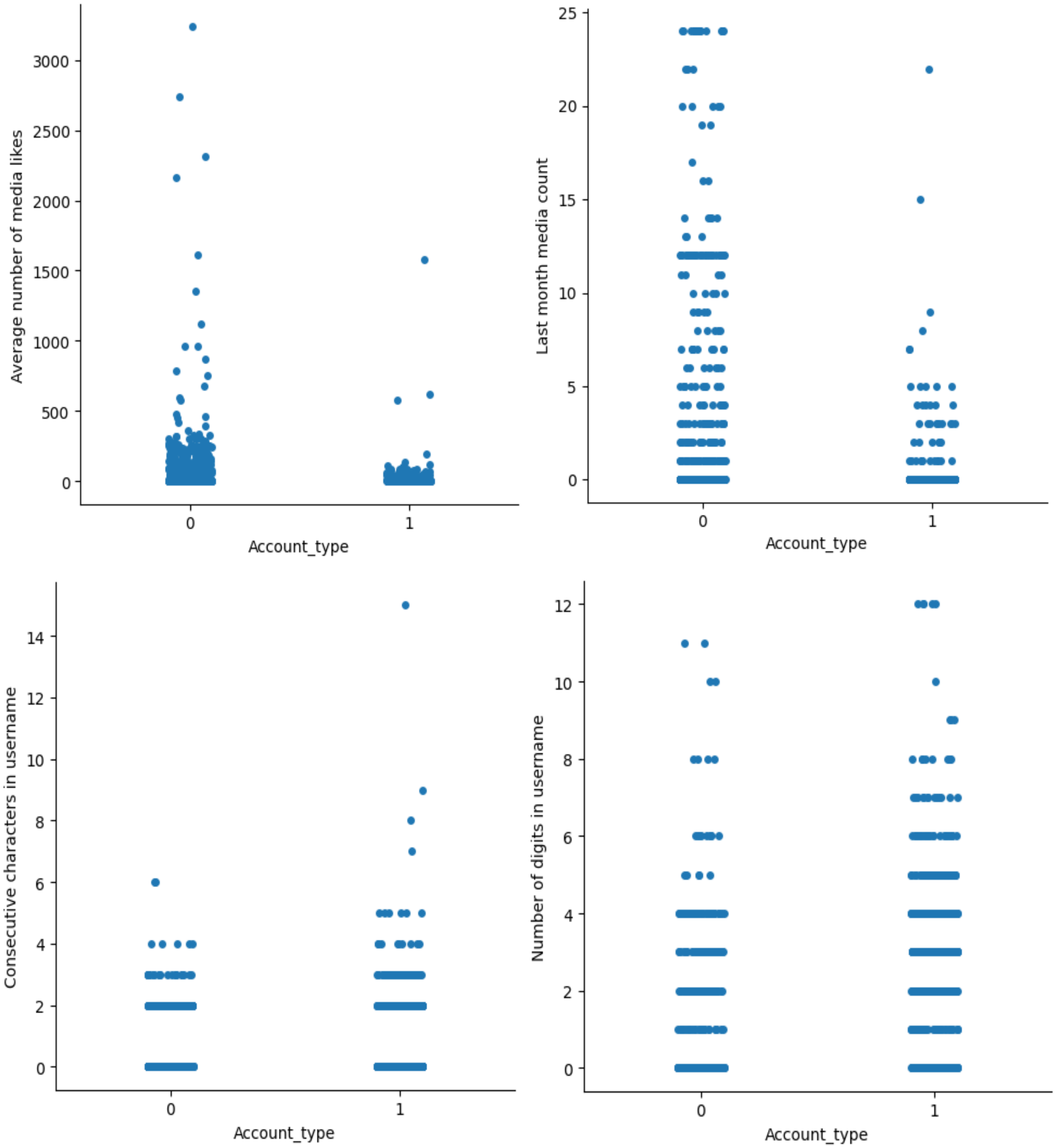

Figure 4.3.7: Visualize Average number of media likes, Last month media count, Consecutive characters in username, Number of digits in username by bot and non-bot (Instagram).

- **K-nearest Neighbors classification algorithm result, Accuracy, Confusion Matrix, Classification Report:**

```
Accuracy: 0.9074733096085409
Confusion Matrix:
 [[ 98  14]
 [ 12 157]]
Classification Report:
              precision    recall  f1-score   support

           0       0.89      0.88      0.88       112
           1       0.92      0.93      0.92       169

    accuracy                           0.91       281
   macro avg       0.90      0.90      0.90       281
weighted avg       0.91      0.91      0.91       281
```

Figure 4.3.8: k-nearest neighbors classification algorithm result (Model-1)

- **Random forest classifier Accuracy, Confusion Matrix, Classification Report:**

```
Accuracy: 0.9537

Confusion Matrix:
 [[107   5]
 [  8 161]]

Classification Report:
              precision    recall  f1-score   support

           0       0.93      0.96      0.94       112
           1       0.97      0.95      0.96       169

    accuracy                           0.95       281
   macro avg       0.95      0.95      0.95       281
weighted avg       0.95      0.95      0.95       281
```

Figure 4.3.9: Random forest classifier result (Model-2).

- **Decision Tree Classifier Accuracy, Confusion Matrix, Classification Report:**

```
Accuracy: 0.92
Confusion Matrix:
[[105   7]
 [ 15 154]]
Classification Report:
              precision    recall  f1-score   support

           0       0.88      0.94      0.91       112
           1       0.96      0.91      0.93       169

    accuracy                           0.92       281
   macro avg       0.92      0.92      0.92       281
weighted avg       0.92      0.92      0.92       281
```

Figure 4.3.10: Decision Tree classifier result (Model-3).

- **XGBoost classifier Accuracy, Confusion Matrix, Classification Report:**

```
Accuracy: 0.95
Confusion Matrix:
 [[108   4]
 [ 11 158]]
Classification Report:
              precision    recall  f1-score   support

           0       0.91      0.96      0.94       112
           1       0.98      0.93      0.95       169

    accuracy                           0.95       281
   macro avg       0.94      0.95      0.94       281
weighted avg       0.95      0.95      0.95       281
```

Figure 4.3.11: XGBoost classifier result (Model-4).

- **Neural Networks classification Accuracy, Confusion Matrix, Classification Report:**

```
Test Loss: 0.1416, Test Accuracy: 0.9573
9/9 [==============================] - 0s 2ms/step

Confusion Matrix:
 [[105   7]
 [  5 164]]

Classification Report:
              precision    recall  f1-score   support

           0       0.95      0.94      0.95       112
           1       0.96      0.97      0.96       169

    accuracy                           0.96       281
   macro avg       0.96      0.95      0.96       281
weighted avg       0.96      0.96      0.96       281
```

Figure 4.3.12: Neural Networks classification result (Model-5).

- **Compare the accuracy of multiple models:**

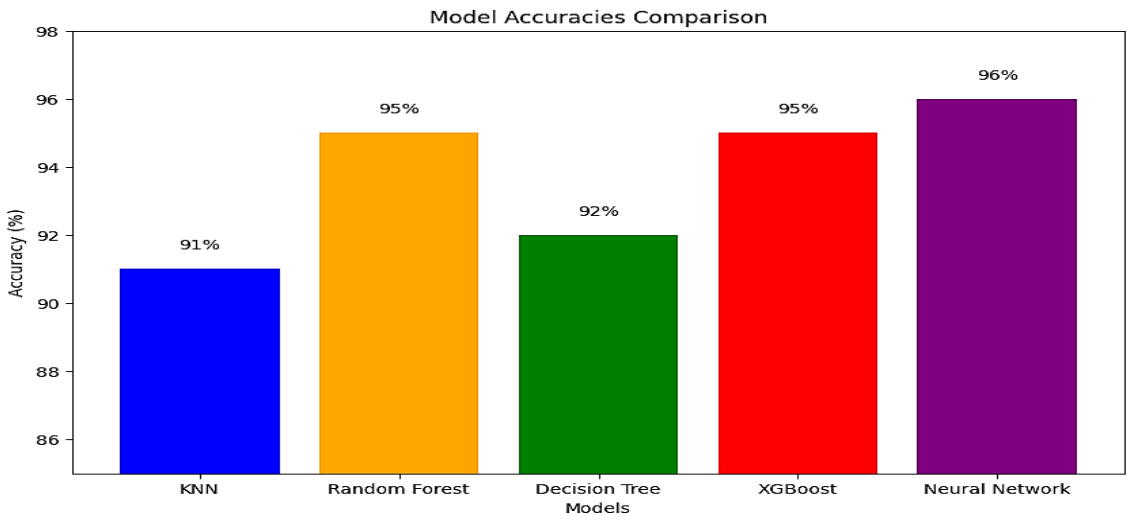

Figure 4.3.13: Compare the accuracy all model (Instagram).

4.3.2 Twitter Bot detection System Testing/ Model Evaluation:

- **Here Twitter Data Frame:**

	id	id_str	screen_name	location	description	url	followers_count	friends_count	listed_count	created_at	favourites_cou
0	8.160000e+17	"815745789754417152"	"HoustonPokeMap"	"Houston, TX"	"Rare and strong PokŽmon in Houston, TX. See m...	"https://t.co/dnWuDbFRkt"	1291	0	10	"Mon Jan 02 02:25:26 +0000 2017"	
1	4.843621e+09	4843621225	kernyeahx	Templeville town, MD, USA	From late 2014 Socium Marketplace will make sh...	NaN	1	349	0	2/1/2016 7:37	
2	4.303727e+09	4303727112	mattlieberisbot	NaN	Inspired by the smart, funny folks at @replyal...	https://t.co/P1e1o0m4KC	1086	0	14	Fri Nov 20 18:53:22 +0000 2015	

Figure 4.3.14: Shape of the Data Frame row 2797, column 20.

