Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 5, May 2013, pg.50 – 55

RESEARCH ARTICLE

MONITORING LOCAL AREA NETWORK USING REMOTE METHOD INVOCATION

Harsh Mittal[1], Manoj Jain[2], Latha Banda[3]

[1]Student of masters of technology Computer Science, Department of Computer Science and Engineering, Lingayas University, Faridabad, Haryana, India

[2]Assistant Professor, Department of Computer Science and Engineering, Lingayas University, Faridabad, Haryana, India

[3]Assistant Professor, Department of Computer Science and Engineering, Lingayas University, Faridabad, Haryana, India

[1] harsh.mittal207@gmail.com; [2] manojjain1972@gmail.com; [3] latha.banda@gmail.com

Abstract— The project aim is to secure the network or a LAN by implementing such a software which is enable to carry out operations which are capable to monitor whole of the network ,sitting on one chair by viewing remote desktop ,passing messages to remote system and is also able to shut down the system by performing remote aborting operations . This software is purely developed in JAVA RMI (REMOTE METHOD INVOCATION). This project is to provide the maximum details about the network to the administrator on their screen without knowing them their users. The administrator can view the static image of client's desktop and then he/she could sends warning message to the user to stop that operation immediately. Even than if client do not stops than administrator has the facility to abort the system remotely or restart the system whatever necessary he thinks.

Key Terms: - Monitoring; RMI; Java; LAN; Security

I. INTRODUCTION

Today the Today the world is rapidly changing the statement "We are in the world" to "world is in our hand" [1]. The main aim of our project is to control and monitor the LAN network where technique used to do so is RMI. Remote Method Invocation (RMI) allows a java object that executes on one machine to invoke a method of a Java object that executes on another machine. This allows us to build distributed applications. Before the use of client and server, the necessary stub is generated. Generation of the skeleton may be required. In the context of RMI, a stub is a java object that resides on the client machine. Its function is to present the same interfaces as the remote server. Remote method calls initiated by the client are actually directed to the stub. The stub works with the other parts of the RMI System to formulate a request that is sent to the remote machine. A remote method may accept arguments that are simple types or objects. In the latter case, the object may have references to other objects .All of this information must be sent to the remote machine. That is, an object passed as an argument to remote method call must be serialized and sent to remote Machine. Hence administrator can view the static snapshot of users' desktop and then he could sends warning messages to the user to stop that operation immediately.

1.1 Network Monitoring

Network monitoring describes the use of a system that constantly monitors a computer network for slow or failing components and that notifies the network administrator. While an intrusion detection system monitors a network for threats from the outside, a network monitoring system monitors the network for problems caused by overloaded and/or crashed servers, network connections or other devices [2].

1.2 Java RMI

Java Remote Method Invocation (RMI): Java RMI is a mechanism that allows one to invoke a method on an object that exists in another address space. The other address space could be on the same machine or a different one. The RMI mechanism is basically an object-oriented RPC mechanism CORBA is another object-oriented RPC mechanism [3].

There are three processes that participate in supporting remote method invocation.

- The Client is the process that is invoking a method on a remote object.
- The Server is the process that owns the remote object. The remote object is an ordinary object in the address space of the server process.
- The Object Registry is a name server that relates objects with names. Objects are registered with the Object Registry. Once an object has been registered, one can use the Object Registry to obtain access to a remote object using the name of the object [8].

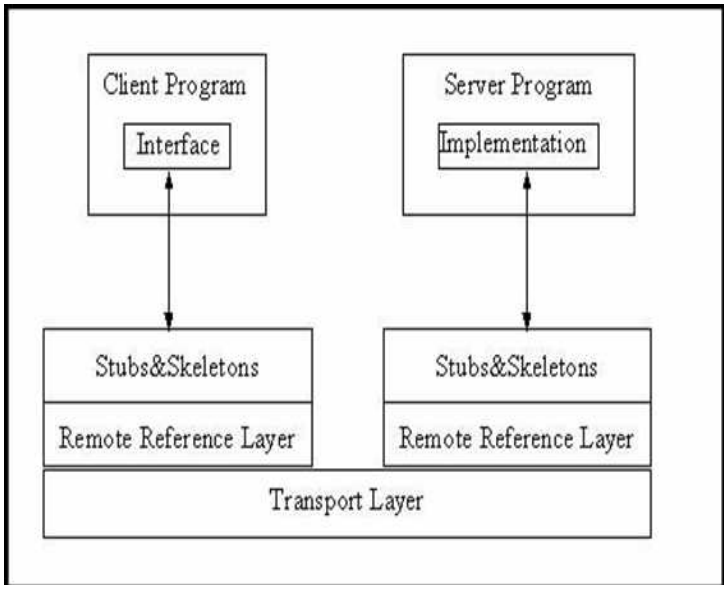

Fig.1 Layers in Java RMI

Figure.1 shows how each of the layers could be enhanced or replaced without affecting the upper layers. The first is the stub and skeleton layer, which lies just beneath the view of the developer. This layer intercepts method calls made by the client to the interface reference variable an redirects these calls to a remote RMI service. The next layer is the remote reference layer. This layer understands how to interpret and manage references made from clients to the remote service objects. The Transport Layer is based on TCP/IP connections between machines in a network. It provides basic connectivity, as well as some firewall penetration strategies.

