American Journal of Engineering Research (AJER) e-ISSN: 2320-0847 p-ISSN : 2320-0936
Volume-8, Issue-7, pp-132-141 www.ajer.org
Research Paper Open Access

Advanced Wireless Surveillance

Nwakamma Mary Jerry[1]., Nwogu U. O[2]., Ossai Reginald[3].
Federal Polytechnic Nekede, Owerri
Corresponding Author: Nwakamma Mary Jerry

ABSTRACT: *Wireless communication and mobile technologies are already well established in modern surveillance systems with the use of Close Circuit Television (CCTV). Mobile-based client applications are commonly used to provide the basic access to camera video streams and other system resources. Camera site devices might connect to the system core by wireless links to address/overcome the environmental conditions. Finally, the surveillance systems themselves can be installed in portable environments such as busses or trains, which require wireless access for infrastructure and internet services, etc. The technology itself is evolving rapidly providing efficient transmission technology, feature-rich and powerful mobile and wireless devices. The users expect to have seamless access and tools where the functionality does not depend on access technologies or access devices. The same functionality is demanded from local client application and remote mobile browser. Thus, the aim of this paper is to explore advanced surveillance technologies where mobile and wireless access methods are used to provide an enhanced functionality. An analysis of these technology and performance factors are presented and discussed.*

KEYWORDS*: Mobile, Surveillance, CCTV, Wireless Communication.*

Date of Submission: 30-06-2019 Date of Acceptance: 19-07-2019

I. INTRODUCTION

The availability of internet access, the development of applications technologies and increasing processing capabilities of different access devices have a big impact on a variety of access methods in surveillance. Surveillance systems originate from CCTV (Closed Circuit TV) systems.

In traditional CCTV the access tools and methods were dependent on user's location, e.g. operating room or administrator premises. The security measures aimed to provide physical security. The performance of the access application was dependent on the particular installed hardware.

These systems were difficult to upgrade and were not easily scalable. Therefore surveillance systems have moved from traditional analogue into digital and IP-based technologies. The access applications have been made hardwareindependent. The type of access were dependent only on type of the user not his or her physical location. The systems were opened for public domain services such as time synchronization, email and SMS servicesetc

Close Circuit Television (CCTV) systems provide surveillance capabilities used in the protection of people, assets, and systems. A CCTV system serves mainly as a security force multiplier, providing surveillance for a larger area, more of the time, than would be feasible with security personnel alone. CCTV systems are often used to support comprehensive security systems by incorporating video coverage and security alarms for barriers, intrusion detection, and access control.

CCTV System Layout: CCTV uses components that are directly connected to generate, transmit, display, and store video data. A CCTV system can be as simple as a camera purchased from a retail electronics store connected to a video monitor. However, larger systems operated by professional security personnel are comprised of a number of components falling into several basic categories:

- Cameras;
- Lenses;
- Housings and mounts;
- Monitors;
- Switchers and multiplexers; and

- Video recorders.

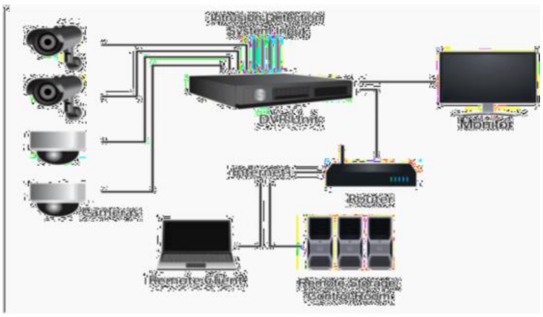


Fig 1: CCTV layout

Many features exist within each of these categories that can satisfy an agency's operational requirements in the most challenging environments. The most complex CCTV systems may incorporate hundreds of cameras and sensors integrated into one overall security network.

Advantages and Uses of CCTV System: In the world today, surveillance is used in particular to:

- Monitor access to a building's perimeter;
- Monitor equipment and data;
- Detect and follow acts of vandalism and theft;
- Monitor traffic;
- Support criminal investigations and control access.

II. STRUCTURE

Surveillance System and the Units: Growing security concerns, increasing crime rates and terrorist activity, as well as an increasing general demand for more protection of people and assets are affecting the growth of the security and, more specifically, the video surveillance market. Potential application areas range from home monitoring, elderly care, and smart environments to security and surveillance in public or corporate buildings. Computer vision based solutions have the potential for very discriminating detection and very low false alarms. Surveillance systems are typically categorized into three distinct generation. The first generation uses analog equipment throughout the complete system. The second generation uses analog cameras but digital back-end equipment. The third generation completed the digital transformation and the cameras which have the ability to convert the video signal to digital before sending them sometimes over and IP.

