International Journal of Engineering Innovations in Advanced Technology
ISSN: 2582-1431 (Online), Volume-1 Issue-4, December 2019

UTILIZATION OF CORPORATE NETWORKS FOR FLEXIBLE DATA SHARING AMONG CORPORAL SYSTEM

Dr. Y. Dasaratha Rami Reddy
Associate Professor, BVSR Engineering College, Chimakurthy, Prakasam, India.
Email: dasradh@gmail.com

G. Sreenivasa Reddy
Associate Professor, BVSR Engineering College, Chimakurthy, Prakasam, India.
Email: gsrbvsr@gmail.com

***Abstract*: Many companies use corporations Information exchange network between companies and ensure communication between them. common interest. helps math Costs and Benefits. Despite the advantages, yes. Inherent security risks, network capacity and efficiency in such an information exchange system. To solve these problems: We offer a new system called ComPeer. Providing flexible information exchange services. A cloud environment based on equivalent technology. Through Database, P2P technology and cloud integration. The calculation makes the system economical and flexible An extensible network platform for enterprise networks Deploy data sharing applications and services: Participants are based on an approved payment model.**

Keywords: Corporate system, Compeer, P2P, Information exange system

I INTRODUCTION

Many companies collect and store confidential information about their employees and customers, such as social security numbers, credit card and account information, and medical and other personal information. Many of them have a legal obligation to protect this information. Getting into the wrong hands can lead to fraud and identity theft. Therefore, any company that collects and stores confidential information should consider the security implications of using peer-to-peer (P2P) file sharing software and reduce the risks associated with it. Firms with a peer-to-peer economy are seen as an alternative to traditional capitalism, which has the means of production and final products. Businesses act as centralized intermediaries, selling finished products and services to consumers and hiring the people needed to lead production processes. A capitalist economy can have a peer-to-peer economy. Open source software (ie peer-to-peer) coexists with commercial and commercial software. Services such as Uber or Airbnb are offered as alternatives to taxi and live services or to hotels and guesthouses, respectively. The company acts as a hybrid between traditional capitalist firms and true peer-to-peer services, providing intermediary services, including networks that connect buyers and sellers and process payments, but use individual contractors to serve customers directly. If a third party is not involved in P2P transactions, there is a high risk that the supplier will not ship, the product will not be of the expected quality or the buyer will not pay. Reduced overheads and, consequently, lower prices may absorb this additional risk.

II RELATED WORK

Peer-to-peer (P2P) technology is an easier way to share music, videos and documents, play games and make calls online. This technology allows computers that use the same or compatible peer-to-peer programs to create networks and share digital files directly with other computers on the network. Almost anyone can connect to a peer-to-peer network by installing certain software, allowing millions of computers to connect simultaneously. Bear Share, LimeWire, Ka Zaa, eMule, Vuze, uTorrent and BitTorrent are examples of peer-to-peer file sharing programs. If your peer-to-peer file sharing software is not set up correctly, anyone on your peer-to-peer network can access unshared files. The Federal Trade

Commission (FTC), the U.S. National Agency for Consumer Protection, has published a series of initiatives to highlight security vulnerabilities that can occur when an organization allows its employees and others with network access to use shared P2P files. . wrote this guide. This guide also provides a list of actions that a network administrator or security professional can take to resolve these issues. security risk peer-to-peer file sharing program allows you to download files from your computer and make them available to other users on your network. P2P users can mark with which disks and folders they can share files. In turn, other users can download and view all files stored in these designated areas. People who use peer-to-peer file sharing software may accidentally share files. You can choose to randomly share a disk or folder that contains confidential information, or you can accidentally save personal files to a shared disk or folder and make those personal files available to others. Viruses and other malware can also change disks or folders designated for sharing and threaten individual files. As a result, rather than just sharing music, users' personal tax returns, personal medical records, or business documents can generally be circulated on P2P networks. When a P2P user downloads someone else's file, they cannot extract or delete the file. You can share files between computers long after they have been deleted from the original computer. And if there are security vulnerabilities or vulnerabilities in P2P file sharing software or in an organization's network, the P2P program could open the door to attacks on other computers on the network.