1.3 LAN SECURITY ISSUES

Today the IT managers face five LAN security issues [4]:

- *Porous perimeters*— The conventional approach to enterprise security has been to apply security at the perimeter of the network. Today, however, perimeter defenses are no longer sufficient. Increasingly, sites no longer consist just of predictable managed desktops but include a mix of unmanaged mobile devices, such as laptops and PDAs. Sometimes these devices belong to employees, but often businesses must allow guests such as contractors, partners, and others with unmanaged mobile devices to directly connect to the internal network. These devices may be infected with malware and thus could inject a worm, bot, trojan, or other malware directly into the access port of the corporate network, bypassing perimeter defences [4].

- *Increasingly sophisticated attack*-- Perimeter-based security strategies are also no match for the increasing sophistication of attacks on the network. The hacker profile has begun to shift from adolescents crashing systems for fun to professional criminals bent on taking over systems for profit[4].
- *Unaudiable network*-- Many enterprises built LANs with the assumption that internal users are trustworthy. Little thought was given to understanding exactly what devices are connected to the network, where these devices are located, and what users are doing with them. As a result, enterprises are finding themselves ill-equipped to deal with problems introduced by mobile end systems and end users[4].
  Furthermore, the increasing number of regulations on data protection and compliance verification, including privacy, financial, health records, state information processing laws, and even anti-terrorism acts, has raised the importance of auditing network activity[4].
- *Uncooperative client*-- Even with security awareness programs and employee censure for lax security practices, users still view security as something that gets in the way of doing their job. Users will often abort full disk scans, or even disable anti-virus or anti-spyware applications, if they believe they measurably slow down the computer.
  Network access control mechanisms that perform periodic integrity re-assessments and policy compliance verification, and that have the ability to isolate an endpoint that fails, can mitigate the potential damage done by uncooperative employees [4].
- *Risky applications*-- New types of collaborative computing tools, such as Instant Messaging, VoIP, and wireless, are increasingly in demand, since they enhance productivity and allow users to be in touch 24x7. However, many of these tools bring with them increased security risks, primarily because their reach extends within and beyond the traditional network boundary. Exploiting vulnerabilities in these applications can provide hackers a fast path into the network. Many of these kinds of exploits are difficult to detect and control, since they tunnel over allowed protocols such as IM and HTTP, and traditional firewalls cannot distinguish them from benign traffic[4].

II. FEATURES CONTROLLED BY PROPOSED SYSTEM

*2.1 NET VIEW***:** Get on your screen, the list of entire client's in LAN. Keep pinging every time to check the latest status of the PC's.

*2.2 PROCESS VIEW***:** Get the details of all processes running on the client's machine, by viewing the static image of the client's desktop.

*2.3 CHAT PROCESS***:** If the server finds anything illegal then server has a facility to send the warning message to the client.

*2.4 SHUT DOWN***:** Shut down the client's machine by server.

*2.5 RECORDS***:** When the server shut down the client's machine, at that instant of static image has saved to the database as a record.

III. ARCHITECTURE OF THE PROPOSED SYSTEM

Server gets the IP addresses of all the client's connected to the LAN using Remote Method Invocation (RMI). There is one more advantage of using RMI is that suppose you are using wireless network like WiFi then also you can get the IP addresses of client's and keep pinging every time to check the latest status of the LAN.

There is client server architecture between clients and server but to get the static image of client's without knowing them, this is not satisfactory. We need another client application which runs on client's machine and one server application which runs on server machine. Both these application start working when the system is started and these applications are running in the background doesn't know anything about it.

By viewing the static image of the client's desktop, the server can judge that is there anything illegal or out of the range of client's privilege are running on the client's desktop. If it is then the server has a communication facility and the server communicate with the client's by sending warning massages. The client cannot send back or communicate to the server. The communication is unidirectional, it is not two way.

When the server shutdowns the client's machine; at that instant of client's machine image is also saved to database. This will reduce the size of the database; we can save only those images when the server chats or shutdown the client. Rest of the images are discarded. This database is used as a record by the server for why the client's machine is shutdown.

