JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Forensic Cyber Security in Sensitive Message Blocking for Social Media

[1] Sneha V Masaguppi & [2] S.H Manjula

[1]Student, [2]Professor
[1, 2] Department of Computer Science and Engineering,
[1, 2] College Name: University Visvesvaraya College of Engineering

Abstract: Sharing any form of information is now easier. There are many social media sites that allow people to communicate with each other or share any information through these kinds of sites. There is a lot of advantages in using these sites except the major concern is security. The technique of inferring anything about a user's characteristics from the form and substance of their writing present in a collection of data is known as cyber security forensics. The rise of social media as a key medium of communication has thrown into question the long-held belief that forensic investigators will have access to form writing. We presented the Sensitive Message Blocking System (SMBS) in this system, which extracts characteristics from very short samples of text and uses scalable supervised learning to train Sensitive-Keyword models and make predictions to classify whether the message is sensitive or non-sensitive. If the message is sensitive then it will classify whether it is Less Sensitive, Medium Sensitive, or More Sensitive. There is a decision-making system that will decide whether to post the message on the wall or not.

Index Terms: *Sensitive Message Blocking System, Classifier, Supervised Model*

I. INTRODUCTION

Nowadays, many of the online social networking sites such as Facebook, Twitter, etc., have different communication patterns which are changing the public's communication site to site by also increasing their social circle. All these patterns are removing security concerns from the people. Simultaneously, observing less security concern of people on these social networks, formation of gang or organization is coming into the picture to conduct criminal activities using these online social networking sites. One common approach of gang criminal suspects' investigation is to find 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 them. In such a scenario, the police need to equip enough human and material resources, which increases labor costs, material, and financial expenses, and even causes panic in the public. The police built a cloud server associated with crime analysis to continuously collect information related to public security, such as location, criminal histories, image, and text format, to address this problem. These data are used by the server to check relationships between suspects and provide hints for uncovering criminal groups and excluding unidentified suspects. It also aids in determining whether the user is a suspect .

LITRATURE SURVEY:

To check on gang criminal activities we can go through infection analysis and emotion analysis which plays a very important role.[10], [11]. There are many different applications available in social networks for crime analysis that follows machine learning techniques. To allocate crime types into some categories based on preset criteria, Rigopoulos and Karadimas [12] prepared a model based on the application of Nex Class methodology and a decision support system. Ingilevich and Ivanov [13] used linear regression, logistic regression, and gradient enhancement methods to predict the number of crimes in different regions of the city based on gang robbery crime. In many scenarios, we can see that social network analysis is the most commonly used tool in gang crime investigations, evidence collection, and data analysis. Sun et al. [15] gave an improved fully homomorphism encryption (FHE) scheme based on HElib [28] by reducing the ciphertext size, the modulus, and decryption noise. Based on these, they implemented a private decision tree classifier, and the result showed that it has a better performance. Nonetheless, in practice, it is inefficient. Later, Abadi et al. [16] proposed a deep learning technique based on differential privacy. Thus the main aim of providing security is by introducing some noise to the original data before training to prevent the inverse attack by taking the data set directly from the training model, and this privacy-preserving scheme does not rely on the cloud. Flamenco et al. [17] invented a multiparty machine learning technique in which a trustworthy SGX is used(Software Guard Extensions). In the cloud, a processor was used to train unknown data. Cloud-assisted privacy preservation or no cloud approach which mainly focuses on privacy problems can be done in a data training phase. Bost et al. [18] presented many building pieces for privacy issues during the classification

