DETECTION OF SYBIL ATTACKS IN ONLINE SOCIAL NETWORKS

Student Name: Muhammad Taha Yousaf
Enrollment No. 01-243212-014
Supervisor: Dr. Saba Mahmood

A thesis submitted in fulfilment of the requirements for the award of degree of Masters of Science (Computer Science)

Department of Computer Science

BAHRIA UNIVERSITY ISLAMABAD

November 2023

Approval of Examination

Scholar Name: Muhammad Taha Yousaf
Registration Number:
Enrollment: 01-243212-014
Program of Study: Masters in Computer Science
Thesis Title: Detection of Sybil Attacks in Online Social Networks

It is to certify that the above scholar's thesis has been completed to my satisfaction and, to my belief, its standard is appropriate for submission for examination. I have also conducted plagiarism test of this thesis using HEC prescribed software and found similarity index 15%. that is within the permissible limit set by the HEC for the MS/M.Phil degree thesis. I have also found the thesis in a format recognized by the BU for the MS/M.Phil thesis.

Principal Supervisor Name: Dr Saba Mahmood
Principal Supervisor Signature:
Date:

Author's Declaration

I, Muhammad Taha Yousaf hereby state that my MS/M.Phil thesis titled "Detection of Sybil attacks in Online Social Networks" is my own work and has not been submitted previously by me for taking any degree from Bahria university or anywhere else in the country/world. At any time if my statement is found to be incorrect even after my graduation, the University has the right to withdraw/cancel my MS/M.Phil degree.

Name of Scholar: Muhammad Taha Yousaf

Date: 28th Octuber, 2023

Plagiarism Undertaking

I, solemnly declare that research work presented in the thesis titled "Detection of Sybil attacks in Online Social Networks" is solely my research work with no significant contribution from any other person. Small contribution / help wherever taken has been duly acknowledged and that complete thesis has been written by me. I understand the zero tolerance policy of the HEC and Bahria University towards plagiarism. Therefore I as an Author of the above titled thesis declare that no portion of my thesis has been plagiarized and any material used as reference is properly referred / cited.

I undertake that if I am found guilty of any formal plagiarism in the above titled thesis even after award of MS/M.Phil degree, the university reserves the right to withdraw / revoke my MS/M.Phil degree and that HEC and the University has the right to publish my name on the HEC / University website on which names of scholars are placed who submitted plagiarized thesis.

Name of Scholar: Muhammad Taha Yousaf

Date: 12 September, 2023

Dedication

I dedicated my thesis to my parents for their endless love, support and encouragement throughout my pursuit for education. I hope this achievement with fulfill the dream they envisioned for me.

Acknowledgements

In preparing this thesis, I was in contact with many people, researchers, academicians, and practitioners. They have contributed towards my understanding and thoughts. In particular, I wish to express my sincere appreciation to my main thesis supervisor, Dr. Saba Mahmood , for encouragement, critics, and guidance. I am also very thankful to my supervisor for their guidance, advices and motivation. Without their continued support and interest, this thesis would not have been the same as presented here.

Librarians at Bahria University also deserve special thanks for their assistance in supplying the relevant literatures. My fellow postgraduate students should also be recognised for their support. My sincere appreciation also extends to all my colleagues and others who have provided assistance at various occasions. Their views and tips are useful indeed.

Abstract

Online social networks (OSNs) like Facebook and Twitter have become increasingly popular, offering a wide range of virtual interaction techniques and real-world social connections. The users of social media increasing day-by-day, these networks are expected to expand as mobile device usage and mobile social networks become more popular. However, Sybil attacks are a growing security issue in OSNs, where attackers use various methods to target large populations, creating fake identities and accessing networks. We carried out the comparison between "Content based", and "user behavior based and graph based hybrid approach" to detect the Sybil's attacks in OSNs. For user behavior and graph based approach, we extract the features from dataset and then find the behavior-similarities between the nodes and find the betweenness centrality between nodes. Behavior similarities values assigned to the edges as weights. and betweenness centrality value assigned to nodes. To detect Sybil nodes we define the threshold 20%, the behavior similarities value less then the threshold value, the edge become a Sybil edge whereas the to detect sybil nodes, the value of betweenness centrality less the threshold, the node become a Sybil node. For content based approach, we detect Sybil nodes in OSNs.Content based approach utilizes Machine Learning algorithms suc as Naive Basiyan, Multi Laye precepton, KNN, Random Forest, Logistic regression, SVC and ADA Boost. The Random Forest Algorithms perform well from all these algorithms to identifies Sybil nodes with high accuracy, precision and recall. we compared these two approaches to identify the attack edges and sybil nodes in social networks and the results revealed that the user behavior based and graph based hybrid technique perform well in term to identify the Sybil attacks with accuracy of 98.87%.

TABLE OF CONTENTS

LIST OF TABLE

LIST OF FIGURE

LIST OF SYMBOLS

$\mathcal{D}$, d	–	Diameter
$\mathcal{F}$	–	Force
g	–	Gravity=9.81
I	–	Moment of inertia
l	–	Length
m	–	Mass
$\mathcal{N}$	–	Rotational Velocity
$\mathcal{P}$	–	Pressure
$\mathcal{Q}$	–	Volumetric flow rate
r	–	Radius
$\mathcal{T}$	–	Torque
$\mathcal{R}$e	–	Reynold number
$\mathcal{V}$	–	Velocity
w	–	Angular velocity
x	–	Displacement
z	–	Height
θ	–	Angle
ρ	–	Density

CHAPTER 1

INTRODUCTION

In recent years, online social networks (OSNs) such as Facebook and Twitter have become significant popularity. OSNs are built on real-world social connections and provide a plethora of virtual-interaction strategies for its users[1]. The estimated 3.96 billion users of social networking sites in 2022 are still expected to increase as mobile device usage and mobile social networks gain popularity. The most popular social networks usually support a wide range of languages, allowing users to communicate with friends and other users across national, political, and geographical boundaries[2].

Social networks are have become grow day by day, Sybil attacks are more popular security issue in OSN. Sybil attacker use different methods to target the huge number of population in social networks. In Sybil attack, attacker can create single node to create multiple fake identities simultaneously, use to access target networks and do malicious activity against the target identity[3]. Sybil Attacks can have significant consequences. They may result in the development of echo chambers, which are closed groups where incorrect or extreme viewpoints are reinforced, distorting public dialogue[4].

There are two types of user, normal users and sybil users in OSN. The normal users are those user who are active in OSN (like facebook, twitter users) and the Sybil user are those who can create multiple accounts using one node and can do malicious activity against the normal user. First attacker can send request to normal user, once user accept attacker request, edge is formed between user node and Sybil node then they theft of personal information as shown in figure 1. In order to make social networks more secured, reliable, and effective, researchers should focus on the detection of Sybil's attacks in OSN's.

In this paper we introduced the comparison between the content based and "Users-behavior based and graph-based hybrid approach" to identify Sybil attacks in OSNs as shown in figure 2. In user behavior,We discover behavioural patterns such as suggested friends, mutual friends, pages liked, and groups. These behavioural similarities are values that are assigned as edge weights

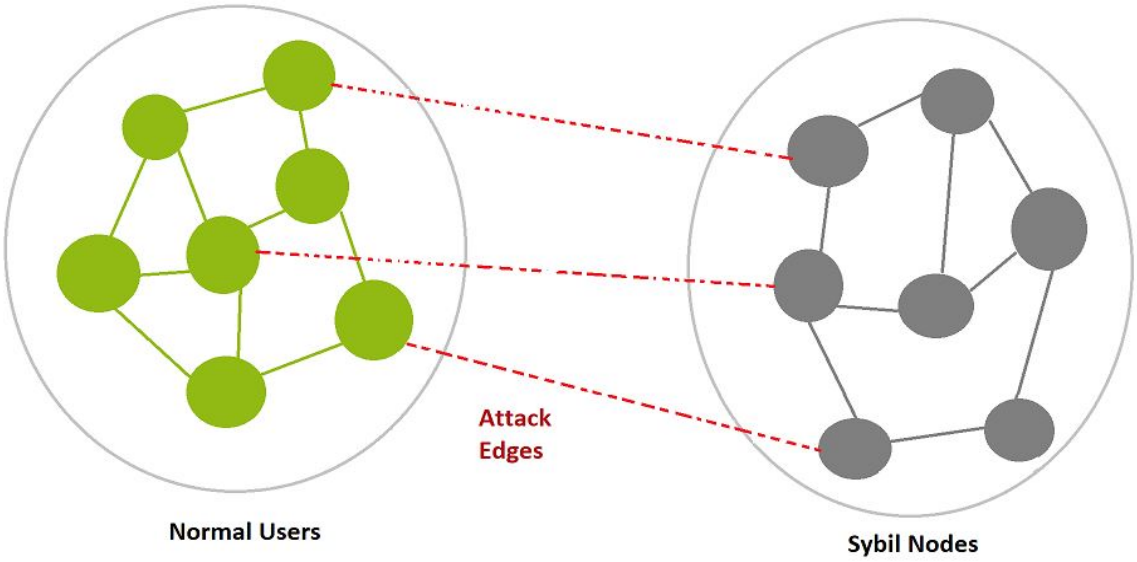

Figure 1.1: Relationship between normal user and Sybil users

to edges. And then find the betweenness-centrality (graph based approach) between the nodes and then identify the Sybil attacks. For content based approach, We extract features from datasets and apply Machine learning algorithm like KNN, Multi layer Precepton, Random forest, Naive Bayesian, SVC and ADA Boost.

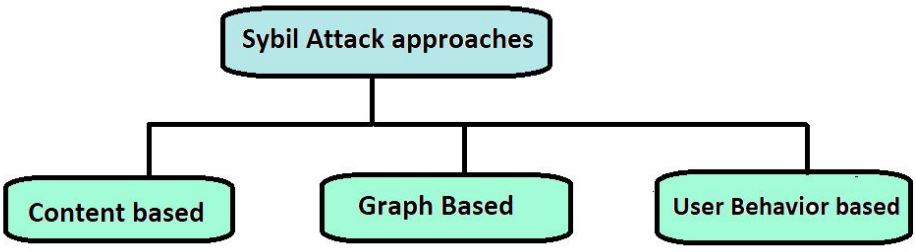

Figure 1.2: Sybil Attack Detection Approaches in OSN

1.1 Problem Analysis

Social networks are the most widely used in this advanced period, and their user base is increasing constantly. Over 4.48 billion people utilise social media, according to a 2021 estimate, with an average user utilising 6.6 social media networks each month. According to a study by [5], over 65.86% of monthly users of popular websites like Facebook check in to use social media every day. Sybil accounts are growing as well. In 2022, phishing attempts and email frauds will be most frequent threats from sybil attackers for both individuals and businesses. Millions of people have been affected by many phishing assaults at the same time, such as the Facebook phishing campaign. The most significant and frequent effects on people are caused by these cybercrimes[6]. The existing method[7] uses a hybrid approach combining user behaviour and graph analysis to identify Sybil's attacks in OSNs with a threshold of 10%. This method has several drawbacks, including a high false rate, poor accuracy score, and assumption-based methodology.

1.2 Research scope and Limitation

As the advanced era methods, the number of users on websites like Facebook, Instagram, Twitter, and others is increasing daily. Sybil's attacks are increasing along with growth of internet websites. Our goal is to detect Sybil attacks in Open Social Networks. We employ a hybrid strategy based on graphs, user behaviour, and content to increase the accuracy of Sybil's identification.