Units of Surveillance System

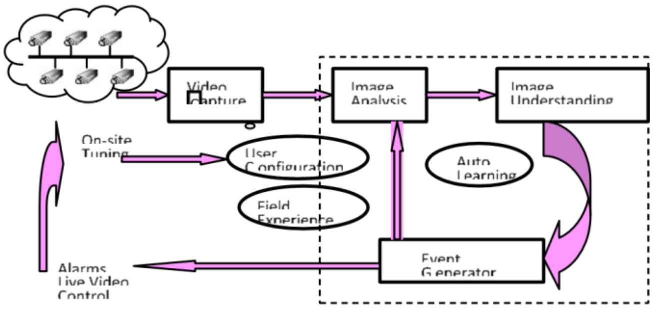


Fig 2: Video SurveillanceSystem Architecture

Each camera deployed in a surveillance system requires power and the means to transmit video data to monitoring and storage systems. These requirements can necessitate modifications to a facility's infrastructure, such as installing new poles for mounting cameras.

Need to Expand and Integrate More System: The inevitable and continuous changing face of surveillance technology suggests that surveillance is in a constant state of flux, in terms of technical features, the public's reaction, its use and management by authorities, and the nature of security. Surveillance systems are increasingly used for varied purposes and places, which Jean Ruegg, Valérie November and Francisco Klauser (2004) suggest is due to the rise in the number of possible applications of video surveillance.

Intelligent video algorithms, such as sophisticated motion detection, can identify unusual walking patterns and alert a guard to watch a particular video screen. Object-recognition algorithms can identify someone who might simply be loitering, or even a briefcase or other suspicious object that is left somewhere it shouldn't be. Again, the system can alert a monitoring guard so that appropriate action can be taken.

The most advanced intelligent video algorithm is facial recognition. However, most experts agree that use of this technology as an efficient tool in the private sector is still several years down the road.

III. WIRELESS SURVEILLANCE SYSTEM

The availability of internet access, the development of applications technologies and increasing processing capabilities of different access devices have a big impact on a variety of access methods in surveillance.

Surveillance systems originate from CCTV (Closed Circuit TV) systems. In traditional CCTV the access tools and methods were dependent on user's location, e.g. operating room or administrator premises. The security measures aimed to provide physical security. The performance of the access application was dependent on the particular installed hardware. These systems were difficult to upgrade and were not easily scalable. Therefore surveillance systems have moved from traditional analogue into digital and IP-based technologies.

A wireless surveillance system is a desirable technology because of its low installation cost, when compared to a wired system. By becoming more familiar with the currently available wireless security camera systems, we were able to determine where we should make improvements. There are many products on the market today with features that help to enhance the performance of wireless security systems, but there are still numerous drawbacks to these systems. Each of the systems discussed in the following sections have their own strengths and weaknesses and by evaluating these strengths and weaknesses, we were better able to determine characteristics that would distinguish our product from the current products on the market.

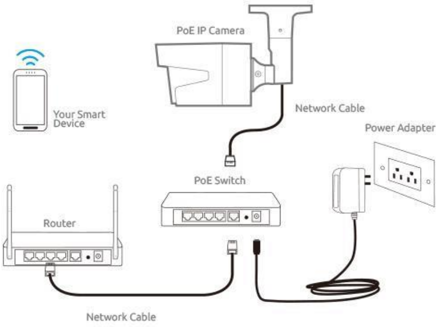


Fig 3: Wireless Surveillance system

The Transmission Protocols: Wireless options for transmitting video can be advantageous due to ease of installation, lack of cabling requirements, and assured mobility. There are some disadvantages of wireless systems such as the need for a dedicated frequency to transmit signals, signal interruptions, and signal interference. There are also increasing concerns over cyber security and the need for information assurance hardening.

IP Network Transmission: IP-based systems have emerged as an attractive alternative to other technologies, due in large part to their ability to achieve high-performance video capabilities at a low cost. The industry has found ways to implement IP-based systems that use existing cameras, cables, and other equipment. However, organizations planning and designing new systems should consider IP-based technology. This section addresses the basic parameters of an IP-based network system.

IP and Surveillance: IP-based CCTV systems are designed to provide the ability to monitor, record, and stream video over a network to computers or other equipment. The system can use existing local area networks (LANs), wide area networks (WANs), and/or wireless LANs (WLANs) to save on installation costs. However, for added security, an organization could install its own private area network (PAN) cabling and support hardware. Power over Ethernet (PoE) technology is also an option within an IP-based system to increase savings and reliability. PoE enables various networked devices to receive power and data through one standard cable, which can be a significant cost savings when designing CCTV systems.

