International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-4 Issue-6, August 2015

Advanced Security System using Web Remote

Rustom Mamlook, Omer Fraz Khan

Abstract— Our paper proposes a design of an Advanced Security System using Web Remote (ASSWR). Our system uses an embedded system module interfaced with an Alarm device. A web Computer Controller for registering and routing the alert signals issued by the monitored devices to multiple monitoring sites was used. Our Embedded system module design was tested using software simulator. The hardware was constructed to simulate a real security system. Web Service was implemented and devices were controlled over World Wide Web Network using windows Forms as well as a Web Application interface. The used Communication channel in our paper is Web Sockets and Http over TCP/IP along with integration of communication within microcontrollers over UART (Universal Asynchronous Receive/Transmitter).

Keywords: Web Remote Security System; Embedded System; Software based security system simulator; Web application for security; Security over Web Sockets and Http.

I. INTRODUCTION

Security is fundamental to protecting human rights and creating an environment for socioeconomic development. The concept of security has been broadened beyond traditional notions of territorial deface to include the safety and well-being of people and their freedom from fear. The importance of securing areas and facilities has increased with the advancement of technology. The need to protect a house, an office, a company or any other premises has led to innovations in security systems and their implementation. The main objective of our paper is to develop a web remote security system that could be used for issuing alerts to clients connected over internet network. A home-alarm system is a set of electronic devices that has been set up to alert the occupants and local authorities of an intrusion within a residence. An industrial-alarm system employs computers interfaced with controllers to control and get alerts on status of many types of devices such as air conditioning and central heating systems, fire-safety systems, 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 analog security systems. For consumer's point of view the computers connected to internet provides economy and 24 hours connectivity to other remote locations connected to the network.

Manuscript published on 30 August 2015.
***** Correspondence Author (s)
Rustom Mamlook, Department of Electrical & Computer Engineering, Dhofar University, Salalah Sultanate of Oman.
Omer Fraz Khan, Department of Electrical & Computer Engineering, Dhofar University, Salalah Sultanate of Oman.

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 enabling further extension of remote services available to the managers and supervisors. The security system under study has the following:

- Accessible using a web based monitor has an alarm notifier, and is controlled over cellular network using data link to World Wide Web.
- Efficient, low cost and scalable to home and office security system [1].
- Self-configurable with minimum technical support required to setup at 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 real event.
- Effective in minimizing or avoiding damage as a result 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 an implementation of alarm pattern detection and prioritization algorithms.
- Controller can also make logical decisions effective within its domain and independent of the remote server.

Web server exists on Internet while both personal computer and the mobile station connect to the internet over WAN (Wide Area Network) and GSM technology respectively. Web Server is designed on top of internet information server as it is a set of functions implemented in programming languages. Web server enables data to travel among clients alerting each other about the status of devices connected to either client. Information on an alert signal can reliably travel over both internet and GSM. The acquired signal enables the alerting unit to generate sound or flashlight in a remote location alerting the occupants on any abnormal situation at the reporting site. Our paper discusses the design and implementation of microcontroller based hardware (AIEC) and its accompanying software.

II. USE OF WIRELESS TECHNOLOGY

Existing wireless technologies [2] includes short-range z-wave, zig-bee, 2.4 GHz Bluetooth, Wi-Fi, and long range 3G/4G (GPRS) or microwave as land based and satellite solutions.

In our design short-range communication such as Bluetooth was employed between the hardware controller and the client locally while long-range communication such as 4G is used between the clients at remote sites. For details on the software library utilized for making Bluetooth connection, refer to the lines of code in Appendix A.

III. USE OF WIRED TECHNOLOGY

Existing wired technologies include short-range Local Area Network over Ethernet cable or fibre optic while long-range Wide Area Network (WAN) over Ethernet or fibre optic. In our design the clients and server connect to the internet using WAN over CAT-5E Ethernet cable. The software code necessary to achieve the connection between two LAN based wired devices is included in Appendix A.

IV. RELATED WORK

Intelligent residential security alarm and remote control system based on single chip computer, was considered by Liu Zhen-ya and et al [3] in a previous design presents an 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 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.

In a similar research as Web based remote security system (WRSS) [4], model development on installation of proper sensors for fire, smoke, break-in and other threat detecting mechanisms was discussed. Information generated by these sensors is sent to servers dynamically and is made available to the owners of property to monitor. The WRSS methodology does not consider the auto-response generation and server connectivity re-routing in case of sensors or sensor's path failure.