- **Here is Distribution Class of Account Types bot and non-bot :**

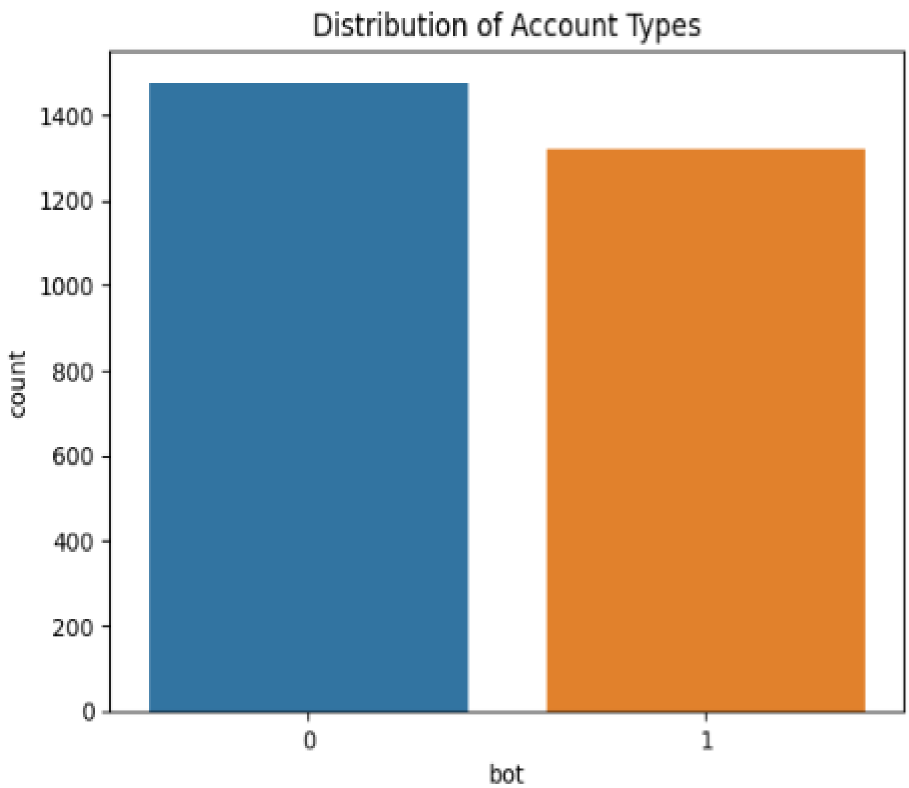

Figure 4.3.15: Class Counts of bot and non-bot (Twitter).

- **Side-by-side scatter plots comparing the relationship between the Bots Friends vs Followers and Non-Bots Friends vs Followers :**

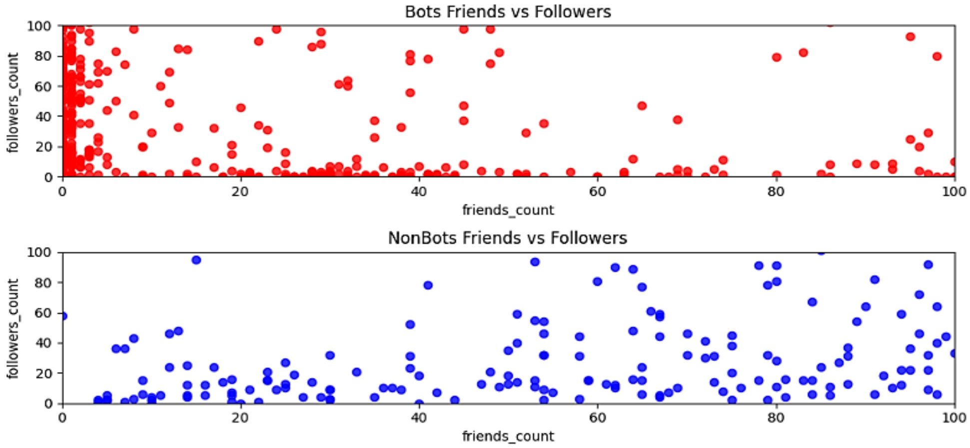

Figure 4.3.16: Comparing between Bots Friends vs Followers and Non-Bots Friends vs Followers.

- **Pearson Correlation Matrix:**

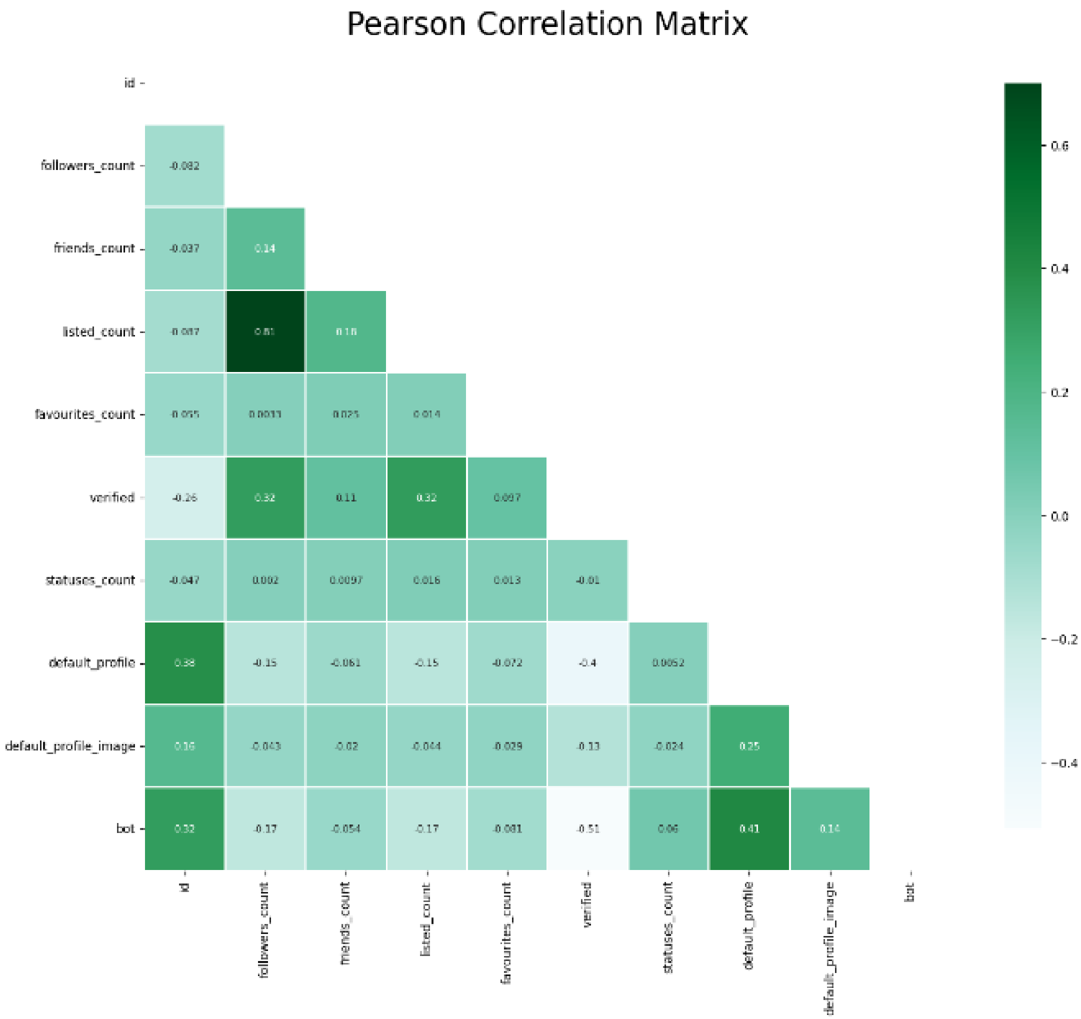

Figure 4.3.17: Pearson Correlation Matrix (Twitter)

- **Distribution of followers_count, friends_count, listed_count by bot and non-bot:**

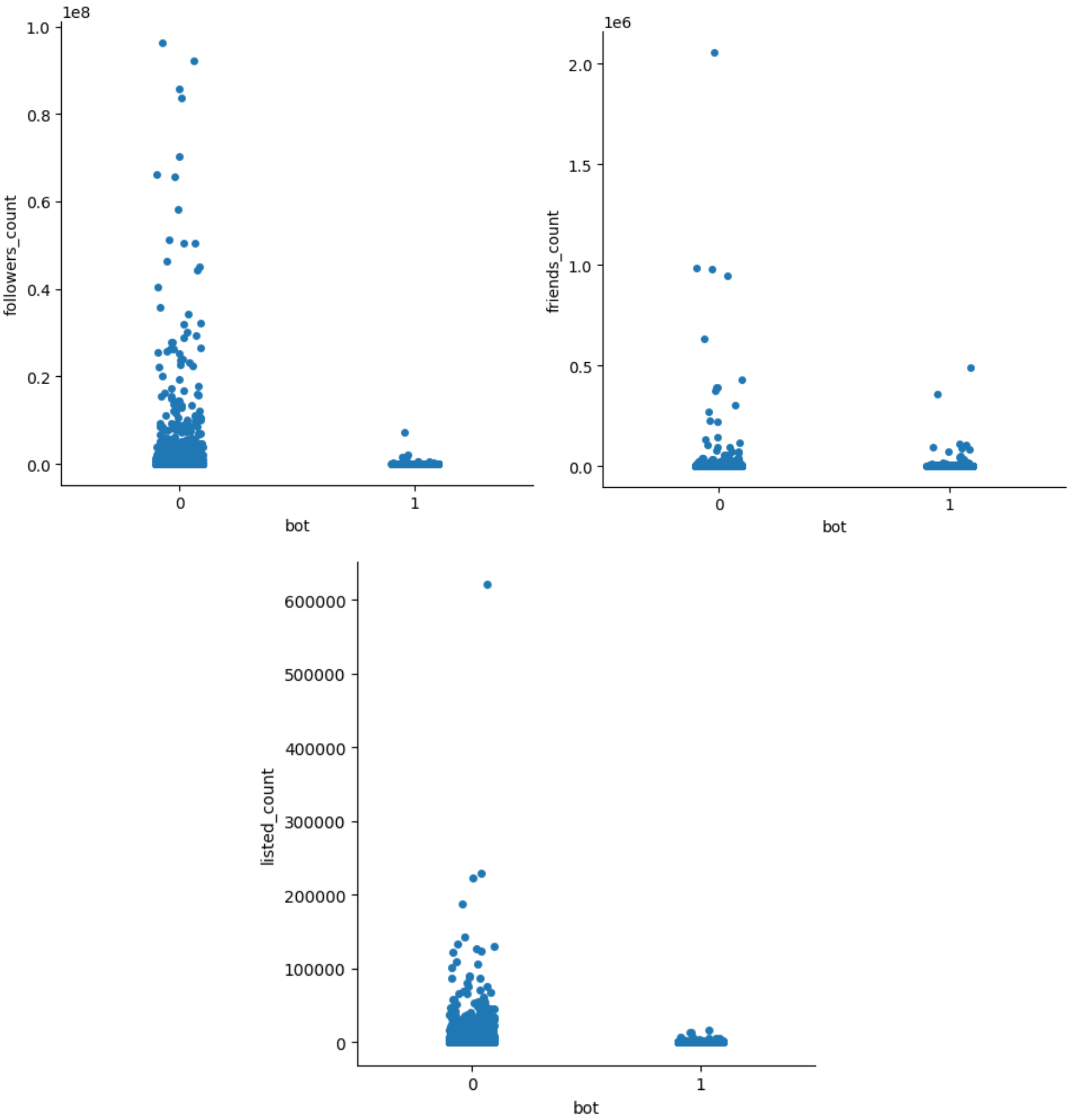

Figure 4.3.18: Visualize followers_count, friends_count, listed_count by bot and non-bot.

