INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN 2278 – 0211 (Online)

A Framework for GSM-Based Video Surveillance with Cloud Storage, Nigerian Perspective

Nwokolo Chinyere Pauline
Lecturer, Department of Computer Engineering, Federal Polytechnic, Oko Anambra State, Nigeria
Nwankwo Vincent Ikechi
Lecturer, Department of Electronic and Computer Engineering, Nnamdi Azikiwe University, Nigeria

Abstract:
This paper presents a framework for On-Demand Cloud-Based Real-Time Video Surveillance (OD-CBRTVS) system which is activated either by phone call or SMS. It is based on GSM and IP (Internet Protocol) technology which enable the system to render on-demand video surveillance with remote storage. GPS (Global Positioning System) technology has been deployed to acquire location data of subscribers (clients). The system comprises a Master Control Station (MCS) which receives request for service from subscribers and a number of client stations each of which has some surveillance IP cameras. It features a distributed processing scenario such that when a request for service signal is sent to the MCS by a client from an arbitrary location, the request is decoded according to the registered location data of the subscriber and the signal is sent to the appropriate client station for video surveillance service rendering. GSM modules have been used to enable communication between the master control station, and the client stations, while IP video surveillance infrastructure has been utilized to handle video capture and cloud-based storage. The system automation has been achieved by interfacing a GSM module to PIC18F4550 microcontroller unit at the MCS (or base station) to enable PC interface, while PIC18F4520 units were used at the client stations which require no connection to PC.

Keywords: *Master control station, client station, video surveillance, GSM, cloud-based storage*

1. Introduction

Criminal activities have been an issue of global concern with varying degrees from country to country. In Nigeria for example, crime has evolved over the years from the use of traditional weapons to the more sophisticated weapons and the advanced free fraud today. Political, religious, and ethnic/tribal violence are also common place. Clandestine activities of various cult groups and various forms of ritual killings are frequent occurrences. In northern Nigeria, religious violence and terrorist attacks is peculiar, in the South-South, militancy is popular and like extremist attacks in northern Nigeria, it has received global attention. In the South-East, cultism ferocity and robbery attacks are common forms of violence, while in the South West, political violence and thuggery are intrinsic. The list is not exhaustive. Fig.1. is the map of Nigeria showing the six geopolitical regions and the thirty-six states of federation including the centrally located Federal Capital Territory (FCT), Abuja which is the proposed site for the Master Control Station of the surveillance infrastructure.

