國 立 中 央 大 學

資 訊 工 程 學 系
碩 士 論 文

Uncovering Internet Armies on PTT

研究生: 卓沛妤
指導教授: 許富皓

中 華 民 國 一 百 一 十 一 年 六 月

國立中央大學圖書館學位論文授權書

填單日期：111 / 7 / 1　　2019.9 版

授權人姓名	卓沛妤	學 號	109522020
系所名稱	資訊工程研究所	學位類別	■碩士　□博士
論文名稱	Uncovering Internet Armies on PTT	指導教授	許富皓

學位論文網路公開授權

授權本人撰寫之學位論文全文電子檔：

・在「**國立中央大學圖書館博碩士論文系統**」.

(✓)同意立即網路公開

(　)同意 於西元＿＿＿年＿＿＿月＿＿＿日網路公開

(　)不同意網路公開，原因是：＿＿＿＿＿＿＿＿＿＿

・在**國家圖書館「臺灣博碩士論文知識加值系統」**

(✓)同意立即網路公開

(　)同意 於西元＿＿＿年＿＿＿月＿＿＿日網路公開

(　)不同意網路公開，原因是：＿＿＿＿＿＿＿＿＿＿

依著作權法規定，非專屬、無償授權國立中央大學、台灣聯合大學系統與國家圖書館，不限地域、時間與次數，以文件、錄影帶、錄音帶、光碟、微縮、數位化或其他方式將上列授權標的基於非營利目的進行重製。

學位論文紙本延後公開申請 (紙本學位論文**立即公開者此欄免填**)

本人撰寫之學位論文紙本因以下原因將延後公開

・**延後原因**

(　)已申請專利並檢附證明，專利申請案號：

(　)準備以上列論文投稿期刊

(　)涉國家機密

(　)依法不得提供，請說明：＿＿＿＿＿＿＿＿

・**公開日期**：西元＿＿＿＿年＿＿＿＿月＿＿＿＿日

※繳交教務處註冊組之紙本論文(送繳國家圖書館)若不立即公開，請加填「國家圖書館學位論文延後公開申請書」

研究生簽名：卓沛妤　　指導教授簽名：許富皓

*本授權書請完整填寫並親筆簽名後，裝訂於論文**封面之次頁**。

國立中央大學碩士班研究生

論文指導教授推薦書

資訊工程 學系/研究所 卓沛妤 研究生所提之論文 Uncovering Internet Armies on PTT 係由本人指導撰述，同意提付審查。

指導教授 [signature] (簽章)

111 年 5 月 10 日

104.07.24

國立中央大學碩士班研究生

論文口試委員審定書

資訊工程學系碩士班學系/研究所卓沛妤研究生

所提之論文 Uncovering Internet Armies on PTT

經本委員會審議，認定符合碩士資格標準。

學位考試委員會召集人 孫宏民

委　　員 許通安

黃俊穎

中華民國 111 年 6 月 30 日

101.06.15

中文摘要：

由於網路平台的大幅擴張，網軍(Internet army)這個工作也隨之增加，公關公司會付錢給學生或無工作者，讓他們發文或回覆來影響輿論風向。

PTT 在台灣是相當大的網路平台，由於其匿名性以及能見度高，大量的網軍因此將這個平台視為主要的攻擊對象，許多網軍會針對特殊議題進行帶風向。

因此，找到一種方法來偵測匿名平台中的網軍是很重要的議題。在此篇研究中，I.A.D 系統針對網軍進行分析獲得數個網軍的特徵，並藉由網軍特徵建立預測模型，使系統能夠判斷使用者是否是網軍。

關鍵字：網軍偵測、PTT、機器學習

Abstract:

As the expansion of online social network, the occupation number of Internet army has increased. Students or unemployed post some article or reply to get paid by public relationship company, who are also known as paid poster, would impact peoples' opinions.

In Taiwan, PTT is such a large platform with anonymity and visibility. Because of influence of PTT, it has become a main target of Internet armies. Therefore, it is an important issue to find out a method to detect Internet armies on anonymous platform. In this research, I.A.D. system(Internet Armies Detection) analyze and find out some the features of Internet army. In addition, I.A.D. also build predicted models by features of Internet army. This makes the system to identify whether a user is Internet army or not.

CONTENTS

1.Introduction

The Internet army, also called the Internet water army, is organized by a large number of people. This new type of occupation has become popular with the fast expansion of the Internet. These people, often hired by public relationship (PR) companies, get paid by posting articles or sharing some purposeful comments. If there are enough Internet armies on the Internet, they can create a hot or trending topic to benefit their customer. For instance, creating a hot topic before a TV show is broadcast, the host company hires Internet armies to publish some positive or negative news to attract attention and trigger curiosity.

PTT is a unique platform in Taiwan unlike other online social networks, PTT is the largest bulletin board system built in 1995. It is definitely an anonymous platform which allows people to communicate and share experiences. In Taiwan, it is such an influential platform that has organized many large protests. Because of the influence of PTT, it became a large target of Internet armies.

Internet army detection is slightly different from fake accounts detection. Internet armies spread disinformation to impact people's thinking about target issues. However, fake accounts might spend time propagating spam messages, spreading malware, and pretending to be new followers. Internet army detection have such different purposes that they need to find a new method on Internet armies detection.

Although the importance of Internet army detection, there is little research on these fields. Compared with Internet army detection, many different researches have been

presented to detect fake accounts with different approaches. In fake accounts detection, there are two types of approaches, featured-based approaches, and graph-based approaches.

For the featured based approaches, researchers collect different attributes such as numbers of followers, numbers of tweets, number of times the user was replied to, and so on. [5] By analyzing these attributes, researchers could distinguish whether the account is fake or not. Researchers also use different machine learning algorithms to progress the accuracy of fake account detection.

