Security and Privacy Issues on Social Networks

***Abstract*--In this survey, the issues related to privacy and security in social networks are highlighted. Social networks are filled with very sensitive information which need to be protected from various threats. While coming towards privacy, it also an important concern which should be taken care off because transparency can lead to security issues and get effected by threats. Here, how privacy relates to security is also explained. Next, we discuss about some of the mechanisms involved in protecting the privacy and security. We are focusing on an example of Facebook, where attackers making use of it for stealing personal information of users. Now-a-days huge number of social mobile applications are developing for allowing people interact each other more frequently. Among these applications, location based applications are more vulnerable to security breaches. Finally, we discussed about current researches going on in the field of network security for managing the data of users securely.**

***Keywords*—**Applications, Attacks, Clickjacking, Cloning, Client-Server, Encryption, Facebook, Malware, Network, Security, Techniques, Threats.

Introduction:

Here we discuss about the threats which effects the user's data in terms of privacy and security of fragile information. As everyone know that social network reports as a web applications where users create their profiles to connect different persons. They can share their information on these kinds of social networks whether it is private or public. Hence it maintains large set of delicate data. The concept of social network security helps us in having pleasure towards social networks while pacifying security risks. By using various network security mechanisms, the risks and security threats affecting the organizations can be resolved. The victims who use these kinds of network may face the threats due lack of security measures.

As we all know, social networks are used to communicate with friends, family and colleagues for the different purposes. Till last few years, people have been using "net model" (Websites) to share information, to communicate within and outside of business organizations. But now-a-days, Mobile applications are in trend, where almost all Social Networking websites launched the mobile applications. The people can now, exchange the information with other people anywhere, anytime. In recent days, the researchers came to know that semantic web technologies (FOAF) and RDF based vocabularies adapted to access different web based social networks which made it so simple. These made sharing of the information easy which helps the owners to gain control over the accessing information. In the business field or in an organization they most probably use client-server architecture to share the information among their employees. Here, we have two kinds of information, explicit and implicit. Explicit information is based on the purpose of the user that is to be stated which is not necessarily not accurate. For example, we can see the details of the users like birthday, place of study/work, etc. on their profile page. Basing on the explicit information, implicit information concludes about a user or community where both are not accurate. For example, the user connects to different users and they can express their views based on their interests. Interestingly, we can say that explicit and implicit information are almost accurate and always have close bounds.

In fact, the user's personal information is exploited for business or marketing purposes and used by government to track the person, with use of online predators in worst cases. It is a challenging issue that security mechanisms of social networks can give protection to the private information and the resources that are access to share.

Background

Social networks are consisting of different individuals, work and relationships which are defined as the "small-world networks". In this section, we have given a brief introduction about the mobile social networking and related technologies.

a) Mobile computing:

Smart phones can allow people to connect easily through the internet and it develops the best environment for the third-party application developers. The main advantage of smart phones is, they can be carried easily to everywhere and can connect to different online social networking sites with help of mobile applications. The smart phones which has the capability of wireless connections, internet access and the third-party development applications usage has been raised to an extent level.

b) Social networks:

In social networks, the most usage of Facebook had a wide range of users. 200 million active users who visit the static page facebook.com moreover 100 million users use it daily. Nearly 1user out of 10 users who visits internet daily log on to Facebook page when we compare with the comScore's global internet usage statistics. By survey, we can say that over 30 million users are using the Facebook in smart phones who are 50% more active than the non-mobile users.

c) Existing mobile network applications

By using user location and context information there are many applications which integrate the social network applications in a simple and traditional manner. The mobile phones which are having access to the social networks, provides an interface application which is optimized to those mobile phones. The application for iPhone, blackberry which is having an instance application where users interact natively with the Facebook from his/her phone. Here the sensor network is also one approach for social network which turns phone into a sensor extension social network. One of the approaches named "CenceMe", which enrich the focus on user context in social network. User's mobile device when integrated deeply should be more than the sum of their parts where these applications do not consider for both users context and social network information.

In general, whozthat is an application which uses mobile computing technology for the transfer of contextual information which is taken from the social networking sites to the user useful application. Serendipity is also an application which is similar to whozthat with the same mechanism. LAMSN services like Brightkite and Loopt have some functionality like whozthat and social aware. These services have their own popularity databases compare to something which is more popular sites in social network such as Facebook in sharing contextual information like serendipity.

