Privacy and Security Issues In Mobile Social Networking and in Modern Shopping Experience

Sanjeev Kulkarni[1]
Angadi Institute of Technology & Management, Belgaum, India
sanjeev.d.kulkarni@gmail.com

Kirna Kumari[2]
Angadi Institute of Technology & Management, Belgaum, India
kumari.kiran18@gmail.com

Naheeda Kittur[3]
Angadi Institute of Technology & Management, Belgaum, India
nida.kittur@gmail.com

Abstract— Future shopping applications collect basic profile information of the person and provide great service on recommending books, electronics and other products based on user profile, previous shopping history and relationships between the items categories derived from purchases of all the users on the site. The mining of user's profile greatly enhances a person's shopping experience on modern online shops. We have compared two tailor made protocols with our proposed system. The main purpose of this paper is solving the privacy and security issues.

Keywords-Social Networking, Persons Identity, Privacy & Security Issues, GPS, Near Field Commpunications, Reccomendation Engine.

I INTRODUCING SOCIAL NETWORKING

A social network is a social structure made of nodes (which are generally individuals or organizations) that are tied by one or more specific types of interdependency, such as values, visions, ideas, financial exchange, friendship, relationships, kinship, dislike, conflict or trade. Social network analysis views social relationships in terms of nodes and ties. Nodes are the individual actors within the networks, and ties are the relationships between the actors. The resulting graph-based structures are often very complex. There can be many kinds of ties between the nodes. Research in a number of academic fields has shown that social networks operate on many levels, from families up to the level of nations, and play a critical role in determining the way problems are solved, organizations are run, and the degree to which individuals succeed in achieving their goals [9].

Social Applications Powered by Mobile/PSN

All social applications are called as social network applications, if we are thinking of building a social application then that means we are trying to build a social network. A social network is a collection of people bound together through a specific set of social relations which means connection between people that permits the exchange of information.

One popular use for this new technology is social networking between businesses. Companies have found that social networking sites such as Facebook and Twitter are great ways to build their brand image. Companies are able to drive traffic to their own online sites while encouraging their consumers and clients to have discussions on how to improve or change products or services.

Social networks are also being used by teachers and students as a communication tool. Because many students are already using a wide-range of social networking sites, teachers have begun to familiarize themselves with this trend and are now using it to their advantage. Teachers and professors are doing everything from creating chat-room forums and groups to extend classroom discussion to posting assignments, tests and quizzes, to assisting with homework outside of the classroom setting. Social networks are also being used to foster teacher-parent communication. These sites make it possible and more convenient for parents to ask questions and voice concerns without having to meet face-to-face. The use of online social networks by libraries is also an increasingly prevalent and growing tool that is being used to communicate with more potential library users, as well as extending the services provided by individual libraries.

A confluence of advancements of mobile phones, sensors and Internet brings many opportunities to enhance our experiences in everyday tasks and functions. Social networks also depict the relationships between various users of the networks such as members list of their friends and relations. Since people spend more hours on the social network, profiles can be mined using the stated profile, usage patterns, group patterns and many more. It is possible for individuals and marketers to get benefited from the information, provided the privacy and data security concerns are addressed.

II PRIVACY ISSUES

The information that is leaked online could be used against them. Some examples are listed below:

If you are having an online conversation with your friend(s) or with other members then you should be aware of conversation, because the Internet keeps a permanent record of what we say to each other.

Social networks introducing geo-location services a record of where we go and how long we spend there will also be maintained and that can be seen by countless others and that a record will be kept somewhere on the Internet. Thieves will keep the track of each person and family members, sometime it proves to be harmful to them.

Certain information could be used in cyber bullying and/or cyber stalking.

