ISSN:0975-9646

An Alert Security System Interface Using GSM with Android

E. Rajkumar,
Assistant Professor , Department Of Computer Science And Engineering,
Karpaga vinayaga college of Engineering & Technology, Chennai

***Abstract*— Home alert security system is so important to protect home and valuables. Many alert security systems has been developed which informs the owner in a remote location of the incidents but there is no automatic alert mechanism when there is a movement, also there is no mechanism to open the door of the house if the person visited is friend or relative. This paper looks into the development of a microcontroller and GSM based alert security in houses by developing an android application. If any interrupt occurs, immediately it is detected and communicated to the android phone via SMS by the GSM and microcontroller. Webcam is connected to track the person and the image is stored in the server. The system will wait for the reply from the mobile user for some period of time to trigger the buzzer which was kept in the house, if there was no reply then the system will automatically alert the surroundings by triggering the buzzer. If user's friends or relatives visited the house user can control door of his house by pressing open and close options from the mobile.**

I. INTRODUCTION

Recently surveillance systems have become more important for everyone's security. The embedded surveillance system, frequently used in a home, an office or a factory, uses a sensor triggered to turn on a camera. Some designs use different types of sensors to achieve reliability by means of the different features of each sensor. In this paper the previous design process [1][2] is extended by using both multiple PIR sensors and ultrasonic sensors as a sensor group, ultrasonic receivers and transmitters are located at opposite ends. However, to reduce the interference from other frequencies in ultrasonic signals, a coding signal is used to enhance the ability to distinguish the random interference. To enhance system reliability in the experiment, focus on how to improve the shortcomings of the ultrasonic sensor. Some research explores the influence of attenuation in air and crosstalk of ultrasonic signals by using a coding signal, while some provides improvement of the ultrasonic signal by using different coding signal types.

This paper discusses an approach where an authorized remote mobile user receives an SMS. When a third party tries to enter his house in a remote location. Android applications are developed using java and can be ported to new platform easily thereby fostering huge number of useful mobile applications. A hardware circuit with a switch and a GSM modem embedded is installed and connected to the door of the house. When the intruder tries to open the door, the switch triggers an interrupt and subsequently sends a signal into the microcontroller which subsequently triggers the GSM modem to transmit a warning SMS into already registered number in the modem. The image taken by the camera is compared with the reference images taken by the camera. If same image persist, then no alert is initiated. If it is different image, Immediately alert is send to user android mobile. User can take decision based alert message. If person visited the house is friend or relative, the user will allow them into the house by pressing button in the mobile.

II EXISTING METHODOLOGY

There are many Home security system through out the world. Various approach has been proposed at various times. However, Home alert security system using ANDROID is still ongoing research project field. Some of the previous approach listed below:

A) Implementation of ZIGBEE-GSM based home security system monitoring and remote control system.[1]

Arbab Waheed Ahmad, Naeem Jan, Saeed Iqbal, Chankil Lee [IEEE 54th International Midwest Symposium on Circuits and Systems] [2011] has proposed the system consists of a control console interfaced with different sensors using ZigBee. The activities are conveyed to remote user through SMS or call using GSM technology. Upon reply the remote user can control his premises again through GSM-ZigBee combination. The design has been implemented the concept of serial communication and mobile phone AT-commands. The software is programmed using C- language and the hardware using ZigBee EM357 module, and Sony Ericsson T290i mobile phone set. This system offers a low cost, low power consumption and user friendly way of a reliable portable monitoring and control of the secured environment but it is used for short range communication.

B) Exploiting Bluetooth on Android mobile devices for home security application [2]

Josh Potts and Somsak Sukittanon [IEEE Southeast Conference] [2012] has proposed developed a security system that interfaces with android mobile device. The mobile device and security system communicate via Bluetooth because a short range only communications system was desired. the mobile application can be loaded onto any compatible device, and once loaded, interface with the security system. Commands to lock, unlock, or check the status of the door to which the security system is installed can be sent quickly from the mobile device via a simple, easy to use GUI. The development of security system that integrates with an android mobile device using bluetooth as a wireless connection protocol. The protocol incorporates data encryption for security and interference

avoidance. This system only used for short range communications only. From the previous approaches *A)* and *B)* is identified that it is not possible to monitor the house continuously when the person leaves. There is a lack of simultaneous communication to the remote user, the admin has to watch the videos continuously through television. The device used may fail when there is a continuous monitoring. There is no update to the admin when there is any intrusion. Many methods proposed only short range of communication. To overcome this problems there is no big implementation was introduced.