A simple IP-based CCTV system, such as the one seen in Figure 4-5, consists of a network camera (although analog cameras can be used with additional equipment), a network switch, and a PC for viewing, storing, and analyzing data and managing the CCTV system.

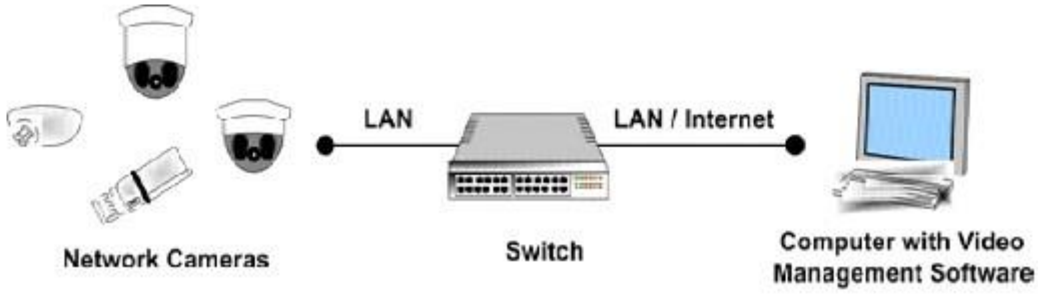


Figure 6. IP-Based Surveillance System

Traditional analog-based surveillance systems require dedicated point-to-point cabling from each camera to the recording and/or viewing locations. In an IP-based CCTV system, video is digitized at the camera and can then be transmitted over the IP network to virtually any location around the world. Most analog systems are traditionally unidirectional, whereas network based systems are bidirectional, easier to integrate into larger systems, and highly scalable.

Network cameras and other devices can not only send audio/video, but can also send other data like text or short message service (SMS) messages to users as well as receive audio and data (which can activate alarms, door entries, and external alarms). In addition, IP-based systems have the ability to interface and communicate with multiple parallel applications (e.g., motion detection or license plate readers).

Benefits of IP-Based Systems: Digital systems in general have a variety of advantages over analog systems such as ease of use, advanced search capabilities, simultaneous record and playback, improved image quality, and efficient compression and storage options. IP-based systems also provide many benefits that include: Remote accessibility;

- High image quality;
- Future integration with digital technologies;
- Flexibility;
- Scalability; and
- Cost-effective transmission.

IP-Based System Components: The flexibility of IP-based systems is attributed to the variety of configurations and types of components compatible with IP technology. Since the number of possible custom configurations is so vast, the following list is just a sample of the type of components compatible with IP-based systems.

Cameras: Both IP network cameras and analog cameras can be used in an IP-based system. **Video Encoders**– When using analog cameras, a video encoder or video server needs to be connected to the analog cameras to convert the video to a digital format. The encoder then sends the data over an IP network.

Network Switches: Switches allow CCTV devices to communicate with each other and share information.

Networks: A network can be small or extensive, wired or wireless or a combination thereof. The most common approach taken by organizations is to use LANs or WANs. Network bandwidth capacity can be increased by adding switches and routers. Wireless networks are a good option when traditional wired networks are too costly or difficult to install.

Power over Ethernet: PoE is an option for using a wired network to distribute both data and power.

PC with Web Browser: PCs can access live and recorded video over the Internet as needed.

PC with Video Management Software: PCs can record and store video from cameras, as well as view live and recorded video as needed. Additionally, video management software can support video being accessed over smartphones or tablets.

Storage Devices: Video transmitted through an IP system can be stored on a server, a network device such as direct attached storage (DAS), storage area networks (SAN), network attached storage (NAS), or a PC hard disk. These storage devices are discussed further in Section 5.

Mobile Devices: IP-based systems can be easily configured to facilitate access to video via the Internet from smartphones, laptops, and other mobile devices.

PTZ CAMERAS

The pan–tilt–zoom camera (PTZ camera) is a camera that is capable of remote directional and zoom control.PTZ reflects the movement options of the camera.

A high-resolution camera digitally zooms and pans into portions of the image, with no physical camera movement.PTZ Cameras are commonly used in applications such as surveillance, video conferencing, live production, lecture capture and distance learning.

