International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

Social Network-Based Suspect Sensing for Privacy-Preserving Criminal Suspects

Manam Vamsi Krishna[1]
#1 Research scholar , Computer Science and Engineering
Pursing PhD in Sri Satya Sai University of Technology and Medical sciences

ABSTRACT:

With improvement of on-line social networks, many crook suspects use social community to speak with every other. In order to achieve treasured crook clues, full-size lookup works have been finished to analyze crook suspects' social data. However, most of them did no longer pay tons interest on privacy-preserving problems, which might also leak some touchy records in the evaluation process. To resolve this problem, we advocate a novel evaluation method of crook suspects through exploiting social records and crime records that are gathered through social community and police records systems. We allow the social cloud server and public protection cloud server to change social facts of crook suspects and user's public statistics in a privacypreserving way. Specifically, we recommend a privacy-preserving statistics retrieving approach based totally on oblivious switch to assurance that solely the licensed entities can operate queries on suspects' social data, whilst the social cloud server can't infer something at some point of the query. Moreover, various constructing blocks, such as encrypted records comparing, impervious classification and regression tree (CART) mannequin are additionally proposed. Based on these constructing blocks, we designed a privacy-preserving crook suspects sensing scheme. Finally, we exhibit a overall performance assessment which indicates that our scheme can decorate evaluation of crook suspects except privateness leakage, whilst with low overhead.

1.INTRODUCTION

WITH the non-stop improvement of the Internet, on-line social networks have emerged rapidly, such as WeChat, Facebook, and Twitter, which has substantially modified the way human beings communicate, improved people's social circle, and abstracted people's situation on social community evaluation and mining. At the identical time, crook conduct is additionally rising closer to gang and organizational development. From a psychological and sociological factor of view, human beings with robust social members of the family and comparable spatial trajectories (such as, normal get right of entry to in the identical net cafe) are viable to be of the equal group. One typical strategy of gang crook suspects' investigation is to decide the unique goal of numerous suspects in advance, and manually screen and gather facts of particular suspects to find out different associated crook suspects or crook gangs that are intently associated to. In such a scenario, the police wants to equip sufficient human and fabric resources, which most likely will increase labor costs, cloth and monetary expenses, and even motives anxiousness or panic of the society. To get to the bottom of such problem, a cloud server related with crime evaluation was once mounted by using the police to always accumulate data associated with public security, i.e., location, crook records, and credibility in photograph and text format. The server makes use of these records to analyze the doable connections amongst the suspects and supply clues for excavating crook gangs, and aside from undiscovered suspects [1].

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

Moreover, it helps to analyze whether or not the consumer is a suspect. However, it is the lack of enough social facts to infer whether or not there are any viable suspects in their private social circle [2]. Considerable functions in social networks have been proposed to analyze the user's social information for the duration of their social interplay [3]. For example, the drift of dollars from banks and the buy documents of e-commerce can help alert crimes; face cognizance technological know-how can assist hit upon suspects thru on-line image identification. The mixture of these social records and monitored non-public records can reinforce the evaluation of crook suspects. Suppose Eve is a precise suspect arrested by using the police, and offers the police the get entry to authorization, and if police finds that Alice often contacts with Eve, who has numerous crook documents before, thus, Alice has excessive opportunity to be in a doable suspected crime. Personal data, i.e., crook records, location, credibility, and social data, i.e., contact duration, contact frequency, are normally accrued and saved by using one of a kind provider providers, such as police's cloud server and social community provider vendors (Twitter). To defend information privacy, information sharing amongst these events turns into very essential for the evaluation of plausible crook suspects [4], [5]. Meanwhile, each private information and social data, such as crook archives and contact information, are touchy [4], [6]. For a unique crook suspect ui, the police can gain the ui's social records from provider providers. The evaluation provider company (ASP) hosts a discovered model, and gives suspects evaluation carrier for the police to use such a mannequin remotely. In such a scenario, the private and social records are personal to the suspects which must be included towards the carrier providers, whilst the mannequin is a treasured asset to classifier owner, which need to no longer be disclosed to untrusted party, and evaluation records and classification effects are additionally personal to the police. To remedy such a problem, private and social records are encrypted and saved in carrier providers, and thru statistics sharing, police can securely acquire the plaintext of private and social data. Moreover, the evaluation statistics have to additionally be in ciphertext structure when the police submits it to the ASP for analysis. However, such approach may also restriction the information processing capability of the ASPs [7]. Therefore, it is a serious undertaking to whole the facts evaluation whilst defending privateness of workable crook suspects. In addition, the question goal and effects are precious property to the police, which may additionally incorporate some touchy statistics about unique suspects and unknown suspects, such as identity, which ought to additionally be blanketed in opposition to provider providers. Therefore, get entry to sample safety is additionally a difficult project when the use of social information to make stronger the evaluation of plausible suspects.

