ISSN 2348 – 9928
IJAICT Volume 5, Issue 3, March 2018 Doi:01.0401/ijaict.2015.11.04 Published on 05 (3) 2018

A SURVEY ON PROFIL$_R$: TOWARDS PRESERVING PRIVACY AND FUNCTIONALITY IN GEOSOCIAL NETWORKS

Ms. J. Aneeta Maria ***UG Student***

Ms. R. Shanmugapriya ***UG Student***

Ms. S. Veena ***UG Student***

Ms. Mishmala Sushith ***Associative professor***

Information Technology,
Kalaignar Karunanidhi Institute of Technology,
Coimbatore, Tamil Nadu, India.

Abstract— The sharing of one's own personal data in the online social networks has become such a sort of common task. In this paper we have reviewed the concepts of the techniques that enable us to locate our buddies online, the reasons for the leakage of our personal data to the third party vendors which are being used for the purposes of targeted ads. This paper also enlightens the anonymity for continuous queries, secure function evaluation technique, L-diversity method. The various privacy measures for the different environment has also been studied in detail.

Keywords— Location, Online Social Networks, Privacy, Security Sharing

I. INTRODUCTION

Online social networks has been a part of the day to day life and also a significant source for the third party vendors to extract the personal data for making the targeted advertisements and personalized recommendations to promote the business by their owners. These has also been a place where occurs the spatio-temporal incentives on posting and reviews. Providing the personal information keeps exposing people to certain risks. Without the information the provider cannot target on the people and with the leaked information there is no privacy for the users of these online social networks.

The remainder of this paper has been sections as follows the concept of finding the online presence of our peer and the methods by which our personal data has been leaked to the third party is explained in the section 2. The L-diversity,secure function evaluation as well as anonymity on continuous queries in briefed on section 3. The section 4 consists of the privacy featuring of the various environment. Finally section 5 sums up the conclusion of the project.

II. PERSONAL INFORMATION AND LEAKAGE

The personally identifiable information is the persons individual personal data on one's own or the data which could be acquired through other information [2]. Since the online social networks influence has been more people are providing their personal data to a vast extend by which the third parties are being accessing these dates from these sites.

1) Each user posses a unique identifier in the social networking sites which could be appeared in the url when we perform some actions. If 3rd party could access this unique identifier then the personal information can be retrieved by means of the live headers of HTTP.

2) The external applications of the online social networks might have download permissions which are unknown to the user.

The prevention could be done only by the way of limiting the details . Blocking the reference header directly in the browser as such as Firefox. The visible part with the unique identifier should be striped. Even the users email information and zip could be leaked which are not a part of online social networks. These identifier usage can be reduced by means of the specific values of the session.

The online social networks motivates the users for building up an presence on online which indicates their identity on offline too.[9] These networks constructs an illusion as if online accounts resemble for the actual offline person, whereas in realism the social networks present online lacks the basics for detecting impersonation. The author has hence thereby proposed the online social network users the ability to recognize everyone on the basis of the interaction made by them and also with the experience they possess. The impersonation is believed to be thwarted by those users possessing the shared knowledge exclusively, only a pair of friends share the secrete information.This has also described the existing protocols those using the shared secrets for the public key exchange which are being concealed from the attackers. The results from the Facebook user study is pictured so that the exclusive knowledge is shared between the Facebook friends thereby the attackers could rarely be able to guess it. The friend identification is also

showed where it could be extended through the trust built on web by means of the graph of friends on online social networks. The impersonation has always been a fundamental problem in this. The information on existing friends in Facebook is taken to be the advantage in Bond Breaker as practical tool which helps in identifying friends in the social networks.

[1] Consumer alert is a program which was in 2012 to notify the incentive writings of the fake reviews to promote the product that arrives as a bunch from the IP addresses of the same system. These alerts are removed within 90days and also renewed.