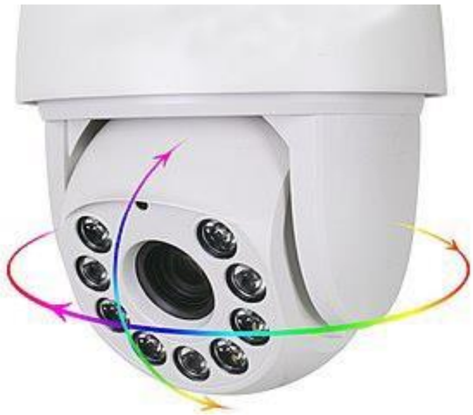


Figure 7: A PTZ Camera.

GEOVISION DVRs (HYBRID WIRELESS SURVEILLANCE SYSTEM)

GeoVision DVRs are PC based surveillance systems designed to process video, audio and data from local and remote network surveillance environment.

With more special features and more integration versatility provided, the GeoVision DVRs Surveillance System delivers more powerful and streamlined surveillance operation performance as well as enhanced management efficiency.

In addition it offers advantages that convert into low cost of installation and unlimited connectivity options. With video, audio, data, and I/O devices combined all into one system and through uniform software platform interface, each of these solutions provides a full list of features and functionalities that can quickly fulfill various clients' particular security surveillance requirements.

IV. ADVANCED WIRELESS SECURITY SYSTEMS

In the present day, security systems play an important role in the protection of lives and investment. This is achieved by the incorporation of various subsystems into the security system with a single control unit such as surveillance, intruder control, access control, fire detection, etc.

Currently another trend is to provide seamless access to the system and use of wireless and mobile technologies. The users expect to have access tools where the functionality does not depend on access technologies and devices. The same functionality is required from the local client application and remote mobile browsers.

Video surveillance systems accommodating wireless or mobile technologies are areas of ongoing research. The key research areas are focused around architectural considerations required to support receivers' mobility, and their security and dependability aspects or innovative solutions based on wireless (sensors) and mobile technologies. The researched scenarios are usually presented using small or medium size surveillance systems or other innovative solutions.

The subject of transition of complex surveillance into world of wireless, mobile and cloud technologies is relatively unexplored (excluding the security aspects of connectivity).

In case of complex surveillance system the transition towards mobile and wireless solutions is rather continuous than disruptive change of applications, architecture and system design in general. Therefore, it is worth to analyze the existing solutions in context of characteristics and limitations of new technologies.

The access applications have been made hardware independent. The type of access were dependent only on type of the user not his or her physical location. The systems were opened for public domain services such as time synchronization, email and SMS services etc.

Objective: By the strategic placement of security cameras in certain corners of the house to deter thieves and criminal behavior and, in certain circumstances, to use recorded footage in the investigation of and prosecution for criminal activity. To develop web based applications for capturing the video and images for recording and storing into database. Person can access the video images from the remote place from internet access. From the remote place user can access the camera security system with the smartphone having internet. Developing mobile application to install on Windows mobile phone for client purpose. Employ a close and private accountable process to access the data. To provide authentication and authorization on web based system. To restrict misuse or abuse of the system or of the footage. It provides safety and prevents any untoward incidents from happening such as potential home invasions or robberies. Fire is one of the leading causes of home destruction. Since fires are dangerous, you can increase home security by learning how fires are started and what you can do to prevent fires from occurring. To control Crime types which include murder, violent crimes, rapes, robberies, aggravated assault, property crimes, grand auto theft, larceny, theft, etc

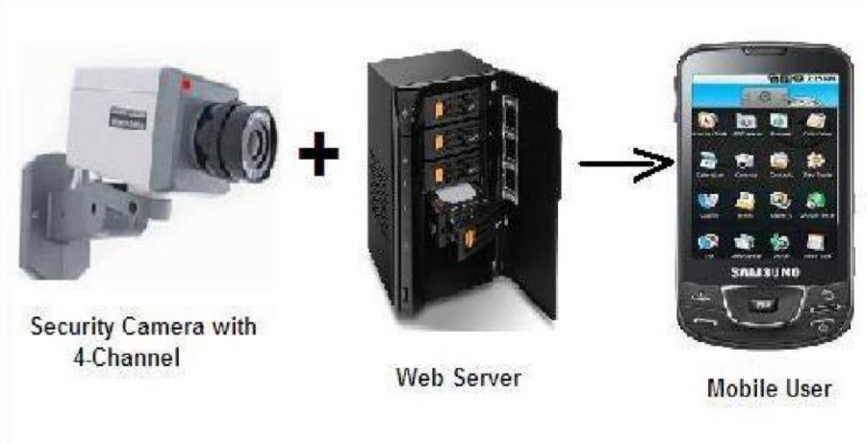
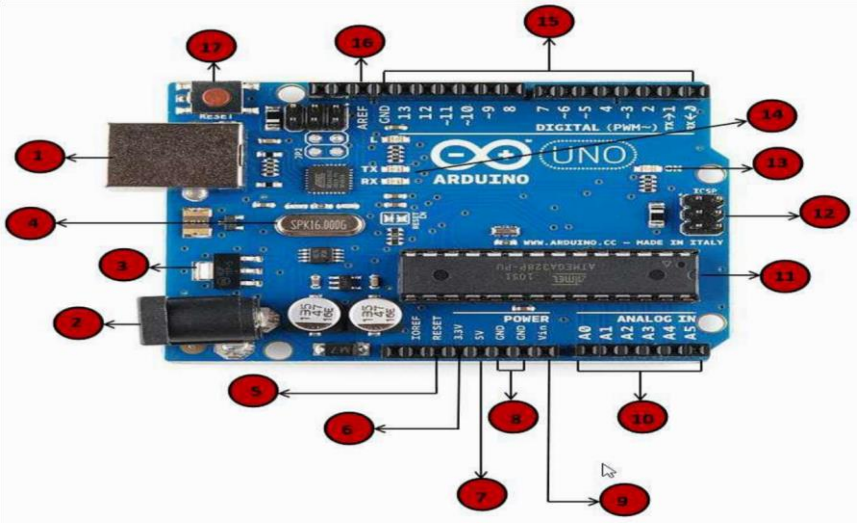


