ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 6, November 2013

Creating an Intelligent Environment in Mobile Technology

Priyanka V. Kampasi, Y. C. Kulkarni

Abstract: ***In this paper, we propose an intelligent system comprising of an Android based mobile phone and a workstation. The mobile phone will not only act as a tool for remotely handing the various software applications in the PC but also be used for handling the hardware components. Recently the mobile phones have been used for handling PC but only when it is in on state and it has to be reset manually if it hangs during operation. Therefore, in this paper, we not only propose various modules or functions that can revolutionize the PC to Cell phone communication but also try to start and reset a switched off workstation through a cell phone. The system is basically focused for those people who travel around the globe and need to be consistently connected to their workplace or home pc at the same time.***
The proposed system has a great potential and it will benefit the software engineers for a long time.

Keywords**: Android OS, Cell Phone, GSM Modem, Microcontroller, Microprocessor, PC/Laptop.**

I. INTRODUCTION

We know that nowadays there is a common saying-'life without a cell is hell'. It means that just like food, water and clothing, a cell phone has also become the necessity of life. It is used by almost everybody today. The use of mobile phones has revolutionized the growth of technology. However, the perception of Cell phones has changed drastically with the invention of Android based OS for the mobile phones. Earlier the mobile phone was used only as a means of communication but with the use of Android OS, the potential of mobile phones has increased manifolds. Android OS provides us with platform through which we can operate various other devices like televisions and PCs through a mobile phone. Android is a powerful operating system enhancing the features and capabilities of cell phone by providing a range of applications and thus turning it into a Smart phone. Some of the current features and specifications of Android are:

1. GSM Technology
2. Dalvik Virtual Machine- it is optimized for mobile device.
3. Integrated browser- it is based on open source web kit engine.
4. Application Framework- it enables reuse and replacement of components.
5. Optimized graphics- it is peered by custom 2D and 3D library
6. Media Support
7. SQLite
8. Bluetooth, EDGE,3G, Wi-Fi, camera, GPS, compass etc.[2]

Android software stack provides various packages for networking and it also provides high performance for android cellular mobiles. VNC architecture and VNC protocols are used for client and server transactions. Other aspect to be considered is the remote visualization mechanisms that are useful to achieve a remote display to other devices. This is possible through Visual Networking Computing. VNC is a graphical desktop sharing system providing remote control via network. It allows capturing a mouse and a keyboard.[3] Everybody these days possesses a Mobile Phone. As they are small in size and easily portable, they become a smarter choice for accessing the remote desktop or a laptop rather than carrying it. This paper proposes the use of Mobile Phones (equipped with Internet features) by the IT professionals to access their office computers after proper authentication check.

The overall system will require hardware components like a Modem, Microcontroller, Microprocessor and a USB Port to accomplish this task. For secure transmission of data between the cellular device and the PC, encryption algorithm (SHA 1) will be used.

Apart from this, we can also implement our system to make our Mobile phone act as a remote control for switching on or off the lights, adjusting the thermostat of our AC. It could also be used for indicating the temperature in high temperature zones like Nuclear Reactors, chemical laboratories etc.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 6, November 2013

II. PROPOSED ARCHITECTURE

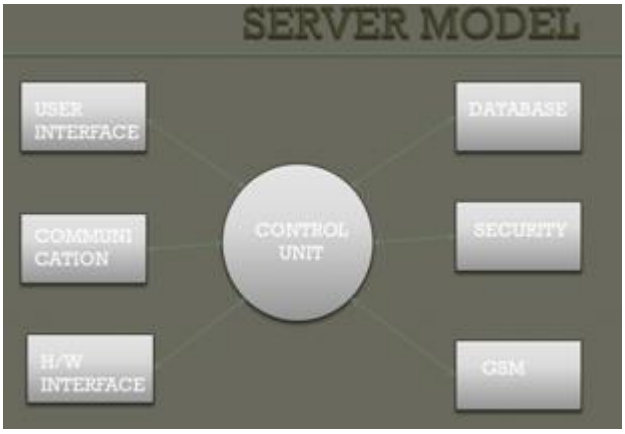

Fig.1. (a) Modules of the Server (DFD)