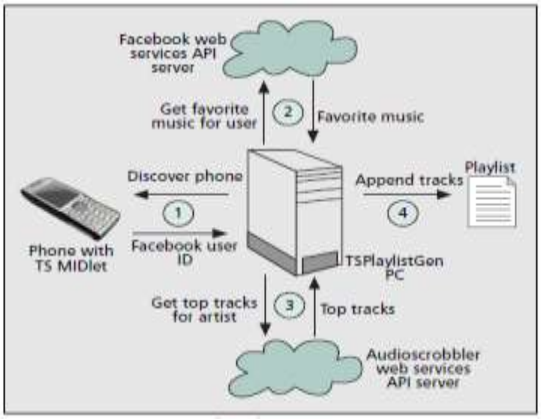
There is also the threat posed in the real world from your activities online, for example updating your social network profile that you are on vacation for two weeks could be used by criminals to target empty houses to be burgled, especially if you have your home address published on the site and regularly update people on the latest electronic gadget like android phones that you have purchased [13].

Most people often use non-secure passwords and base them on items typically close to them like names of family members, date of birth etc. That information could be used by criminals to guess your password and compromise your social network account to spam your contacts. If you use the same password across all your systems such as banking and email then they could be compromised too.

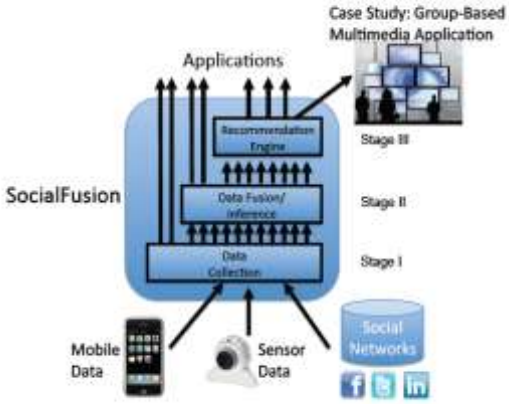
Social networks are just another outlet for humans to interact and share their views. One should look at social networks as opportunities to interact with one another or other people locally or globally and not as threats. In order to be an active user of social networks one has to make many friends and business contacts online [12][15].

If people are not anonymous on these social networks then their value is severely determined. It is not possible take someone's opinion or recommendations on board if they are anonymous. Anonymity, does not necessarily equate to privacy. Unless we have other reasons to be anonymous, e.g. accessing sites from within a totalitarian regime, then we do not think of using software solutions to help with anonymity is the answer.

III RELATED WORK


Facebook web services API server
Get favorite music for user
2
Favorite music
Discover phone
1
Facebook user ID
Phone with TS MIDlet
Append tracks
4
Playlist
TSPlaylistGen PC
Get top tracks for artist
3
Top tracks
Audioscrobbler web services API server

WhozThat allows us to build local context-aware applications and services. These services listen to the announced IDs and adapt their behavior to the people that are located near the service. Consider uses of social data in applications like a video/musical juke box where social data can be used to play or suggest movies and titles to the user based on an individual's or the group's interests. In this case, profile data is submitted to the juke box and the juke box determines the list of songs/video suited to the audience. Social data here can be anonymised in case a person/group wants to remain unidentified [4].



In the side shown figure illustrates SocialFusion's multi-stage computing framework. The first stage collects together data from three major classes of data input streams, namely social networks, mobile phones, and sensor networks. The second stage incorporates inference functionality whose task is to fuse the data and thus derive higher-level contextual meaning in the form of descriptors from the raw data. These descriptors, combined with the original data, are then supplied to a third stage consisting of a recommendation engine that decides what kind of context-aware action to take [5].

Suggested Works: WhozThat integrates existing social networks like MySpace, Facebook with mobile phones to provide context-aware audio, but it does not integrate with any sensors to provide more efficient and fully context-aware inference and recommendation in ubiquitous computing environments. Such kind of protocol services are for shorter range and not for longer range services and apart from risk on data security and person's identity. However, if the user decides to buy the album or video at the kiosk or even swipe the store card during a different action at the kiosk, then data is no longer anonymous. The credit card/store card information provided will now uniquely identify the user and annonymised profile that was received from the social network is now associated with the card. Privacy of profile data is forever lost. Similarly, providing anonymised data and then purchasing in any shopping scenario would essentially give away social data.

