International Journal on Applications in Basic and Applied Sciences
Volume 1: Issue 3: March 2015, pp 11-15. www.aetsjournal.com

Exploiting GSM on Android Mobile Devices for Home Security Application and devices

[1]R. Arun Prakash, [2]S. Kishore Kumar & [3]Prof. R. Selvarasu

[1,2]UG Students, [3]Head of the Department
Arunai Engineering
College Department of
Electronics and Instrumentation
Engineering
Tiruvannamalai - 606603
arunboss996@gmail.com,kshr.newzea@gmail.com,selvarasunaveen@gmail.com

***Abstract*— A Home Automation Technique based on ARM controller. This technique has an IR sensor to detect the person. If the IR sensor detects a person then the keypad will be activated to enter the pass code. A SMS will be sent to the owner for authentication. Depending on the owner's replay the door will open. If the person enters a wrong password, an intimation message will be sent to the owner and at the mean time buzzer will be activated. Android app is used to control the lamp. The firmware for this project is written in embedded 'C' language and the machine codes for the program are stored in the non-volatile Flash memory of the embedded controller.**

***Keywords*— Android, GSM, Stepper Motor, Memory and Sensor.**

I. INTRODUCTION

To make calls will also be utilized for remote switching and control activities. [4] the security of one's belonging once someone leaves his\her home is continually a priority with increasing variety of incident of larceny theft etc…, several machine controlled system has been developed that informs the owner in an exceedingly remote location concerning any intrusion or commits to intrude within the house [5].this survey paper provides a concise Today, the mobile device have been integrated in to our everyday life. Consequently home automation and security or becoming increasingly prominent features on mobile devices commands to lock, unlock, or check the status of the door. [1], this flexible home control and monitoring system control using an embedded micro-web server, IP connectivity for accessing and control devices and appliances remotely using android base smart phone app[2].

The main plan is to mechanically management and the monitor electrical and electronic appliances. consistent with the marketing research firm ABI regarding four million home automations systems were oversubscribed globally in 2013 [3].

Mobile phone industry is classified among the fastest growing engineers branches.it has to be exploited for vast applications. Reliability and affordability. mobile cellular home subscribe have reached saturation point with such information the basic cell phone that was mainly utilized overview of mobile network security attack vectors using the back end system and the web browser, but also the hardware layer and the user as attack enable. We show different and similarities between normal security work and the mobile security [6]. In the java enabled android smart phone under GSM cellular communications serves as a remote control tool by interacting with a system made by ARM microcontroller and GSM modem, which will be sending short messages to user's mobile cell phone in case of intrusion [7].

In the remote monitoring system based on SMS and GSM was implemented. Based on the total design of the system, the hardware and software designed. In this paper the GSM network is medium for transmitting the remote signal .this includes two parts that are the monitoring centre and the remote monitoring station .the monitoring centres consist if a computer and communication module of GSM [8].in this work, the security of SMS in GSM network has been discussed especially for the use of SMS as such business tool. Here, we have introduced the complete security solutions.in this system we have a security scheme for improving the SMS security [9]. Das *et al* discussed the use of motion detectors and webcams for remote surveillance in the home, along with the ability to control appliances. The system streamed video to a mobile device when a motion detector was set off. The mobile device could also control any appliances integrated into the smart home system through the X10 technology [10]. Piyare and Tazil described the implementation of home automation through Bluetooth on Symbian phones. Since Bluetooth has become so prevalent in mobile devices, it was seen as a simple, secure, and low cost solution for wirelessly connecting a mobile device to a

home automation system [11]. This paper is the extension of your previous work and presents a low cost and flexible home control and monitoring system using an embedded micro-web server. With IP connectivity for accessing and controlling devices and appliances remotely using android based smart phone apps [12].

II. System Design

A. GSM on Android Mobile Devices

GSM (Global System for Mobile communications) is the technology that underpins most of the world's mobile phone networks. The GSM platform is a hugely successful wireless technology and an unprecedented. Story of global achievement and cooperation. GSM has become the world's fastest growing communications technology of all time and the leading global mobile standard, spanning 210 countries. Today, GSM technology is in use by more than one in five of the world's population – by mid-March 2006 there were over 1.7 billion GSM subscribers, representing approximately 77% of the world's cellular market. The growth of GSM continues unabated with almost 400 million new customers in the last 12 months. The progress hasn't stopped there. Today's GSM platform is living, growing and evolving and already offers an expanded and feature-rich 'family' of voice and multimedia service.