1.3 Motivation

Online social networks play an important role in communication, information sharing, and social interaction, but they are also subject to security risks like Sybil attacks. In order to deceive real users and spread misinformation, spam campaigns, and targeted phishing attacks are all products of these attacks, which involve attackers creating false identities or accounts. Sybil Attacks can have serious consequences, damage trust among users, and result in real harm. We are creating efficient techniques and instruments for spotting and stopping Sybil attacks in order to counter these threats. It is difficult to identify and differentiate between Sybil accounts and actual users due to the dynamic nature of OSNs, user interactions, and attacker methods. The main motivation of this research is to advance cybersecurity, increase security and trustworthiness, and help develop reliable methods for identifying Sybil

attacks.

1.4 Our Contributions

The following are some of our work's major contributions:

- In order to identify Sybil's attacks in OSNs, we examine "users behavior-based and graph-based hybrid approach" and content-based methods. Then we compare these two methods.
- When using content-based methods, we utilise machine learning techniques. The Ml algorithms are Ada boost classifiers, KNN, SVC, naive Bayes, multi-layer perception, logistic regression, and KNN respectively.
- In Content based approach, we apply graph technique (betweenness centrality) and detect the Sybil's nodes in OSNs.
- In the social network graphs, we evaluate the behavioural similarities and determine the attack edges.
- We utilise attack-edge detection and recognition of Sybils attacks by using the betweenness centrality for graph-based approaches.
- We compare our content-based approach to the test with the existing Sybil attack detection algorithms after analysing it on spambot datasets, Congress network datasets, and soc karate datasets. The experimental findings demonstrate the effectiveness of our graph-based hybrid technique using the Soc Karate dataset and user behaviour in detecting Sybil's attacks identification.

1.5 Thesis Organization

The rest of the document is arranged as follows. We address the literature reviews that are relevant to our work in this article in chapter 2. We describe the methodology, and machine learning techniques in Chapter 3. In Chapter 4, we provide the analysis the comparison between our approaches and empirical results from machine learning algorithms and users-behavior and graph-based hybrid approach. Finally, in chapter 5, we conclude our work and discuss the future work.

CHAPTER 2

RELATED WORK

In this chapter of the literature review, we analyze the important subject of Sybil attack detection in OSNs using machine learning, with a focus on the usage of social spambot datasets. Sybil attacks are a typical threat in OSNs when malicious users create several fake identities to interfere with the network's normal operation. It is crucial to recognise and thwart these assaults if we want to maintain the confidence in these platforms.

Due to their accurate portrayal of user behavior and assaults, social spambot datasets have become essential for research into Sybil attack detection. These datasets offer a rich supply of data for training machine learning models since they include elements like user profiles, relationships, and content produced by both genuine users and spambots.They frequently include ground truth labels, facilitating supervised learning techniques, and include a variety of characteristics, boosting model robustness.

For study in this area, well-known social spambot datasets including Cresci-2015, CyberSM, Botometer, and Bot-IoT have been used extensively. Because of the variety of social networks and bot behaviors covered by these datasets, researchers may analyze and create detection algorithms that are specialized for particular environments.Machine learning strategies for detecting Sybil attacks range from supervised methods that make use of labeled data to semi-supervised and unsupervised algorithms that can handle situations with few labeled samples. The development of unique characteristics by researchers to increase the discriminative strength of models is a key component of feature engineering.

Metrics like precision, recall, F1-score, accuracy, and ROC-AUC, which rate several facets of detection efficiency, are used to analyze model performance. Challenges such as data imbalance, generalization, adaptive attackers, and ethical issues still exist, highlighting the necessity for continued study to keep up with emerging threats and protect online social networks.

2.0.1 Sybil's Attacks in Online Social Networks

The integrity and security of OSNs are always under threat from sybil assaults. In order to enter and control the network, hostile persons or organisations establish several phony accounts, frequently made to seem like actual users[8]. The effects of Sybil assaults are extensive, spanning everything from getting an unfair edge and disseminating false information to jeopardizing the network's entire credibility.

In an attempt to solve the issue raised by Sybil's attacks, a significant amount of study has been done, which has led to the examination of several detection and mitigation strategies. Machine learning has become one of these strategies' most efficient methods in thwarting Sybil assaults. Machine learning algorithms have demonstrated potential in spotting patterns and behaviors suggestive of Sybil activity, driven by their capacity to process and analyze enormous amounts of data. These algorithms may successfully differentiate between authentic users and Sybil accounts by utilizing a wide range of data obtained from user profiles, network interactions, and content.

It is important to note, however, that the level of quality and variation of the datasets used for both training and evaluation have a significant impact on how effective machine learning-based methods are. Realistic social network dynamics must be adequately reflected in high-quality datasets that cover a range of scenarios. Datasets including instances of Sybil accounts with ground truth labels for supervised learning as well as authentic user data are very useful.

2.0.2 Characteristics and Importance of Social Spambot Dataset

For the purpose of developing, testing, and benchmarking machine learning models for the detection of Sybil attacks, high-quality datasets must be readily available. The social spambots dataset is one particular kind of dataset that has gained popularity recently. These databases include user profiles, social interactions, and material produced in online social networks by both genuine users and spammers.

2.0.3 Machine Learning Approaches for Sybil Attack Detection

Due to the fact that they're able to find complex trends within large datasets, machine learning techniques have a huge potential for Sybil attack detection. To address the issue, researchers have attempted a variety of solutions, including supervised, semi-supervised, and unstructured methods. Supervised approaches train models using labeled data, allowing them to discriminate be-

Table 2.1: Characteristics and Importance of Social Spambot Datasets

Sr. No.	**Author(s)**	**Characteristics**	**Importance**
1	Lee et al. (2011) [9]	Realistic representation of social network data, including profiles, interactions, and content.	Enables the development of machine learning models for Sybil attack detection using actual data.
2	Stringhini et al. (2015) [10]	Ground truth labels distinguishing between legitimate users and spambots.	Provides labeled data for supervised machine learning, benchmarking, and evaluation.
3	Ferrara et al. (2016) [11]	Diverse set of features, including user attributes, textual content, and network-related information.	Enhances feature diversity for training robust detection models.
4	Varol et al. (2017) [12]	Scalable to adapt to evolving online social networks.	Allows researchers to address the challenges posed by growing and changing social platforms.
5	Davis et al. (2016) [13]	Multiple social media platforms covered (e.g., Twitter) for cross-network analysis.	Facilitates research on Sybil detection across different online social networks.
6	Cresci et al. (2015) [14]	Mixed dataset with both legitimate and spambot accounts.	Allows for the study of spambot behavior in the context of real users, increasing model robustness.
7	Mouti et al. (2020) [15]	Temporal data capturing changes in user behavior over time.	Supports research into detecting evolving Sybil attacks and temporal analysis.
8	Magno et al. (2012) [16]	User-generated content, including text, images, and links.	Provides rich data for content-based analysis and detection.
9	Kumar et al. (2018) [17]	Focus on detecting Sybil attacks in IoT networks.	Offers insights into the detection of spambots operating in unconventional settings.

tween Sybil attackers and legitimate users. Unsupervised algorithms discover abnormalities and suspicious patterns without the requirement for preexisting labels, whereas semi-supervised techniques use both labeled and unlabeled data to increase accuracy. By giving security professionals strong tools to effectively counteract Sybil assaults, these machine learning approaches raise the security and credibility of online social networks.

The Author [7] proposed a method in which detecting Sybil nodes and identifying attack edges in the social network graph using a hybrid technique based on user behaviour and graph theory. The author uses features of behavior to evaluate the strength of connections between nodes. They study user behavior, track patterns of engagement, and find behavior-based characteristics. They make use of attack-edge identification and Sybil node detection by using graph-based structural characteristics (betweenness-centrality). They tested their proposed method to the test using real-world datasets and compared it to other Sybil assault detection methods already in use.
In this work author [18] suggests an approach that makes better use of victim prediction in Sybil detection. To predict victims, they created a victim classifier first. Six innovative features are extracted for the sufferers. These elements, which include user personal information, user behaviour, and message content, all have three dimensions. The edge weights in the graph model are then changed in accordance with the outcomes of the predictions. Next, the graph model is subjected to trust propagation. In order to ensure that most regular users rank higher than Sybil's, we ranked every account in the end.
The authors [19] proposed SybilExposer, a computationally efficient approach for identifying Sybil communities. The first human identification of reliable nodes—which might be difficult for big OSNs—is not necessary when using SybilExposer. Using a range of real-world OSN datasets, we thoroughly evaluate and compare SybilExposer with other cutting-edge algorithms (SybilRank, SybilDefender, and SybilShield). To discern between Sybil and real communities, the SybilExposer technique looks at the intra- and inter-community degrees of each community in the social graph. The method is based on the idea that truthful communities have more intercommunity edges among themselves, while Sybil communities have less intercommunity linkages than honest communities. Random trips that start in honest communities seldom end in Sybil communities because Sybil societies have minimal borders between communities. The algorithm operates in two steps: first, it uses a modified Louvain technique to extract communities from the full network; second, it ranks communities based on the degree correlations that exist both inside and between communities. According to their findings, SybilExposer performs better than

the state-of-the-art in terms of computing costs and efficiency.

The author [20]analyzes several approaches and strategies for efficiently identifying Sybil accounts in OSNs. To identify trends and abnormalities in user behavior and network interactions that may point to the presence of Sybil attackers, it probably looks into machine learning methods, graph analysis, or a mix of the two. Feature extraction from user profiles, activity patterns, or network topologies is frequently used in these strategies. It is impossible to overestimate the significance of precise Sybil detection in OSNs since it has a direct influence on users' experiences, online security, and the entire credibility of these platforms. The study presumably highlights challenges in Sybil detection, including the shifting attack strategies and the requirement for trustworthy evaluation requirements.

In this work, author[21] proposed the hybrid method to evaluating trust for OSNs that the author developed uses dynamic characteristics and similarity is interaction-based and graph-based. The direct trust measure and indirect trust inference are the two steps of the suggested technique. The indirect trust inference phase pre-processes the social network graph and produces the trusted graph, whereas the direct trust measure phase computes the trust scores between each directly linked node in the network. In order to implement the friend request identification and Sybil attack detection apps, the author used the suggested methodologies.

To identify Sybil's in OSNs, the Author[22] suggested a content-based end-to-end classification methodology. The proposed model automatically extracts lower and higher features from the input data using self-normalizing CNN and bidirectional SN-LSTM. The extraction and generation of higher features from the feature map sequence is suggested using a bidirectional SN-LSTM (Self-Normalizing Long Short-Term Memory) network. The MIB dataset, a real-world dataset for the Sybil detection in OSNs, is used to assess the suggested technique. The results of the experiments demonstrate that our model outperforms a number of cutting-edge content-based techniques.

In this article, the authors [23] present a prediction system that may be used to manipulate a deep-learning solution model. Three interconnected modules make up their suggested system: a feature extraction method, a data collecting module, and a deep regression model. Each of these modules performs a thorough analysis and assessment of Twitter user profiles.