III. ALGORITHM AND SECURE FUCTIONS

In the mobile services which are of location based, the privacy preservation is given importance. [4] The users privacy is preserved by means of various cloaking techniques. The privacy disclosure as well as the poor quality of service are not being suited in the case of continuous queries. The two algorithms proposed here are the bottom-up cloaking and hybrid cloaking methods defined for the anonymous continuous queries.The Greedy cloaking algorithm proposed posses the success rate as highest one but it elapses a long cloaking time particularly at times of the high levels of privacy. The another proposed algorithm in this paper is the bottom up cloaking algorithm which contributes for the best efficiency yet the anonymization cost , postponed time as well as the the ratio of cloaking success are worse relatively: The hybrid cloaking algorithm proves to be the one with best performance in overall by means of the performance metrics on various terms.

A novel approach is used to multiparty computation in secure manner [15]. It actually avoids the use of sectre sharing & characterizing which is verifiable.This scheme involved to manipulation of cypher-text.It is underlying in private key shared by the participants.The main use of this is high degree of conceptual and simplicity of structural.It i also used for decrease the message complexity and sub-stained flexibility in order to giving input and output formats. It is called Mix and Match. Nonetheless is highly intensive manipulation bits.Mix and Match is suitable for sealed-bid auctions.So we used Mix and Match here based on auction. That is fully private and non interactive.It may be ready to adapt with strategies of wide range.

Electronic banking services are for the customer needs [14]. These electronic payments system have an impact on personal privacy and the illegal use that cause criminal use of payments. This is based on the third party.This can improve the lifestyle of each individual.This system is advantage when compared to anonymous payments systems,that this system doesn't have any security.A crypto-graphic system is been proposed for the anonymous payment system.Inability of third parties and ability of an individual and report can't be stolen.That represents the analogy and descriptions.Here the concept is or the basic idea to expose is blind signature,implementation by carbon paper,that will envelope within a slip of paper.for the voting purposes also this idea is been used.Here this has featured with two key digital signature.A function of signing and commuting.

The online content ratings services allows to find and share the content from new articles from videos to business [11].The services like yelp and Digg are increasingly becoming popular.These popularity is leading and increase the level of malicious activity such as multiple identity attacks and buying of ratings from users.we propose Iolaus, a system that leverage social network of online content rating system to defend against such attacks.

Two novel techniques are used in Iolaus.

- To defend against multiple identity attacks weighing ratings are used.
- To mitigate the effect of "bought"ratings relative ratings are used. Isolaus can perform existing approaches and serve as a practical defense against multiple-identity and rating-buying attacks.

Online content sharing services are used to find and share content that is used by users.Iolaus is designed to re-lace the existing content rating aggregation logic used by operator collect ratings by a set of user account on a set of content providing rating on a given piece of data.i.e is rater.

Geosocial Networks extend the online social networks with center and their functionality on the location of the users [5]. Most GSN provide similar functionality user check in at venues ,reporting their location to the geo-social network provider.the use of incentives has introduces reasons for cheating,motivating user to commit location fraud.By X_{ACT} we can detect the location of cheating attacks.it has been proved empirically and analytically.

X_{ACT} consists of mechanism that

- Bread-cast unpredictable WIFI ssids.
- Display QR codes encoding venue certified information.
- Implement challenge response.

X_{ACT} requires at least one attacker at the venue and also shows warm hole attacks.

Due to the Sybil accounts as well as Fake identities that prevail in online communities the CAPTCHAs and the other Sybil detectors based on graph could not be proven to be an effective defenses [10]. In this paper the author has developed an approach for detection where those users which have similar clickstreams are group to be a behavioral clusters, through the similarity graph which has partitioning to capture the clickstream sequence distances.

The practical section of this paper have been explained in two steps. Firstly the code is shipped to the team of security sections at LinkedIn as well as Renren. There those are evaluated in the environment of production to fresh data which evolves to be positive. These are then reported. Secondly the approach on the basic limits are discussed on the effect of the Sybil accounts which could exactly mimic the normal users clickstream patterns.

