ISSN: 2347-6540
International Journal of Latest Research In Engineering and Computing (IJLREC)
Volume 9, Issue 1, Page No. 30-32, 2022
www.ijlrec.com

PEER-TO-PEER CONFIDENTIALITY IN SOCIAL APPLICATIONS

Ankit[1]
MCA student, Uttaranchal University
ankitaleria25@gmail.com

Abhishek Deshwal[2]
MCA student, Uttaranchal University
abhideshwal1999@gmail.com

Abstract- ***Despite the massive success of social networking among its users, social networking tools somehow manage to make it to the news headlines that are concerned with a users private and personal data. Due to this, various applications and networks have come up with decentralized alternatives to ensure the complete safety of a user data, P2P is one such promising alternative that aims to provide confidentiality to the data. Recent P2P developments such as encryption and improved anonymity ensures safeguarding of the data and protects it from any sort of intentional or unintentional exploitation. With the help of encryption, anonymity, fine-grained privacy settings with matching access controls, and encouraging user awareness P2P is capable of yielding the most secure usage experience present till date.***

Keywords: P2P, ***encryption, social networking***

I. INTRODUCTION

It has become a trend to use social networking to connect with the loved ones within a matter of few seconds. With the large number of people joining social media everyday it has become a trend to share pictures, location, wall postings and even audio/video messages. Users possessing minimal technical skills are easily able to access them and are able to share a large amount of personal information with ease. Users sometimes let their guard down while posting their personal information, unaware of the threat it poses as the social networking platforms sometimes suffer from vulnerabilities regarding its privacy.

Facebook & WhatsApp (Meta) are very common and known example of data abuse and misuse. Although they attempt to mitigate the privacy and data of their users yet they still make the headlines. The service provider in turn has access to all of the users data and such information can be misused not only by the provider himself but also through hackers or other malware that might be present in the application.[1] Centralized storage of personal information is known to be a major factor that often leads to unintended disclosure of a user's information and that is why various decentralized alternatives have been proposed. [5] Hence P2P or what is known to be peer-to-peer data encryption plays a crucial role in storing the data as external storage is hardly trusted. [2] These systems have to be efficient in not only protecting the user data but also has to effectively protect the network's privacy against any sort of information leakage involving users behavior or access rights. Michael Rogers et al. (2007) defines P2P as an "Internet overlay in which the resources and infrastructure are provided by the users, and new users may only join the network by personal invitation." Private P2P networks are more feasible over public P2P networks when it comes to confidentiality as they can be bootstrapped. Although network address translators and/or firewalls might create a problem for P2P networks regardless of the network type. [17]

Hence, a P2P network may be defined as a virtual network that has been framed over physical network already in existence. It autonomously interacts and share resources with the help of specialized protocols. General known characteristics for P2P are - Resource sharing, decentralization, scalability, interconnection between peers, self organizing, stability, anonymity and shared cost of ownership. [9]

PRIVACY IN SHARING, NETWORKING AND PERSONAL DATA

Though law enforcement and judicial entities ensure to safeguard the data & traffic on telephone and email, however private companies use their largely drawn database for targeted marketing strategies and several other commercial purposes with the personal information such as the demographics, behavioral preferences and belongings of an individual. For example, cookies along with several other pieces of data might depict personal choices of a potential customer by recording the number of times that person visited a web page. This information altogether is enough to target the customer and possibly generate a lead.

In order to be successful in the long run, the ways in which the personal data of a user is tampered has a large impact on the power structures such as the market who in-turn might tamper with the privacy & rights of the user. In order to counter problems such as intentional or unintentional disclosure of data and its exploitation, recent P2P developments such as encryption and improved anonymity ensure best results for safeguarding of the data. The encryption of P2P traffic helps in safer encryption of data and make the connection streams comparatively harder to detect, therefore making it more difficult to attack or block the

data traffic. Whereas, the P2P network helps in protecting the identity of the users and nodes on any network with the help of anonymizing peers. By using both encryption and anonymity together P2P is capable of yielding the most secure usage experience present till date. [15] [18]. Authenticity, integrity and confidentiality during two way communication is crucial in Online Social Networking. [6][7] Ideally, nodes must be directly able to engage in communication related security without requiring the use of external services from the P2P network.[14] Also, the authentication of any user should purely be based upon his/her knowledge.[10]

REQUIREMENTS FOR P2P BASED ONLINE SOCIAL NETWORKING

Primarily there is the need for a reliable network that is capable of interconnecting all the nodes and can integrate an id management. Along with this a mechanism to store the data with complete reliability is needed that also has a fine-grained access control mechanism.[9][20] Moreover the requirements are discussed further:

1. Id Management - Use of non replicable credentials that can prevent a possible hijack. In order to achieve this cryptographic algorithm to login and decentralized registration should take place. Also the access to an account should not be bounded to one specific device i.e. a user should be able to login from various devices without any hassle.
2. Management of large data sets - Along with the ability to store simple data, the system must provide various structures that are capable of storing large data sets. For eg: comments.
3. Efficient Routing - The overlay chosen for P2P has various factors dependent upon it, the routing protocols are required for communication structures, building further data, along with reliable and authenticated delivery of messages.
4. Security Management - Authenticating the users before providing them access to the network is one such way to manage the security. Suitable replicas and access control management functions should be provided in order to provide the independence to the user to control and individually pick who all can have access to his/her data. Digital signatures also ensure and verify if the data is correct, authenticated and untampered. Finally, end to end encryption secures the communication channels with the help of suitable cryptographic methods.
5. Content availability - The stored content should be consistent even when the user goes offline, [14] this can only be achieved through mechanisms such as storage and data replication.
6. User management - Users are provided unique ids that differentiates them from others. The user ids can be used for login, accessing the data and even during direct communication with peers etc.
7. Relevant communication channels - To send out messages securely and efficiently, the platform must be fast and powerful and it should support different communication strategies like posting, subscribing, following etc. But the platform must also prevent clogging due to heavy user traffic.
8. Graphical User Interface - The GUI should be appealing and must integrate the visualization in a structured manner. [9]

CONCLUSION

P2P-based Online Social Networking has been a result of finding alternative solutions to the shortcomings of the centralized Online Social Networking by providing a decentralized platform. [6][7][10] It is known to be more secure, preserves the privacy of a user and is scalable. The P2P platform has indeed demonstrated that it is capable of meeting all goals through implementation of novel solutions. [19] [20] It ensures reliable communication, security, storage and data availability along with robustness. However the technology is ever changing and evolving very fast and many changes are observed everyday.

REFERENCES

[1] Afify Y (2008) Access control in a peer-to-peer social network. Master's thesis, EPFL, Lausanne, Switzerland
[2] Bachmann, A., Becker, A., Buerckner, D., Hilker, M., Kock, F., Lehmann, M., ... & Funk, B. (2011).
[3] Online peer-to-peer lending-a literature review. Journal of Internet Banking and Commerce, 16(2), 1.Bodriagov, O., & Buchegger, S. (2013). Encryption for peer-to-peer social networks. In Security and Privacy in Social Networks (pp. 47-65). Springer, New York, NY.
[4] Buchegger, S., & Datta, A. (2009, February). A case for P2P infrastructure for social networks- opportunities & challenges. In 2009 Sixth International Conference on Wireless On-Demand Network Systems and Services (pp. 161-168). IEEE.
[5] Buchegger, S., Schiöberg, D., Vu, L. H., & Datta, A. (2009, March). PeerSoN: P2P social networking: early experiences and insights. In Proceedings of the Second ACM EuroSys Workshop on Social Network Systems (pp. 46-52).
[6] Chowdhury, S. R., Roy, A. R., Shaikh, M., & Daudjee, K. (2015). A taxonomy of decentralized online social networks. Peer-to-Peer Networking and Applications, 8(3), 367-383.
[7] Cutillo, L. A., Molva, R., & Önen, M. (2011, June). Safebook: A distributed privacy preserving online social network. In 2011 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (pp. 1-3). IEEE.

[8] Dürr, M., Maier, M., & Dorfmeister, F. (2012, September). Vegas--A Secure and Privacy-Preserving Peer-to-Peer Online Social Network. In 2012 International Conference on Privacy, Security, Risk and Trust and 2012 International Confernece on Social Computing (pp. 868-874). IEEE.
[9] Graffi, K., & Masinde, N. (2021). LibreSocial: A peer-to-peer framework for online social networks. Concurrency and Computation: Practice and Experience, 33(8), e6150.
[10] Jain, I., Gorantla, M. C., & Saxena, A. (2011, December). An anonymous peer-to-peer based online social network. In 2011 Annual IEEE India Conference (pp. 1-5). IEEE.
[11] Krishnan, R., Smith, M. D., & Telang, R. (2003). The economics of peer-to-peer networks. Available at SSRN 504062.
[12] Lee, Y., Lee, K. M., & Lee, S. H. (2020). Blockchain-based reputation management for custom manufacturing service in the peer-to-peer networking environment. Peer-to-Peer Networking and Applications, 13(2), 671-683.
[13] Li, Z., Shen, H., & Sapra, K. (2012). Leveraging social networks to combat collusion in reputation systems for peer-to-peer networks. IEEE Transactions on Computers, 62(9), 1745-1759.
[14] Masinde, N., & Graffi, K. (2020). Peer-to-Peer-Based Social Networks: A Comprehensive Survey. SN Computer Science, 1(5), 1-51.
[15] Masood, S., Shahid, M. A., Sharif, M., & Yasmin, M. (2018). Comparative analysis of peer to peer networks. International Journal of Advanced Networking and Applications, 9(4), 3477-3491.
[16] Musiani, F. (2010). When social links are network links: The dawn of peer-to-peer social networks and its implications for privacy. Observatorio (OBS*), 4(3).
[17] Rogers, M., & Bhatti, S. (2007). How to disappear completely: A survey of private peer-to-peer networks. networks, 13, 14.
[18] Shen, X., Yu, H., Buford, J., & Akon, M. (Eds.). (2010). Handbook of peer-to-peer networking (Vol.34). Springer Science & Business Media.
[19] Steinmetz, R., & Wehrle, K. (Eds.). (2005). Peer-to-peer systems and applications (Vol. 3485). Springer.
[20] Zhang, Y., & Fang, Y. (2007). A fine-grained reputation system for reliable service selection in peer- to-peer networks. IEEE Transactions on Parallel and Distributed Systems, 18(8), 1134-1145.