Fig 10: Mobile user can access information from remote place

V. ARDUINO UNO

Arduino is a tool for making computers that can sense and control more of the physical world than the computer. It's an open-source physical computing platform based on a simple microcontroller board, and a development environment for writing software for the board. Implementing arduino into a wireless surveillance system requires the use of hardware and software configurations integrated into the IP Based system.

Arduino Configuration



1 **Power USB:** Arduino board can be powered by using the USB cable from your computer. All you need to do is connect the USB cable to the USB connection (1).

2

3

Power (Barrel Jack): Arduino boards can be powered directly from the AC mains power supply by connecting it to the Barrel Jack (2).

Voltage Regulator: The function of the voltage regulator is to control the voltage given to the Arduino board and stabilize the DC voltages used by the processor and other elements.

Crystal Oscillator: The crystal oscillator helps Arduino in dealing with time issues. How does Arduino calculate time? The answer is, by using the crystal oscillator. The number printed on top of the Arduino crystal is 16.000H9H. It tells us that the frequency is 16,000,000 Hertz or 16 MHz.

Arduino Reset: You can reset your Arduino board, i.e., start your program from the beginning. You can reset the UNO board in two ways. First, by using the reset button (17) on the board. Second, you can connect an external reset button to the Arduino pin labelled RESET (5).

Pins (3.3, 5, GND, Vin): 3.3V (6): Supply 3.3 output volt 5V (7): Supply 5 output volt .Most of the components used with Arduino board works fine with 3.3 volt and 5 volt. GND (8)(Ground): There are several GND pins on the Arduino, any of which can be used to ground your circuit. Vin (9): This pin also can be used to power the Arduino board from an external power source, like AC mains power supply.

10 **Analog pins:** The Arduino UNO board has five analog input pins A0 through A5. These pins can read the signal from an analog sensor like the humidity sensor or temperature sensor and convert it into a digital value that can be read by the microprocessor.

11 **Main microcontroller:** Each Arduino board has its own microcontroller (11). You can assume it as the brain of your board. The main IC (integrated circuit) on the Arduino is slightly different from board to board. The microcontrollers are usually of the ATMEL Company. You must know what IC your board has before loading up a new program from the Arduino IDE. This information is available on the top of the IC. For more details about the IC construction and functions,you can refer to the data sheet.

12 **ICSP pin:** Mostly, ICSP (12) is an AVR, a tiny programming header for the Arduino consisting of MOSI, MISO, SCK, RESET, VCC, and GND. It is often referred to as an SPI (Serial Peripheral Interface), which could be considered as an "expansion" of the output. Actually, you are slaving the output device to the master of the SPI bus.

13 **Power LED indicator:** This LED should light up when you plug your Arduino into a power source to indicate that your board is powered up correctly. If this light does not turn on, then there is something wrong with the connection.

