International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 5, Issue 1
January 2018

ExR: A Proposed Framework to Detect Potential Suspects Involved in Illicit Activities Via OSN

Ms. Juhi Patel
Babu Madhav Institute of Information Technology, Uka Tarsadia University,
Bardoli, Gujarat

ABSTRACT

In these recent years, crimes throughout the world have increased drastically, exhibiting varying and innovative modus operandi thus evolving in parallel with the technology advancements. Most of the criminal offences whether cyber or contemporary are based on gaining financial benefits. Out of all the financial offences, organ harvesting, trafficking and illicit trading are some of the major crimes that have attained favoritism among cross border smugglers. These smugglers exploit the online social networks to plan out their activities, expand their gangs and identify potential victims. Although government agencies have tried to come up with technical solutions for these problems, usage of advance technology and its applications still need to be explored. This paper proposes a framework that could be used to identify a potential suspect carrying out illegal activities through an online social network. The paper also proposes a self-learning based intelligent scanner as a pre-requisite to the proposed framework

Keywords

Suspect,post, comments, crime, offenders, online social network.

1. INTRODUCTION

The current statistics of conviction ratio for crimes is very low which play a role in motivating criminal offenders to do more crimes. [1] Among all the reported crimes, only a minority of them reach a conviction [2] as many of them fall prey to delayed trials, missing or tampering evidences, poor investigation, hostile victims, hostile witnesses and missing or tampered testimonies.

Social networks provide an extremely suitable space to instantly share text or multimedia information between two persons or their neighbors in the social graph. [5] Advantages available from these online platforms can be exploited by criminals to access an online user's confidential information by checking status updates and check-ins resulting into a possibility of making him a potential victim [5]. Offenders have shifted their focus towards servers, operating systems and direct applications as they have identified it as the easiest route for accessing sensitive data [8]. Many of these offenders make use of the deep web which enable them to anonymously browse and communicate in an untraceable way due to which even some legit vendors of illicit products have begun using deep web [6] [18]. Offenders like online abusers use the online social networking websites to abuse and exploit children and women sexually by creation of fake profiles, derogatory comments and posts [7]. Most of the time, offensive and hate filled posts go unblocked on the OSN which let the offenders to continue with their acts [8] C. Arunkumar and Dr. P. Sakthivel have stated that modern terrorists have also begun using modern techniques over internet and social media to instigate a cyber-war against the common people and government [17].

Summarizing reasons which have inclined local gangs and organized crimes groups towards social networks are:

1. Easy availability of networks and cheaper data plans
2. Avoiding adjustment of schedules/time/place for personal meetings
3. Larger scope for probable victim targets

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 5, Issue 1
January 2018

4. Easy opportunity for cross- border communications
5. Easy possibilities to influences on young targets due to lack awareness and immaturity
6. Availability of TOR networks and virtual private networks giving the flexibility to remain anonymous
7. crypto – currencies giving the flexibility to transact through black money, anonymously

The usage of OSN has resulted into an influx of:

- Successful and easy seizure of new victims [5][7]
- Threatening/blackmailing target victims for ransom
- Illicit trading especially inter-nation trading, sometimes by making use of TOR [6][15]
- Expanding gangs [17]
- Hiring personnel to stalk targets and hack target accounts
- Discussing and planning crimes [13][17]

As an effort to put an end to these activities, the foremost step that can be done is to successfully identify such offenders on social networks**.** This might not prove to be easy based on issues such as voluptuous amount of data, rising number of social networks, usage of compromised accounts thus acting under the hood and exploitation of freedom of expression by legit users.

As it is quite prominent that criminal offenders are quite active in the OSNs, a behavior analysis of their activities may help the law enforcement to take appropriate decisions and use the data for prediction of probable criminal offences in the future. The proposed model in this paper shall be able to detect a potential suspect by tracing and analyzing a user's online social network data such as posts, comments and tags. The proposed model also aims to trace and analyze individual comments made by a user's friend so as to identify probable suspects connected to the user resulting into creation of a mapping of the probable suspects. Currently the framework does not identify which parameters to consider while selecting a user to trace and analyze, however an intelligent self-learning scanner POSScan has been proposed in the paper which would allow extraction of user posts from the social network.

Additionally, one of the main features that separates this model from the existing models used in information retrieval from OSN is the filtration of false positives prior to the analysis of posts and comments. These false positive will filter out posts/comments made by legit aggressive users, communal vigilantes, protestors and hate crime supporters.

2. RELATED WORK

Operational intelligence analysis methods can be used to gain a specific legal outcome such as inter-suspect links, involvement detection in crimes, profiling known or probable suspects and many other [3]. Idiographic digital profiling can be used to understand motives, modus operandi and link illicit acts [4].