Protecting confidential information online There are no shortcuts when dealing with security vulnerabilities in peer-to-peer file sharing. Whether or not you allow peer-to-peer file sharing applications, follow these steps to ensure that your confidential information on your network is secure. Delete unnecessary confidential information and limit the storage of files that contain confidential information. Reduce or eliminate the use of peer-to-peer file sharing programs on computers used to store or access confidential information. Use an appropriate file naming convention. Monitor your network for unauthorized peer-to-peer file sharing applications. Block traffic related to unauthorized peer-to-peer file sharing programs on your network perimeter or network firewall. Educate network staff and others about the security risks inherent in using peer-to-peer file sharing programs. There are many factors involved in deciding to allow or allow peer-to-peer file sharing programs on an organization's network. For example, what type and location of confidential information on your network? Which computers can access files that contain confidential information? What are the security measures to protect these files?If your network contains confidential information that is not required for your business, it is best to delete this information securely and permanently. Protect your privacy to help you decide what types of files you can delete. Read our business guide. However, if you have confidential information needed to do business on your network, compare the benefits of using a peer-to-peer file sharing program with the security risks associated with the program. Does your company need to share files outside of your organization? Is there a way employees can share files securely? Even if you decide to ban or allow peer-to-peer file sharing programs on your network, it's still important to create a policy and take the right steps to implement and implement it.

This reduces the risk of accidentally sharing confidential information. Communications and networking in today's business world There are two fundamentally different types of communication networks. Telephony and computer networks are slowly converging into a single digital network, using common internet technologies and equipment. Voice and data networks have also become stronger (faster), portable (small and mobile) and cheaper. Today, more than 60% of Internet users in the United States use high-speed broadband connections from telephone and cable companies at speeds of up to 1 million bits per second.

The cost of this service has dropped exponentially. Voice and data communications and access to the Internet via wireless broadband platforms are becoming more common. In addition to client computers, the main components used in a simple network are: Network Interface Card (NIC): Usually built into the client computer Connection medium: cable or wireless signal for data transmission Network Operating System (NOS): Software that manages network communications and coordinates network resources that can reside on any computer or dedicated server computer. Hub or switch: A device that connects network components to a hub and sends data packets to all connected devices. A switch is like a hub, but it can send data in a certain direction. A router is a network device designed to connect two or more networks.

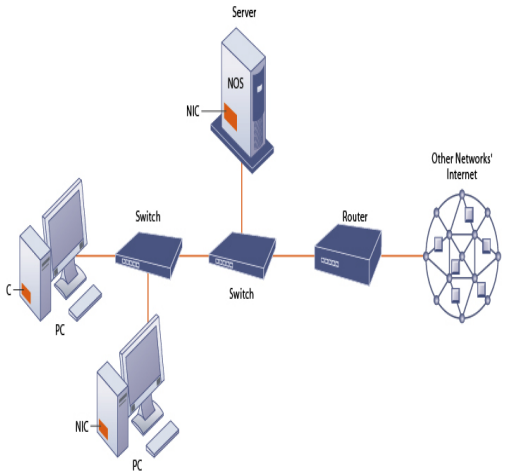

Figure 1 components of a simple computer network

The network infrastructure of a large enterprise usually consists of a small local area network (LAN) connected to the enterprise's shared corporate network for data and voice communications and several high-performance servers that support corporate websites, intranets. , extranets or server systems. such as sales, orders and financial transactions. Businesses are facing the challenge of strengthening these networks and it will become easier as connections become digital. Figure 2.