III PROPOSED METHODOLOGY

In the Proposed system an Ultrasonic Sensor and PIR Sensor are fabricated . Ultrasonic sensor is used to detect the human movement and PIR sensor is used to detect the temperature of the human being. Once these Sensors are sensed, the web camera is initiated to capture the image unauthorized movement. An automatic alert is generated to the administrator about the unauthorized movement and also an Android application is developed which is used to view the image of the Unauthorized User from the Server's database.

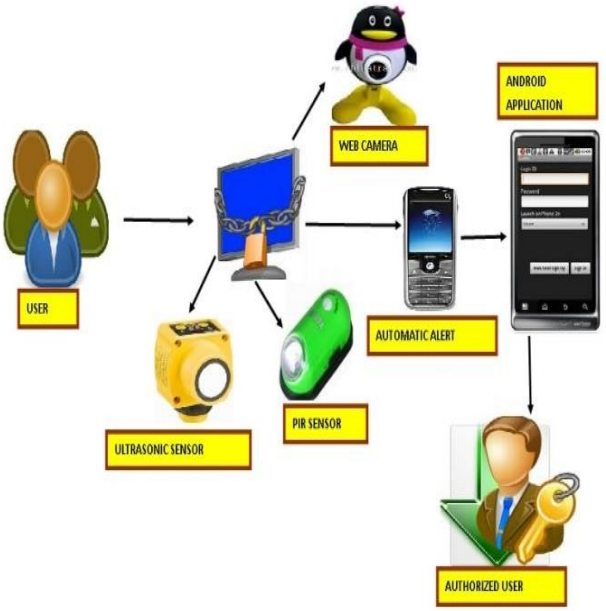

Fig 1: Architecture diagram of the system

The user registered in the process by providing name, mobile number, address for communication & other personal information. Ultrasonic sensor is used to detect the human movement and PIR sensor is used to detect the temperature of the human being. Once these Sensors are sensed, the web camera is initiated to capture the image unauthorized movement. If the motion is detected immediately system initiates the mobile phone connected with the server for sending alert SMS to the admin's mobile number. An android application which is used to view the image of the unauthorized user from the server's database.

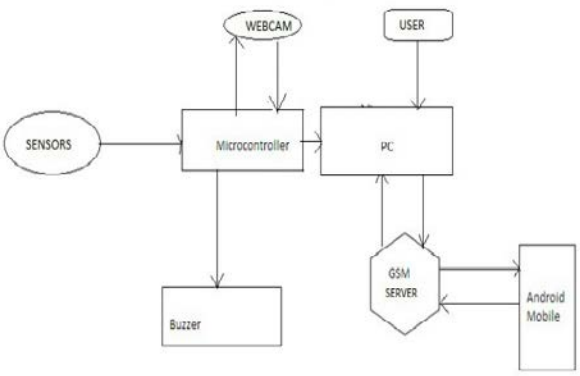

Fig 2: Block diagram of the system

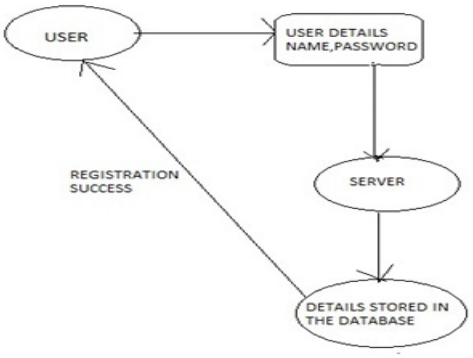

Fig 3: Registration process diagram

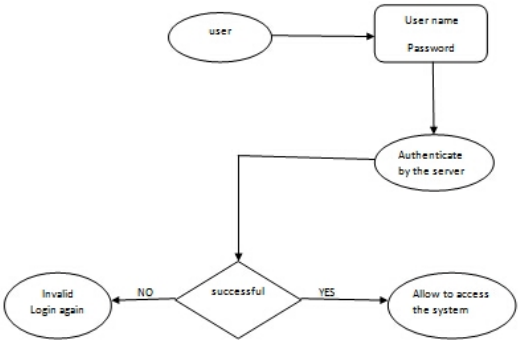

Fig 4:Sign-in process

Fig [3] and Fig [4] describes the registration & sign-in process of the system. The new user should be registered for the secured authentication process. The user should provide the name, mobile number, address for communication and other personal information. Then the server stores the details of the user in the database. Once registration is over the user will enter into the system by providing the username and password. Then the user will be authenticated; else the system will not allow the user to access the cloud.