On the other hand, graph-based approaches regard user relationships as more important things. They always care more about users who reply to the same article and get their similarity of user activity. For example, users who always take the same activity can be identified as the same group. If someone in a group is exposed as a fake account, others accounts in this group have higher probability to be a fake account as well.

Since such previous works on fake accounts, there exist Internet army detection based on featured based approaches and graph-based approaches. Cheng Chen et al. used ground truth to find out potential paid posters. Then they analyze these potential paid posters in order to investigate their features. According to the analysis results, they used LIBSVM as the tool to model and classify potential paid posters. On the other hand, Guirong Chen et al. used a graph-based approach which investigated synchronic activity of the Internet water army on BBS. They construct the social networks based on users' behaviors similarity and use an hierarchical clustering algorithm to cluster users.

In this research, I designed a new approach, called I.A.D. system, to detect Internet armies specifically on PPT. I.A.D. focused on detecting and characterizing Internet armies. Firstly, I.A.D. propose an assumption of Internet armies that corresponds to objectives defined in public. Based on this assumption, it labeled the users whether they are Internet armies or not on PTT. Secondly, I.A.D. analyze the behavioral patterns of Internet armies and identify several key features. These features are so different from normal online social networks because of the anonymity and characteristics of PTT. Finally, these specific features were used to understand the accuracy of Internet army detection on different machine learning methods.

1.1 Research Motivation

Internet armies have become a large problem because it results in detriment to online experience and trust. Internet armies, also called paid posters or Internet water army, earn money by posting comments and articles. Because of the expansion of online social networks, the job opportunity of Internet armies is rapidly growing. They were used in a good way to promote a brand or a new product. However, Internet armies were used in malicious ways. For example, spreading negative news about their political rivals.

PTT is such a popular platform that is used by lots of people. Because of the anonymity, people are more willing to share their experiences and information. It also has a strong influence on public issues. Because of its influence, PTT has become a hot target of Internet armies. There is a reason why we need to find a good approach to detecting Internet armies on PTT to increase people's trust online and reduce online influence by public relationship (PR) companies.

1.2 Contribution

PTT is a unique social platform in Taiwan. However, because of its influence, there are lots of Internet armies that launch information warfare on PTT. In this research, I designed an approach to detect internet armies on PTT, called I.A.D. system, which is totally different from normal online social networks. Moreover, I.A.D. system retrieved a few features about Internet armies on PTT. These features were used in different machine learning algorithms and built models. In this research, I.A.D. system can identify an unknown user whether he/ she is an Internet army or not.

2. Background

In this section, I introduce two important topics of my thesis in more detail, the Internet army, and the PTT Bulletin Board System.

2.1 Internet army

Internet armies are a group of writers online who always publish lots of opinions or comments in a short time on online social networks. They were paid to launch information warfare or media framing. For example, They share comments to change people's opinion on a particular issue and publish some negative news to attack their competitor for their purpose. This type of job is rapidly growing because of the high use of online social networks, such as Facebook, Twitter, etc. Internet armies are referred to as the "Internet water army" in China, who are well organized to launch flood-like information warfare with large size of people. Companies or political parties use lots of comments to impact particular issues.

The social media about Internet armies did not just appear in China. In fact, it is a worldwide phenomenon. In 2020, Joe Biden won the US presidential election. President Donald Trump has filed dozens of lawsuits across the country in an attempt to contest the election results. As Donald Trump continued to dispute the result of the US election, many misleading posts had been spreading on social media about the vote. These posts declared that dead people were casting votes in the key state of Michigan. However, Michigan authorities clarify that these posts were misinformation. [1]

In addition, Facebook has reported disinformation campaigns recently. It revealed that Russia continues to be the largest producer of disinformation on social media, with the country being the source of the fakest and misleading Facebook accounts. This report also mentioned that Facebook discovered dozens of accounts of abnormal behavior targeting Americans during the 2020 U.S. presidential election. The top three sources of those networks of these abnormal accounts were Russia, Iran, and the U.S. itself.[2]

The problem of Internet armies has increased because of the success of online social networks. Internet armies will hide behind the network and launch information warfare, for example, spreading disinformation to impact people's thinking about target issues. This is the reason why we need to find an effective method to defend Internet armies and identify these malicious users.

2.2 PTT Bulletin Board System

PTT Bulletin Board System also called "批踢踢實業坊", is called PTT for short. It is the largest bulletin board system (BBS) in Taiwan. It was founded by Yi-Chin Tu and other students from the National Taiwan University in 1995. PTT was constructed by Linux and open-source software for the first time. At first, PTT was used as an academic platform, which is used to discuss class information online. As other BBS which were constructed by other schools gradually faded away, PTT gradually became the largest platform to discuss news and issues and nowadays is used by various types of people.

PTT has more than 1.5 million registered users. During peak hours, there were over 150,000 users online. The BBS has over 20,000 boards covering multiple types of topics. and more than 20,000 articles and 500,000 comments are posted every day. Each board

has its rule to manage users' activities, such as publishing articles and reply, in its board. Users are limited by their number of logins, which count only once a day. In other words, users could publish articles and reply to articles if they log in for enough days.

PTT has a black backboard with white words. Its articles are always without pictures and videos. People only use words to communicate with each other. Users will share their opinions and comment on the article.

The commendation system in PTT implements an article commendation (推文) and criticism (噓文) scheme. Users could agree with poster using commendation(推文) and disagree with poster using criticism(噓文). Moreover, commendation and criticism give a score for the article. Under this system, users can evaluate an article by giving it a tuei (推), adding a point, or a hsü (噓), subtracting a point. Finally, an article will get a score from the system. When the score is higher than 100, the article is so popular, also called bào（爆）, in PTT.