2.LITERATURE SURVEY

[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. 2018.

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.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

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] S. Seo et al., "Partially generative neural networks for gang crime classification with partial information," in Proc. AAAI/ACM Conf. AI, Ethics, Soc., New York, NY, USA, 2018, pp. 257–263, doi: 10.1145/3278721.3278758.

More than 1 million homicides, robberies, and aggravated assaults occur in the United States each year. These crimes are often further classified into different types based on the circumstances surrounding the crime (e.g., domestic violence, gang-related). Despite recent technological advances in AI and machine learning, these additional classification tasks are still done manually by specially trained police officers. In this paper, we provide the first attempt to develop a more automatic system for classifying crimes. In particular, we study the question of classifying whether a given violent crime is gang-related. We introduce a novel Partially Generative Neural Networks (PGNN) that is able to accurately classify gang-related crimes both when full information is available and when there is only partial information. Our PGNN is the first generative-classification model that enables to work when some features of the test examples are missing. Using a crime event dataset from Los Angeles covering 2014-2016, we experimentally show that our PGNN outperforms all other typically used classifiers for the problem of classifying gangrelated violent crimes.

3.PROPOSED SYSTEM

In this project we are identifying criminals by analysing social networks communication as criminals will use social network post to communicate with each other and all existing technologies were identifying criminals just by adding noise to dataset and this technique is not completely secure. To enhance data security author is proposing privacy preserving data retrieval technique to identify criminals from social networks. To implement this project author has explained following modules.

1) Identify suspected criminals: In this module author analysing social networks post to extract suspected criminal details such as criminal record, location and contact duration. But due to security reason no social network will expose location and contact duration in dataset so we are identifying username from social network post data.

2) PPDR (Privacy Preserving Data Retrieval) Module: using this module police can send privacy query to cloud server and then cloud server will search or predict privacy (encrypted) query on privacy dataset to get privacy preserving data retrieval. In this module author using PROXY Encryption such as HOMOMORPHIC encryption to encrypt dataset and then this encrypted dataset will be publish or outsource on cloud server by ASP. While querying police will send encrypted query to cloud server and then cloud server has to execute encrypted query on encrypted dataset and due to this reason cloud server cannot know or steal anything from query or result and thus privacy data retrieval will be achieved.

3) Classifier: Using this module ASP will outsource encrypted dataset to cloud server and then cloud owner or classifier will classify given query on encrypted dataset to get classification result and this classification

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

result will be obtained using CART algorithm.

3.1 Function implemented in this project

CloudServer: This application accept encrypted query from police and then execute query on encrypted dataset to get classification result and then sent this result to police

