DOI:

Journal of Computers and Intelligent Systems
Vol. 2, No. 2, 2024, pages 73 - 81
Journal Homepage:
https://journals.iub.edu.pk/index.php/JCIS/

File Sharing & Copyright Infringement in Peer-to-Peer

M. Zulkifl Hasan[1], Muhammad Zunnurain Hussain[2], Muhammad Musa[1], Ahmad Mujahid[1], Dr. Muhammad Saifullah [3], Junaid Iqbal Baig[4]

[1]University of Central Punjab, FoIT, Department of Computer Science, Pakistan
[2]Bahria University Lahore, FoIT & Computer Science, Pakistan
[3]Government Sadiq Egerton Graduate College, Bahawalpur, Pakistan
[4]COMSATS University Islamabad, Vehari Campus, Pakistan

ARTICLE INFO

Article History:

Received: May 22, 2024
Revised: May 23, 2024
Accepted: May 23, 2024
Available Online: May 24, 2024

Keywords:

Server-Client
P2P
Copyright Infringement
Domestic Viewpoint
Foreign Viewpoint

Classification Codes:

Funding:

This research received no specific grant from any funding agency in the public or not-for-profit sector.

ABSTRACT

In the past, we used a centralized system which is server-client architecture but today along with server-client peer-to-peer or P2P(Peer to Peer) is widely used which is based on the decentralized system in it each client is also a server purpose of the server for all the different clients as well by analyzing various articles, research papers, and literary works. We investigate many software and technological innovations including Napster, uTorrent, BitTorrent, and Gnutella. Peer-to-peer technology might go either way in the future; perhaps the copyright legislation has made it better or worse. Peer-to-peer has an impact on the music and film industries, among others, since it makes it simple for users to distribute information that is protected by copyright. Additionally, this article considers copyright infringement from both domestic and foreign viewpoints. The article demonstrates the connection between peer-to-peer file sharing and copyright infringement in general as well as the difficulties in safeguarding owners' copyrights on a P2P network. People mistakenly assume that it is impossible to identify and track copyright violations, yet some tools and procedures may be used to identify material that is protected by copyrights.

Corresponding Author's Email:

Citation:

1. Introduction

P2P networks are another name for peer-to-peer networks. The method that digital material is exchanged online is altered by peer-to-peer. The first choice is a client-server architecture, which is a more conventional approach. In this design, clients connect directly to servers, giving them access to all the data they need. A central server manages connections between different clients. In contrast, peer-to-peer networking does not employ any servers and solely depends on direct client connections, with each client acting as a separate server for every other client. [1]. The method is incredibly effective, scalable, and quick. Peer-to-peer file sharing has several unintended

effects, including security risks, the distribution of copyrighted content, serverless communication, and infringement risks. These risks include:

- Security Concerns
- Serverless Transmission
- Copyright Distribution
- Infringement Violations

Peer-to-peer is spread therefore no server or centralized location is required, which also makes it unlikely that there will be a bottleneck or single point of failure [2]. Peer-to-peer use increased significantly in the 1990s and has continued among users because peer-to-peer networks have made it easier for individuals to trade a variety of files [3]. Peer-to-peer technology will become more important as technology advances. The peer-to-peer protocol that is now used most often and by the greatest number of users is BitTorrent [7].

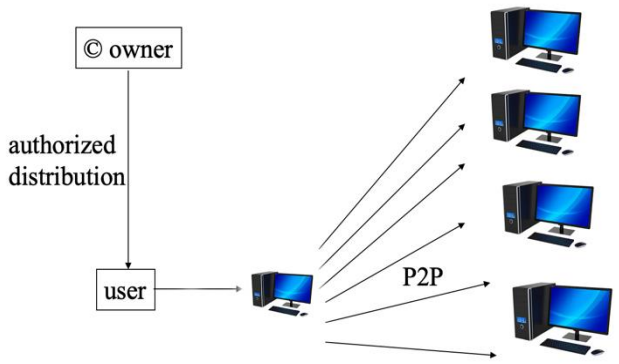

Figure 1: Lifecycle of a Work on P2P

Copyright infringement refers to the unauthorized use, alteration, or dissemination of another person's creative work. As with peer-to-peer, a central server is not present, making copyright infringement simpler as compared previously. [1] Any information that is copyrighted may be freely shared between customers without any effort on either side of the transaction. Since the owner of the material has the right to choose how it is presented to the public, it is forbidden to distribute any information that is protected by copyright. To ensure the safety of their copyrighted information, several individuals and businesses often scan and monitor various peer-to-peer networks As part of this procedure, the IP addresses of the countless users who participate in similar activities [2]. The IDS may be used to locate peer startups, but not enough is known about them for appropriate action to be taken.

