Peer To Peer Confidentiality in Networking

Brahmi Bora

Computer Science and Engineering, Graphic Era Hill University, Dehradun, Uttarakhand, India

Rahul Chauhan

Computer Science and Engineering, Graphic Era Hill University, Dehradun, Uttarakhand, India

Sagar Giri

Computer Science and Engineering, Graphic Era Hill University, Dehradun, Uttarakhand, India

Ruchira Rawat

Computer Science and Engin eering,Graphic Era Deemed to be University, Dehradun, Uttarakhand, India

ABSTRACT: Peer to peer networking is always with us since the advent of technologies. But, is it safe? is it safe to share sensitive information? These are the biggest question we have to face. so, as we know peer to peer technologies promise networks that are self-organizing and secure by design, in which the final data sovereignty lies at the corresponding user A peer-to-peer network is a distributed computing architecture that divides tasks and workloads between its members. Its members are equally entitled to participate in the network. Also, Digital oblivion is a concept that addresses the issue of user control over their personal content in online social networks. It encapsulates the idea that users should have the agency to determine the fate of their uploaded content, especially in instances involving sensitive or potentially harmful information. This concept arises from the realization that the digital landscape has become a repository of our lives, containing a trove of personal information and experiences. With the proliferation of OSNs, this information is more accessible than ever before, making it imperative for users to have tools to manage their digital footprint effectively. Peer to peer confidentiality in networking is safe but up to a extend because everybody has an antibody. everything has their own assets and liabilities.

Keywords – Peer to Peer, Networking, computer architecture, social networks OSNs, confidentiality

I. INTRODUCTION

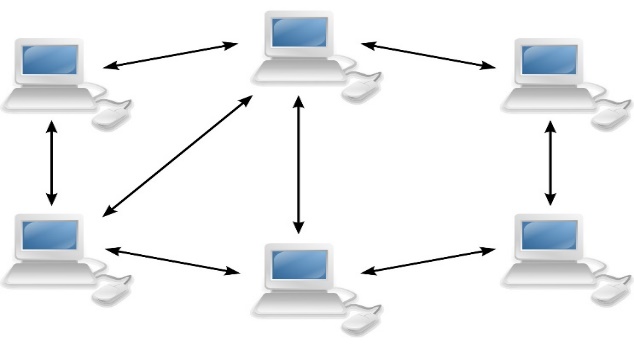


Fig 1. Peer to Peer networking architecture

II. CHARACTERISTIC OF PEER-TO-PEER

Peer-to-peer networks exist in small local areas (LANs), primarily in homes. Both cellular and wireless home networks can be configured as peer-to-peer environments. Computers in a peer-to-peer network use the same network protocol and software. Connected devices are often connected to devices in close proximity in homes, small businesses, and schools. However, some peer-to-peer networks use the Internet and have locations around the world. A home network using broadband routers is a hybrid peer-to-peer and client-server environment. Routers provide a centralized connection to the Internet, but files, printers, and other shared items are managed directly between the respective local computers. Peer-to-Peer and P2P Networks Peer-to-Peer Internet Networks With the development of P2P file-sharing networks such as Napster, peer-to-peer networks became popular. nineties. Technically, many P2P networks are not peer-to-peer networks, but structural models, as they use centralized servers for specific tasks (such as browsing).

III. PEER-TO-PEER AND AD-HOC WI-FI NETWORKS

Wi-Fi (wireless) networks support ad-hoc connections between devices. Unlike networks that use wireless routers as intermediaries, ad-hoc Wi-Fi networks are purely point-to-point networks. Devices that make up a private network do not need to communicate.

IV. ADVANTAGES OF PEER-TO-PEER NETWORKS

P2P networks are very powerful. If the device fails to connect, the network continues. In a client-server network, when one server fails, the entire network crashes. Shared workgroup computers can be configured to share files, printers, and other services across any network. Apparatus. A peer-to-peer network allows information to be shared in both directions, whether it is downloading or uploading from a computer. On the Internet, peer-to-peer networks manage large volumes of data traffic by distributing the load among multiple computers. Because P2P networks are not entirely dependent on a central server, they are more capable and perform better than client-server networks in the event of a failure or outage. Peer-to-peer networks are easy to measure. As the number of devices on the network increases, the performance of the P2P network increases because each additional computer can be used to process data.