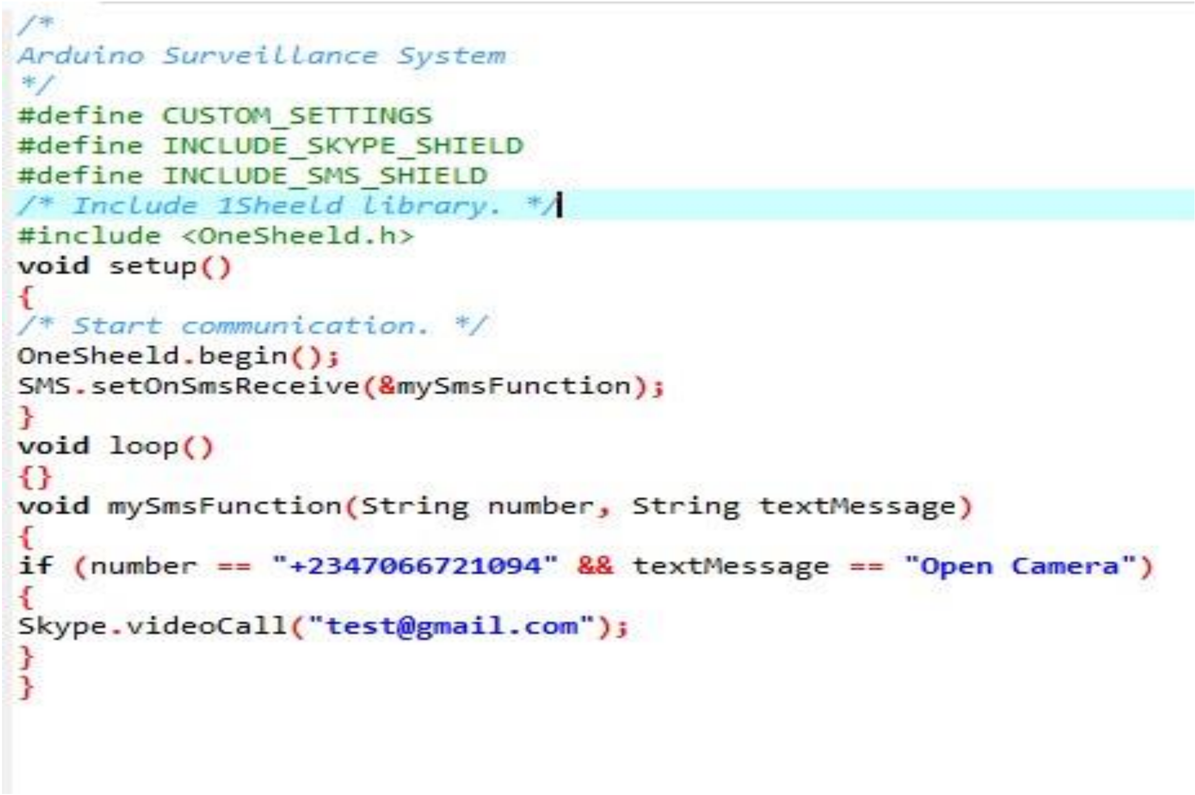
14 **TX and RX LEDs:** On your board, you will find two labels: TX (transmit) and RX (receive). They appear in two places on the Arduino UNO board. First, at the digital pins 0 and 1, to indicate the pins responsible for serial communication. Second, the TX and RX led (13). The TX led flasheswith different speed while sending the serial data. The speed of flashing depends on the baud rate used by the board. RX flashes during the receiving process.

15 **Digital I / O:** The Arduino UNO board has 14 digital I/O pins (15) (of which 6 provide PWM (Pulse Width Modulation) output. These pins can be configured to work as input digital pins to read logic values (0 or 1) or as digital output pins to drive different modules like LEDs, relays, etc. The pins labeled “~” can be used to generate PWM.

16 **AREF:** AREF stands for Analog Reference. It is sometimes, used to set an external reference voltage (between 0 and 5 Volts) as the upper limit for the analog input pins.

VI. SYSTEM DESIGN

In this system, a code is written into the Arduino software installed on the server. The code will use the Arduino SMS Shield library to check over all the SMSs received in Smartphone 1. When an SMS is received from a certain phone number and with certain text which are added to the code, a video call will be initiated on smartphone 2 which will be displaying the Camera Feed.



```
/*
Arduino Surveillance System
*/
#define CUSTOM_SETTINGS
#define INCLUDE_SKYPE_SHIELD
#define INCLUDE_SMS_SHIELD
/* Include 1Sheeld library. */
#include <OneSheeld.h>
void setup()
{
/* Start communication. */
OneSheeld.begin();
SMS.setOnSmsReceive(&mySmsFunction);
}
void loop()
{}
void mySmsFunction(String number, String textMessage)
{
if (number == "+2347066721094" && textMessage == "Open Camera")
{
Skype.videoCall("test@gmail.com");
}
}
```