IV PRIVACY & SECURITY ISSUES IN WhozThat/SocialFusion

Despite safeguards protecting both location and data privacy, a user's anonymity may still be compromised by revealing context-aware recommendations in public settings. Even though a participating user may have taken precautions in each of his individual data streams to independently shield certain information from others, e.g. financial or relationship status, the correlative power of SocialFusion in integrating multiple information sources may reveal in its recommendation potentially damaging or embarrassing information[5][11].

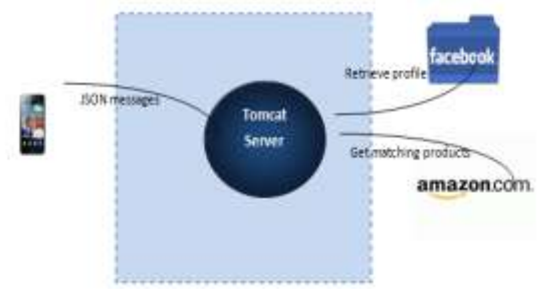
Social Fusion uses a slightly different approach to K-anonymizing the data. Given a partial release of data from a private data set, wherein all data is quasi-identical, the released data must map to at least k distinct sets of individuals within the data set. We have made progress on developing a new approach to K-anonymize diverse streams to preserve individual privacy. Prior work in K-anonymity seems unsuitable for context-aware mobile social networks because it assumes access to the entire data set, makes wrong assumptions about quasi-identifiers, or assumes that data may be distorted or generalized and still useful. For example, the algorithms may distort the data in some manner, either by introducing a random perturbation or transformation into the social graph, or by generalizing or "fuzzifying" the information. Such generalization may distort context-aware recommendations and output actions. We seek to develop a new class of K-anonymity algorithms that selectively withhold data, thereby preserving both the K-anonymity of the released data and its accuracy. We are thus developing K-anonymity algorithms, which meet our new K-anonymity definition using optimized or selective holding [14][15].

Peer-to-peer mobile social network systems, like WhozThat and SocialAware, exchange users' social network identifiers between devices using short-range wireless technology such as Bluetooth. In contrast to these systems, a mobile device in client-server mobile social network systems, such as Brightkite and Loopt, notifies a centralized server about the current location of the device (available via GPS, cell-tower identification, or other mechanisms) [6]. By querying the server, mobile devices in these client-server systems can find nearby users, information about these nearby users, and other items of interest.

Direct Anonymity Issues: The information exchange model of the mobile social network systems discussed previously provides little protection for the user's privacy. These systems require the user to allow access to his or her social networks profile information and at the same time associate that information with the user's identity. For instance, Facebook applications generally require the user to agree to give the application access to his/her information through Facebook's API, intrinsically tying such information to the user's identity [5]. In the WhozThat and SocialAware systems, anyone near the mobile user can use a Bluetooth device to snoop a user's shared social network ID or eavesdrop on data sent openly over a wireless connection, since all data transmitted over the wireless connection is sent in the clear, although relatively weak provisions for link-layer encryption exist [17].

The Indirect or K-Anonymity Problem: One worthwhile challenge is that of supporting complex mobile social networking applications with personal information without compromising the anonymity of the users providing the information. Even if the user does not directly provide his/her identification information, the user's provided social network information (such as preferences) may be mapped back to the user's identity through the social network site or information cached within mobile and stationary devices in the environment. The indirect anonymity problem exists when a piece of information indirectly compromises a user's identity. An example of this is when a piece of information unique to a user is given out, such as a list of the user's favorite movies, this information might then be easily mapped back to the user.