SybilTrap is a semi-supervised graph-based learning strategy that preserves the underlying data of both content-based and structure-based methods, according to the author [24]. SybilTrap is designed to work in any context and is resistant to various assault techniques. The performance of SybilTrap was

Table 2.2: Comparison of Sybil Attack Detection

Sr. No.	**Author**	**Methodology**	**Dataset**	**Limitations**
1	Ajethava et al. (2022)[7]	*user behavior-based and graph-based hybrid approach*	Twitter, Weibo	Requires manual labeling of trusted nodes.
2	Zhou et al. (2020)[18]	*Victim prediction to improve Sybil detection accuracy*	Twitter	Requires ground-truth data on victim nodes.
3	Misra et al. (2016)[19]	*SybilExposer to find Sybil communities*	Facebook, Twitter	Does not scale well to large datasets.
4	Bansal et al. (2016)[20]	*Survey of Sybil detection techniques*	Various	Does not provide a comprehensive evaluation of the techniques.
5	Djethava et al. (2022)[21]	*Interaction-based and graph-based hybrid trust evaluation approach*	Twitter	Requires a large amount of training data.
6	Egao et al. (2020)[22]	*Content-based end-to-end classification model*	MIB dataset	Sensitive to the quality of the training data.
7	Al et al. (2018)[24]	*SybilTrap, a semi-supervised learning method based on graphs*	Twitter	Requires a large amount of labeled data.
8	Fal et al. (2018)[23]	*Prediction system for Sybil detection*	Twitter	Requires ground-truth data on Sybil nodes.
9	Mao et al. (2022)[25]	*SybilHunter, a hybrid graph-based Sybil detection approach*	Weibo	Requires a large amount of training data.

assessed on both real and simulated networks. The accuracy of Sybil node identification was increased by using local node properties. To help users identify and respond to interactions according to the kind of social network, the author makes use of social graphs and interactions. Those on the blacklist (LB), on the other hand, are thought to be malevolent; those on the whitelist (LW) have passed rigorous screening and are considered trustworthy. A Sybil node creates as many links as it can that point to trustworthy users in an attempt to penetrate the target online social network. By creating a tonne of beneficial connections with other Sybil nodes, it does this. The attack edge is a representation of the relationship between the whitelist and the blacklist. The system runs on several detection levels, including individual, group, and event levels, and employs particular keywords for current events or social network user identifiers for user profiles.

By collecting user social behaviour patterns, the author[25] proposes SybilHunter, a hybrid graph-based Sybil detection approach. Based on the weighted-strong-social (WSS) graph it creates, SybilHunter constructs Sybil nodes. We assess and replicate our methodology using a Weibo dataset. The weighted-strong-social graph model developed by the authors takes into account both the OSN structure and user activity patterns. It preserves Sybil and benign edges while eliminating numerous attack edges. Graphs and user activity patterns should be combined in order to identify sybils. Based on locally observable user behaviours, the hybrid method computes the trustworthiness of individuals and user pairs, adding it to the OSN structure.

CHAPTER 3

METHODOLOGY

In this chapter, We discuss the specifics of our approach's implementation. A research paper that discusses the identification of Sybil's attacks in OSNs must include a methodology chapter. It explains the methodical approach, methods, and process used to look into, recognise, and find Sybil attacks on OSN's.

3.1 User-behavior and graph-based Hybrid approach and Content base approach framework

In order to identify Sybil attacks in OSNs, we compare two approaches: the "user- behaviour based and graph-based hybrid approach" and the "content-based approach." In Content based approaches, we extract features from dataset1 "The paradigm Shift of socail spambots"[26] and apply ML algorithms. These algorithm is used to identify the Sybil nodes. These ML algorithms are Logistic Regression, Multi-Layer Precepton, Naive Bayesian, SVC kernal and ADA Boost classifier as shown in figure in figure 3.1. The interaction between Sybil account and normal user is that normal user accept friend request of Sybil account and an undirected graph is established between them. Each node have some edges that shows the relation between Sybil node and normal user as shown in figure 1.1. To detect these edges, we use ML Logistic Regression, Multi-Layer Precepton, Naive Bayesian, SVC kernal and ADA Boost classifier respectively.

The Second approach is "user-behaviour based and graph-based hybrid approach" to identify Sybil's nodes and attack edges. For this approach, we use dataset2 "Soc-karate" [27] and dataset3 "Twitter Interaction Network for the US Congress" [28]. In dataset2, We find the behavior similarities using user behavior approach and assigined the weights to the edges between two nodes. And then find the betweenness-centrality for each node using graph

based approach to leverage attack edge identification. The architecture for Machine learning algorithms (Content Based Approach) is shown as figure 3.2.

Dataset3 is directed graph, In this data weight is already assigend to the edges that are calculated by the relations of nodes. then find betweenness-centrailty for each node to leverage attack edge identification.

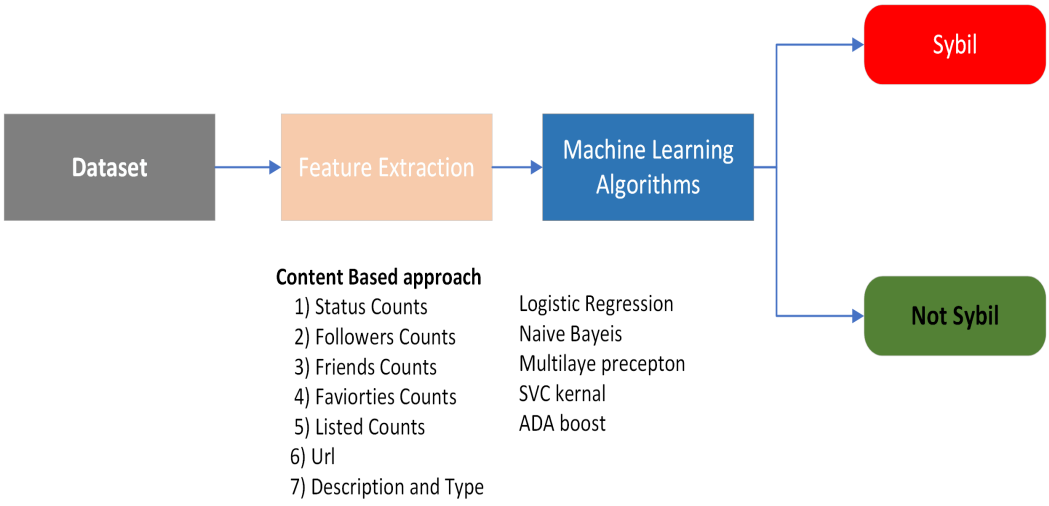

Figure 3.1: The Architecture for Machine Learning Algorithms(Content Based Approach)

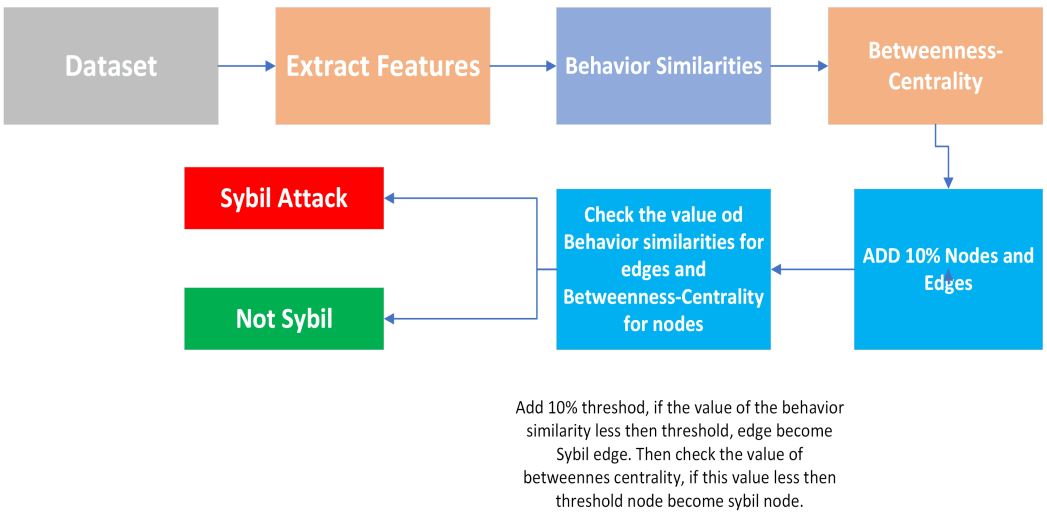

Figure 3.2: Architecture for User-behaviour based and graph based hybrid approach

3.2 User-behaviour based and Graph-based hybrid approach

3.2.1 The Sybil attack detection scheme

Users of online social networks may form groups on sites like Facebook where people with similar interests may gather to participate in several kinds of relevant activities. Attackers are free to join any open Facebook group with the goal of performing malicious activities. There are several methods in the literature for detecting Sybil attacks. However, previous approaches had a number of limitations, such as large false rates, low precesions, and irrational assumptions. Most existing techniques are either behavior or graph-based, and some of them have been proposed to have a small number of features, which leads to poor performance. The Users-behavior based and graph-based hybrid technique that has been developed to identify Sybil attacks in trusted groups like Facebook groups and strengthen their security and reliable. Furthermore, we want to raise the efficiency of the proposed technique, lower false positive rates, and raise the accuracy score. Benign users tend to engage with strangers less frequently, which results in weaker interactions with them. As a result, determining the tie measure's strength may be helpful in locating Sybil assaults in OSNs. To find the behavior-based characteristics, we look at user behaviour and interaction patterns. Based on behavioural similarities, we determine the intensity of links between users and pinpoint attack edges in the network graph. Attack-edge identification and the determination of Sybil nodes are done using a graph-based structural property of nodes called betweenness-centrality.

3.2.2 User behavior and graph based hybrid approach framework

The system architecture of our Sybil detection of attacks approach is described. In the context of the social graph, we provide a graph-based approach technique based on users behaviour to locate Sybil nodes and locate attack edges. We gather information from social media platforms and present it as a graph of social networks, where nodes represent distinct accounts and edges denote connections between them. We examine user behaviour and interaction patterns to identify the behavior-based features. By using the behavioural similarities, we are able to determine the strength of the connections between nodes. By employing the connection-strength metric, we are able to determine the network's attack edges. To determine the strength of the links between nodes, we employ a variety of behaviour factors, such as group-join, likes, pages-likes, suggested friends, and mutual friends. We use betweenness-centrality, a graph-based structural feature, to take advantage of attack-edge identification and find Sybil nodes. Using the pre-defined criterion of 20%,

Table 3.1: Mathemathic Equations and their Description

Sybmbol	Description
$\|V\|, N$	Total nodes in Social Network graph
$\mathrm{V}^i.FL, V^j.FL$	Friend list of nodes $\mathrm{V}^i and V^j$
$\mathrm{V}^i.SL, V^j.SL$	Suggested friends list of node $\mathrm{V}^i and V^j$
$\mathrm{V}^i.LI, V^j.LI$	Likes of nodes $\mathrm{V}^i and V^j$
$\mathrm{V}^i.PL, V^j.PL$	Pages liked by nodes $\mathrm{V}^i and V^j$
$\mathrm{V}^i.GJ, V^j.GJ$	Groups joined by nodes $\mathrm{V}^i and V^j$
$\mathrm{S}_{MF}(V^i, V^j)$	The mutual-friends similarity between nodes V^i, V^j
$\mathrm{S}_{SF}(V^i, V^j)$	The suggested-friends similarity between nodes V^i, V^j
$\mathrm{S}_{LI}(V^i, V^j)$	The likes similarity between nodes V^i, V^j
$\mathrm{S}_{PL}(V^i, V^j)$	The pages-Like similarity between nodes V^i, V^j
$\mathrm{S}_{GJ}(V^i, V^j)$	The groups-join similarity between nodes V^i, V^j
$\mathrm{CS}(\mathrm{V}^i, V^j)j)$	The connection-strength value between nodes V^i, V^j

we compare the values of connection-strength and betweenness-centrality to identify Sybil nodes and identify attack edges in the social network graph.

3.2.3 Using the user-behavior based features to identify attack edges

We use characteristics based on user activity to identify the attack edges and measure the strength of the connectivity between the nodes. to compare the behaviour characteristic similarity score in order to determine the connection strength of each link. We consider behaviour factors such as likes, pages-likes, suggesting friends, joining groups, and shared friends in our study. Once the behaviour characteristics are defined, the Jaccard coefficient similarity [29] metric is used to calculate the behaviour features similarity score.