In conventional Industrial Instrumentation, Programmable Logic Controllers (PLC) are highly dependent on direct input of sensors over instrumentation control lines whereas our paper discussed implementation of Controller Network and a Main Server, with Controller taking the role of Server in absence of main Server.

V. METHODOLOGY

The hardware part utilizes a PIC (Peripheral Interface Controller) type of Microcontroller while the programming languages for the software designed are C#, JavaScript and .NET Framework from Microsoft called Signa lR. We utilize the ASMX web service [5] licensed under Microsoft Web Technology. The microcontroller is programmed using the software called mikro Baisc [6] from Mikro Elektronica and simulation of the design is done in Proteus VSM [7]. The system consists of several basic steps starting from getting access to login using web page in a web browser along with installation of an administrator program on the computer [8]. An overview of the system is shown in Figure 1.

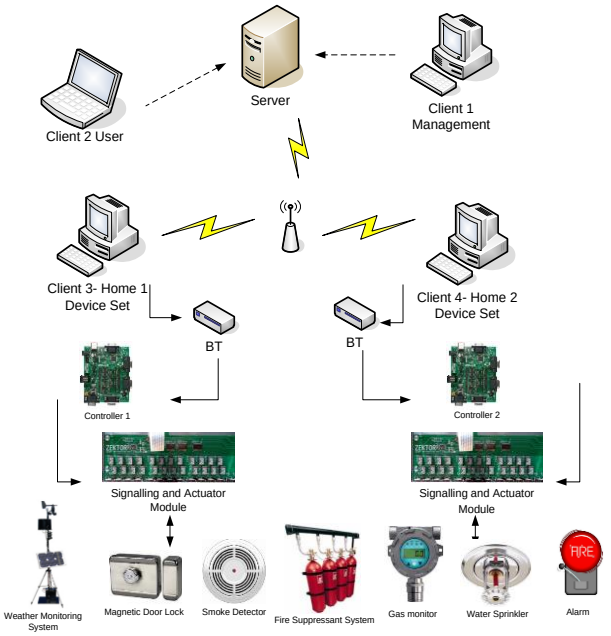

Figure 1: Overview of (RACC)

During the sending Command part, a message is sent as a post request to server and analyzed for the type of command and the type of client which initiated it. Each sending unit also sends the same post message to the neighbouring networked clients having their connected alarms. The client is registered at the server as flowchart in Figure 2. At transmitter part, the alarm is connected to the controller using signalling and actuator module. The flowchart of client interaction with controller is shown in Figure 3. 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, controller can self activate or deactivate a signal that would directly or indirectly effect the operation of the device/s monitored. Figure 4 shows a flowchart of Server, Client and Controller's role in the system's process chain.