- **Distribution of favourites_count, verified, statuses_count by bot and non-bot.**

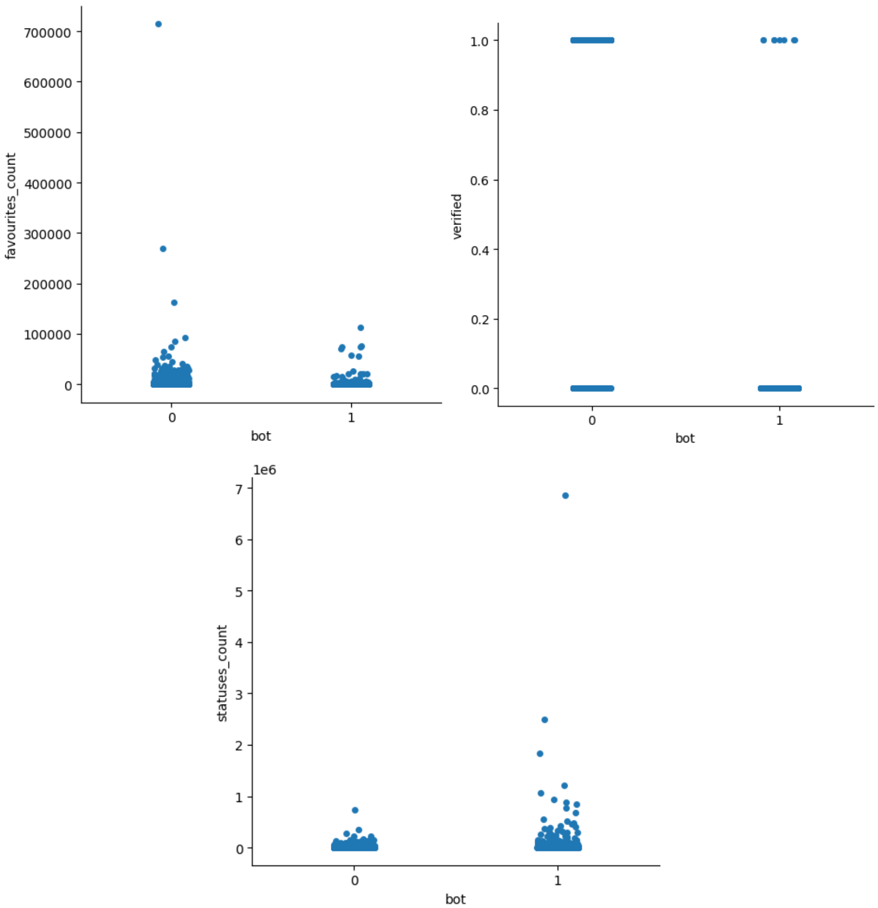

Figure 4.3.19: Visualize favourites_count, verified, statuses_count by bot and non-bot.

- **k-nearest neighbors KNN classification algorithm result, Accuracy, Confusion Matrix, Classification Report:**

```
Accuracy: 0.8714285714285714

Confusion Matrix:
[[251  39]
 [ 33 237]]

Classification Report:
              precision    recall  f1-score   support

           0       0.88      0.87      0.87       290
           1       0.86      0.88      0.87       270

    accuracy                           0.87       560
   macro avg       0.87      0.87      0.87       560
weighted avg       0.87      0.87      0.87       560
```

Figure 4.3.20: k-nearest neighbors classification algorithm result (Model-1)

- **Random forest classifier Accuracy, Confusion Matrix, Classification Report:**

```
Accuracy: 0.9071428571428571

Confusion Matrix:
[[264  26]
 [ 26 244]]

Classification Report:
              precision    recall  f1-score   support

           0       0.91      0.91      0.91       290
           1       0.90      0.90      0.90       270

    accuracy                           0.91       560
   macro avg       0.91      0.91      0.91       560
weighted avg       0.91      0.91      0.91       560
```

Figure 4.3.21: Random forest classifier result (Model-2).

- **Decision Tree Classifier Accuracy, Confusion Matrix, Classification Report:**

```
Accuracy: 0.8928571428571429

Confusion Matrix:
[[263  27]
 [ 33 237]]

Classification Report:
              precision    recall  f1-score   support

           0       0.89      0.91      0.90       290
           1       0.90      0.88      0.89       270

    accuracy                           0.89       560
   macro avg       0.89      0.89      0.89       560
weighted avg       0.89      0.89      0.89       560
```

Figure 4.3.22: Random forest classifier result (Model-3).

- **XGBoost classifier Accuracy, Confusion Matrix, Classification Report:**

```
Accuracy: 0.90
Confusion Matrix:
 [[264  26]
 [ 29 241]]
Classification Report:
              precision    recall  f1-score   support

           0       0.90      0.91      0.91       290
           1       0.90      0.89      0.90       270

    accuracy                           0.90       560
   macro avg       0.90      0.90      0.90       560
weighted avg       0.90      0.90      0.90       560
```

Figure 4.3.23: XGBoost classifier result (Model-4).

- **Neural Networks classification Accuracy, Confusion Matrix, Classification Report:**

```
Test Loss: 0.3944, Test Accuracy: 0.8179
18/18 [==============================] - 0s 2ms/step

Confusion Matrix:
[[227  63]
 [ 39 231]]

Classification Report:
              precision    recall  f1-score   support

           0       0.85      0.78      0.82       290
           1       0.79      0.86      0.82       270

    accuracy                           0.82       560
   macro avg       0.82      0.82      0.82       560
weighted avg       0.82      0.82      0.82       560
```

Figure 4.3.24: Neural Networks classification result (Model-5).

- **Compare the accuracy of multiple models:**

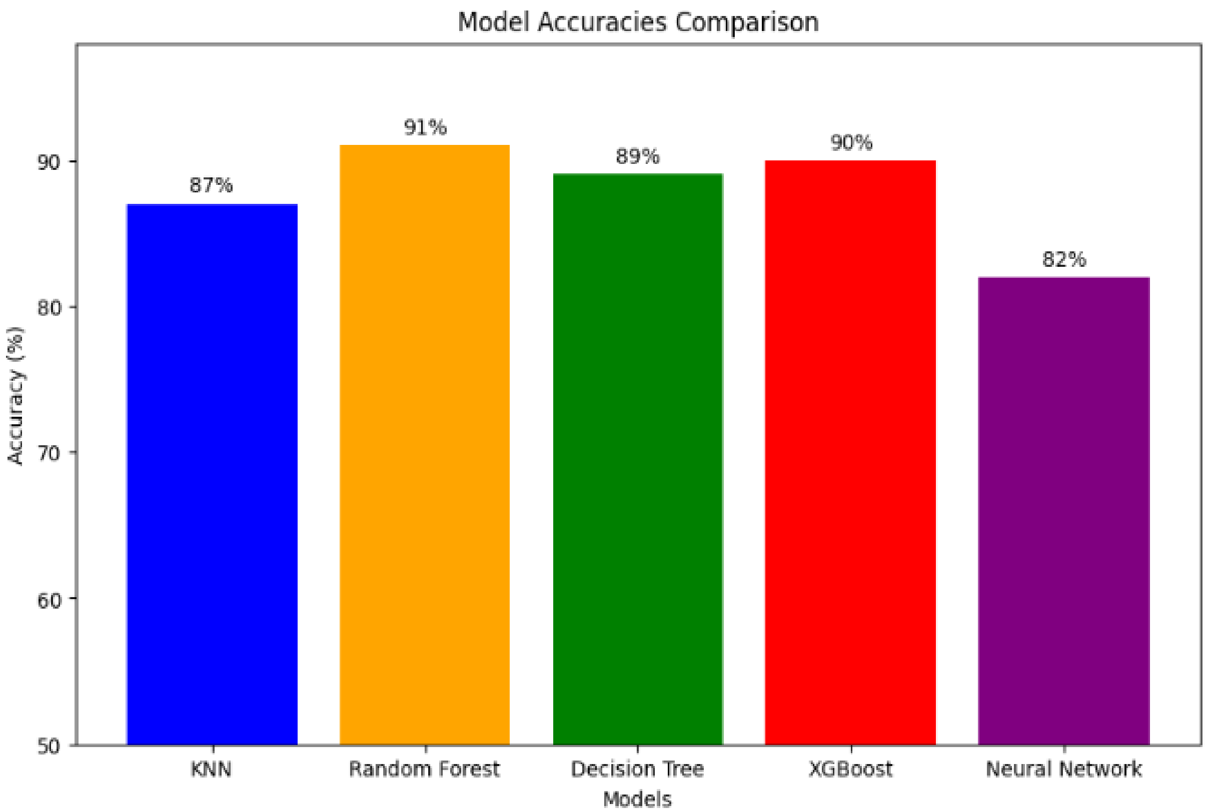

Figure 4.3.26: Compare the accuracy all model (Twitter).

4.3.3 TikTok Bot detection System Testing/ Model Evaluation:

- **Here TikTok DataFrame**:

	IsAccountPrivate	IsVerified	HasProfilePicture	AnzahlFolgeIch	AnzahlFollower	AnzahlLikes	HasInstagramLink
0	False	False	True	3171	93	3	False
1	False	False	True	2255	132	78	False
2	False	False	False	1	5	0	False
3	False	False	True	1168	89	0	False
4	False	False	True	169	6	0	False
5	False	False	True	60	3	4	False
6	False	False	True	3788	1606	11000	False

Figure 4.3.27: Shape of the DataFrame row 2864, column 35.