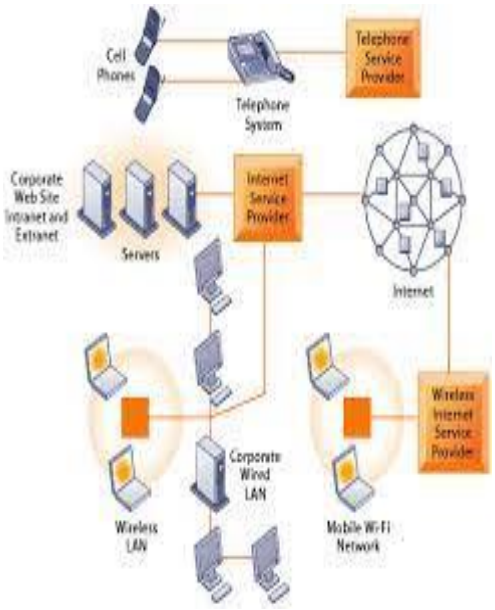

Figure 2 Infrastructure of a coporate network

Today's corporate network infrastructure is a diverse collection of public switched telephone networks. Internet; Connect to the local network of a company that connects workgroups, departments, or offices. Today's digital networks are based on three main technologies. Client / Server Computing: In client / server computing, client computers are connected through a network controlled by a server computer that defines the connection rules for the network and provides the address of each client and device on the network. Packet switching: A method of splitting a message into smaller packets, sending them independently over different routes in the network using routers and then collecting them back to their destination. Figure 3

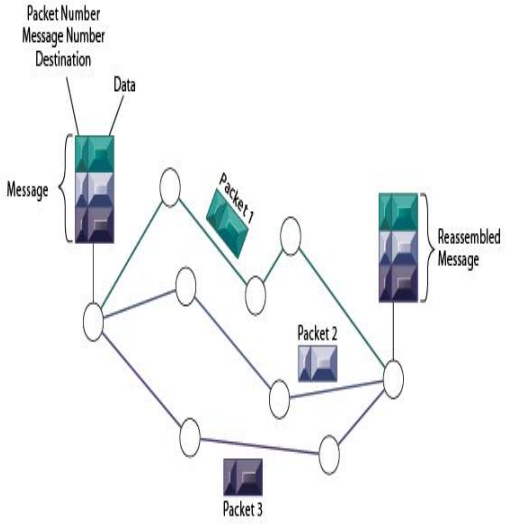

Figure 3 Computer Network Package and Communication Package

The data is grouped into small packets that are transmitted independently over different communication channels and reassembled at their final destination. Common protocol and TCP / IP: A common communication protocol provides a set of rules that allow communication between different components of a communications network. TCP / IP is a set of protocols that provides a way to pack messages, redirect them to the correct address, and reassemble them for installation, making it the

preferred model for accessing a wide range of networks, computers, and the Internet. The TCP / IP reference model consists of four layers. Two computers using TCP / IP can communicate even if they are based on different hardware and software platforms. Figure 4

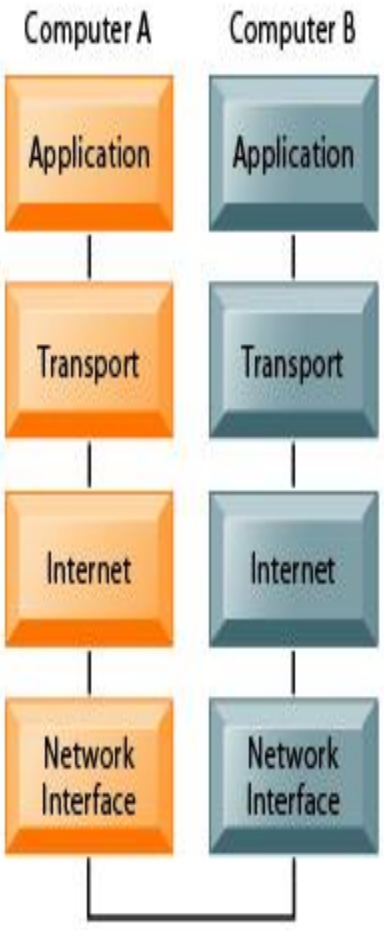

Figure 4 Transport Management Protocol / Internet Protocol (TCP / IP) reference model.

This figure shows the four layers of the TCP / IP reference model for communication.