In [11], due to Facebook popularity and higher tendency of exploitation, footprints from memory areas and devices were extracted using forensic toolkits to detect potential evidence. In [12], messages sent over 'Manipal Net' (a self-created OSN for research by the authors) were extracted and analyzed to find clusters of users involved in suspicious activity. In [14], data from two social media namely whisper and twitter has been gathered and analyzed to identify hate crime supporters and hate speech by users. In [15], the authors had developed and used a dark crawler to access the deep web via the TOR network simultaneously while accessing the public network to study the extremist contents on TOR in relation online crimes.In [9], the authors used three features of URLS namely lexical features, hosts, and domains along with classification methods to detect malicious links in OSN.

In [10], the authors used an auto intimation technique that would alert the admin when a user would send repeated messages over the social network more than 5 times.

In [16], user posts and their reactions were collected from the Facebook social network to analyze user predictions for supermarket chains. In [18], superficial information retrieval method is proposed to identify

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 5, Issue 1
January 2018

social relations between unstructured web documents and data. In [19], a mathematical model based on Naïve Bayes method has been used to identify security threats in OSN. In [20], a clustering technique called Genetic Weighted K-Means Clustering has been proposed and used along with Negative Selection Classification algorithm to predict criminal behavior in OSN. To identify clusters and behavior, user's opinions and experiences were collected based on their usage of online social network and the dataset containing the opinions was created.

3. PROPOSED FRAMEWORK

i. Assumptions

Before discussing the framework, several indirect assumptions are involved based on the features of online social networks which are listed below:

Open access to data- online social networks come with some default privileges for the user which involve adding posts, comments, tags, text/video/voice communication and uploading of media files. These sites provide security settings which, if used properly would prevent users from tracking others. However there are few users which make use of these settings. Also, some features such as about the user, timeline (Facebook) is visible even after applying the security settings. As this data is open and readily available, it would be easy to use the data for analysis and prediction of user's behavior.

OSN Trends- uploading media files especially selfie is the biggest trend on OSN. Also status updates and check-in provide real time information of the user which can be misused by i) a legit user and by ii) criminal offender to play a foul, making the user a 'target victim'.

User tags and comments – online social networks allow user to tag their friends, give comments and put likes. This data might also be able to provide some kind of prediction especially mapping all the friends, tags, comments and likes altogether would help in identifying the nature of the whole group. In some cases it might be actually possible to affirm whether the group is involved in some kind of illicit or violent activity as there are many videos and pictures uploaded on these online social networks which show live kills, arms and weapons that are liked and supported even by legit users.

ii. Pre-requisie POSScan

To use the proposed framework, a self- learning intelligent scanner POSScan is proposed which would fetch directly user profile from an OSN. The POSScan will be retrieving a user profile based on earlier cases of similar nature that involved suspects exploiting social networks to their benefit.Initially the POSScan must be trained with information of similar cases in the past during which the scanner will be able to determine keywords and patterns which were used in solving the previous cases and remember it. While scanning the social network for a user profile to analyze, the scanner shall use its remembered memory and fetch user profile accordingly.

Alternatively, user profile can also be selected randomly, geographically or by available suspects.

Following diagram shows the initial POSScan learning phase which uses previous case database and smart POSScan database.

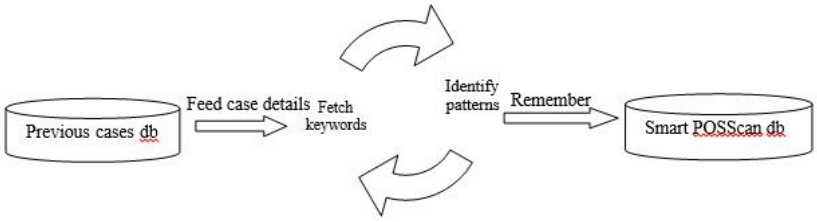

Fig. 1. POSScan learning phase

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 5, Issue 1
January 2018

The POSScan shall be executed through the below steps after going through the initial learning phase.

1. Scan the social network to detect a profile based on a. a particular case suspect b. previous case keywords/patterns c. geographical area d. random
2. Pass the scanned user profile through the ExR framework

iii. The ExR Framework

The ExR framework will be processed as depicted through the below steps:

1. Extract posts one by one in decreasing order or chronology (based or not based on parameters)
2. Extract user/suspect media files (if exists)
3. Extract basic information and friends list (if exists)
4. Run post analysis and identify the nature of post
5. Filter out false-positives
6. Run comment analysis and identify the nature of the comment
7. Repeat the steps 4 and 5 until i) a suspicion is met ii) all the posts of the user's profile are analyzed

The framework is as depicted below

:

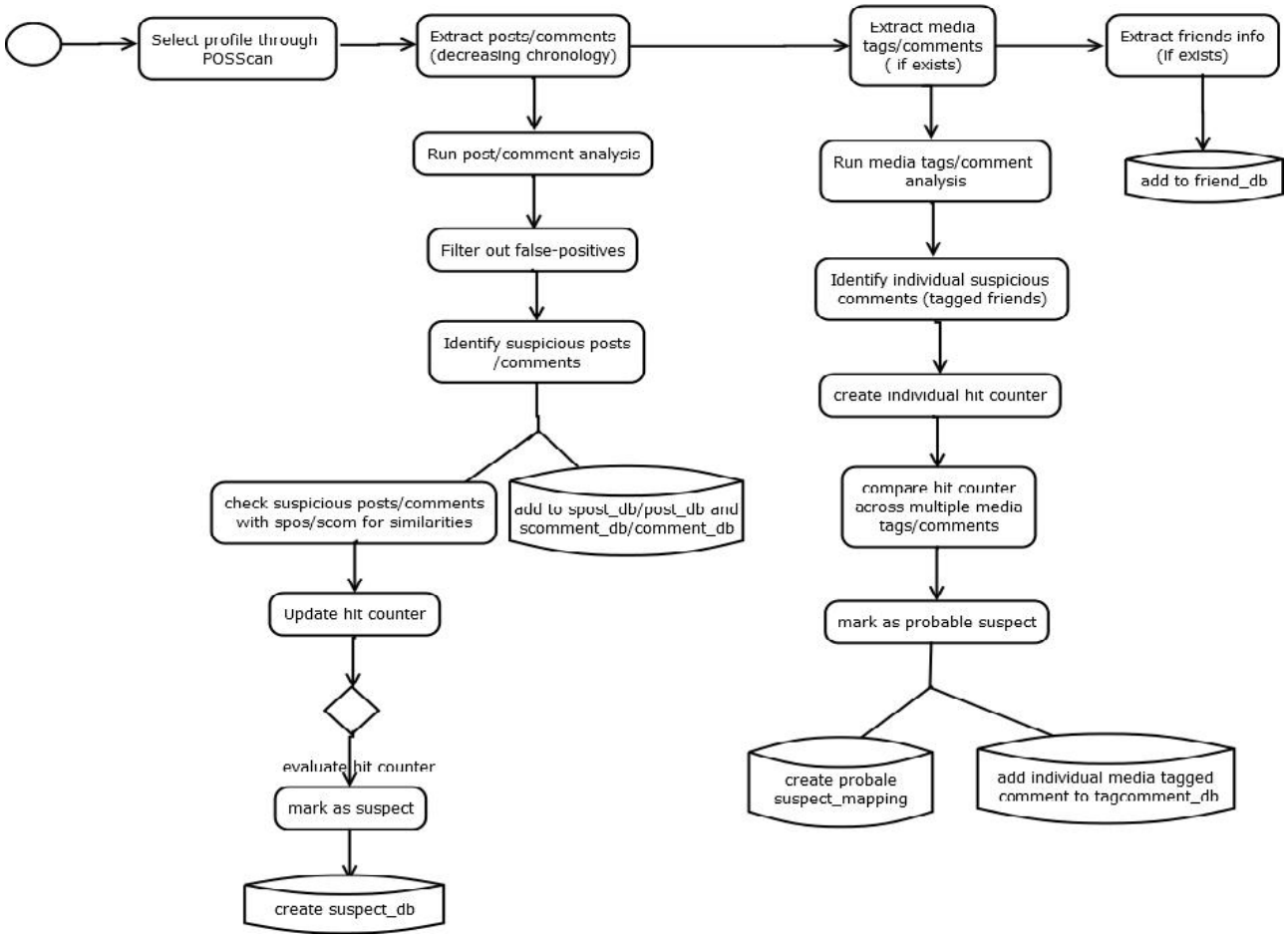

Fig. 2. ExR Framewor

Here in the framework naming conventions are:

- Sdatabasenamedb - for suspect data/posts/comments/tag
- databasenamedb - for non-suspected data/posts/comments/tag
- suspect_db - for storing detected suspect data
- suspect_mapping - for storing details of alleged suspect's tagged friends
- friends_db - for storing data on friends
- hit counter - for counting number of suspicious posts/comments/tags

After successful extraction and analysis the following can be done.

