International Journal of Advanced Research in Engineering Technology & Science
ISSN: 2349-2819
Email: editor@ijarets.org Volume-8, Issue-9 September – 2021 www.ijarets.org

CONFIDENTIALITY IN SOCIAL MEDIA APPLICATIONS USING P-2-P NETWORKING AND DISTRIBUTED HASH TABLE

Dr. Vikas Jain,

Assistant Professor, SCRIET-DCA,

Ch. Charan Singh University, Meerut, Uttar Pradesh, India

ABSTRACT

Social networking platforms like Facebook and Twitter are adding users daily. These websites provide real-time communication, media sharing, and message sending. Note that most of these platforms use centralized computer systems, meaning there is only one provider. You must trust this source to safeguard data and communication. Providers seek to benefit from their data, but consumers battle to protect data sovereignty and privacy. Even privately run federated social networks rely on a few dedicated volunteers who help the community and provide them access to the data they monitor. Due to its self-organization and security, peer-to-peer (P2P) networks may ensure data security. Users no longer require a central authority to protect their sensitive data. These networks provide end-to-end communication, access control, anonymity, censorship resistance, and large-scale data breaches caused by misused trust. This poll has three objectives. The paper describes peer-to-peer (P2P) online social networks and its zero-trust requirements. Second, it delves further into peer-to-peer (P2P) frameworks, which enable complex and demanding applications. These include elements that earlier peer-to-peer surveys missed. User and identity management, secure data storage, encrypted communication, permissions control, and extensibility are included. Third, it summarizes P2P online social network application frameworks, architectures, and ideas. In particular, it assesses solution maturity, interdependencies, and technical details.

Keywords: - *peer-to-peer network, online social networks, frameworks*

INTRODUCTION

Following the dramatic rise to fame of the early social networking systems, there are today hundreds of different social networking systems. This is due to the surge of new entrants that have entered the market. Centralization is a characteristic that is shared by all social media platforms, despite the fact that their user bases and features may be very distinct from one another. A large number of algorithms, such as buddy suggestion, may be executed in this situation much more quickly and at a lower cost. Additionally, the centralized structure makes it possible to provide a user experience that is straightforward and based on browsers.

Increasing the capacity of centralized systems to accommodate millions of users is a challenge that might be considered a negative. Current processes demonstrate, without a shadow of a doubt, that the problem can be handled if enough resources is allocated to it. However, in order to justify the large operating expenditures that are needed to maintain the infrastructure that is necessary in order to supply the service to millions of customers, sound economic strategies are essential. There is a strong motivation for social media platforms: (i) to utilize user data to enhance the effectiveness of advertisements and (ii) even provide approved third parties access to user data. This is because advertisements are a significant source of income

for the majority of social media platforms. Nevertheless, several platforms have business structures that are completely distinct. In the absence of specific legislation or unambiguous guarantees, this behavior poses significant threats to the safety of people' personal information and the right of individuals to have their privacy protected.

The tight terms of service that many social media networks have added another layer of complexity to the situation. Because of these principles, users are granted a worldwide right to use any content that they submit, which is non-exclusive, transferable, sub-licensable, and royalty-free. Some individuals believe that social media platforms drive users into "walled gardens" where they do not have full control over their data. This is due to the fact that the personal information of users is a significant value to online social media firms. Finally, but certainly not least, centralized social networking platforms place service providers in a position to censor users either before or after they post, and they may be legally forced to do any of these things, regardless of how private the information is. This is the case regardless of whether the content is public or private. Indeed, in light of the recent controversy surrounding the PRISM program and Edward Snowden's exposure of classified documents, many people have questioned the privacy risks that are associated with the social networking applications that are now available.

As a result, we believe that a strategy based on peer-to-peer interactions or distributed technologies is not only practicable, but also much sought. To begin, the number of users has a direct correlation with the availability of resources, which implies that peer-to-peer (P2P) systems are able to accomplish larger resource scaling with greater ease. Taking into consideration the very high resource needs, this characteristic is especially desirable for social networking systems that exchange media. Another explanation is that peer-to-peer (P2P) distribution is successful for the majority of the content that is available on these networks. This is due to the fact that its popularity increases in a power-law or exponential form over time. There is a possibility that fallback techniques for material that is less popular might be added to this. Regarding the issue of censorship, a peer-to-peer (P2P) system effectively removes the problem from the very beginning. Given that there is no centralized body that has the ability to regularly filter data, users are the sole owners and are legally responsible for the transmission of anything that is considered to be offensive. It is still possible to conduct assaults against decentralized and peer-to-peer social networks. For example, we may inject "sybil nodes" into the network, which are nodes that have phony identities and are meant to damage the reputation system of a peer-to-peer network. On the other hand, the purpose of this work is not to scrutinize attacks of this kind.