Mutual friends

The friends that two distinct users have in connection and have added to their friend lists are known as mutual friends. Using the Jaccard coefficient, we

compute the mutual friend similarity score[29]. Table 3.1 explains the symbols.

$$S_{MF}(V^i, V^j) = \frac{|V^i.FL \cap V^j.FL|}{|V^i.FL| + |V^j.FL| - |V^i.FL \cap V^j.FL|} \tag{3.1}$$

Suggested Friends:

Based on a few common characteristics, including hobbies, extracurricular activities, and vocations, OSNs create the suggested friend list. Although they are not on the user's list of recommended friends, these suggested friends are most likely the user's friends or acquaintances. Those that have been recommended to users can be added to their friend lists. A friend list that is dynamic might be suggested. Based on their shared recommended friends, we compare the nodes' (users') similarity using the Jaccard coefficient[29]. Each symbol is explained in Table 3.1.

$$\mathrm{S}_{SF}(V^i, V^j) = \frac{\left|V^i.SL \cap V^j.SL\right|}{|V^i.SL| + |V^j.SL| - |V^i.SL \cap V^j.SL|} \tag{3.2}$$

Likes:

Facebook along with other social media platforms offer the standard "Like" button. Those who click the "like" button can express their opinions. Similar interests will nearly always lead people to one another through shared "likes." people of Sybil have the opportunity to engage with some of the trustworthy people, although the likelihood of them having similar interests is minimal. Table 3.1 provides an explanation of the symbols and indicates the degree of "likes" similarity between users (nodes). .

$$\mathrm{S}_{LI}(V^i, V^j) = \frac{\left|V^i.LI \cap V^j.LI\right|}{|V^i.LI| + |V^j.LI| - |V^i.LI \cap V^j.LI|} \tag{3.3}$$

Pages

Pages are online areas on social networks such as Facebook where businesses, public personalities, brands, corporations, organisations, NGOs, and professions may communicate with their supporters or customers. Users can create personal pages on a variety of social networking sites. "Follow" or "like" pages that grab their interest. Updates on Facebook sites liked by users will appear in their News Feed. We calculate the pages-like resemblance between the users (nodes) using the Jaccard coefficient [29]; table 3.1 provides an explanation of the symbols.

$$\mathrm{S}_{PL}(V^i, V^j) = \frac{\left|V^i.PL \cap V^j.PL\right|}{|V^i.PL| + |V^j.PL| - |V^i.PL \cap V^j.PL|} \quad (3.4)$$

Group

Groups on social media platforms like Facebook let users communicate about topics of interest, debate problems, voice their thoughts, and share relevant information. We calculate the group similarity between nodes using the Jaccard's Coefficient metrix[29]; table 3.1 explains the symbols.

$$S_{GJ}(V^i, V^j) = \frac{|V^i.GJ \cap V^j.GJ|}{|V^i.GJ| + |V^j.GJ| - |V^i.GJ \cap V^j.GJ|} \quad (3.5)$$

On the above features, we can calculate the behavior similarity between the nodes as follow:

$$\mathrm{CS}(\mathrm{V}^i, V^j) = Mutual{-}friendssimilarityscore S_{MF}(V^i, V^j) + Suggested{-} friendsimilarityscore S_{SF}(V^i, V^j) + likessimilarityscore S_{LI}(V^i, V^j) + Pages{-} likessimilarityscore S_{PL}(V^i, V^j) + Groups - joinsimilarityscore S_{PL}(V^i, V^j) \quad (3.6)$$

These behavior similarities values assigned to the edges as weights, that are connected the nodes with each other.

Betweenness Centrality

Betweenness centrality quantifies the frequency with which a single node follows the shortest route between other nodes. Nodes with strong betweenness-centrality can be found along many of the shortest pathways[30]. Find the shortest route throughout the network between each pair of nodes. Determine how many of these shortest paths pass by each node in the network. How frequently a node appears on a path can be calculated using the shortest paths connecting other node pairs.To normalise the count, divide it by the total number of shortest routes in the network. Next, the node's betweenness centrality score is displayed. The mathematical formula which determines the node 'v' in a network's betweenness centrality may be written as follows:

$$C_{btw}(V^i) = \sum_{V^s, V^t, \epsilon V} \frac{\delta v^s v^t(V^i)}{\delta v^s v^t} \tag{3.7}$$

Where, $C_{btw}(V^i)$ represents the betweenness centrality value of node V^i. $\delta v^s v_i^t$ is the shortest route between the two nodes, v^s and v^t. $\delta v^s v_i^t$ is the shortest path via node V_i that connects v^s and v^t. Attack edges connect sybil nodes, which have betweenness centrality values below a certain threshold.

In this work, we calculate betweennness centrality to idetify the sybiles attacks. Applying a threshold of 0.2 to both nodes and edges in a social network graph might be a useful strategy for detecting possible Sybil attacks in the context of network security and anomaly identification. A malicious act known as the Sybil attack involves an adversary generating several fake identities in order to undermine the security of a network. We can evaluate the possibility of Sybil attacks using the betweenness centrality metric, which evaluates the amount to which a node or edge resides on the shortest pathways between other nodes in the network. Let's focus on nodes first. A user or other entity is represented by each node in a social network. We can identify nodes that serve as mediators in the network by measuring the betweenness centrality for each node. Nodes with betweenness centralities below 0.2 can be seen as having a lesser impact on the network's communication patterns. A Sybil attacker may be present if a node's betweenness centrality is lower than this level since it could indicate that the node is not actively engaging in meaningful contact with other nodes. Let's look at edges next. Edges in a social network reflect the relationships or connections between nodes. We may find edges that are essential in tying various portions of the network together by calculating

the betweenness centrality for each edge. A betweenness centrality of less than 0.1 for edges may indicate that they are not necessary for preserving effective communication routes between nodes. A possible Sybil attack may be detected if an edge's betweenness centrality falls below this threshold, suggesting that the edge is not enabling important network connections.

The first step is to add 20% nodes and edges in the datasets that we assume these nodes and edges are Sybil nodes and edges. After that, we identify nodes and edges with betweenness centrality values below the 0.2 threshold. The existence of Sybil attackes has to be confirmed by more research and analysis. Investigate Sybil nodes and edges thoroughly for any additional odd behaviour, such as unusual communication patterns, sudden changes in their network activity, or indications of impersonation. In summary, a particular technique for identifying possible Sybil attacks in a social network is to apply a betweenness centrality with the threshold of 0.2 to both nodes and edges. To ensure the presence of malicious activity and implement the necessary protective measures, it is necessary to enhance this analysis with additional security measures and rigorous evaluation of the detected nodes and edges. We employ a "users-behaviour based and graph-based hybrid approach" to identify Sybil attacks in OSNs for datasets 2 and 3. We utilise user behaviour similarities for edges and centrality of betweenness (graph feature) values of node from these two datasets as they are network-based datasets.

3.3 Machine learning based approaches

Our approach to machine learning algorithms is content-based. We employ the Paradigm Shift dataset for social media spam bots. We extract attributes such as status count, friend count, listed count, Url, description, and kind from this dataset. The following machine learning techniques are used to predict sybils and non-sybil nodes from fake accounts using the provided dataset.

3.3.1 Machine learning Algorithm

The procedure for doing binary classification using logistic regression on a collection of social media account data to differentiate between authentic and fraudulent accounts. The process of utilizing logistic regression to perform binary classification on a collection of social media account data in order to distinguish between real and false accounts. For data preparation, two datasets named "genuineaccounts.csv" and "fakefollowers.csv," which presumably contain data on social media accounts, are loaded by the code first. Once

each row in the merged datasets has been given a binary label (0 for real, 1 for fake), the data is shuffled. The non-numeric values in a few columns are removed, and any missing values are set to zeros. Additionally, after splitting the data into training and testing sets, the algorithm utilises LabelEncoder to encode the binary labels. It also normalises the feature data using a standard scale.

3.3.2 Random Forest Algorithms

Using Scikit-Learn, this code does random forest regression:To ensure repeatability, the data is divided into training and testing sets, with a test size of 24% and a random seed.StandardScaler may be used to standardise feature data so that each feature has a mean of 0 and a normal deviation of 1. 10,000 decision trees are used to initialise a Random Forest Regressor, which is subsequently fitted to the standard training set.creates predictions (Rf_pred) on the test data using the training model.compares the expected values to the actual test labels (y_test) to determine the R-squared (R2) score, a metric for the regression model's success.The R2 score is used by the algorithm to assess how well the random forest regression model performs on the test data.

3.3.3 Naive Bayes Classifier

The Bayes Theorem [31] serves as the foundation for the naïve bayes classifier. Unlike other classifiers, it is extremely quick and scalable. Applications of this classifier in binary and multiclass scenarios are common. Naive Bayes predicts the target class by using the likelihood of other classes. Second, Naive Bayes makes the assumption that there is no relationship between any of the qualities. Naive Bayes is typically used by spam detection systems, such as email spam detection systems. Because Naive Bayes is also a reasonably basic strategy, it is often used as a supplement to other models. The conditional probability that, should event B occur, event A will take place. Because of the set of probability principles, an individual may adjust their forecast of an event depending on newly acquired or received knowledge to provide better predictions.

- The chance that event A will occur provided that event B has already happened is expressed as P(A | B).
- The chance that event B will occur given that event A has taken place previously is expressed as P(B | A).
- The probability of an occurrence is P(A) of event A.

- The probability of an occurrence is P(B) of event B.

3.3.4 Multi-Layer Prercepton

Multilayer perceptrons (MLPs) are artificial neural networks that forward data [32]. A layer for input, an output layer, and and a hidden layer are its three typical layers. MLP works very well in instances when the two variables are linearly inseparable. It is often used for prediction and pattern recognition. The neuron is trained by the back propagation method. ReLU and sigmoid are the two activation techniques that are most commonly employed.

MLPs are widely used in pattern recognition and prediction tasks, which is consistent with the goal of spotting anomalies in network behaviour that can indicate Sybil attacks. The individual neurons of the MLP are modified to generate precise predictions through a training procedure in which the network learns from labelled data. Backpropagation is a training method that modifies the internal parameters of the network to reduce prediction errors.

The sigmoid function and Rectified Linear Unit (ReLU) are two frequently used activation functions in MLPs. The network acquires non-linearity from these activation functions, enabling it to recognize deep links and patterns in the input. These activation routines provide the MLP the ability to identify tiny changes in user behaviour that may be indications of malicious Sybil accounts when it comes to Sybil attack detection.

3.3.5 Logistic regression

Logistic regression is used in both prediction and classification analysis [33]. Logistic regression is used to determine the probability of an event, such as voting or not, based on a collection of independent factors and independent data. Since the result is a probability, the range of the dependent variables is 0 to 1. The Centre for Complex Networks and System Research, Indiana University's Media School, the Network Science Institute, and the Existing System Botometer worked together to construct the systemcitemartini2021bot[34]. The foundation of the system's design is a machine learning model that uses the provided Twitter username to determine a score. A low score indicates a human or probably human profile, whereas a high score indicates a phoney, inactive, or spambot profile.

This system harnesses machine learning techniques and logistic regression in particular to assign a score to Twitter usernames provided to it. This score serves as an indicator of the authenticity of the associated profile. Profiles with low scores are indicative of genuine human users or likely human users, while those with high scores are suggestive of fake, inactive, or spambot profiles.

In essence, logistic regression plays a significant role in the Botometer's scoring system, helping to distinguish between genuine human users and possibly fake identities on social media sites. The continuous attempts to recognize and resist Sybil attacks, a persistent threaten in online social networks, are aided by this use of logistic regression.

3.3.6 KNN

K-Nearest Neighbours is a supervised machine learning technique used in regression-based and classification approaches[35]. The KNN algorithm operates by supposing similarities between the properties in the dataset in order to build categories. The procedure is repeated K/N times in order to improve the categories. After the model is trained, each new data point will be classified into one of the pre-established categories based on the model's predictions.