The K-anonymity problem occurs when n pieces of information or n sets of related information can be used together to uniquely map back to a user's identity. Furthermore, if a set of information can only be mapped to a set of k or fewer sets of users, the user's anonymity is still compromised to a degree related to k. The challenge is to design an algorithm that can decide what information should and should not be given out in order to guarantee the anonymity of associated users. The abundance and diversity of social network information makes this privacy guarantee more complicated than it may initially appear. More formally, the particular problem is to find what personal information can be shared such that this information cannot be used to associate the user's identity with a specific context [1].



V. OUR PROPOSED SYSTEM

In the side shown figure mobile is an intermediary device between social network shopping application i.e. amazon.com shopping application. First application of this tailor made proposed system contacts the social network that is facebook and gets friends profile and secondly this our system detects those friends location who are around him/her using GPS. Third step is to detecting group and retrieves social friend's profile through social network and match friends preference with shopping application and finally after matching the products list it will be displayed on the mobile personal computer or cell phone as recommended list.

In order to avoid loss of anonymity, we propose that the mobile with its computing power, connectivity and display act as the intermediary for the social data and store's products and offers. In this case, mobile will receive the social data and store offers. Mobile at this time, can query of additional categorization for a given product from the store, if required. The Store already has this information. Additionally, mobile can also store historical information locally and use that piece of information in making decisions. Mobile can now compute the matching offers/interests. This computation is not insensitive since the profile is already synthesized on the social network. This scheme is also applicable in the group dynamics.

VI COMPARISON TABLE:

	WhoZ That & Social Fusion	Our Proposed Solution
Group detection	Server can detect the group provided the location updates are available. It uses fuzzy algorithms collating location sensor and social data to do group detection. However, this requires that location has to be updated on the server thus leading to leakage of location data to a third party [2][4].	In our proposed project, group detection is done on the mobile.
Privacy	Reads data from Social Networks/Service provider like Netflix/IMDB. K-anonymised data in server [1]. Homogeneity Attack: k-Anonymity can create groups that leak information due to lack of diversity in the sensitive attribute [1]. Background Knowledge Attack: k-Anonymity does not protect against attacks based on background knowledge [1].	Mobile is intermediary device social data, database and recommendation engine. Group detection and preference aggregations are done on the mobile. Since, mobile is an intermediary device, no data is sent to server. Therefore, data is more secured and identity of the person remains anonymised.
Recommendations	Social-Fusion organizes input data streams into three major classes, namely mobile data from smartphones, sensor data from fixed sensor networks, and social networking data from online social networks. Since all layers are integrated or fussed into server all tasks like preference matching and execution of recommendation engine takes place in the server i.e. SocialFusion system [2].	Recommendation engine external preference matching is on both sides on the mobile as well as on the server. In our proposed project some part of profile matching is done on server to save memory space and main part of profile matching is on the mobile to protect data and identity of a person.
Static / Dynamic	Theses tailor made protocols supports for only static (in particular shop)	Theses tailor made protocols supports for only dynamic not restricted to particular shop)

VII. CONCLUSION:

Social data mining and sharing of this data to third party corporations and merchants will become inevitable and precisely because of this inevitable progression, there is a great fear from general public, activists and governments that privacy of people will be lost forever. People are also concerned that such social data can be used for malicious purposes, may affect job prospects and other aspects of life. Social networking sites are only too aware of these sentiments and struggling hard to provide privacy and yet try and use that data and monetize it to make their business a successful commercial venture.

VIII REFERENCES

Ashwin Machanavajjhala, Johannes Gehrke, Daniel Kifer, "ℓ-Diversity: Privacy Beyond k-Anonymity". Published in ACM Journal Name, Vol. V, No. N, Month 20YY, pp. 1–47.

Fusing Mobile, Sensor, and Social Data To Fully Enable Context-Aware Computing by Aaron Beach, Mike Gartrell, Xinyu Xing, Richard Han, Qin Lv, Shivakant Mishra, Karim Seada, 1. University of Colorado at Boulder, 2. Nokia Research Center Palo Alto.

