International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 9 (2018) pp. 6613-6619

Remote Computer Controller for Alarms Alert System

Rustom Mamlook[#], Omer Fraz Khan

Department of Electrical & Computer Engineering, Dhofar University, Sultanate of Oman.
*(*Corresponding Author)*

Abstract

Remote connectivity is fundamental to monitoring conditions for a safe environment. The importance of securing areas and facilities has increased with advancement in technology. Applications specific monitoring and alert systems provide insights into the monitored processes. The coverage area of such systems focuses on the process itself. Some of the examples are monitoring of critical areas of the facility to prevent unauthorized entry, alerting about the levels and over spillage of liquid, alert on the power outage etc. With a need to protect a house, an office, a company or any other premises many innovations in security systems and their implementation exist. Our paper discusses the design of a Remote Computer Controller for Alarms Alert (RCCAA) System using an embedded system module interfaced to an Alarm device that uses a web-based Computer Controller to register and route the alert signals from monitored devices to multiple locations for monitoring. The design and development of the prototype use an embedded system hardware. Software simulator such as Proteus tests the hardware before final implementation. On the Server side, web service enables the command and control of devices using a Web-based Browser. C# Windows Forms makes the Graphical User Interface (GUI) for the Desktop environment. Programming Language CSharp (C#) is our choice. The pattern of design is Model View Controller (MVC) for Web Application interface. The communication channel in the design is Web Sockets and Http over TCP/IP. Sensors interface with microcontrollers over UART [[1]] (Universal Asynchronous Receiver/Transmitter) protocol. We utilize occupant detection, magnetic ,global positioning, proximity and current detection for the types of sensors in this paper. For an online user with access credentials, alarms and alerts are accessible through the web-based page but when the user is offline, alerts go to his mobile phone through short messaging service (SMS).

INTRODUCTION

The main objective of our paper is to develop a remote alarm system for issuing security alerts to the clients connected to the Internet network. The importance of securing areas and facilities has increased with the advancement of technology. A home alarm system is a set of electronic devices that have been set up to alert the occupants and local authorities about an intrusion within a residence. An industrial-alarm system employs computers interfaced with controllers to control and get alerts on the status of many types of devices such as air conditioning and central heating systems in large buildings, fire, safety and security systems and burglar alarms, manufacturing processes, traffic lights and pedestrian crossings etc.

Integration of today's security systems with computers has become very efficient and cost-effective because of the underlining communication technologies available to us through computers, which were previously not found in analogy security systems.

From consumer's point of view, the computers connected to internet provides economy and 24 hours' connectivity to other remote locations connected to the network. On the other hand, a secondary network providing Mobile stations access to the Internet using GSM (Global Systems for Mobile) also brings together the mobile and handheld devices to the internet ecosystem enables a further extension of remote services available to the managers and supervisors. The security system under study has to have the following:

- Accessible using a web-based monitoring, alarm notification, and control systems over a cellular network using data link to World Wide Web.
- Efficient, low cost and scalable to home and office security system.
- Self-configurable with the minimum technical support required to set up on the server as well as client end.
- Fail-safe and constantly operational round the clock.
- Able to distinguish between the false event (sequence of alarm signals) and a real event.
- Effective in minimizing or avoiding damage because of a disaster. For example, if a flood occurs at a remote site, the Alarm Interface Embedded Controller (AIEC) issues an alarm. The intelligent network controller can locally or remotely invoke a command to turn on a sump pump instead of wasting valuable time waiting for somebody to arrive at the facility. In the event of an unauthorized entry into a secure area, the AIEC can initiate a visual and audible alarm. Further, if wired to a camera, the AIEC can activate it for remote

surveillance.

- Non-intrusive to the user looking at various alarm systems with at least an implementation of alarm pattern detection and prioritization algorithms.
- The controller can also make logical decisions effective within its domain and independent of the remote server.

