International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-3 Issue-11, April 2014

Pocket Droid – A PC Remote Control

Amogh Pendharkar, Preeti Sharma, Chhaya Varade, Rekha Jadhav

Abstract— In today's world, electronic devices and PC's holds a valuable position in ones' life. An important aspect of the technology is to remotely monitor these devices. We are aware of multiple Remote Control applications which provides an effective way to control and monitor devices easily and quickly. This paper proposes an idea for remote controlling of Android mobile devices, evaluating the network and obtaining the accurate and optimal solution in different cases. In this paper we have explored various importance of using Pocket Droid Application. One can use Pocket Droid to share files between PC and android device, activate and kill the applications installed on the Target PC, shutdown the Target PC and much more. Pocket Droid surrounds the Client and Server application. In which, the Server application has been implemented in JAVA and Client application in Android.

Keywords — Android phone, IP address, JAVA, Window OS, remote desktop, remote visualization, smart phone, wireless handheld devices.

I. INTRODUCTION

Today, the world is rapidly changing the statement "We are in the world" to "World is in our hands". To control and monitor the LAN network from our wireless handheld device i.e. cell phone from anywhere irrespective of distance. Say, you have a LAN setup at your office. Sitting at home you want to learn the LAN status. You can do so by storing this project in your cell phone and executing the same. With this evolution comes the need to integrate these devices with others so they can take actions. Technological development has improved the capabilities of mobile devices with varieties of technical features that previously conceived only in PC architectures. With the advent of Pocket Droid, there is a need to integrate these devices so that interaction between the PC and mobile can be monitored and effective interaction can be accomplished. This paper proposes the implementation of mobile based PC control system using android software [3].

II. RELATED WORK

Extending the Wireless LAN (WLAN) to be a core technology will mean providing granular WLAN authorization and access control. In this guide, learn about Wireless LAN access control, as well as managing users on guest wireless networks and controlling Wi-Fi embedded devices on the WLAN [4].

Manuscript published on 30 April 2014.
*****Correspondence Author(s)
Amogh Pendharkar, Student, Bachelor of Engineering, Information Technology, G. H. Raisoni Institute of Engineering & Technology, Pune, India.
Preeti Sharma, Student, Bachelor of Engineering, Information Technology, G. H. Raisoni Institute of Engineering & Technology, Pune, India.
Prof. Chhaya Varade, Department of Information Technology, G. H. Raisoni Institute of Engineering & Technology, Pune, India.
Prof. R. P. Jadhav , Department of Information Technology, G. H. Raisoni Institute of Engineering & Technology, Pune, India.

While WLANs were once used to offer network access to guests or employees in common areas, they are now often extended to reach every laptop and desktop in the enterprise. What's more, they also support both corporate and personal smart phones and tablets, as well as embedded Wi-Fi devices, such as copy machines and surveillance cameras. With all these users and clients, network managers must implement granular WLAN access control and network authorization [4][8].

III. FLAWS IN CURRENT SYSTEM

Old methods of securing guest wireless networks are no longer sufficient. Once upon a time, wireless guest networks were given their own service set identifiers (SSIDs) and mapped onto an isolated Ethernet VLAN. HTTP requests from newly connected clients were sometimes redirected to a captive portal, where guests had to accept "terms of service" before being released onto the Internet. This left the door open for infected devices to access the guest SSID and the VLAN. It also left that captive portal open for attack. As a result, enterprises must consider other methods for securing these networks. A number of companies sell equipment that comes with built-in guest management [4][7]. This equipment requires users to sign in and create accounts, and allows enterprises to create walled-gardens of access depending on their own user policy. Captive portals can require guests to run anti-virus programs, and they allow the IT team to configure permitted destinations, ports and URLs tied to bandwidth limits and priorities. Companies can also integrate a NAC or IDS product to do checks on wireless guest networks.

IV. FEATURES OF POCKET DROID

[1] Net View: It will show list of Computer in network.
[2] Process List: It will display list of processes in computer.
[3] Activate Process: It will run new process on client machine.
[4] Kill Process: It will kill process on particular client machine.
[5] Shut Down: It will shut down the client machine.
[6] Image Capture: It will take the screen shot of the Desktop on phone.
[7] Send Message: We can send message to the machine selected.
[8] View Screenshot: View Remote Computer Screenshot.
[9] Detect Removable drives: detect external devices connected to client computers.
[10] Virus Detection: Getting alert notification if PC consists of some malicious data.
[11] Message Broadcasting: Sending messages to client PC.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

V. ARCHITECTURE

Figure (b) shows the internal software structure of the client side and server side of Pocket Droid System. Each side is divided into well-defined components and their functionalities. Client is an android device which controls the remote PC. Query is fires using SQLite database whenever client wants the list of PC. There are mainly two servers present in our system: One is the main server who handles the requests from the android device and the other one communicates with the PC's present in the LAN. Database contains only one table which stores the IMEI number of mobile phone.