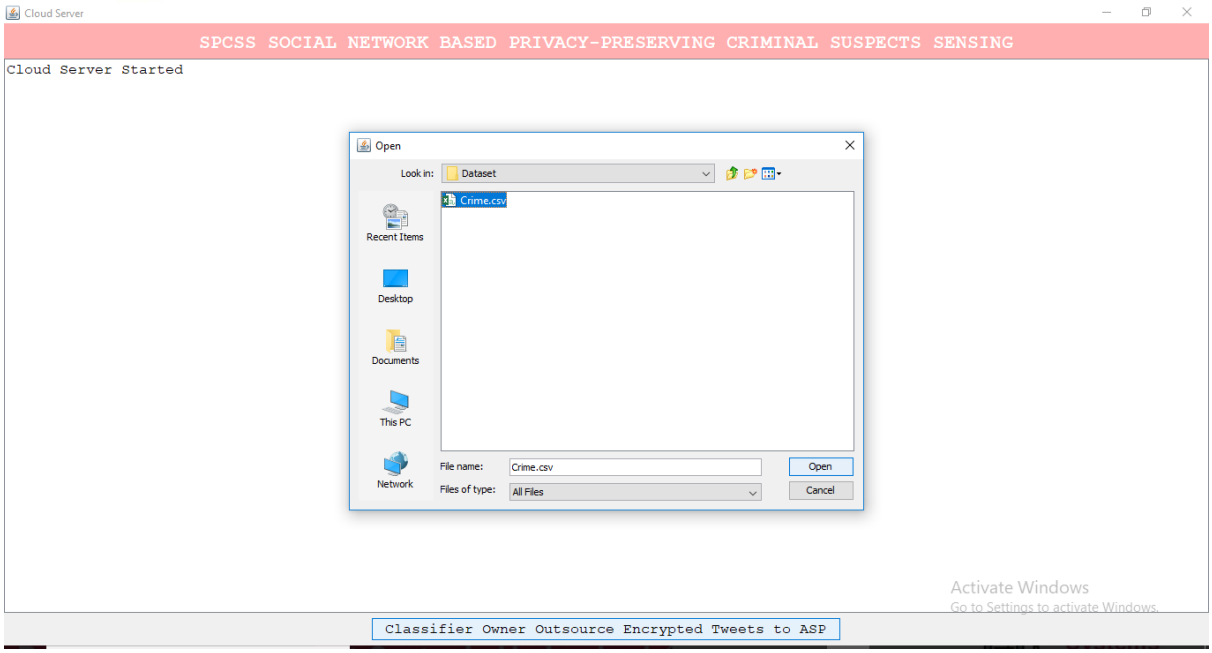
ASP: This user will upload dataset and then apply HOMOMORPHIC encryption on dataset and then outsource this dataset to cloud for storage and to process query

Police User: This user will login to application by using username as 'police' and password as 'police' and then send query to cloud server and get query result.

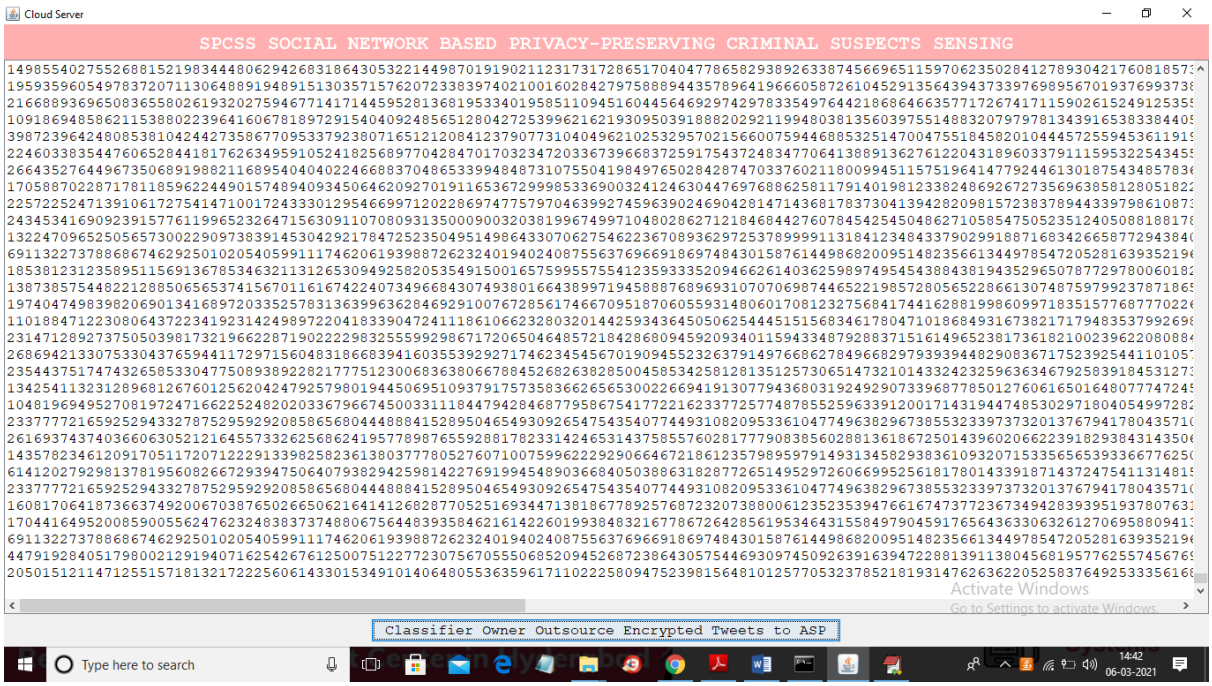
4.RESULTS AND DISCUSSIONS

Now in above screen click on 'Classifier Owner Outsource Encrypted Tweets to ASP' button to upload dataset and to encrypt it