Unlike other online social media, a user profile only shows some basic information about the user. For instance, it shows the number of days from the register, whether the user is online, the number of posts, and so on. Therefore, it is hard to detect Internet armies only using user information.

Each article is posted on a particular board. Each board restricts its context by its rules. For example, the "Boy-Girl" board only discusses relationship issues, and the "Baseball" board only talks about baseball games or baseball players.

The PTT post page is really simple. An article comprises the author's user ID, posting time, posting board, and context. On the other hand, the article context usually consists of words instead of videos and pictures. Replies to the post below article also consist of words too. The number of characters is limited in each reply. It can be believed that users need to spend more time than other online social media in launching an article. Therefore, since more replies in an article will make the article become a hot topic, which catches people's attention and affect people on particular issues, Internet armies would spend more time on replying to other articles rather than publishing an article in PTT.

PTT has many types of board, including news information, jobs discussion, normal chat, and movie discussion. The most popular board is the Gossiping board, which has most people online all the time. In "Gossiping", people would talk about worldwide issues, political issues, gender issues, and hot topics.

Because of the Gossiping discussion and its popularity, it can believe that there are potentially many hidden Internet armies. For example, Hui-RuYang and her Internet armies were accused of contempt of cop because they indirectly result in the suicide of diplomats by hype negative information. Other boards such as the "Movie" board, the "C_Chat" board, etc. different from the Gossiping, people discuss more casual topics on these boards. It is the reason why these boards are not considered as the main target of Internet armies.

3. Related work

In this section, first of all is to introduce the related work of Internet army detection. However, because there are few related works of Internet army detection, it also refer to the method of fake accounts detection.

3.1 Internet Army Detection

Previous studies usually focused on online social media, such as Sina and Sohu. Cheng Chen et al. disclosed the organizational structure of the Internet army (a.k.a. Internet water army) and investigated the behavior pattern on the comments of Sina and Sohu news. However, because Sina and Sohu are normal online social media, their user profile would be helpful to detect the internet army. [3]

The Bulletin board system (BBS) system is different from normal social media. The BBS system is more anonymous which is unable to get information from user profiles such as online time or personal information to distinguish someone's identity. Guirong Chen et al. propose a divide-and-conquer algorithm according to the fact that the Internet army always appears in groups. It compares user behavior similarity between user's pairs to build a graph and show their similarity. Then they delete the edges which are under a certain threshold. Finally, they used a hierarchical clustering algorithm on the pruned network to find out big clusters. [4]

3.2 Fake Account Detection

Fake accounts were registered by duplicate information or fake information. They perform various malicious activities such as spreading spams, phishing URLs, malware, disinformation [11, 12], and stealing private user data.

Although there are few studies in the Internet army, much research on fake account detection is closely related to Internet army detection. Inspired by the importance of fake account detection, many researchers investigate efficient fake account detection. Most detection mechanisms
attempt to classify fake accounts by feature-based detection or graph-level structures.

3.2.1 Feature based detection

This approach relies on user-level activity and account detail, such as user profiles. Features were extracted from users' daily activity and association with other users, then those features were applied to build classifiers through different machine learning approaches. Ahmed El Azab et al. determined the minimized set of the main factors which influence the detection of fake accounts, and these factors were applied on different classification algorithms. [5] Supervised machine learning techniques are used to identify fake accounts on a Twitter dataset with different extracted features. [6,7] The research on Facebook also considers more features about user activity such as likes, comments, tagging, and sharing. [8]

Many researchers have used lots of different machine learning algorithms on fake accounts detection. Sarah Khaled et al. designed a new algorithm that combined the SVM and NN, called the “SVM-NN” algorithm to detect whether the user is fake or real.[9]

3.2.2 Graph-based approaches

Compared with feature-based approaches, Graph-based approaches take more computation on building a graph. In Graph-based approaches, every network can be defined as G=(V, E). They build a graph by adding edges between users based on the similarity of users' activity. For example, two users often reply to the same article or same publisher, which would add a thick edge between the two users. The thickness between two users depends on user activity or profile similarity. The thicker edges mean the higher similarity between the two users.

Because fake accounts always have strict requirements on their mission such as level of prevalence and strict deadline[10], they'll have the same target and perform similarly. Therefore, according to the graph-based approach, researchers can build a network, then find subgraphs to find groups of fake accounts.

4. Methodology

The first part of the method is introducing system architecture in this research, I.A.D. system. The second part is system execution flow, which introduced the detail of how the system execute.

4.1 System Architecture

I.A.D. is the system that was designed in this research. The I.A.D. system provided a method that can identify Internet armies on the BBS platform. Fig.1 is the I.A.D. system architecture. Firstly, the data collector of I.A.D. would collect the data and transfer data into local storage. Then local storage transmits data to the data analyzer. The data analyzer would analyze the data which contain user activities, label the potential Internet armies and analyze the Internet armies features. With these features, the result generator can generate an answer whether a user is Internet army or not. In the result generator, there are three types of a model built by SVM, random forest, and decision tree.