OBJECTIVE

1. To the study Peer-to-peer confidentiality in social applications.
2. To the street Safeguarding user data from software developers and others.

Social Networks

The next generation of the Internet, which is already being referred to as Web 2.0, has just started to develop. Immediately after the first Web 2.0 conference hosted by O'Reilly Media in 2004, the term "Web 2.0" started to get more popularity. There is an alternative definition for Web 2.0. During the course of his investigation of Web 2.0, Tim O'Reilly discovered eight primary patterns. Using the web as a platform upon

which application programming interfaces (APIs) are utilized to construct software applications is the primary emphasis of Web 2.0, according to Tim O'Reilly. According to Web 2.0, the Internet is now regarded to be a two-way street, meaning that users are able to participate in discussion in both ways throughout the network. Two of the numerous pillars upon which Web 2.0 is built are the ever-expanding user bases of social networking sites such as Myspace, Facebook, and Hi5, as well as the content that is contributed by users themselves. Users have the option of creating an account, and after they have successfully logged in, they will be led through the process of constructing a profile that will act as their online identity inside these services. The accumulation of all of these accounts constitutes the "friend list" of a participant. Whenever one person extends an invitation to another user to become their "friend," the profile of the other user will include a photo of the two of them together. In this way, people have the opportunity to construct their own networks of friends. The participants in these systems have the ability to access the friend lists of their friends, which is a significant departure from the real world, where it is possible that we do not have the ability to know who our friends' friends are. Despite this, the process is continuing to be pretty comparable. The "friend's" list is more than simply a list of individuals we are close to, which is the conventional definition of a "friend," since it also allows users to be accessible to the public. This is because a user may add new friends by choosing a profile. Even while the participant may not really know any of their "virtual" friends in real life, they can have hundreds of them in their virtual world.

The user profiles and friend lists that are available on social networking sites are two of the sites' most crucial features. The third one is a commenting system that gives users the opportunity to share their thoughts as they relate to the profiles of their friends. These comments are available for reading by anybody who has access to that profile.

Profiles, friend lists, and comments are the three primary components that make up the framework of social networking platforms. Moreover, in order to persuade people to sign up for each social network, additional services could be provided by different social networks. Through the use of the Friend system on a social networking site, it is possible to communicate with anybody who has a public profile on that site. The objective is to provide individuals with the opportunity to interact with other individuals who share their interests and to create a "small world" for themselves on the internet.

P2P technologies

Peer-to-peer networks, often known as P2P networks, are networks in which neither the servers nor the clients are physically located in a single point throughout the network. Every single node in a peer-to-peer (P2P) network acts as both a server and a client for the other nodes in the network. The client-server approach, in which a small number of privileged servers engage in conversation with a large number of ignorant consumer clients, stands in striking contrast to this situation. Many individuals now use their home computers and broadband Internet connections for a variety of additional activities in addition to sending and receiving emails and exploring the internet over the internet. They serve as an alternative to peer-to-peer (P2P) networks, which are networks in which users participate in communication in real time to establish communities that function as shared resources. These communities include filesystems, virtual computers, and search engines. Multiple peer-to-peer (P2P) technologies are now accessible to users. These technologies use a variety of methods in order to get access to the data that is stored in the systems of the other.

P2P approaches

A hybrid peer-to-peer system is one that combines client-server and peer-to-peer (P2P) methods, such as Napster, in order to do a variety of tasks. By using Napster, you are able to exchange audio files with other users. Downloading files is made possible by a piece of software that is included with the product. If you are interested in indexing audio files, Napster provides a directory of audio files that are saved on several computers located all over the world. Give me the opportunity to explain how this process works. Napster gives users the ability to submit a playlist that contains an assortment of music files that they are prepared to share with the community. The server is responsible for matching file requests with a list of providers, despite the fact that the files are sent straight from one computer to another. Unlike in a client-server configuration, these files do not go via Napster's servers in order to reach their destination. Due to the fact that Napster utilizes the P2P technique, which is a technology that circumvents the structure of the Internet, computers that do not have domain names are nonetheless able to discover each other and distribute specific files among themselves.

The pure peer-to-peer technique is used for everything in Gnutella, which is yet another peer-to-peer application. It is recommended that you give Gnutella a go if you are searching for a music sharing application similar to Napster, but without the central server directory. Users of Gnutella are required to first download the application before they can access the system and begin using it. When one computer makes a request for a file, other computers in the network authenticate the request and then pass it on to even other computers in the network until the file is located. This process continues until the file is downloaded.