Among the issues considered: If you decide to ban a P2P file sharing program, how do you prevent it from being installed and used? If you decide to allow peer-to-peer file sharing applications, how do you protect sensitive information stored on your organization's network? If you allow

your employees, contractors, or vendors to use offline computers for remote access, what additional steps are you taking to prevent confidential file sharing through peer-to-peer file sharing programs installed on those computers? How do you educate your employees about the risks of using peer-to-peer file sharing programs? Will there be sanctions for non-compliance with the policy?How can you determine if your policy is effective? If you decide to ban the use of P2P file sharing programs ...If you decide to completely ban peer-to-peer file sharing programs, you need policies and procedures to prevent them from being installed on computers on your network, to detect installed P2P programs, and to block related traffic. To avoid installing P2P file sharing programs:Use administrative security measures to block access to sites used to download peer-to-peer file sharing programs from the network. You can filter sites based on URL, IP address, file name, and content, or use commercial products to take action. The control should block access to sites that offer free software downloads. These sites are often the source of P2P file sharing programs.Implement administrative security measures to prevent employees from installing unauthorized software on your organization's computers. To identify installed peer-to-peer file sharing programs and to block related traffic:Scanning tools are often used on personal computers and networks to find and remove P2P file sharing programs. Commercially available scanning tools can detect many P2P applications. Tools that allow network administrators to restrict, monitor, and manage access to peer-to-peer file sharing networks in corporate networks, including intrusion detection

systems (IDS), intrusion prevention systems (IPS), or firewalls installs that properly detect and restrict peer traffic. Inbound and outbound traffic connections to the Internet. Different P2P file sharing programs use different protocols, so research may be required to configure these tools. Commercial hardware and software vendors can help. Detect and monitor P2P traffic by installing IDS, IPS, and firewall configuration-based file transfer history. Use methods

such as network monitoring and streaming tools to determine if there is peer-to-peer traffic on your network and to determine the nature, possible names, and content of files sent and received over the network through the peer-to-peer shared application files. Check your online history and activity logs for large files or increased traffic that may indicate that large files are shared. Install a data loss prevention tool that scans files online to see if they contain certain types of confidential information, such as social security numbers. Periodically check the records generated by these tools to ensure that confidential information is exported. To protect confidential information: Restrict the places where you can save or copy work files that contain confidential information. For example, you can create a dedicated and well-protected network server to host these files, or you can use a file manager. These tools and methods can block confidential information and limit the extent to which peer-to-peer file sharing programs are prohibited.If possible, use application-level encryption to protect the information in your files. This type of encryption helps protect accidentally shared files on a peer-to-peer network. If you use encryption, keep passwords and encryption keys safe. Make sure it is not available on a shared disk or folder. Use

conventions for file names that are less likely to determine what information the file contains. For example, it is easy to define terms such as "ssn", "tax" or "medical" in a file name. If you encounter an unauthorized P2P program on your network, check it yourself or consult a third-party service provider for confidential information. Be careful about the terminology you use, as your search terms will be visible to others in your peer-to-peer network. Some search terms (e.g., including "sn") may increase the risk of confidential information, while others (for example, company or product name) may not. Contact a security professional to manage these risks. If you decide to allow P2P file sharing programs ...If you decide to allow peer-to-peer file sharing programs on your organization's computers, we recommend that you try and control the use of unauthorized files to prevent sharing. First, look at several P2P file sharing programs and choose the right one for your organization. Then allow only approved programs and configurations. To control the installation of allowed peer-to-peer file sharing programs:Approved programs are delivered directly to authorized users from an internal server, rather than from a regular download site. This reduces the chances of viruses or other malware in the program.

To verify using a peer-to-peer file sharing program:

Update your approved peer-to-peer software frequently from approved and verified sources to ensure that you have the latest security fixes.A file type that contains confidential information, usually .doc, .docx, .xls, .xlsx, .mda, .mdb, .txt, etc. PDF. If your business needs to share file types, consider using a file-sharing program other than peer-to-peer. Use the tools and methods above to detect unauthorized P2P file sharing

