CHAPTER ONE

INTRODUCTION

1.1 Background of Study

Remote sensing is the acquisition of information about an object or phenomenon without making physical contact with the object and thus in contrast to on-site observation. Remote sensing is used in numerous fields, including geography, land surveying and most Earth Science disciplines for example, hydrology and ecology (Giacomo, Grazia., Marcin & Robertas, 2016). Other fields where remote sensing is used include oceanography, glaciology, geology. It also has military, intelligence, commercial, economic, planning, and humanitarian applications.

In current usage, the term "remote sensing" generally refers to the use of satellite- or aircraft-based sensor technologies to detect and classify objects on Earth, including on the surface and in the atmosphere and oceans, based on propagated signals (e.g. electromagnetic radiation). It may be split into "active" remote sensing (i.e., when a signal is emitted by a satellite or aircraft and its reflection by the object is detected by the sensor) and "passive" remote sensing (i.e., when the reflection of sunlight is detected by the sensor) (Schowengerdt, 2007; Schott, 2007; Liu, Philippa, Guo & Mason, 2009; Guo, Huang, Li., Sun, & Zhang, 2013).

In this research, infrared surveillance cameras would be used as excellent examples of both passive and active sensors, to be automatically activated for video capture and storage from a remote location. During a bright sunny day, enough sunlight illuminates the targets which reflect toward the camera lens such that the camera simply records the radiation from sunlight which is reflected by the sensed object (passive mode). On a cloudy day or inside a room, there is often not enough sunlight for the camera to record the targets adequately. Instead, it uses its own infrared energy source - a flash - to illuminate the targets and record the radiation reflected from the targets (active mode).

Surveillance systems have been a key component of many organization’s safety and security group for decades. 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.

Interestingly, criminal activities have tremendously increased especially at places of high national security all over the world. There is also increased threat from armed robbers and hoodlums who invade locations of both public and private interest even in broad daylight and at night. 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. The attacks killed 2,996 people, injured over 6000 others, and caused at least $10billion in property and infrastructure damage (Morgan, 2009). These incidents of crime often occur without anybody being able to trace the perpetrators. There is therefore no reason to wait until it happens to one. The prevention or resolution of just one crime would be enough to pay for video surveillance system many times over.

As security concerns increase, the need to visually monitor and record events in an organization's environment has become even more important. Moreover, the value of video surveillance has grown significantly with the introduction of motion, heat, and sound detection sensors as well as sophisticated video analytics. As a result, many nontraditional groups have also found value in video monitoring and recording. In transportation, video surveillance systems monitor traffic congestion. In retail shops, video can be helpful in identifying customer movement throughout a store, or serve to alert management when the number of checkout lines should be changed. Some video analytics packages even offer the ability to identify a liquid spill and generate an alert enabling faster response by custodial services, thus avoiding a slip and fall situation. Product and package shipment operations can use recorded video to help track and validate the movement of cargo and help to locate lost packages. Additionally, video surveillance can be integrated to complement access control policies, providing video evidence of access credential use. Video surveillance has evolved not only in its application, but also in its deployment.

This evolution of video surveillance, includes the emergence of the fourth generation of video surveillance systems which is known for being network-centric. These systems are realized through an open, standards-based, internet protocol functional and management architecture.

Essentially, this work introduces an on-demand cloud based model which would be activated by GSM only, for migration of traffic capture onto a converged infrastructure, such as server cluster mainframe computer storage. The adoption of a

network-centric system architecture that meets the extensive requirements for a real time video surveillance will offer remedial alternatives to security challenges in mission critical environments. A cloud computing based IP video surveillance architecture could provide several benefits such as;

i. Increased reliability

ii. Higher system availability

iii. Greater utility (any surveillance camera to any monitoring or recording device for any application, anywhere)

iv. Increased accessibility and mobility

v. Multivendor video surveillance system i.e. interoperability.