Napster was the name of first P2P network use to share files. Napster employs a centralized directory system, in contrast to other file-sharing systems, which allows all clients and peers to connect directly to the same database, where all of the information is published. The procedure of tracking and locating is significantly streamlined by this kind of method [4]. Another decentralized peer-to-peer network system is Gnutella. Since there is no centralized server, clients must query nearby peers or clients for content. Tracking and finding in this program are already somewhat challenging without the central server [5]. When this occurs, downloading is slower since the data is spread over several nodes, which makes it less efficient and drives the development of more efficient programs like Kazaa [7]. Factors that affect P2P data transmission:

- Cyber Attacks
- Copyrighted Data
- Trojans
- Concerns regarding Privacy

Security methods for Data infringement:

- Encryption
- Hashing algorithms
- Licensing of data content
- Registering Patents

A. Novel Contribution:

This article introduces a new framework for identifying and tracking copyright violations in P2P networks, leveraging advanced monitoring tools and algorithms. It also proposes an innovative approach to enhance security and data integrity in P2P file sharing through the implementation of blockchain technology. Furthermore, the study provides comprehensive recommendations for policymakers to mitigate the risks associated with P2P networks.

B. Results and Recommendations:

The analysis of scholarly articles and reports led to the identification of several effective measures for combating copyright infringement and enhancing security in P2P networks. Key findings and recommendations include:

Enhanced DRM and Watermarking: Implementing robust DRM and watermarking techniques has proven to be effective in protecting copyrighted content. It is recommended that content creators and distributors adopt these technologies to safeguard their intellectual property.

Advanced Detection Systems: Utilizing advanced content recognition systems and filtering techniques can significantly improve the detection of copyrighted material being shared illegally. These systems should be continuously updated to adapt to new methods of infringement.

User Awareness Campaigns: Raising awareness among users about the risks of malware and the importance of respecting copyright laws is crucial. Educational campaigns can reduce the incidence of malicious content and promote lawful behavior.

Privacy and Security Measures: Implementing privacy-preserving techniques such as onion routing and reputation systems can help protect user privacy while ensuring network security. These measures should be integrated into P2P protocols to enhance overall safety.

Collaboration with ISPs: Internet Service Providers (ISPs) play a vital role in monitoring and managing P2P traffic. Collaborating with ISPs to block unauthorized sharing of copyrighted material can be an effective strategy. ISPs can leverage their ability to manage internet protocols to prevent infringing activities.

By adopting these recommendations, stakeholders can address the challenges associated with P2P networks more effectively, ensuring a safer and more secure environment for data sharing and copyright protection.

2. Related Work

According to Ashraf, F., & Iqbal [1], several P2P networks serve different P2P technology niches. P2P networks are beneficial for developing some systems for the distribution of digital content to increase performance. P2P technologies have developed far faster than more seasoned ones. This paper seeks to examine and provide a comprehensive analysis. It also compares wired Unstructured P2P file-sharing networks and highlights their unique qualities. This research has examined a range of P2P network characteristics to better understand how P2P network features operate in different contexts. Current P2P networks have been thoroughly analyzed, taking into consideration a variety of essential wired and wireless features. The research demonstrates how effectively different systems work in various scenarios. In this study, P2P file sharing technologies for the networks are systematically and logically examined.

M. Naser and Z. K. Al-Enizi [2] Four strategies that legally reduce the infringement of digital content on domestic as well as international level and new peer-to-peer technology are necessary to give copyright owners a way to sue individuals and lawbreakers with the help of legal system and apply the law to that particular condition while maintaining a fairness between using studies on peer-to-peer technologies and copyright owners. The laws, with file-sharing, apply to any activity related to copyright over peer-to-peer on a local, domestic, and worldwide scale. A unified set of international rules must regulate all intellectual property. Any reproduced works might be the subject of legal action, regardless of where the occurrences took place.