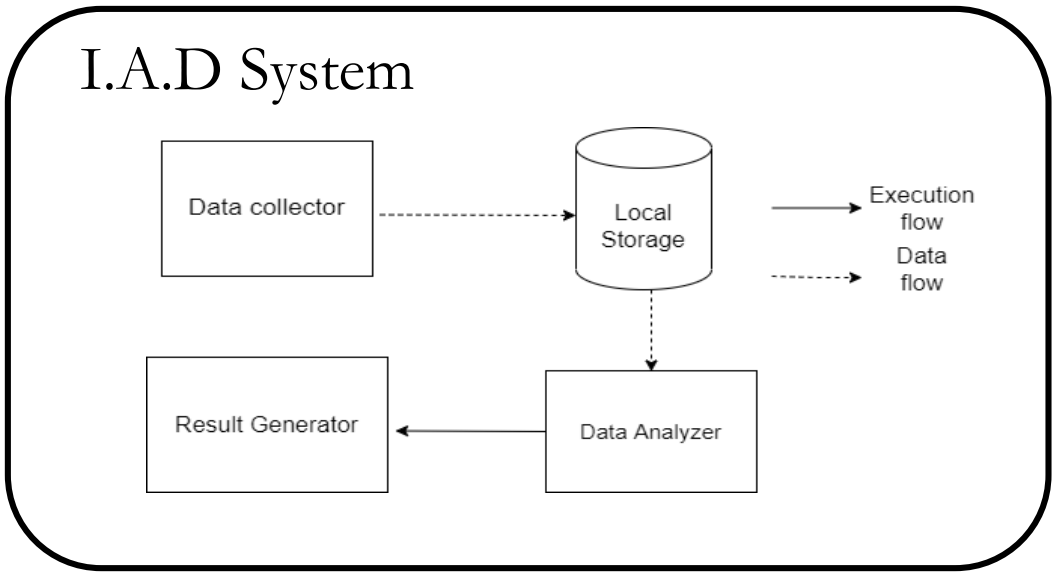

Fig.1: I.A.D. System Architecture

4.2 System Execution Flow

In Fig.2, this picture shows the simple system execution flow. It first collects data by I.A.D data collector. Then I.A.D data analyzer would label potential Internet armies and analyze Internet armies features based on the collected users' activities and the label. Finally, using the features and taking three different classification algorithms which were used by fake account detection. Then building the model that would be able to identify a user whether he/she is Internet army or not.

To introduce the experiment in more detail, Fig.3 shows the detail of system execution flow. Firstly, I.A.D searched the hot article in "Gossiping " which believed that more Internet armies exist. Below the article, all the user IDs were collected. PTTBrain is a website that collects the user's activities in the last six months in PTT. In this step, I.A.D. search the user activities and collect all the activities in August 2020 based on collected user IDs.After collecting user activities, it is important to label the Internet armies. By defining a few ground truths, I.A.D. has the standard to label a user whether he/she is Internet army or not. The next step is to collect the label results and the user activities into MySQL. With the label results and user activities, I.A.D. could find out some features that were useful in Internet armies detection. Finally, I.A.D takes advantage of features and splits the data into training data and testing data.

Then using training data to build three different models by three different classification algorithms, SVM, random forest, and decision tree. After building three different models, I.A.D. conduct the performance evaluation by their testing data.