- **Here is Distribution Class of Account Types bot and non-bot :**

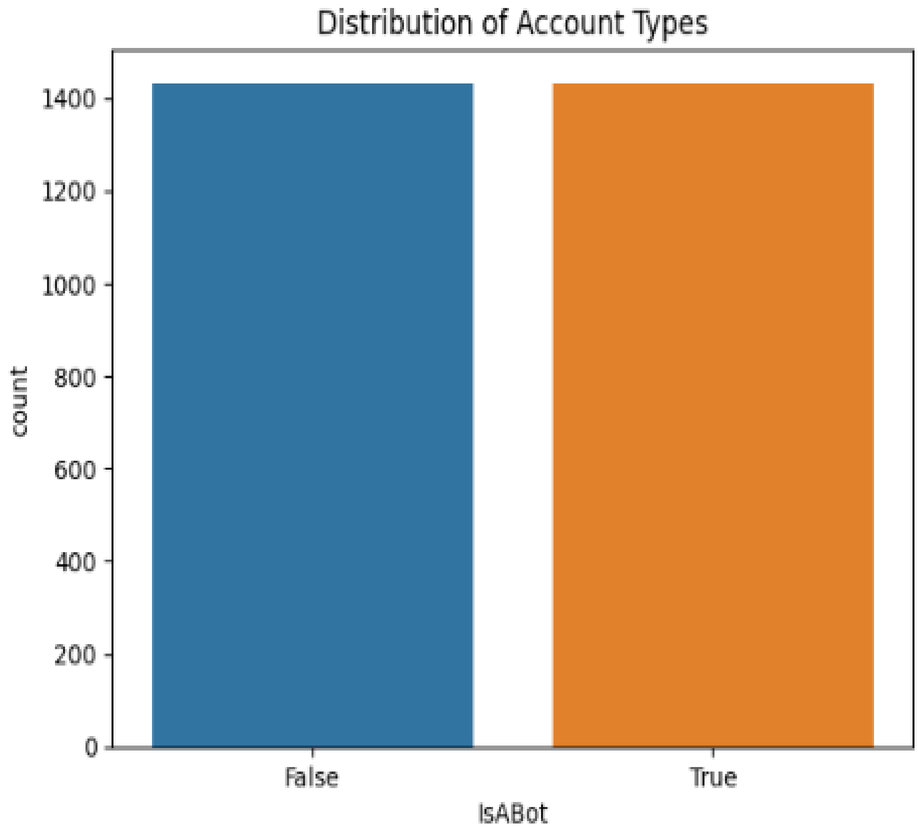

Figure 4.3.28: Class Counts of bot and non-bot (TikTok).

- **Side-by-side scatter plots comparing the relationship between the number of Bots Follower vs Likes and NonBots Follower vs Likes for two groups: Bots and Non-Bots:**

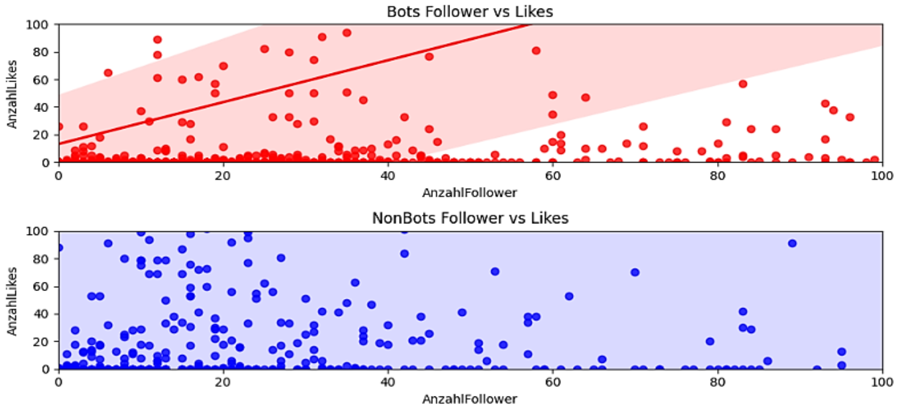

Figure 4.3.29: Comparing between Bots Follower vs Likes and NonBots Follower vs Likes.

- **Pearson Correlation Matrix:**

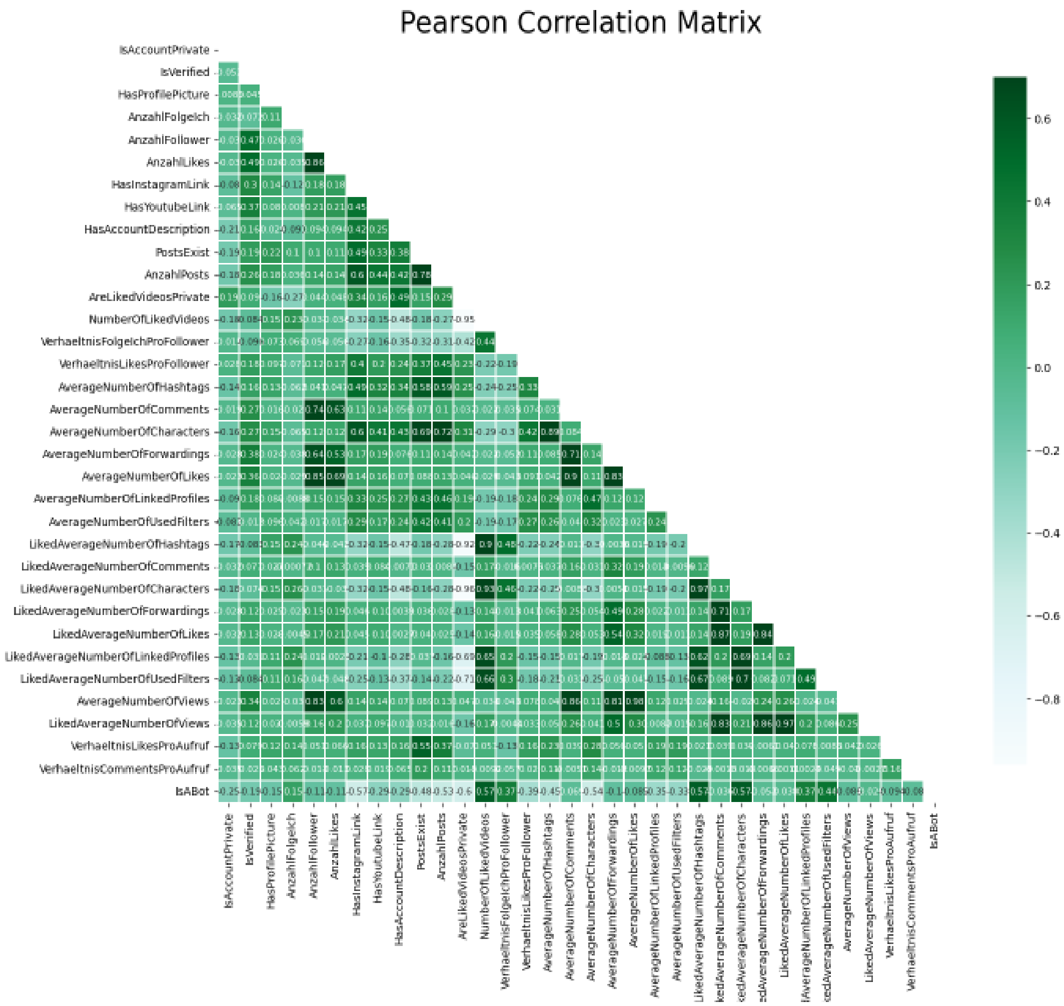

Figure 4.3.30: Pearson Correlation Matrix (TikTok).

- **Distribution of IsAccountPrivate, IsVerified, HasProfilePicture, AnzahlFolgeIch, AnzahlFollower, AnzahlLikes, HasInstagramLink, HasYoutubeLink, HasAccountDescription, HasLinkInDescription, PostsExist,AnzahlPosts, , NumberOfLikedVideos by bot and non-bot:**

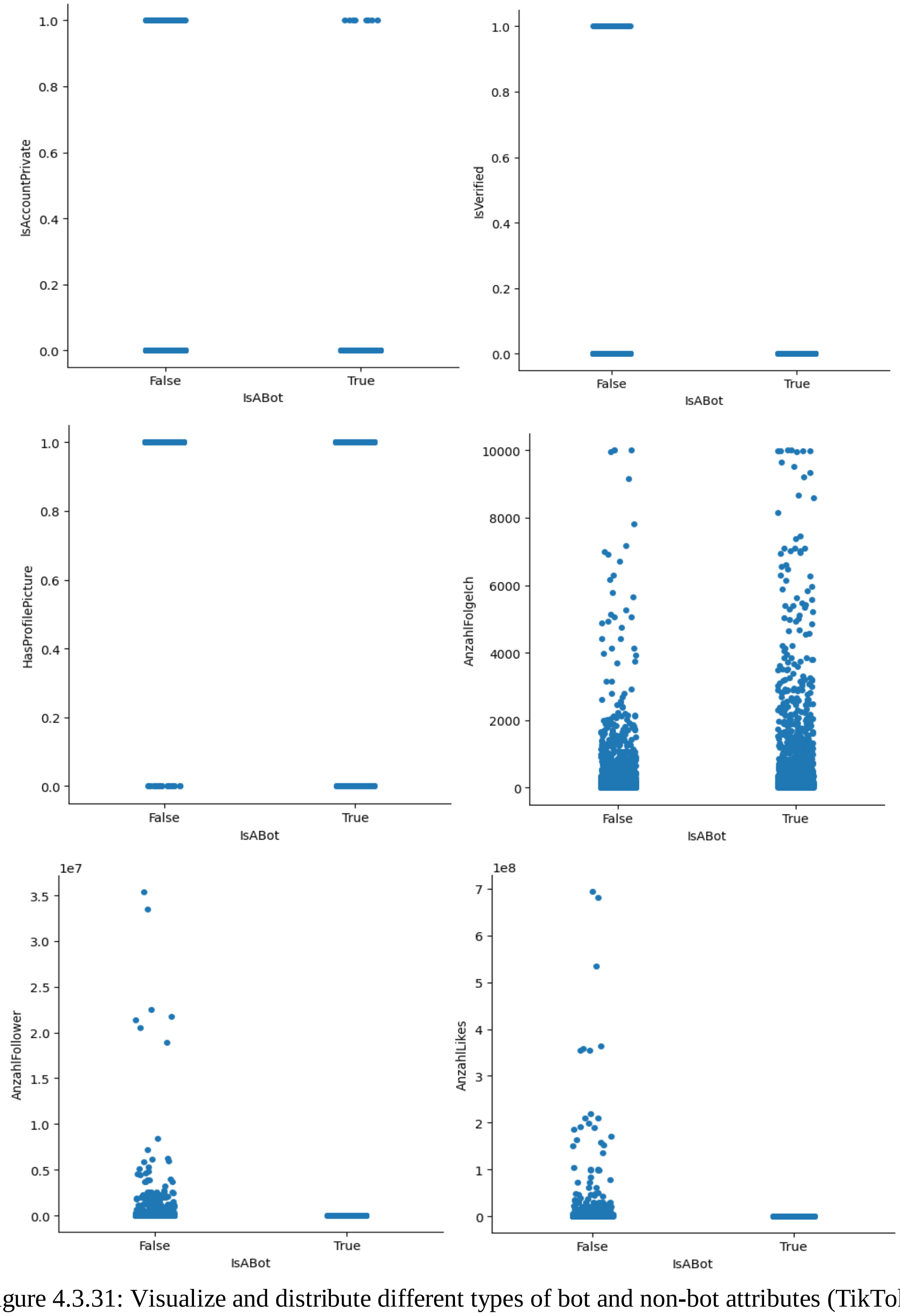

Figure 4.3.31: Visualize and distribute different types of bot and non-bot attributes (TikTok).