Categories in Social networks sites

Based on the main purpose, social networking sites are categorized as follows:

a) Contact Sites

Popular sites for example LinkedIn, PLAXO, where the major need is for sharing contact and which the contact details can be accessed by others such as Friends or the unknown individuals or Organizations with the permission, so these sites can expose each individual contact and help them in many ways.

b) Social Networking sites

Social sites such as Facebook, Myspace, TWITTER mostly focus on people and their activities in their day to day life and share information with others. Anyhow these are majorly used as personal sites, now-a-days most of the organizations are focusing on these sites to promote their products at a free of cost and parallelly they are becoming as some commercial sites too.

c) Visual Information Sharing Sites

There are so many sites and applications related to visual sharing such as YouTube, flicker and snapchat allowing to share video and live photo content. Snapchat can also considered as social networking site because what the video we share can be viewed by other users and also YouTube does the films and their trailers, education and gadget related videos that can be shared/viewed.

d) Game and Interactive Virtual Reality sites

Most of the virtual reality sites such as second life, world of Warcraft. In these sites the users mostly create avatars and communicate with others as creating a virtual world. In these sites most of the people play games in according to Warcraft. People create their own army and play with others. These are majorly referred as Massively Multiplayer Online Role Playing Games (MMORPG). Some social networking sites such as Facebook provides the platform for their users to play games while communicating. Other sites such as AtoZgames can be used to share the game what they have played with others.

Security Threats and Privacy Issues

Now-a-days, with increasing usage of social networks, the users are able to enjoy benefits of social networking and they are also effected with threats to privacy and security without their knowledge. These threats can be categorized into four types namely Classic threats, Modern threats, Combination threats and threads targeting Children and Teenagers. We had a detailed description of these threats in the next paragraphs.

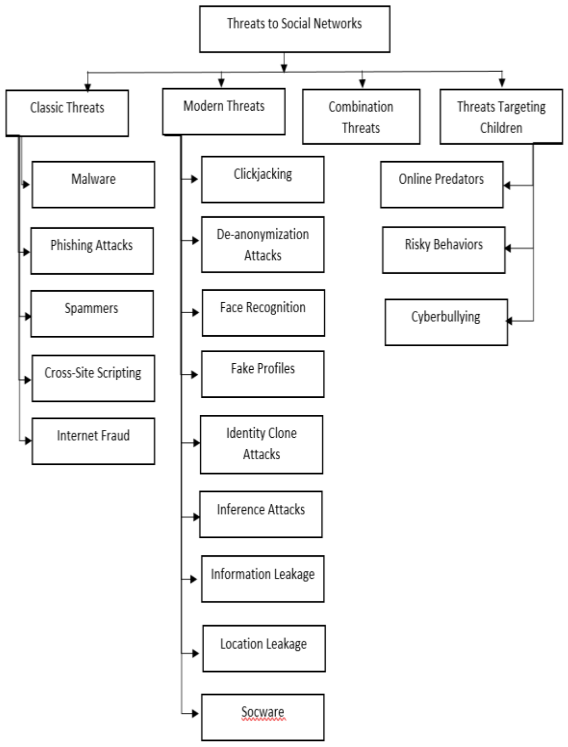

Fig 1: Threats to Social Network users

Classic Threats

These threats are in existence since the usage of Internet has increased. Even though these threats are older, these threats are becoming viral because they can spread faster among network users.

The target of these threats is to steal the personal information of users posted on social networks. These not only attack the user but also the people who are in contact with user.

For example-If a malicious code is planted inside a attractive application or a message then a innocent user may open that message and get effected with the threat. In most of the cases, these threats are responsible for stealing the user's resources such as bank details, credit and debit card details, phone numbers, social network account and password details and in some cases, they can even steal the computer's power and internet bandwidth to make the user part of their crime. Once the account details are leaked, the control over the account is transferred to attacker from the user.

The types of classic threats

a) Malware:

Malwares interrupts the computers from normal operation and making their status to abnormal and collects the personal data of the user. Malwares spread making use of internet or social networks as a medium from one user to another user. The first successful malware which tensed the users of various social networking sites like Facebook, Myspace, Twitter is named as "Koobface".

b) Phishing attacks:

These attacks are considered as social engineering and these attacks purpose is to steal the user's sensitive information by cloning a popular and trusted website. Once Facebook users has faced this kind of situation. The attackers duplicated the login page of Facebook and attracted the users to login from the duplicated page and stole account usernames and passwords of billions of users. They used this data to post spam URLs on the user's timeline to attract the friends.