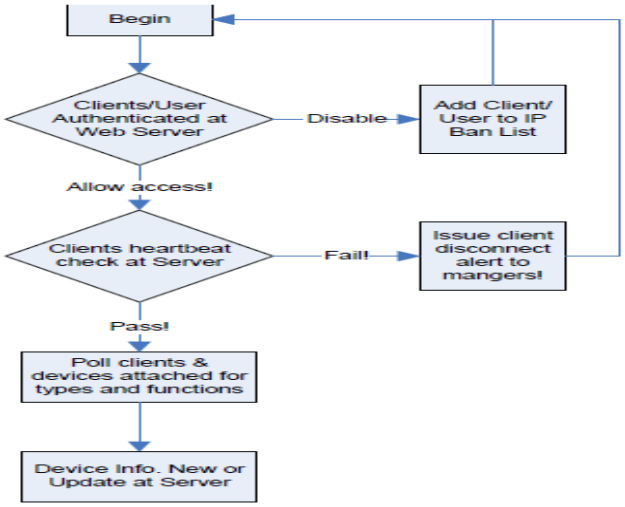

Figure 2: Clients authentication and Device Abilities retrieval

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

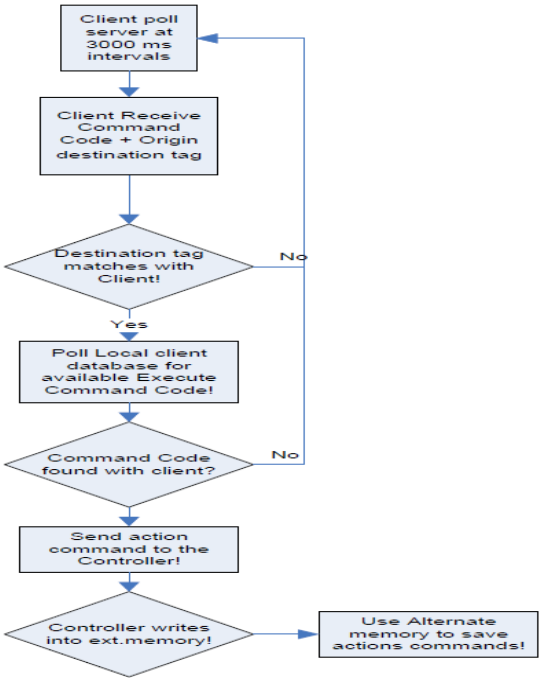

Figure 3: Client and Controller interaction

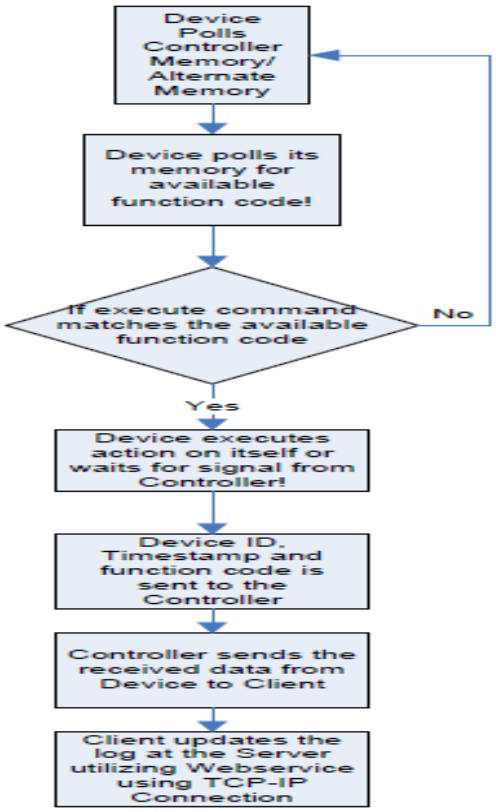

Figure 4: Device, Controller and Client Interaction

For security reasons, NAT (Network Address Translation) and firewalls introduced by routing networks have made the inter-networking of clients difficult and led to the development of NAT-Traversal technologies [9]. In 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 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. One of such proposition to avoid service disconnection due to DNS failure is to use virtual private network over web network.

VI. PSEUDO CODE

The following programming function prototypes can be sequentially listed as the pseudo code for the software control part:

a. Server Ping Clients (Client1, Client2, Client3, Client N; where N is the max number of clients that can be handled by the server depending on the bandwidth of connection between the server and the client's network. (Appendix A: 1a)
b. Get Client List(Device Type, functions Code) function returns one list for each client (Appendix A: 1a)
c. Add New Clients(Client1, Client2, Client3...); (Appendix A: 1b
d. Update Client Data base(Client1, Client2, Client3...);
e. Update Device Database (ClientID, Device1, Device2, Device3...);
f. Generate List (Client Address, User Name, Controller MAC, Device ID, Device Definition);
g. CheckHeartBeat(ClientAddress,ServerAddress,Interval ,HeartBeatSignal);
h. Get Sites List (Domain, Site Address List, Site Devices Connected);
i. Select Site (Site Address);
j. Select Device(Selected Site, Device Address);
k. SendCommand(SelectedDevice,CommandType,Origin Client,DestinationClient); (Appendix A: 1c and 1d)
l. AuthenticateClients(OriginClient,CommandType,Desti nationClient,AuthenticationHash);
m. SelectCommand(AuthenticatedHash,CommandCodes, Origin,Destination,RegisteredHomes,RegisteredDevice s);
n. QueuedCommads(CommandQueue,currentCommand, DateTimeStamp,CommandInExecution)
o. ExecuteCommand(currentCommand,CommandStatus, Elapsed,TimeToFinish) (Appendix A: 2)

VII. IDENTIFIER DATA DESIGN

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

1. ***Client Identification data:*** Date needed at the server side to register the client in its database.

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:*** Data required at the server and by other controllers for identification of a controller.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

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:*** Data required at the server and by other controllers for identification of devices.