V. SECURITY ISSUES

Like user-server networks, peer-to-peer networks are vulnerable to security attacks. Since every device participates in network traffic, it is easy for hackers to initiate a denial of service. P2P software operates as both a server and a client, making peer-to-peer networks more vulnerable to remote attacks than client-server networks. False information can be distributed in a P2P network by changing network information to identify malicious code.

TABLE II. REVIEWS OF PREVIOUS WORK

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **S.No** | **Work** | **Author** | **Review** | **Citations** |
| 1 | A Peer-to-peer Agent Community for digital oblivion in online social networks. | Klara Stokes and Nicklas Carlsson | Working of peer-to-peer networking and installation of digital oblivion in social networks. also, what will the future work on it. | Klara Stokes and Nicklas Carlsson,  Department of Computer and Information Science  University of Link ¨oping  Link ¨oping, Sweden  Email: [name.surname@liu.se](mailto:name.surname@liu.se) |
| 2 | Privacy preserving social networking through decentralization. | Leucio Antonio cutillo, refik molva and Thorsten strufe. | The literature contains knowledge about the concern of people data on online networking. | Leucio Antonio cutillo, refik molva and Thorsten strufe. Institut eurecom, Sophia antipolis France.  Email: {cutillo, molva, [strufe}@eurecom.fr](mailto:strufe%7d@eurecom.fr) |
| 3 | Privacy and security for online social networks: challenges and opportunities. | chi zhang and jinyuan sun, Xiaoyan zhu, yugang fang | Privacy concern on facebook, myspace and twitter type platform, as they raise the online concerns and raise the security concerns. | chi zhang and jinyuan sun, Xiaoyan zhu, yugang fang, university of florida, Xidan umiversity. |

V. HISTORY OF PEER-TO-PEER NETWORKING

Before the development of P2P, USENET appeared in 1979. The network allows users to read and publish messages. Unlike the forums we use today, there is no central server. It is used to copy the new message to all servers of the node.

P2P networks were first used after the advent of personal computers in the 1980s.

In August 1988 Internet Relay Chat emerged as the pioneering peer, to peer network for conversations. Moving forward to June 1999 Napster, a file sharing software utilizing peer to peer technology was introduced. Notably it allowed users to share files among themselves. However Napster faced issues. Eventually had to shut down due, to unauthorized data sharing.

However the concept of network sharing, peer, to peer (P2P) has gained popularity. Back in June 2000 Gnutella emerged as the pioneering distributed P2P file sharing system. It enabled users to retrieve data from designated directories, on users’ computers.

VI. P2P NETWORK TYPES

Unstructured P2P Network-In this type of P2P network every device has an opportunity to contribute. It is relatively simple to establish because devices can connect directly to the network. However the absence of a defined structure makes it challenging to locate content. Examples of networks include Napster and Gnutella.  
Structured P2P Network-This type of P2P network is designed using software that creates an infrastructure, for organizing nodes in a particular structure. While the setup process may not be straightforward it offers users access to content. Prominent examples include P Grid and Kademlia.  
Hybrid P2P Network-A hybrid P2P network combines elements from both P2P networks and client server architectures. One common example is the utilization of a server for node location purposes.

VII. Functioning of P2P Networking

Peer to peer (P2P) networking is a form of computer networking where each participant within the network can function as both a client and a server. This differs from client server models where clients primarily communicate with a server. Within a P2P network every node or peer holds status. Can directly communicate with other nodes without intermediaries. Below is an overview explaining how peer to peer networking operates;

Node Discovery; Nodes within a P2P network must. Establish connections, with one another.

There are ways to achieve this including using a directory distributed hash tables (DHTs) or multicast.

Peer Recognition; Every peer, within the network possesses an identifier. In instances this identifier is granted by a governing body; however in numerous P2P systems it is determined by an inherent characteristic of the node itself such, as its IP address or a cryptographic key.