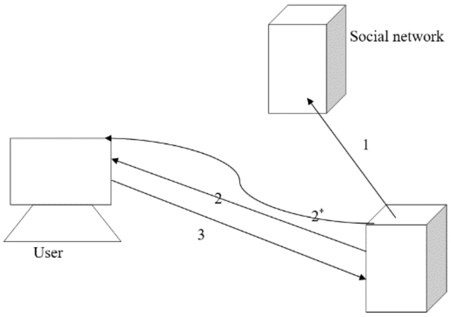

Fig 2: process of phishing attacks

The sequence of process is explained in the following steps

1- Information from the social networks is collected by the attacker.

2-Send the personal details with constructed application or fabricated message.

2^* -Social network provides a place to the fabricated message.

3-Sensitive information which is additional is to be collected.

c) Spammers:

These types of attacks make electronic mailing system as medium to advertise the third parties even the users are not interested about them. They collect email addresses of the users from various sources like chatrooms, websites, pop-ups, third party applications. The spammers make money by selling this data to third parties and these third parties use that data to advertise for themselves through emails.

d) Cross-site scripting:

These attacks take advantage of vulnerabilities in web-applications, plug-ins, networks systems on which the users depend. The attackers inject the malicious code into the compromised applications and gain privileged permissions from users without user's knowledge to access the sensitive content stored in computer or other opened along with the spammed website.

e) Internet fraud:

The attackers anyhow manage to enter account of users who travel abroad. They pretend as they original users and ask friends of the users to transfer money to bank account.

Modern threats:

The main function of these threats is to collect the personal information of both the user and his/her friends through social networking as a medium. There are different types of Modern threats

a) Clickjacking

It's a technique which makes the user to click on strange on a social networking site. But, that not the same what the user intended to click. A spam message is hidden behind the mask what user clicked which makes user to post that spam message on user's timeline. In 2009, the twitter's users were attacked with this kind threat named "Don't click". The attacked posted a spam message with mask showing "Don't click" along with duplicate link. But, there the spam URL is hidden behind mask. This made the twitter users to post the same message on their accounts.

b) De-anonymization attacks:

In this kind of attack, what attackers think to do is they first focus on the group of the social network where the victim share their similar interests like same school, work or some place. So, attacker's first focus on the group then it becomes easy to access the individual user. Attackers use the method to steal the URL's of the victims that they had visited in the past. This method is known as history-stealing method. To know about this technique first we must know about the concepts of social network link and history stealing need to be described.

Two types of links are there in social network links i.e., static and dynamic link. Static link is used to display the user's home section and it is same for all social network users. Whereas dynamic link represents for each user or a group has some unique information. For example:

http:// www.facebook.com/groups/gropuID

In history stealing, first attackers attract the users to visit their web pages by sending URLs in a social network group. Then it is easy to attackers to check whether the victim visited the URL or not by looking at the browsing history of the victims. Here the browsing history can be seen by the attackers in the form conditional logic CSS with an attribute: visited and display using client-side script. So, by using this history-stealing method, attackers can steal the browsing history of the victims and find the direct link to victim’s timeline.

c) Face recognition

The main target of this attack is profile pictures uploaded on online social networks. The attackers make use of those pictures to create a biometric database. These photos can be easily obtained from online social networks because most of the profile pictures uploaded are set to privacy as public which can be easily viewed and downloaded. The threat behind the face recognition is, the attackers matches the face images with the other websites which are bonded with more sensitive information like bank details, social security number and lot of other sensitive information which is not supposed to share with the other people.

d) Fake profiles

Fake profiles are nothing but copies of original user’s profile. They create a duplicate profile with information available of the original user and send requests to the user friends and sometimes to the people who always accepts every friend request. The reason for creation of these Fake profile is to access information which can only done by being as friend of the user on the online social networks. The stealing of information of user’s friends is not only aim of fake profile. The attackers post spam messages, cheat the people by asking money and lot illegal activities are done on behalf of user.

e) Identity Clone Attacks

This technique is almost like creating fake profiles. This technique not only targets normal people but also higher officials. It duplicates user’s online presence in same network or any other networks. The attackers make the people who are in contact with the user to build trust with the cloned profile. And later influence the people to follow their commands without having any knowledge to the original user. Once a defense ministry senior commander’s profile was duplicated and the attackers succeeded to collect the data of other officials by making them to become friends newly created duplicate Facebook profile.

f) Inference attacks

This is powerful attack which can predict the user’s personal information even the user not chose to share that information. These attacks are implemented by performing data mining techniques on the publicly available data. Through this attack most of the confidential information of a user is revealed. The attackers mainly target organizations rather than individual user using these attacks.