stage, including secure comparison, secure dot product, and safe argmax. Hassani et al. [19] suggested a differential privacy-based social network analysis approach that preserves privacy. For decision trees and random forests, Wu et al. [20] suggested a safety evaluation based on homomorphism encryption. Tai et al. [21] suggested a semi-honest and one-side secure model with a privacy-preserving decision tree assessment.]. As a result, the computational cost of sparse decision trees is reduced, and their performance improves by using these methods. Joye and Salehi [22] modified the DGK (Damgard, Geisler, and Krøigaard) comparison protocol in [23]. For encrypted data comparison which will go against timing attacks and also gives better performance. They used [20]'s brilliant idea of hiding the indexes of the comparison nodes at each level of the tree with a random permutation and reduced the comparison numbers from decision nodes m to tree level d. However, it is a time-consuming mechanism because in classification the decision tree structure constantly keeps changing. Gang crime has geospatial, topical, and chronological relevance since it is a geospatial phenomenon. As a member of gang crime, its published data on Facebook, LinkedIn, and other public sources can help to determine the leadership qualities of the organization. As a result, it is better to analyze the possible criminal suspect's data with current criminal suspects by considering each and every aspect such as personal information, social data, etc.

EXSISTING METHOD

We used Web-based services to get important information from a large amount of data. Nowadays, Facebook, Instagram, Whatsapp are the most popular social media sites, with a huge amount of users having an account. Facebook and Instagram having several functions such as a request to friends, friend's suggestions, and sharing out our photos, some videos, audios to others. Even though Facebook allows the users to communicate some information through their account. As a result, there is a chance that the submitted remark will be offensive. Through this social media may cause serious issues like harassing and blackmailing can also occur, from this kind of disadvantages there are some advantages in the social media networking sites.

II. PROPOSED METHOD

The purpose of this system is to prohibit users from sharing sensitive material on social media and to provide statistics to administrators about users who attempt to post sensitive messages on social media frequently. Social networking sites give a space or area for users to update their status. This space is referred to as a "Wall." However, on occasion, someone may publish abusive messages on a specific user's wall, posing a major threat to the user's reputation. We can use the Information Filtering (IF) technique to avoid such a major problem.

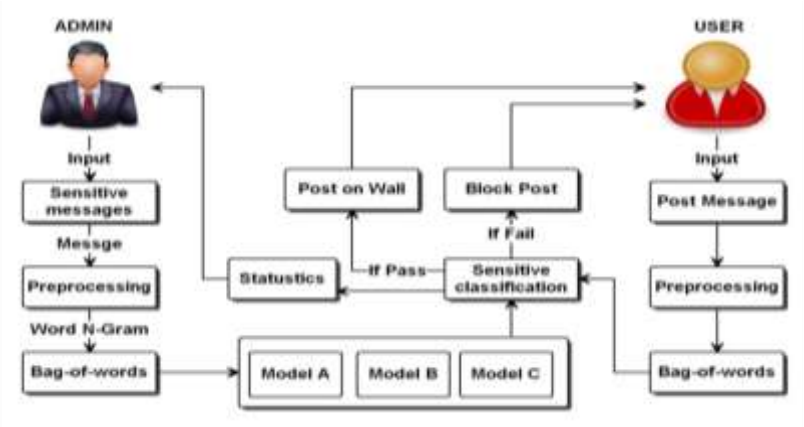

Fig 1. ***Proposed System Architecture***

This system uses use N-Gram technique for content-based filtering and Weight-age concept for policy-based filtering method. With the help of these concept this system will detect whether the post contains sensitive data or not.

At first ,when the user tries to post a message, the message will be received and then given for pre-processing where all stop words such as: is ,are ,to ,for, etc., and special characters like @,#, $, !, etc., will be eliminated from the message. The remaining part of the message will be treated as key words and that key word sequences are given to N-Gram process.
In N-Gram processing, key word sequences are converted into Bag of Words, where keywords are in certain pattern, that pattern will be compared with the sensitive message patterns in database, based on pattern matching process some score will be provide to each pattern. The accumulated score is treated as a Sensitive Weight age(SW) of the message. This Sensitive Weight age(SW) will be compared with threshold. If Sensitive Weight age(SW) score is less then the threshold, the user can post and also view the post. If it is more then the threshold, the post will be blocked and not be visible to anyone. Notification will be displayed to the user saying that the post contains some sensitive information or message.