File Sharing: One of the most widely used examples of peer-to-peer. Networks is file sharing. Direct sharing of peers. Peer-to-peer communication without referring to a centralized server. Examples BitTorrent is one of the examples of P2P file-sharing protocols.

Decentralization: P2P networks are inherently decentralized, this implies that there is no central server guiding communication. This involves all nodes that can either ask or send,providing resources.

Distributed Hash Tables (DHTs): Many P2P networks use

The distribution of data and the routing are done by DHTs. queries. By using DHTs, these are achieved without any additional costs.Decentralized accessing and order of information.

network.

Communication Protocols: Peers communicate with each other using a variety of protocols. These protocols define interoperability, standards and protocols for data exchange.” Examples include file-sharing protocols like BitTorrent and Chord. For DHT-based systems.

Security and Trust: This leads us to security, which is a very important concern. P2P networks. It is important to maintain information integrity by having authenticated communication between nodes. Cryptographic communication to build trust and loyal relationships among employees.

Scalability: They are scalable by design. So ideally the capacity should increase rather than decrease as the number of nodes joining the network increases and improves the overall performance.

Fault tolerance: So most people are familiar with this in the case of P2P networks. Resilient to node failure. When one node fails, the network must continue to function and this failure must not Disrupt the entire operation.

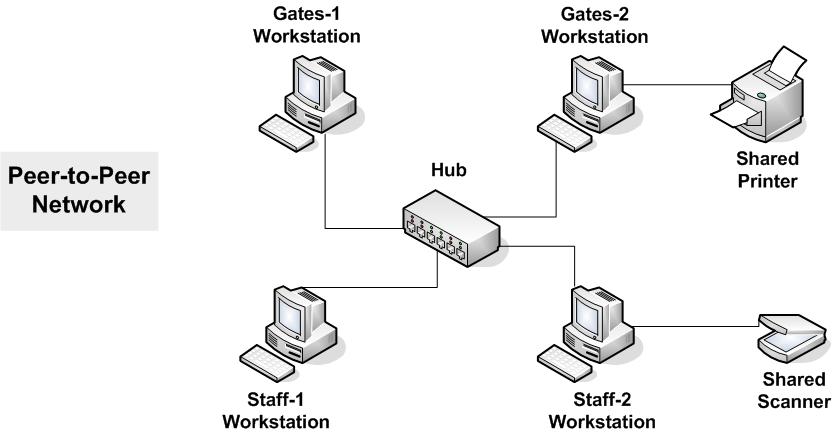


Fig 2: Working of P2P networking

VII. NEED FOR STUDY

I have gone through couple of past research in best of my knowledge there is a gap and scope of improvement in research outcomes:

1. Most of the research are in favour and more improvement on peer-to-peer confidentiality in networking. We should not promote to over sharing of information.
2. As of my analysis, people have three modes:
   * Ignorance: a nature of human to ignore disadvantages of peer-to-peer social networking and taking it lightly.
   * Denial: deny the fact that it is harmful.
   * Panic: when all the things got damage and we caught by the harm then everybody will be got panicked as they are not prepared.
3. According to The Siasat daily: telegram said that: we re most secured when comes to protecting IP addresses during calls /25th oct, 2023.
4. According to Forbes: Absolute privacy in web3 is an illusion. /23th oct 2023.
5. Everything has their own flaws.

VII. SIGNIFICANCEOF P2P CONFIDENTIALITY IN NETWORKING

1. P2P creates a free and shared for everyone to share their feelings, emotions, information as they want, they can talk with each other and discuss it freely that helps them to work of change.
2. P2P (Peer, to Peer) confidentiality in networking is crucial for safeguarding information exchanged between peers in a network. It serves purposes;
3. \*\*Privacy Protection\*\*; P2P networks often involve communication between nodes or peers. Maintaining confidentiality is vital to prevent parties from intercepting the transmitted data. This becomes particularly significant when dealing with messages, financial transactions or sensitive business data.
4. \*\*Security and Trust\*\*; In a P2P network trust among peers is established through their interactions. If confidentiality is compromised it can undermine this trust leading to issues. Users may hesitate to share information if they lack confidence in its privacy.
5. \*\*Legal and Regulatory Compliance\*\*; Various jurisdictions have laws and regulations concerning the handling and transmission of types of data such, as personal information or financial records. Adhering to these regulations ensures compliance. Avoids complications.