There are two primary ways in which FreeNet differs from Gnutella, despite the fact that both FreeNet and Gnutella use a P2P method that is entirely decentralized. This means that the person who first uploads material to FreeNet may maintain their anonymity since all of the data that is kept there is encrypted. The information is then moved to another computer in a random fashion once it has been posted. The owner of such a machine is completely unaware of the information that is kept on it. Because FreeNet does not have a central directory, the search engine examines the whole network whenever someone looks for a file on FreeNet. In continuation, FreeNet has an emphasis on effectiveness.

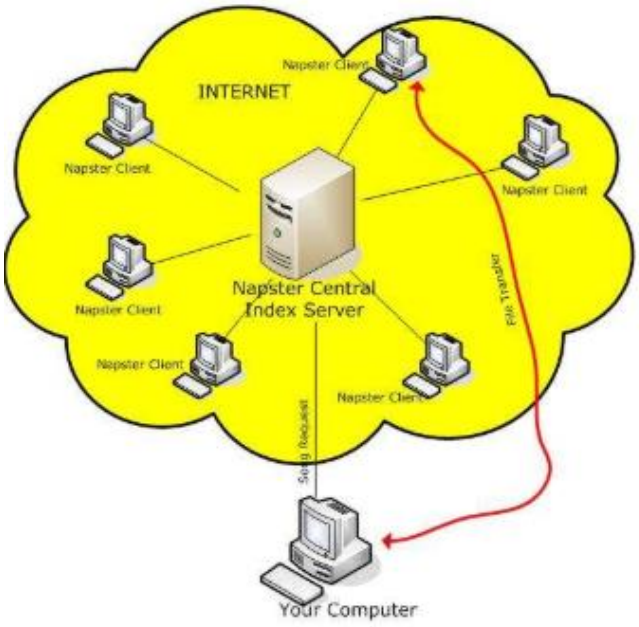

Figure 1: Napster's architecture

Furthermore, in contrast to Gnutella, it keeps track of popular files and ensures that there are several copies of them everywhere. In situations when there is a significant demand for data, FreeNet will also transmit it to a point that is close by. If we take this action, we will be able to reduce the risk that the servers that are hosting the data will become overloaded. This ensures that files can still be accessible, even in the event that the primary computer fails to function properly.

Distributed hash table

As soon as a user joined Napster, their node would interact with the index server of the network. The index server would then conduct searches and lead users to the nodes that stored the results of those searches. As a result of this essential component, the system was vulnerable to attacks and had legal complications. Whenever Gnutella conducted a search, it sent a message to each and every machine in the network. This was made possible by the use of a flooded query method. nonetheless, in comparison to Napster, this method was inefficient; nonetheless, it did remove a single point of failure. Last but not least, Freenet also used a heuristic key-based routing scheme, despite the fact that it was also entirely dispersed. In this system, each file was assigned a key, and files that shared the same key had a tendency to cluster on the same set of nodes. It is likely that requests were sent to a cluster of peers located across the network in order to avoid contacting many peers themselves. Having stated that, Freenet did not provide any guarantees about the finding of data.

A more structured key-based routing is used by distributed hash tables (DHT) in order to accomplish the decentralization that Freenet and Gnutella have achieved, as well as the efficiency and guaranteed results that Napster has achieved. Unfortunately, DHTs are comparable to Freenet in that they only provide exact-match searches and do not permit keyword searches by default. However, it is possible to add keyword searches to a DHT to make it more comprehensive. The DHT technology is an essential component of the BitTorrent protocol.

.

Figure 2: Gnutella's architecture

P2P in building social networks

The year 2007 saw a meteoric rise in the number of people using social networking services. According to Alexa, seven out of the ten websites that were the most popular in October 2007 were related to the Web 2.0 platform. According to ComScore, MySpace receives more than 55 million unique views each and every month, and the site's growth rate is a consistent 23% year over year. Bebo, on the other hand, had a growth of 83% in the number of unique visitors, while Facebook saw an increase of 129%. Because of the rapid pace of expansion, there are now additional challenges to deal with. The providers of social media sites must to be aware of the many challenges that are presented by Web 2.0 sites.

- Users go to social media to create profiles and share content, which generates a lot of stuff. Thus, social media networks must support picture and video sharing. This necessitates storing massive volumes of rich media that is quickly accessible.
- Many individuals use social media. This is because individuals spend more time on social media than other websites. Social networking site page views correlate with visitor clicks. This is because social networking sites commonly show photographs, videos, and messages on a single page with thumbnails or short descriptions that users must click on to see the full versions.

