ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

Privacy Based Two Tales over Online Social Networks

[1] Shaik Ayesha, [2] Asma, [3] Husna, [4] Dr.Anuradha.S.G
[1] Dept of CSE, RYMEC , [2] Dept of CSE ,RYMEC, [3] Dept of CSE,RYMEC, [4] Asst prof

Abstract: **- Privacy is very important in online social networks as a lot of critical information is being exchanged over the network. So there is a need for security in such applications. Thus this application adds a level of security by using encryption technique (AES-Advanced Encryption Standard) to ensure that the data is not readable over the network and this application also includes privacy settings to specify what should be accessed by whom. The system takes the password while the user registers and encrypts it using AES algorithm and stores in the database. When the user tries to log in into the system, the system fetches the password of the user Id specified and decrypts it using AES and if the password matches, the system allows access to the application. Privacy setting is also provided by the system which specifies which part of the profile should be accessed by who.**

Keywords**: Online social networks, privacy, AES, privacy settings, Social privacy.**

I. INTRODUCTION

Privacy is one of the friction points that emerge when communication get mediate in OSN[2].Privacy has become a primary concern among social network analysis and web or data scientist. OSN are attractive applications which enable a group of users to share data and stay connected. OSN are among the most popular data sharing application and have been soaring in recent years. some well known general OSNs include facebook, twitter that are familiar to many of us.OSN facilitates families and friends to stay connected and maintain their social relations in more convenient way than traditional conversation mails and emails and hence gain numerous popularity among social groups[1]. The impact of data loss to user privacy in OSN. We consider two scenarios the first scenario a social networking privacy settings and has wrong privacy settings in place. The users' information such as age, gender, DOB, mobile number becomes publicly accessible in the internet. In the second scenario a group of user accounts are compromised I a security incident. A malicious user is able to manipulate these compromised user accounts to collect more data from social networks[3].

Motivation:

Our work is motivated by the following observations. As a lot of critical information is been exchanged over online social networks so there is a need for security. In existing system user does not have authority to restrict his friend to view his profile post and comment. The remainder of the paper is organized as follows section II is the review of literature. Section III defines the related work. Section IV describes the system architecture and V section concludes the paper.

II. LITERATURE SURVEY

Title: Two tales of privacy in online social networks

Author: Seda G¨urses and Claudia Diaz KU Leuven ESAT/COSIC, iMinds

Problem: The challenges identified in this paper with integrating surveillance and social privacy are also likely to occur in relation to institutional privacy, given fundamental differences in assumptions and research methods.

Solution: . The article provides a comparative analysis of solutions addressing the surveillance and social privacy problems, and explores how the entanglement of these two types of problems can be addressed in computer science privacy research.

Title: Two Tales of Privacy in Online Social Networking

Author: Rajendra Mane College of Engineering and Technology. Punam P. Sawant, Ankita T. Bobhate, Sneha M. Jadhav, Mangesh K. Gosavi

Problem: This author address the three problems namely surveillance, social privacy & institutional problem.

Solution: To overcome this problems RSA & deffie helmen algorithms are used.

Title: International Journal & Magazine of Engineering, Technology, Management and Research

Author: S.Laxmi Manasa M.Tech. Student, Dept of CSE, Indur Institute of Engineering and Technology, Telangana, India.
M.Komala Assistant Professor, Dept of CSE, Indur Institute of Engineering and Technology, Telangana , India.

Problem: : This author address the three problems namely surveillance, social privacy & institutional problem.
Solution: Our implementation does not manage keys and instead defers to the user at the time of encryption and decryption to enter the password, however, it is possible to modify our plugin to automatically distribute keys to the friends, and receive keys from friends through web based email services. We have manually verified that the encrypted profiles look plausible without revealing significant private information. We are quick to point out, however, that our experience is limited owing to our small user base. A second purpose of our implementation exercise is to study the feasibility of maintaining the dictionaries. We find that the size grows sublinearly reflecting overlapping values across different users.
Title: Two Tales of Privacy on Online Social Network

Author: Amitha Varsha. R1, Jeba Moses. T2

Problem: This paper explains about the privacy in online social network about how to protect the personal information ,sensitive data , photos etc. .from the hackers or the unknown person

Solution: privacy settings. In one solution, users are able to view their effective permissions as they change their privacy settings

Title: Privacy Impact Assessment for Online Social Networks

Author: Yong Wang Raj Kumar Nepali College of Business and Information Systems College of Business and Information Systems Dakota State University Dakota State University Madison

Problem: Two particular challenges are considered in the paper, i.e., when a social network user's partial user information is disclosed and when a group of user accounts are compromised. This paper provides a quantitative analysis approach for government agencies, enterprises, and organizations to assess privacy impact for online social networks when a security incident occurs.

Solution:. In this paper, focus on how disclosed information affects a person's privacy in online social networks. A quantitative analysis approach to assess privacy impact requires measuring privacy.