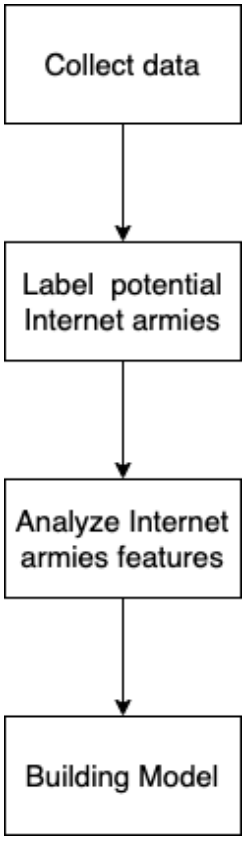

Fig.2 System Execution Flow

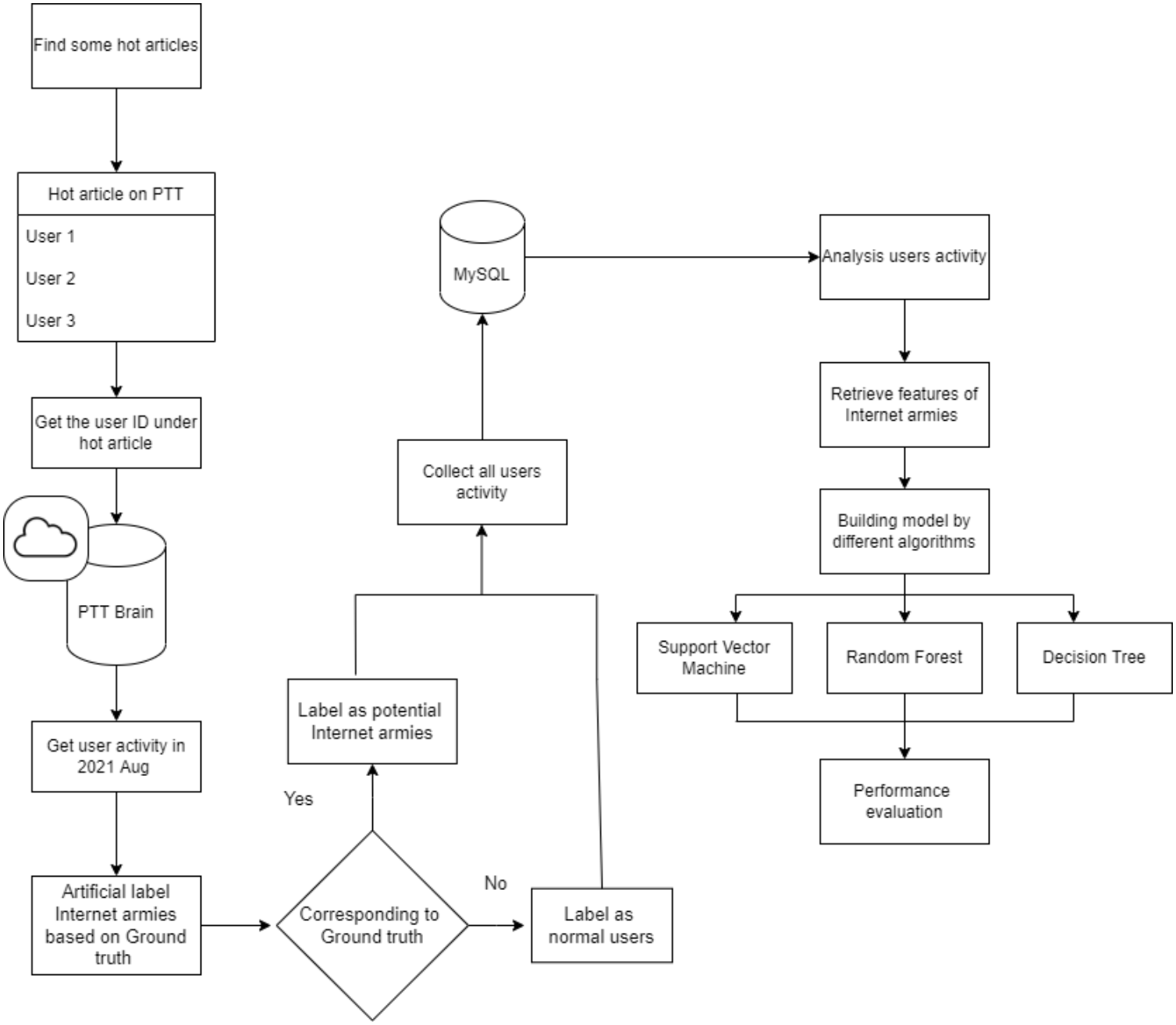

Fig.2 The details of System Execution Flow

4.2.1 Data collection

To design an approach to detect Internet armies on PTT, the system need to collect real-world datasets firstly. I.A.D. used a dataset from PTTBrain, which collects and tidies

up users' data in PTT. In PTTBrain, a user's daily activity was collected on their website.

In this research, I.A.D. assumed that Internet armies must exist in hot news, especially about policy. In this assumption, the system randomly collect replies posters on these hot news. Then I.A.D. system find out these users' activities by PTTBrain. I.A.D. collect users' activities from August 1, 2021, to August 31, 2021. For each user, I.A.D. recorded the following relevant information: article name(reply to which article), reply content, reply date, reply time, article post DateTime, floor, and board name(reply to which board).

4.2.2 Manual Identification

In order to identify Internet armies, setting a confident "ground truth" is an important thing to accomplish Internet armies detection. The reason why we need to set "ground truth" is that we could not know someone is an Internet army unless he/she confesses or the public relations companies exposed all the Internet armies accounts. In fake account detection, researchers can detect fake accounts based on their malicious activity and have datasets for fake accounts. Because fake accounts may have many types of jobs such as spreading malware or advertisements, they present abnormal activities.

Whereas Internet armies most important job is to launch information warfare and change spin control. They need to influence public opinion in favor of the target issue. Therefore, they need to hide behind people and pretend to be normal users. Their activities are more similar to normal users compared with fake accounts.

Potential Internet armies correspond to at least one of the following "ground truth".

1. Potential Internet armies use duplicate words in their replies such as particular political party, particular vaccine, and particular hate speech.
2. Potential Internet armies always reply to similar articles in order to influence public opinion on target issues.
3. Because Internet armies get more paid by posting more comments, they have a tendency to not interact with other users, which can reduce time to read other users' reply content.
4. Potential Internet armies spend most of their time on target issues and articles. They rarely share their experience or chat with other users.
5. Some potential Internet armies only reply on weekdays. They even did not have activities on weekends.

It is believed that any reasonable person would agree that a user who posts thirty replies with similar words is a potential Internet army. On the other hand, any reasonable person would agree that a user who posts more than forty replies to the same issue in different article threads is also a potential Internet army. As a result, 52 potential Internet armies and 53 normal users were identified and used in the final machine learning training.

4.2.3 Experiment

In this research, I.A.D. took the following steps to build the model of Internet armies detection.

Step:

1. Firstly, I.A.D collect the user id of repliers from several popular articles.

2. I.A.D. searched for this user history activity from Aug 1st to Aug 30th on PTT Brain. By their user history, I.A.D. system also label the potential Internet armies based on “ground truth”.
3. After I.A.D. label the users, I.A.D. find out several features that may influence whether a user is an Internet army or not.
4. I.A.D. used the features tha have found on three different machine learning algorithms, support vector machine, decision tree, and random forest. Comparing these different algorithms and finding out the greatest predict model.

5. Evaluation

In this section, the first part is the feature analysis of Internet army, which were labeled by artificial. After labeling the users, there are some remarkably outcomes. It shows that there are different features between Internet armies and normal users. The last part is the performance evaluation of three different models.

5.1 Feature Analysis

In this section, it performs the analysis of investigated features that are useful in capturing potential Internet armies. I.A.D. use the PTTbrain dataset as its training data. I.A.D. collected the user dataset and performed the statistical analysis. Firstly, I.A.D. perform four features that have an influence on Internet armies detection: average interval time, number of replies on a daily average, board weight, and reply to article time. In the following figures, I use “ia” as Internet armies and “nu” as normal users.

5.1.1 Average Interval Time

In Fig.1, I.A.D. calculated the average interval reply time between two replies by the same users. Compared to normal users' behaviors, the reply behavior of these potential Internet armies is very concentrated over a period of time. It can be believed that Internet armies submit their replies as often as possible because they get paid by how many replies they have submitted.