Fig 11: Arduino code

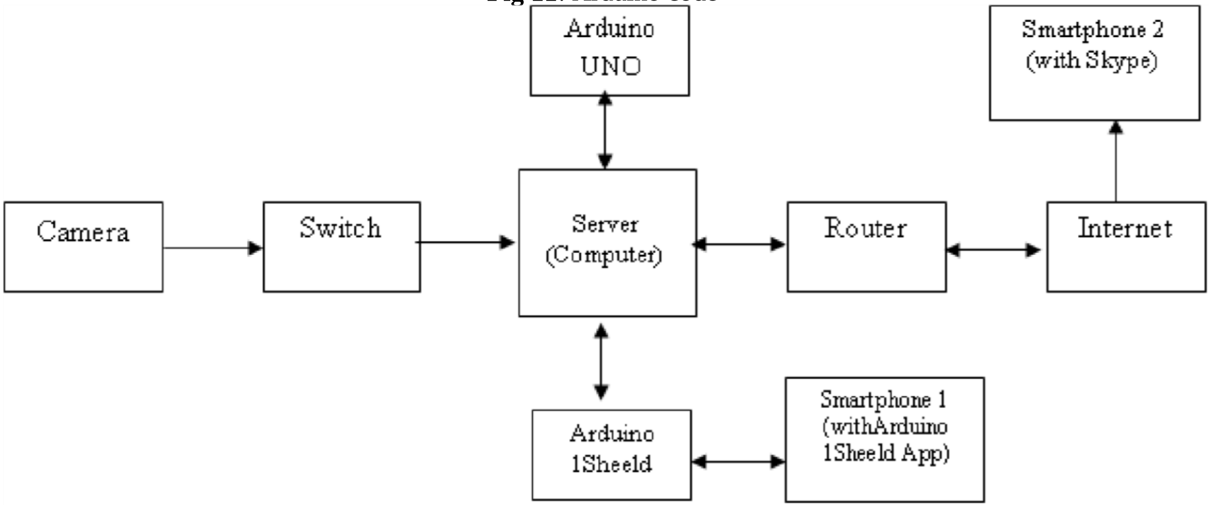


Fig 12: Block diagram of the system

ARDUINO 1SHEELD FEATURES

1Sheeld is a new easily configured shield for Arduino. It is connected to a mobile app that allow the usage of all smartphones' capabilities such as LCD Screen, Gyroscope, Switches, LEDs, Accelerometer, Magnetometer, GSM, Wi-Fi, GPS …etc. into the Arduino software. 1Sheeld consists of two parts.

The first part is a shield (Hardware) that is physically connected to the Arduino board and acts as a wireless middle-man, piping data between the Arduino software and the smartphone wirelessly.

The second part is an app (Software) on the smartphones that manages the communication between the shield and the smartphone.

The 1Sheeld can be used as input or output from Arduino and make use of all of the sensors and peripherals already available on the smartphone The 1shield is used to control the arduino program. It can automatically control the smartphone features like call, sms, and app-launch.

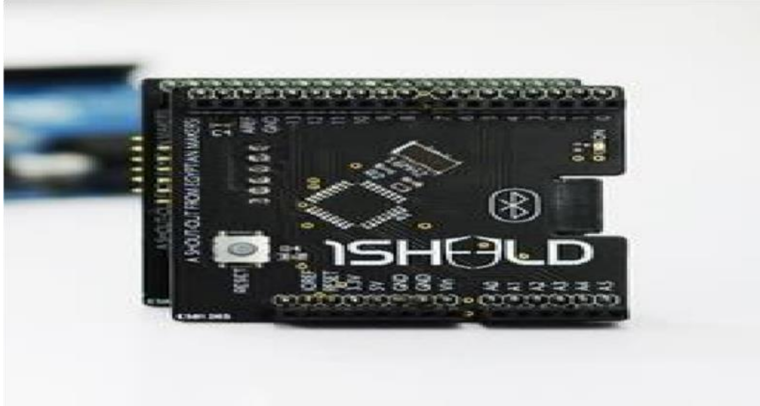


Fig 13: 1Sheeld Board

JUSTIFICATION

The 1Sheeld is a versatile tool which have functionalities that can grant control of security cameras (Angles, Zoom, Scan, Pan) with the use of PTZ cameras.

Skype is the preferred Video app for use on the smart phone because of its dedicated video calling functionality. Skype offers a free video call functionality and works better with 1Sheeld app installed than other video calling apps.The 1Sheeld can be installed on major mobile operating systems like the Android and iOS.The phone number used is only dedicated to the arduino program. Any random number can be used.