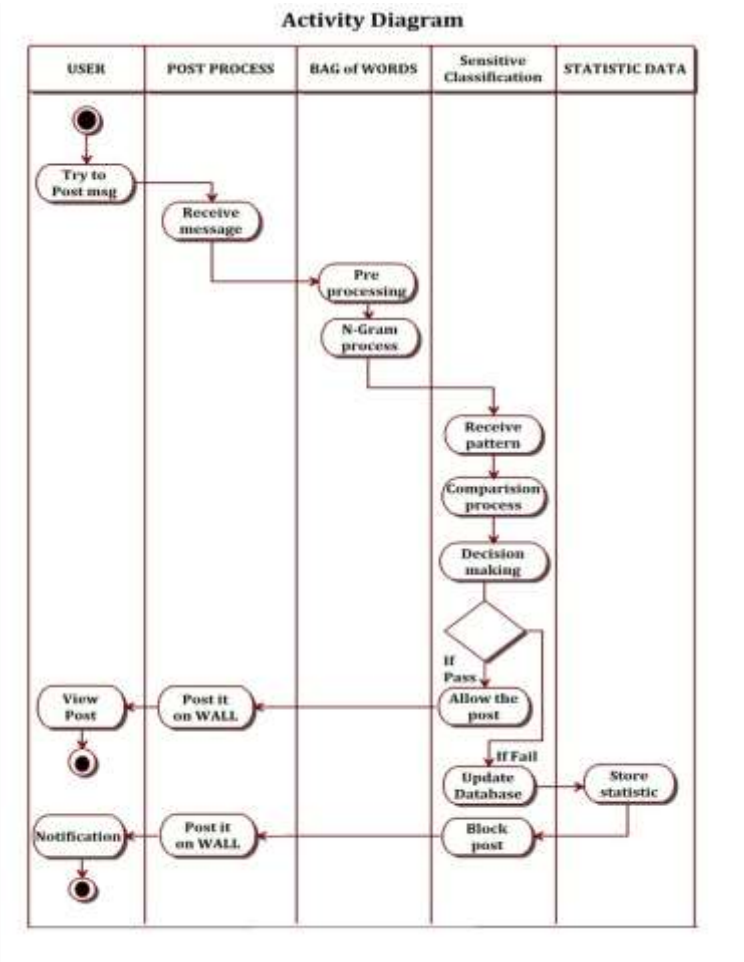

Fig 2: Sensitive Message Blocking System (SMBS)

SCREENSHOTS

Fig 3: Less Sensitive Information.

If the User posts any Image, other user can also look at the image posted and like others post as well. When the user post the image, other user will get notification of the users that your friend has posted the image. So if the user wants to comment anything then they can comment but it should not fall under sensitive classification. User will be allowed to post on positive comments.