IV. PRIVACY IN SOCIAL NETWORKS

In this paper ,the main use of geo social network is discussed by the authors [13] .It is mainly used to notify the user when his/her buddies happens in proximity.Normally network is providing the proximity service.otherwise it is called as service provider.It is the main problem for who are not trust sp to handle the data &liking to realize their location information to participants.Two protocols used here to provide privacy with spans controllable privacy. Centralized architecture used in proposed system.it is updated issued from mobile devices that based on location only ***we can find proximity.***

1. User do not trust sp
2. User would like to control precision of the location

Two protocols are

1. C-Hide&Seek
2. C-Hide&Hash

In this two protocols C-Hide&Hash technique is most efficient than the other one.

Social Networking service improves the growth of network and giving more security and privacy for users [14] . The centralized storage represent weakness that so far and not satisfying been addressed.To solve this problem Safebook was introduced. Safebook has decentralized storage system.In SNS the computer network data and structures re stored.commercial providers running the SNS like Linkedh corp, facebook, google, myspace Inc .Through this account ,videos ,images,pictures can be shared in secure manner by the registered user.Authorized user can share the information with another user securely.mainly on social networks ,information are conveyed between the users as secret.OSN supporting for decentralization.It ignores the central entity of omniscient and relationships of social networks.

Nowadays online social networking protect the security and privacy of social networking information of the users as little bit [8].It can be easily identified and understand by other users.So the information given in this sites not secure one.The stored information may be cheated by attackers.So many users feel victimized and dis-empowered by online social networks providers.This paper presents lockr that can improve the privacy of centralized and decentralized sharing system in online.This lockr provides three privacy benefits to online social network users.

1.The content social networking from all the functionality of OSNs provide will be separated. Their social information will be decoupling to the users.They can select the information should be stored in which OSN&information should be handled by which third parties&who can access that.this kind of flexibility provides privacy to the users information.

2.Second ,locker ensures that digitally signed social relationships need to access social data cannot be reused.and also for unintended purposes online social networks are been used.so online social networks has been the trusted one for the users.this also reduces the relationship between the other social users.through this key locker enables the message encryption.without exposing to others this can be verified by a common privacy threat by sharing the data in a decentralized way.

3.This paper relates the lockers design and implementation and integrate with a flickr a centralized online social networks and bit torrent,a decentralized.here lockers critical primary is demonstrated.and also this has secondary benefit that is site management and accelerating content delivery.

[3] The authors explains as that the users need to search for nearby points of interest based on service,that preserves the users location.we are presenting a technique for the retrieval of information that is private and allows the users data from a database server without revealing what is being processed in the server.This operation will make efficient resources for hardware such as smartphones,that have limited processing power,memory and wireless bandwidth.our algorithm make use of a variable sized heavy traffic region,increases location privacy of the user and maintains same traffic cost.

Our proposal do not trust on third party component and have a compromise between user privacy and computational efficiency.

The problem is that if the user's actual location is provided as the origin to the lsb's,that performs on look up of pols,then lbs will learn that location.And this approach cannot rely on a

secure processors that is not even found in smart phones and other applications.

In order to know the user interest along with their preferences the process of online behavioral advertising method is followed where the users has been tracked [6]. These data obtained from tracking are used for the targeted ads purposes.The author in this paper has proposed an practical architecture which targets the user interest but still without damaging the privacy of the users.The behavioral tracking and targeting on users profile is made at users browser. The major complication in this is pictured as billing where correct advertisers must be billed by the ad-networks without the actual knowledge about that the ad that has been displayed for the user.This enlightens those many issues which must get addressed for maintaining the tension of user privacy and behavioral targeting. The various issues as if the advertising budgets, the issues on billing, latency of the networks, efficacy of targeting, the behavior of the malicious as well as many other issues are addressed.The crypto-graphic system of billing proposed in this paper enables the behavioral advertising on the privacy preservation.

To provide services to the user the location co-ordinates are rely on location based social applications[12] .Today in smart phones these applications are passed to the untrusted third party. These servers has the application logic to send the information. several techniques are been employed these design are been followed.