programs (or unauthorized versions of authorized P2P programs) on your network and block relevant traffic. To protect confidential information. † P2P method for parallel processing Parallelism idea for each connection By designating all tuples as a single processing node Implement in the set of nodes that contain them. will be processed Connect in parallel. We use common combinations of iterations. aspect. A small meal is repeated for everyone. Process the nodes and combine them with large sections of the table. Query when the query contains multiple aggregations and groupings A plan can be displayed as a processing diagram. Processing schedule: On request Processing schedule: It is created as follows:□ For each node, assign a level ID to each node.□ The root node is the equation that accepts the query, Who is responsible for collecting the results user. Suppose the search contains x connections and y "groups". property, the maximum level of the chart is met†□ Processes only all nodes except the root node A concatenation operator or "group" operator. □ Level nodes receive input data from ComPeer. storage system. After processing, A node sends data to its parent node. □ Any operator that does not evaluate as non-rootThe nodes are managed by the root. Change the cost of the network in recurring connections as follows: parallelism. Profits can be offset if they are highIn a peer-to-peer network, the number of tuples is redistributed. Therefore, we offer a cost estimation model. This is Parallel processing of cost models that include I / O and CPU The total cost is governed by time.

III CONCLUSION

We discussed specific challenges, such as: Data sharing and processing between companies Medium and recommended ComPeer systems Flexible data

sharing service through cloud computing integration, P2P database and technology. Our system can Efficient management of common work tasks in corporate networks Near-linear queries can provide bandwidth if you have numbers. Normal seeds grow. So ComPeer has great prospects. It is a solution for efficient data sharing through the corporate network.

REFERENCES

1. Gang Chen, Tianlei Hu, Dawei Jiang, Peng Lu, Kian-Lee Tan, Hoang Tam Vo, and Sai Wu, "BestPeer++: A Peer-toPeer Based Large-Scale Data Processing Platform" Vol. 26,No. 6, June 2014.
2. A. Abouzeid, K. Bajda-Pawlikowski, D.J. Abadi, A. Rasin, and A. Silberschatz, "HadoopDB: An Architectural Hybrid of MapReduce and DBMS Technologies for Analytical Workloads," Proc. VLDB Endowment, vol. 2, no. 1, pp. 922-933, 2009.
3. C. Batini, M. Lenzerini, and S. Navathe, "A Comparative Analysis of Methodologies for Database Schema Integration," ACM Computing Surveys, vol. 18, no. 4, pp. 323-364, 1986.
4. D. Bermbach and S. Tai, "Eventual Consistency: How Soon is Eventual? An Evaluation of Amazon s3's Consistency Behavior," in Proc. 6th Workshop Middleware Serv. Oriented Comput. (MW4SOC '11), pp. 1:1-1:6, NY, USA, 2011.
5. Ramakrishnan, and R. Sears, "Benchmarking Cloud Serving Systems with YCSB," Proc. First ACM Symp. Cloud Computing, pp. 143- 154, 2010.
6. 6. Bonifacio, M., Bouquet, P., Mameli, G., Nori, M.: Peer-mediated distributed knowl-edge management. In: van Elst, L., Dignum, V., Abecker, A. (eds.) AMKM 2003.
7. LNCS (LNAI), vol. 2926, pp. 31–47. Springer, Heidelberg (2004)
8. Bouquet, P., Don`a, A., Scrafini, L., Zanobini, S.: ConTcXtualizcd Local Ontology Specification via CTXML. In: AAAI Workshop on Meaning Negotiation, pp. 64–72(2002)
9. Castano, S., Ferrara, A., Montanelli, S.: H-Match: an Algorithm for Dynamically Matching Ontologies in Peer-based Systems. In: The 1st VLDB Int. Workshop on Semantic Web and Databases (SWDB), pp. 231–250 (2003)
10. 9. Castano, S., Montanelli, S.: Enforcing a Semantic Routing Mechanism based on Peer Context Matching. In: Proc. of the 2nd Int. ECAI Workshop on Contexts and Ontologies: Theory, Practice and Applications (2006)
11. Choi, N., Song, I., Han, H.: A survey on ontology mapping. SIGMOD Rec. 35(3),34–41 (2006)
12. Colazzo, D., Sartiani, C.: Mapping Maintenance in XML P2P Databases. In: Bier-man, G., Koch, C. (eds.) DBPL 2005. LNCS, vol. 3774, pp. 74–89. Springer, Heidelberg (2005).