g) Information leakage

In this attack, the attackers make use of openly shared information and communication by the user with his/her friends or other users over the network. Sometimes, the users share confidential information like health information, sobriety status, financial information though chatting or any other communication openly. This information is collected by the attackers and sold to insurance companies, employment providing companies to keep track of their customers or employees.

h) Location leakage:

Now-a-days the smart mobile devices are playing an important role in human life. The people are becoming enthusiastic to share their location status when travel on vacation. But these mobile devices not only share the user’s location status when the user wants, it keeps track of the user all the time and give location updates to network provider all the time. Not only network provider, the applications running on the mobile can also have the access to your location status. For an example, A user tweeted about his vacation on the twitter and left for a vacation. The burglars can make use this information to plan their burglary.

Socware: This attack spreads the harmful messages and software over the internet. The attackers attract the users by offering great rewards and influence them to install harmful software in their systems. After users installed that software, the attackers spread these types of software using the original user’s credentials making the user part of this attack.

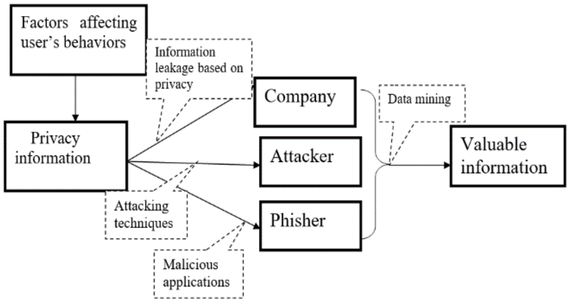

Fig 3: generalized flow of process for security attacks

Combination Threats:

Combination attacks are more sophisticated attacks which are developed by combining both classic and modern threats. For example, a phishing attack collects account information and password of Facebook and update a status on the user's timeline with a spam message hidden inside a mask of an attractive message which is a part of modern attack called Clickjacking.

These attacks are considered as sophisticated attacks because both classic and modern attacks have different recovery processes. In case of classic attacks, the user can be recovered by rebooting the computer or installing a good antivirus. But in case of modern attacks, it is difficult to reset the identity, this is because changing an email id is easy but it is not that easy to change home address.

Threats Targeting children:

There are some threats that target children and teenagers. Now the children are having great knowledge in using the computers, but not aware of these threats. So, there is need for parents to educate their children about these attacks.

a) Online predators

Here, the adults influence the children to harmful activities like pornography, sexual exploitation, for collecting personal information of parents. The attackers pretend to be friends with innocent children and builds trust in children by hiding his actual identity until first meeting. This meeting may lead to rape or kidnap. Otherwise, they can also use children for porn distribution, Internet sexual exploitation, consumption of child porn. Fortunately, most of children now are aware these types of frauds but still every parent should keep track of child's activities.

b) Risky Behaviors:

The activities like chatting with strangers, sharing personal information with unknown friends, explicit talk about sex to strangers, sending private photos and videos to strangers are considered as risky behaviors. These behaviors alone itself can cause damage, the combination will lead uncoverable damage.

c) Cyberbullying

Cyberbullying makes technological communication as a medium such as chat rooms, phones, emails, etc. The attacker harasses the victim by sending embarrassing messages or pictures, videos, sexual content. It also involves posting the victim's personal information or photos on the internet with or without knowledge of victim. The children and teenagers are more effected than adults.

Security and privacy in Mobile Social Networks (MSNs)

There are two models in Mobile Social Networks, one is called peer-to-peer mobile social networks and another one is client-server mobile social networks. The peer-to-peer MSNs model is cost effective method which do not require a centralized Networking system. These applications make use of technologies like Bluetooth or Wi-Fi to establish communication between two or more people. The users can directly communicate with their trusted buddies to share data or to exchange information. When coming to client-server applications, middleman involves in handling the data and information shared between the users. This is considered as centralized networking system. The social network application providers or third party application providers shares the content on behalf of the users.

a) Direct Anonymity issues

Here the Information is leaked after taking the permission from the user. In Peer-to Peer model, the attacker can collect Social Network ID of a user by logging with date and time. It is possible when the mobile or device is stationary. Using these logs, the attacker can construct a user's history of locations visited which lead to compromised privacy. And the other issue is, when exchanging of Network IDs is done in cleartext somebody can snoop the data when connected to your wireless connection.