These LBSA are been used for the untrusted third party servers. they are encrypted data stores and moved to the client devices. the location co-ordinates are encrypted when it is shared and this can be decrypted only by the users. This techniques improves the location privacy for users. It also supports or provide flexibility to a wide variety of location based applications. Proposing new application for the design. Applications as collaborative content downloading, here the security, trust became a problem. If the application are used to share the encrypted data and also non social applications can also be extended. And also need to develop the novel mechanisms for the users to discover the key securely to encrypt the data on server without revealing the key to the server.

V. CONCLUSION

This survey paper explains the various existing methods and process by which the personal data has been reaching the third parties. It also gives a brief notes on the various privacy measures in existence which has been a contribution for the creation of the profil$_r$ framework. It details the ways and protocols for the tracking of the online buddies.

References

[1] Yelp, Inc., San Francisco, CA, USA. (2014, Feb. 28) [Online]. Available: http://www.yelp.com

[2] B. Krishnamurthy and C. E. Wills, “On the leakage of personally identifiable information via online social networks,” Comput. Commun. Rev., vol. 40, no. 1, pp. 112–117, 2010

[3] F. G. Olumofin, P. K. Tysowski, I. Goldberg, and U. Hengartner, “Achieving efficient query privacy for location based services,” in Proc. Privacy Enhancing Technol., 2010, pp. 93–110.

[4] X. Pan, X. Meng, and J. Xu, “Distortion-based anonymity for continuous queries in location-based mobile services,” in Proc. GIS, 2009, pp. 256–265.

[5] A. Machanavajjhala, J. Gehrke, D. Kifer, and M. Venkitasubramaniam, “L-diversity: Privacy beyond k-anonymity,” in Proc. 22nd Int. Conf. Data Eng. (ICDE), 2006, pp. 1–24. Forman, G. 2003. An extensive empirical study of feature selection metrics for text classification. J. Mach. Learn. Res. 3 (Mar. 2003), 1289-1305.

[6] V. Toubiana, A. Narayanan, D. Boneh, H. Nissenbaum, and S. Barocas, “Adnostic: Privacy preserving targeted advertising,” in Proc. Network Distrib. Syst. Security (NDSS) Symp., 2010, pp. 1–3.

[7] A. Cutillo, R. Molva, and T. Strufe, “Safebook: Feasibility of transitive cooperation for privacy on a decentralized social network,” in Proc. IEEE WOWMOM, Jun. 2009, pp. 1–6.

[8] A. Tootoonchian, S. Saroiu, Y. Ganjali, and A. Wolman, “Lockr: Better privacy for social networks,” in Proc. ACM CoNEXT, 2009, pp. 1–12.

[9] R. Baden, N. Spring, and B. Bhattacharjee, “Identifying close friends on the internet,” in Proc. Hotnets, 2009, pp. 1–6.

[10] G. Wang, T. Konolige, C. Wilson, X. Wang, H. Zheng, and B. Y. Zhao, “You are how you click: Clickstream analysis for sybil detection,” in Proc. USENIX Security, 2013, pp. 1–15.

[11] A. M. Kakhki, C. Kliman-Silver, and A. Mislove, “Iolaus: Securing online content rating systems,” in Proc. 22nd Int. World Wide Web Conf. (WWW), Rio de Janeiro, Brazil, May 2013, pp. 1–5.

[12]] K. P. N. Puttaswamy and B. Y. Zhao, “Preserving privacy in location based mobile social applications,” in Proc. 11th Workshop Mobile Comput. Syst. Appl., New York, NY, USA, 2010, pp. 1–6.

[13] S. Mascetti, D. Freni, C. Bettini, X. Sean Wang, and S. Jajodia, “Privacy in geo-social networks: Proximity notification with untrusted service providers and curious buddies,” VLDB J., vol. 20, no. 4, pp. 541–566, Aug. 2011.

[14] D. Chaum, “Blind signatures for untraceable payments,” in Proc. Adv. Cryptol. CRYPTO, 1982, pp. 199–203.

[15] M. Jakobsson and A. Juels, “Mix and match: Secure function evaluation via ciphertexts,” in Proc. Adv. Cryptol. 6th Int. Conf. Theory Appl. Cryptol. Inf. Security, 2000, pp. 162–177.