Successful social networks based on P2P

Skype

When it comes to peer-to-peer (P2P) technologies, Skype is the most widely used one that is built on Kazaa file sharing. Skype allows users to have discussions of a high quality, send and receive instant messages, make video calls, hold conference calls, transfer files, and drastically cut the cost of traditional phone calls. Skype users can do all of these things regardless of where they are located. Since the release of version 1.4, Skype has been a social networking system. At that time, it started to include capabilities that are comparable to those that are present in social networks. When you look at your profile, you will be able to see the number of people that are on your Skype contact list. It is via these contact lists that social networks are established. Whether or not to share certain contacts is a choice that users have the ability to make.

There are three basic components that make up a Skype network. These are the login server, ordinary nodes, and super nodes. It is referred to as a Skype node when a computer is used to run the Skype application, which is more generally referred to as a Skype client. The term "super node" refers to an ordinary computer that is capable of running Skype. However, Skype has selected super nodes to handle some aspects of the administration and coordination of the peer-to-peer network rather than regular computers. Despite the fact that Skype has not disclosed the requirements for becoming a super node, it is evident that having a quicker broadband Internet connection boosts your chances of becoming a super node. However, you do not have any control over whether or not you become a super node. The number of super nodes is in the thousands, whereas the number of normal nodes is in the millions.

One of the most important functions of a Skype client (SC) is the ability to log in, search for other users, start and stop chats, transmit material, and send notifications of presence. At the time of login, a node is required to register with a Skype server and authenticate its identity. When a user logs in to Skype, for the purpose of verifying their identity, the service keeps the login credentials that they have provided. In addition to the obfuscated list of servers that is included inside the Skype executable, there are other Skype login servers that make use of certain ports. Just login servers are all that Skype has; it does not have a central server.

In order to join the Skype community and validate the user's credentials with the central server, a super node is necessary for SC authentication. This is part of the Skype authentication process. In order to ensure that they are able to connect to the appropriate super node, each SC is required to maintain a record of the IP addresses and ports of all of the super nodes that are included inside its local table. This information is known as host cache (HC), and it is stored in the Windows Registry of the single computer that has been selected. SC is responsible for constructing and updating HC at fixed periods. There are a number of bootstrap super nodes that are included with Skype. These are addresses that have already been set for a variety of nodes.

Every time you start Skype, it will make an attempt to connect to this Special Network (SN) by reading the data from the host cache and then obtaining the first IP and port from that location. In the event that the connection is unsuccessful for whatever reason (for example, the SN is down, it is no longer a member of the network, etc.), it reads the following paragraph from the database. Skype will notify the user of a login issue at starting if it is unable to establish a connection to any of the IPs that have been specified. Therefore, in order for the software to effectively connect to the network and operate, the host cache has to have at least one item that is genuine. It is necessary to have both the IP address and the port number of a functioning Super Node in order to have a valid entry. Not only does Skype enable secure connections, but it also delivers high-quality voice conversations while requiring just a little amount of data to be sent. In order to prevent unwanted access to data while it is being sent over a network, the Advanced Encryption Standard (AES) encodes all of the data.

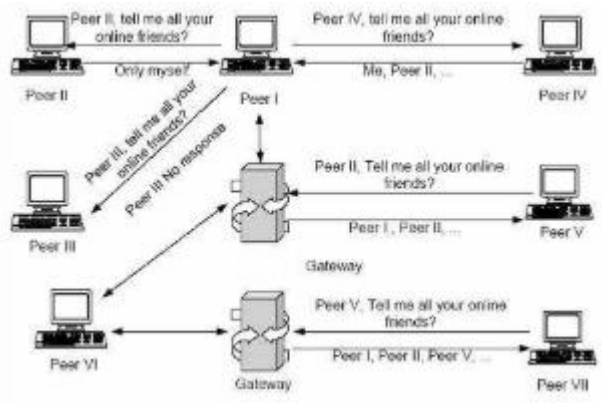

Figure 3: Peers discover in Maze

CONCLUSION

Libre Social, a peer-to-peer (P2P) social network platform, is described in this article. This Open Social Network (OSN) program aims to create a secure, distributed online social network with high-quality services and low operating costs. Even if it runs on unreliable, insecure, and malicious user devices. This article describes the technological requirements for a peer-to-peer (P2P) online social network (OSN) and how Libre Social met them. We do this to fulfill OSN criteria. Libre Social is built on Free Pastry, a structured peer-to-peer overlay with identity management and security enhancements. This ensures logarithmic routing efficiency. Distributed sets, distributed linked-lists, and prefix hash trees improve PAST file storage. These features enable the storage and access management of complex data like albums, comments, and inbox messages. These improvements allow the implementation of more advanced searching algorithms like range searches. Aggregated metrics from Libre Social may be used to monitor QoS. System monitoring and testing plugins enable this. This allows changes to reach optimal service quality criteria. The P2P architecture enables many features, including friends, messages, photos, walls, group/forums, file storage, voting, and audio/video chat. Social networking platform Libre Social lets individuals converse. Modern and simple user interface makes this product appealing.

