Online Social Network - A Threat to Privacy and Security of Human Society

P.Krubhala, P.Niranjana, G.Sindhu Priya

Department of Computer Science and Engineering, NSCET name of organization, acronyms acceptable, Theni, India

Abstract- With over 1 billion users connected through online social media, user confidentiality is becoming even more important and is widely argue in the media and researched in academia. Social networking sites are a powerful and fun way to communicate with the world. The Internet is the safe place for only those people who aware of the risk and the security, and can take steps to protect themselves, so the best solution is to learn. Social media is a good service because it lets you to share what actually you want to share, but it can also be used for negative purposes, and in both cases you are responsible for your security. Protection and preventative techniques are not very difficult, but you need to be careful while you are on the Internet. In this paper we provide a brief overview of some attire to users' privacy. We classify these threats as: users' block, design pitfall and limitations, implicit flows of information, and clash of stimulus. We also describe about the privacy and security issues associated with social network systems.

Index Terms- Social networks, Privacy

I. INTRODUCTION

The level of human connectivity has reached extraordinary levels with over1 billion people using one or more online social networks including Facebook, Twitter, YouTube, and GoogleC. The enormous amount of data provided and shared on these social networks may include the following information about a user: personal details, current address, hometown, email addresses, instant messenger usernames, activities, interests, favorite sports, favorite teams, favorite athletes, favorite music, television shows, games, languages, his religious views, political views, inspirations, favorite quotations, service users history, education history, relationship status, family members, and software applications. The user also provides revise in the form of status information or Tweets, which could include: a thought, an act, a link they want to contribute a video. All these information confess a lot about the user, which will be of interest to various groups.

Social networks, due to many such unfavorable incidents, have been blame for breaching the privacy of their users. Both in academia and in the media, the importance of a user's confidentiality has been rarely discussed. In addition to some proposed technical solutions, there have been a huge number of initiatives to educate users so that they do not provide an excessive amount of personal information

Furthermore, social network information is now being correlated with users' physical locations, allowing information about users' preferences and social relationships to interact in real-time with their physical environment. This fusion of online social networks with real-world mobile computing has created a fast growing set of applications that have unique requirements and unique implications that are not yet fully understood. LAMSN systems such as WhozThat [1] and Serendipity [2] provide the infrastructure to leverage social networking context within a local physical proximity using mobile smart phones. However, such systems pay little heed to the security and privacy concerns associated with revealing one's personal social networking preferences and friendship information to the ubiquitous computing environment.

II. SUMMARY OF OUR WORK IN THIS PAPER

We present significant security and privacy problems that are present in most existing mobile social network systems. Because these systems have not been designed with security and privacy in mind, these issues are unsurprising. The contributions we make in this paper are the following

1. First thing is regarding the impact of social networks in today's world.
2. The next section deals with the privacy problem affiliated with the online social networking along with their security associated complication.
3. And finally we scrutinize the design flaws and limitations of a social networking systems.

III. IMPACT ON SOCIAL NETWORK

The growth of social networks has exploded over the last year. In particular, usage of Facebook has spread internationally and to users of a wide age range. According to Facebook.com's statistics page, the site has over 200 million active users [3] [4], of which over 100 million log on everyday. To compare this with Com Score's global Internet usage statistics [5], this would imply that nearly 1 in 10 of all Internet users log on to Facebook everyday and that the active Facebook Internet population is larger than any single country's Internet population (China is the largest with 179.7 million Internet users [5]). Mobile users in particular are active Facebook users. According to Facebook statistics (March 2009) there are currently over 30 million active mobile users of Facebook, and those users are almost 50% more active on Facebook than non-mobile users.

The increasing sophistication of information technology with its capacity to collect, analyse and disseminate information is posing significant threats to social networks users privacy. It is now common wisdom that the power, capacity and speed of information technology are accelerating rapidly. The extent of

privacy invasion or certainly the potential to invade privacy increases correspondingly.[6] Many social networks can be broken up into many categories and most networks fall into more than one category [6]. The present paper is outlining the 3 most daily used social networking sites giving examples and characteristics in order to understand the spectrum of the issue with social network privacy.Every minute of the day:

1.100,000 tweets are sent
2. 684,478 pieces of content are shared on Facebook
3.2 million search queries are made on Google
4.48 hours of video are uploaded to YouTube
5. 47,000 apps are downloaded from the App Store
6.3,600 photos are shared on Instagram
7.571 websites are created

A Types of social network sites

Lets have a brief introduction about the types of social networking sites.