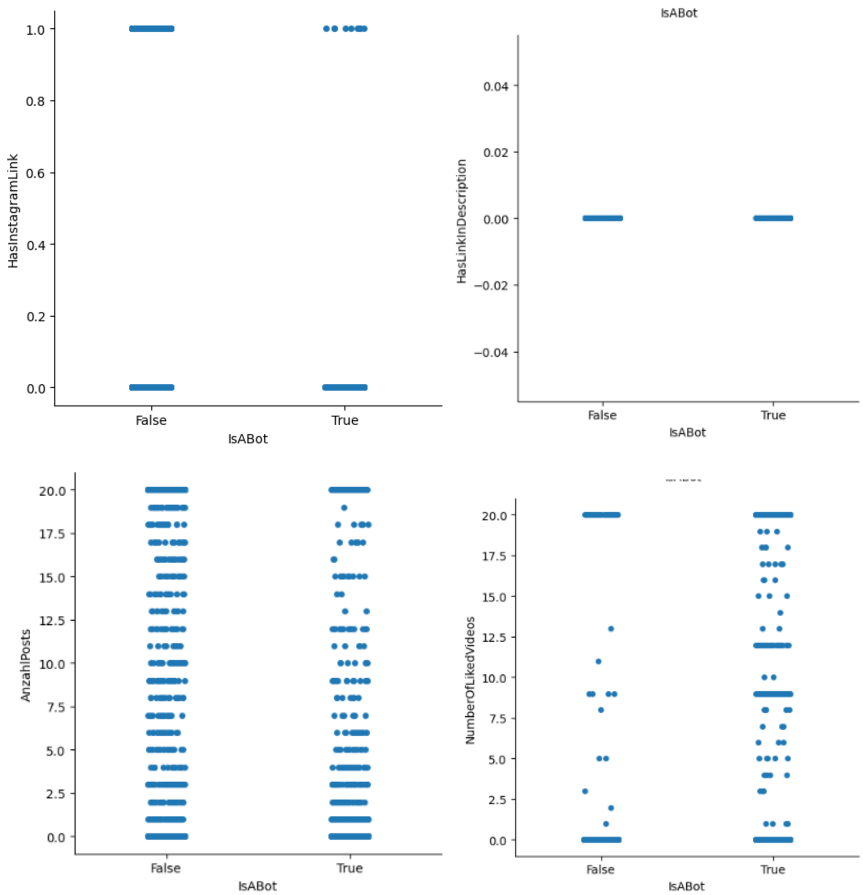

Figure 4.3.31: Visualize and distribute different types of bot and non-bot attributes (TikTok).

- **Distribution of VerhaeltnisFolgeIchProFollower, VerhaeltnisLikesProFollower, VerhaeltnisLikesProAufruf, VerhaeltnisCommentsProAufruf by bot and non-bot:**

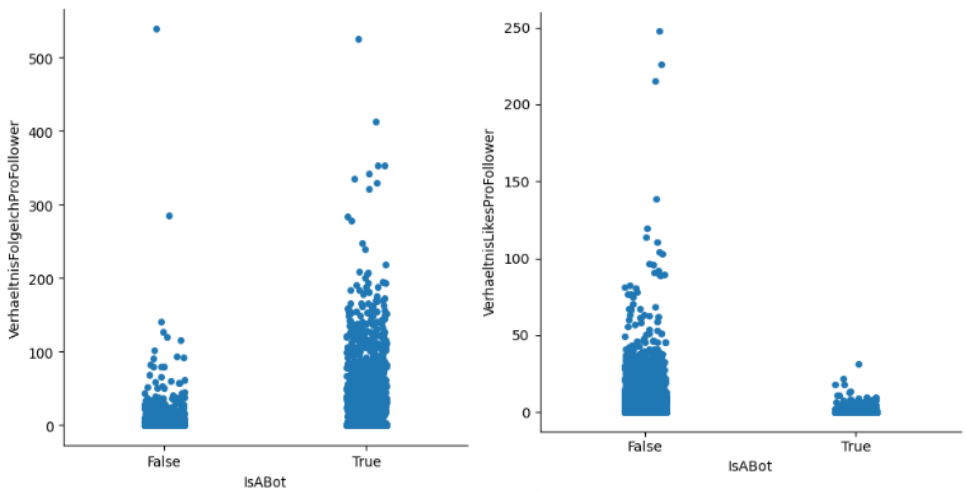

Figure 4.3.32: Visualize and distribute different types of bot and non-bot attributes (TikTok)

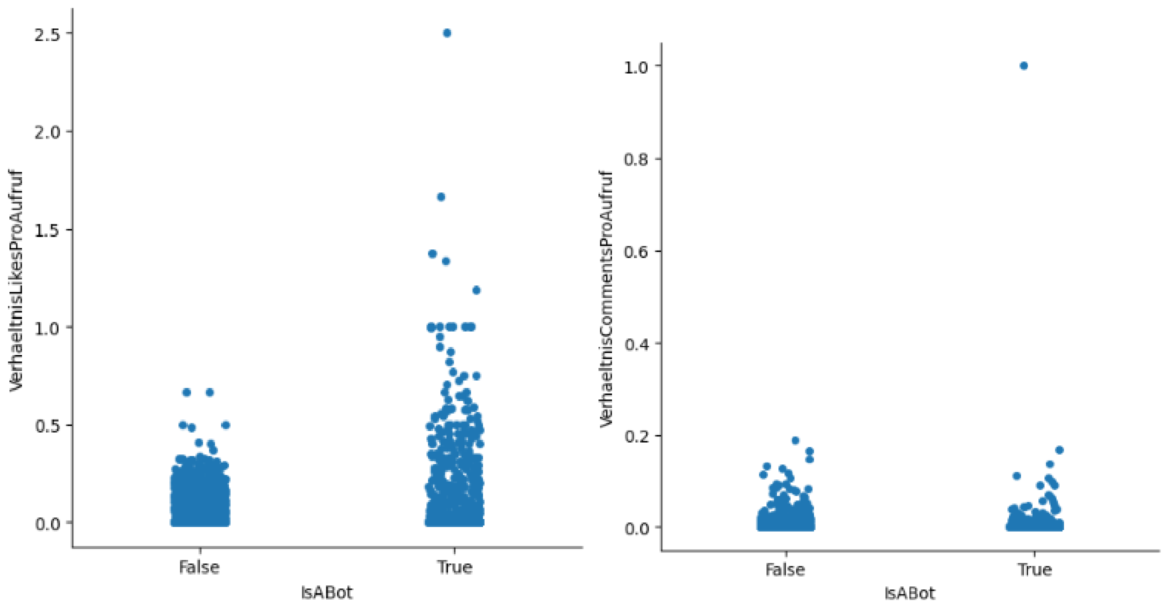

Figure 4.3.32.1: Visualize and distribute different types of bot and non-bot attributes (TikTok).

- **Distribution of LikedAverageNumberOfHashtags, LikedAverageNumberOfComments,LikedAverageNumberOfLikes,LikedAverageNumberOfLinkedProfiles, LikedAverageNumberOfViews by bot and non-bot:**

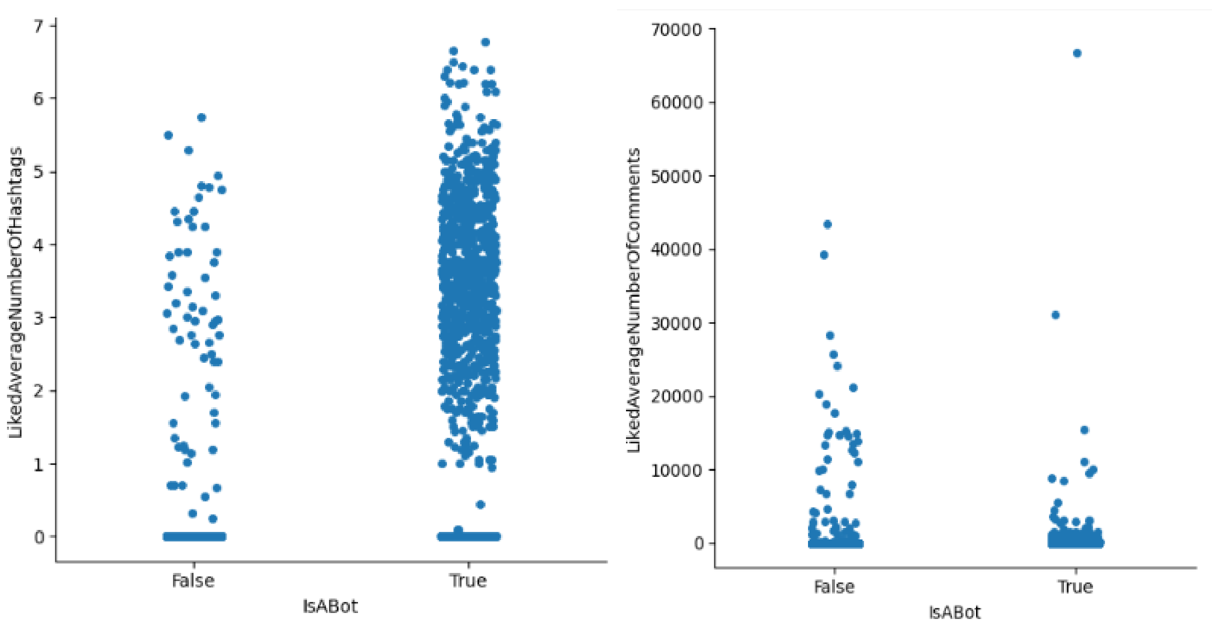

Figure 4.3.33: Visualize and distribute different types of bot and non-bot attributes (TikTok).

