WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Social Network Based Privacy Preserving Criminal Suspect Sensing

Saivignesh T, Kishore R, Nigash V

AVC College of Engineering, Mannampandal

GUIDED BY: Mrs. R.Ramya, M.E., Assistant Professor, Department of Computer Science and Engineering, A.V.C. College of Engineering Mannampandal Mayiladuthurai.

Correspondence Author: E-mail: saivignesh2211@gmail.com

ABSTRACT

With development of online social networks, many criminal suspects use social network to communicate with each other. In order to obtain valuable criminal clues, considerable research works have been done to analyze criminal suspects' social data. However, most of them did not pay much attention on privacy-preserving problems, which may leak some sensitive data in the analysis process. To solve this problem, we propose a novel analysis approach of criminal suspects by exploiting social data and crime data that are collected by social network and police information systems. We enable the social cloud server and public security cloud server to exchange social information of criminal suspects and user's public information in a privacy-preserving way. Specifically, we propose a privacy-preserving data retrieving method based on oblivious transfer to guarantee that only the authorized entities can perform queries on suspects' social data, while the social cloud server cannot infer anything during the query. Moreover, several building blocks, such as encrypted data comparing, secure classification and regression tree (CART) model are also proposed. Based on these building blocks, we designed a privacy-preserving criminal suspects sensing scheme. Finally, we demonstrate a performance evaluation which shows that our scheme can enhance analysis of criminal suspects without privacy leakage, while with low overhead.

INTRODUCTION

Now a days social media became a part of our life. We are spending more time on social media. Both good and bad things are in social media. We have to make use of that properly. With the continuous development of the Internet, online social networks have emerged rapidly, such as We Chat, Facebook, and Twitter, which has greatly changed the way people communicate, expanded people's social circle, and abstracted people's concern on social network analysis and mining. At the same time, criminal behaviour is also emerging towards gang and organizational development. From a psychological and sociological point of view, people with strong social relations and similar spatial trajectories (such as, frequent access in the same internet cafe) are possible to be of the same group. One traditional approach of gang criminal suspects' investigation is to determine the specific target of several suspects in advance, and manually monitor and collect information of specific suspects to discover other related criminal suspects or criminal gangs that are closely related to. In such a scenario, the police needs to equip enough human and material resources, which undoubtedly increases labour costs, material and financial expenses, and even causes anxiety or panic of the society. In Facebook, lot of bad activities are being performed. For example, a person creating account on the name of another person and giving friend requests to his/her friends. After they accepting the requests, the persons started conversation with them. They may ask money from them and starting misbehaviour activities. To avoid this, our proposed system will monitor the similar account creation by a person and monitor their conversation. If they ask money and any other relayed things, it will be suspected.

1. Related works

[1] Social Media (SM) evidence is a new and rapidly emerging frontier in digital forensics. The trail of digital information on social media, if explored correctly, can offer remarkable support in criminal investigations. However, exploring social media for potential evidence and presenting these proofs in court is not a straightforward task. Social media evidence must be collected by a legally and scientifically appropriate forensic process and also coincide with the privacy rights of individuals. Following the legal process is a challenging task for legal practitioners and investigators due to the highly dynamic and heterogeneous nature of social media. Forensic investigators can conduct effective investigations and collect legally sound evidence efficiently if they are provided with sophisticated tools to manage the diversity and size of social media content. This article explains the current state of evidence acquisition, admissibility, and jurisdiction in social media forensics. It also describes the immediate challenges for the collection, analysis, presentation, and validation of social media evidence in legal proceedings. Furthermore, the research gaps in the domain and few research objectives with potential research directions are presented.

[2] Neural networks are a machine learning method that excel in solving classification and forecasting problems. They have also been shown to be a useful tool for working with big data oriented environments such as law enforcement. This article reviews and examines existing research on the utilization of neural networks for forecasting crime and other police decision making problem solving. Neural network models to predict specific types of crime using location and time information and to predict a crime's location when given the crime and time of day are developed to demonstrate the application of neural networks to police decision making. The neural network crime prediction models utilize geo-spatiality to provide immediate information on crimes to enhance law enforcement decision making. The neural network models are able to predict the type of crime being committed

16.4% of the time for 27 different types of crime or 27.1% of the time when similar crimes are grouped into seven categories of crime. The location prediction neural networks are able to predict the zip code location or adjacent location 31.2% of the time.