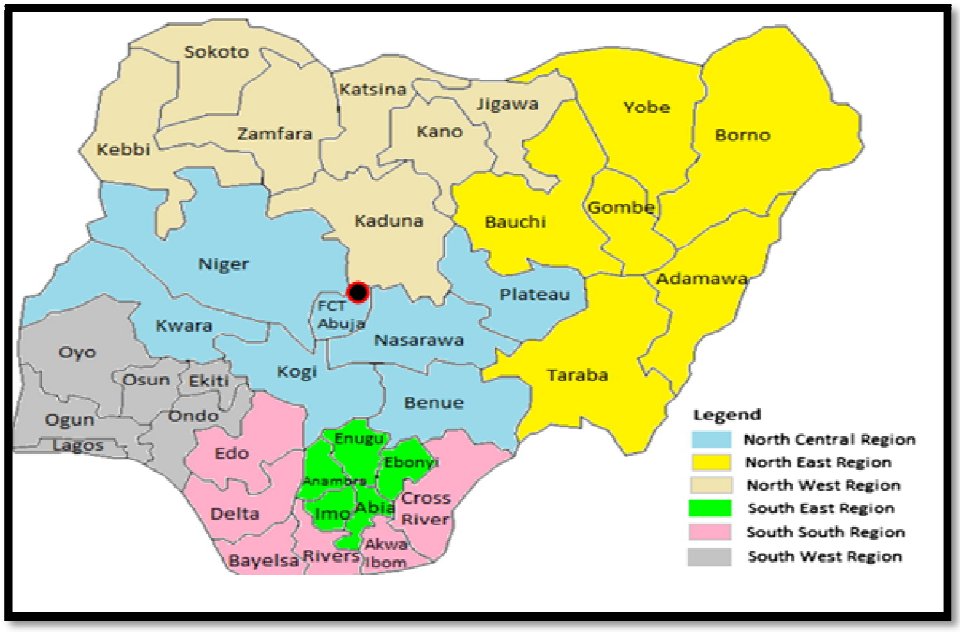

Figure1: Map of Nigeria Showing the Six Geopolitical Regions

As criminal activities increase, the need to visually monitor and record events in an organization's environment has become even more important. It is known that there exists a strong tie between governance and economic growth. Interestingly, the current federal government administration is bent on fighting corruption, this fight must take off from the basics through instituting democratically elected leaders indeed who go in by votes of the masses not by election rigging. Nigeria has got to a stage where every event that matters must be kept under video surveillance with remote storage for transparency if corruption must be fought and won. The word surveillance comes from a French phrase for "watching over" (*sur* means "from above" and veiller means "to watch") and is in contrast to more recent developments such as sousveillance (Minsky & Mann, 2013)

Essentially, the use of a real-time on-demand video surveillance with cloud-based storage model for migration of traffic capture onto a converged infrastructure, such as server cluster mainframe computer storage will be presented in this work.

Security consciousness has consequently risen among all the nations, especially, since after the tragic incident of September 11, 2001 attacks on the world trade centre in New York City during which 2996 deaths were recorded, with about 6000 injured (Mathew J. Morgan, 2009). These incidents of crime often occur without anybody being able to trace the perpetrators. As a result, a lot of research work have been ongoing to combat crime.

A framework for a cloud-based multimedia surveillance system was proposed by Anwar Hossain (2014). The author highlighted several research and technical issues which include large storage demands and optimal strategies for sensor data acquisition among others. The framework being presented in this paper integrates on-demand feature by enabling the system to be activated only by SMS or Phone call. This automatically filters the input data being acquired by the deployed surveillance cameras such that only relevant data are captured and stored.

Adeyemo et al. (2016) presented a framework for a Cloud Based Health Monitoring System. In the study, the Cloud database acted as the central data bank to which user's medical data can be uploaded from both mobile device applications and web browser devices and then downloaded for analysis by the medical practitioner for user's (patient) monitoring and guidance. The authors focused on leveraging the cloud infrastructure for managing medical data as it concerns the patients and the doctors.

2. Components of the Proposed System

The system is highly encompassing and sits at the centre of various arms of engineering and a good number of technologies as depicted in Figure 2.