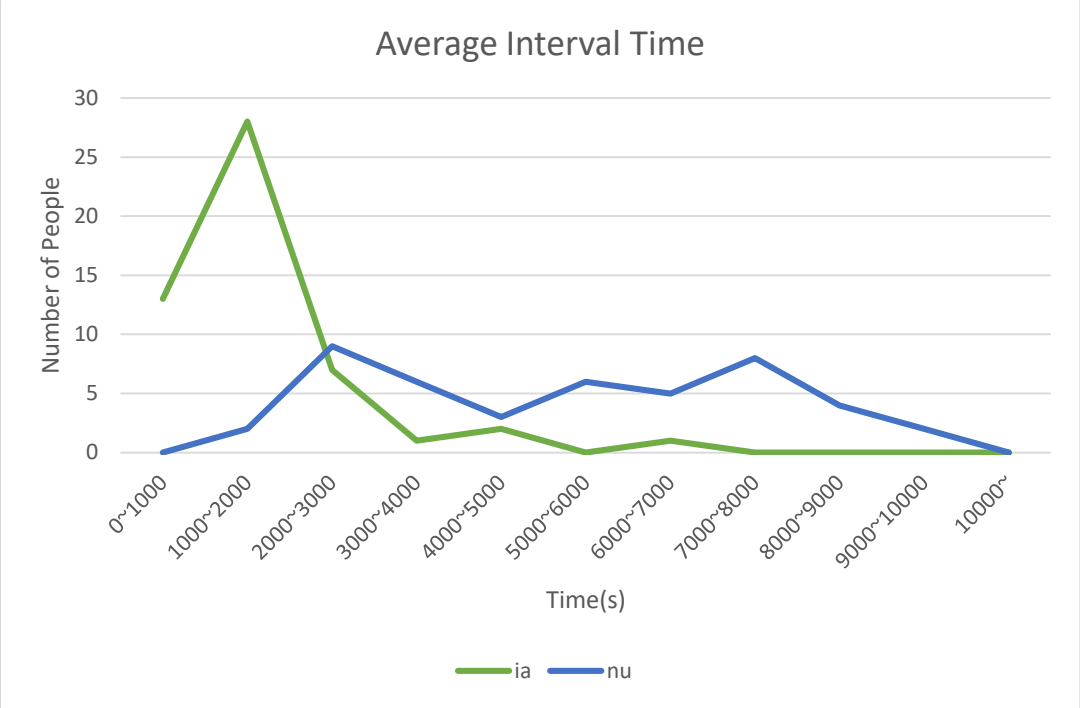

Fig.1 Average Interval Time: the figure demonstrated that most Internet armies(ia) submitted the second reply after 2000 seconds on average. Normal users' (nu) average interval time of reply are more separated.

5.1.2 Number of Replies

In addition to the average interval time of replies, I.A.D. also count the number of replies in a day on average. In Fig.2, it demonstrated that normal users' daily replies are around 0~20 replies. However, Internet armies' daily replies are separated from 30~100 replies. Because Internet armies need to hype their target topics. They need to submit more replies and increase the article score to be hot, also called bào（爆）, in PTT.

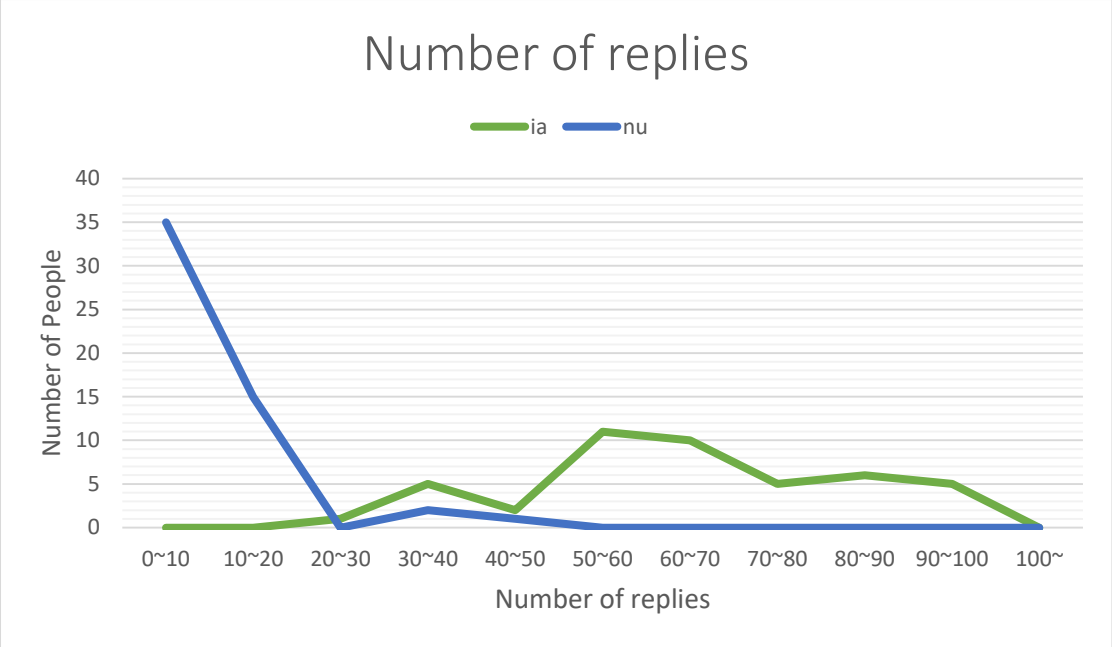

Fig.2 Number of Replies: Most of normal user daily replies are around 0~20 on average. Internet armies' daily replies are around 30~100 on average.

5.1.3 Board Weight

In the“Gossiping” board and the “HatePolitics”, people would talk about worldwide issues, political issues, gender issues, and hot topics. It could be believed that there are potentially many hidden Internet armies because these boards would talk about many influential issues.

In this section, I.A.D. calculated the percentage of replies on “Gossiping” and “HatePolitics”, compared with all the user replies. In Fig.3, it shows that most of their replies were in “Gossiping” and “HatePolitics”, and their board weight concentrated in 0.8 to 1. It indicates that Internet armies pay more attention to “Gossiping” and “HatePolitics”.They were not willing to waste their time on others' boards. Nevertheless, the board weight of normal users was separated. It shows that they have the characteristics of randomness and heterogeneity.