1) Social Networking Sites

Facebook, Twitter, LinkedIn, Google+, MySpace

Micro- blogging is similar to blogs, it is a micro journal of what is happening right now, people share what is going on in their individual life or information individual wants to share.[7]. In general terms these sites allow users to add friends, send messages and share content.

2. Social Media Sharing Sites

Photo sharing Instagram, Flickr, Photobucket, Picasa and Youtube, Vimeo, SoundCloud, MySpace and etc.

These social networking sites allow users to easily share video and photography content online. Photo sharing sites allow people to upload photos to share either privately with only selected other users or publicly. Creative commons licensing rights can grant permissions for others to use the photos by simply embedding the codes in their blogs [7].

3. Location Based Networks

Foursquare, Gowalla, Loopt

Typically entered via smart phones, these applications rather than social networking sites feature check- in capabilities so that users can, if they choose, share their location with their social connections.

Figure 1: Social media types representation

IV. PRIVACY

On the Internet, privacy, a major concern of users, can be divided into these concerns: What personal information can be shared with whom Whether messages can be exchanged without anyone else seeing them Whether and how one can send messages anonymously Personal Information Privacy Most Web users want to understand that personal information they share will not be shared with anyone else without their permission.

Information privacy, or data privacy (or data protection), is the relationship between collection and dissemination of data, technology, the public expectation of privacy, and the legal and political issues surrounding them. Privacy concerns exist wherever personally identifiable information or other sensitive information is collected and stored – in digital form or otherwise. Improper or non-existent disclosure control can be the root cause for privacy issues.

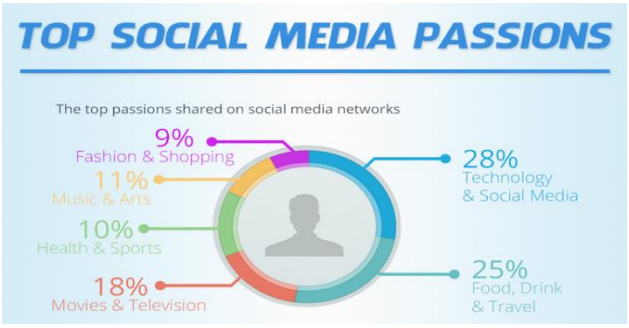

Figure 2: Information shared in social media

A. Definitions of Privacy

There is no one recognized definition of confidentiality in academia or in government circles.Over the course of time several definitions have been gone in to. In this field we look into some of those definitions. One of the first definitions of confidentiality, by Aristotle, makes a distinction between political activity as public and family as private [7].Implied here are barrier that might be suggested by the walls of a family house, an assumption which is made explicit, though also modified, in a far more recent definition, that of Associate Justice John Paul Steven of the US Supreme Court. Here, the home is not the exclusive locus of privacy, but is, rather, the informing image or design in light of which privacy in other contexts may be interpret. This is an interesting definition. The Internet has managed to dim the boundaries that would have been suggested by the walls of a house.

However, privacy on the Internet is a more complex affair than physical metaphors of intrusion and exposure can capture alone. Defense against publication of private information can protect the exposure of that information, but what if it is used, rather to produce targeted advertisements, with no publication. William Parent provides a definition of privacy which does not rest on an implicit physical dimension, as follows [7]:Privacy is the condition of not having undocumented personal knowledge about one possessed by others. A person's privacy is subside exactly to the degree that others possess this kind of knowledge about him.

This definition rests on the notion of "informed consent" as defined by Aristotle [7]. If there is any information about other need a documentary evidence. An idea of privacy breach understood in these terms thus remains very valid in the era of cloud computing. Samuel Warren's and Louis Brandies' 1890 paper [9], "The Right to Privacy," in which they refer to Judge Cooley summarizing it as consisting of the right "to be let alone." The current establishment casts this as a right to: Control over information about oneself. It is in this tradition of thought that Alan Westin defined privacy as an individual right, held by all people, [29]:To control, edit, manage, and delete information about them[selves] and decide when, how, and to what extent information is communicated to others.