PROCEDURE

- Plug in Arduino to PC/Laptop and upload the code to the 1Sheeld in ‘uploading mode’ □ Open the 1Sheeld application and connect to 1Sheeld board.
- Switch bvack the 1Sheeld to “Operating mode”.
- Choose Skype and SMS shields, and make sure you have an internet connection.
- Open your smartphone and send an SMS to the used phone with this Text “Open Camera” □ And in just seconds a Skype video call will be initiated.

PROS AND CONS

The Pros

- Less costly to install and maintain.
- Surveillance videos can be accessed remotely at any location.
- Allows monitoring of areas where it’s impossible or expensive to install wired security cameras. □ Convenient and easy to integrate with other security systems.
- Continued decrease in pricing.

The Cons

- Vulnerability to security threats.
- The risk of data loss.
- Signal interference.
- The insufficient range for larger buildings thus requiring additional access points or repeaters.
- Slower data transmission than wired networks.
- Installation of a secured enterprise wireless network can be complicated, requiring a professional installer.
- Network availability (3G, 4G, etc.)

VII. CONCLUSION

Security System will put you in front of crimes, accidents, and incidents. Once you have secured your home you want to secure your computer, especially if you have Internet access. Securing your computer will help you escape Identity theft, as well as other crimes. Predators swarm the Internet, searching for prey all the time. Since the statistics are increasing technology, designers are working hard each day to help us find the level of security we need.

Modern technology has made security systems possible. When it comes to improving the security of businesses, the market provides consumers with two options – wired security systems or wireless surveillance systems. The latter has several distinct advantages over the traditional counterpart.

Wireless surveillance systems are ideal for larger properties where coverage due to distance can be very expensive. They can be installed at any location within the property and administered over the network by application of Arduino UNO hardware and software, a computer and a mobile device. This security solution is very convenient for security personnel or even business owners especially at times when they are away from their businesses.

However, like any other products, there are advantages and disadvantages of wireless surveillance. One particular issue worth mentioning is the threat of security breaches and vulnerability to viruses providing attackers the opportunity to hack confidential business information.

REFERENCES

[1]. Bing-Fei, W., Hsin-Yuan, P., Chao-Jung, Ch., Yi Huang, Ch. (2005) An Encrypted Mobile Embedded Surveillance System. Proc. IEEE Symp. on Intelligent Vehicles, 502 – 507.

[2]. Dujovne, D., Turletti, T. (2006) Multicast in 802.11 WLANs: An Experimental Study. Int. Symp. on Modeling analysis and simulation of wireless and mobile systems, 130 - 138

[3]. Gudipudi S., Mary J., Ruth T., and Prashanth Y., (2015) Image Tracking Based Home Security Using ArduinoMicrocontroller," International Journal of Innovative Research in Computer and Communication Engineering. (3): 8.

[4]. Hye-Soo, K., Eun-Seok Ryo, Ch., Jayant, N. (2010) Channel-adaptive Video Transmission Using H.264 SVC over Mobile WiMAX Network. Digest of Tech. Papers. Int. Conf. on Consumer Electronics ICCE'10, 441 - 442

[5]. Jun H., Chengdong W., Zhongjia Y., Jiyuan T., Qiaoqiao W., and Yun Z, (2008) Research of Intelligent Home Security Surveillance System Based on ZigBee," International Symposium on Intelligent Information Technology Application Workshops, Shanghai, pp. 554-57

[6]. Mahendran. N, Geo J.M., and Veenesh. M.U, (2013) Multiple sensor feeding supported, building automation system using arduino platform", With Exposure of 802.15.4 Functionalities, International Journal of Engineering Trends and Technology, 4: 2

[7]. Ruichao, L., Jing, H., Lianfeng, S. (2009) Design and Implementation of a Video Surveillance System Based on 3G Network. Int. Conf. on Wireless Communication and Signal Processing WCSP. 1 - 4

[8]. Sathishkumar M., and Rajini S., (2017) Smart Surveillance System Using PIR Sensor Network and GSM" International Journal of Advanced Research in Computer Engineering &Techn**.** 1: 7

[9]. Sneha N., Avinash G., and Tareek M.P., (2012) Design of a Home Embedded Surveillance System with Pyroelectric Infrared Sensor & Ultra-Low Alert Power" International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE) 1: 8

[10]. Xiangjun Z., Shaodong Y., and Le L. (2008) "Multimedia sensor networks design for smart home surveillance," Control and Decision Conference, 2008, pp.431-435

Nwakamma Mary Jerry "Advanced Wireless Surveillance" American Journal of Engineering Research (AJER), vol.8, no.07, 2019, pp.132-141