The use of K-Nearest Neighbours (KNN), a supervised machine learning approach, to Sybil attack detection is covered in this paragraph. KNN classifies data points using a regression and classification-based methodology. The similarity principle, which maintains that related data bits belong in the same category, serves as the foundation for how it functions.

The KNN classifier is used K/N times in the case of Sybil attack detection, where K is the number of nearest neighbours taken into consideration for each data point and N is the total number of data points in the dataset. Through the computation of the similarity between each data item and its K nearest neighbours, the approach improves the categories at this regular interval. The model constantly trains itself to find underlying patterns in the data, allowing it to discriminate between potentially hazardous and real objects.

Once the KNN model has been trained on the dataset, predictions may be made using it. A new data point is introduced, and the model determines which category it belongs in based on how similar it is to the current data points. This means that KNN may help in determining if a new entity exhibits behaviour compatible with actual users or displays suspicious patterns connected to possible Sybil attackers in the context of Sybil attack detection. By contributing in the detection of Sybil threats, this method makes use of the capabilities of supervised machine learning to improve the security of online networks.

3.3.7 Apply graph based technique in Content based approach

From tweets.csv, we extract the features "id" and "userid" for the "Paradigm Shift of Social Spambots" dataset. The individual "id" is the one who may respond or retweet "userid," whereas "userid" is the one who can tweet.

Social spambots may be identified by analysing their activity patterns using betweenness centrality. A node's importance in a network is indicated by its betweenness centrality. The number of shortest paths between each pair of network nodes that pass through a particular node is used to calculate it. Since a node with a high betweenness centrality is most likely a critical node, removing it might make the network unstable. Betweenness centrality can be used to detect nodes that have a high number of shortest linkages linking real nodes in the case of social spambots. This is due to the fact that spambots are frequently used to swiftly transmit spam to a huge number of individuals.

The dataset may be partitioned into 10,000-row samples, and we can calculate the betweenness centrality between the id and the user-id for each sample. Since it might be computationally demanding to determine betweenness centrality for large networks, we can divide the dataset into samples of 10,000 rows each. to divide the dataset into 20 samples, with 10,000 rows in each sample. For each sample, a threshold of 20% is set to evaluate the betweenness centrality of nodes (user−id, id). If a node's betweenness centrality is more than the threshold, it is categorised as a Sybil node. The line dividing a true node from a Sybil node is called a Sybil edge.

CHAPTER 4

ANALYSIS & RESULTS

The findings of our comprehensive study of Sybil's attack detection in OSN's utilising machine learning techniques—a content-based approach, a graph-based approach, and a method based on user behaviour to identify the attack edges—are presented in this chapter. This study's goal is to evaluate how well different feature engineering techniques and machine learning algorithms recognise Sybil accounts in online social networks. We also examine these algorithms' performance on various datasets and setups for experiments.

4.1 Dataset Description

Before discussing the findings and analysis, it is essential to provide an overview of the datasets that were used in our research. Three datasets are used in our experiment to evaluate our Sybil detection models: "The Paradigm-Shift of Social Spambots" [26], "Soc-karate" [27], and "Twitter Interaction Network for the US Congress" [28].

4.1.1 The Paradigm-Shift of Social Spambots dataset

The dataset 1 integrates a simulated social network environment with a real-world social media dataset gathered from a reputable online platform. The dataset underwent pre-processing to guarantee consistency and anonymize user data in order to protect privacy. Social network datasets are frequently shown as graphs, with vertices serving as nodes and lines linking the vertices serving as edges. This form makes it possible for academics to examine the dynamics and structure of social networks using methods from graph theory and network analysis.

The first dataset was combined from two csv files that contained 3474 real accounts and 3351 fake accounts, respectively. There are following feature that we extracted, that are:

- Status Count,
- Friends Count,
- Listed Count,
- Follower Count,
- Favourites Count,
- URL,
- Geo Enabled,
- Description and
- type

This dataset might include a set of data related to social spambots. It can contain details about specific spambot accounts, their actions, features, and communications on OSNs platforms. For researchers, data scientists, and cybersecurity professionals to investigate and understand the behaviour of social spambots. For the purpose of detecting and preventing spambot activity, it can be utilized to create machine learning models and algorithms. To enhance security protocols on OSNs, researchers can examine the dataset to find trends, patterns, and features of spambot behaviour. It can be used to assess how well anti-spambot policies put in place by social media businesses are working.

Status Count:

This attribute most likely represents how many tweets, posts, or status updates the social media account has uploaded. It may provide information on the account's degree of activity. When compared to normal users, spambots may have a particularly high or low status count.

Friends Count:

The number of accounts (usually users or bots) that the account follows is referred to as its "friends count." Spambots could follow too many accounts or have a disproportionately low number of friends compared to their followers.

Listed Count:

A high listed count can suggest that the account is influential or intriguing. The listed count shows how frequently the account has been added to lists by other users. Spambots may attempt to inflate this number to make it seem more reliable.

Follower Count:

The number of accounts that follow a particular social media account is referred to as its follower count. Spambots may have an extremely high follower count, which is frequently attained using follow-back programmes or buying followers.

Favourites Count:

If the account has a URL, such as a website or a connection to an external resource, it is likely indicated by this feature. Spambot accounts may employ URLs for a number of objectives, such as advertising goods, services, or harmful websites.

URL:

This characteristic most likely indicates whether the account is linked to a URL, such as a website or an external resource, via a link. URLs can be used by spambot accounts for a variety of things, such as advertising goods, services, or malacious websites.

Geo Enabled:

The term "geo enabled" often indicates whether location-based services are enabled for the account. In their profiles, some spambots could give false or misleading information about their location.

Description:

A brief introduction or account description is given in the description. It may include language that summarises the account's objectives, passions, or affiliations. Spambot descriptions could contain phrases that are relevant to their goals, including political allegiances, or sales pitches.

Type:

Each account is probably divided into several types by the "Type" function, which may include classifications like "spambot," "fake account," "legitimate user," etc. For researchers and analysts to distinguish between various sorts of accounts in the dataset, this label is essential.

4.1.2 Soc karate dataset

The second dataset is called the Soc-Karate dataset [27]. A social network containing user conversations from a university karate club is called the soc-Karate dataset. It comprises 78 edges (friendship ties) and 34 nodes (club members). The dynamics of social interactions and community structure are commonly studied using this dataset in network analysis and social network research. It has 34 nodes that represent each unique club member and 78 edges that depict the friendship links between club members. This dataset serves as a standard case study for social network research and network analysis. Studies on the dynamics of social connections, the establishment of communities, and the results of network fragmentation or division frequently make use of it.

4.1.3 Twitter Interaction Network for the US Congress dataset

The third dataset is called "Twitter Interaction Network for the US Congress" [28]. This network serves as the House of Representatives' and the Senate's Twitter engagement platform during the 117th US Congress. The original data was collected via the Twitter API, and the empirical transmission probabilities were calculated based on the frequency with which a member retweeted, quoted, replied to, or discussed a tweet from another member. Table 4.1 shows that it consists of 475 nodes and 10222 edges. A senate or a member of the house is represented by each of the 475 nodes. 10,222 edges, which represent Twitter interactions including mentions, quotes, retweets, and replies, link these nodes. These edges, which show the empirical propagation likelihood of a member responding to or quoting a tweet from another member, give insightful data on social media interactions and information flow across the legislative arms of the US government.

4.2 Experimental Setup

There are several machine learning techniques, including but not limited to Support Vector Classification (SVC), Random Forest, and Neural Networks,

Table 4.1: Summary of soc-karate and congress network dataset

Dataset	Type	Nodes	Edges
Soc-karate	Undirected	34	78
Congress Network	directed	475	10222

were used in our research. To improve the performance of each algorithm, we carried out a thorough evaluation process that including feature selection and hyperparameter modifications. Using a hybrid technique that combines user behaviour and graph analysis on two datasets to identify attacker edges with a threshold of 0.2 (20%) Furthermore, we analysed the effectiveness of Sybil identification through the use of many indicators of performance, such as accuracy, recall, precision, and F1-score.

4.3 Results

As we are apply comparison based techniques in which initially finding Sybil accounts by applying machine learning techniques on content based. And apply betweenness centrality on users behavior based and graph based hybrid approach to identify Sybils nodes and Sybils attacks. We discuss the performance of various machine learning methods using content based approach and use graph based and user behavior based hybrid approach results in this part using the findings from our research to identify Sybil nodes and sybil edges in online social networks. Here is an overview of the main findings:

4.3.1 Performance of Machine Learning Classifiers

Table 4.1 presents the comparative performance of machine learning algorithms on Dataset. It is evident that Random Forest and Gradient Boosting consistently outperformed other algorithms across the dataset, achieving high precision, recall, and F1-scores. SVC also exhibited commendable performance on Dataset.

Logistic Regression

This model is effective in identifying Sybil attacks because it is well-suited for binary classification tasks. It has a high precision that is 9.418%, which indicating that it's good at minimizing false positives, and have a respectable

Table 4.2: Machine Learning Models

ML Model	**Accuracy**	**Precision**	**Recall**	**F1-Score**
Logistic Regression	97.98%	98.41%	98.31 %	97.74%
Naive Bayes Classifier	74.31%	98.07%	96.13%	93.97%
MLP Classifier	97.14%	98.37%	97.23%	97.16%
SVC Classifier	88.49%	92.03%	97.59%	94.94%
ADA Boost	90.10%	91.41%	90.28%	91.06%
Random Forest	98.09%	98.47%	98.33%	98.30%
KNN	94.54%	97.98%	97.71%	97.82%

recall of 98.31%, suggesting its ability to capture actual positive instances. The F1-Score 97.74% that indicates a balanced trade-off between recall and precision.

Naive Bayes Classifier

The naives Bayes classifier achieved 74.31% accuracy. Its precision of 98.07% indicates that it can correctly categorise sybil assaults, even though it isn't as exact as some other models. Recall is 96.13%, indicating that it is effective at identifying true positive cases, and the F1-Score of 93.97% shows an acceptable balance between precision and recall.

MLP Classifier (Multi-Layer Perceptron)

A high accuracy of 97.14% achieved by the MLP Classifier. This model can detect sybil attacks since it can identify complicated patterns in the data. With precision, recall, and F1-Score all standing around 97.23%, it performs at a high level, demonstrating that it is able to both minimize false positives and effectively capture actual positive instances.

SVC Classifier (Support Vector Classifier)

An accuracy of 88.49% achieved by the SVC Classifier. Fortunately it isn't the most accurate model on our list, it does have a precision of 92.03%, which shows that it can classify sybil attacks with false positives. With a high recall of 97.59%, it is also capable of capturing actual positive situations. The F1-Score is 94.94%, that show balanced performance .

ADA Boost (Adaptive Boosting)

ADA Boost classifier achieved an accuracy of 90.10%. This ensemble learning technique that is useful for identifying sybil attack since it combines multiple weak classifiers to get a powerful one. It has a high precision of 91.41%, indicating that it can minimize false positives, and a recall of 90.28%, indicating that it is effective at capturing actual positive instances. The F1-Score is- 91.06%, however, it suggests some trade-off between recall and precision.

KNN (K-Nearest Neighbors)

KNN achieved a 94.54% accuracy. When nearby instances are relevant, an instance-based learning method can effectively detect sybil attack by classifying data points by comparing them to their neighbours. It has a high recall of 97.71%, demonstrating its ability in capturing actual positive instances, and a precision of 97.98%, which reduces false positives. The F1-Score of 97.82% indicates a performance that strikes a balance between recall and precision.