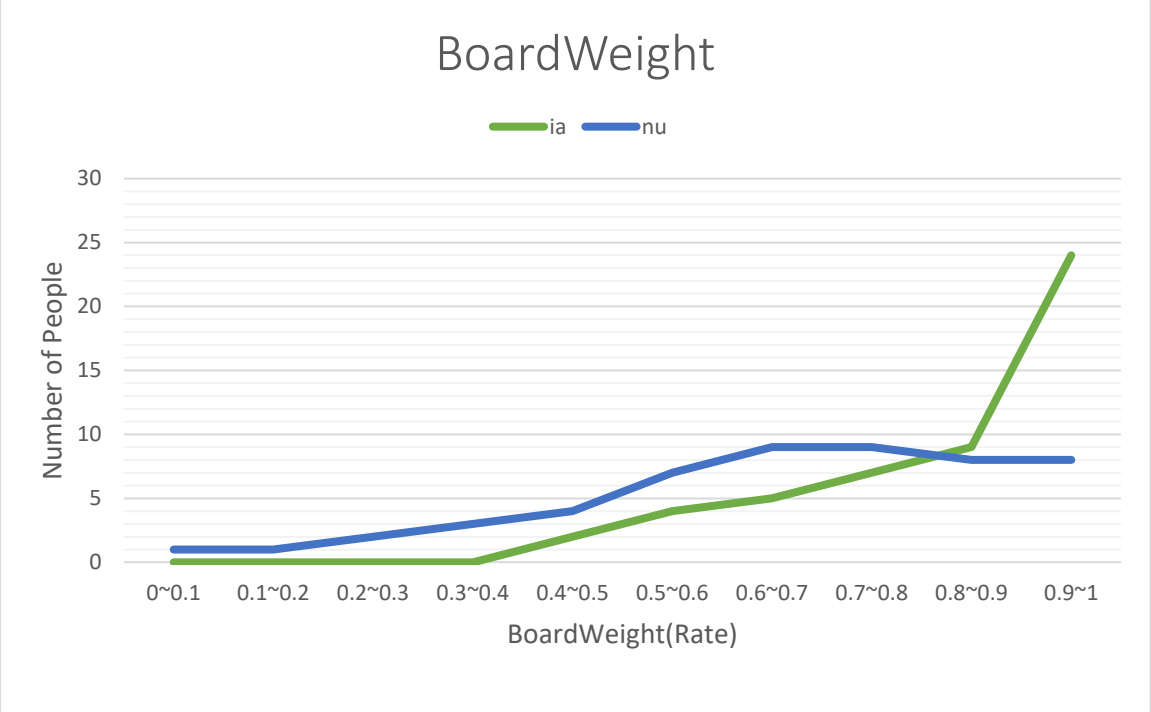

Fig.3 Board Weight: The board weight of normal users was a smooth line. The board weight of Internet armies has a steep rise of 0.8.

5.1.4 Reply to Article Time

I.A.D. calculated the time interval from posts by the author to replies by the users. Fig.4 illustrates that Internet armies reply to their target article faster than normal users. When a new mission starts, they need to hype their targeted discussion in a short period of time. Therefore, their average time interval of replies to articles will be shorter than normal users.

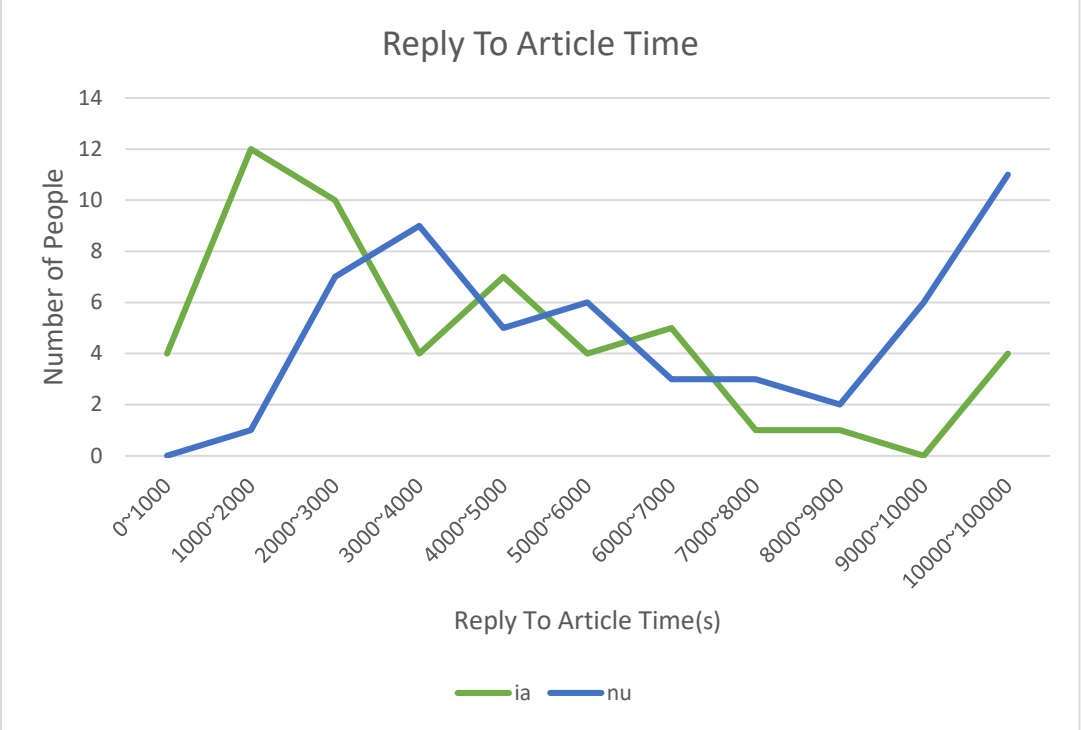

Fig.4 Reply To Article Time: Internet armies perform a shorter reply time interval than normal users.