Saeed Kazi, Mikael Savia,, "LOCATION TRACKING USING GPS". Department of Computer Sciences and Information Systems.

Beach, Mike Gartrell, Sirisha Akkala, Jack Elston, John Kelley, Keisuke Nishimoto,Baishakhi Ray, Sergei Razgulin, Karthik Sundaresan, Bonnie Surendar, Michael Terada, and Richard Han, University of Colorado at Boulder. WhozThat? Evolving an Ecosystem for Context-Aware Mobile Social Networks, IEEE Network, July/August 2008, Page No.: 50-55.

Aaron Beach, Mike Gartrell, and Richard Han, University of Colorado at Boulder, Solutions to Security and Privacy Issues in Mobile Social Networking.

M. Weiser, "Some computer science issues in ubiquitous computing," Communications of the ACM, vol. 36, no. 7, 1993.

N. Eagle and A. Pentland, "Social serendipity: Mobilizing social software," IEEE Pervasive Computing, vol. 4, no. 2, 2005.

E. Miluzzo, N. D. Lane, K. Fodor, R. Peterson, H. Lu, M. Musolesi, S. B. Eisenman, X. Zheng, and A. T. Campbell, "Sensing meets mobile social networks: the design, implementation and evaluation of the cenceme application," in Proc. of ACM SenSys, 2008.

C. M. Gartrell, "Socialaware: Context-aware multimedia presentation via mobile social networks," Master's thesis, University of Colorado at Boulder, December 2008.

G. Adomavicius and A. Tuzhilin, “Toward the next generation of recommender systems: A survey of the state-of-the-art and possible extensions," IEEE Trans. Knowledge and Data Engineering, vol. 17, no. 6, 2005.

A. Jameson, “More than the sum of its members: challenges for group recommender systems," in Proc. of ACM AVI, 2004.

G. Miklau, D. Jensen, P. Weis, and S. Srivastava, "Anonymizing social networks," University of Massachusetts Amherst, Tech. Rep., 2007.

Q. Wei and Y. Lu, "Preservation of privacy in publishing SocialNetwork data," in Proc. of IEEE ISECS, 2008.

B. Thompson and D. Yao, “The union-split algorithm and cluster-based anonymization of social networks," in Proc. of ACM ASIACCS, 2009.

A. Campan and T. Truta, “A clustering approach for data and structural anonymity in social networks," in Proc. of ACM PinKDD, 2008.

M. Wirz, D. Roggen, and G. Troster, “Decentralized detection of group formations from wearable acceleration sensors," in Proc. of IEEE SocialCom, 2009.

E. Miluzzo, N. D. Lane, S. B. Eisenman, and A. T. Campbell, "Cenceme - injecting sensing presence into social networking applications," in Proc. of EuroSSC, 2007.

A. Campan and T. Truta, "A clustering approach for data and structural anonymity in social networks," in Proc. of ACM PinKDD, 2008

Authors Bibliography with Photo

	First Author Sanjeev Kulkarni has completed M.Sc in Computer Science, MCA and M.Phil in Computer Science and pursuing Ph.D in Computer Science from Shivaji University, Kolhapur, under the guidance of Dr. A.M Sankpal and Dr. R.R Mudholkar and he has submitted final thesis on January 4th 2013. He has published four papers in International Journals and five papers presented in International Conferences. Presently, he is working as Assistant Professor and HOD in Angadi Institute of Technology and Management, Belgaum, India.
	Second Author Kirna Kumari has completed her Bachelor degree in Computer Science and pursuing Masters Degree in Computer Science (Final Sem). She has published one paper in International Journal and presented one paper in International Conference
	Third Author Naheeda Kittur has completed her Bachelor degree in Computer Science and pursuing Masters Degree in Computer Science (Final Sem). She has published one paper in International Journal and presented one paper in International Conference.