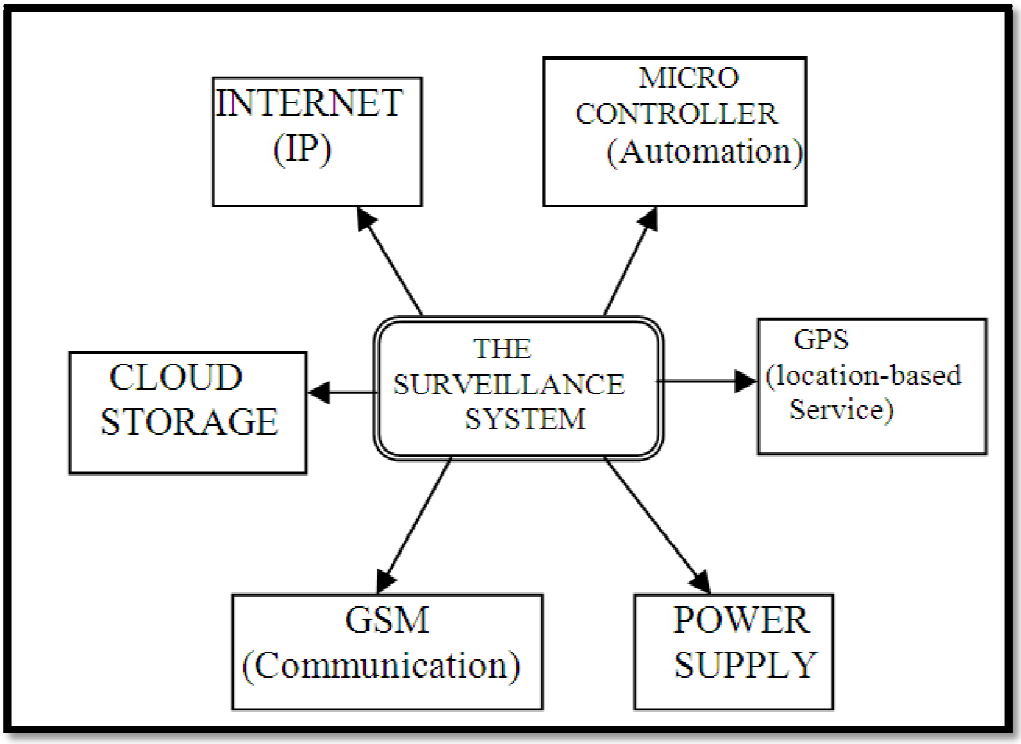

Figure 2: Technologies, Protocols and Systems Involved in Developing OD-CBRTVS

3. Overview of OD-CBRTVS

A subscriber (client) could send a request signal either by phone call or SMS from anywhere to the Master Control Station (MCS) which checks the client's validity. If client is found valid, the MCS determines the class of request and sends the signal to the Client Station (CS) in charge of the client. The MCS sends service activation signal to the corresponding client's location and triggers surveillance action over the area for instantaneous video capture into the cloud network.

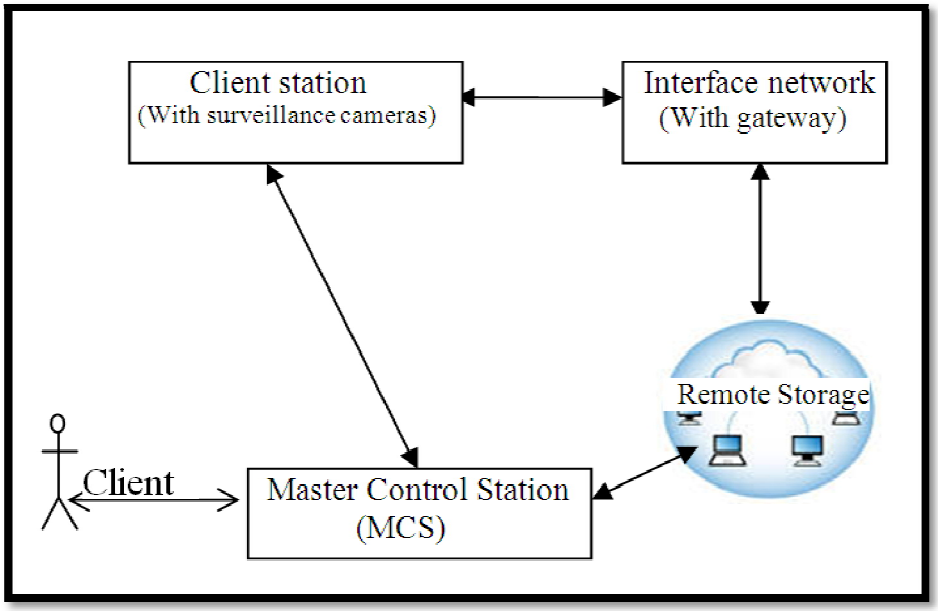

Figure 3: Block Diagram of Proposed OD-CBRTVS

In Fig. 3, signal is sent by client with mobile phone from arbitrary location to the master control station which is linked to a control station that handles the particular client location.

Table 1 contains a list of 36 states in Nigeria with the corresponding state codes which identify each state. A client control station is located at each state capital to render on-demand surveillance to subscribers to the system.

