IJRRECS/June 2015/Volume-3/Issue-6/4181-4185 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

STRATEGIES FOR TACKLING CONFIDENTIALITY ISSUES IN WEB-BASED SERVICES

B.Manasa[1], P.Swapna[2]

[1]M.Tech Student, Dept of CSE, Malla Reddy Engineering College for Women, Hyderabad, T.S, India

[2]Assistant Professor, Dept of CSE, Malla Reddy Engineering College for Women, Hyderabad, T.S, India

ABSTRACT:

Online social networks describe the social networks that are recognized through web-based services through which people can forward social relationships. A most important feature of social networks is the articulation of a variety of types of relationships among profiles to make easy social communication with others. Privacy does not only include fortification of personal information, which users distribute at their profiles, most probably accessible by their contacts only. The significance of quantifying privacy in social networks is even more significant providing scale of the networks. Researchers from several sub-disciplines in computer science have handled several problems that happen in social networks, and projected a varied range of privacy solutions which include design principles to tackle privacy issues of social networks. The objectives of our work are to put these approaches to privacy in social networks into point of view. Three types of privacy problems were distinguished by researchers in tackling computer science. Surveillance, social privacy, as well as institutional privacy problems finish up being considered as if they were self-regulating happening. Each of these approaches abstract away difficulty of privacy in social networks to spotlight on more solvable questions. Privacy Enhancing Technologies refers to technologies particularly considered to defend citizens' online privacy in the direction of overbearing states. The privacy efforts tackled by privacy enhancing technologies are in numerous ways a reformulation of previous security threats, for instance confidentiality breaches.

Keywords: Online social networks, Privacy, Computer science, Surveillance, Privacy Enhancing Technologies, Social privacy, Institutional privacy.

1. INTRODUCTION:

Social network describes a structure made of individuals or organizations, and ties interactions, as well as connections. Users of online social networks generate their own social spaces and upload several types of personal information. Social networks make easy social interaction by permitting users to establish associations and bond to other users. The most essential features of social networks are the capability to distribute personal data with others in a comparatively privacy-preserving method. Protection of user confidentiality is most important objective for social networks [1]. Privacy does not only include fortification of personal information, which users distribute at their profiles, most probably accessible by their contacts only. All information and actions of user has to be concealed from any other party internal, unless openly disclosed by users themselves. Requiring open revelation directly leads to requirement for access control. Access towards information on a user might only be granted by user directly, and it should be fine grained since profile and each attribute has to be independently controllable [2][3]. Mechanisms of access control are utilized in social networks to facilitate users to manage the distribution of their own data and defend their privacy. Several problems that happen in social networks were controlled and several privacy solutions work outs were made which include design principles to tackle privacy issues of social networks.

2. VARIOUS ISSUES RELATED TO PRIVACY IN SOCIAL NETWORKS:

Online social networks as shown in fig1describe the social networks that are recognized through web-based services through which people can forward social relationships. A most important feature of social networks is the articulation of a variety of types of relationships among profiles to make easy social communication with others. The significance of quantifying privacy in social networks is even more significant providing scale of the networks. Protecting enormous amount of equivalent personal information is an important task. Researchers from several sub-disciplines in

computer science have handled several problems that happen in social networks, and projected a varied range of privacy solutions which include design principles to tackle privacy issues of social networks. The objectives of our work are to put these approaches to privacy in social networks into point of view. Three types of privacy problems were distinguished by researchers in tackling computer science. The initial approach deals with surveillance problem that take place when personal information as well as social interactions of social network users is leveraged by service providers. The second approach deals with problems that come into view through the required renegotiation of boundaries since social interactions get intervened by social networks services known as social privacy. The third approach deal with problems connected to users losing control over the collection of information in social networks identified as "institutional privacy. Each of these approaches abstract away difficulty of privacy in social networks to spotlight on more solvable questions. Surveillance, social privacy, as well as institutional privacy problems finish up being considered as if they were self-regulating happening [4]. Surveillance problems of online social networks are not autonomous of social privacy problems. Social practices in social networks might include consequences for efficiency of intrusive surveillance measures. Research of computer science on institutional privacy learns ways of getting better practices of organizational data management. Research on institutional privacy is associated with regulatory methods to confidentiality.