In the Nigerian system, issues of security threats, attacks and violence are still on the increase. For instance, electoral malpractices at polling stations during election processes have been the order of the day. Armed robbery attacks including snatching of cars go on day and night both in the streets and on the highways. The boko-haram incidents have remained worrisome till date. There is therefore an obvious need for a system such as the On-Demand Real-Time GPS-Based Remote Security Video Sensing System which would subsequently be referred to as OD-RGRSVS or simply RGRSVS for ease of reference. The proposed OD-RGRSVS is a cloud model that would be basically activated for real-time video capture and cloud storage by only valid GSM signal. Optimization strategies such as virtualization at the primary and secondary cloud server clusters, load balancing at the video surveillance gateways, and CPU task scheduling would be applied with the dynamic behavior of the network traffic profiled for performance analysis that would yield results for satisfactory QoS.

1.2 Statement of the Problem

Astronomical rise in crime rate: Insecurity of life, property and infrastructure is increasing in Nigeria and world over at an alarming rate with crime wave rising astronomically. This necessitates real time monitoring to capture crime scenes from remote locations. The causes of insecurity include but are not limited to; determined hoodlums with political motivations, cult members' molestations, armed gangs and robbery activities. Examples include; invasion of banks even in broad daylight, car snatching day and night, hired assassination menace which may or may not be politically motivated, and incidents of loss of human lives sometimes on a very large

scale and without any solution in sight. All these are now the order of the day. Sadly, security agencies many a time arrive at crime scenes when the bandits must have concluded their attacks and gone. These affect lives and infrastructure at places of gathering such as stadia, open squares, churches, eating places, shopping malls, market places, schools offices and homes. The failure of organized surveillance apparatus to combat the problem is worrisome.

Surveillance Video processing of irrelevant footage: Many of the conventional video surveillance systems are triggered to capture and store video footage by mere motion, heat or sound sensors. This leads to capture and storage of both relevant and irrelevant camera footage which wastes huge amounts of storage space.

Storage space limitations of video footage: Despite the application of video compression formats including H.264, many video surveillance systems still battle with storage limitations being not cloud-based. Many surveillance systems usually store camera footage from 30 to 90 days. For home / Do-It-Yourself type of simple IP camera setup, it usually lasts 2 days - 7 days. Many a time, the system will auto-overwrite the earliest video records once the storage capacity has been reached thereby being forced to adopt First-In-First-Out (FIFO) queuing discipline simply because of storage space limitations

Vandalization of on-site video surveillance storage infrastructure : On-site video surveillance infrastructure such as DVR with local storage are subject to vandalism. There is therefore a continuous search for ways to mitigate these problems not only by governments and corporate bodies but also private individuals.

1.3 Research Aim and Objectives

The aim of this dissertation is to develop a real-time GPS-based remote security video sensing system. The specific objectives are as follows;

- To develop a real-time on-demand remote sensing framework that can be activated by phone call or SMS from any location and store sensed video data to the cloud.
- To design and build a prototype of real-time GPS-based on-demand remote security video sensing system.
- To develop a business model that provides automated on-demand remote video sensing to subscribers.

- To develop a mathematical model for the cloud storage sever clusters and characterize requests to the system as a Poisson process
- To develop an algorithm for instantaneous data capture and transmission into the cloud.
- To simulate the real-time remote video sensing system with cloud storage and provide precise information on the throughput, latency and resource utilization for satisfactory Quality of Service.
- To validate the simulated model using a suitable simulation software.

1.4 Justification for the Research

- There is need to capture crime scenes and provide secure video evidence especially now that crime is on the increase.
- It is important to eliminate irrelevant footage in order to reduce storage cost at such a time when there is geometric and progressive rise in huge amounts of data processed by video surveillance apparatus.
- Therefore, on-demand video capture will help to limit data capture to only what is necessary.

Elimination of irrelevant footage processing would help to bring down processing overhead at the video surveillance infrastructure nodes by obviating the need to commence video footage filtration after unwanted video recordings must have taken place.