Random forest Algorithm

With 98.09% accuracy, 98.47% precision, 98.33% recall, and a 98.30% F-1 score, the Random Forest model showed outstanding results. This shows that the model made excellent predictions since it correctly classified instances, reduced false positives (precision), effectively caught relevant instances (recall), and balanced precision and recall.

4.3.2 Performance of User behavior based and Graph based hybrid approach

We utilise two datasets that include social interactions for the US Congress dataset network and Soc-Karate dataset. We provide the datasets to illustrate the attack scenario and put our recommended solution into practise. Since we think there is a limit on the number of Sybil nodes, we added 20% extra Sybil nodes to the total node count of the dataset. Table 4.3 gives an updated description of the dataset.

The updated datasets with attack edges and Sybil nodes. The original and updated soc-karate network datasets' networks. Table 4.3 presents the dataset including 20% sybils nodes and sybils edges. The Soc Karate dataset has seven Sybil nodes and thirteen Sybil edges, as seen in figure 4.1. We must specify a threshold of 20%.

Table 4.3: Dataset Detail

Dataset	**Nodes**	**Edges**	**Sybil nodes**	**Sybil egdes**
Soc karate	34	78	7	13
Congress network	475	10222	94	2044

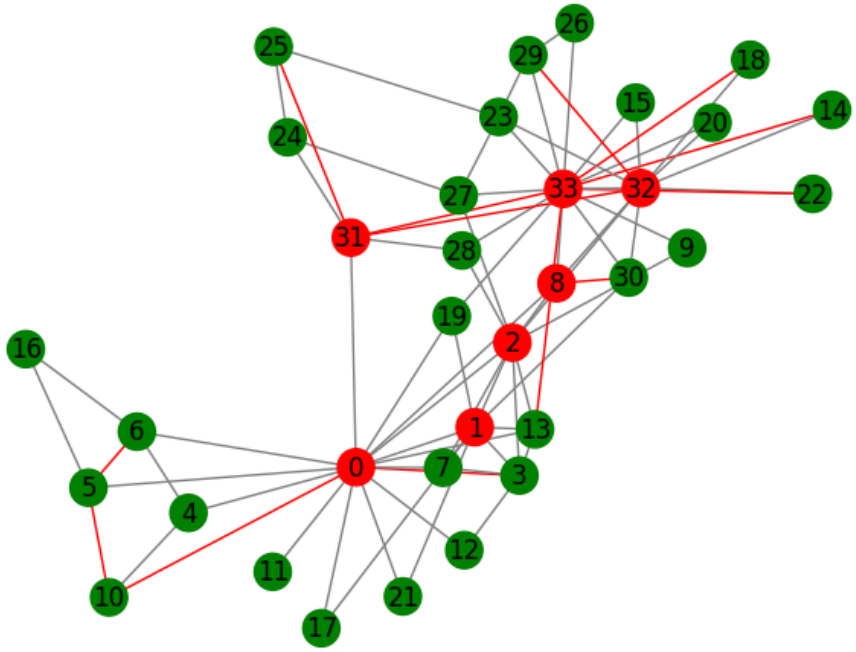

Figure 4.1: Sybil Attack Detection

Table 4.4: Empirical Results of User behavior and graph based hybrid approach

Datasets	**Accuracy**	**Precision**	**Recall**	**F1-Score**
Soc Karate	98.82%	98.93 %	98.58%	98.74%
Congress network	98.70%	98.53%	98.65%	98.64%

To identify the nodes and edges of Sybil's. We evaluate behavioural similarities between nodes before calculating the betweenness-similarity between them. We include threshold1 20% nodes and edges in the dataset; these are considered Sybil nodes and attack edges. After that, the threshold2 is reset to

20%, and the edges' behaviour similarity values are examined. An edge is designated as a Sybil edge if the behaviour similarity value is less than threshold 2. Check if the betweenness centrality value is less than the threshold 2 after that. The node is categorised as a Sybil node if it is. An edge is categorised as a Sybil attack edge if there are any Sybil edges between these nodes.

We consider the results metrics True Positive Rate (TPR), True Negative Rate (TNR), False Positive Rate (FPR), False Negative Rate (FNR), and Detection Rate for calculating assessment metrics. We test our proposed method in terms of accuracy, precision, recall, and F1-score. The following are their formulas:

$$Accuracy = \frac{TPR + TNR}{TPR + FPR + TNR + FNR} \tag{4.1}$$

$$Precision = \frac{TPR}{TPR + FPR} \tag{4.2}$$

$$Recall = \frac{TPR}{TPR + FNR} \tag{4.3}$$

$$F1 - score = 2 * \frac{precision * recall}{precision + recall} \tag{4.4}$$

In table 4.4, the empirical results are shown using graph based and user behavior hybrid approach. Figure 4.2 show the comparison between soc karate and congress network datasets. Based on these comparisons, the congress network approach is not as effective as the soc karate technique in identifying Sybil's attack in social networks.

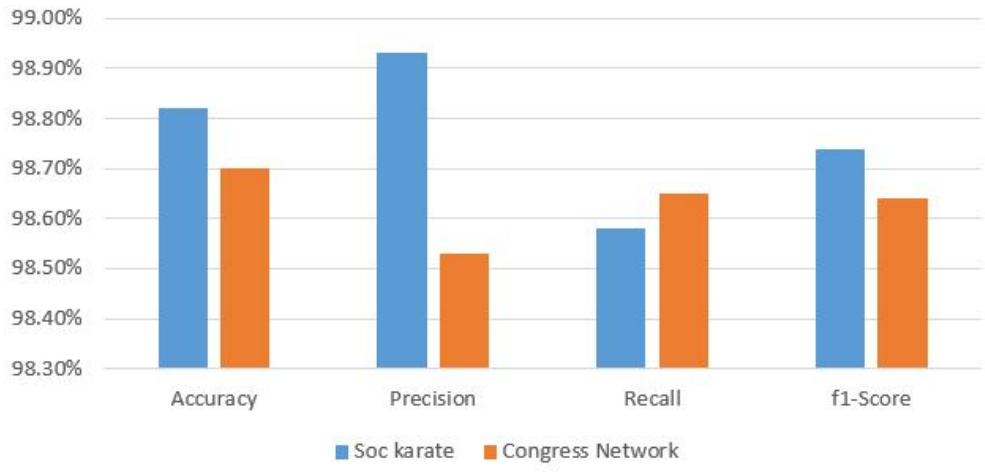

Figure 4.2: Comparison between Soc-karate and Congress Network datasets

4.4 Analyzed the comparison between Content based and User behavior and graph based hybrid approach

The content-based machine learning method, which has enormous recall, accuracy, precision, and F1-score, is compared with the "users behaviour based and graph based hybrid approach" in Figure 4.3. We compare its findings with the Soc Karate and Congress network graphs since the Random Forest algorithm works better than the other methods. In terms of recall, accuracy, precision, and F1-score for the identification of Sybil nodes and edges, these comparisons show that the hybrid technique based on user behaviour and graphs works better than the other approaches.

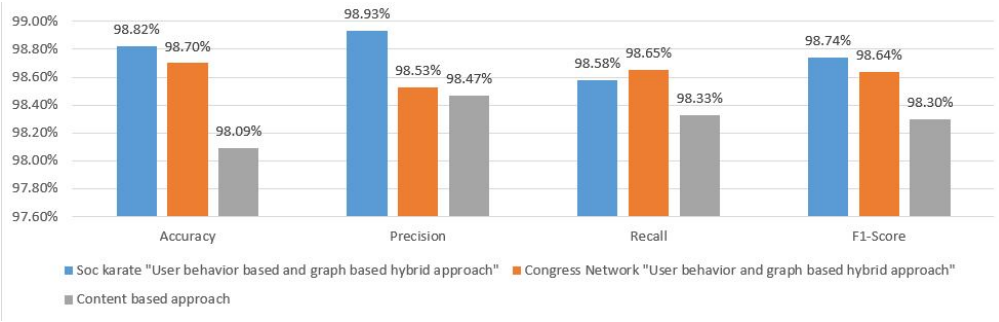

Figure 4.3: Comparison between Content based and User behavior and graph based hybrid approach

4.4.1 Analyzed the comparison between Machine learning algorithm with Graph based technique in Content based approach

Machine learning techniques including the ADA boost classifier, Random forest, Naive Bayes, KNN, multilayer perception, logistic regression, and SVC can be used to locate Sybil nodes. Table 4.2 shows that Random forest has the highest detection rate (97.93%) for Sybil nodes among machine learning approaches. To determine the Sybil nodes and Sybil edges in the content-based method, we employ the betweenness centrality in the graph-based strategy. We evaluate the nodes' betweenness centrality and set a 20% thresshold. If the threshold value is more than the betweenness centrality, the node is classified as a Sybil node. The accuracy and detection rate of the graph-based approach were 67.23% and 62.18%, respectively.

We compared the machine learning algorithms used in the content-based approach with those in the graph-based methods. Their comparison shows that the Sybil node identification rate is greater than the graph method in the content-based approach, as seen in figure 4.4.

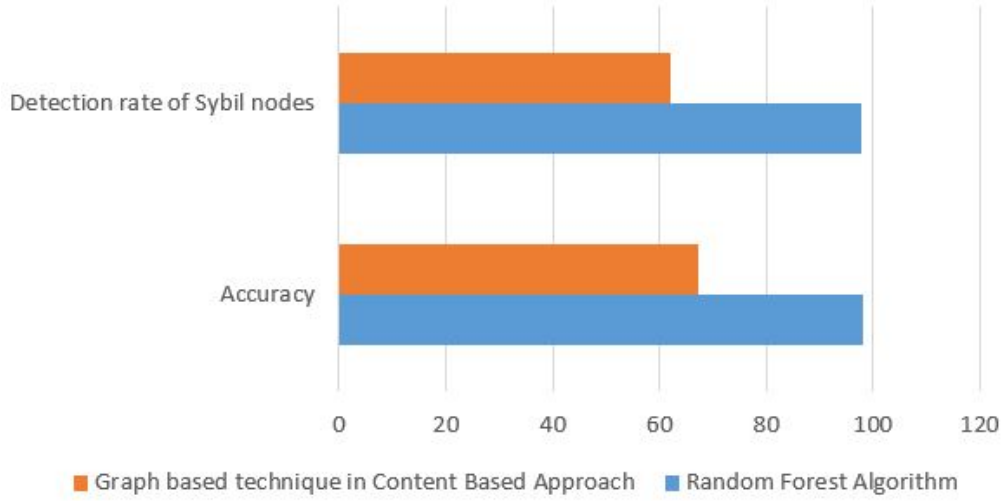

Figure 4.4: Comparison between Random Forest Algorithm and graph based technique in Content based approach

4.5 Comparison with Previous User behavior and graph based approach with our approaches

The previous hybrid technique, which identified Sybil's nodes and egdes in the dataset with a threshold of 10%, was based on user behaviour and graph analysis. In order to identify Sybil nodes and attack edges, we established a threshold2 of 10% for behaviour similarities and betweenness centrality. Their suggested methodology's primary drawbacks are its poor recall, accuracy, and F1-score. In order to compare our method with the prior one, we first add threshold1 (10%) to dataset 3 and set threshold2 (10%) to identify Sybil edges and nodes. The detection rate of Sybil edges and nodes with a 10% threshold is displayed in table 4.5.

We establish a threshold1 of 20% in the datasets for our hybrid technique based on user behaviour and graph analysis. In order to identify Sybil nodes and attack edges, we established a threshold2 of 20% for behaviour similarities and betweenness centrality. Additionally, we add the threshold1 20% in the socfb-Bowdoin47 [27], socfb-Brandeis99 [27], and new dataset Congress networks. To detect the Sybil nodes and Sybil edges, we set the threshold2 20%. The detection rate of Sybil edges and nodes with a 20% threshold is displayed in Table 4.6.