Web server exists on the Internet while both personal computers and the mobile station connected to the internet over WAN (Wide Area Network) and GSM technology respectively. Web Server designed on top of internet information server. The web server provides a set of functions to enable data and information exchange among clients informing each other about the status of sensors connected to them. Information about an alert signal can now reliably travel over both internet and GSM. This signal required to generate a sound or indication alarm on a panel in a remote location to alert the user about any abnormal situation. Our paper is about the utilizing Web and GSM networks. A discrete embedded system such as a microcontroller-based hardware and its accompanying firmware provides connectivity to both networks.

USE OF WIRELESS TECHNOLOGY

Existing wireless technologies [2] includes short-range z-wave, zig-bee, 2.4 GHz Bluetooth, Wi-Fi, medium range LoRaWAN and long-range 3G/4G, GPRS, radio and microwave as land-based. Other satellite solutions for wireless communication are quite expensive and not common in public domain. In our design, short-range communication such as Bluetooth connects the hardware controller locally for the clients requesting information from the sensors using their personal device, while long-range communication such as 3G/4G provides a link between the clients' access from remote sites.

USE OF WIRED TECHNOLOGY

Existing wired technologies include short-range Local Area Network over Ethernet cable or fiber optic while long-range Wide Area Network (WAN) over Ethernet or fiber optic. In our design, the clients and server connect to the Wide Area Network (WAN/Internet) using Asymmetric digital subscriber line (ADSL) router provided by Internet Service Provider (Omantel) over CAT-5E Ethernet cable. In wired network scheme, multi-dependency layers exist where one downed link can disrupt the service, which makes it unsuitable for mission-critical application such as ours. The ability to switch from one network to another handles to some extent the workability in case of disconnection in one network. E.g. in case of a downed 4G link, 3G is used. If both 3G and 4G are down, we can downgrade to GPRS (2G) or further down to ADSL network.

SIMILIAR WORK

Intelligent residential security alarm and remote control system based on single chip computer, Liu Zhen-ya et al [[3]] in a similar design present intelligent residential burglar alarm, emergency, fire toxic gas leakage remote automatic sound alarm and remote control system based on Intel 8051 single chip. This system relies on the analog ISDN (Integrated Services Digital Network) network to send DTMF (Dual Tone Multi-Frequency) as compared to our system relying on TCP-IP (Transmission Control Protocol/Internet Protocol) network.

In the area of TCP-IP networking, most of the alarm controller systems are available as propriety solutions for the commercial reasons with a few implementations towards academic research and study.

METHODOLOGY

The hardware part utilizes a PIC (Peripheral Interface Controller) type of Microcontroller while the programming languages for the software designed is C#, JavaScript and using .NET [[4]] Framework from Microsoft and other technologies like SignalR. We utilize the ASMX web service [[5]] proprietary to Microsoft Web Technology. The microcontroller is programmed using the proprietary software mikroBaisc [[6]] from MikroElektronica and simulation of the design is done in Proteus VSM [[7]].

Figure 2 shows a block diagram of Remote Alarm Computer Controller (RACC). The system consists of several parts, from getting access to log in using a web page in a web browser along with installing a piece of program in administrator’s computer [[8]].