III. RELATED WORK

Three types of privacy problem has been distinguished that researchers in computer science will tackle the first approach addresses the "surveillance problem" that arises when the personal information and social interactions of OSN users are leveraged by governments and service providers. The second approach addresses problems related to users losing control and oversight over the collection and processing of their information in OSNs, also known as "institutional privacy". The third approach addresses those problems that emerge through the necessary renegotiation of boundaries as social interactions get mediated by OSN services, in short called "social privacy". From the above problems as many people increasingly utilize social networks allow user to publish details about themselves & their lives & alos connect to their friends the information revealed in these networks should remain private & not published at just because you have changed your privacy setting or deleted incriminating photos does not mean your information cant come back to haunt you. These sites does not use secure encryption, meaning there is a chance an your profile and use it against you. From the above problem we have overcome the solution by using two levels of security. By using AES algorithm to provide privacy from unauthorized user. By using domain restriction have privacy setting where user can restrict his/her friends to view his/her contents.

IV. SYSTEM ARCHITECTURE

This architecture defines two levels of security over online social networks first level when user gets login the password is encrypted & stored in the database. To encrypt the password we are using AES algorithm. A database is allowed to manage all the data of the users that get registered or while accessing the data, adding information, retrieving information and performing the operations. The second level of security is domain restriction as shown in figure here we are providing a limitation in domain itself that is while user accepting the friend request he/she can accept that user as a close friend or aquatances or a restricted list which means who can

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

access what by providing checklist this will stored in database.

V. DESIGN & IMPLEMENTATION

Implementation includes AES algorithm and domain restriction which provides a security over social network AES algorithm is the first level of security which uses 256 k bytes of key when user getting register a password is encrypted using AES algorithm and stored in the data base when user tries to login into application if password matches with the encrypted password it allows the user to use the application if the user is unauthorized or password given is not matched with the encrypted user is undefined. If password matches it is decrypted using AES algorithm. When unauthorized user tries to access the key he cannot access as the key is in encrypted form. Domain restriction is another level of security where user itself gives the restriction to his/her friends to view his profile, status, post, comments & views[2][5][6][7][10][11]. Friends either be close acquaintances or restricted list. We are implementing a different functionalities where user can edit his profile & also view his & his friends status and also he can change password and also he can friends to his list by sending request to his friends & also he can view his pending friend's requests.

VI. RESULTS

Fig(1):This figure defines the registration of new user

Fig(2): Login page Which allows the user to access the application

Fig(3):Users Own profile where he/she can edit his profile update his status he/she can view his and his friends status and also can change password.

Fig(4):In this figure we can give a authority to his close , acquaintances or restricted friends to view his status ,post and comments by giving a privacy setting

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

Fig (5):This is how we give a privacy setting to the profile picture , status, contact no, post and comment to view among the close friends, acquaintances and restricted list.

Fig(6): You are here to add a new friend to your friends list

VII. CONCLUSION

In this paper we proposed a two tales of privacy approach for social privacy problem. Two tales of privacy enhances the ability of users to assign their own privacy policies instead of depending on the server of that site. Our project covers some existing features and at the same time provides the many new privacy & security options for the users of social networking sites. Along with categories users are able to communicate by encrypting data to make the communication more secure category based sharing is nothing but attribute based sharing where user can control whom to give access for which type of data. This is new era of data communication that fulfills some security issues.

REFERENCES

[1] Sun, J., Zhu, X., & Fang, Y. (2010, March). A privacy-preserving scheme for online social networks with efficient revocation. In INFOCOM, 2010 Proceedings IEEE (pp. 1-9). IEEE

[2] Gürses, S., & Diaz, C. (2013) Two tales of privacy in online social networks. IEEE Security & Privacy, 11(3), 29-37.

[3] Wang, Y., & Nepali, R. K. (2015, June). Privacy impact assessment for online social networks. In Collaboration Technologies and Systems (CTS), 2015 International Conference on (pp. 370-375). IEEE.

[4] Pensa, R. G., & Di Blasi, G. (2016, August) A centrality-based measure of user privacy in online social networks In Advances in Social Networks Analysis and Mining (ASONAM), 2016 IEEE/ACM International Conference on (pp. 1438-1439). IEEE.

[5] Thakare, P., & Dakhore, H. A Survey on Securing User Data in Social Networks using Privacy Preserving Options.

[6] Kumar, P. P., Srinivas, K., & Kumar, D. N. (2014). A Review on Privacy Preserving in Online Social Network and Its Approaches.

[7] Gunjal, D. V., & Rahane, K. U. A Privacy Based Two Tales Over Online Social networks.

[8] Amitha Varsha. R, Jeba Moses. T. Two Tales of Privacy on Online Social Network.

[9] S.Laxmi Manasa , M.Komala .A Privacy Based Two Tales over Online Social Networks.

[10] Punam P. Sawant, Ankita T. Bobhate, Sneha M Jadhav, Mangesh K. Gosavi Two Tales of Privacy in Online Social Networking.

[11] Prasad, M. S., Kumar, C. S., & Ramya, V. Two Tales Of Privacy in online Social Networks.