We used a criterion of 10% to compare the user behaviour base and graph-based hybrid technique to the previous method, as shown in figure 4.5. We utilise datasets from Congress Networks, whereas the previous approach employed the socfb-bowdoin47 and socfb-brandies99 datasets. Their compar-

Table 4.5: Sybil Node Detection and Attack Edges Detection Rates with 10% Threshold

Dataset	Sybil Node Detection Rate (%)	Attack Edges Detection Rate (%)
socfb-Bowdoin47	98.04	98.96
socfb-Brandeis99	97.69	98.64
Congress Network	98.31	98.77

Table 4.6: Sybil Node Detection and Attack Edges Detection Rates with 20% Threshold

Dataset	Sybil Node Detection Rate (%)	Attack Edges Detection Rate (%)
socfb-Bowdoin47	98.27	98.89
socfb-Brandeis99	97.83	98.54
Congress Network	98.87	98.94

isons show that the congress networks graph has a greater detection rate of Sybil nodes than the previous technique, and that the socfb-Bowdoin47 network has a high detection rate when using a 10% threshold for attack edges. The Congress network graph is superior at locating Sybil nodes, even though the socfb-Bowdoin47 dataset is superior to the other graph method in terms of detecting Sybil assaults.

We also examined the hybrid technique using graphs and user behaviour, as shown in figure 4.6, with a threshold of 20%. Their comparisons show that when the attack edge threshold is set at 20%, the Congress network has a high detection rate. Furthermore, in comparison to the previous technique, the Congress network graph has a high detection rate of Sybil nodes. In terms of detecting Sybil attacks and nodes, the Congress network graph outperforms the other graph technique.

4.6 Analysis

In this section, we analyze the data we have collected and extract significant results from our experiments.

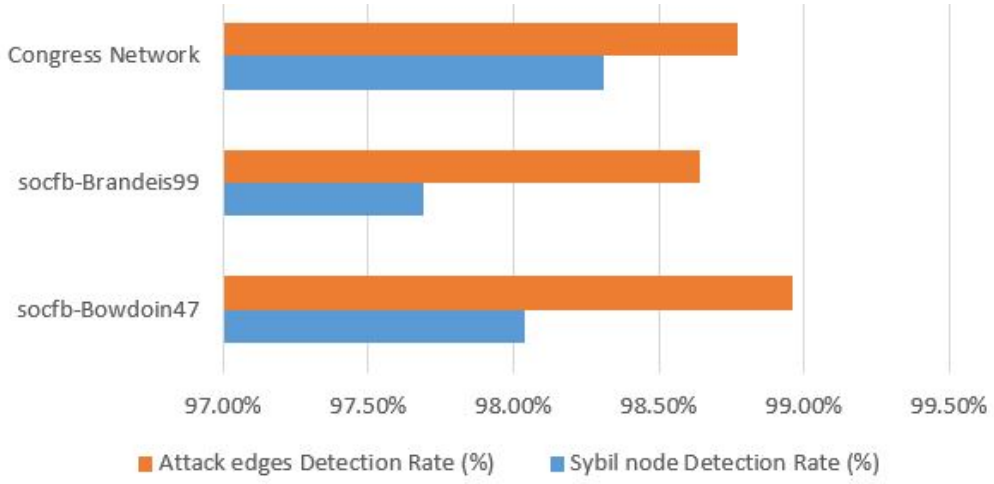

Figure 4.5: Comparison for Detection rate of dataset we use with previous techniques datasets with threshold 10%

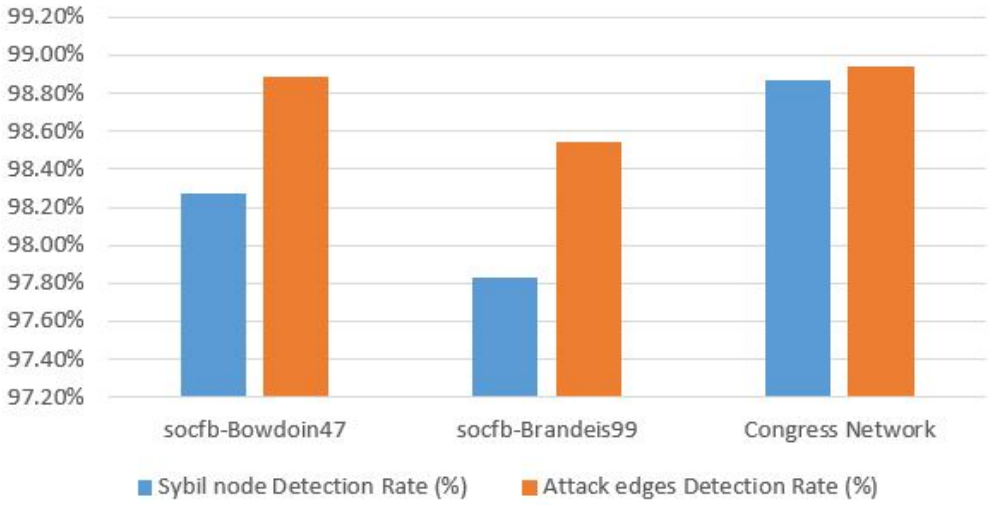

Figure 4.6: Comparison for Detection rate of dataset we use with previous techniques datasets with threshold 20%

4.6.1 Algorithmic Performance

Our results show that ensemble techniques, like as Random Forest and ADA Boosting, are quite effective in detecting Sybil across simulated datasets. They make excellent applicants for such tasks because they can manage noise and capture complicated correlations within the data. SVC demonstrated competitive performance in the simulated context despite not being as consistently robust, demonstrating its potential for Sybil detection in restricted situations.

While our analysis, user behavior and graph based hybrid approach can detect Sybil nodes and Sybil edges with better detection rate.

4.6.2 Feature Engineering

Feature engineering in Sybil attack detection for OSN involves creating features from users behavior-based and graph-based data. While common friends, recommended friends, group participation, likes, and pages are examples of user behavior-based features, node betweenness-centrality is a graph-based feature. These features increase OSN security by enabling the distinction between actual and Sybil accounts. This highlights the significance of network and user-centric factors in Sybil detection activities.

4.6.3 Dataset Variation

It is noteworthy to observe that the algorithms performed on the dataset1. Due to its complexity and noise, this dataset presented more challenges. This emphasises the importance of adaptable models and the importance of taking the dataset features into account when developing Sybil detection techniques.

4.7 Conclusion

In this chapter, we discussed the findings and analysis of our Sybil detection experiments in online social networks machine learning techniques annd identify the sybil nodes and sybil edges. Our results indicate that ensemble techniques like Random Forest and ADA Boosting, when used in conjunction with efficient feature engineering, can successfully identify Sybil accounts. The properties of the dataset, however, may have an impact on how well these algorithms function.

We will address the implications of our findings and provide recommendations for additional study in the area of Sybil's detection in OSN's in this chapter. .

CHAPTER 5

CONCLUSION & FUTURE WORK

Future studies on Sybil attacks are required in a number of areas. Implementation of better detection mechanisms is an essential topic. Current detection techniques usually need a high level of node trust or are computationally expensive. It is necessary to develop new detection techniques that are more effective and scalable.

5.1 Conclusion

Finally, further research is required to determine how Sybil attacks affect developing systems and applications. How, for instance, do Sybil attacks impact the security and trustworthiness of self-driving vehicles or the Internet of Things? We can create more efficient defences by understanding the effects of Sybil attacks on these new system.

A hybrid technique for identifying Sybil attacks utilising user-based and graph-based data is proposed in the paper "Users behaviour based and graph-based hybrid approach" to detect Sybil attacks in OSNs. As demonstrated by the analysis's findings, the suggested method may successfully identify Sybil attempts even in cases while the attackers are intelligent and skilled.

The study's conclusions show that the recommended method outperforms current state-of-the-art Sybil attack detection methods. Even when the attackers are prepared and trained, the proposed technique may successfully detect Sybil attempts.

Overall, the method suggested in the study offers an updated and potentially effective way to identify Sybil attacks. It's crucial to remember that the paper only evaluates the suggested technique on one online social network. Future research are required to evaluate the suggested method against a wider range of attack vectors and various topologies of networks. .

We developed by evaluating our previous work on Sybil attack detection techniques, including user-based and graph-based methods with threshold

20%. Then, we created and put into practice a strategy that integrated these approaches. Our strategy tried to maximize the benefits of approaches by improving detection precision.

We evaluated the efficacy of our technique by detailed evaluation on real-world datasets. The findings showed that in terms of detection accuracy, false positive rates, and resilience against changing attack techniques, our system performed better than previous user-based and graph-based approaches. Our method increased the TPR while reducing the FPR by using user- and network-centric features.

5.2 Future Work

There are still a few aspects that need to be researched and developed further, even if our content-based, and "users behaviour based and graph based Hybrid approaches" greatly enhance Sybils attack detection:

- Deep Learning Integration: Using deep learning methods like deep neural networks and graph neural networks may help to improve the precision of Sybil attack detection. Deep learning models have the ability to automatically identify complicated relationships and patterns in network data, possibly enhancing detection performance.

- Real-time detection: To avoid attacks as they happen, real-time Sybil attack detection systems must be created. Future research should concentrate on creating algorithms that can identify Sybil accounts in real-time, providing that risks are effectively addressed.

- Adaptive Attack Models: Attackers using Sybil are always changing their strategies. The ability of attackers to avoid detection should be made more difficult in the future by investigating adaptive detection models that can swiftly adapt to new attack patterns and behaviours.

- Large-Scale Social Networks:It is imperative that we expand our research to include immense online social networks. Future research in this area should focus on analyzing how our strategy grows with network size and evaluating its effectiveness on large datasets.

In conclusion, Sybils attacks detection in OSN's is a challenging but crucial task. Although the area of Sybil attack detection is constantly changing. OSN's security and dependabillity should be maintained, hence further research and development in this field are required.

REFERENCES

[1] H. Gao, J. Hu, T. Huang, J. Wang, Y. Chen, Security issues in online social networks, IEEE Internet Computing 15 (4) (2011) 56–63.

[2] J. Vayola, Biggest social media platform 2022, https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/ (2022).

[3] author, Sybil attack, https://www.imperva.com/learn/application-security/sybil-attack//.

[4] M. Del Vicario, A. Bessi, F. Zollo, F. Petroni, A. Scala, G. Caldarelli, H. E. Stanley, W. Quattrociocchi, The spreading of misinformation online, Proceedings of the national academy of Sciences 113 (3) (2016) 554–559.

[5] B. Dean, Social network usage, https://backlinko.com/social-media-users//.

[6] V. mujovic, Top cybercrime cases of 2022, https://techgenix.com/top-cybercrime-cases-2022/: :text=The%20biggest%20cybercrime%20threats %20for,people%20and%20do%20so%20frequently//.

[7] G. Jethava, U. P. Rao, User behavior-based and graph-based hybrid approach for detection of sybil attack in online social networks, Computers and Electrical Engineering 99 (2022) 107753.

[8] A. Hamid, M. Alam, H. Sheherin, A.-S. K. Pathan, Cyber security concerns in social networking service, International Journal of Communication Networks and Information Security 12 (2) (2020) 198–212.

[9] W. Lee, J. Caverlee, G. I. Webb, Seven ways to detect social spambots, ACM Transactions on the Web (TWEB) 5 (3) (2011) 1–26.

[10] G. Stringhini, C. Kruegel, G. Vigna, The evil twin: Measuring and deterring sybil attacks in online social networks, ACM Transactions on the Internet of Things (TIOT) 2 (2) (2015) 1–25.