S/No.	State	State Code	Client Station Location
1.	Abia	001	Umuahia
2.	Adamawa	002	Yola
3.	Akwa Ibom	003	Uyo
4.	Anambra	004	Awka
5.	Bauchi	005	Bauchi
6.	Bayelsa	006	Yenegoa
7.	Benue	007	Makurdi
8.	Borno	008	Maiduguri
9.	Cross River	009	Calabar
10.	Delta	010	Asaba
11.	Ebonyi	011	Abakaliki
12.	Edo	012	Benin
13.	Ekiti	013	Ado-Ekiti
14.	Enugu	014	Enugu
15.	Gombe	015	Gombe
16.	Imo	016	Owerri
17.	Jigawa	017	Dutse
18.	Kaduna	018	Kaduna
19.	Kano	019	Kano
20.	Katsina	020	Katsina
21.	Kebbi	021	Birnin Kebbi
22.	Kogi	022	Lokoja
23.	Kwara	023	Ilorin
24.	Lagos	024	Ikeja
25.	Nasarawa	025	Lafia
26.	Niger	026	Minna
27.	Ogun	027	Abeokuta
28.	Ondo	028	Akure
29.	Osun	029	Oshogbo
30.	Oyo	030	Ibadan
31.	Plateau	031	Jos
32.	Rivers	032	Port Harcourt
33.	Sokoto	033	Sokoto
34.	Taraba	034	Jalingo
35.	Yobe	035	Damaturu
36.	Zamfara	036	Gusau

Table 1: Client Control Stations in 36 States of the Federation

3.1. OD-CBRTVS IP Video Surveillance System

The OD-CBRTVS IP surveillance is a form of digitized and networked version of closed-circuit television. In an IP surveillance system, an IP camera records video footage and the resulting content is distributed over an IP (Internet protocol) network. Digitization offers a number of benefits over traditional analogue CCTV, including:

Improved search capability.

Greater ease of use.

Better quality images and no degradation of content over time.

The ability to record and play simultaneously.

Content compression for improved storage.

The IP cameras use the Internet Protocol (IP) that runs on Local Area Networks (LANs) to transmit video across data networks in digital form. IP can optionally be transmitted across the public internet, allowing users to view their cameras through any internet connection available through a computer or a 3G phone.

3.2. IP Network-Centric Video Surveillance

Cisco systems proposed recommendations on how to build third- and fourth-generation video surveillance systems in a white paper [7]. The business case for adopting such architectures was articulated. Such video surveillance architecture provides several benefits which include;

- Increased reliability
- Higher system availability
- Greater utility (any camera to any monitoring/ recording device for any application, anywhere)
- Increased accessibility and mobility
- Multivendor video surveillance system "best of breed" interoperability
- Ability to enhance other building management system capabilities through improved interoperability

4. Methods

The system design features distributed processing by having a centralized Master Control Station (MCS) and distributing the work to multiple control stations which are client stations (or client locations) as shown in Fig.4.