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

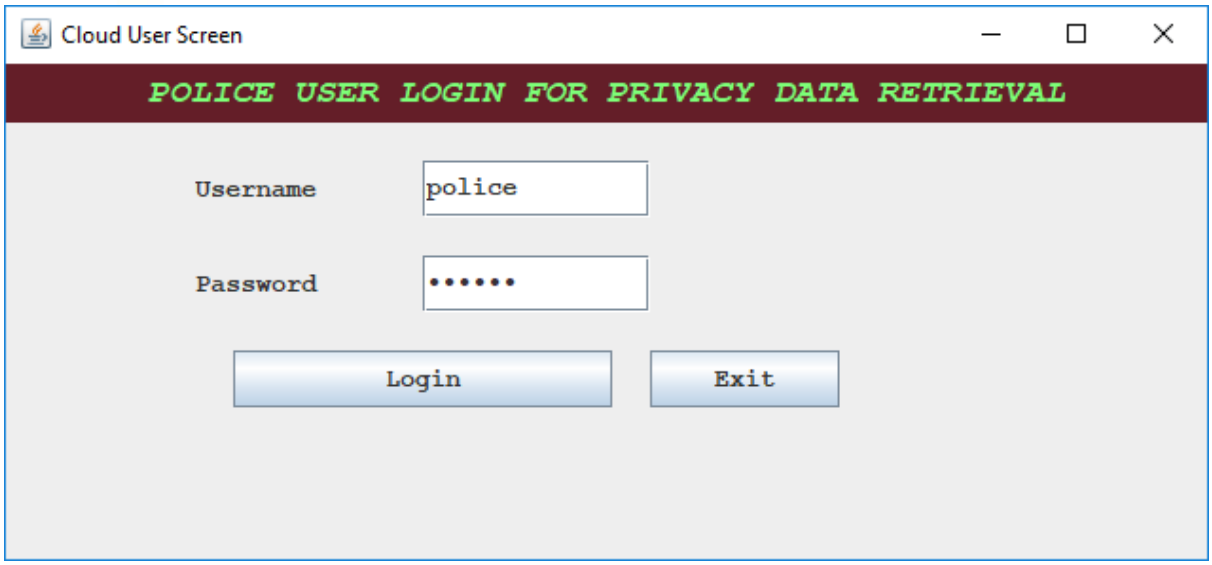


In above screen selecting and uploading 'Crime.csv' file and then click on 'Open' button to load dataset and to encrypt dataset and to get below screen