REFERENCE

1. Pallis G, Zeinalipour-Yazti D, DikaiakosMD. Vakali A, Jain LC. Online Social Networks: Status and Trends.New Directions inWeb Data Management 1. Berlin, Heidelberg: Springer; 2011:213-234.

2. Greenwood S, Perrin A, Duggan M. Social Media Update 2016. Washington, DC: Pew Research Center; 2016.

3. Bengel G, Baun C, Kunze M, Stucky K-U. Masterkurs Parallele und Verteilte Systeme: Grundlagen und Programmierung von Multicore-Prozessoren, Multiprozessoren, Cluster, Grid und Cloud. New York, NY: Springer; 2015.

4. Guidi B, ContiM, Ricci L. P2P architectures for distributed online social networks. Paper presented at: Proceedings of the 2013 International Conference on High Performance Computing & Simulation (HPCS). Helsinki, Finland; 2013:678-681; IEEE.

5. Maqsood T, Khalid O, Irfan R, Madani SA, Khan SU. Scalability issues in online social networks. ACM Comput Surv. 2016;49(2):40:1-40:42.

6. Ananthula S, Abuzaghleh O, Alla NB, Chaganti SP, Kaja PC, Mogilineedi D. Measuring privacy in online social networks. Int J Secur Priv Trust Manag. 2015;4(2):1-9.

7. Krishnamurthy B, Wills CE. On the leakage of personally identifiable information via online social networks. WOSN '09. New York, NY: ACM; 2009:7-12.

8. Aiello LM, Ruffo G. LotusNet: tunable privacy for distributed online social network services. Comput Commun. 2012;35(1):75-88.

9. Krishnamurthy B, Wills CE. Characterizing privacy in online social networks. WOSN '08. New York, NY: ACM; 2008:37-42.

10. Becker J, Chen H. Measuring Privacy Risk in Online Social Networks. Oakland, CA: University of California, Davis; 2009.

11. Datta A, Buchegger S, Vu L-H, Strufe T, Rzadca K. Decentralized Online Social Networks. Boston, MA: Springer; 2010:349-378.

12. Conti M, De Salve A, Guidi B, Pitto F, Ricci L. Trusted dynamic storage for dunbar-based P2P online social networks. In: Meersman R, Panetto H, Dillon T, et al., eds. On the Move to Meaningful Internet Systems: OTM 2014 Conferences. Berlin, Heidelberg/Germany: Springer; 2014:400-417.

13. Buchegger S, Datta A. A case for P2P infrastructure for social networks-opportunities & challenges. Paper presented at: Proceedings of the 2009 6th International Conference on Wireless On-Demand Network Systems and Services 2009. Snowbird, UT; 2009:161-168.

14. Paul T, Buchegger S, Strufe T. Decentralized Social Networking Services. Milano: Springer Milan; 2011:187-199.

15. Buford JF, Yu H. Peer-to-Peer Networking and Applications: Synopsis and Research Directions. Boston, MA: Springer; 2010:3-45.

16. Rodrigues R, Druschel P. Peer-to-Peer Systems. Commun ACM. 2010;53(10):72-82.

17. Urdaneta G, Pierre G, Steen MV. A survey of DHT security techniques. ACM Comput Surv. 2011;43(2):8:1-8:49.

18. Graffi K, Podrajanski S, Mukherjee P, Kovacevic A, Steinmetz R. A distributed platform for multimedia communities. Paper presented at: Proceedings of the 2008 10th IEEE International Symposium on Multimedia. Berkeley, CA; 2008:208-213; IEEE.

19. GraffiK, Podrajanski S,Mukherjee P,KovacevicA, Steinmetz R. LifeSocial.KOM:A P2P-based platform for secure online social networks. Paper presented at: Proceedings of the 2010 IEEE Tenth

International Conference on Peer-to-Peer Computing (P2P) 2010. Delft, Netherlands; 2010:1-2; IEEE.

20. Graffi K, Podrajanski S, Mukherjee P, Kovacevic A, Steinmetz R. LifeSocial. KOM: a secure and P2P-based solution for online social networks. 2011 IEEE Consumer Communications and Networking Conference (CCNC). Las Vegas, NV; 2011:554-558; IEEE.