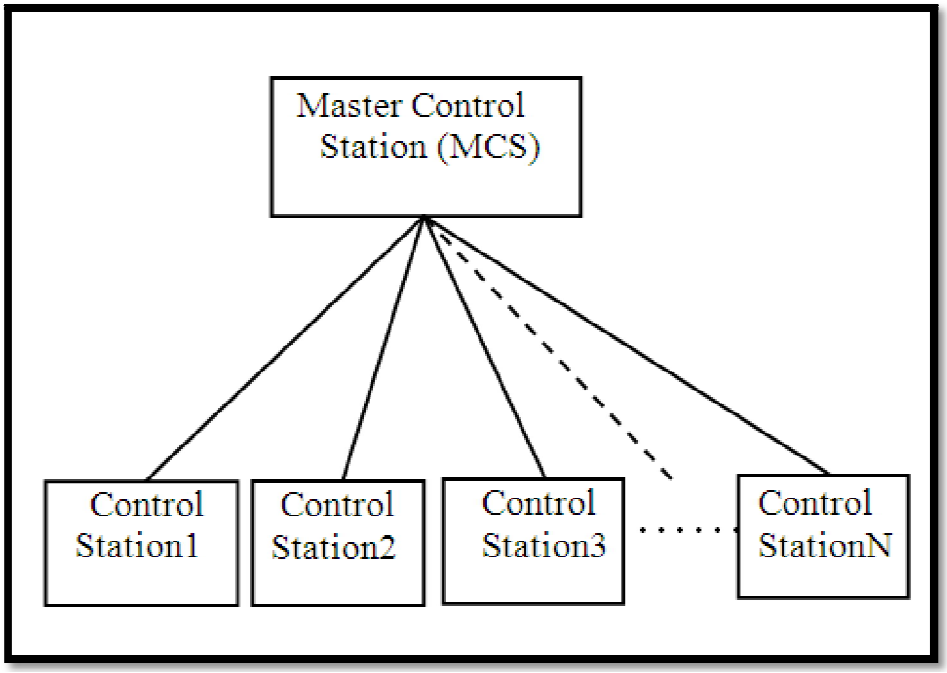

Figure 4: Single Master Node / Sub-Control Model

While this model is simple for process control, it has an implicit drawback in that all processes communicate with one master node and hence a potential communication bottleneck (Rallings et al.1998). However, as the number of processing nodes increases extra communication (sub-control nodes) could be introduced to share the communication burden. When and how these extra nodes are added depends upon the number of processing nodes, the channel capacity, and the data management strategy. The idea behind the surveillance infrastructure being discussed is that there is a centrally located base station (the master control station) connected to a number of control stations to which client cameras are connected, such that there is a distributed arrangement as shown in Fig. 5.

Typical surveillance systems have high demand for large storage to store huge amount of data coming from multiple sensors. These data are processed in real-time and often in an off-line fashion to detect safety events (Rodriguez-Silva et al. & Chang et al ,2012). However, typical surveillance systems cannot cope with the continuous demand for massive storage. A cloud storage comes as a remedy with the ability to link up various types of network Storage devices to meet specific requirements of surveillance systems.

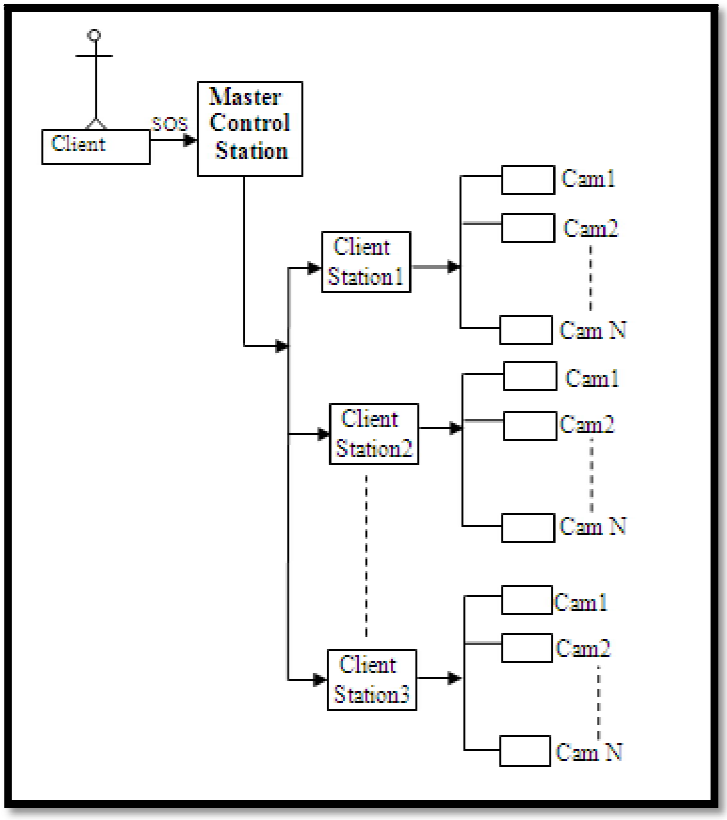

Figure 5: A Distributed Arrangement of OD-CBRTVS

A distributed system is a model in which components located on networked computers communicate and coordinate their actions by passing messages (Coulouris et al., 2012). A computer program that runs in a distributed system is called a distributed program, and distributed programming is the process of writing such programs (Andrews & Gregory, 2000).

5. Hardware Design

The hardware design is conceptually made up of subsystems which comprise a master control station (or base station) wirelessly linked to client stations in such a way that each master control station is connected to a number of client stations within its service domain. This arrangement conforms to the distributed systems scenario as shown in Fig. 5.

5.1. Master Control Station (MCS)

Every request signal from client's GSM handset is received at the master control station (Fig.6) via the GSM module connected to PIC 18F4550 MCU (Microcontroller Unit). The unit decodes the call or SMS to know control station meant to process the request and sends the request to the station to render video surveillance as a service.