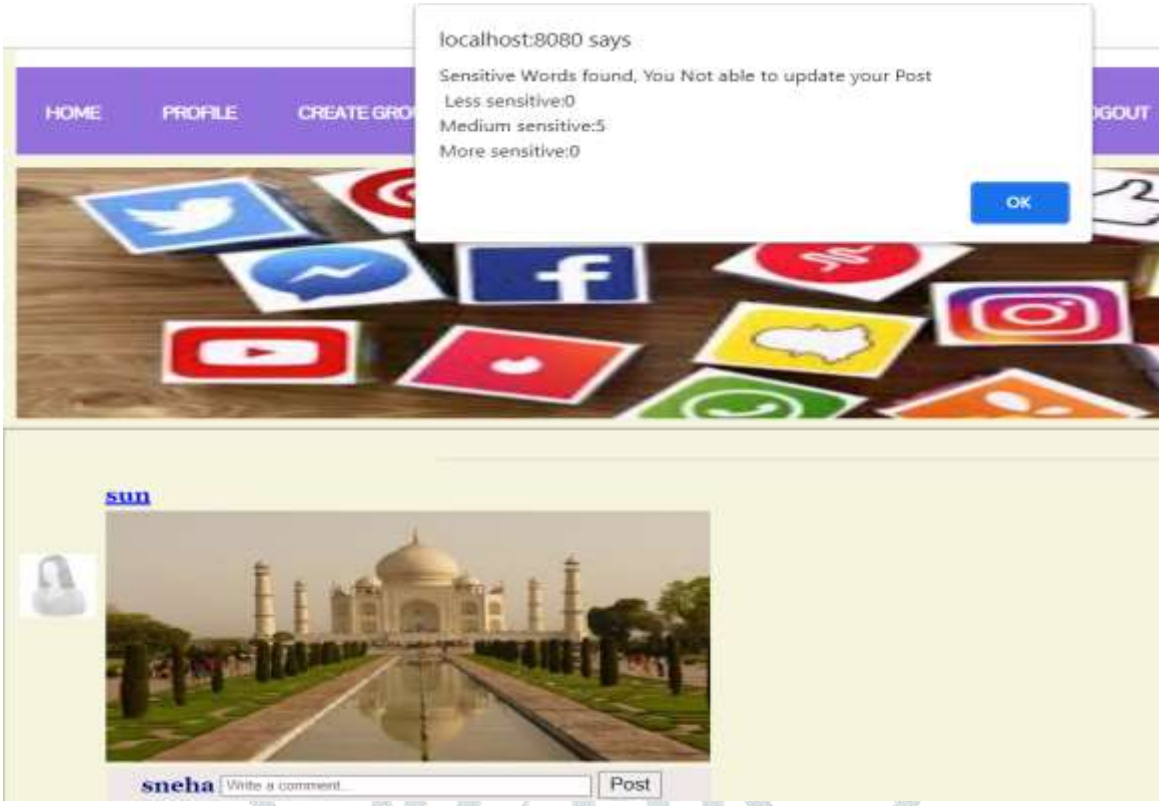

Fig 4: Medium Sensitive Information

In this Scenario the user will be allowed to create group and look at the images posted by his/her friends. The Image posted can be liked and commented but user can only comment only positive comment and negative comment will be blocked and the user will be not allowed to post on the wall. The Admin will get the report of all the users trying to post negative comments. Here the words of Less, Medium and more sensitive words will be added by the admin. So based on the user words or comments, the classification will be done and the user will be shown pop up and told it falls under medium sensitive category and will be blocked.