Algorithm 1 System start-up

1: (Kpubs Kpriv): Keygen(π)

2: Dealer stores Ida. Kpub

3: Agent A stores Kpric

Algorithm 2 Agent A uploads content F to the OSN

1: Create a perceptual hash H := H (F) of F

2: Use the digital signature algorithm and A's private key to sign the hash, S:= Sign(H. Kpriv)

3: Create a serial number NN(F) for F

4: Use watermark embedding algorithm to embed the signature and the serial number into F. Y:=Embed((N, S).F)

5: Forward the watermarked content Y to the OSN client, who can upload it to the OSN

IV. SYSTEM ANALYSIS

Here we analyze the security and privacy of the following components of the system: (i) the digital oblivion community, (ii) U2C R1 authentication through digital signature and wa- termarking, and (iii) U2C R2 authentication through tags and trust management.

Algorithm 3 Agent A requests for oblivion of content F

1: if agent A originally uploaded F then

2: M := (N(F), @F, IdA), where @F is a link to F

3: else if user U(A) is tagged with tag T T(F, U(A), U(B)) in content F by user with agent B then

4: M:= {H(F), T, I\*d\_{A}, I\*d\_{B}}

5: else if user U(A) receives tag request T\_{R}(F, U(A), U(B)) in content F by user with agent B then T\_{R} :=

6: M:= {H(F), T\_{R}, I\*d\_{A}, I\*d\_{B}}

7: end if

8: Send M to the neighbors of A in the P2P community through limited broadcasting

9: Add M to a list of sent oblivion requests L\_{M}

Algorithm 4 Agent X receives oblivion request M

1: if M={N(F) F, Id\_{A}} then

2: Get content F from link F

3: Get public key Kpub of the agent with identity I\*d\_{A} from the dealer

4:Use algorithm Recover(Y) to recover the embed- ded watermark M containing the signature Z := Sign(H(F), Kpriv)

5: Use algorithm Verify(Z. Kpub) to obtain H(F) from the watermark

6: Obtain the perceptual hash H(F) directly from the F

7: Compare the two versions of perceptual hash to see if the signature is valid

8: if signature is valid then

9: Add N(F) to the list of accepted oblivion requests L\_{0}

10: end if

11: else if M = {H(F), T, I\*d\_{A}, I\*d\_{B}} then

12: if T exists and the combined trust TrustComb (X, A, B) is high enough then

13: Add (H(F), B) to the list of accepted oblivion re- quests L\_{0}

14: end if

15: else if M = {H(F), T\_{R}, I\*d\_{A}, I\*d\_{B}} then

16: if combined trust TrustComb(X, A, B) is high enough then

17: Add (H(F), B) to the list of accepted oblivion re- quests Lo

18: end if

19: end if

Algorithm 5 Oblivion viewing of content F

1: if content is watermarked then

2: if embedded serial number N(F) is among the serial

3: numbers on oblivion list Lo then Instruct the OSN client to forget F

4: end if

5: else if perceptual hash H(F) is among the perceptual hashes on oblivion list Lo then

6: Instruct the OSN client to forget F

7: end if

Algorithm 6 Agent A adds new friend that has agent B

1: for M on A's list of sent oblivion requests LM do

2: Send M to B

3: end for

Algorithm 7 Agent C disapproves the oblivion of content F

1: Broadcast the message (H(F), Idc) to the community

IX. P2P CONFIDENTIALITY IS DANGEROUS

As with all security measures, (P2P) privacy can have flaws or risks if not used correctly. It is important to understand these issues:  
  
Misconfiguration: If P2P security measures are not configured correctly there is a risk of leaving negativity that attackers can use. For example, if the encryption key is not managed properly, this can lead to unauthorized access.  
  