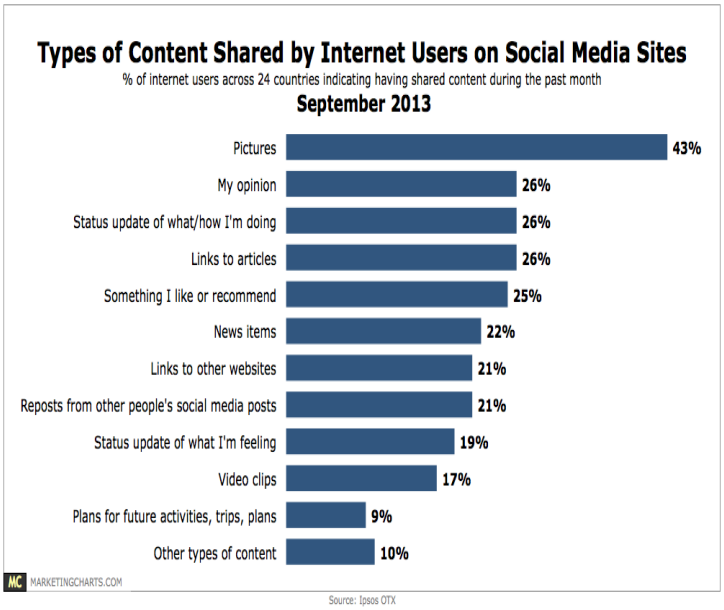

Figure 3: Privacy data in social media

A. Types of Privacy issues

1. Privacy concerns regarding Social Media Sharing Services

Social media sharing services are services, which allow its users to generate and share different types of content. Youtube and Vimeo are an example for sharing service for video and audio, Instagram and flicker are the ones for sharing photos and there are many more. However the aim of this paper is not to go in depth into what kind of different sharing service providers, platforms, apps and etc. there are on the market but to discuss about the privacy issues that arise with sharing different kinds of content on these networks.

Posting Content such as picture and video arise new privacy concerns due to their context revealing details about the physical and social context of the subject. Ahern, Eckles et al. (2007: 357) analysing the issue and conducting studies on Privacy Patterns and Considerations in online and mobile photo sharing claim: The growing amount of online personal content exposes users to a new set of privacy concerns. Digital cameras, and lately, a new class of camera phone applications that can upload photos or video content directly to the web, make publishing of personal content increasingly easy. Privacy concerns are especially acute in the case of multimedia collections, as they could reveal much of the user's personal and social environment.[9]

Commonly users do not think or are not even aware of the risks when they share something online. Based on Das and Sahoo (2011) survey often the decision about sharing something is "made on the moment", however in todays networked world, the next day the content you have shared is accessible to parents, teachers, employers, Aware and Obama (2009) state: Far too many users believe that their postings on the Internet are private between them and the recipient. The reality, however, is that once the statement is typed, it can be copied, saved and forwarded. In addition, the user no longer owns all the information posted to social networks. "So if you're using Gmail or Yahoo mail or Flickr or. YouTube or belong to Facebook you've given up complete control of your personal information' [11]

Video and photo sharing services can pose a great threat especially for teenagers and youngsters, due to their vulnerability. Although. However it is important to mention that there has been a number of cases when youngsters have been harassed by paedophiles online and these cases have also led to suicide

2. *Privacy concerns regarding Social networking services*

The following chapter looks into the privacy issues of social networking services. Social Networking sites as mentioned earlier are the sites aimed for micro-blogging, to document about ones life, his/hers likings and dislikings and everyday happenings.

Susan B. Barnes a Professor in the Department of Communication at the Rochester Institute of Technology in New York claims that in America, people live in a paradoxical world of privacy. As we know people will freely give up personal information to join social networks on the Internet and social networking tools have almost become indispensable for them. Many people may not be aware of the fact that their privacy has already been jeopardized and they are not taking steps to protect their personal information from being used by others. [14]

Social networking sites (such as Facebook, Orkut) create a central repository of personal information. These archives are persistent and cumulative. Instead of replacing old information with new materials, online journals are archive–oriented compilations of entries that can be searched. While American adults are concerned about how the government and corporations are centrally collecting data about citizens and consumers, teenagers are freely giving up personal and private information in online journals. Adults are concerned about invasion of privacy, while teens freely give up personal information. This occurs because often teens are not aware of the public nature of the Internet. [14]

Facebook has met criticism on a range of issues, including online privacy, child safety and hate speech. The Electronic Frontier Foundation has identified two personal information aggregation techniques called "connections" and "instant personalization" that assure anyone has access even to personal information you may not have intended to be public. [15]There has been many more privacy issues with Facebook