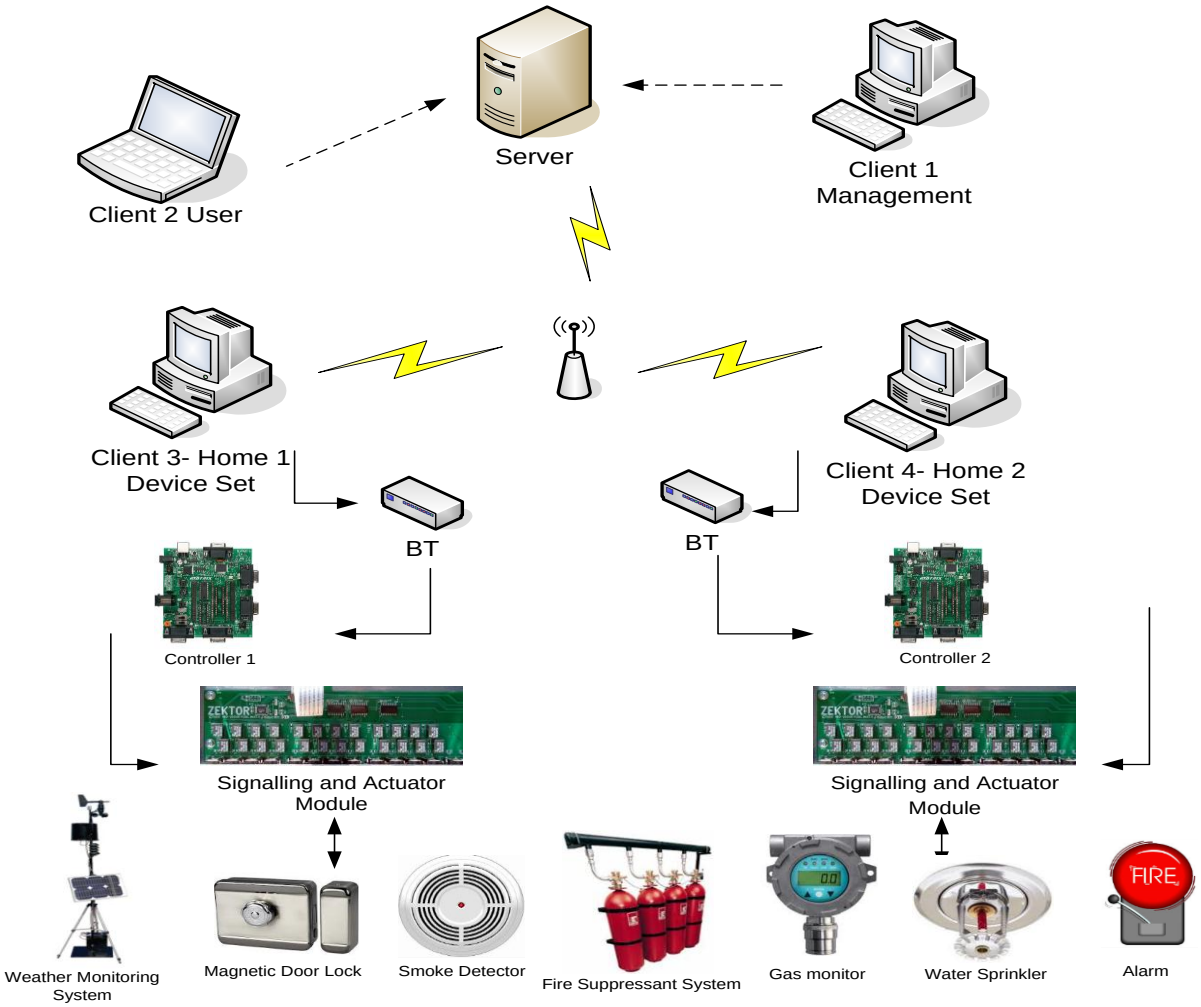

Figure 1: Overview of (RACC)

At the send Command part, a user using form message to send a request to the server and the server sends it to client intended, which is connected to the alarm. At transmitter part, the alarm is connected to the controller using Signalling and Actuator module. The controller scans the alarms and devices connected to it and register alerts issued. It then does a pre-analysis of the alerts as compared to other devices in the ecosystem. It will give action priority to any command issued from the server. Whereas in case of absence of any command and control from the server, the controller can self-activate or deactivate a signal that would directly or indirectly affect the operation of the device/s monitored.

