Research Article

Data sharing and monitoring using LAN

Usha N. Katore, Mr. Sharad M. Rokade , Mr. Kishor N. Shedage and Mr. Devidas S. Thosar

Department of Computer Engineering, Department of Computer Engineering, SVIT, Chincholi, Nashik

Abstract

The current situation for files and data sharing using LAN we must access shared folders. Once sharing folders receiver of other machines needs to check the update folder on share location on his machine. Also, the receiver doesn't get any notifications. This process has got a lot of time. So, the new System going to implement as Data sharing and monitoring using a LAN

Keywords: Sharing, monitoring, grouping, notification, messaging, etc

Introduction

A local area network is a data communication network, typically a packet communication network, limited in geographic scope. **A** local area network generally provides high-bandwidth communication over inexpensive transmission media. This paper discusses data sharing and monitoring, their structures, the **sorts** of protocols that used with them, and their applications. The share per PC is the achievable saturation throughput per PC when stations operate with different MAC parameters. Local area networks have particular value in the monitoring and control of systems that have several separate sensors, actuators, and control units dispersed over a large area.

Literature Survey

Several researches have proposed by researchers for sharing preserving in the LAN network. A detailed survey has carried out to identify the various research articles available in the literature in all the categories of privacy sharing and monitoring in the LAN network, and to analyze the major contributions and its advantages.

The following are the kind of literature applied for assessment of the state-of-art work on data sharing and monitoring in LAN network.

Although the static server model can make resource Share better in LAN, reduce duplicate requirement from

WAN and save more bandwidth for other users. We need to

Keep one or more static server for resource register, search, Listen, and so on. If the server node shuts down, the whole system cannot work or all shared service will be interrupted. Due to these reasons, we

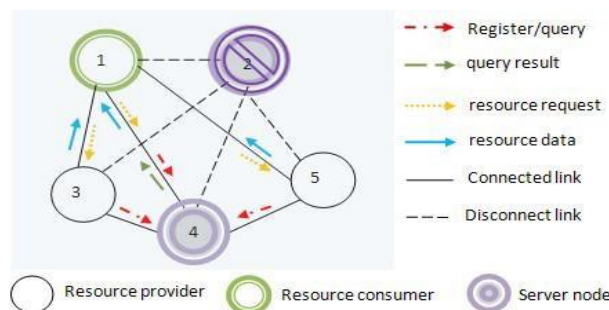make some changes to the model in Section II, and the improved model is demonstrated as in Fig.1.

Figure 1. The improved model

In the new model, there will no static server node.
We will use a dynamic node as a server node inFig.1 show, in the beginning, node 2 works as a server, if node 2 is interrupted by some reason, the system will choose another useable node from LAN as the new server (node 4 for example), that will make the whole system can work uninterrupted.

A. Security
The newly build application has provided security through SHA-1 while the user sends data to others at the receiver end receiver has to enter a password to access the folder send by the sender.

B. Maintaining a LAN machine
Server of the LAN will monitor what the user doing on his machine.
Ex. In college, the school or Organization server will monitor what going on in the LAN machine whether people are doing the given task.

Proposed Methodology

In the proposed system going to implement data sharing in which the sender can send data to any group of machines or any particular machine, the server will monitor all the users after a particular time. While user copy data and going to paste that time he will get which user is available in the same LAN from a selected group he can also send data to a particular user while sending data it will provide a password and the receiver also has to enter a password to open that file.

A. Architecture

Define abbreviations and acronyms the first time they are used in the text, even after they have been defined in the abstract. Abbreviations such as IEEE, SI, MKS, CGS, sc, dc do not have to be defined. Do not use abbreviations in the title or heads unless they are unavoidable.