3. *Location based social networks and privacy*

Location based social networks are part of what is called Location based services (LBS).They are made possible by linking Global positioning system (GPS), which track user's location, to the capabilities of the World Wide Web, along with other vital features such as instant messaging. [22]

Location-Based Social Networks (LBSN) derive from LBSs and are often referred to as Geosocial Networking. As reported in Microsoft Research "a LBSN does not only mean adding a location to an existing social network so that people in the social structure can share location-embedded information, but also consists of the new social structure made up of individuals connected by the interdependency derived from their locations in the physical world as well as their location-tagged media content, such as photos, video, and texts" [23].Further, the connection between users goes beyond sharing physical locations but also involve sharing knowledge like common interests, behaviour, and activities. Such pervasive tools represent a challenge to privacy.

LBSN users face the situation that the information they publish on the such platforms could be used to track their unwanted situations like being the victim of stalking.The Privacy advocates fear that Foursquare, along with other geolocation apps Gowalla and Google Latitude, are vulnerable to "data scraping", namely, the sophisticated trawling and monitoring of user activity in an effort to build a rich database of personal information.

Specifically the insurgence of applications designed to function as venues information aggregators can potentially represent a major threat to privacy and LBSN. Another issue related to is known as 'opt-in' vs 'opt-out' default settings. An opt-in scenario refers to having default settings where a platform requires user to join or sign up to specific given service in order to receive the benefits of it. The provider is then granted permission to access the user's data and to offer the service.

4. Sites Convergence

A recent issue related to privacy on today's internet is the that users often have 'profiles' and accounts on different site that due to their different nature a number of information become publicly available that if puzzled together provide a picture of the user in certain cases more private that the user would like to be.

eg-convergence of sites: Subject A is the same as in example 1, subject C is a company like Linkedin. In 2012, LinkedIn announced its acquisition of the start-up Rapportive,[27] which created a browser plug-in taking contact information from social networks such as Twitter and Facebook, and placing them into Google's Gmail.

V. SECURITY

In addition to privacy concerns, social networking sites can be used by cyber criminals to attack you or your devices. Here are some steps to protect yourself:

1. Login: Protect your social networking account with a strong password and do not share this password with anyone or re-use it for other sites. In addition, some social networking sites support stronger authentication, such as two-step verification. Enable stronger authentication methods whenever possible.

2. Encryption: Many social networking sites allow you to use encryption called HTTPS to secure your connection to the site. Some sites like Twitter and Google+ have this enabled by default, while other sites require you to manually enabled HTTPS via account settings. Whenever possible use HTTPS.

3. Email: Be suspicious of emails that claim to come from a social networking site; these can easily be spoofed attacks sent by cyber criminals. The safest way to reply to such messages is to log in to the website directly, perhaps from a saved bookmark, and check any messages or notifications using the website.

4. Malicious Links/Scams: Be cautious of suspicious links or potential scams posted on social networking sites. Cyber criminals can post malicious links and if you click on them, they take you to websites that attempt to infect your computer. In addition, just because a message is posted by a friend does not mean it is from them, as their account may have been compromised.

5. Apps: Some social networking sites give you the ability to add or install third-party applications, such as games. Keep in mind there is little or no quality control or review of these applications; they may have full access to your account and private information.

A. Design Flaws and Limitations

1.Productivity

One reason why organizations on social networking within the geographical point is that the incontrovertible fact that workers pay a good deal of your time change their profiles and sites throughout the day. If each worker in an exceedingly 50-strong men spent half-hour on a social networking website daily, that might compute to a loss of half-dozen,500 hours of productivity in one year! though this could be a generalization, organizations look terribly rigorously at productivity problems, and twenty five hours of non-productive work per day doesn't think again well with management. once you consider the common wage per hour you get a much better (and decisive) image. There is additionally a control on company morale. workers don't appreciate colleagues outlay hours on social networking sites (and others) whereas they're functioning to hide the work. The impact is additional pronounced if no action is taken against the abusers.

2.Resources

Although updates from sites like Facebook or LinkedIn might not take up immense amounts of information measure, the provision of (bandwidth-hungry) video links denote on these sites creates issues for IT directors. there's a price to web browsing, particularly once high levels of information measure area unit needed.