Device Type/De-finition	*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	Xxxx	name secret combination		

4. ***Server Identification data:*** Server identifies itself to the other devices using related address relay over open web service. Only clients and devices with existing signatures at the server will be accepted, while others will be rejected by server.

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:*** Each alert is identified with its code, originating device, and destination user, controller or device. Please note that alert signals originating at any point (client/server/controller/device) can terminate either at server, client, controller or device. Alert signals inherently multicast to every node in the network either through gateway or inter-device interfaces.

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:*** Control commands are processed by the Controllers and logged by servers and clients**.** Control commands differentiate from alert signals in a way that they are used for initiating a control action by use of actuators connected to the controllers.

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		

VIII. SERVER & CLIENT MODEL

Our software presents an authentication interface to user on both Client PC and Server PC; former called as Client because Controllers and Devices are interfaced to it while the latter called as Server because an administrator is logged into the system using higher privileges. Software design is same for both Client and Server implementation. Software running on each PC connects the PC's with each other in a peer to peer fashion. This enables central information (such as site address and devices types) to be available at multiple sites hence required for redundancy for safety from disconnection of service. Security challenges can be satisfied using the inherent security of network topology by designing and strategically placing servers and clients so that if one network fails the others are ready to replace the failed node in a network.

IX. SERVER PROCESSING OF DATA

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

X. SERVER APPLICATION

An application server acts as a set of components accessible to the software client, through an API (Application Programming Interface) defined for the operating platform. For web applications, these components are usually present in the same running environment as its web server(s) as shown in

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

Figure 5, and their main job is to support the execution of functions and methods from remote clients. The server's worldwide public IP Address is available to clients which have the ability to access the functions on the server exposed as web service. Web Service class is inherited from System. Web. Services. Web Service Class as the following excerpt shows:

```
[WebService(Namespace =
"http://ofksigns.redirectme.net/")]
[WebServiceBinding(ConformsTo=
WsiProfiles.BasicProfile1_1)]
Publicclass Control Service:
System.Web.Services.WebService {
Variables are declared as follows:
Static protected ArrayList arrUsers = new ArrayList ();
Static protected ArrayList arrMessage = new ArrayList ();
Static protected ArrayList arrClients = new ArrayList ();
Static protected ArrayList arrCommand = new ArrayList ();

Public Control Service()
//Constructor
```

Web Methods such as Get Clients ( ) and Add Clients ( ) are implemented at the Server side. The Web Method Tag is used in defining a Function within a web service as follows:

```
[Web Method]
Public string Get Clients()
Stringstr Client = string. Empty;
for (inti = 0; i<arr Clients. Count; i++)
strClient = strClient + arrUsers[i].ToString() +
"|";
{returnstr Client;}
[Web Method]
public void AddClient(string strClient)
boolbFlag = false;
for (inti = 0; i < arrClients.Count; i++)
if (arrClients[i].ToString() == strClient)
bFlag = true;
else
SendMessage("Ser@ver", arrClients[i].ToString(),
strClient + " has logged in.");
if (bFlag == false)
arr Clients. Add (str Client);
```

XI. 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 underling code for the web service changes at the server. Such updates can be automatically propagated to the clients by the server upon client's request. The two types of clients, one is a regular client to which device controller is connected and the other is a control client acting as administrator as shown in Figure 5. 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:

```
Str Client = lbl Client Name. Text;
strMe = lbl User Name. Text;
strServiceIP =
(string)ConfigurationManager.AppSettings["Control
Service"];
CtrlSrv.Url = "http://" + strServiceIP + "";
Calling the web service for 'AddUser' for adding
himself after logging.
CtrlSrv.AddUser (lblUser Name. Text);
CtrlSrv. AddClient (lblClient Name. Text);

The following code represents Control-Client application
connecting to Serial Port:
publicboolconnetport()
boolIsopen;
serialport1.Close();
try
if (!this.serialport1.IsOpen)
this.serialport1.PortName = com;
this.serialport1.Open ();
this.serialport1.BaudRate = mybaudrate;
this.serialport1.StopBits =
System.IO.Ports.StopBits.One;
this.serialport1.Parity =
System.IO.Ports.Parity.None;
this.serialport1.Handshake =
System.IO.Ports.Handshake.None;
Isopen = serialport1.IsOpen;
Isopen = true;
catch (Exception ex)
Isopen = false;
throw ex;
return Is open;
```