Aronov (2021). [3] emphasizes how changes in societal perception and the idea of copyright protection have been brought about by the advancement of technology. Since using peer-to-peer (P2P) technologies sharing works like music, books, and videos become too much easy one may argue that copyright protection has been compromised. The significance of the problem is determined by Peer-to-Peer is one of the most extensively utilized technologies that contributed in the expansion of illegal sharing of content on the Internet.

Peer-to-peer content sharing and data distribution software, according to Gkantsidis, C., and Rodriguez Rodriguez, P. [4], may enable the transmission of huge files more readily across unstable networks. Researchers are interested in network encryption because it has the potential to improve stability and performance and eliminate network workload. In this survey study, we look at, rate, and contrast. This study is, to our knowledge, the first thorough examination of the operation of P2P data sharing systems.

Peer-to-peer data sharing and communication strategies are intended to transform it simpler to share large files over unstable networks [5]. Coding of the network is a transmission method that caught the attention because it may hasten downloads, increase the overall performance and capability of the systems to transfer files, and lessen network sharing. In this survey study, we evaluate and appraise the current network coding approaches which are required to boost the effectiveness of P2P data-sharing systems. According to us, this study is an in-depth investigation that is focused on the functioning of P2P file-sharing systems.

M. Hossein Zadeh, H. Navidi, M. B. Shareh, H. H. S. Javadi, and [6] Sybil nodes, work together and assume false identities to evade the restrictions of the system. P2P networks are most likely the target of these assaults. Previous studies have not shown simultaneous resistance to these two assaults. The suggested method simultaneously addresses both issues by making use of a special centrality connection in the incentive mechanism. The peer reputation in this respect will be greater the more diverse the nodes that are utilizing a peer's service. The findings demonstrate that as a network matures, becomes relevant and obvious in participating nodes to get fewer benefits.

3. Used Approach

We utilized a comprehensive collection of scholarly research articles to understand the mechanics of peer-to-peer (P2P) networks, the data-sharing processes they facilitate, and the resulting copyright infringements. Our selection criteria focused on the most pertinent research papers, reports, and literature to highlight the key challenges faced by content owners and individuals in P2P networks regarding data sharing and copyright infringement. This review underscores the significance of P2P networks compared to traditional server-client architectures, identifying specific issues and solutions like detection systems, content recognition, watermarking, filtering techniques, pattern recognition, and data mining.

We conducted a thorough analysis of the challenges posed by P2P data sharing, particularly in terms of copyright infringement. Our examination revealed various proposed solutions, including Digital Rights Management (DRM) and watermarking techniques, which help mitigate these issues. Additionally, we explored detection and scalability challenges in P2P networks, presenting solutions such as content recognition techniques and various filtering methods.

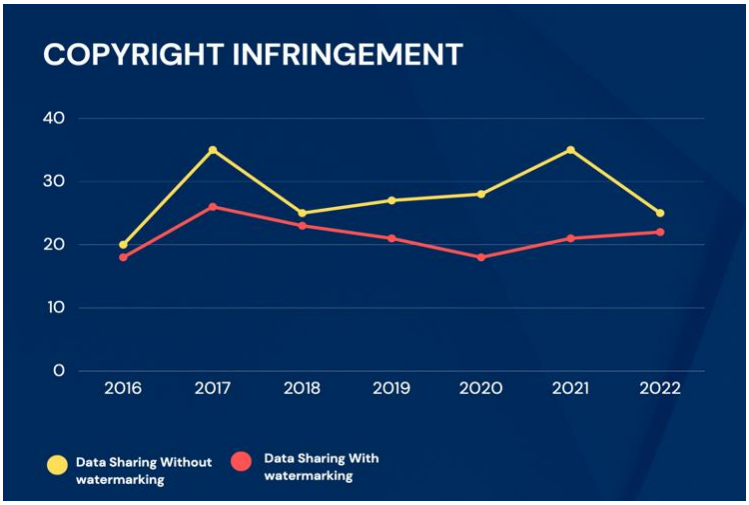

Figure 2. Copyright Infringement

Furthermore, our analysis included the security risks associated with Peer to Peer (P2P) data sharing, emphasizing the prevalence of malicious content. While traditional methods like antivirus and anti-malware software can help reduce malware incidence, we also stressed the importance of raising user awareness about these risks.