Complexity: Implementing strong P2P privacy can be difficult. It requires a solid understanding of encryption, key management and network security. If done incorrectly, it can cause errors or even cause

distrust.  
  
Overtrust: Relying solely on P2P privacy can lead to a false sense of security. It is important to remember that no system is weak. Other security measures such as firewalls, intrusion detection systems and regular security audits should also be in place.  
  
Key Management: Proper management of encryption keys is important. Confidentiality may be compromised if the key is lost, stolen or tampered with. Adherence to effective management practices is essential.  
  
Performance Impact: There may be a performance impact depending on the encryption level and resources of the participating peers. This will slow down data transfer speed, especially on low-power devices or networks.  
  
User Training: Users must understand the importance of P2P privacy and how to use the systemsecurely. Without proper training, they can compromise security by doing things like sharing keys or using weak passwords.  
  
Compatibility and interoperability: It will be difficult to ensure that different P2P systems and software communicate securely. If not managed properly, it can lead to data integrity and privacy issues.  
  
Trust of Peers: In P2P networks, trust is created by peers. A peer's breach of confidentiality can undermine trust in the network. This may cause disruptions in communication and collaboration.  
  
Despite the potential risks associated with P2P privacy, it is worth noting that it can provide security and speed when used correctly. It is important to plan for security, carefully measure it, and carefully review and update threats to modify them. Additionally, using multiple layers of security, such as encryption, access control, and regular security audits, can help reduce the risks associated with P2P privacy.

X. CONCLUSION

From a close, this research shows on how crucial is peer-to-peer privacy in the internet world. It forms a basis for the security of information sent through nodes in a networked environment. Privacy, trust, and compliance depend on these protections. In addition, this literature review has been focused on providing an overview of what is known about the issue under consideration and improving digital erased memories privacy in social networks. Nonetheless, there still exist some gaps in information and a number of misconceptions with regard to the issue of P2P privacy. Indeed, the possible dangers in P2P’s confidentiality should be clearly addressed, while putting emphasis on good key management practices as well as thorough training of users. Allowing the benefits of open sharing while maintaining the safety for sensitive data required, in order to come up with a safe networking setting. Finally, it must be emphasized that P2P privacy in the network is crucial. As such, it is the foundation on which reliable and fair P2P communication between the different people and organisations in this regard is based on for them to do this with confidence. We need to recognize the possible hazards associated with P2P Networks and come up with the best practices for protecting this type of information.

REFERENCES

1. A Peer-to-Peer Agent Community for Digital Oblivion in Online Social Networks Klara Stokes and Niklas Carlsson

Department of Computer and Information Science

University of Link ¨oping Link ¨oping, Sweden

Email: [name.surname@liu.se](mailto:name.surname@liu.se)

1. man, Au Yeung, C., Liccardi, I., Lu, K., Seneviratne, O., Berners-Lee, T.:

‘Decentralization: the future of online social networking’. Proc. W3C

Workshop on the Future of Social Networking Position Papers,

Barcelona, Spain, January 2009

1. **Manna, S, V Jalodia, K Kumar, V Tripathi, S Sharma, and D Arora, ‘Predicting Preeminent Machine Learning Approach on Stars’, in *Proceedings of International Conference on Technological Advancements in Computational Sciences, ICTACS 2022*, 2022, pp. 587–91.**
2. Raji, F., Miri, A., Devarpana Jazzi, M., Malek, B.: ‘DEFF: a new

architecture for private online social networks’, Special Issue on

Security and Privacy in Ubiquitous Computing, Security and

Communication Networks (SCN), John Wiley & Sons, 2012,

Available at <http://onlinelibrary.wiley.com/doi/10.1002/sec.533/abstract>

1. **Painuly, S, P Kohli, P Matta, and S Sharma, ‘Advance Applications and Future Challenges of 5G IoT’, in *Proceedings of the 3rd International Conference on Intelligent Sustainable Systems, ICISS 2020*, 2020, pp. 1381–84.**
2. Katari, S., Hecker, A.: ‘A peer-to-peer social network overlay for efficient

information retrieval and diffusion’, Commun. Comput. Inf. Sci., 2011,

185, pp. 24–33

1. Trieu, Q.L., Pham, T.-V.: ‘STARS: ad hoc peer-to-peer online social

network’, Lecture Notes in Computer Science, 2012, 7653, pp. 385–394

1. Antonio Cutillo, L., Molva, R., Strufe, T.: ‘Safebook: feasibility of

transitive cooperation for privacy on a decentralized social network’.