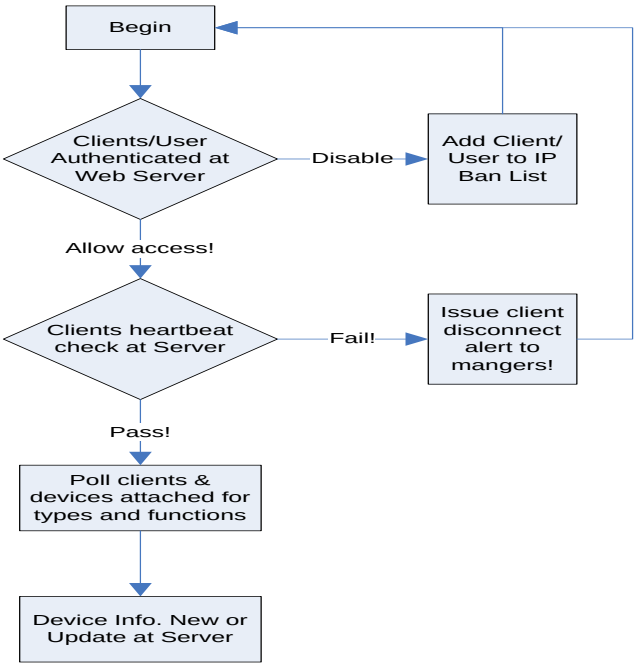

Figure 2: Clients authentication and Device Abilities retrieval

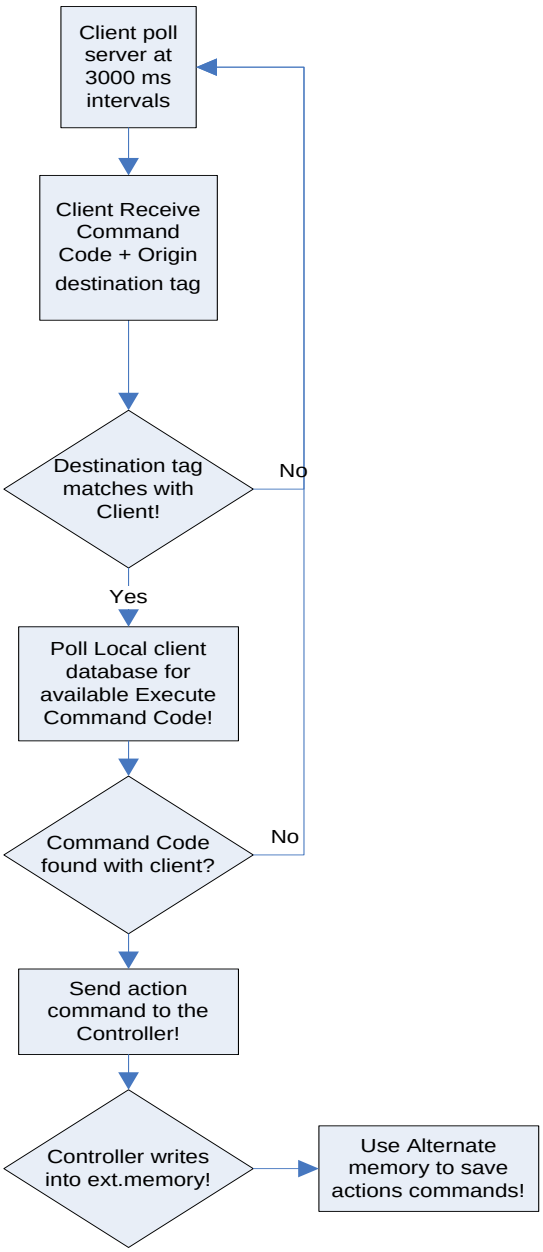

Figure 3: Client and Controller interaction

NAT (Network Address Translation) and firewalls introduced by routing networks of internet service providers have disabled ease of internetworking of clients and led to the development of NAT-Traversal technologies [[9]]. For our paper, we have utilized a web server to circumvent the NAT issue by enabling intermediate communications between clients over dynamic IP using Domain Name Service (DNS) forwarding to public IP over common HTTP port 80 [[10]]. In a real system, such dependency on dynamic to static DNS service has to be avoided to minimize the odds of communication failure due to DNS server's disconnection.