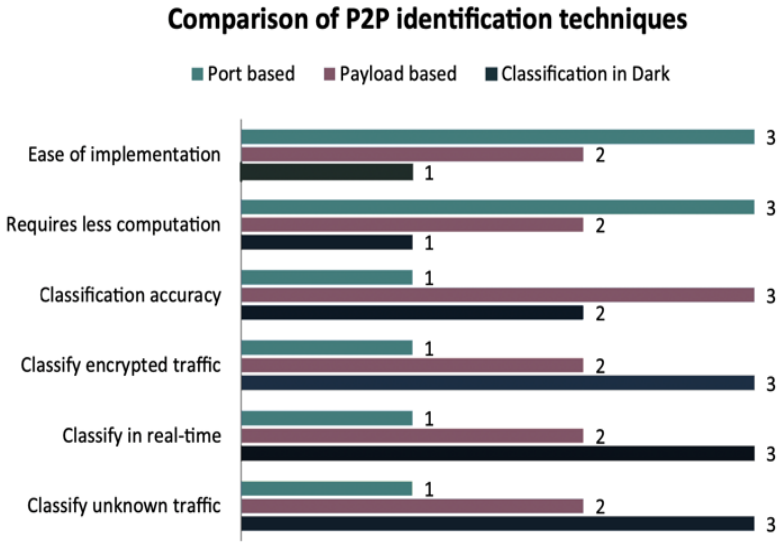

Figure 3. Comparison of P2P Identification Techniques

We addressed privacy concerns and system attacks, reviewing solutions proposed by different scholars. These include techniques such as onion routing, privacy-preserving mechanisms, and reputation systems. Our review provides a comprehensive understanding of these issues and their potential solutions, contributing to the ongoing discourse on Peer to Peer P2P network security and copyright protection.

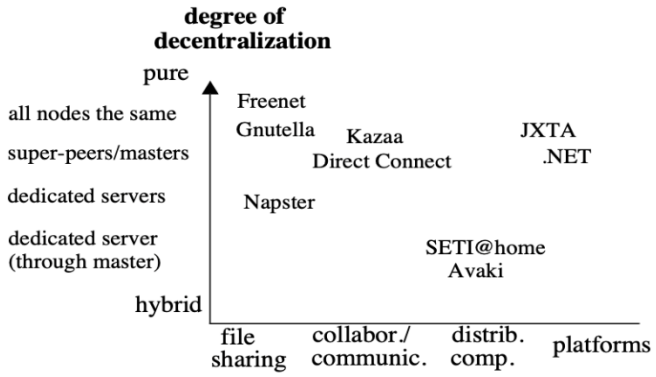

Figure 4. Degree of Decentralization

4. Challenges in P2P

Some challenges in Peer to Peer (P2P) data sharing:

A. Copyright infringement

Peer to Peer (P2P) is the major source of sharing copyrighted content without the permission of the owner who owns the content. This is illegal and causes legal action on both the person who uploaded it and the person who downloaded it, but it is not taken seriously and become a very common practice to it so people believe they could not be tracked or traced easily with peer-to-peer to network.

B. Difficulty in Detection

Peer-to-peer networks have a distributed nature that's why it is very complex to track and trace the people who perform copyright infringement. Due to the presence of a single central server locating the files become more difficult than in the past. Identifying the individual is not an easy task.

C. Scalability:

Peer-to-peer networks are growing with each passing day and the content shared through this network is also increasing in volume directly with the number of users so addressing the copyrighted content issue is becoming more challenging day by day. Server-Client architecture is not as scalable as the peer-to-peer network because every user uses their computing power and bandwidth because of decentralization.

D. Security and Malware Risks

Content that is shared through peer-to-peer networks is unregulated that's why there is a huge chance of viruses and malware passing along with the files and causing different kinds of security risks which can be harmful for your device and existing data in the device.

E. Privacy:

Data sharing on peer-to-peer may have some privacy concern as well of them including data leakage, metadata can be stolen, or maybe malicious content can interrupt it this can be harmful to the uploader as well as to the person who downloads it.

F. Sybil Attack:

This type of attack is common in this network in this attack user of the network makes a different account of himself using fake information and causes disturbance in the network so that digital content cannot be shared properly.