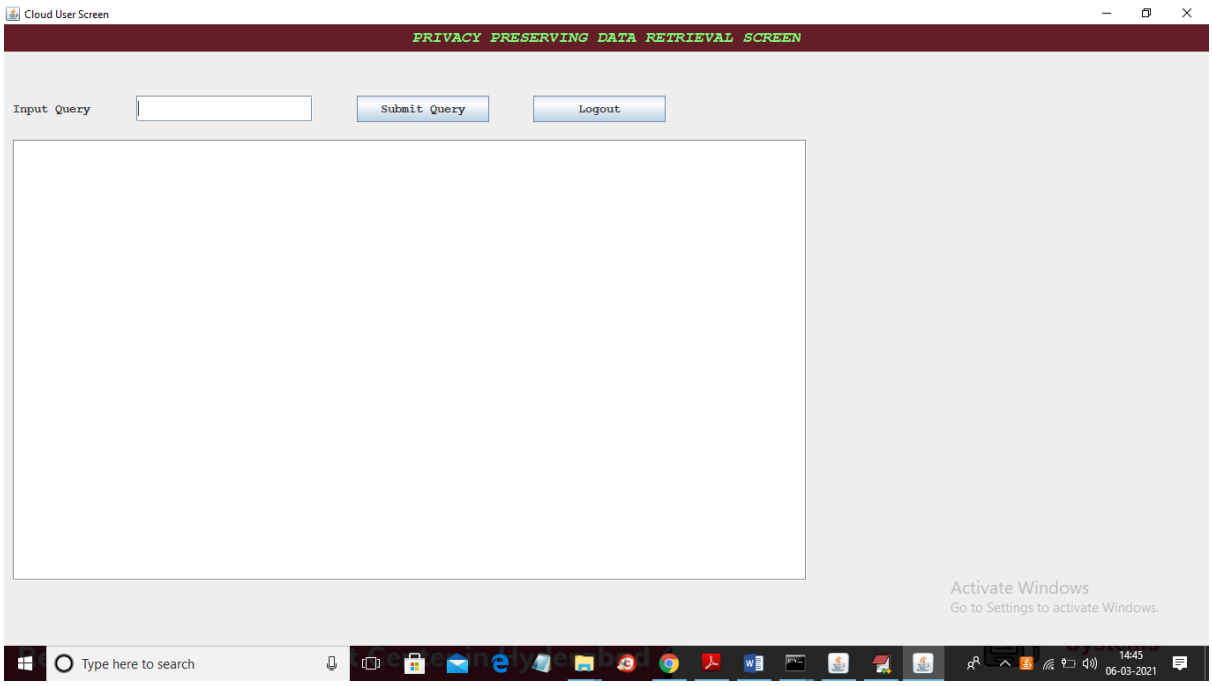


In above screen entire dataset encrypted in numeric format and from above dataset cloud server cannot steal or know anything from above encrypted dataset. Now double click on 'run.bat' file from 'PoliceUser' folder to get below screen

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

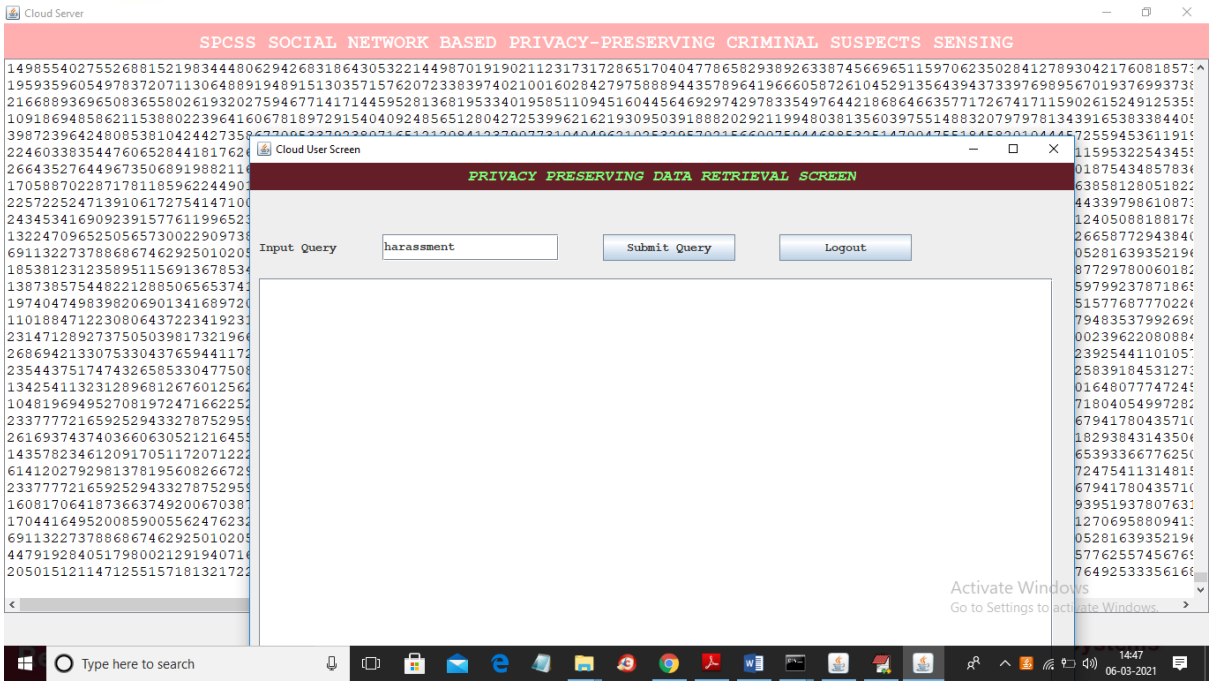


In above screen enter username and password as ‘police’ and ‘police’ and then click on ‘Login’ button to get below screen