Fig [5] describes the process flow of the system. Intrusion detected then microcontroller initiate the camera for video streaming then the information is send to the user through the server by message alert. The user login to the application and request for video. If intrusion is unauthorized then the user takes necessary action else stops the streaming

V. USER LOGIN VERIFY

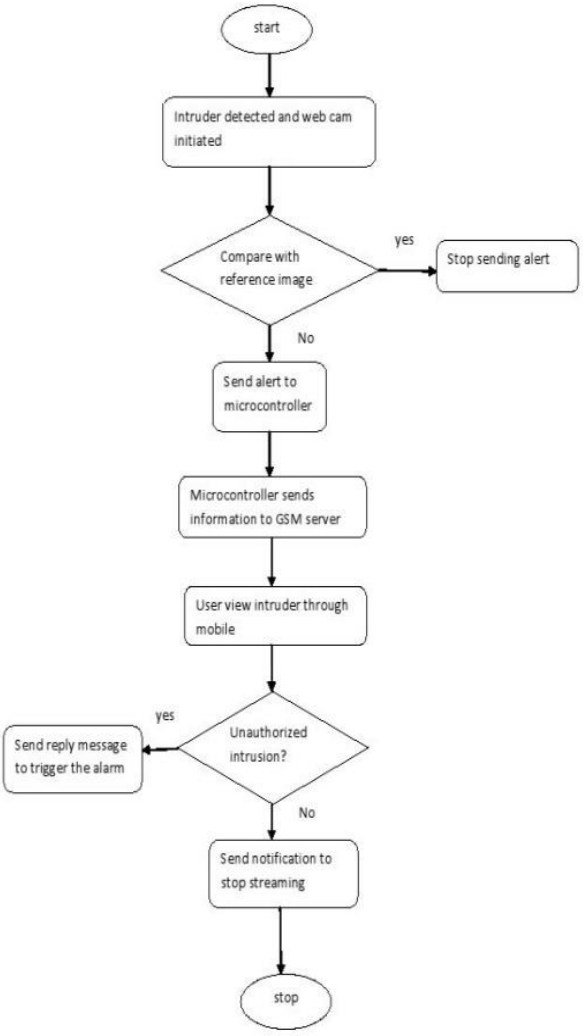

Fig 5: Process Flow of the System

IV ANDROID APPLICATION

```
package com.android.src.technopolice;
public class TechnoPoliceEntity { public static String
ipaddress = null; public static String mobileNo = null;
public static String getMobileNo() { return mobileNo;
}
public static void setMobileNo(String mobileNo) {
TechnoPoliceEntity.mobileNo = mobileNo;
}
public static String getIpaddress() { return ipaddress;
}
public static void setIpaddress(String ipaddress) {
TechnoPoliceEntity.ipaddress = ipaddress;
```

```
import java.util.Properties;
import javax.activation.DataHandler; import
javax.mail.BodyPart;
import javax.mail.Message;
import javax.mail.MessagingException; import
javax.mail.PasswordAuthentication; import
javax.mail.Session;
import javax.mail.Transport;
import javax.mail.internet.InternetAddress; public class
SendMailTLS {
public static void sendMail(String path,String email,String
pass){ final String username = email;
final String password = pass;
final String recipientAddress = email; Properties props =
new Properties(); props.put("mail.smtp.auth", "true");
props.put("mail.smtp.starttls.enable", "true");
props.put("mail.smtp.host", "smtp.gmail.com");
props.put("mail.smtp.port", "587");
Session session = Session.getInstance(props, new
javax.mail.Authenticator() {
protected PasswordAuthentication
getPasswordAuthentication() { return new
PasswordAuthentication(username, password);}});
try {
Message message = new MimeMessage(session);
//message.setFrom(new
                                        InternetAdd
ress("from- email@gmail.com"));
message.setFrom(new InternetAddress(username));
message.setRecipients(Message.RecipientType.TO,Interne
tAddre ss.parse(username));
message.setSubject("Reg : Some One Detected");
Transport.send(message);
MimeMultipart multipart = new
MimeMultipart("related"); BodyPart messageBodyPart =
new MimeBodyPart(); String htmlText = "<br><br><img
src=\"cid:image\">";
messageBodyPart.setContent(htmlText, "text/html");
multipart.addBodyPart(messageBodyPart);
messageBodyPart = new MimeBodyPart();
DataSource fds = new FileDataSource(path);
messageBodyPart.setDataHandler(new DataHandler(fds));
messageBodyPart.setHeader("Content-ID","<image>");
multipart.addBodyPart(messageBodyPart);
Transport.send(message,
message.getRecipients(Message.RecipientType.TO));
} catch (MessagingException e) { throw new
RuntimeException(e);
```