1. Comparing post and comment analysis with each other would help to identify with precision what kind of activity the suspect user is involved in. The analysis might also be able to throw light on his past activities and reveal his human nature which then in turn can be used for criminal profiling.
2. Create a mapping of the user/suspect and the available friends list to predict uncertainties or anomalies
3. Create a mapping of all the individual post of the alleged suspect to identify anomalies and co-relations

4. CONCLUSION AND LIMITATIONS

The ExR model if used efficiently along with the POSScan would be helpful to collect incriminating evidence along with other useful data that would help in criminal profiling. Firstly, successful analysis of user posts itself would help in identifying anomalies and suspicious behavior. Analyzing media tags however would allow the investigator to correlate the user's ideologies along with his tagged friends by efficient analysis of individual comments made by tagged friends on the tagged media post. This analysis would then be used to identify probable suspect hence allowing the investigator to create a probable suspect mapping based on media tags and its comments. To avail maximum benefit from the ExRmodel, it must be implemented as a self-learning extraction-run intelligent model so that the completed successful identification patterns could be reused in detection and evidence collection of future suspects. There are a few limitations to this model though. One of the main limitations is the assumption that a probable suspect offender who has an active OSN profile would actually be revealing his illicit actions in an open online network as the ratio of this data is yet to be known with accuracy. Also if there is no available suspect or previous criminal case information that could be fed to the POSScan scanner, manual intervention would be required where the investigator would be required to manually extract and select random user posts for analysis. The model also would not able to identify suspects without any user posts and suspects accessing the OSN through the TOR networks. The model shall also give a higher accuracy of suspect identification if an additional functionality to perform chat analysis could be implemented.

REFERENCES

[1] P. H. Rughani, Artificial Intelligence Based Digital Forensics Framework, International Journal of Advanced Research in Computer Science, October 2017.
[2] Ministry of Home Affairs[online], http://www.mha1.nic.in/par2013/par2016-pdfd/ls-190716
[3] Interpol [online], https://www.interpol.int/INTERPOL-expertise/Criminal-Intelligence-analysis
[4] G. M. Steel, Idiographic Digital Profiling: Behavioral Analysis Based on Digital Forensics, Journal of Digital Forensics, Security and Law, 2014.
[5] A. Sarkar, S. Agarwal, A. Ghosh, A. Nath, Impacts of Social Networks: A Comprehensive Study on Positive and Negative Effects on Different Age Groups in a Society,International Journal of Advance Research in Computer Science and Management Studies, May 2015.
[6] Interpol [online], https://www.interpol.int/media/files/crime-areas/Trafficking-in-iilicit-goods/Against -organized-crime-Interpol-trafficking-and-counterfeiting-casebook, 2014.
[7] V.P. Singh, Online social networks and threat to privacy, The Banaras Law Journal, 2014.

[8] Hague Security Delta [online], https: //www.thehaguesecuritydelta.com /media /com_hsd /report /57 /document /4aa6-3786enw.pdf
[9] B. Alghamdi, J. Watson, Y. Xu, Toward Detecting Malicious Links in Online Social Networks through User Behavior, IEEE, presented at the International Conference on Web Intelligence Workshops, 2016.
[10] R.T. Natarajan, S. S. Ram, C. Chellappan, A tool to identify offensive gangs in social networks, International Journal of Engineering Science and Computing, 2016.
[11] K. Wong, A Lai, J. Yeung, W. Lee, P. Chan , Facebook forensics, Valkyrie-x Security Research Group.
[12] S. Kumar, S. Singh, Detection of User Cluster with Suspicious Activity in Online Social Networking Site, IEEE, presented at 2nd International Conference on Advanced Computing, Networking and Security, Surathkal, Karnataka, Dec 2013.
[13] R. Kaur, S. Singh, Survey of data mining and social network analysis based anomaly detection techniques,Egyptian Informatics Journal, July 2016
[14] L. Silva, M. Mondal, D. Correa, F. Benevenuto, I. Weber, Analyzing the Targets of Hate in Online Social Media, 2016.
[15] A. Zulkarnine, R. Frank, B. Monk, J. Mitchell, G. Davies, Surfacing Collaborated Networks in Dark Web to Find Illicit and Criminal Content, 2016.
[16] F. Krebs, B. Lubascher, T. Moers, P. Schaap, G. Spanakis, Social Emotion Mining Techniques for Facebook Posts Reaction Prediction, 2018.
[17] C. Kumar, P. Sakthivel,Modern terrorism and national security in India, Imperial Journal of Interdisciplinary Research.
[18] K. Mahyuddin, M. Nasution, A. Shahrul, S. Sood, Social Network Extraction: Superficial Method and Information Retrieval, 2011.
[19] J. Joshuva, Identifying Security Threats On Social Network Using Pattern Recognition in messages, Master Thesis and Doctoral Dissertations, University of Tennessee at Chattanooga, December 2017.
[20] V. Soundarya, U. Kanimozhi, D. Manjula, Recommendation System for Criminal Behavioral Analysis on Social Network using Genetic Weighted K-Means Clustering, Journal of Computers, 2017.