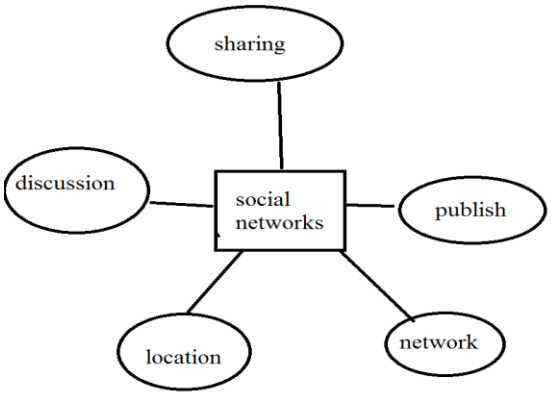

Fig 1: An overview of social networking

3. OVERVIEW TOWARDS PRIVACY IN TACKLING COMPUTER SCIENCE:

Surveillant assemblage is type of surveillance that takes place when a law enforcement as well as intelligence agency globally acts all together with providers of online social networks. Some privacy researchers put forward solutions that counter surveillant assemblages through an additional type of code such as software

itself and is one of the secure points for technical privacy solutions, which known as Privacy Enhancing Technologies. Privacy Enhancing Technologies refers to technologies particularly considered to defend citizens' online privacy in the direction of overbearing states. Social privacy considers the concerns that users pose when technically mediated communications disturb social confines. An imperative body of work tackling social privacy problems in social networks comes from HCI as well as Access Control communities. The intention is to build up design principles that help out individual users in making improved privacy decisions and hence getting better combined seclusion practices. In Access Control, methods from user modelling intend to build up "meaningful" privacy settings that are instinctive to use [5]. Privacy Enhancing Technologies grew out of cryptography as well as research of computer security. The privacy efforts tackled by privacy enhancing technologies are in numerous ways a reformulation of previous security threats, for instance confidentiality breaches. Privacy enhancing technologies facilitates individuals to connect with others, share, access as well as publish information online, which are free from surveillance and interference. PETs intend to improve the capability of a user to distribute as well as access information on social networks by providing her with method to avoid restriction. The prominence of PETs is hence on preventing the revelation of user information, with supposition that controlling how information is used after revelation is not possible [6]. PETs influence cryptography in order that users themselves contain the capability to put off unwanted disclosures rather than relying on provider to implement privacy settings.

4. CONCLUSION:

Social networks make easy social interaction by permitting users to establish associations and bond to other users. The most essential features of social networks are the capability to distribute personal data with others in a comparatively privacy-preserving method. Protecting enormous amount of equivalent personal information is an important task. Researchers from several sub-disciplines in computer science have handled several problems that happen in social networks, and projected a varied range of privacy solutions which include design principles to

tackle privacy issues of social networks. Three types of privacy problems were distinguished by researchers in tackling computer science. Surveillance, social privacy, as well as institutional privacy problems finish up being considered as if they were self-regulating happening. Surveillance problems of online social networks are not autonomous of social privacy problems. Social practices in social networks might include consequences for efficiency of intrusive surveillance measures. Research of computer science on institutional privacy learns ways of getting better practices of organizational data management. Some privacy researchers put forward solutions that counter surveillant assemblages through an additional type of code such as software itself and is one of the secure points for technical privacy solutions, which known as Privacy Enhancing Technologies. Privacy Enhancing Technologies grew out of cryptography as well as research of computer security.

REFERENCES

[1] F. Beato, M. Kohlweiss, and K. Wouters. Scramble! your social network data. In Privacy Enhancing TechnologiesSymposium, PETS 2011, volume 6794 of LNCS, pages 211–225. Springer, 2011.

[2] B. Berendt, O. G¨unther, and S. Spiekermann. Privacy in E-Commerce: Stated Preferences vs. Actual Behavior. Communications of the ACM, 48(4):101–106, 2005.

[3] E. De Cristofaro, C. Soriente, G. Tsudik, and A. Williams. Hummingbird: Privacy at the time of twitter. In IEEE Symposium on Security and Privacy, pages 285–299. IEEE Computer Society, 2012.

[4] James Grimmelmann. Saving facebook. Iowa Law Review, 94:1137– 1206, 2009.

[5] Kevin D. Haggerty and Richard V. Ericson. The Surveillant Assemblage. British Journal of Sociology, 51(4):605 – 622, 2000.

[6] Heather Richter Lipford, Jason Watson, Michael Whitney, Katherine Froiland, and Robert W. Reeder. Visual vs. Compact: A Comparison of Privacy Policy Interfaces. In Proceedings of the 28th international conference on Human factors in computing systems, CHI ’10, pages 1111–1114, New York, NY, USA, 2010. ACM.