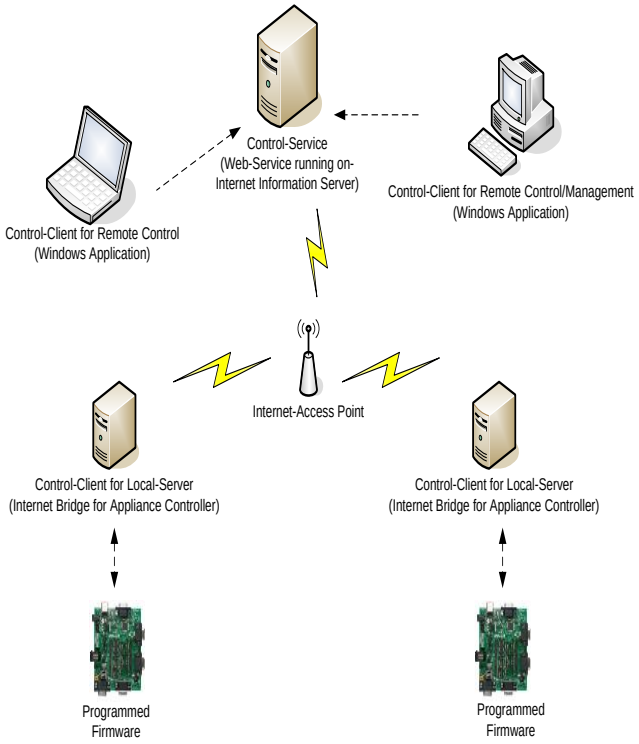

Figure 2: System's software components

XII. CONTROLLER HARDWARE DESIGN

A controller once connected to the PC is termed as a master microcontroller. The hardware and software design is same for all controllers irrespective of their functionality as master or slave. Our system can have multiple master controllers and many slave microcontrollers. A typical master controller along with its interfaces with devices and slave microcontroller are shown in FIGURE **6**: ALARM DESIGN USING MASTER-SLAVE **MICROCONTROLLER** Microcontroller

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

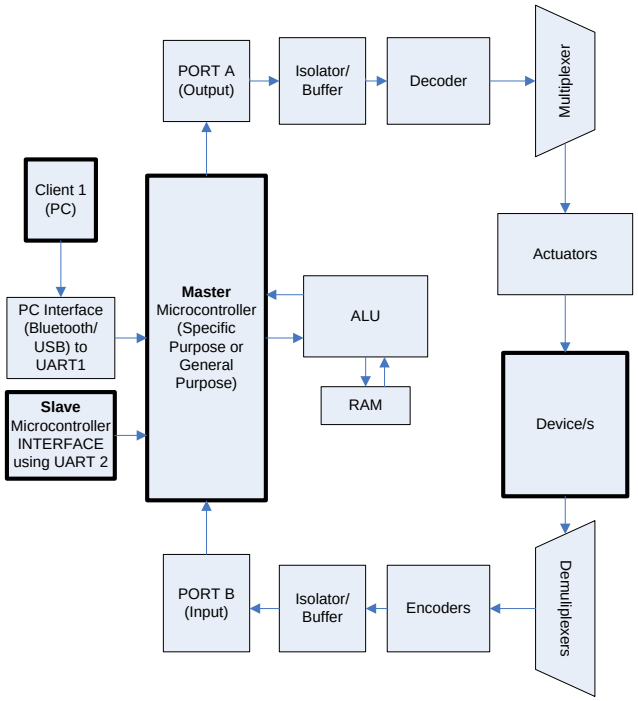

Figure 6: Alarm design using Master-Slave Microcontroller setup

Isolators/Buffers as shown are opto-couplers while actuators can be relays and power control devices. ALU stands for arithmetic logic has the program instructions hardcoded in to 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's and device's statuses. Firmware of a slave microcontroller exists in the internal ROM which is assigned a MAC (Media Access Controller) Address for the identification of Master/Slave Microcontrollers in the controller's network.