[11] E. Ferrara, O. Varol, C. A. Davis, F. Menczer, A. Flammini, The rise of social bots, Computer Science Review 10 (2016) 14–32.

[12] O. Varol, E. Ferrara, C. A. Davis, F. Menczer, A. Flammini, Online human-bot interaction: A large-scale study, arXiv preprint arXiv:1703.03105 (2017).

[13] C. A. Davis, O. Varol, E. Ferrara, A. Flammini, F. Menczer, Botornot: A system to evaluate social bots, arXiv preprint arXiv:1602.06506 (2016).

[14] S. Cresci, P. Lio, C. Mascolo, M. Tesconi, A. Spognardi, The paradigm of social spambots: Countering social bots with social honeypots, arXiv preprint arXiv:1508.07676 (2015).

[15] A. Mouti, E. Ferrara, O. Varol, A. Flammini, F. Menczer, Critical temporal analysis of social bot detection, arXiv preprint arXiv:2005.07843 (2020).

[16] G. Magno, L. M. Aiello, G. Rossi, Across the network: A large-scale study of social spam, arXiv preprint arXiv:1205.1450 (2012).

[17] S. Kumar, Y. Zhang, X. Wang, X. Zhang, F. Chen, Battle of the iot bots: A large-scale study of sybil attacks in iot networks, arXiv preprint arXiv:1805.03653 (2018).

[18] Q. Zhou, G. Chen, An efficient victim prediction for sybil detection in online social network, IEEE Access 8 (2020) 123228–123237.

[19] S. Misra, A. S. M. Tayeen, W. Xu, Sybilexposer: An effective scheme to detect sybil communities in online social networks, in: 2016 IEEE International Conference on Communications (ICC), IEEE, 2016, pp. 1–6.

[20] H. Bansal, M. Misra, Sybil detection in online social networks (osns), in: 2016 IEEE 6th International Conference on Advanced Computing (IACC), IEEE, 2016, pp. 569–576.

[21] G. Jethava, U. P. Rao, An interaction-based and graph-based hybrid approach to evaluate trust in online social networks (osns), Arabian Journal for Science and Engineering 47 (8) (2022) 9615–9628.

[22] T. Gao, J. Yang, W. Peng, L. Jiang, Y. Sun, F. Li, A content-based method for sybil detection in online social networks via deep learning, IEEE Access 8 (2020) 38753–38766.

[23] M. Al-Qurishi, M. Alrubaian, S. M. M. Rahman, A. Alamri, M. M. Hassan, A prediction system of sybil attack in social network using deep-regression model, Future Generation Computer Systems 87 (2018) 743–753.

[24] M. Al-Qurishi, S. M. M. Rahman, A. Alamri, M. A. Mostafa, M. Al-Rubaian, M. S. Hossain, B. B. Gupta, Sybiltrap: A graph-based semi-supervised sybil defense scheme for online social networks, Concurrency and Computation: Practice and Experience 30 (5) (2018) e4276.

[25] J. Mao, X. Li, X. Luo, Q. Lin, Sybilhunter: Hybrid graph-based sybil detection by aggregating user behaviors, Neurocomputing (2022).

[26] S. Cresci, R. Di Pietro, M. Petrocchi, A. Spognardi, M. Tesconi, The paradigm-shift of social spambots: Evidence, theories, and tools for the arms race, in: Proceedings of the 26th international conference on world wide web companion, 2017, pp. 963–972.

[27] W. W. Zachary, An information flow model for conflict and fission in small groups, Journal of anthropological research 33 (4) (1977) 452–473.

[28] C. G. Fink, K. Fullin, G. Gutierrez, N. Omodt, S. Zinnecker, G. Sprint, S. McCulloch, A centrality measure for quantifying spread on weighted, directed networks, Physica A (2023).

[29] P. Jaccard, Étude comparative de la distribution florale dans une portion des alpes et des jura, Bull Soc Vaudoise Sci Nat 37 (1901) 547–579.

[30] A. Disney, Social network analysis 101: centrality measures explained, `https://cambridge-intelligence.com/keylines-faqs-social-network-analysis//`.

[31] D.-H. Vu, Privacy-preserving naive bayes classification in semi-fully distributed data model, Computers & Security 115 (2022) 102630.

[32] B. Irmak, Ş. Gülcü, Training of the feed-forward artificial neural networks using butterfly optimization algorithm, MANAS Journal of Engineering 9 (2) (2021) 160–168.

[33] A. Mehbodniya, J. L. Webber, M. Shabaz, H. Mohafez, K. Yadav, Machine learning technique to detect sybil attack on iot based sensor network, IETE Journal of Research (2021) 1–9.

[34] M. B. Torusdağ, M. Kutlu, A. A. Selçuk, Are we secure from bots? investigating vulnerabilities of botometer, in: 2020 5th International Conference on Computer Science and Engineering (UBMK), IEEE, 2020, pp. 343–348.

[35] V. D. Sharma, S. K. Yadav, S. K. Yadav, K. N. Singh, S. Sharma, Withdrawn: An effective approach to protect social media account from spam mail–a machine learning approach (2021).

sybil new

ORIGINALITY REPORT

15%	9%	9%	6%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Gordhan Jethava, Udai Pratap Rao. "User behavior-based and graph-based hybrid approach for detection of Sybil Attack in online social networks", Computers and Electrical Engineering, 2022 Publication	3%
2	d-scribes.philhist.unibas.ch Internet Source	2%
3	Submitted to Winston Churchill Middle School Student Paper	1%
4	Submitted to Higher Education Commission Pakistan Student Paper	1%
5	Gordhan Jethava, Udai Pratap Rao. "An Interaction-Based and Graph-Based Hybrid Approach to Evaluate Trust in Online Social Networks (OSNs)", Arabian Journal for Science and Engineering, 2021 Publication	1%
6	Hussain Ali, Ismaeel Malik, Saba Mahmood, Farah Akif, Javaria Amin. "Sybil Detection in	1%

	Online Social Networks", 2022 17th International Conference on Emerging Technologies (ICET), 2022 Publication	
7	Blessy Antony, S. Revathy. "Enhancing security in online social networks: introducing the DeepSybil model for Sybil attack detection", Multimedia Tools and Applications, 2023 Publication	<1 %
8	www.mdpi.com Internet Source	<1 %
9	digitalcollection.utem.edu.my Internet Source	<1 %
10	eprints.utm.my Internet Source	<1 %
11	Tianyu Gao, Jin Yang, Wenjun Peng, Luyu Jiang, Yihao Sun, Fangchuan Li. "A Content-Based Method for Sybil Detection in Online Social Networks via Deep Learning", IEEE Access, 2020 Publication	<1 %
12	scholarsmine.mst.edu Internet Source	<1 %
13	Muhammad Al-Qurishi, Sk Md Mizanur Rahman, Atif Alamri, Mohamed A. Mostafa, Majed Al-Rubaian, M. Shamim Hossain, B.B.	<1 %

	Gupta. "SybilTrap: A graph-based semi-supervised Sybil defense scheme for online social networks", Concurrency and Computation: Practice and Experience, 2018 Publication	
14	www.researchgate.net Internet Source	<1 %
15	snap.stanford.edu Internet Source	<1 %
16	Submitted to Colorado State University, Global Campus Student Paper	<1 %
17	www.svnit.ac.in Internet Source	<1 %
18	Submitted to University of Leeds Student Paper	<1 %
19	1library.net Internet Source	<1 %
20	Jian Mao, Xiang Li, Xiling Luo, Qixiao Lin. "SybilHunter: Hybrid Graph-based Sybil Detection by Aggregating User behaviors", Neurocomputing, 2022 Publication	<1 %
21	Submitted to Heriot-Watt University Student Paper	<1 %
	link.springer.com	

22	Internet Source	<1%
23	pdfs.semanticscholar.org Internet Source	<1%
24	digitalcommons.usf.edu Internet Source	<1%
25	repository.bilkent.edu.tr Internet Source	<1%
26	www.nmit.ac.in Internet Source	<1%
27	Swapnaa Jayaraman. "Six degrees of jonathan grudin", Proceedings of the 2004 ACM conference on Computer supported cooperative work - CSCW 04 CSCW 04, 2004 Publication	<1%
28	Qingqing Zhou, Guo Chen. "An Efficient Victim Prediction for Sybil Detection in Online Social Network", IEEE Access, 2020 Publication	<1%
29	Aditya Kaushik, Aditya Sehgal, Smit Vora, Vatsal Palan, Suchita Patil. "Presaging The Signs Of Diabetes Using Machine Learning Algorithms", 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT), 2021 Publication	<1%

30	Submitted to Bahcesehir University Student Paper	<1%
31	Gao, Hongyu, Jun Hu, Tuo Huang, Jingnan Wang, and Yan Chen. "Security Issues in Online Social Networks", IEEE Internet Computing, 2011. Publication	<1%
32	Zheng Qu, Chen Lyu, Chi-Hung Chi. "MUSH: Multi-Stimuli Hawkes Process based Sybil Attacker Detector for User-Review Social Networks", IEEE Transactions on Network and Service Management, 2022 Publication	<1%
33	Submitted to London College of Contemporary Arts Student Paper	<1%
34	fdocuments.us Internet Source	<1%
35	prr.hec.gov.pk Internet Source	<1%
36	www.coursehero.com Internet Source	<1%
37	bradscholars.brad.ac.uk Internet Source	<1%
38	Digital Pictures, 1995. Publication	<1%

39	Munmun Bhattacharya, Sandip Roy, Samiran Chattopadhyay, Ashok Kumar Das, Sachin Shetty. "A comprehensive survey on online social networks security and privacy issues: Threats, machine learning-based solutions, and open challenges", SECURITY AND PRIVACY, 2022 Publication	<1 %
40	coek.info Internet Source	<1 %
41	de.slideshare.net Internet Source	<1 %
42	ebin.pub Internet Source	<1 %
43	mafiadoc.com Internet Source	<1 %
44	scholarworks.utep.edu Internet Source	<1 %
45	Elmira Pourabbasi, Vahid Majidnezhad, Saeid Taghavi Afshord, Yasser Jafari. "A new single-chromosome evolutionary algorithm for community detection in complex networks by combining content and structural information", Expert Systems with Applications, 2021 Publication	<1 %

46	Submitted to Greenwich School of Management Student Paper	<1 %
47	Yuto Yamaguchi, Toshiyuki Amagasa, Hiroyuki Kitagawa, Yohei Ikawa. "Online User Location Inference Exploiting Spatiotemporal Correlations in Social Streams", Proceedings of the 23rd ACM International Conference on Conference on Information and Knowledge Management - CIKM '14, 2014 Publication	<1 %
48	Zineb Ellaky, Faouzia Benabbou, Sara Ouahabi. "Systematic Literature Review of Social Media Bots Detection Systems", Journal of King Saud University - Computer and Information Sciences, 2023 Publication	<1 %
49	arxiv.org Internet Source	<1 %
50	docs.mipro-proceedings.com Internet Source	<1 %
51	vdoc.pub Internet Source	<1 %
52	webthesis.biblio.polito.it Internet Source	<1 %
53	www.ncbi.nlm.nih.gov Internet Source	

		<1 %
54	www.tandfonline.com Internet Source	<1 %
55	Imrul Kayes, Adriana Iamnitchi. "Privacy and security in online social networks: A survey", Online Social Networks and Media, 2017 Publication	<1 %
56	Lecture Notes in Computer Science, 2015. Publication	<1 %
57	Zhen Wang, Chris T. Bauch, Samit Bhattacharyya, Alberto d'Onofrio et al. "Statistical physics of vaccination", Physics Reports, 2016 Publication	<1 %

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		