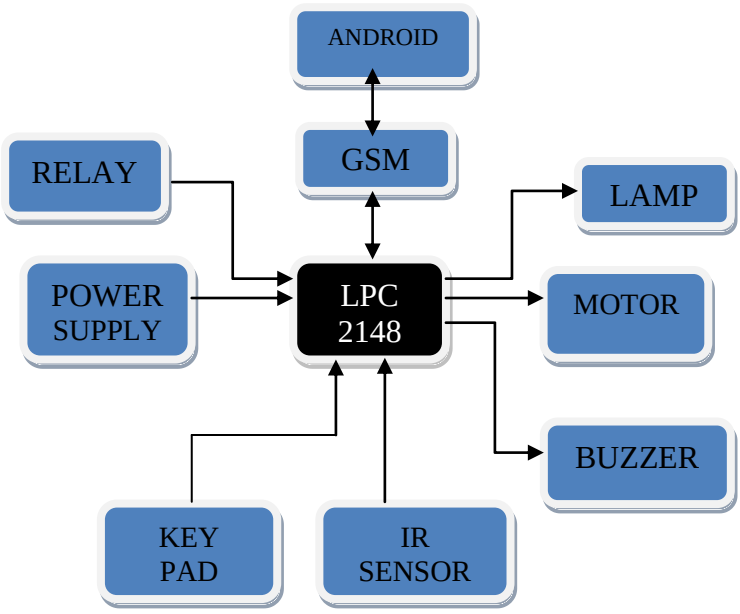

Fig. 1 (a) diagram of home security using GSM on Android mobile devices

While a piconet acts as an infrastructure mode network, multiple piconets can create an ad hoc network because the master of one piconet can be a slave in another. To avoid interference and collisions, GSM uses an adaptive pseudo-random frequency hopping technology that is synchronized to the master's clock. Bluetooth offers four security modes based on use of a mutual pin entered into both devices. Authentication and encryption/decryption keys are made after devices are paired with the appropriate pin. GSM development capability was officially added to the Android operating system with the release of the Android 2.1 API. Before this release, there was an API add-on for developers who wished to use GSM in their applications, but has fallen out of use in favour of the official GSM API software. To use Bluetooth in an application, a developer must declare the GSM and GSM ADMIN permissions in the application. Users will be notified of these permissions before download and must allow these permissions to continue downloading the application.

B. Home Security Controller

In-home Security Controller*:* Fig.1 illustrated the diagram of a home security system using android mobile devices. This project called for an Android smartphone or tablet with Bluetooth capabilities and a microcontroller security interface on the door to be secured. The testing device used was the Motorola Backflip running the Android 2.1 update, a personally owned device that was on hand. The in-home security interface of the door was made of several major components. An Arduino Mega2560 microcontroller was chosen for this project for the ease of programming and ability to quickly prototype. The Mega uses the Atmel ATmega2560 chip. A BlueSmirf gold Bluetooth transceiver [8] was chosen for communication because it came pre-packaged on a break-out board. As illustrated in Fig. 2b, door position was determined by use of a magnetic switch similar to those found on window alarm systems that was connected to the Arduino board. In addition to using the Android device to lock or unlock the door, a switch that used a physical key was installed in the door jamb along with status lights of the system. The locking mechanism itself was a linear actuator, originally purposed for use in the power locking mechanism of a car, and a set of transistors to reverse the voltage polarity and lock/unlock the door.

C. Android SDK and Arduino Firmware

Android uses a Java based language. To develop an Android app, a tool named Eclipse is required as well as Android's SDK [9], which is an add-on for the Eclipse program. When creating a new application for the

Android, the platform version must be selected, e.g. 1.5, 1.6, 2.1, or 2.2. However, the version can differ on the Android device depending on which Android device is being used.

The three main components required in the creation of the Android app are: the java file, which is a file that contains all code required for completion of desired tasks and functions; an xml file, which contains the layout for how the application will look to a user; and a resource folder, which contains all images, sounds, and graphics files needed for the application. For Arduino firmware, the IDE is provided as the open- source by the company [10]. The tool can run on multiple platforms, e.g. Windows, OS X, and UNIX. The language is a Wiring-based language which is similar to C/C++ style. Two programs were created for this project that had to be able to communicate with one another via Bluetooth channel. One was on the Android mobile device and other was on Arduino board inside the in-home security controller.