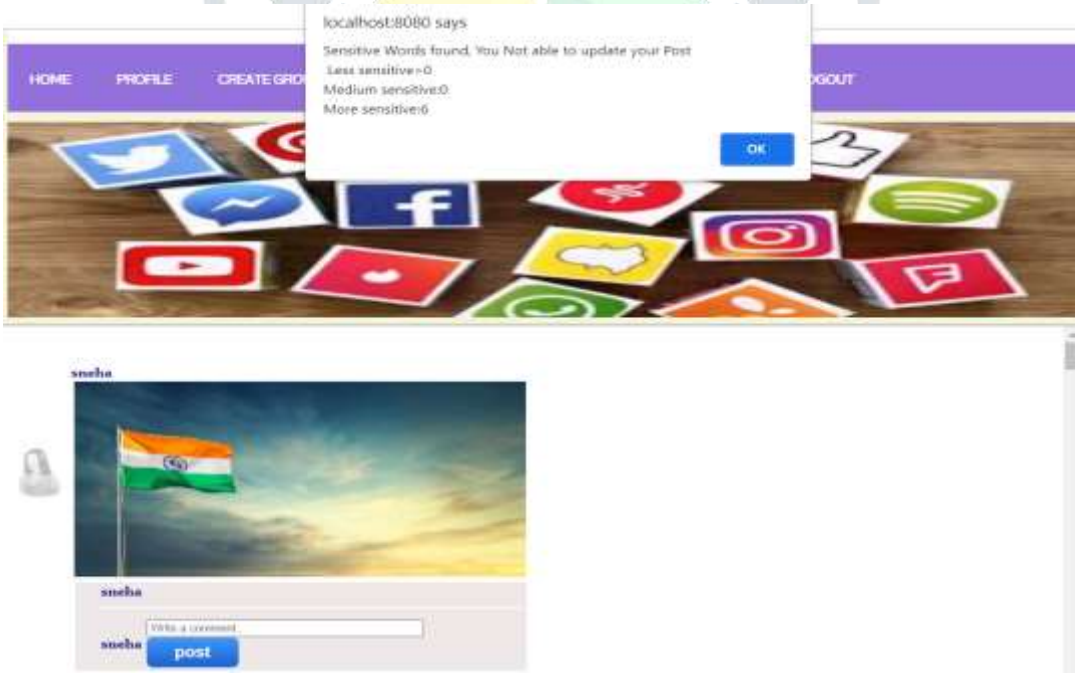

Fig 5: More Sensitive Information

In this Scenario the user will be allowed to create group and look at the images posted by his/her friends. The Image posted can be liked and commented but user can only comment only positive comment and negative comment will be blocked and the user will be not allowed to post on the wall. The Admin will get the report of all the users trying to post negative comments. Here the words of Less, Medium and more sensitive words will be added by the admin. So based on the user words or comments, the classification will be done and the user will be shown pop up and told it falls under medium sensitive category and will be blocked.

Hence by this user cannot comment anything negative on anyone post and anything abusive words will be not found on the platforms.
Hence the platform will reduce crimes as much as possible and anybody will be free to keep his profile open because of positive comments and none of the abusive crimes will be found.

Result analysis:

Nowadays there are several social media sites are there which make people keep a constant relationship with each other. It is very easy to share any kind of data. There are some good advantages in such social media sites but small disadvantages like poor security which make some problems to people when they are using their account. with the continuous development of the internet, online social media networks have developed quickly, such as Instagram, Facebook, and Twitter which has greatly changed the way of conversation of the people, develop the social circle and extract the people's interest in the social media research. At the same time, illegal behavior is also rising towards gang and organizational development We know that Facebook allows users to make a message to unknown persons from their account. Because of this it may cause serious problems to the user and are affected the user by their social image. Through that, some social media network users can get some vulgar and rude messages on the particular user account.