VI.SENDING SMS

```
package com.android.src.technopolice; import
java.util.Properties;
import javax.activation.DataHandler; import
javax.activation.DataSource; import javax.mail.Message;
import javax.mail.MessagingException; import
javax.mail.PasswordAuthentication; import
javax.mail.Session;
import javax.mail.Transport;
import javax.mail.internet.InternetAddress; public class
SendMailTLS {
```

```
public static void sendMail(String path){
final String username =
"sendmailnotification@gmail.com";// final String
password = "version2.0";// finalStringrecipientAddress=
"sendmailnotification@gmail.com";

Properties props = new Properties();
props.put("mail.smtp.auth", "true");
//props.put("mail.smtp.starttls.enable", "true");
props.put("mail.smtp.starttls.enable", "flase");
props.put("mail.smtp.host", "smtp.gmail.com");
//props.put("mail.smtp.ssl.trust", "smtp.gmail.com");
props.put("mail.smtp.port", "587");
Session session = Session.getInstance(props, new
javax.mail.Authenticator() {
Protected PasswordAuthentication
getPasswordAuthentication() {
return new PasswordAuthentication(username, password);
}
});
try {
Message message = new MimeMessage(session);
//message.setFrom(new
                                        InternetAddres
s("from- email@gmail.com"));
message.setFrom(new InternetAddress(username));
//message.setRecipients(Message.RecipientType.TO,Inter
netA ddress.parse("cskarthik2001@gmail.com"));
message.setRecipients(Message.RecipientType.TO,Interne
tAd dress.parse(recipientAddress));
message.setSubject("Reg Tehno Police");
/*message.setText("Dear Sir,"
+ "\n\n Testing!"); Transport.send(message);
System.out.println("Done");*/
MimeMultipart multipart = new
MimeMultipart("related");
} catch (MessagingException e) { throw new
RuntimeException(e);
}
}}
```

VIII . SERVER COMMUNICATION

```
import android.widget.Toast;
public class ServerCommunication { private Socket client;
private FileInputStream fileInputStream;
private BufferedInputStream bufferedInputStream; private
OutputStream outputStream;
private InputStream inStream = null; private static int
filesize = 10000000; int i = 0;
String replyString = "";
 public String getServerCommunication(String
imagePath){ File file = new File(imagePath);
try {
client = new
Socket(TechnoPoliceEntity.getIpaddress(),4444); byte[]
mybytearray = new byte[(int) file.length()];
fileInputStream = new FileInputStream(file);
bufferedInputStream=new
BufferedInputStream(fileInputStream);
bufferedInputStream.read(mybytearray,0,
mybytearray.length); outputStream =
client.getOutputStream();
outputStream.write(mybytearray, 0, mybytearray.length);
outputStream.flush();
bufferedInputStream.close(); outputStream.close();
System.out.println("File Sent");
System.out.print("reply String.....>"+replyString);
} catch (UnknownHostException ue) {
ue.printStackTrace();
} catch (IOException e) { e.printStackTrace();finally{ try{
if(client != null){ client.close();}
}catch(Exception ex){ ex.printStackTrace();
System.out.println(ex);
```