PSEUDO CODE

a. Server PingClients (Client1, Client2, Client3, ClientN; where N is the max number of clients that can be handled by the server depending on the bandwidth of the connection between the server and the client's network.

b. GetClientList (DeviceType, functionsCode) function returns one list for each client.

c. AddNewClients (Client1, Client2, Client3...);

d. UpdateClientDatabase (Client1, Client2, Client3...);

e. UpdateDeviceDatabase (ClientID, Device1, Device2, Device3...);

f. GenerateList(ClientAddress, UserName, ControllerMAC, DeviceID, DeviceDefinition);

g. CheckHeartBeat(ClientAddress,ServerAddress,Interval,HeartBeatSignal);

h. GetHomesList(Domain,HomeAddressList,HomeDevicesConnected);

i. SelectHome(HomeAddress);

j. SelectDevice(SelectedHome,DeviceAddress);

k. SendCommand(SelectedDevice,CommandType,OriginClient,DestinationClient);

l. AuthenticateClients(OriginClient,CommandType,DestinationClient,AuthenticationHash);

m. SelectCommand(AuthenticatedHash,CommandCodes,Origin,Destination,RegisteredHomes,RegisteredDevices);

n. QueuedCommads(CommandQueue,currentCommand,DateTimeStamp,CommandInExecution)

o. ExecuteCommand(currentCommand,CommandStatus,Elapsed,TimeToFinish)

IDENTIFIER DATA DESIGN

Communication of client with server involves the transmission and reception of the following data:

1. Client Identification data

User Name	*Client System Name*	*Client System MAC Address*	*Client System IP Address*
Logged in User	System Name	MAC-48	IPV4

2. Controller Identification data

Controller Type/Definition	*Status*	*Controller MAC Address*
Type Codes	Status Codes	MAC-48
xxxx	On/Off/Standby/Hybernate/Sleep S3,S2,S1	xx;xx:xx:xx

3. Device Identification data

Device Type/Definition	*Status*	*Main Function*	*User Name*	*Client System Name*	*Device MAC Address*
Type Codes	Status Codes	Ability Codes	Logged in User	System Name	MAC-48
xxxx	On/Off/Armed-Disarmed/Standby/Hybernate/Sleep S3,S2,S1				

4. Server Identification data

Server Domain	*Server I.P. Address*	*Web Service Address*	*Server Port*
Domain Name of Server	Dynamic (DNS) Managed by remote DNS for NAT Traversal	Domain Name + Web Service Name	Server's Binding Port listening to Clients
ofksigns.redirectme.net	Dynamic to Static		Port No. 80

5. Alerts Identification data

Alert Type	*Alert Time Stamp*	*Alert Origin*	*Alert Destination*
Code	Date and Time of Alert Issue	Device + System Address	Users + Controller + Device Address
	24 hours format		

6. Control Commands Identification data

Command Type	*Corresponding Alert Code*	*Command Time Stamp*	*Command Origin*	*Command Destination*
Code	Code	Date and Time of Issue	User + System Address	Client + Controller + Device Address
Command Codes	Alert Code	24 hours format		

SERVER PROCESSING OF DATA

The server processes command received and compare with the set of sequences and patterns previously learned from device issuing alerts and client interactions and saves the parameters into the database. These patterns can be used to generate algorithms for future case studies.

SERVER APPLICATION

An application server acts as a set of components accessible to the software developer or developed software client, through an API (Application Programming Interface) defined by the platform itself. For Web applications, these components are usually performed in the same running environment as its web server(s), and their main job is to support the execution of functions and methods from remote clients, which possess the server's worldwide public IP Address, and has the ability to access the functions available through web service.