3. Proposed methodology

To solve the above problems, personal sensitive data should be encrypted before uploaded onto the data is secure against the social hackers or shoulder surfers. However, the data encryption is provide additional security. This proposed mechanism provide efficient access control mechanism on ciphertext decryption so that only the authorized users can accessthe plaintext data is challenging. The sensitive data are encrypted before share to the social network.

MODULES DESCRIPTION

Special Individual - Special individual is the person who's name is similar to another person. The person who is creating an account in the name which is already exist, that person will be treated as special individual. The activities of that particular user will be tracked whether he is doing any misbehavior activities. Monitoring and Analaying User Activity - The particular person who creates in the name of already exist person, his/her activities will be monitored. If he/she perform any illegal activities, it will be monitored. Goup Detection - In this module, the person who is trying to create fake account, having any contact with another person who is having the same intention. Also if they are doing criminal activities as a group of people, it will detected and monitored.

Criminal Activity Detection - It is the activity of suspecting criminal activities performed by the people. The detected activities will be displayed detail in the form of report. Content Filtering– It filters words features other words similar to what the user wants to convey. The goal is to block content that contains harmful information. If the fake user asking money or other related thing to another user, it will be suspected using content filtering.

RESULTS AND DISCUSSION

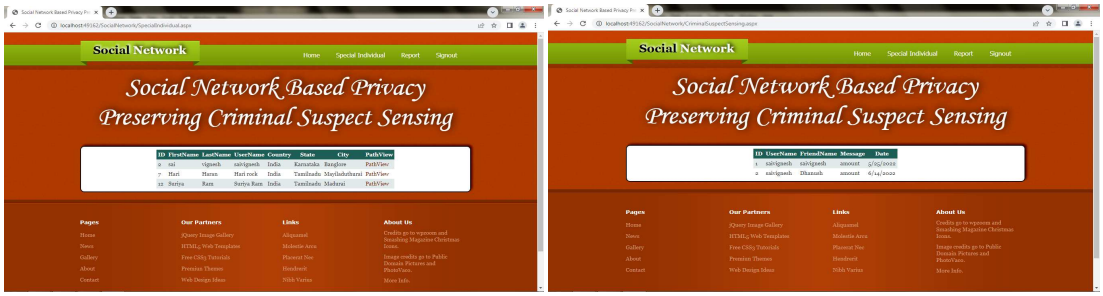

Fig. 1 - (a) Special Individual List; (b) Criminal Activity Detection.

CONCLUSION

The use of OSN in law enforcement agencies has entirely changed in their traditional techniques and procedure in which law enforcement professionals using it in criminal intelligence and investigative activity.Law enforcement greatly benefits from resources as a fruitful tool to prevent, mitigate, respond, and investigate criminal activity. The outline of our work described how criminal committed crimes by using these sites for illegal purposes, and we categorized the crimes that are involving OSNs. Forensics investigators were following two approaches in obtaining data from OSNs; collecting publicly available information of user's subscribes and cooperation with social network provider in order to obtain restricted data of any particular user. There should be transparency in sharing personal information between law enforcement of social networks companies and law enforcement authorizes.

FUTURE ENHANCEMENT

In this article, we propose a privacy-preserving criminal suspects sensing scheme considering social data associated with personal data to perform criminal suspect's analysis. This scheme employs a privacy-preserving data retrieving (PPDR) method based on oblivious transfer to enable access pattern protection, and several building blocks to construct to enable the cloud servers to infer criminal suspect's status, and preserve data privacy using classification and regression tree *(CART)* model.

REFERENCES

1. H. Arshad, A. Jantan, and E. Omolara, "Evidence collection and forensics on social networks: Research challenges and directions," Digit.Invest., vol. 28, pp. 126–138, Mar. 2019.
2. S. Seoet al., "Partially generative neural networks for gang crime classification with partial information," in Proc. AAAI/ACMConf. AI, Ethics, Soc., New York, NY, USA, 2018, pp. 257 263, doi: 10.1145/3278721.3278758.
3. D. Ramalingam, V. Chinnaiah, and A. Jeyagobi, "Privacy preserving schemes for secure interactions in online social networks," in Proc. Int.Conf. Soft Comput. Syst., vol. 837, 2018, pp. 548–557.
4. S. Jiang, M. Duan, and L. Wang, "Toward privacy-preserving symptoms matching in SDN based mobile healthcare social networks," IEEE Internet Things J., vol. 5, no. 3, pp. 1379–1388, Jun. 2018, doi: 10.1109/JIOT.2018.2799209.