5.2 Identify Internet armies

In this section, I.A.D. focus on building machine learning models to identify Internet armies based on the four features. It train three different classification algorithms to build the models. These algorithms are: Random Forest [16], [17], Decision Tree [18], and Support Vector Machine [19]. The outcome was performed by five standard indicators which are calculated by a confusion matrix. These five standard indicators are True positive rate(TPR), True negative rate(TNR), False positive rate(FPR), False negative rate(FNR), and accuracy.

5.2.1 Experiment result

Table 1 presents five indicator values by applying three classification algorithms. This table shows that Support Vector Machine(SVM) has the highest

accuracy. True positive rate(TPR), also called recall, has the same outcome between SVM and random forest. On the other hand, the higher precision means the higher percentage of true positives compared with the number of labeled positive classes.

	TPR(Recall)	TNR	PPV(Precision)	NPV	Accuracy
Decision tree	0.9	0.92	0.95	0.85	0.91
Random forest	0.95	0.92	0.95	0.92	0.94
SVM	0.95	1	1	0.92	0.97

Table1 Experiment result: These table shows three different model on standard indicator outcomes: True positive rate(TPR), True negative rate(TNR), False positive rate(FPR), False negative rate(FNR), and accuracy.

6. Conclusion

PTT is an influential social platform that is a hot target for Internet armies. Internet armies would launch information warfare and impact people's opinions. In this research, I defined a ground truth that was used to label potential Internet armies. After labeling the Internet armies and collecting users' activity, The I.A.D found some features which can be used to identify Internet armies efficiently on PTT. In addition, I.A.D. also built three different machine learning models. SVM is the best classification method in these three predicted models.

In the future, researchers can use a larger dataset to find out more features that can help in detecting Internet armies.

6.1 Future work

This research shows that feature-based classification is a helpful classification method. However, it still could be improved. In I.A.D system, it take same number of normal users and Internet armies as the training data. But normal users have higher percentage in real situation. It may be a better solution to higher up the rate of normal users in further experiment. On the other hand, due to the similarity of the features in social network, it is reasonable that I.A.D system can be used in the wider range.

Reference

1. https://www.bbc.com/news/election-us-2020-54811410
2. https://www.usnews.com/news/politics/articles/2021-05-26/russia-still-largest-driver-of-disinformation-on-social-media-facebook-report-finds
3. Cheng Chen, Kui Wu ,Venkatesh Srinivasan ,Xudong Zhang. ”Battling the Internet Water Army: Detection of Hidden Paid Posters “ in 2013 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining
4. Guirong Chen, Wandong Cai, Jiuming Huang, Xianlong Jiao.” Uncovering and Characterizing Internet Water Army in Online Forums ” in 2016 IEEE First International Conference on Data Science in Cyberspace
5. A. E. Azab, A. M. Idrees, M. A. Mahmoud, and H. Hefny, "Fake Account Detection in Twitter Based on Minimum Weighted Feature set," International Journal of Computer, Electrical, Automation, Control and Information Engineering, vol. 10, no. 1, pp. 13-18, 201
6. S. Crescia, R. D. Pietrob, M. Petrocchia, A. Spognardia and M. Tesconia, "Fame for sale: efficient detection of fake Twitter followers," Decision Support Systems, vol. 80, pp. 56-71, 2015.
7. S. Khaled, H. M. O. Mokhtar, and N. El-Tazi, "Detecting Fake Accounts on Social Media," in 2018 IEEE International Conference on Big Data (Big Data), Seattle, WA, USA, 2018.

8. A. Gupta and R. Kaushal, "Towards Detecting Fake User Accounts in Facebook," 2017
9. Sarah Khaled, Neamat El-Tazi, Hoda M. O. Mokhtar. “Detecting Fake Accounts on Social Media ”2018 IEEE International Conference on Big Data (Big Data)
10. Qiang Cao, Xiaowei Yang, Jieqi Yu, Christopher Palow. “Uncovering Large Groups of Active Malicious Accounts in Online Social Networks” Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. November 2014 Pages 477–488
11. Hacking Financial Market. 2016. http://goo.gl/4AkWyt
12. Kurt Thomas, Chris Grier, Justin Ma, Vern Paxson, and Dawn Song. 2011. Design and evaluation of a real-time URL spam filtering service. In IEEE S & P
13. Quinlan, J. R. (1987). "Simplifying decision trees". International Journal of Man-Machine Studies. 27 (3): 221–234. CiteSeerX 10.1.1.18.4267.
14. L. Breiman, "Random forests," Machine Learning, 2001.
15. T. Joachims, Learning to Classify Text Using Support Vector Machines: Methods, Theory, and Algorithms. Boston: Kluwer Academic Publishers, 2002.
16. L. Breiman, "Random forests," Machine Learning, 2001.
17. Manuel Fern_andez Delgado, Eva Cernadas, Sen_en Barro, and Dinani Amorim, "Do we Need Hundreds of Classifiers to Solve Real World Classification Problems?," Journal of Machine Learning Research, vol. 15, pp. 3133-3181, 2014.
18. Lior Rokach and Oded Maimon, Data Mining and Knowledge Discovery Handbook - Chapter 9 (Decision Trees), Oded Maimon and Lior Rokach, Eds., 2005.
19. T. Joachims, Learning to Classify Text Using Support Vector Machines: Methods, Theory, and Algorithms. Boston: Kluwer Academic Publishers, 2002