Proc. IEEE Int. Symp. a World of Wireless, Mobile and Multimedia Networks and Workshops (WoWMoM), Kos, Greece, June 2009,

pp. 94–101

1. **K. S. Gill, V. Anand, R. Chauhan, S. Thapliyal and R. Gupta, "A Convolutional Neural Network-Based Method for Real- Time Eye State Identification in Driver Drowsiness Detection," 2023 3rd International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON), Bangalore, India, 2023, pp. 1-5, doi: 10.1109/SMARTGENCON60755.2023.10442238.**
2. Graf, K., Gross, c., Stingl, D., Hartung, D., Kovacevic, A., Steinmetz, R.: ‘LifeSocial.KOM: a secure and P2P-based solution for online

social networks’. Proc. IEEE Int. Conf. on Consumer Communications

and Networking (CCNC), Las Vegas, USA, January 2011, pp. 554–558

1. Bodriagov, O., Buchegger, S.: ‘P2P social networks with broadcast encryption protected privacy’. IFIP Summer School on Privacy and

Identity Management for Emerging Internet Applications, Trento,

Italy, September 2011, pp. 197–206

1. Jahid, S., Nilizadeh, S., Mittal, P., Borisov, N., Kapadia, A.: ‘DECENT:A Decentralized Architecture for Enforcing Privacy in Online Social

Networks’. Proc. Int. Workshop on Security and Social Networking,

(SESOC ’12), Lugano, Switzerland, March 2012, pp. 326–332

1. Narendula, R.: ‘The Case of Decentralized Online Social Networks’,Technical Report, School of Computer and Communication Sciences,EPFL, Switzerland, 2012
2. **V. Tanwar, V. Anand, R. Chauhan and D. Rawat, "Improved Brain Tumor Classification Made Possible Through the Use of Transfer Learning Model ResNet50," 2023 3rd International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON), Bangalore, India, 2023, pp. 1-5, doi: 10.1109/SMARTGENCON60755.2023.10442138.**
3. Stoica, I., Morris, R., Karger, D., Kaashoek, F., Balakrishnan, H.:

Chord: a scalable peer-to-peer lookup service for internet applications’, IEEE/ACM Trans. Netw., 2003, 11, (1), pp. 17–32

1. Pouwelse, J.A., Garbacki, P., Wang, J., et al.: ‘TRIBLER: a social-based

peer-to-peer system’, Concurrency Comput.: Pract. Exp. – Recent Adv.

Peer-to-Peer Syst. Secur., 2008, 20, (2), pp. 127–138

1. Greschbach, B., Kreitz, G., Buchegger, S.: ‘The devil is in the metadata -New privacy challenges in Decentralised Online Social Networks’. Proc.

IEEE Int. Conf. on Pervasive Computing and Communications Workshops (PerCom), Lugano, Switzerland, March 2012, pp. 333–339

1. Chor, B., Kushilevitz, E., Goldreich, O., Sudan, M.: ‘Private informationretrieval’, J. ACM (JACM), 1998, 45, (6), pp. 965–981 Tan, S-Y., Heng, S-H., Goi, B-M.: ‘Java implementation for pairing-based cryptosystems’, Lect. Notes Comput. Sci. Comput. Sci. Appl., 2010, 6019, pp. 188–198
2. Mishra, N., Sharma, T.K., Sharma, V., Vimal, V., Secure Framework for Data Security in Cloud Computing (2018) Advances in Intelligent Systems and Computing, 583, pp. 61-71. DOI: 10.1007/978-981-10-5687-1\_6
3. Durgapal, A., Vimal, V.(2021). Prediction of Stock Price Using Statistical and Ensemble learning Models: A Comparative Study. IEEE 8th Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering, UPCON 2021, 2021.