3.Viruses and Malware

This threat is usually unnoticed by organizations. Hackers area unit drawn to social networking sites as a result of they see the potential to commit fraud and launch spam and malware attacks. There area unit quite fifty,000 applications on the market for Facebook (according to the company) and whereas FaceBook could create each effort to supply protection against malware, these third-party applications might not all be safe. Some have the potential to be accustomed infect computers with malicious

code, that successively may be accustomed collect knowledge from that user's website. Electronic messaging on social networking sites is additionally a priority, and therefore the Koobface worm is simply one example of however messages area unit accustomed unfold malicious code and worms.

4.Social Engineering

Social engineering is changing into a creation and additional and additional individuals area unit falling victim to on-line scams that appear real. this will lead to knowledge or fraud. Users is also convinced to administer personal details like social insurance numbers, employment details and then on. By assembling such info, knowledge larceny becomes a significant risk. On the opposite hand, individuals have a habit of posting details in their social networking profiles. whereas they might ne'er disclose bound info once meeting somebody for the primary time, they see nothing wrong with posting it on-line for all to envision on their profile, personal web log or different social networking website account. This knowledge will usually be well-mined by cyber criminals.

5.Reputation and Legal Liability

At then time of authorship, there are no major company lawsuits involving proof from social networking sites. as an example, one young worker wrote on her profile that her job was boring and shortly received her walking orders from her boss. What if a dissatisfied worker set to complain a couple of product or the company's inefficiencies in his or her profile? There are serious legal consequences if workers use these sites and click on on links to look at objectionable, illicit or offensive content. AN leader might be command to blame for failing to shield workers from viewing such material. The legal prices, fines and harm to the organization's name might be substantial.

6.Fake Accounts and biological research Attacks

Thus, it's terribly simple for Associate in Nursing offender to register accounts in the name of somebody else, though it's prohibited by the privacy policies of most service suppliers. The act of making bogus accounts is additionally referred to as a sybil attack.

An offender will use personal data, e.g. photos and videos of the victim, on the faux profile to win the trust of his friends and allow them to permit the bogus account into their circle of trust. this fashion the offender can have access to the data of the friends of his victim, that his friends have united to share with the victim and not essentially the offender.

The process of making bogus accounts, is named a "cloning attack," when the attacker clones (creates virtually precise copies) of real social network accounts and then adds identical and/or alternative contacts as their victim. Bilge et al. [5] showed the ease of launching an automatic hoax attack against some in style social networks by causation friend requests to friends of many their cloned victims.

7.Crawling

Crawling a social media is fairly a new concept. Most of the social media sites are cropped in the past decade. This is the data most companies wanted product review, brand analysis, and overall brand related items.

Some of the social networking sites like Twitter, Instagram is not that much easy task for in-house data acquisition departments there structures are more complex they have limitation for crawl they amount of data. This kind of work is performed better by using this Prompt Cloud's Social Media Data Acquisition Service – which can take care of your end-to-end requirements and provide you with the desired data in a minimal turnaround time. Most of the popular social networking sites such as Twitter and Facebook let crawlers extract data only through their own API so as to control the amount of information about their users and their activities.

Figure 4: Social media representation

8.Graph Theory

Earlier stage onwards social network idea is based on graph theory. This method is used to identify the number of nodes and there links(for example affluences and the followers).Affluences are called as users they have influence on the activities or opinion of other users by way of followership or influence on decision made by other users on the network.

Graph theory was very much useful for large scale datasets. Centrality measure is used to forms the clusters & cohesiveness among [19] social network. It measure was used to inspect the representation of power and influence that forms clusters and cohesiveness [16] on social network. Centrality metric The authors [34] employed parameterized centrality metric approach to study the network structure and to rank nodes connectivity. Their work formed an extension of a-centrality approach which measures the number of alleviated paths that exist among nodes.

VI. CONCLUSION

Social networking sites have become a potential target for attackers due to the availability of sensitive information, as well as its large user base. Therefore, privacy and security issues in online social networks are increasing. This survey paper addressed different privacy and security issues, as well as the techniques that attackers use to overcome social network security mechanisms, or to take advantage of some flaws in social networking site. Privacy issue is one of the main concerns, since many social network user are not careful about what they expose on their social network space. The second issue is identity theft; attackers make use of social networks account to steal victim's identities. The third is the spam issue. Attackers make use of social networks to increase spam click through rate, which is more effective than the traditional email spam. The forth is the malware issue. Attackers use social networks as a channel to spread malware, since it can spread very fast through connectivity among users. Social networking sites are always

facing new kind of malware. Lastly, physical threats, which are the most harmful issues, were addressed.