Server is provided with a GUI based application in J2ME to send command message instantly. Server sends command to the client like Get IP list, chat, shutdown.

LAN monitoring using RMI technology can be used in offices, malls as well as school, colleges or university level.

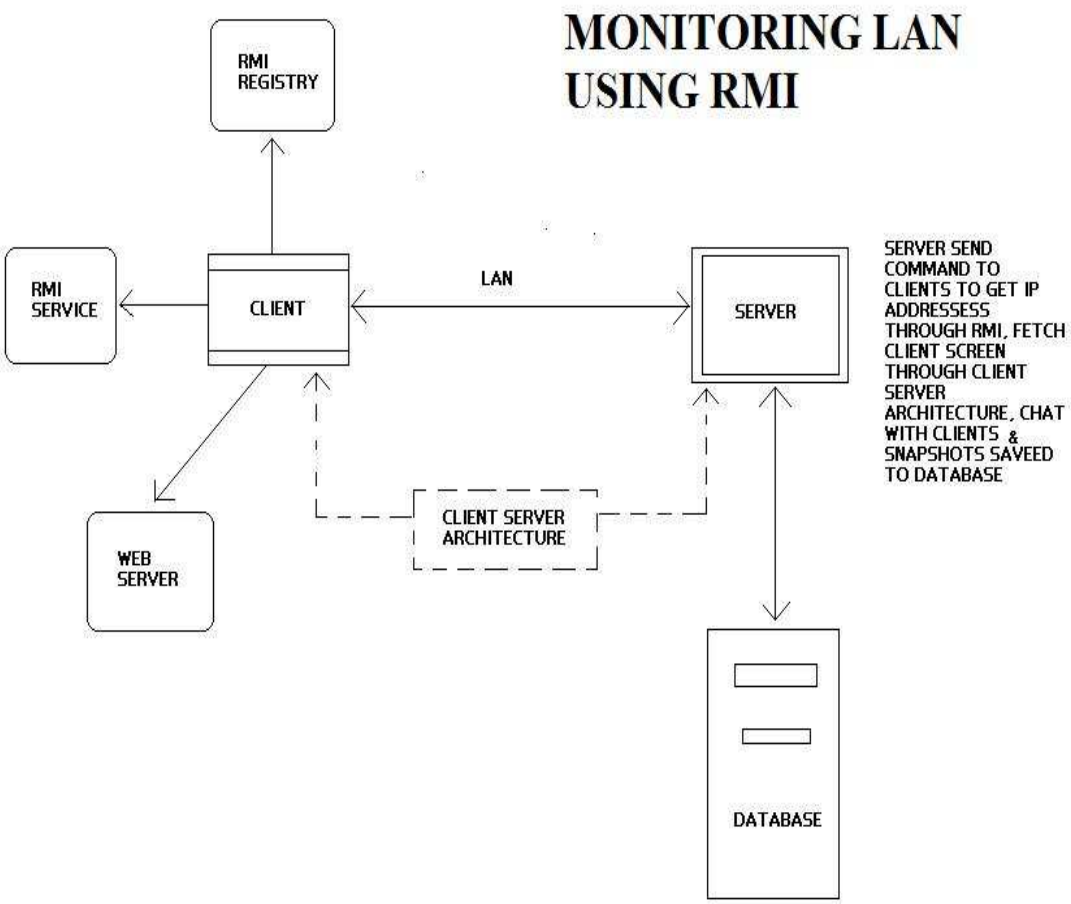

Fig.2 Architecture of monitoring LAN using RMI

IV. BLOCK DIAGRAM OF PROPOSED SYSTEM

From the block diagram of proposed system we see that the main server has the power or authority to monitor whole of the LAN. Server or administrator sends the request message to the client through RMI. But the client does not know there is a remote request came and without knowledge of client the automatically response message generate on behalf of request in the form of IP addresses and this will send to the server. Now with the use of client server architecture, the server gets the static image of any of the clients desktop. If server or administrator finds anything objectionable in the network or any particular system, an administrator has the power to abort that operation by sending warning messages to the user to stop that operation immediately. Even than if client do not stops than administrator has the facility to abort the system remotely or restart the system whatever necessary he thinks When the server shutdown the client, at that instant of images are saved to the database as a record.