Device Controller's PIC (Peripheral Interface Controller) microcontroller communicates with serial port (Bluetooth) over UART [11] (universal asynchronous receiver/transmitter**)** using the following Mikro Basic Code:

```
if (UART1_Data_Ready() <> 0) then
uart_rd = UART1_Read()
bytetostr(uart_rd,uart_rd_str)
UART1_Write_Text(uart_rd_str)
delay_ms(2000)
end if
```

XIII. NETWORK CONTROLLERS (INTERFACE NODES)

Master Controllers communicate with other master and slave controllers in a network using interface called ***interface nodes***. ***Interface nodes*** utilize 2.4 GHz radio channel for short range communication or TCP/IP and http for long range communication. In case of Long distance communication, for example in Figure 7 shown below, when Master 1 and Master 2 are located at different remote sites **interface nodes** can shift to TCP/IP, http or GSM/GPRS [12] network connections for long range communication among clients. Clients can also share slave controller's status over company's Virtual Private Network or through Public Internet Gateways. Such setup forms a device network pool [13] which has the following features:

a. Controllers are aware of other Controllers using interface nodes.

b. Client to Client communication occurs either directly over http or by means of interface nodes in a star-network scheme.

c. Designated Client can be given more privileges.

d. Master Controllers can respond to alternate client in case one client fails.

e. Slave controllers can switch to alternate network in case one network fails, ensuring master-master communications.

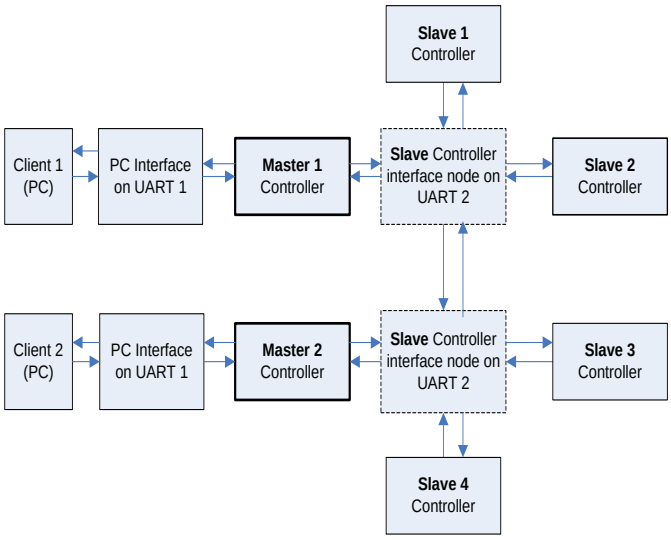

Figure 7: Block Diagram Master Controller connects to Slave Controllers using Slave interface node

XIV. SECURITY OF DATA COMMUNICATION

Communications between the alert issuing devices passing through the server all the way up to client receiving the alert are encrypted using XTEA (Extended Tiny Encryption Algorithm) securing the system from man in the middle attacks. We use the following XTEA [14] encrypt routine for encryption of data at the originating end.

```
void encrypt (uint32_t* data, uint32_t* key) {
uint32_t v0=data [0], v1=data[1], sum=0, i;
Uint32_t delta=0x9e3779b9;
uint32_t k0=key[0], k1=key[1], k2=key[2],
k3=key[3];
for (i=0; i<32; i++ )
{
sum += delta;
v0 += ((v1<<4) + k0) ^ (v1 + sum) ^ ((v1>>5) + k1);
v1 += ((v0<<4) + k2) ^ (v0 + sum) ^ ((v0>>5) + k3);
 }
data[0]=v0;
data[1]=v1;
```

We use the following XTEA decrypt routine for decryption of data at the receiving end. Note that output data (0) and data (1) are concatenated for combining the data.

```
void decrypt (uint32_t* data, uint32_t* key) {
uint32_t v0=data[0], v1=data[1], sum=0xC6EF3720, i;
uint32_t delta=0x9e3779b9;
uint32_t k0=key[0], k1=key[1], k2=key[2],
k3=key[3];
for (i=0; i<32; i++)
```

```
v1 -= ((v0<<4) + k2) ^ (v0 + sum) ^ ((v0>>5) + k3);
 v0 -= ((v1<<4) + k0) ^ (v1 + sum) ^ ((v1>>5) + k1);
sum -= delta;
data[0]=v0;
data[1]=v1;
```

XV. ALARM INTRUSION PREVENTION MECHANISM

Signal originating from each device has its hash code which changes every time a new timestamp is registered. This hash is fed as Key or Salt [15] to the encrypting algorithm.

```
void encrypt (uint32_t* data, uint32_t* key)
void decrypt (uint32_t* data, uint32_t* key)
```

Hash code is generated by using the following parameters:

Alert Code	Control Command	Date-Time Stamp	Device-MAC Address

XVI. RESULTS & CONCLUSION

The alarm device was simulated in Proteus for testing. Commands from a Bluetooth terminal [16] were tested by providing them to the program instructions encoded in to the Microcontroller's model in Proteus. Client was tested to be identifying on another client's GUI (Graphical User Interface) over World Wide Web and commands were sentover TCP/IP protocol from one client to another client connected to the alarm circuit. Previously, an alarm system is a set of electronic devices that has been set up to alert the administrators and local authorities related to an activity within a premise. On the other hand the development of a system based on our research is to alert the user in a remote area. The system is portable as it can be made accessible using handheld devices. Our Research offers support in improving existing security systems as well as extending systems beyond local networks [17] to internet ecosystem. The objective of the research was to develop a prototype of system complying with scalability, safety, efficiency and high production availability which have been successfully achieved to some extent while some areas such as making the system fail proof [18], are still open to further research [19] and enhancements to meet defensive military needs [20] as well as meeting regional standards [21].

ACKNOWLEDGMENT

The research council (TRC) is the premier technical body in Oman. As its representatives are in the campus of Dhofar University in Oman, it is the best suitable organization for faculties like us. Furthermore the peoples in the TRC are helpful and innovation friendly. Internet Service Provider, Oman telecommunication authority (Omantel) has a vast infrastructure of fibre optic wired network as well as wireless data connectivity. It is due to their outstanding provision of 24/7 data connectivity that has made our system successful with uninterrupted communication channel available at our disposal round the clock. We are grateful for the research labs and resources provided by the Dhofar University Salalah, Oman.

REFERENCES

1. Sheikh Izzal Azid and Sushil Kumar, 2011, "Performance of a Low Cost Based Home Security system", International Journal of Smart Home, The University of South Pacific, Fiji.
2. Wireless Technologies retrieved from: http://docwiki.cisco.com/wiki/Wireless_Technologies, last accessed on 2015.
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. Web based remote security system (WRSS) model development, Wanaka, S.V. ; Dept. of Electr. & Comput. Eng., Florida Int. Univ, Miami, FL, USA; De La Cruz, M. Published in Southeastcon 2000. Proceedings of the IEEE
5. Microsoft .NET framework retrieved from: http://www.microsoft.com/net Last accessed on: 2014
6. Web ASMX Service .NET Microsoft Technology retrieved from https://msdn.microsoft.com/en-us/magazine/cc163674.aspx last accessed on: 2015.
7. http://www.mikroe.com/ a website for development tools, compilers for programming microcontrollers and related hardware components, last accessed on: 2015.
8. http://www.labcenter.com/index.cfm source of simulator for PIC and other types of microcontrollers, Last accessed on: 2015.
9. http://www.bitpipe.com/tlist/Internet.html, last accessed on 2015.
10. Retrieved from: http://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/26704-nat-faq-00.html Last accessed on: Nov 10, 2014.
11. DNS Concepts and facilities retrieved from http://tools.ietf.org/html/rfc882 , Domain Names: Implementation & Specification retrieved from http://tools.ietf.org/html/rfc883, last accessed on Dec 25, 2014.
12. Retrieved from http://en.wikipedia.org/wiki/Tiny_Encryption_Algorithm Article explaining the algorithm released for the public domain called as TEA. With XTEA and XXTEA both modified versions of TEA against crypto-attacks are also explained, last accessed on Dec 25, 2014.
13. Y. Zhao and Z. Ye, 2008,"A Low Cost GSM/GPRS Based Wireless Home Security System", IEEE Transactions on Consumer Electronics, 54(2), pp. 567-572, 2008.
14. Jun Zhang, Hui Wang, Tianhua Meng and Guangming Song, 2011,"Design of a Wireless Sensor Network Based Monitoring System for Home Automation", International Conference on Future Computer Sciences and Application (ICFCSA), pp. 57-60, Nanjing, June 2011.
15. UART communication document retrieved from: https://www.freebsd.org/doc/en_US.ISO8859-1/articles/serial-uart/, Last Accessed on Dec 2015.
16. Grain of Salt: An Automated Way to Test Stream Ciphers through SAT Solvers, Mate Soos, Research paper available at http://gforge.inria.fr/frs/download.php/27285/grainofsalt-1.1-desc.pdf, Last accessed on Feb, 14 2015.
17. Chun-Liang HSU, Sheng-Yuan Yang and Wei-Bin Wu, 2009,"Constructing Intelligent Home- Security System Design With Combining Phone-Net And Bluetooth Mechanism", Proceedings of the Eighth International Conference on Machine Learning and Cybernetics, St. John's University, Taiwan.
18. Mega lingam R.K, Nair R.N, Prakhya S.M, Mohan M,2011 " Low Power, intelligent, wireless, home security system for elderly people", Third International Conference on Electronics Computer Technology (ICECT) Proceedings , Volume 4, Page 320 -324.
19. WIRELESS HOME SECURITY SYSTEM WITH MOBILE, Prof. (Dr.) Khanna SamratVivekanand Omprakash, Published in International Journal of Advanced Engineering Technology
20. Using Security Logs for Collecting and Reporting Technical Security Metrics, Risto Vaarandi and Mauno Pihelgas, published in 2014 IEEE Military Communications Conference and also included in Proceedings of the 2014 IEEE Military Communications Conference
21. A study of the compliance of alarm installations in Perth, Western Australia: Are security alarm systems being installed to Australian Standard AS2201.1 - "systems installed in a client's premises." , Originally published in the Proceedings of 7th Australian Information Warfare and Security Conference, Edith Cowan University, Perth Western Australia, 4th - 5th December, 2006.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Appendix A