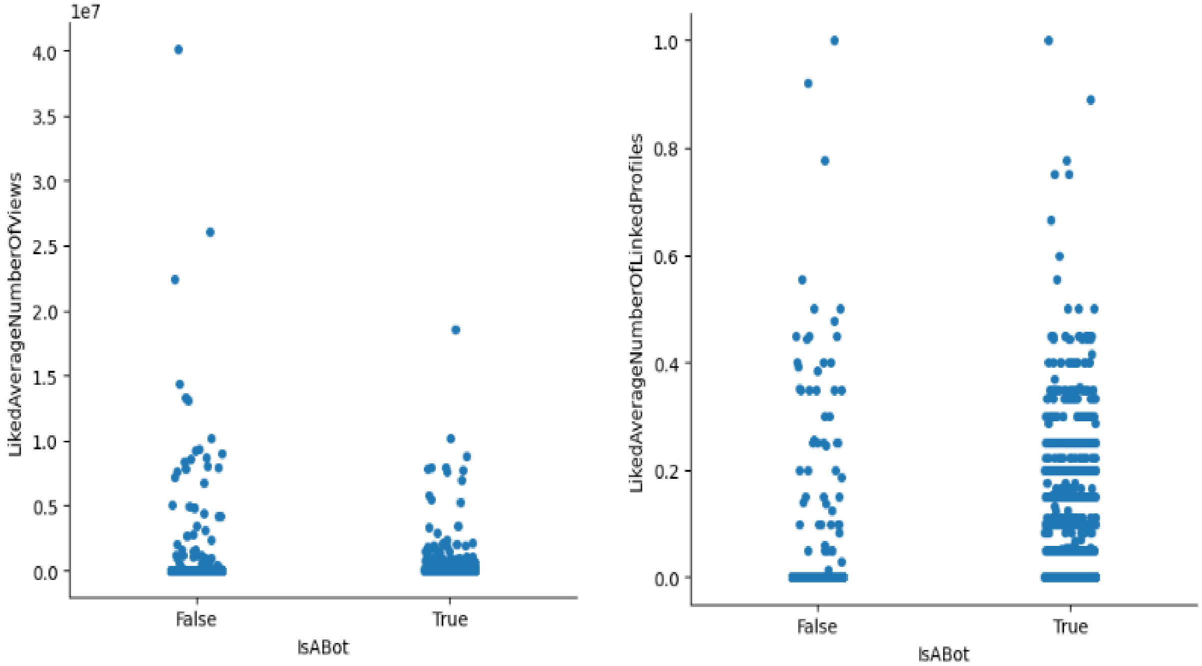

Figure 4.3.33.1: Visualize and distribute different types of bot and non-bot attributes (TikTok).

- **Distribution of AverageNumberOfHashtags, AverageNumberOfComments, AverageNumberOfCharacters, AverageNumberOfLinkedProfiles, AverageNumberOfUsedFilters, AverageNumberOfViews by bot and non-bot:**

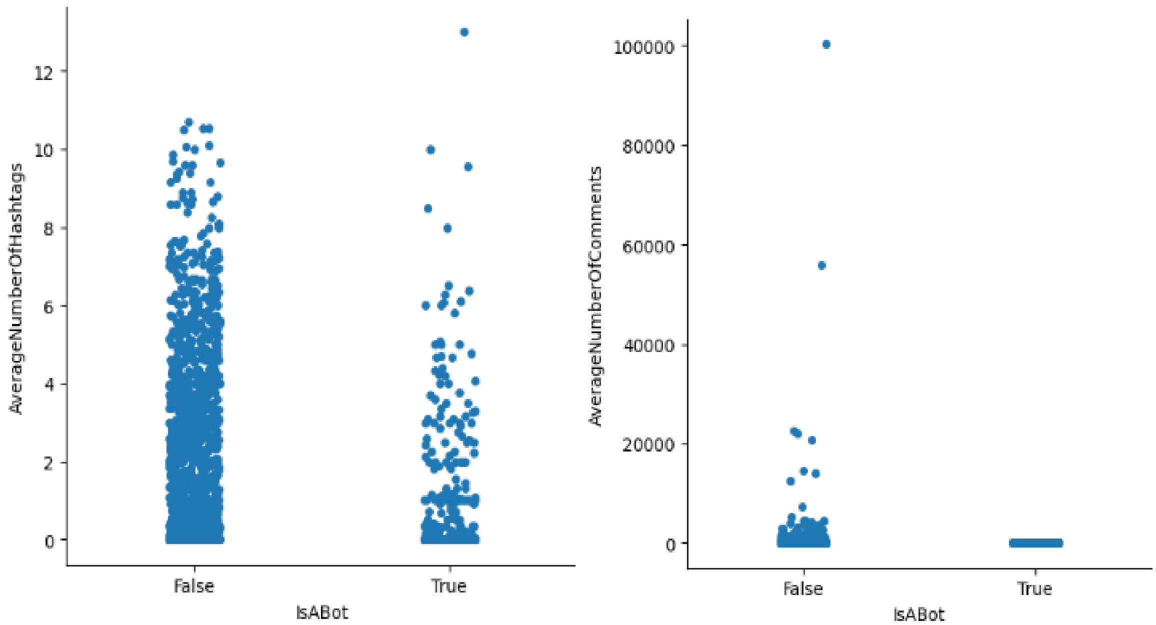

Figure 4.3.34: Visualize and distribute different types of bot and non-bot attributes (TikTok).

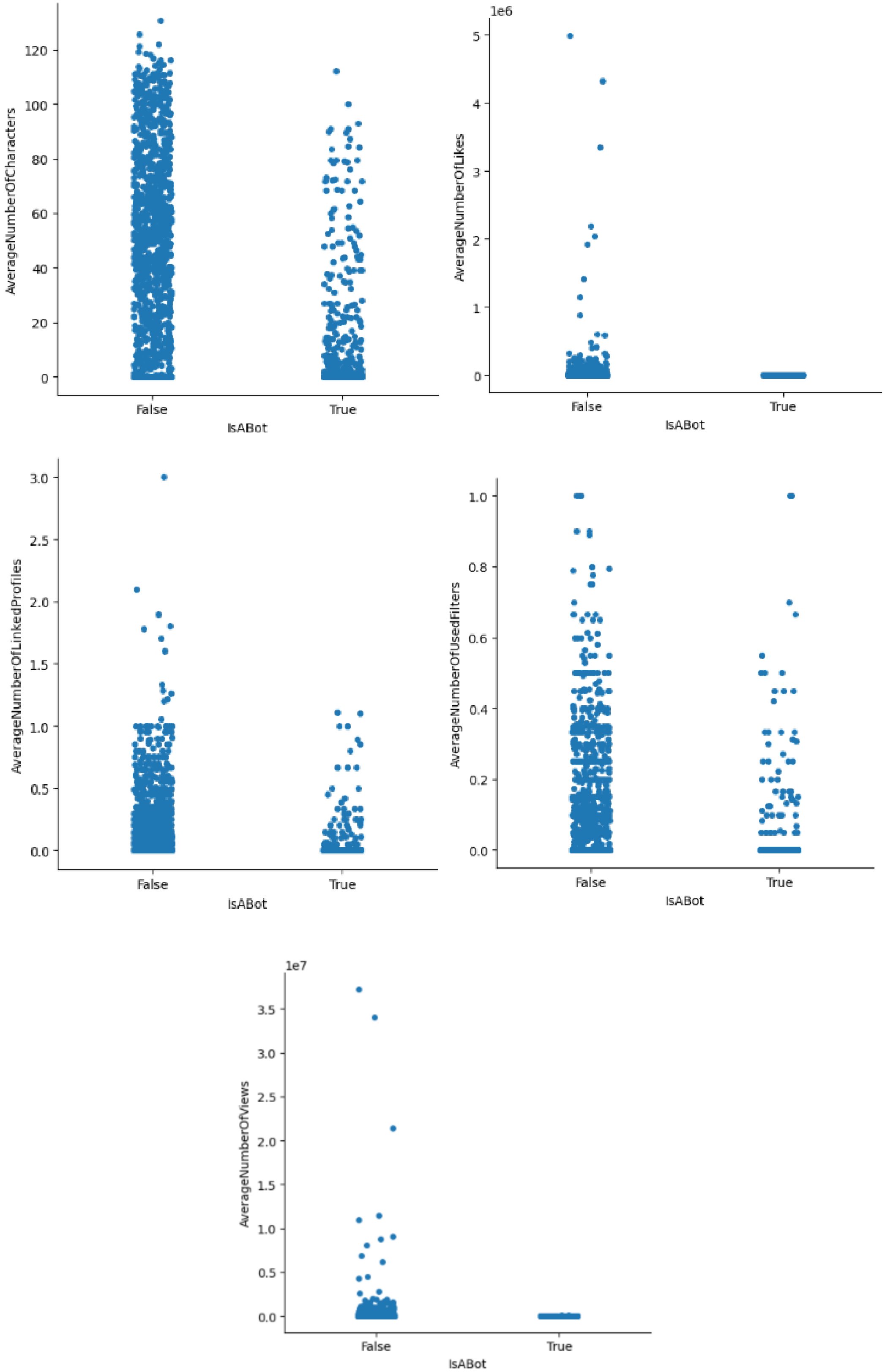

Figure 4.3.34.1: Visualize and distribute different types of bot and non-bot attributes (TikTok).

- **k-nearest neighbors classification algorithm result, Accuracy, Confusion Matrix, Classification Report:**

```
Accuracy: 0.944153577661431

Confusion Matrix:
[[264  13]
 [ 19 277]]

Classification Report:
              precision    recall  f1-score   support

       False       0.93      0.95      0.94       277
        True       0.96      0.94      0.95       296

    accuracy                           0.94       573
   macro avg       0.94      0.94      0.94       573
weighted avg       0.94      0.94      0.94       573
```

Figure 4.3.35: k-nearest neighbors classification algorithm result (Model-1)

- **Random forest classifier Accuracy, Confusion Matrix, Classification Report:**

```
Accuracy: 0.9721
Precision: 0.9791
Recall: 0.9656
F1 Score: 0.9723

Confusion Matrix:
[[276   6]
 [ 10 281]]

Classification Report:
              precision    recall  f1-score   support

           0       0.97      0.98      0.97       282
           1       0.98      0.97      0.97       291

    accuracy                           0.97       573
   macro avg       0.97      0.97      0.97       573
weighted avg       0.97      0.97      0.97       573
```

Figure 4.3.36: Random forest classifier result (Model-2).

- **Decision Tree Classifier Accuracy, Confusion Matrix, Classification Report:**

```
Confusion Matrix:
[[259  18]
 [  9 287]]
Accuracy: 95.29%
Precision: 94.10%
Recall: 96.96%
F1 Score: 95.51%
```

Figure 4.3.37: Random forest classifier result (Model-3).

- **XGBoost classifier Accuracy, Confusion Matrix, Classification Report:**

```
Accuracy: 0.97
Confusion Matrix:
 [[268   9]
 [  9 287]]
Classification Report:
               precision    recall  f1-score   support

       False       0.97      0.97      0.97       277
        True       0.97      0.97      0.97       296

    accuracy                           0.97       573
   macro avg       0.97      0.97      0.97       573
weighted avg       0.97      0.97      0.97       573
```

Figure 4.3.38: XGBoost classifier result (Model-4).