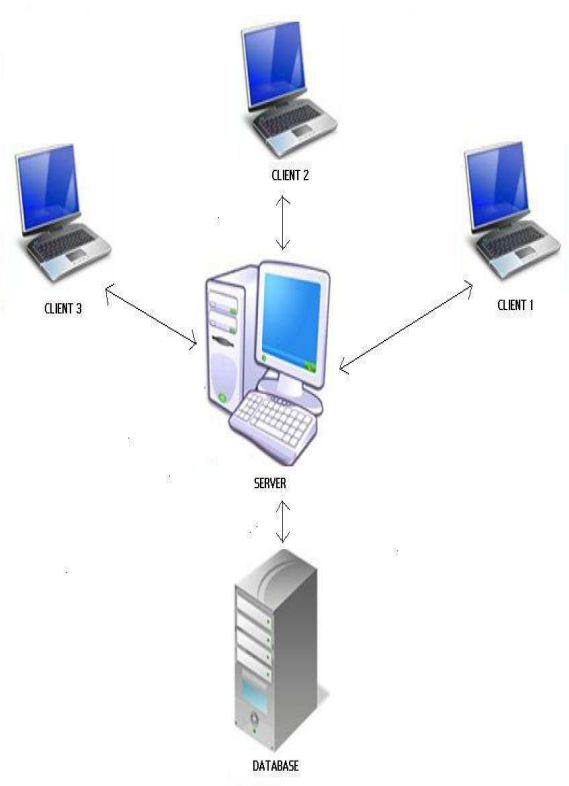

Fig.3 Block diagram of proposed system

V. TECHNOLOGY USED IN PROPOSED SYSTEM

In RMI based LAN monitoring system we use technology like

1. SERVLET: By using servlet in this system we communicate with client and server.
2. NET BEANS: For better programming we use net beans for designing this system.
3. PROCESS BUILDER: This class is used in this system which is very important to create operating system processes.
4. ABSTRACT WINDOW TOOLKIT: This is java's toolkit used for windowing, graphics and user interface creation for this system.
5. J2EE**:** It is collection of java programming API's used for java platform programs. It is used to program this system.

VI. APPLICATIONS OF PROPOSED SYSTEM

1. LAN monitoring at the office level can be used to monitor the office LAN by the administrator at any time. This project is to maintain confidentiality, integrity and availability of the network infrastructure. Server or administrator does not have to depend on any third party information regarding the LAN and can instead check the LAN status himself.

2. LAN monitoring at the school, university/college level can be used for monitoring, logging and retention of network packets that traverse university networks. The goal of this project is to maintain confidentiality, integrity and availability of the university network infrastructure and information assets.

3. LAN monitoring at the malls is used to monitor all information of malls by administrator at any time.

4. This LAN monitoring system is for monitoring multiple computers but this can also be used in homes to monitor children.

VII. CONCLUSION

This paper explains the basics of monitoring LAN using RMI. This paper on Network security works as security provider to whole of the network. This is a complete front end project build in JAVA RMI used to provide the authority to the administrator to stop any illegal process and make him enable to monitor whole of the LAN and the work carried on connecting nodes. The project consists of several boundaries or limitations beyond which the project yields erroneous results. Nonetheless the project serves the vast functionalities regarding its performance.

REFERENCES

[1] Wang Zhenqi and Wang Xinyu , The Research And Design Of Content-Based Network Monitor System, in 2nd International Conference on Power Electronics and Intelligent Transportation System, 2009.
[2] http://en.wikipedia.org/wiki/Network_monitoring
[3] http://www.eg.bucknell.edu/~cs379/Distributed Systems/rmi_tut.html.
[4] http://archive.itmanagementnews.com/itmanagementnews 5420060301TheTopFiveLANSecurityIssuesFac ing ITManagersToday.html.
[5] Covkun and Ardam, A Remote Controller for Home and Office Appliances By Telephone, IEEE Transactions on Consumer Electronics, Vol. 44, No. 4, NOVEMBER 1998.
[6] Dinesh C. Verma, Simplifying Network Administration Using Policy-Based Management, IEEE Network, March/April 2002.
[7] Allen Householder, Kevin Houle, and Chad Dougherty, Computer Attack Trends Challenges Internet security, IEEE Security and Privacy 2002
[8] Evangelos P. Markatos, Dionisios N. Pnevmatikatos, Web-Conscious Storage Management for Web Proxies, IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 10, NO. 6, DECEMBER 2002.
[9] Ninghui Li and John C. Mitchell, Securing Java RMI-based Distributed Applications, Proceedings of the 20th Annual Computer Security Applications Conference (ACSAC'04).
[10] L. Deri, nCap: Wire-speed Packet Capture and Transmission, IEEE 2005.
[11] Mamata Bhamare, Tejashree Malshikare, Renuka Salunke, Priyanka Waghmare, "GSM Based LAN Monitoring and Controlling", International Journal of Modern Engineering Research (IJMER), Vol.2, Issue.2, Mar-Apr 2012 pp-387-389 ISSN: 2249-6645.