5. SOLUTIONS OF P2P FILE SHARING

Solutions regarding file sharing and copyright infringement:

A. Solution for Copyright infringement

There are some solutions regarding this problem available one of them is DRM which is Digital Rights management they implement different types of software that help in the prevention of unauthorized reproduction and distribution of copyrighted content on the peer-to-peer network. There is also the concept of watermarking in which there is a distinct and unique identifier is present in the digital content which can be tracked and traced to help in the prevention of infringement.

B. Difficulty in Detection

We can use monitoring to identify individuals that involve in these activities but it required the mutual collaboration of content owners, Internet service providers, and majorly the agencies responsible for the enforcement of law like this. The role of Internet Service Provider(ISP) is that they can easily block the internet protocol (IP) addresses of the individuals who are monitored so they cannot access peer-to-peer networks with ease.

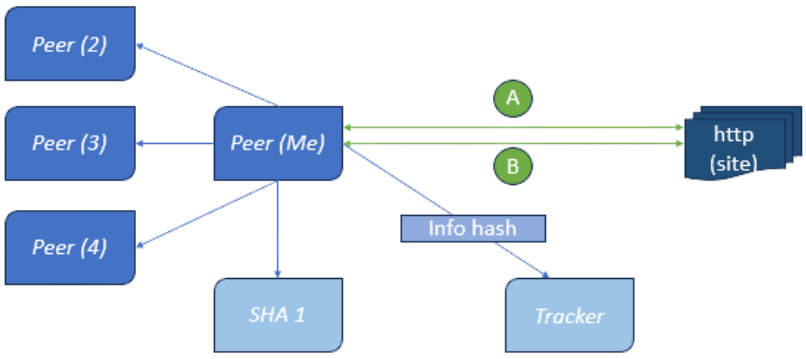

Figure 5: Workflow of P2P Communication

C. Scalability Solution:

To address the scalability issue, we can use different kind of techniques such as content recognition technologies which can detect digital content while they are being shared efficiently by using digital signatures. Furthermore, we can use collaborative filtering along with the reporting technique which helps in filtering based upon reporting of the user multiple time. Moreover, Datamining is used to recognize the pattern for the detection of illegal activities.

D. Security and Malware Avoidance:

To avoid the risk involved with security we can use anti-viruses and anti-malware software which prevent the intrusion of unwanted files into your device this software remains up to date to reduce the chance of downloading harmful files from peer-to-peer networks. Moreover, awareness could be of huge help if people don't know about the potential risks who could they protect themselves without knowing the best practices to follow?

E. Privacy:

There are different techniques for privacy issues in peer-to-peer networks one of them is anonymization in this we use a mechanism like onion routing which protect the digital content being shared [11]. We can also use a

privacy-preserving protocol this protocol helps to secure the computation and increase the privacy of the network [12].

F. Sybil Attack:

To eliminate attacks like the Sybil reputation system is existed through which we can estimate how much specific peer is trustful and all the work is based upon the feedback[13]. Another analysis technique that is useful to analyze the specific Sybil peer to understand the pattern is social network analysis [14].

6. Conclusion

In conclusion, peer-to-peer (P2P) data sharing presents both significant challenges and potential solutions in the modern digital landscape. While P2P networks offer numerous benefits such as decentralized architecture, scalability, and improved efficiency, they also bring about various obstacles that need to be addressed. The primary challenges include data privacy and security, reliability, availability, scalability, and legal compliance. To mitigate these issues, techniques like encryption, digital signatures, redundancy, caching, distributed hash tables, distributed indexing, content replication, and load balancing can be employed. These measures enhance data security, ensure data availability, improve scalability, and optimize network performance. Moreover, addressing legal and ethical concerns regarding copyright infringement is crucial. Ensuring compliance with intellectual property laws and fostering responsible data-sharing practices are essential for the sustainable use of P2P networks. In summary, while P2P networks offer many advantages, they also pose significant challenges. By leveraging technological advancements, robust protocols, and legal frameworks, we can address these challenges and harness the potential of P2P networks while ensuring user privacy, data integrity, and legal compliance.

References

[1] Ashraf, F., & Iqbal, S. (2019) Researchgate.net. Retrieved May 25, 2023

[2] Z. K. Al-Enizi and M. Naser, “The law applicable to P2P networks on national and international bases for violating intellectual property rights,” Int. J. Cyber Warf. Terror., vol. 12, no. 1, pp. 1–10, 2022.