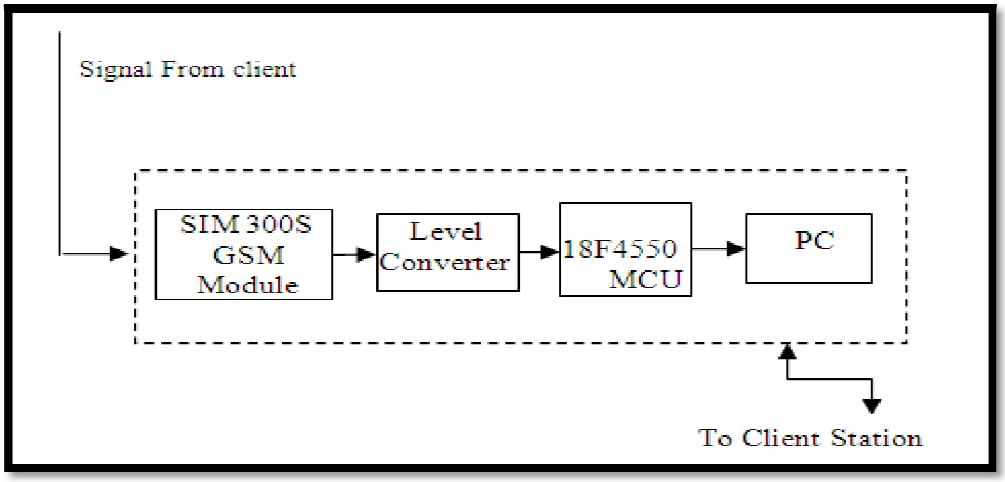

Figure 6: Master Control Station Block Diagram

5.2. Client Station (CS)

The Client Station (Fig.7) consists of GSM module which receives signal from the MCS, determines with the aid of the microcontroller initiates surveillance action over the area according to the request from the client end. The location of each subscriber (client) to this system is equipped with broad band internet connectivity. The modem is connected to router, and the router to the DVR to which the digital cameras are connected (Fig.9). The outdoor camera rotation is controlled by servomotor such that one camera can serve a number of clients.

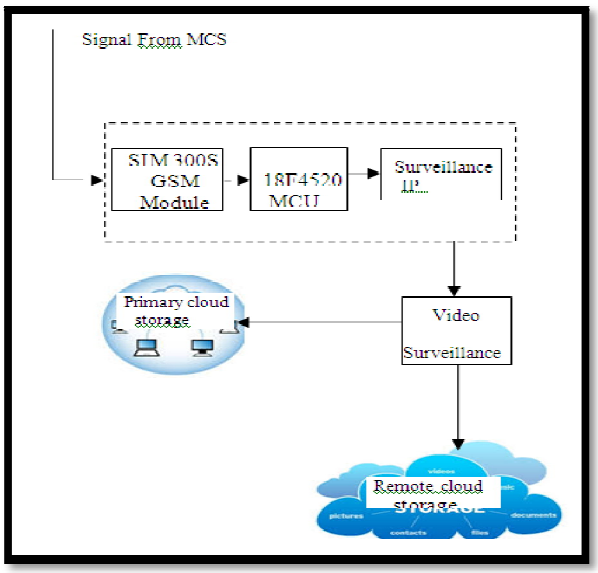

Figure 7: A Client Station Block Diagram

A client (or subscriber) can send request at any time from anywhere to the MCS which validates the request and triggers video surveillance at the client's location. The entities are primarily linked up by GSM network. The client station receives commands via SIM 300S GSM module connected to 18F420 MCU which triggers the system to capture and transmit for as long as commanded when valid signal is received. A flowchart for the client station is shown in Fig.8.