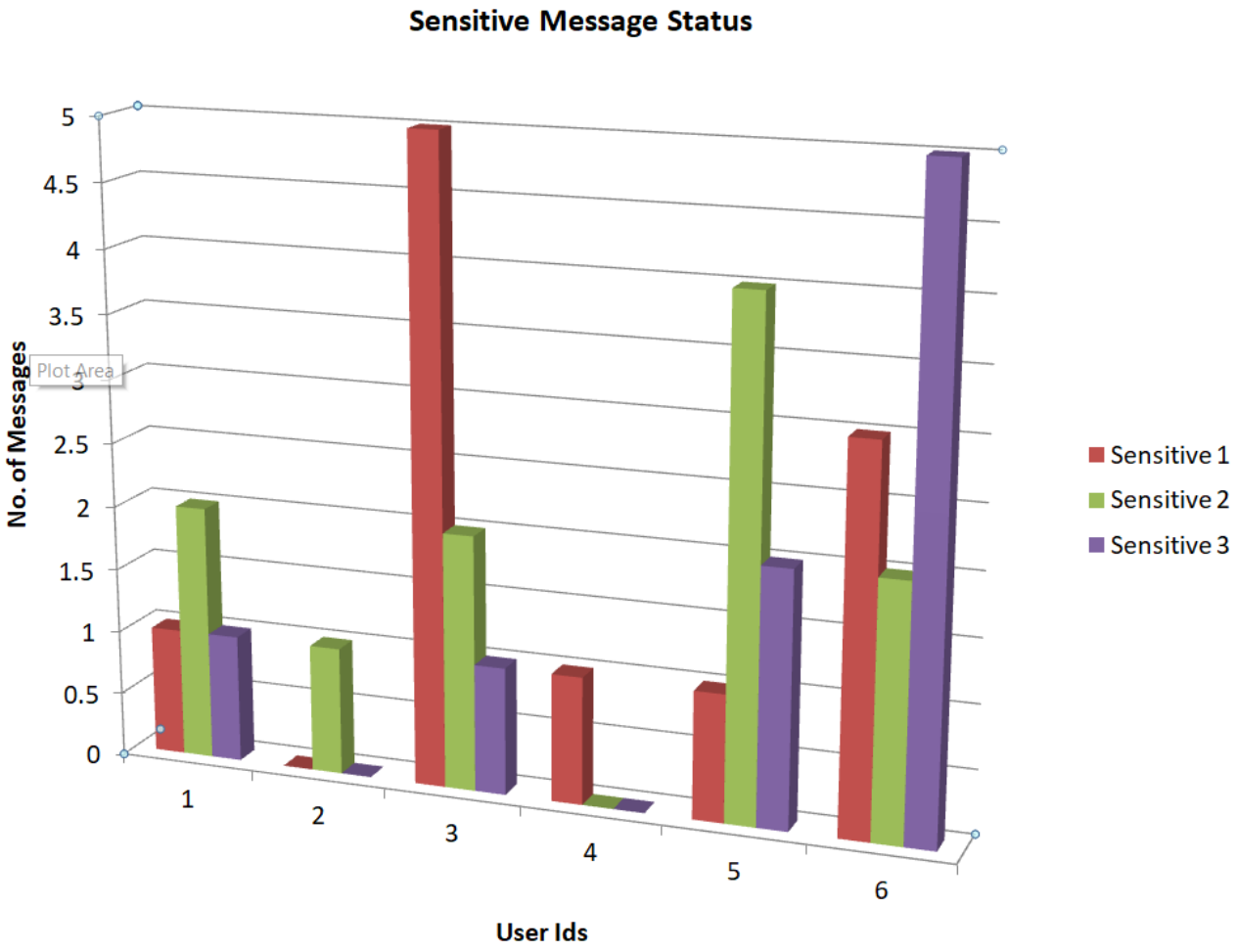

Fig 6. ***Graph considering the users comments falling under Sensitive Classification***

III. CONCLUSION

Sharing of information has become much easier through social networking sites which helps people to stay connected. As we have Facebook which allows the user to post a message or comment on each other walls. However, if the comment is obscene, it may have a negative impact on the user's reputation. To avoid this issue, information filtering is deployed to filter the message's content. As a result, we examined various information filtering approaches in this work, such as content-based filtering and policy-based filtering. The best filtering method is the content-based filtering method because it filters away harmful or non-neural terms from the input message and allows only pleasant comments to be displayed on a user's wall. This will help us in avoiding unwanted communications which may affect user’s reputation, which is more valuable in this society

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.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] V 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 symp- toms 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 solu- tions," 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 pri- vacy 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.

[11] A. Tundis, A. Jain, G. Bhatia, and M. Muhlhauser, "Similarity analysis of criminals on social networks: An example on Twitter," in Proc. 28th Int. Conf. Comput. Commun. Netw. (ICCCN), Valencia, Spain, Jul./Aug. 2019, pp. 1–9, doi: 10.1109/ICCCN.2019.8847028.

[12] G. Rigopoulos and N. V. Karadimas, "Military student assignment using NexClass decision support system," in Proc. 3rd Int. Conf. Math. Comput. Sci. Ind. (MCSI), Chania, Greece, Aug. 2016, pp. 213–218, doi: 10.1109/MCSI.2016.047.