Client-Server mobile social networks also have Direct Anonymity issues. Here the Network IDs are not directly exchanged between the users, still the devices participated in this communication can track the Social Network usernames and full names of the users which lead to compromised privacy again.

b) Eavesdropping

This is a technique of stealing or listening of confidential information without the knowledge of users. When comes to network security, this attack is done on Network layer which collects small packets of data from other computers. This has great success rate because the encryption services in this layer are not that effective when compared to other layers.

c) Spoofing Attacks

This is a technique which is not only responsible for stealing data but also responsible for gaining privileged access control over the user accounts by pretending as original user. This includes injecting a malicious code into the compromised Social Networking Mobile applications.

d) Replay Attacks

This attack involves snooping data from original communication and later fakes the authentication which took place at time of original communication. The attacker pretends as original user and requests another user for personal information, any other information which is not supposed to be revealed publicly.

Security Mechanisms for Social Networks

Threat prevention mechanisms are listed below. They are categorized as Operator solutions and Commercial Solutions.

Operator Solutions

a) Authentication Mechanism.

This mechanism confirms that the person who tries to logging into the system is the authorized person or not a socialbot. Some social networks use authentication mechanisms such as CAPTCHA, security question, multi-factor authentication and some other sites will ask for their government issued ID to confirm that he/she the real user. For Example, GMAIL has the Multi Authentication system which means after entering the credentials also GMAIL team will send a code to the users mobile to recheck the account owner is real or not. By Introducing such mechanisms, it can prevent fake users to enter into others account and get their account hacked.

b) Security and Privacy settings.

Some social web sites provide security and privacy settings which are helpful for the user to hide the data form other unwanted users. For example, Facebook provide these settings in which a user can make a post and he can set it as that post can be viewed by friend or friends of friends or everyone in such a way most of the social networking sites provide them but most of the users keep these settings in default mode.

c) Internal Protection Mechanism

To protect the user form spammers, fake profiles and some others threats social network sites constructs some defensive mechanism called internal protection mechanism.

Commercial Solutions

a) FB Phishing Protector

This an Add-on for the Firefox which send the warning message for the FB user that skeptical activity is found. This provides security against all kinds for phishing attacks.

b) Norton Safe Web

Norton Safe Web is a popular application which is having more than 600,000 users, if we install that in our system and add it as an add-on to all the browsers that we are using it immediately pop-up when our system is under any suspicious attack and say some unwanted data tries to enter your system do you want to continue or not.

c) Minor Monitor

This is introduced by Infoglide's. This is a kind of parental control web service in which parents can take a quick view on their child activities over the social web sites.

Cryptography techniques used in social network security.

a) IBC for Bilinear Pairings:

Identity-based cryptography permits the public key to get the public identity information like name, email etc. Two popular scientists named Boneh and Franklin first invented Id-based encryption scheme, in that they take G_1 and G_2 be the additive and multiplicative groups having the same prime order q. they applied discrete logarithm problem for G_1 and G_2. Let P is a random generator for G_1 and is constructed with the following properties

1. Bilinear: e(aP, bQ) =$e(aP, bQ) = e(P,Q)^{ab}$, $\forall\, P, Q \in G_1 \; and \; \forall a, b \in Z_q^*$

2. Non-degenerate: ∃P, Q ∈G_1 such that e$(P, Q) \neq 1$
3. It can be computed that e(P, Q), $\forall P, Q \in G_1$

b) Broadcast Encryption

Broadcast encryption allows the transmitter to send the encrypted data to all the users and only the privileged set of users can decrypt the data. For example, highly secured telephone calls, emails, TV broadcastings and some internet applications uses high broadcasting encryptions such as windows EFS. It restricts file sharing, mailing and some applications from sending confidential data. This follows an algorithm which is given below (SETUP, BROADCAST, DECRYPT) here

- SETUP: takes the public key of a user let k where k ∊ S, here S is the set of all users and constructs users secret Γ_k;
- BROADCAST takes the set of revoked users let be R and the decryption key Y, and gives the broadcast cipher text C;
- DECRYPT: it is executed by user k ∊ S and compute decryption key Y which is encrypted in ciphertext C, if k ∊ R` here R` denotes the set of non-revoked users, finally if k ∊ R DECRYPT fails.

c) Searchable Public-key Encryption

It simply allows all email servers to tell whether the requested keyword is present in emails or not. At the same time, it makes sure the receiver doesn't gain any excess knowledge about the encrypted emails. Data which is encrypted by using receivers public key is stored in the remote server by the sender which is decrypted and used by the receiver. In this mechanism receiver generates the trapdoors and send them to the server then server look on the encrypted data which is transmitted by the user and only returns data containing set of keywords to the receiver. In this mechanism, all the encryption and decryption in PEKS will be performed by some other parties, where the public-key encryption is monitored.