CLIENT APPLICATION

During development of our client application, we utilized the functions provided by the server application as web service. The functions of this web service are available to each software client through a web API called Web Service Reference. During the development phase of the client application, the developer has to update its Service Reference if the underlying code for the web service changes at the server. The server upon client's request can automatically propagate such updates to the clients. Control-Client implements a proxy object of the web service available at the server using web service as shown by the following excerpts from Control-Client Code:

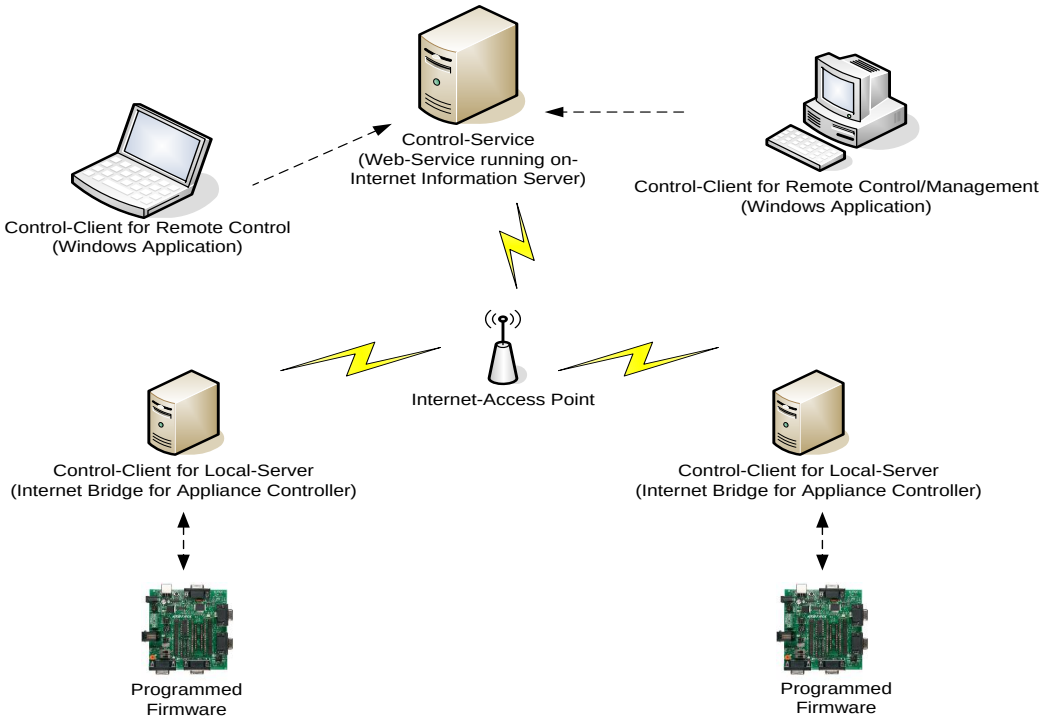

Figure 4: System's software components

HARDWARE DESIGN OF DEVICE CONTROLLER

A slave controller once connected to the PC behaves like a master microcontroller. Our design can have multiple master controllers and many slave microcontrollers. A typical master controller along with its interfaces with devices and slave microcontroller shown in Figure 5. Isolators/Buffers as shown are optocouplers while actuators can be relays and power control devices. ALU stands for arithmetic logic has the program instructions hard coded into the Microcontroller's internal memory also can be later reconfigured if design may require. ALU accesses RAM for accessing the commands in queues and other related information such as slave microcontroller and device's statuses. The Firmware of a slave microcontroller exists in the internal ROM, which has a MAC (Media Access Controller) Address for the identification of Master/Slave Microcontrollers in the controller's network.