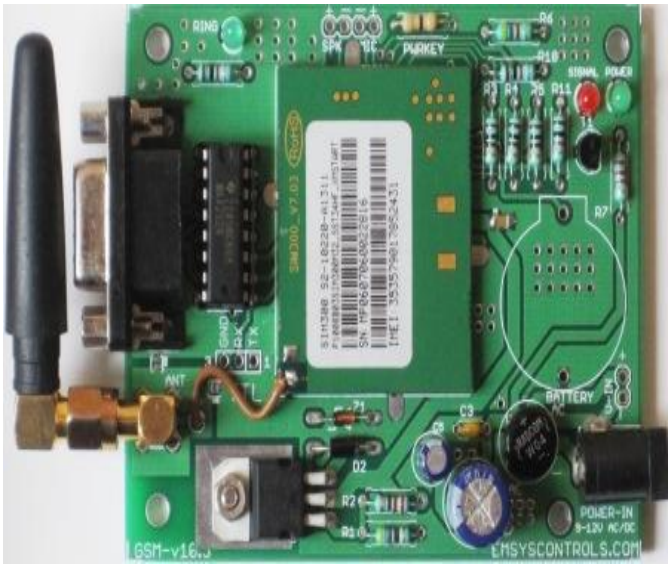

Fig. 2. (a) Screenshots of Android mobile application For home security

Fig 2(b) the wiring circuit of in-home security controller

They needed to be able to communicate with each other in a secure manner over short range. Bluetooth fulfils both these requirements and was used as the communication protocol for the project. The Android app was created in two major development steps. The first step had the MAC address of the microcontroller directly coded into the app for initial testing, and the second was an improvement of the first in that it allowed a user to search for the device, which becomes the final design. The basic steps for connecting to Bluetooth were the same for both versions of the application. To connect to Bluetooth, first one must connect to the Bluetooth radio by calling it as an adapter in the app source code. Then, once a device's address has been obtained, a variable associated with the device is created. This device variable allows for the creation of a socket, similar to what is seen in TCP connections. The socket is yet another object in the program, and has to be connected before communications can occur. The input stream reader and output stream writer objects were used to read and write data to the other program. Fig. 3 shows the snippet code of how to connect to a GSM socket in Android devices.

As shown in Fig. 2a, the finished application had two buttons and two menu options. The buttons were used to unlock/lock the door and to check the status of the door. One menu option allowed the user to search for devices and the other gave more information about the application. An image of a lock that changed based on door status was also put on the application to give a visual representation of the last status of the lock. Fig. 4 shows the procedure on Android devices for checking the status and waiting for reply. The application would take two steps to lock/ unlock the door or one to

check the status. When the lock/unlock button was pressed, the app would first send a check message to the door and wait for a response. The door would send back one of three responses, "locked" if the door was locked, "unlocked" if the door was unlocked, or "door" if the door was ajar. The app would then either alert the user by a toast popup message that the door was open or lock/unlock the door. The door was locked or unlocked by the commands "lock" and "unlock" respectively. Then the status of the door would be checked again to confirm the appropriate action had been taken. If the status button was pushed, then only the initial check of the door's status would be performed.

The door side programming, Arduino firmware, was by comparison much simpler because there was no graphic user interface to work with. The entire user interface consisted of the door, a keyhole, and two LEDs.

One LED was a power indicator, and the other was a door ajar indicator. This program continually monitored the door ajar switch when it did not receive any commands from the app. When a command was received and the door was confirmed as closed, the appropriate action would be taken. The system would either ignore the command if it was to already in the state requested by the app or it would actuate the locking pin appropriately. This is done by connecting the transistor array's bases to two pins on the Arduino. Initially, both inputs are held low, then one is put to five volts for 500 milliseconds and returned to low. The input that is put to high depends on what action is required. After every request by the app, a confirmation message is sent after any actions are taken, as mentioned previously. Confirmation messages are not sent if the key is used to lock/unlock the door because the assumption that the owner of the key would also be the owner of the mobile device and not need to be informed about this on the device. This key was added to the system as a precautionary measure in the event that the mobile device was lost.

III. RESULTS

When the project was completed, the mobile device was able to communicate approximately thirty feet away from the microcontroller through concrete walls. The total time from initiation of a lock/unlock to action was approximately one second. This could be shortened through use of smaller delays in the program, but delays were left long in this project to ensure that data was sent successfully. The hardware was modified to draw power from a 120V to 12V transformer that was available, so that it could be added to any existing structure. To keep all the electronics relatively stable, the normal convention of the locking pin in the door was ignored. Instead, the linear actuator was placed in the door jamb, along with the microcontroller and key switch.