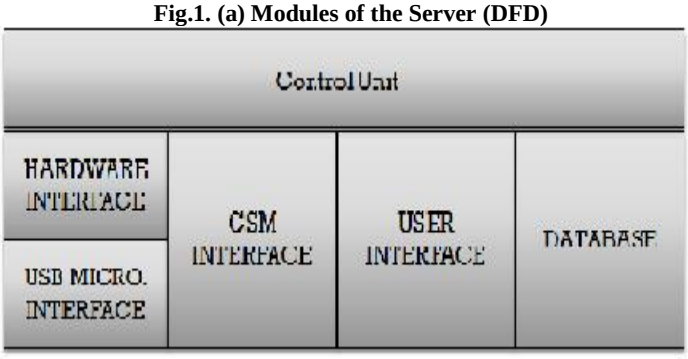

Fig.1. (b) Modules of the Server (Block Diagram)

The system proposed in this paper will contain both hardware and software modules. The hardware will comprise of a GSM modem, microcontroller, microprocessor, an android based mobile phone and a CPU/laptop. The software modules will be created using extensive java libraries. A client application will be present on the Smart phone and the process will begin when an authorized user will enter a password in that application and give a command to switch on the computer. The system will first verify the password given by the user and if found authentic, a switched off computer machine will be automatically switched on. This will be enabled with the help of GSM modem, microcontroller and a microprocessor. Once the computer is in ON state, the system will automatically generate a OTP(one time password) and send it to the authorized user via an SMS. This password will be encrypted for security reasons using a very powerful encryption algorithm SHA1.

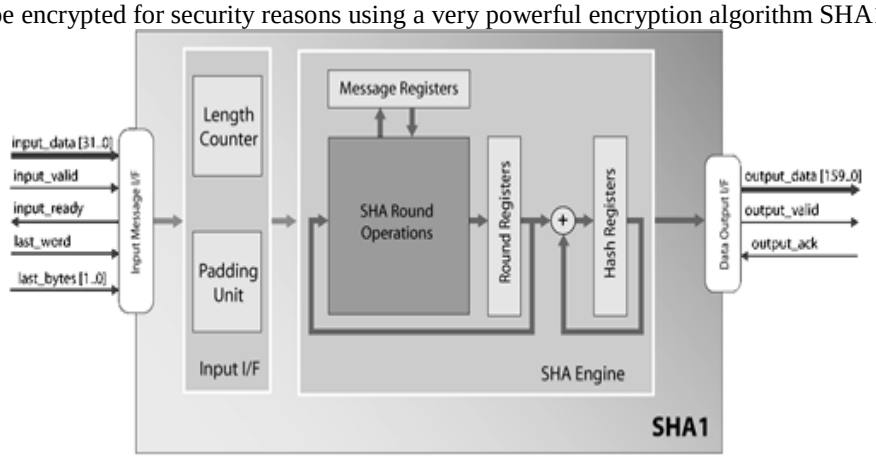

Fig.2. Working of SHA Algorithm

Image Source
http://www.cast-inc.com

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 6, November 2013

The SHA1 core is a high-performance implementation of the SHA-1 Secure Hash message digest Algorithm. This one-way hash function conforms to the 1995 US Federal Information Processing Standard (FIPS) 180-1. It accepts a large, variable-length message and produces a fixed-length message authorization code.

The core is composed of two main modules, the SHA1 Engine Module and the Input Interface Module as shown in the block diagram. The SHA1 Engine Module applies the SHA1 loops on a single 512-bit message block, while the Input Interface Module performs the message padding. The processing of one 512-bit block is performed in 82 clock cycles, and the bit-rate achieved is 6.24Mbps/MHz on the input of the SHA1core.The SHA1 core is equipped with fully-stable input and output interfaces. These enable the user's application to stop the input stream according to a data arrival rate, or to stop the output stream when the core is not able to receive data. On receiving a password through an SMS, the authorized user will feed it to his client application therefore enabling his application to access the computer services. As soon as the system is connected, the data transfer can take place. For providing security to the data transmission also SHA will be used.