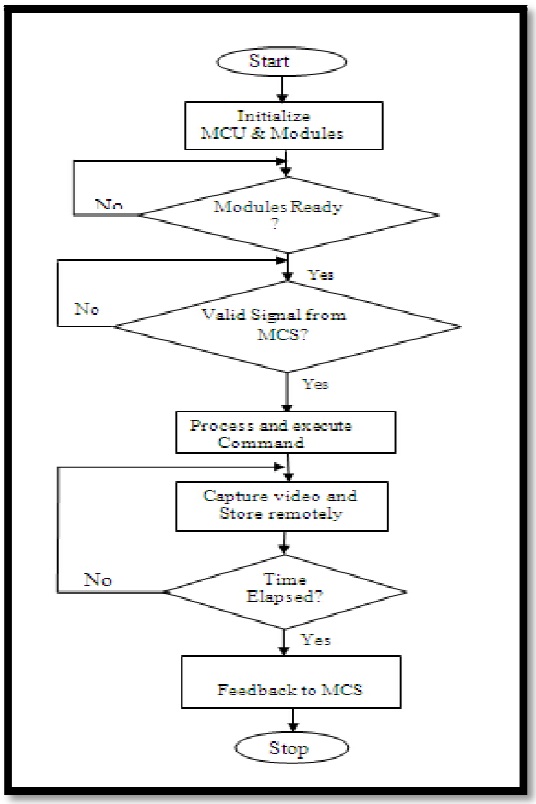

Figure 8: Client Station Flowchart

The MCS flowchart is shown in Fig.9.

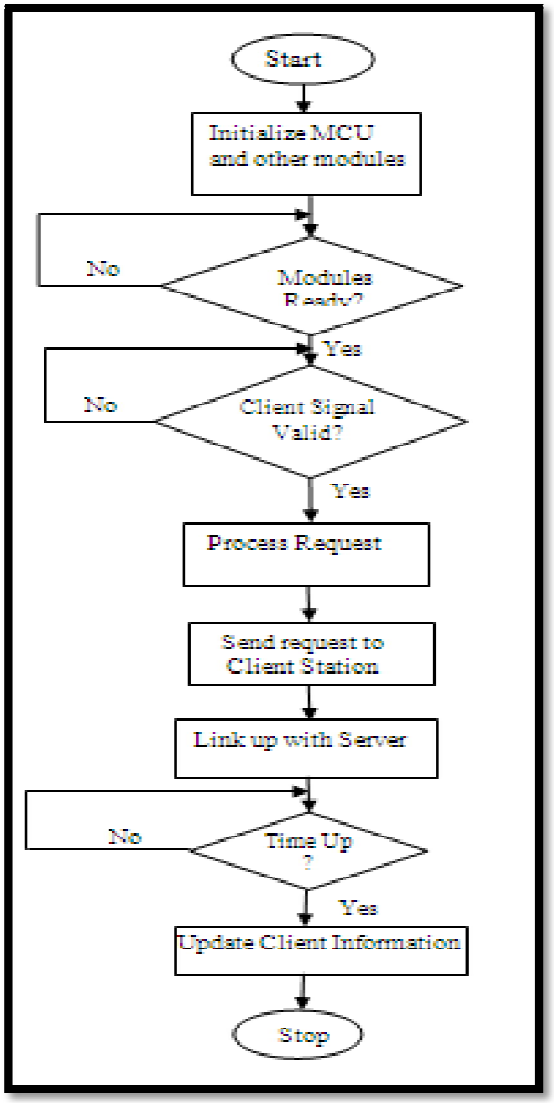

Figure 9: Master Control Station Flowchart

Every request for service primarily goes to the Master Control Station which determines the client station to handle a particular request.

From the master control station operation flowchart in Fig.9, when the system is powered up, the MCU and other modules initialize. The system checks whether the modules are ready, followed by whether there is any valid request signal from clients. If any valid signal is detected, control is transferred to the client station responsible for covering the location. The cameras are activated and video recording with remote storage is carried out according to the request.

As a control measure, the MCS should always send a control command (precisely "**CL**") as a prefix to the receiving station each time a valid request is to be executed.

6. Hardware Prototype for OD-CBRTVS

A hardware prototype of the system has been designed and implemented using a master control station and a client station as shown in the block diagram (Fig.10).

In the prototype, client's location and subscription data were stored in the database residing in the EEPROM of the MCS microcontroller, which is referenced as a lookup table on reception of valid signal. In computer science, a lookup table is an array that replaces runtime computation with a simpler array indexing operation. This significantly helps save processing time.