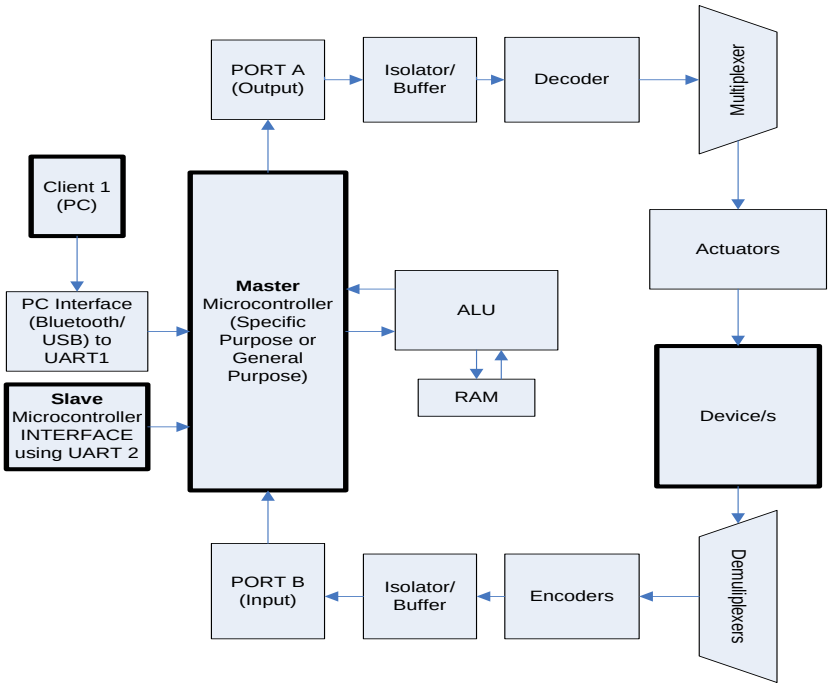

Figure 5: Alarm design using Master-Slave Microcontroller setup

DEVICE CONTROLLERS NETWORK

Masters and Slaves interconnect and from Slave Controller nodes contributing to controllers network. Slave microcontrollers can connect to Slave Interface node using Bluetooth or more efficient RFID with a very small footprint for the short-range distance between slaves within a building or a particular site. In case of long-range communication between Master 1 and Master 2 located at sites globally in remote areas Clients 1 and Client 2, 2 can share Slave controller's statuses among each other over company's Virtual Private Network or over public internet gateways.

RESULTS AND CONCLUSIONS

The alarm circuit was run in Proteus Programming for simulation and testing. Commands from a Bluetooth terminal were tested by providing them to the program instructions encoded into the Microcontroller's model in Proteus. The client was tested to be identifying on another client's GUI (Graphical User Interface) over World Wide Web and commands were sent over TCP/IP protocol from one client to another client connected to the alarm circuit.

The research paper will produce a new system that categorized as a security system. Previously, a home alarm system is a set of electronic devices that have been set up to alert the occupants and local authorities about an intrusion within a residence. There are advantages when using a new system which to help the user when they going outside after leaving the room locked. The main target user is actually for the house, an office, a bank or a company.

A new system categorized as a security system by using a mobile phone to our project. It is intended to help both in improving existing systems as well as during development of new systems and modifications. The objective is to ensure selection of systems complying with applicable as well as safety, efficiency and high production availability.

REFERENCES

[1] UART communication document retrieved from https://www.freebsd.org/doc/en_US.ISO8859-1/articles/serial-uart/

[2] Wireless Technologies retrieved from http://docwiki.cisco.com/wiki/Wireless_Technologies

[3] Intelligent residential security alarm and remote control system based on single chip computer, Authors: Liu Zhen-ya; Sci. Sch., Jiangxi Inst. of Educ., Jiangxi; Wang Zhen-dong; Chen Rong; Wu Xiao-Feng, published in Industrial Electronics and Applications, 2008. ICIEA 2008. 3rd IEEE Conference.

[4] Microsoft .NET framework retrieved from http://www.microsoft.com/net

[5] Web ASMX Service .NET Microsoft Technology retrieved from https://msdn.microsoft.com/en-us/magazine/cc163674.aspx

[6] http://www.mikroe.com/ a website for development tools, compilers for programming microcontrollers and related hardware components.

[7] http://www.labcenter.com/index.cfm source of a simulator for PIC and other types of microcontrollers.

[8] http://www.bitpipe.com/tlist/Internet.html, All Rights Reserved, Copyright 2000 - 2013, Tech Target | Read our Privacy Statement, Dec 16, 2013

[9] Retrieved from http://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/26704-nat-faq-00.html Updated: Nov 10, 2014.

[10] DNS Concepts and facilities retrieved from http://tools.ietf.org/html/rfc882, Domain Names: Implementation & Specification retrieved from http://tools.ietf.org/html/rfc883.