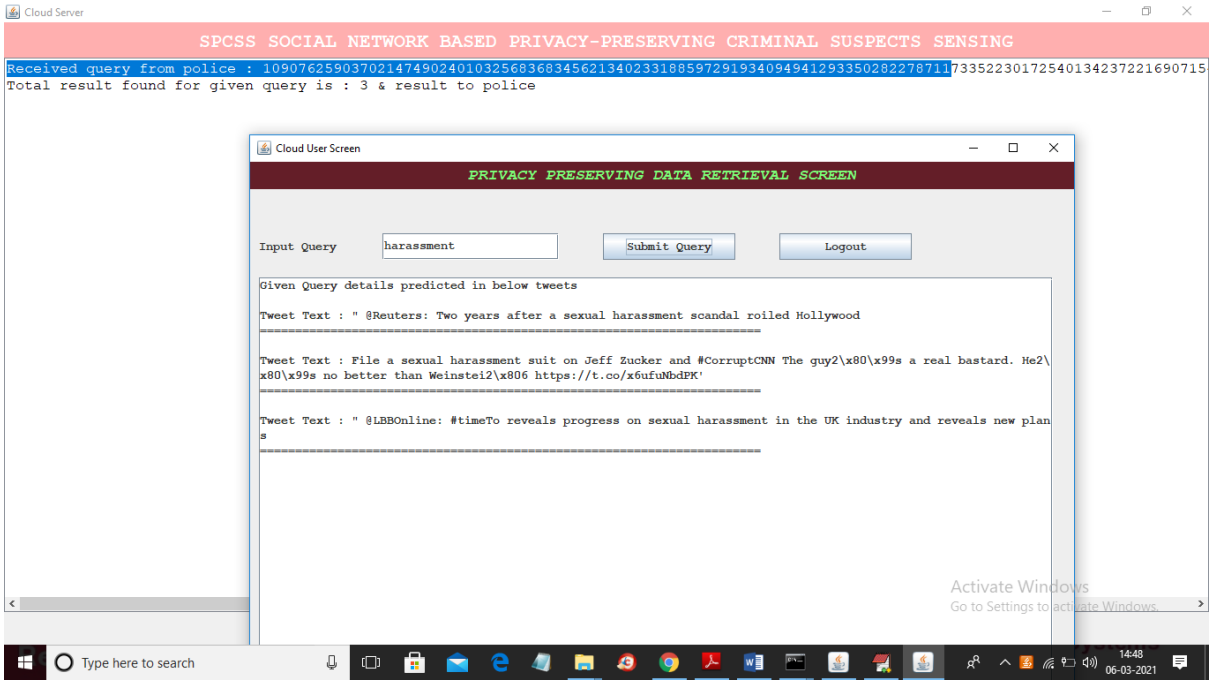


In above screen police will enter some query and then click on ‘Submit Query’ button to get below screen