A. General Users:

These types of user can be a client. They can communicate among themselves. They cannot modify or delete content of another computer.

B. Admin:

Admin is the user who can monitor complete LAN system using cell phone.

C. Server Program:

This is the communication medium program between Admin and clients.

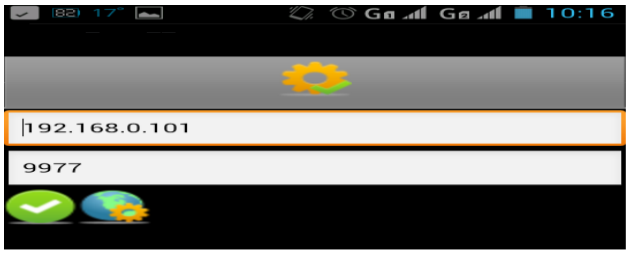

Fig (a) Remote display of android device.

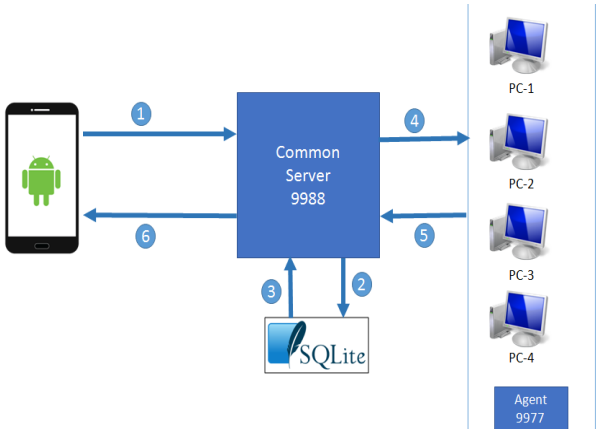

Fig (b) Architecture of Pocket Droid

VI. DESIGN AND IMPLEMENTATION

The system basically involves communication between an android phone and a remote desktop. Errors that occur during processing should be resolved and solved out. The screen resolution should be visible enough to admin. Different types of exception should be handled appropriately.

A. General Constraints:

[1] Network Speed— As number of PC increases in LAN, it introduces an additional overhead on network bandwidth.

[2]Processing speed— processing speed depends on the network connection.

B. Assumptions and Dependencies

[1] User must have basic knowledge of computer.
[2] Must be familiar with basic concepts of Networking and communication.
[3] Speed of the recognition may be depending upon the network traffic.
[4] Screen resolution depend totally depends upon hardware
[5] Admin cell phone should be WI-FI enable.
[6] Cell phone should be compatible with Android.

VII. FUTURE WORK

As a continuation of work in this application, we would include remote monitoring of PC's thought GPRS network and to include the encryption algorithm to prevent data leakage. We will also put efforts for displaying the screen of the target PC on the android phone itself for the purpose of better visualisation.

VIII. CONCLUSION

This paper describes an architecture which will control the multiple PC using android mobile phones. Thus the application does not require any additional equipment or software and the application will work fine irrespective of environmental factors and the server is used in Linux or Windows platform. Security will be maintained on the client side as android phone that needs permission for internet access. The application thus will be beneficial for different Network communications carried out in an industry.

REFERENCES

1. A Framework for Wireless LAN Monitoring and Its Applications Department of Computer Science, University of Maryland College Park, MD 20742
2. Remote Control of Mobile Devices in Android Platform Angels Gonzalez Villan Student Member, IEEE
3. 2010 International Conference on Information and Network Technology (ICINT 2012) IPCSIT vol. 37 (2012)) © (2012) IACSIT Press, Singapore
4. http://developer.android.com/guide/basics/what-is-android.html Retrieved 3rd Sep, 2011.Android. http://www.android.com Retrieved 3rd Sep, 2011.
5. Enterprise Wireless LAN security and WLAN monitoring http://www.airdefense.net/.
6. Wireless Security Auditor (WSA)
7. http://www.research.ibm.com/gsal/wsa/
8. Android. http://www.android.com Retrieved March 1st, 2011.
9. Gmote. http://www.gmote.org/ Retrieved 21st Aug, 2011.
10. Remote Droid. http://remotedroid.net/ Retrieved 23rd Aug, 2011.
11. IEEE Computer Society LAN MAN Standard Committee,IEEE 802.11 Management Information Base In IEEEStd 802.11-1999,1999.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)