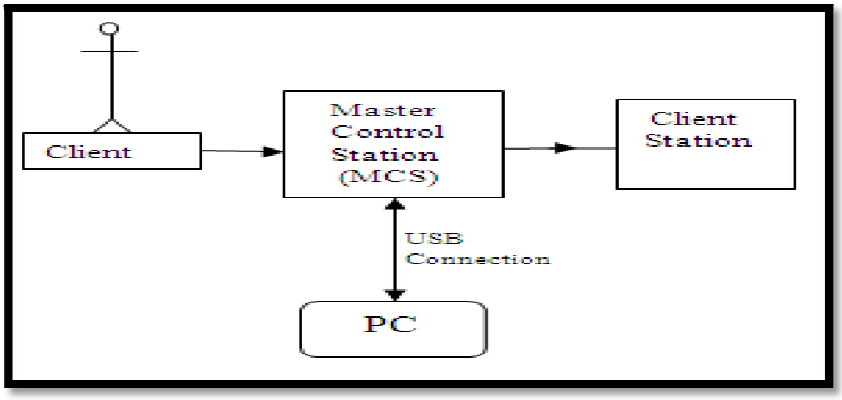

Figure 10.: A Block Diagram of Hardware Prototyp of an *MCS Connected to a Client station*

The MCS is connected to PC via USB. The PC contains a VB.Net database management application which was designed for updating client's location data in the EEPROM of the microcontroller. These location data serve as look-up table to the microcontroller. The application enables direct read/write access to the database.

7. Conclusion

The framework so developed has the flexibility to cover both as little as a small city, and as wide as the globe depending on channel capacity and management strategy. As an application, video surveillance has demonstrated its value and benefits countless times by providing real-time monitoring of a facility's environment, people, and assets, recording events for subsequent investigation, proof of compliance and audit purposes, which helps give zero tolerance to corruption. The system is very cost effective considering cloud storage and ultra-filtration feature due to GSM-only activation.

8. References

i. B. Adeyemo et al. (2016). Framework for a Cloud Based Health Monitoring System. http://ceur-ws.org/Vol-1755/136-140.pdf
ii. Clarke, R. (1988). Information technology and data veillance. Communications of the ACM, 31(5), 498–512.
iii. Coulouris, George; Jean Dollimore; Tim Kindberg; Gordon Blair (2011). Distributed Systems: Concepts and Design (5th Edition). Boston: Addison -
iv. D. A. Rodrıguez-Silva, et al. (2012) "Video surveillance based on cloud storage," in Proceedings of the IEEE 5th International Conference on in Cloud Computing (CLOUD '12), pp. 991–992.
v. Mathew J. Morgan (August 4, 2009). The Impact of 9/11 on Politics and War: The Day that Changed Everything? Palgrave Macmillan. P.222. ISBN0- 230-60763-2.
vi. M. Anwar Hossain (2014). Framework for a Cloud-Based Multimedia Surveillance System. Hindawi Publishing Corporation. International Journal of Distributed Sensor Networks.Volume 2014, Article ID 135257, http://dx.doi.org/10.1155/2014/135257
vii. Michael, K., Roussos, G., Huang, G. Q., Gadh, R., Chattopadhyay, A., Prabhu, S., & Chu, P. (2010). "Planetary-scale RFID services in an age of uberveillance". Proceedings of the IEEE, 98(9), 1663–1671
viii. Minsky M, Kurzweil R, Mann S (2013). "The Society of Intelligent Veillance", Proceedings of the IEEE ISTAS 2013, Toronto, Ontario, Canada, pp 13–17
ix. Philip J. Rallings et al. (1998). Parallel Distributed Processing for Digital Terrain Analysis.
x. R.I.Chang et al (2012). Effective distributed service architecture for ubiquitous video surveillance, Information Systems Frontiers, vol.14,no.3,pp. 499–515.Wesley.ISBN 0- 132-14301-1.
xi. Andrews, Gregory R. (2000), Foundations of Multithreaded, Parallel, and Distributed Programming, Addison–Wesley, ISBN 0-201- 35752-6.
xii. White Paper SPRA951A – Introduction to Video Surveillance Systems Over the Internet Protocol, October 2003.