- **Neural Networks classification Accuracy, Confusion Matrix, Classification Report:**

```
Test Loss: 0.1555, Test Accuracy: 0.9511
18/18 [==============================] - 0s 2ms/step

Confusion Matrix:
[[268  14]
 [ 12 279]]

Classification Report:
              precision    recall  f1-score   support

           0       0.96      0.95      0.95       282
           1       0.95      0.96      0.96       291

    accuracy                           0.95       573
   macro avg       0.95      0.95      0.95       573
weighted avg       0.95      0.95      0.95       573
```

Figure 4.3.39: Neural Networks classification result (Model-5).

- **Compare the accuracy of multiple models:**

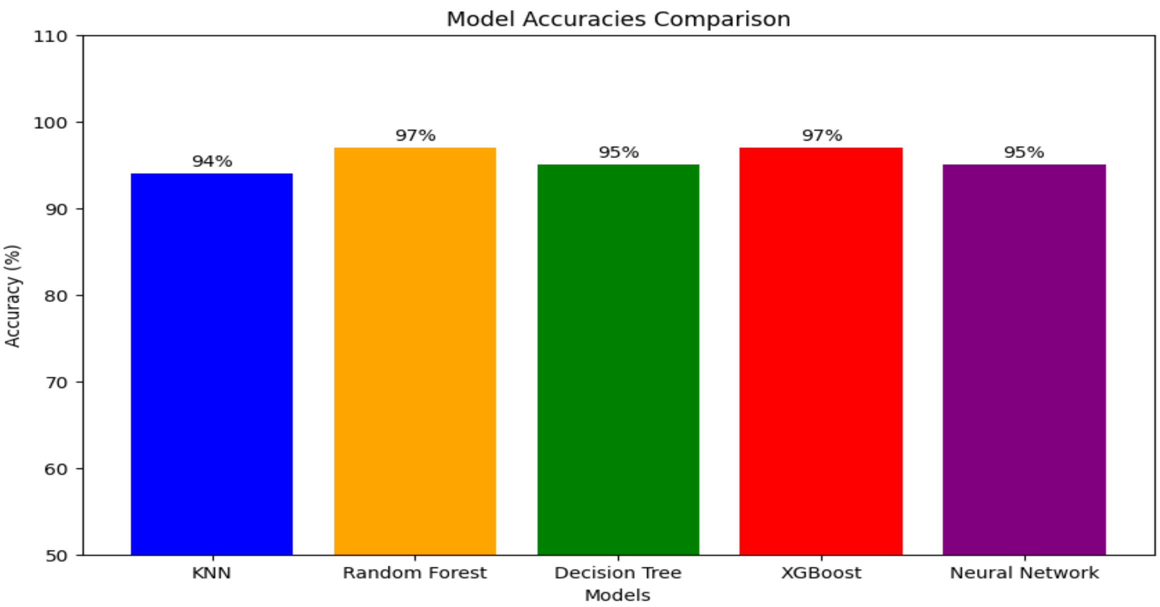

Figure Figure 4.3.40: Compare the accuracy all model (TikTok).

4.4 Summary

The research has successfully developed a robust, accurate, and efficient bot detection system for social media platforms. The system uses supervised machine learning algorithms like K-Nearest Neighbors, Random Forest, Decision Tree, XGBoost, and Neural Network to accurately distinguish between bots and human users. The system undergoes rigorous training, hyperparameter tuning, cross-validation, and iterative improvements to ensure high accuracy and reliability. The system's adaptability is verified through new data testing and stress testing. The implementation phase has demonstrated the system's practicality and effectiveness, making it a reliable tool for enhancing security and user safety on social media platforms.

CHAPTER 5

Result and analysis

5.1 Overview

In this chapter, we delve into a comprehensive exploration of the results and analysis stemming from our research on social media bot detection using advanced supervised machine learning techniques. The core focus of our study is to systematically present and evaluate the outcomes derived from extensive experiments conducted across prominent platforms such as Twitter, TikTok, and Instagram. Our primary objective is to rigorously assess the performance of various machine learning algorithms in effectively identifying bot accounts within these dynamic and evolving social media landscapes. Social media platforms have become integral components of modern communication, commerce, and social interaction. However, the pervasive presence of automated accounts, or bots, poses significant challenges to the authenticity and integrity of these platforms. Bots are programmatically controlled accounts designed to simulate human behavior, often with the intent to manipulate public opinion, amplify certain content, or engage in malicious activities such as spamming and spreading misinformation. Detecting and mitigating the influence of such bots is crucial for maintaining the trustworthiness and reliability of social media environments. Our research contributes to this critical area by conducting a rigorous evaluation of supervised machine learning algorithms tailored specifically for bot detection. Through a series of meticulously designed experiments, we analyze and compare the efficacy of these algorithms in accurately distinguishing between bot and legitimate user accounts across diverse social media platforms. By doing so, we aim to provide empirical evidence of our proposed system's effectiveness while shedding light on its inherent strengths and limitations. Furthermore, this analysis not only serves to validate the practical applicability of our approach but also offers valuable insights into potential enhancements and future directions for refining bot detection methodologies. By examining the nuances of our experimental results, we seek to underscore the significance of our research in bolstering the security and trustworthiness of social media ecosystems. Our findings are intended to inform and empower stakeholders—from platform administrators to cybersecurity experts and policymakers—by equipping them with actionable intelligence to combat the pervasive threat posed by social media bots.

5.2 Experimental Result

- Here my (Instagram) Performance Metrics for Bot Detection Algorithms:

TABLE 5.2.1: PERFORMANCE METRICS ALL MODEL (INSTAGRAM).

Algorithm	Accuracy	Precision	Recall	F1-Score
KNN	0.91	0.92	0.93	0.92
Random Forest	0.95	0.97	0.95	0.96
Decision Tree	0.92	0.96	0.91	0.93
XGBoost	0.95	0.98	0.93	0.95
Neural Network	0.96	0.96	0.97	0.96

- Here my (Twitter) Performance Metrics for Bot Detection Algorithms:

TABLE 5.2.2: PERFORMANCE METRICS ALL MODEL (TWITTER).

Algorithm	Accuracy	Precision	Recall	F1-Score
KNN	0.87	0.86	0.88	0.87
Random Forest	0.91	0.90	0.90	0.91
Decision Tree	0.89	0.90	0.88	0.89
XGBoost	0.90	0.90	0.89	0.90
Neural Network	0.82	0.79	0.86	0.82

- Here my (TikTok) Performance Metrics for Bot Detection Algorithms:

TABLE 5.2.3: PERFORMANCE METRICS ALL MODEL (TIKTOK).

Algorithm	Accuracy	Precision	Recall	F1-Score
KNN	0.94	0.96	0.94	0.95
Random Forest	0.97	0.98	0.97	0.97
Decision Tree	0.95	0.94	0.97	0.96
XGBoost	0.97	0.97	0.97	0.97
Neural Network	0.95	0.95	0.96	0.95

The analysis of bot detection algorithms on Instagram, Twitter, and TikTok reveals that Random Forest and XGBoost consistently outperform in terms of accuracy, recall, and F1-Score. KNN and Decision Tree also show good performance, with KNN having the highest recall. However, Decision Tree shows slightly lower accuracy compared to Random Forest and XGBoost but maintains a well-balanced F1-Score. Twitter, Random Forest consistently achieves high scores across all metrics, indicating its robustness. KNN and XGBoost also perform well, with accuracy above 0.87. However, Neural Network shows comparatively lower performance, especially in precision and recall. Decision Tree maintains consistent performance, aligning closely with other algorithms but trailing in precision. TikTok, Random Forest and XGBoost lead in accuracy, precision, recall, and F1-Score. KNN and Decision Tree also perform exceptionally well, showing high accuracy and balanced precision and recall. Neural Network, while still performing well, is relatively lower compared to Random Forest and XGBoost.

Overall, Random Forest and XGBoost consistently show strong performance across all three platforms, indicating their general effectiveness in bot detection. However, there are slight variations in their effectiveness across different platforms, suggesting that platform-specific nuances may influence algorithm performance. Further investigation into the specific challenges of bot detection on Twitter may be warranted.

5.3 Performance / Comparative Analysis

As a researcher examining the performance metrics of bot detection algorithms on Instagram, Twitter, and TikTok datasets, several key insights emerge: Instagram account bot detection Algorithmic Dominance: Random Forest and XGBoost consistently outperform other algorithms on Instagram, showcasing their effectiveness in accurately identifying bot accounts. Neural Network Consistency: The Neural Network maintains a high level of performance across various metrics, suggesting its reliability in bot detection tasks on Instagram. Twitter account Trade-offs in Performance Twitter poses a more challenging environment, reflected in the balanced tradeoff between precision and recall for Random Forest and XGBoost. The Neural Network also demonstrates a balanced approach. Algorithmic Moderation: While accuracy varies, the algorithms maintain a reasonable balance between correctly identifying bots and minimizing false positives/negatives. TikTok account Overall Excellence all algorithms perform exceptionally well on TikTok, with Random Forest and XGBoost leading the way. This indicates their robustness in handling the unique characteristics of TikTok data for bot detection. Consistency across Metrics Neural Network maintains consistent performance across precision, recall, and F1-Score, highlighting its generalizability.

5.4 Summary

My study on social media bot detection shows crucial insights. The consistent excellence of Random Forest and XGBoost underlines their reliability across platforms. However, the platform-specific adaptability of algorithms emphasizes the need for tailored approaches. Twitter's unique challenges necessitate a balanced precision-recall trade-off. The Neural Network's consistent performance showcases its adaptability, while ongoing refinement remains crucial for addressing evolving bot detection challenges. Practically, precise bot detection enhances platform security and user trust. The findings set the groundwork for future research, helping exploration into ensemble approaches and advanced techniques for improved detection models. Ultimately, the study contributes to a nuanced knowledge of bot detection behavior in a changing area of social media.

CHAPTER 6

Impact on society, environment and sustainability

6.1 Impact on Life

In the pursuit of effective social media bot detection, understanding the broader social impact of my research is paramount. By unraveling the implications of automated accounts on social networks, I aim to recognize its potential to significantly influence user experiences, fortify platform credibility, and shape the overall online environment. This research endeavors to contribute valuable insights into mitigating the adverse effects of social spam and enhancing the authenticity and trustworthiness of online interactions.

6.2 Impact on Society & Environment:

- My research results demonstrate a notable enhancement in user trust and safety. Users are less susceptible to manipulative bot activities, promoting a more secure online environment.
- The research outcomes contribute to fortifying platform credibility through accurate bot detection. Authentic user engagement is promoted, receiving genuine interactions and advertisers.
- The research findings play a pivotal role in minimizing the distribution of false news and misinformation. Users experience a cleaner, more reliable online information environment.
- My research introduces advanced detection mechanisms, optimizing resource allocation. Platforms benefit from improved server efficiency and reduced energy consumption.