REFERENCES

[1] 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.

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

[3] "Facebook statistics," http://www.facebook.com/press/info.php? statistics.

[4] 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.

[5] "Global internet use reaches 1 billion," http://www.comscore.com/press/release.asp?press=2698.

[6] http://social-networks-privacy.wikidot.com/

[7] Privacy: Stanford Encyclopedia of Philosophy, 2002

[8] Samaha, J.: Criminal Justice. Thomson Wadsworth, Belmont, CA (2006)

[9] Warren, S.D., Brandeis, L.D.: The right to privacy. Harv. Law Rev. 4(5), 193–220 (1890)

[10] Chaabane, A., Acs, G., Kaafar, M.: You are what you like! information leakage through users' interests. In: Proc. Annual Network and Distributed System Security Symposium, 2012

[11] Chaum, D.: Untraceable electronic mail, return addresses, and digital pseudonyms. Comm. ACM 24(2), 84–88 (1981)

[12] Chaum, D.: Blind signatures for untraceable payments. In: CRYPTO, pp. 199–203, 1982

[13] Cooper, B.: Italian drugs fugitive jailed after posting pictures of himself with Barack Obama waxwork in London on Facebook. Mail Online February 14, 2012

[14] Dey, R., Tang, C., Ross, K.W., Saxena, N.: Estimating age privacy leakage in online social networks. In: INFOCOM, pp. 2836–2840, 2012

70 S. Mahmood

[15] Dhingra, A.: Where you did sleep last night? . . . thank you, i already know! iSChannel 3(1) (2008)

[16] Donald, A.M., Cranor, L.F.: How technology drives vehicular privacy. J. Law Pol. Inform. Soc. 2, (2006)

[17] Ebersman, D.A.: Facebook Inc., Form S-1 registration statement. United States Securites and Exchange Commission, February 1, 2012

[18] Facebook bug sees Zuckerberg pictures posted online. BBC, December 7, 2011

[19] Facebook Timeline: http://www.facebook.com/about/timeline. Accessed 16 May 2012

[20] Felt, A.: Defacing Facebook: A security case study. 2007

[21] Jagatic, T.N., Johnson, N.A., Jakobsson, M., Menczer, F.: Social phishing. Comm. ACM 50(10), 94–100 (2007)

[22] Lindamood, J., Heatherly, R., Kantarcioglu, M., Thuraisingham, B.M.: Inferring private information using social network data. In: WWW, pp. 1129–1146, 2009

[23] Mackay, W.E.: Triggers and barriers to customizing software. In: CHI, pp. 153–160, 1991

[24] Mahmood, S.: New privacy threats for Facebook and Twitter users. In: IEEE 3PGCIC, 2012

[25] Mahmood, S.: Online social networks: The overt and covert communication channels for terrorists and beyond. In: IEEE HST, 2012

[26] Mahmood, S., Desmedt, Y.: Poster: preliminary analysis of GoogleC's privacy. In: ACM Conference on Computer and Communications Security, pp. 809–812, 2011

[27] Mahmood, S., Desmedt, Y.: Online social networks, a criminals multipurpose toolbox (poster abstract). In: Balzarotti, D., Stolfo, S.J., Cova, M. (eds.) Research in Attacks, Intrusions, and Defenses, vol. 7462 of Lecture Notes in Computer Science, pp. 374–375. Springer, New York

[28] Acquisti, A., Grossklags, J.: Uncertainty, ambiguity and privacy. In: WEIS, 2005

[29] Westin, A., Blom-Cooper, L.: Privacy and Freedom. Bodley Head, London (1970)

AUTHORS

First Author – P.Krubhala, Department of Computer Science and Engineering, NSCET name of organization, acronyms acceptable, Theni, India, Email: krubhala@gmail.com
Second Author – P.Niranjana, Department of Computer Science and Engineering, NSCET name of organization, acronyms acceptable, Theni, India, Email: niranjananscet@gmail.com
Third Author – G.Sindhu Priya, Department of Computer Science and Engineering, NSCET name of organization, acronyms acceptable, Theni, India, Email: sindhugowtham29@gmail.com