[13] V. Ingilevich and S. Ivanov, "Crime rate prediction in the urban environ- ment using social factors," Procedia Comput. Sci., vol. 136, pp. 472–478, Jan. 2018.

[14 B. R. Prathap and K. Ramesha, "Twitter sentiment for analysing different types of crimes," in Proc. Int. Conf. Commun., Com- put. Internet Things, Chennai, India, Feb. 2018, pp. 483–488, doi: 10.1109/IC3IoT.2018.8668140.

[15] X. Sun, P. Zhang, J. K. Liu, J. Yu, and W. Xie, "Private machine learning classification based on fully homomorphic encryption," IEEE Trans. Emerg. Topics Comput., to be published, doi: 10.1109/TETC.2018.2794611.

[16]M. Abadi et al., "Deep learning with differential privacy," in Proc. ACM SIGSAC Conf. Comput. Commun. Secur., New York, NY, USA, 2016, pp. 308–318, doi: 10.1145/2976749.2978318.

[17] O. Ohrimenko et al., "Oblivious multi-party machine learning on trusted processors," in Proc. USENIX Secur., vol. 16, 2016, pp. 619–636.

[18] R. Bost, R. A. Popa, S. Tu, and S. Goldwasser, "Machine learning classification over encrypted data," in Proc. NDSS, 2015.

[19] H. Hassani, X. Huang, M. Ghodsi, and E. S. Silva, "A review of data mining applications in crime," Stat. Anal. Data Mining, ASA Data Sci. J., vol. 9, no. 3, pp. 139–154, Apr. 2016, doi: 10.1002/sam.11312.

[20] D. J. Wu, T. Feng, M. Naehrig, and K. Lauter, "Privately evaluating decision trees and random forests," in Proc. Privacy Enhancing Technol., vol. 4, pp. 335–355, 2016.

[21] R. K. H. Tai, J. P. K. Ma, Y. J. Zhao, and S. S. M. Chow, "Privacy- preserving decision trees evaluation via linear functions," in Proc. Eur. Symp. Res. Comput. Secur. (Lecture Notes in Computer Science), vol. 10493. Berlin, Germany: Springer, 2017, pp. 494–512.

[22] M. Joye and F. Salehi, "Private yet efficient decision tree evaluation," in Data and Applications Security and Privacy XXXII. Berlin, Germany: Springer, 2018, pp. 243–259, doi: 10.1007/978-3-319-95729-6_16.

[23] T. Veugen, "Improving the DGK comparison protocol," in Proc. IEEE Int. Workshop Inf. Forensics Secur. (WIFS), Tenerife, Spain, Dec. 2012, pp. 49–54, doi: 10.1109/WIFS.2012.6412624.

[24] L. Breiman, J. H. Friedman, R. A. Olshen, and C. J. Stone, Classification and Regression Trees. New York, NY, USA: Chapman And Hall, 1993.

[25] P. Paillier and D. Pointcheval, "Efficient public-key cryptosystems provably secure against active adversaries," in Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur., vol. 1999, pp. 165– 179.

AUTHORS

Miss. Sneha V Masaguppi is currently pursuing M.tech in the information Technology branch from UVCE, Bangalore. She completed B.tech at Gogte Institute of Technology, Belagavi. Her research interests are in the field of Web security, Cloud computing and data mining.

Dr. Manjula S H is currently working as a Professor, Department of Computer Science and Engineering, UVCE, Bangalore University, Bengaluru. She is a member of the Academic Senate, VTU Belagavi. She obtained BE and ME in the Department of Computer Science and Engineering from UVCE, Bengaluru.Ph.D.in Computer Science and Engineering, Chennai. She has published 120 technical articles in refereed journals and international conferences and authored three books. Her research interests are in the field of IoT, Cloud Computing, Wireless Sensor Networks and data mining, AI and Machine Learning.