For demonstration purposes, and to avoid major construction work on the building, a mock door approximately half the size of a standard door was constructed. It consisted of several feet of a false wall, the door jamb, and the door itself. The false wall housed the microcontroller, linear actuator and other necessary circuitry. Since no door this size was available, it had to be constructed. Building both the door and the jamb led to the issue of having them both square, which was a major consideration throughout the construction process. The frame was made as square as possible, but was not entirely sturdy because it was not part of a larger structure. There was some resistance when the door was opened or closed, but this did not seem to detract from the true purpose of the project. This was thought to be the best solution for demonstration because it was very easy to install

and repair the electronics and was portable, so that the project could be demonstrated anywhere with ease.

Two major problems arose in the development of this project. The original program prototype for both the mobile device and the microcontroller only communicated a single character to toggle a LED on the microcontroller protoboard. The mobile device user interface consisted on a single button to transmit the character because the MAC address of the microcontroller was hard coded in. Some problems arose when the second version of the mobile device program was developed. The mobile device was reading and writing to its buffers to quickly and losing data. An addition of a delay to the source code of the application fixed this problem. This problem did not occur in the microcontroller because delays had already been added to that code. Another problem arose in the choice of a suitable resistor value for the transistor array. It had to be a relatively small value, approximately 30 Ω, to supply enough current. While that value was on hand, it would quickly burn up because it drew too much power. This problem was overcome by the use of six 180Ω resistors that were placed in parallel.

IV.CONCLUSION

The goal of this project was to create a security interface to an Android mobile device. It was also to be a short range system that was simple to use. The range and security aspects were achieved through the use of the on board Bluetooth radio of the mobile device. Simplicity was a constant factor in design of the user interfaces. The system was able to actuate a pin to lock or unlock a door from a short distance away with the push of a button on the mobile device. It could also check the status of the door. The system also had a physical key included as a backup. Future work would include the design and building of a battery backup system. Improvements to the locking mechanism could also be another aspect for future work. This project could also be expanded to multiple doors and windows. It can be coupled with existing home automation devices to add thoroughness and completeness to the system.

REFERENCES

[1] Kaur, I., "Microcontroller based home automation system with security," *International Journal of Advanced Computer Science and Applications*, vol. 1, no. 6, pp. 60-65, 2010.

[2] Periyar Dasan ,Agan Prabhu,Shanmuga Sundaram ,Senthil Rajan,Kesavan,"A Ubiquitous Home Control And Monitoring System Using Android Based Smart Phone For It," International Journal Of Computer Science And Mobile Computing,IJCSMC,VOL.2,issue.12,December 2013,pg.188-197

[3] micheal j.pont, "embedded c", pearson education, new york ,2002.

[4] gerard rushingabigwi, liguo sun, godfrey lugoloobi, frank mwezi,"an electric circuits remote switchimg system based on GSM radio network"*international journal of research in engineering and technology"*EISSN:2319-1163|Pissn: 2321- 4708.

[5] Niraj R Chauhan | Prof Pranjali P Deshmukh,"Android Based Intelligent Mobile Home Automation Security System" *IJRCS-International Journal Of Research In Computer Science* , ISSN:2349-3828.

[6] micheal becher ,felix c.freiling, Johannes Hoffmann, Thorsten holz,sebestian uellenbeck,Christopher wolf,"mobile security catching up?revealing the nuts and bolts of the security of mobile devices"*2011 IEEE symposium on security and privacy*.

[7] Rupam K.S.,Ayub M.,Himaraka K. and Dhiraj K.Android Interface based GSM home security system. proc. of IEEE *international conference on isssues and challenges in intelligent computing tech iques,2014*.pp.196-201.

[8] hapsari,a.t.,e.y.syamsudin,and I,haque,i.pramana,"design of vehicle position tracking system using short message services and its implantation on FPGA ",*proceedings of the conference on asia south pacific design automation* ,shanghai ,china

[9] alfredo de santis ,aniello Castiglione ,umberto ferraro petrillo,"an extensible framework for efficient secure SMS", *2010 international conference on complex, intelligent and software intensive systems*, may 2010,pp:843-850.

[10] Das, S.R., *et al.*, "Home automation and security for mobile devices," *IEEE PERCOM Workshops*, pp. 141-146, 2011.

[11] Piyare, R., Tazil, M., "Bluetooth based home automation system using cell phone," *IEEE ISCE*, pp. 192-195, 2011..