IX. OUTPUT SCREEN SHOTS

Fig 6: User Login

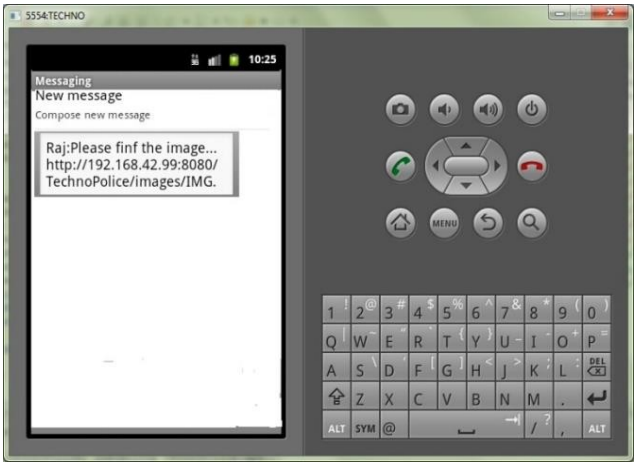

Fig 7: SMS Received through Android

Fig 8: Image received through android

CONCLUSION AND FUTURE WORK

A home security system is implemented by developing an android application. This system shows two different types of sensors PIR sensors and ultrasonic sensors as a sensor group, ultrasonic receivers and transmitters are located at opposite ends.By adding an ultrasonic coding signal our design reduces the miss rate and improves the reliability of the overall system. Android applications are developed using java and can be ported to new platform easily thereby fostering huge number of useful mobile applications

The work can be extended to deploy the APK file which helps the people to read the incoming SMS through voice output. Certain features like triggering an electronic device remotely rather than simply triggering the buzzer might be more useful to the users . The system may be turned into a complete home automation system by implementing different sensors e.g. motion sensors, gas sensors, temperature sensors, etc. in the near future

REFERENCES

[1] Arbab Waheed Ahmad, Naeem Jan, Saeed Iqbal, Chankil Lee "Implementation of ZigBee-GSM based home security Monitoring and Remote Control System", In Proceeding of IEEE 54th International Midwest Symposium on Circuits and Systems (IEEE MWSCAS), 978-1-61284-857-0/111 © 2011 IEEE, Yonsei University, Seoul, Korea.

[2] Josh Potts and Somsak Sukittanon in "Exploiting Bluetooth on ANDROID Mobile Devices for Home Security Application", In Proceeding of IEEE Southeast Conference, pp. 1-4, March 2012, Orlando, Florida, USA.

[3] Mazidi & Mckinlay, "8051 Microcontroller & Embedded Systems", Pearson Education, 2nd Edition, 2006.

[4] Michael J. Pont, "Embedded C", Pearson Education, New York, 2002.

[5] M. Van Der Werff, X. Gui, and W.L. Xu "A Mobile Based Home Automation System", In Proceeding of IEEE 2nd International Conference on Mobile Technology Applications and Systems, pp. 1-5, 2005, Guangzhou, China.

[6] Dhruba Jyoti Gogoi, Rupam Kumar Sharma, "Android Based Emergency Alert Button", In International Journal of Innovative Technology and Exploring Engineering (IJITEE), ISSN: 2278-3075, Volume-2, Issue-4, pp. 26-27, March 2013.

[7] [26] Qadeer, Mohammed A., Rahul Agrawal, Amit Singhal, and Sarosh Umar. "Bluetooth enabled mobile phone remote control for PC." In Advanced Computer Control, 2009. ICACC'09. International Conference on, pp. 747-751. IEEE, 2009.

[8] Deepak Kumar and Mohammed Abdul Qadeer, "SMS Based Emerging Techniques for Monitoring and Controlling Android Mobiles," International Journal of Engineering and Technology vol. 4, no. 6, pp. 798-802, 2012.

[9] Quadeer, Mohammed A., Robin Kasana, and Sarvat Sayeed. "Encrypted Voice calls with ip enabled wireless phones over gsm/cdma/wifi networks." In Computer Engineering and Technology, 2009. ICCET'09. International Conference on, vol. 2, pp. 218-222. IEEE, 2009.

[10] Reto Meier, Professional Android 2 Application Development, 2nd edition Wiley Publishing Inc., 2010.

[11] J.F.. DiMarziio, Android a programmer's Guide, 1st edition, McGrawHill Companies, 2008.