Conclusion

Security and Privacy play an important role in the stream of Network security. The most trending area where an advanced security techniques should be implemented is Social Networking. The most of internet traffic is due to Social Networking as there are huge number of users. So, Social Networking Sites became a platform for information leakage and most of the public is targeted by the attackers through these sites.

In this Survey, we first discussed what is Social Networking and how Social Networking is categorized. Secondly, we detailed about various threats effecting the users of social Networking. After Threats, we have summarized the solution mechanisms involved in providing protection against threats.

Coming to future scope, there is always a need for improved techniques to handle increasing threats in the field of Social Networking. More specifically, the researches should be done to deal with cloning and fake online social networks.

References

1) Jinyuan Sun, Xiaoyan Zhu, and Yuguang Fang. A Privacy-Preserving Scheme for Online Social Networks with Efficient Revocation. IEEE Infocom 2010
2) Michael Fire, Roy Goldschmidt and yuval Elovici. Online Social Networks: Threats and Solutions. 2014.
3) Racha Ajami, Nabeel Al Qirim, Noha Ramadan. Privacy Issues in Mobile Social Networks. 9th International Conference on Mobile Web Information Systems. ELSEVIER 2012.
4) Social Networks- Problems of Security and Data Privacy. Les Fraser 2008. http://www.cepis.org/files/cepis/20090901104125_CEPIS%20social%20network%20Backgroun.pdf
5) Ed Novak, Qun Li. A Survey Of Security and Privacy in Online Social Networks.
6) David Hiatt, Young B Choi. Role Of Security in Social Networking. International Journal of Advanced Computer Science and Applications Vol 7, 2016.
7) Wikipedia. Role-Based Access Control. https://en.wikipedia.org/wiki/Role-based_access_control May 2012.
8) Aaron Beach, Mike Gartell, and Richard Han. Solutions to Security and Privacy Issues in Mobile Social Networking. December 2009.
9) Pritam Gundecha, Geoffrey Barbier, Huan Liu.Exploiting Vulnerability to Secure User Privacy on a Social Networking Site.
10) R. Baden, A. Bender, N. Spring, B. Bhattacharjee, and D. Starin, "Persons: an online social network with user-defined privacy," Proc.ACM SIGCOMM, August-2009.
11) L. A. Cutillo and R. Molva, "Safe book: a privacy-preserving online social network leveraging on real-life trust," IEE Communications Magazine, Vol. 47, no 12, pp.94-101, Dec. 2009.
12) H. Yu, P. B. Gibbons, M. Kamakshi and F. Xiao, "Sybillimit: a near optimal social network defense against sybil attacks," in proc. IEEE Symposium on security and privacy oct-2008.
13) Y. C. Chang and M. Mitzenmacher, "Privacy preserving keyword searches on remote encrypted data, " in applied cryptography and networks security conference, 2005.
14) J. Sun and Y. Fang, "defense against misbehavior in anonymous vehicular ad-hoc networks, " ad-hoc networks, vol-7 nov-2009.

15) F. Hess, efficient identity –based signature schemes based on pairings, SAC-2002, LNCS2595, Spinger-verlag, 2002.

16) Z. Yang, S. Zong, and R. Wright Privacy-Preserving queries on Encrypted Data, In 11th edition Symposium on Research in Security, 2006.

17) David Sancho Senior Threat Researcher "Security Guide to Social Networks" https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp_security_guide_to_social_networks.pdf.

18) A. Beach, M. Gartrell, S. Akkala, J. Elston, J. Kelley, K. Nishimoto, B. Ray, S. Razgulin, K. Sundaresan, B. Surendar, M. Terada, and R. Han, "Whozthat? evolving an ecosystem for context-aware mobile social networks," IEEE Network, vol. 22, no. 4, pp. 50–55, July-August 2008.

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

20) A. Mislove, M. Marcon, K. P. Gummadi, P. Druschel, and B. Bhattacharjee,"Measurement and analysis of online social networks," in Proceedings of the 5th ACM/USENIX Internet Measurement Conference (IMC'07), October 2007.

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

22) Racha Ajami, Noha Ramadan, Nader Mohammed, Jammela Al-Jaroodi,"Security Challenges and Approaches in Outline Social Networks: A Survey," Vol. 11, No.8, August 2011.