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

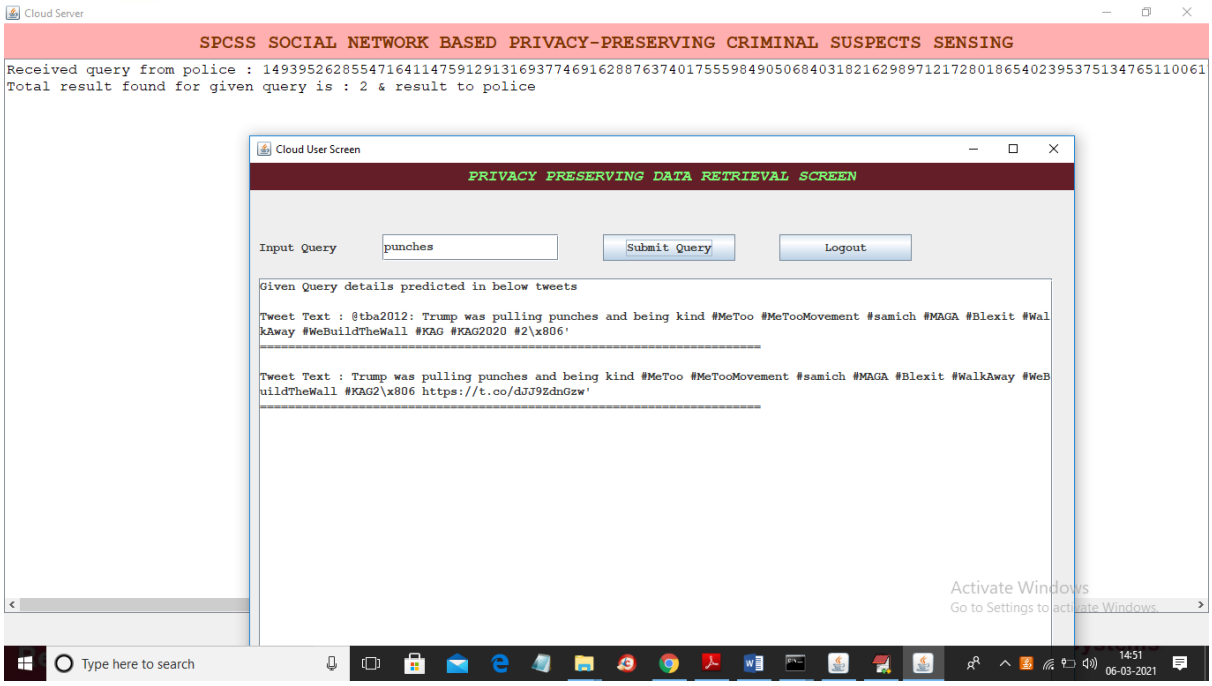


In above screen police enter query as 'harassment' and then submit this query to cloud to get all tweets which are using word 'harassment'



In above screen cloud server receive query in encrypted format and then execute that query on dataset to get query result at front side screen. Now try other query

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362



Similarly send any query to cloud server and get result. So in above result we are using tweets dataset with privacy preserving data retrieval technique

5.CONCLUSION

In this article, we have proposed a criminal suspects analysis approach by utilizing social data and crime data to enhance crime analysis without privacy leakage. In our scheme, nothing of personal and social data is leaked to either of the service providers. Moreover, the access pattern is protected and CART model has been trained, encrypted, and outsourced to the ASP to provide criminal suspects analysis. During the analysis phase, any untrusted party can deduce nothing from the classification model, the police station's inputs, and analysis results. Besides, in our scheme, the police station does not need to take part in the analysis, i.e., they just send a query and wait for the results. The experiments evaluation results show that our approach can achieve good analysis results with the acceptable overhead. For the future work, we plan to extend our work to support CO offline

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. 2018.

[2] S. Seo et al., "Partially generative neural networks for gang crime classification with partial information," in Proc. AAAI/ACM Conf. 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.

[5] K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren, and X. S. Shen, "Security and privacy in smart city applications: Challenges and solutions," IEEE Commun. Mag., vol. 55, no. 1, pp. 122–129, Jan. 2017, doi: 10.1109/MCOM.2017.1600267CM.

[6] R. Yu, J. Kang, X. Huang, S. Xie, Y. Zhang, and S. Gjessing, "MixGroup: Accumulative pseudonym exchanging for location privacy enhancement in vehicular social networks," IEEE Trans. Depend. Secure Comput., vol. 13, no. 1, pp. 93–105, Jan./Feb. 2016.

[7] B. Desmet and V. Hoste, "Online suicide prevention through optimised text classification," Inf. Sci., vol. 439, pp. 61–78, May 2018.

[8] K. Zhang, X. Liang, J. Ni, K. Yang, and X. Shen, "Exploiting social network to enhance human-to-human infection analysis without privacy leakage," IEEE Trans. Depend. Sec. Comput., vol. 15, no. 4, pp. 607–620, Jul./Aug. 2018, doi: 10.1109/TDSC.2016.2626288.

[9] B. Desmet and V. Hoste, "Online suicide prevention through optimised text classification," Inf. Sci., vols. 439–440, pp. 61–78, May 2018, doi: 10.1016/j.ins.2018.02.014.

[10] Z. Yu, F. Yi, Q. Lv, and B. Guo, "Identifying on-site users for social events: Mobility, content, and social relationship," IEEE Trans. Mobile Comput., vol. 17, no. 9, pp. 2055–2068, Sep. 2018, doi: 10.1109/TMC.2018.2794981.

Author's Profile:

MANAM VAMSI KRISHNA.

Research scholar, Computer Science and Engineering

Pursing PhD in Sri Satya Sai University of Technology and Medical sciencesHis Research interests in cryptography & Network security, Cyber Security, computer networks, Data mining