1. Server Side Code Excerpts

a. Commands RX function on the server side is implemented as web method in C# programming language:

```
    [Web Method]
    public string Receive Command(string str Client)
    {
        string strCommand = string.Empty;
        for (int i = 0; i < arrCommand.Count; i++)
        {
            string[] strTo =
arrCommand[i].ToString().Split(':');
            if (strTo[0].ToString() == strClient)
            {
 for (int j = 1; j < strTo.Length; j++)
         strCommand = strCommand + strTo[j] + ":";
                }
Arr Command. Remove At(i); break;
        return strCommand;
```

b. Commands TX function on the server side is implemented as web method in C# programming language:

```
  [Web Method]
    public void Send Command(string str From Client,
string strToClient, string strCommand)
    {
        arrCommand.Add(strToClient + ":" + strFromClient
+ ":" + strCommand);
    }
```

c. Client addition and removal is managed by the following set of functions in C#

```
    [Web Method]
    public void AddUser(string strUser)
    {
        bool bFlag = false;
        for (int i = 0; i < arrUsers.Count; i++)
        {
   if (arrUsers[i].ToString() == strUser)
    bFlag = true;
else
  SendMessage("Ser@ver", arrUsers[i].ToString(), strUser
+ " has logged in.");
        }
if(bFlag == false)
  arrUsers.Add(strUser);
    [Web Method]
    public void AddClient(string strClient)
    {
bool bFlag = false;
  for (int i = 0; i < arrClients.Count; i++)
        {
    if (arrClients[i].ToString() == strClient)
                bFlag = true;
  else
     SendMessage("Ser@ver", arrClients[i].ToString(),
strClient + " has logged in.");
        if (bFlag == false)
            arrClients.Add(strClient);
```

d. Information on Users and Clients is available by call to the following functions in C#

```
    [Web Method]
    public string GetUsers()
        string strUser = string.Empty;
        for (int i = 0; i < arrUsers.Count; i++)
        {
     strUser = strUser + arrUsers[i].ToString() + "|";
        return strUser;
    [WebMethod]
    public string GetClients()
        string strClient = string.Empty;
        for (int i = 0; i < arrClients.Count; i++)
        {
            strClient = strClient +
arrUsers[i].ToString() + "|";
        }
        return strClient;
```

2. Client Side Code Excerpts:

Initiating a command by the user:

```
            try
            {
Check User Authenti cation(user name, user Pass, terminal
ID);
Get Current Device Status(Client Name);

if (e.KeyChar == '\r')
                {
if (InputCommand.Trim().Length > 0 ||
InputCommand.Rtf.Trim().Length > 129)
                    {
EncryptCommand(InputCommand, key);
InputCommand.Clear();// for security reasons
ctrlService.SendCommand(ClientName, UserName,
EncryptedCommand.Text);
catch (Exception ex)
Form1.stat = "Error in sending command" ;
 CheckSecurity();     // Check Security parameters
  CacheTransactions();       // Save the desired command
and event for auto-reinitiating.
ErrorRecoveryProcedure();   // Try again for set duration
by resending the command.
LookupForAlternateRoute();   // involved rechecking for
network availability and alternate network.
            }
```


Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)