[3] A. Aronov, “Copyright protection in the internet age: Whether copyright can combat peer-to-peer technology,” Law and State, no. 1, pp. 73–88, 2021.

[4] C. Gkantsidis and P. Rodriguez Rodriguez, “Cooperative security for network coding file distribution,” in Proceedings IEEE INFOCOM 2006. 25TH IEEE International Conference on Computer Communications, 2006.

[5] A. A. AbuDaqa, A. Mahmoud, M. Abu-Amara, and T. Sheltami, “Survey of network coding based P2P file sharing in large scale networks,” Appl. Sci. (Basel), vol. 10, no. 7, p. 2206, 2020.

[6] M. B. Shareh, H. Navidi, H. H. S. Javadi, and M. HosseinZadeh, “Preventing Sybil attacks in P2P file sharing networks based on the evolutionary game model,” Inf. Sci. (Ny), vol. 470, pp. 94–108, 2019.

[7] Lu, Y., & Liu, X. (2018). Scalable Copyright Protection Techniques in P2P Networks: A Comprehensive Survey. IEEE Access, 6, 32750-32762. (scalability point refrence

[8] Noor, T., Shaikh, Z., Jafri, S. M., & Chen, V. (2021). Copyright Infringement in Peer-to-Peer Networks: Issues, Challenges, and Countermeasures. IEEE Access, 9, 44292-44311.

[9] Li, R., Li, T., & Guo, L. (2020). A Survey of Copyright Protection Techniques for P2P Networks. IEEE Access, 8, 123321-123342.

[10] Vakilinia, S. R., Li, X., Zarepour, M., & Chen, J. (2019). An Overview of Legal and Technical Approaches to Fight Copyright Infringement in P2P Networks. International Journal of Communication Systems, 32(8), 4019.paper

[11] Dingledine, R., Mathewson, N., & Syverson, P. (2004). Tor: The Second-Generation Onion Router. Proceedings of the 13th USENIX Security Symposium, 303-320.

[12] Sion, R., & Carbunar, B. (2009). On the Privacy of Private-Browsing Mechanisms. ACM Transactions on Internet Technology, 9(2), 1-33.

[13] Xiong, L., Liu, J., Chen, W., & Chen, X. (2008). Defending Against Sybil Attacks in Large Social Networks. ACM Transactions on Internet Technology, 8(4), 1-25.

[14] Yu, H., Kaminsky, M., Gibbons, P. B., & Flaxman, A. (2010). SybilGuard: Defending Against Sybil Attacks via Social Networks. ACM SIGCOMM Computer Communication Review, 36(4), 267-278.

[15] Yahaya, A. S., Javaid, N., Almogren, A., Ahmed, A., Gulfam, S. M., & Radwan, A. (2021). Two-stage privacy preservation and secure peer-to-peer energy trading model using blockchain and cloud-based aggregator. IEEE Access: Practical Innovations, Open Solutions, 9, 143121–143137. https://doi.org/10.1109/access.2021.3120737

[16] Nuthakki, S., Bhogawar, S., Venugopal, S. M., & Mullankandy, S. (2023). Conversational AI and Llm's Current And Future Impacts in Improving and Scaling Health Services. *International Journal of Computer Engineering and Technology*, *14*(3), 149-155.

[17] Suyash Bhogawar, C. A., Nuthakki, S., Venugopal, S. M., & Mullankandy, S. The Ethical and Social Implications of Using AI in Healthcare-A Literature Review.

[18] Ramaswamy, L., & Liu, L. (2003). Free riding: a new challenge to peer-to-peer file sharing systems. 36th Annual Hawaii International Conference on System Sciences, 2003. Proceedings of The.

[19] Liang, J., Naoumov, N., & Ross, K. W. (2006). The index poisoning attack in P2P file sharing systems. Proceedings IEEE INFOCOM 2006. 25TH IEEE International Conference on Computer Communications.

[20] Stutzbach, D., Rejaie, R., & Sen, S. (2005). Characterizing unstructured overlay topologies in modern P2P file-sharing systems. Proceedings of the 5th ACM SIGCOMM Conference on Internet Measurement - IMC '05.