III. SYSTEM ARCHITECTURE

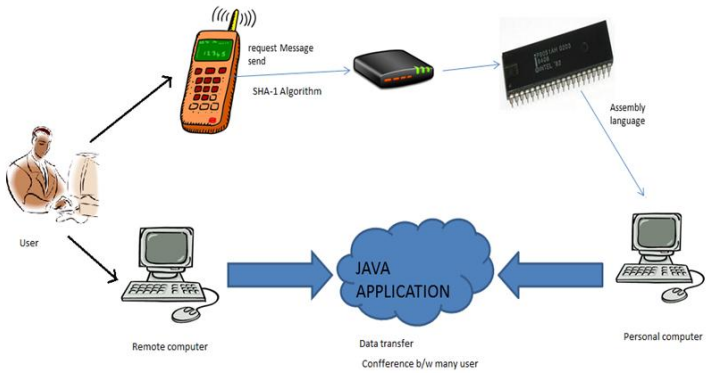

Fig. 3 System Overview

The proposed system will contain various hardware and software modules like Workstation control(power on and reset), Client Authentication, SMTP mail sending, File Transferring, Screen Capturing, Mouse Commands and Keyboard Controls, Application Shortcuts.

1. Power On and Reset:

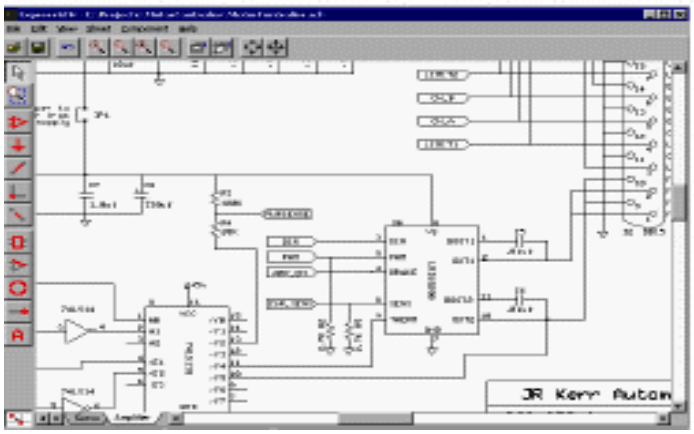

Fig. 4. Circuit diagram showing Hardware control

If the laptop or pc is in the switched off mode and we want to access its services, then the cell phone device can automatically switch it on without any human interference.

Also, if it gets hanged during any operations, then also it can be reset without physically touching the computer.

2. Client Authentication:

This module will check the authenticity of a user based on his/her login credentials. The user will be allowed to enter into the system and access the system services only after successful login. This module ensures the security features of the system.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 6, November 2013

3. SMTP mail sending:

This module will enable a Smart phone to send emails to various recipients even if it is not connected to the internet. Java extension libraries have been used for creating this module. The user only needs to mention the recipients email id and write the mail, rest all will be managed by the software module i.e., connecting to the SMTP server and dispatching the email.

4. File Transferring:

This module will transfer any presentations or files from the user's pc or laptop onto his mobile phone very fast and efficiently without use of any external device like a pen drive or a CD.

5. Screen Capturing:

Desktop sharing commonly refers to a remote frame buffer technology. Desktop sharing allows a user to send screen data to be drawn elsewhere and receive input remotely. Its applications vary from remote system administration to accessing virtual machines. This module will allow capturing of the desktop on our mobile phone. Then we can control our pc from anywhere anytime through the cell phone.

6. Mouse Commands:

This module enables us to give mouse commands to the pc through our mobile phone. The commands like right or left click, mouse drag and drop capabilities can be accomplished by keys of the mobile phone.

7. Keyboard Control:

For accessing any icons/folders/application programs on the laptop or pc we make use of keyboard. In this module, these files or folders can be accessed or manipulated using the Cell phone. The keypad of the mobile phone will impersonate as a keyboard used for a pc.

8. Application Shortcuts:

This powerful feature enables us to access various applications just a click away in order to save time. Just like in mobile phones, there is a concept of speed dial where in a mobile number can be represented by a single digit; similarly this module will make a short cut for an application. Whenever, the user wants to access that application, he only needs to press a single key from his/her cell pad and the application will get opened.