B. Algorithms procedure init

1: $sCPAk(t) \leftarrow 0$ for all $1 \le t \le n$
2: $pk \leftarrow 0$
3: if $k > 1$ do 4: $sUBk \leftarrow 0$
5: else
6: $sUBk \leftarrow q\infty$
7: assign CPA()
Procedure assigns CPA
8: if $pk = 0$ do
9: Generate a new random ordering of Dk into wk
10: $pk \leftarrow pk + 1$
11: if $pk > |Dk|$do
12: backtrack()
13: else 14: $Xk \leftarrow v : = wk(pk)$
15: update shares in CPA (k, v)
16: if $k = n$ do
17: ifcompare CPA cost to upper bound() = true do
18: broadcast (NEW OPTIMUM FOUND)
19: assign CPA()
20: else
21: ifcompare CPA cost to upper bound() = false do
22: assign CPA()
23: else
24: send (CPA MSG) to Ak+1
Procedure backtrack
25: if $k > 1$ do
26: $sCPAk(t) \leftarrow 0$ for all $t \in I- k$
27: send (ZERO SHARE MSG, k) to At for all $t \in I- k$
28: send (BACKTRACK MSG) to Ak−1
29: else
30: broadcast(COMPLETE)
When received (NEW OPTIMUM FOUND) do
31: $sUBk \leftarrow Pt\in Ik \ sCPAk(t)$ 32: OptimalSetting $k \leftarrow Xk$
When received (CPA MSG)do
33: $pk \leftarrow 0$
34: assign CPA()
When received (ZERO SHARE MSG, k0)do 35: $sCPAk(k0) \leftarrow 0$
When received (BACKTRACK MSG)do
36: assign CPA() when received (COMPLETE)do 37: $Xk \leftarrow$ Optimal Setting k 38: Terminate

C. Mathematical Modules

System Description:

• Let S be a system having sets of parameter Set S= ((I) , (R) ,(P) ,(O))
where S is Storage of data according to the classification I = set of all inputs given for storing the data R is a set of rules that drive your input set.
P is a set of all processes in system. O is a set of output expected from system.

• Inputs (I) :I1,I2,I3
Where, I1 = Data Uploading
I2 = Processing
I3 = Securing Data

• Rules (R) : R1,R2
Where, R1 = Sensitive Data should be Different
R2 = Authentication Required

• Processes (P) : P1,P2,P3
Where, P1 = Conceptually Sorting of Data
P2 = Hierarchical Classification
P3 = Similarity of Data

• Output (O):O1, O2, O3

Result and Discussions

According to the interaction characters among SaaS services, I've proposed a privacy disclosure checking method that satisfies users' requirements. I've developed a prototype system, which describes the users' privacy requirements and extends BPEL and its execution engine to meet users' privacy requirements. I've also designed a case and run it on the prototype system to confirm the feasibility and correctness of our method. Our approach can check privacy disclosure behavior among SaaS services, which can effectively prevent service participants from maliciously disclosing users' privacy information, increase service credibility, and provide a basis for privacy protection-oriented credibility measurement. The next step is to detect the release of the data of users' privacy, analyze the data, and discretize the dataset that may be exposed to protect users' privacy before they are released.

References

[1]. Wang Kan, Yuan RuiXi, "Optimize buffering strategy for P2P Video-on-demand systems", Journal of Tsinghua University (Sci&Tech), July 2009, Vol. 49, pp.1054-1057.
[2]. Xu Haimei, Lu Xianliang, "Rare Resource's Sharing Mechanism in Unstructured P2P Networks", Journal of Electronics & Information Technology, Aug 2009, Vol.31,pp.2028-2032.
[3]. Ching-Hsien Hsu, Yun-Chiu Ching, "An Efficient Peer
[4]. Collaboration Strategy for Optimizing P2P Services in Bit Torrent- Like File Sharing Networks", Journal of Internet Technology, Jan 2010, vol.11,pp.79-88.
[5]. Zhang Yi-ming, Lu Xi-cheng, Zheng Qian-bing, and Li Dongsheng. "An efficient search algorithm for Large-scale P2P systems", Journal of Software, June 2008, vol.19, pp.1473-1480. [5] Xu Yi, Wang JiaWei, "Self-adaptive Sharing Policy for Resources in Decentralized P2P Network", Computer Engineering in China, July 2010, Vol.36,pp.270-272.
[6]. Yu XiaoPeng, Zhang Yan, "Network Resource Sharing Research
[7]. Based on Decrease IPv6 P2P Technology", Journal of Jilin University (Information Science Edition) in China, May 2010, Vol.28,pp.284- 290.
[8]. https://www.slac.stanford.edu/grp/scs/net/talk/ornl-96/ornl.html
[9]. list more than three books or published articles. The format for listing publishers of a book within the biography is the title of a book (city, state: publisher name, year) similar to a reference. The current and previous research interests ends the paragraph.
[10]. The third paragraph begins with the author's title and last name (e.g., Dr. Smith, Prof. Jones, Mr. Kajor and Ms.Hunter). List any memberships in professional societies other than the IEEE. Finally, list any awards and work for IEEE committees and publications. If a photograph is provided, the biography will be indented around it. The photograph is placed at the top left of the biography. Personal hobbies will be deleted from the biography.