6.3 Ethical Aspects

- Ethical considerations underscore my commitment to prioritizing user privacy and data security. My research ensures responsible handling of sensitive information, minimizing risks.
- Ethical practices are embedded in my bot detection methods, mitigating the inadvertent removal of legitimate users. Striking a delicate balance between accuracy and user inclusivity remains a cornerstone of our ethical approach.

6.4 Sustainability Plan

Ensuring the sustainability of our social media bot detection system involves continuous improvement, environmental responsibility, and community engagement. We will regularly update and enhance our algorithms to keep pace with evolving bot behaviors and social media trends. By leveraging community feedback and collaborating with industry experts, we aim to refine our methods and stay at the forefront of technological advancements. Additionally, we commit to optimizing our system's resource usage, reducing energy consumption, and promoting eco-friendly practices. This comprehensive approach ensures the long-term effectiveness and minimal environmental impact of our research, fostering a more secure and trustworthy online environment.

6.5 Summary

The social impact of my research results is profound. From fortifying user trust and safety to minimizing information pollution and upholding ethical standards, the implications resonate across the digital landscape. As my findings contribute to a more resilient and ethical online environment, my research recognize the enduring impact of advancing bot detection for the benefit of users and the broader digital community.

CHAPTER 7

Conclusion and future work

7.1 Conclusion

In this study, my aimed to identify bots and non-bots accounts on Instagram, Twitter and TikTok using supervised machine learning algorithm. My project aims to identify bots. The first contribution of my study was to present a publicly available balanced dataset for the identification of bots and non-bots accounts on Instagram, Twitter and TikTok to researchers But TikTok there are very few data sets due to the new platform. Applying different preprocessing steps to this collected data set, I am constructed prediction models with machine learning classification algorithms and reported the prediction performance of these models. Random Forest and XGBoost come out as the top-performing algorithms across Instagram, Twitter, and TikTok, consistently achieving high accuracy levels. Random Forest stands out on Instagram, Twitter, and TikTok for all accuracy in showcasing its robustness in bot detection. But challenges on Twitter presents unique challenges, and Neural Network performs slightly lower, its balanced precision-recall trade-off reflects adaptability in a dynamic Twitter environment. Decision Tree achieves noteworthy accuracy across platforms, with a standout performance of 95% on TikTok. KNN exhibits competitive performance, achieving 94% accuracy on TikTok. The study provides insights into bot detection algorithms' efficiency, practical advice for choosing models, and ethics considerations for responsible online practices in the ever-changing social media. Next study compared the differences accounts behavioral characteristics between bot users and non-bots users. In social media and further explained all model results of differentiation.

7.2 Future Suggested Work

In the future, we can implement a Web service for example API to enable the research community to execute bots-level detection using it. Explore advanced deep learning architectures like RNNs or transformers for more intricate pattern recognition. Investigate Random Forest, XGBoost, KNN, Decision Tree, and Neural Network can yield even more robust and accurate bot detection models. Future study may classify social media user account profile photos using image processing, collect data using API, and work on larger-scale data.However, detection of Twitter bots is still needed due to the problem of vote detection. Twitter has the most bot accounts, and it's only increasing day by day. And other social media accounts will be worked on in the future.

7.3 Limitations / Conflict of Interests

The study on bot detection on Instagram, Twitter, and TikTok has made significant progress using supervised machine learning algorithms. However, there are limitations and potential conflicts of interest. The availability of balanced datasets varied significantly across platforms, with TikTok having limited publicly available datasets. The study focused primarily on Random Forest and XGBoost, which showed high accuracy in bot detection. Platform-specific challenges, such as Twitter's dynamic nature, posed unique challenges for certain algorithms. Ethical considerations regarding user privacy, algorithm bias, and potential unintended consequences of automated bot detection systems must be carefully addressed. The study acknowledges the reliance on datasets and tools from various social media platforms, potentially introducing biases or limitations based on platform policies, access to data, or dependencies on third-party tools. Future research directions may involve more advanced deep learning architectures and larger-scale datasets, but may require careful consideration of ethical guidelines and data privacy regulations. These limitations and conflicts of interest highlight the ongoing challenges and complexities in social media bot detection, urging continuous refinement and ethical scrutiny in future research endeavors.

References:

[1] Mohammad, S., Khan, M. U., Ali, M., Liu, L., Shardlow, M., & Nawaz, R. (2019, July). Bot detection using a single post on social media. In *2019 third world conference on smart trends in systems security and sustainablity (WorldS4)* (pp. 215-220). IEEE

[2] Gannarapu, S., Dawoud, A., Ali, R. S., & Alwan, A. (2020, November). Bot detection using machine learning algorithms on social media platforms. In *2020 5th International Conference on Innovative Technologies in Intelligent Systems and Industrial Applications (CITISIA)* (pp. 1-8). IEEE

[3] Singh, A. P., & Dutta, M. (2019). Spam Detection in Social Networking Sites using Artificial Intelligence Technique. *International Journal of Innovative Technology and Exploring Engineering (IJITEE), ISSN: 2278–3075*, *8*(8S3). IEEE

[4] Ümmü, T. U. N. Ç., Atalar, E., Gargi, M. S., & AYDIN, Z. E. (2022). Classification of Fake, Bot, and Real Accounts on Instagram Using Machine Learning. *Politeknik Dergisi*, 1-1. IEEE

[5] Alzahrani, S., Gore, C., Salehi, A., & Davulcu, H. (2018). Finding organizational accounts based on structural and behavioral factors on twitter. In *Social, Cultural, and Behavioral Modeling: 11th International Conference, SBP-BRiMS 2018, Washington, DC, USA, July 10-13, 2018, Proceedings 11* (pp. 164-175). Springer International Publishing.

[6] Loyola-González, O., Monroy, R., Rodríguez, J., López-Cuevas, A., & Mata-Sánchez, J. I. (2019). Contrast pattern-based classification for bot detection on twitter. *IEEE Access*, *7*, 45800-45817.

[7] Yang, K. C., Varol, O., Hui, P. M., & Menczer, F. (2020, April). Scalable and generalizable social bot detection through data selection. In *Proceedings of the AAAI conference on artificial intelligence* (Vol. 34, No. 01, pp. 1096-1103). IEEE

[8] Davis, C. A., Varol, O., Ferrara, E., Flammini, A., & Menczer, F. (2016, April). Botornot: A system to evaluate social bots. In *Proceedings of the 25th international conference companion on world wide web* (pp. 273-274).

[9] Cai, M., Luo, H., Meng, X., & Cui, Y. (2022). Differences in behavioral characteristics and diffusion mechanisms: A comparative analysis based on social bots and human users. *Frontiers in Physics*, *10*, 875574.

[10] Varol, O., Ferrara, E., Davis, C., Menczer, F., & Flammini, A. (2017, May). Online human-bot interactions: Detection, estimation, and characterization. In *Proceedings of the international AAAI conference on web and social media* (Vol. 11, No. 1, pp. 280-289).

[11] Madahali, L., & Hall, M. (2020, June). Application of the Benford's law to Social bots and Information Operations activities. In *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)* (pp. 1-8). IEEE.

[12] Shen, F., Zhang, E., Zhang, H., Ren, W., Jia, Q., & He, Y. (2023). Examining the differences between human and bot social media accounts: A case study of the Russia-Ukraine War. *First Monday*.

[13] Steel, B., Parker, S., & Ruths, D. (2023). The Invasion of Ukraine Viewed through TikTok: A Dataset.

[14] Yang, K. C. (2023). *Social Media Bots: Detection, Characterization, and Human Perception* (Doctoral dissertation, Indiana University). IEEE

[15] Xiao, C., Freeman, D. M., & Hwa, T. (2015, October). Detecting clusters of fake accounts in online social networks. In *Proceedings of the 8th ACM Workshop on Artificial Intelligence and Security* (pp. 91-101).

[16] Boser, B. E., Guyon, I. M., & Vapnik, V. N. (1992, July). A training algorithm for optimal margin classifiers. In *Proceedings of the fifth annual workshop on Computational learning theory* (pp. 144-152).

[17] Kalameyets, M. (2021). *Algorithms and techniques for bot detection in social networks* (Doctoral dissertation, Université Paul Sabatier-Toulouse III; ITMO University). IEEE

[18] Aljabri, M., Zagrouba, R., Shaahid, A., Alnasser, F., Saleh, A., & Alomari, D. M. (2023). Machine learning-based social media bot detection: A comprehensive literature review. *Social Network Analysis and Mining*, *13*(1), 20.

[19] Zhang, W., & Sun, H. M. (2017, January). Instagram spam detection. In *2017 IEEE 22nd Pacific Rim International Symposium on Dependable Computing (PRDC)* (pp. 227-228). IEEE.

[20] Purba, K. R., Asirvatham, D., & Murugesan, R. K. (2020). Classification of instagram fake users using supervised machine learning algorithms. *International Journal of Electrical and Computer Engineering*, *10*(3), 2763.

[21] Rao, S., Verma, A. K., & Bhatia, T. (2021). A review on social spam detection: challenges, open issues, and future directions. *Expert Systems with Applications*, *186*, 115742.

[22] Van Der Walt, E., & Eloff, J. (2018). Using machine learning to detect fake identities: bots vs humans. *IEEE access*, *6*, 6540-6549.

[23] Shao, C., Ciampaglia, G. L., Varol, O., Yang, K. C., Flammini, A., & Menczer, F. (2018). The spread of low-credibility content by social bots. *Nature communications*, *9*(1), 1-9.

A MULTI-PERSPECTIVE APPROACH UTILIZING SUPERVISED MACHINE LEARNING ALGORITHMS FOR EFFECTIVE SOCIAL MEDIA BOT DETECTION

ORIGINALITY REPORT

14%	8%	5%	8%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Daffodil International University Student Paper	4%
2	dergipark.org.tr Internet Source	1%
3	Sainath Gannarapu, Ahmed Dawoud, Rasha S. Ali, Ali Alwan. "Bot Detection Using Machine Learning Algorithms on Social Media Platforms", 2020 5th International Conference on Innovative Technologies in Intelligent Systems and Industrial Applications (CITISIA), 2020 Publication	1%
4	Submitted to University of Hertfordshire Student Paper	1%
5	Wuxain Zhang, Hung-Min Sun. "Instagram Spam Detection", 2017 IEEE 22nd Pacific Rim International Symposium on Dependable Computing (PRDC), 2017 Publication	1%