IV. LIMITATIONS

- The limitations of the proposed system will be that additional hardware components are required for its working.
- The current size of the files to be transmitted via this application can't be more than 1 MB because of the RAM limitations.

V. FUTURE SCOPE

As the proposed system uses only password based authentication mechanism for implementing the security feature, in future, we can use face recognition biometric system for enhancing security. This may involve sending a user's picture or facial details along with the password to the application for authentication. This may involve calculating the distance between specific facial features like nose to ear length or ear to ear length, facial skin texture etc. The application will calculate these measurements and compare them with the already existing data stored in the database and allow authorization only incase a match is found.

Fig.5. (a) Facial Recognition

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 6, November 2013

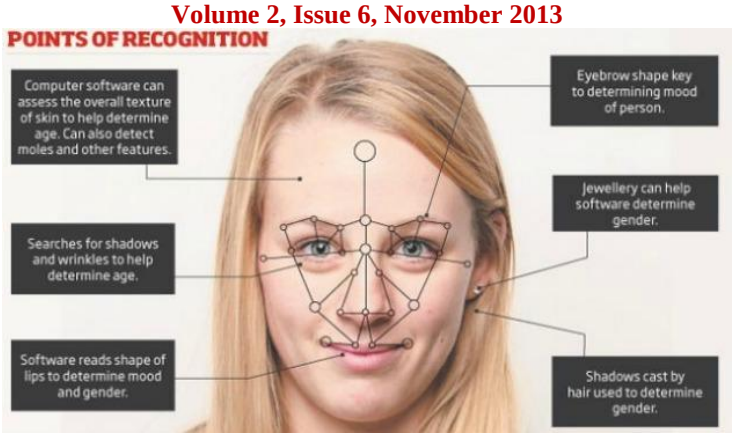

Fig.5. (b) Calculating Biometric Features

Image Sources
http://getandroidstuff.com
http://www.siliconrepublic.com/innovation/item/25335-17-year-olds-facial-recogn

Apart from this, we can also implement our system to make our Mobile phone act as a remote control for switching on or off the lights, adjusting the thermostat of our AC. It could also be used for indicating the temperature in high temperature zones like Nuclear Reactors, chemical laboratories etc (some work has already begun in this domain).

REFERENCES

[1] Two Factor Authentication Using Mobile Phones Fadi Aloul,Syed Zahidi, Wassim El-Hajj.

[2] Remote computer access through mobile phones IJCSI Issues, Vol 9, Issue 5, No.3, September 2012.

[3] PC Application Remote Control via Mobile Phones International Conference on Control Automation and Systems, October 2010.

[4] Towards Ubiquitous Computing via Secure Desktop Service Pan-Lung Tsai, Student Member,IEEE, and Chin-Laung Lei, Member , IEEE.

[5] A Herzberg,"Payments and Banking with Mobile Personal Devices", Communications of the ACM, 46(5), 53-59, May 2008.

[6] J. Brainard, A. Juels, R. L. Rivest," Fourth Factor Authentication": ACM CCS, 168-179, 2010.

[7] National Institute on Standards and Technology Computer Security Resource Center, NIST's Policy on Hash Functions, March 29, 2009.

[8] Niels Ferguson, Bruce Schneier, and Tadayoshi Kohno, Cryptography Engineering, John Wiley & Sons, 2010.

[9] A. Josang and G. Sanderud, "Security in Mobile Communications: Challenges and Opportunities" in Proc. Of the Australian information security workshop conderence on ACSW frontiers, 43-48, 2003.

AUTHOR BIOGRAPHY

Ms. Priyanka V. Kampasi (B.E Computer) is a lecturer in Information Technology department of Bharti Vidyapeeth's Jawaharlal Nehru of Technology currently pursuing MTech from BVDUCOE. She has 6 years teaching experience. She has already written 3 technical research papers which have been published in various renowned International Journals.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 6, November 2013

Mrs. Y. C Kulkarni is an assistant professor in Information Technology department of Bharti Vidyapeeth's Deemed University College of Engineering. She has teaching experience of 24 years.