Threatening attacks are painful reality in today's organizations and societies. Physical security vulnerabilities often lead to advanced kidnapping, assassination, thefts, pipe line and power grids vandalization, burglary and rape. On-Demand Real-Time GPS-Based Remote Security Video Sensing (OD-RGRSVS) system is a modernized paradigm proposed for homeowners, businesses, governments and corporate bodies. A robust OD-RGRSVS leverages on phone call or SMS from a client to activate surveillance IP camera which will instantaneously get rid of capture and storage of unwanted footage. The use of such a video surveillance system would help view the recorded incidents of interest, be it crime scene to identify the burglar for legal prosecution, or ceremonial event with ease. With such a properly configured on-

demand video surveillance apparatus with cloud-based storage, virtually unlimited archiving of only relevant video footage would be achieved.

1.5 Scope of the Research

The system presented in this work is based on GSM, GPS and telecommunication infrastructure technologies involving interface video matrix switches, video surveillance gateways, and cloud based NVR server storage clusters. Digital surveillance IP cameras with day/night and infrared capabilities, including Network Digital Video Recorder (NDVR) with cloud storage will be explored in the context of Tier-4 evolution. The system is designed to be scalable and modeled to provide precise information on the throughput, latency and other network metrics to avoid overloading the system by too many subscribers. Video recordings from the cameras are transmitted to the cloud via the internet for predictive analytics.

CHAPTER TWO

LITERATURE REVIEW

There has been a continuous effort to develop effective monitoring and data capture models that would help researchers sense things about the earth without physically being present at the location (i.e. remote sensing). Nowadays, it is observable that video surveillance systems which comprise surveillance cameras are increasingly deployed to monitor locations and/or events of interest, capture videos and instantly transmit video feeds to either a local or remote storage for various purposes such as crime prevention or deterrence, control events, healthcare, cargo tracking, etc. The wide application areas of video surveillance has led to many works having been done in this area.

2.1. Overview of Video Surveillance Systems

2.1.1. Raptor Nests Monitoring

A video surveillance system for monitoring raptor nests in a temperate forest was proposed. The authors (Lewis, DeSimone, Titus, & Fuller, 2004) monitored northern Goshawk Archipelago and the narrow strip of mainland coastal mountains in southeast Alaska. A video surveillance system excluding batteries and charger was developed. A Video tape was analyzed and used to extract desired video record of nest behavior as many times as necessary to verify their behavior. The system consisted of a miniature color video camera (total vision model mx-40), a time lapse video recorder (VCR, GYYR model TLC2100) and a portable black and white television. Average of 154 deliveries were documented. Some of the deliveries were however unidentified resulting from poor light, bright and blocked camera.

2.1.2. Road Accident Analysis System

Mahmud and Zarrinbashar (2008) explored worldwide interoperability for Microwave Access (WiMax) and General Packet Radio Service *(*GPRS) communications to connect to the server for data computing. The authors sought to find a complete solution for monitoring and managing accident data based on Geographical Information System (GIS) and its related telecommunications infrastructure. An evaluation of the performance of GIS based solution for WIMAX and GPRS integration was carried out in order to develop a multiplatform middle-ware for real-time monitoring and automated services. A derivative of their proposal is a data

warehouse for real-time smart decision support system for automated service and analyses. The system offers location based services by enabling the user access the video of a monitored resource through a handset or laptop and in real-time. Furthermore a Satellite-based Alarm and Surveillance System (SASS) was additionally designed to provide connectivity between alarm and surveillance system on one side, and security centers and other receivers on the other. The SASS system concept supports in-built alarm, video, audio and data transmission capability, with the terminal linked to a gateway station via a geostationary satellite.

2.1.3. Computer Vision System for In-House Video Surveillance

Cucchiara, Grana, Prati, and Vezzani (2005) discussed an in-house video surveillance that controls the safety of people living in domestic environments. In particular, the indoor video surveillance, makes it possible for elderly and disabled people to live with a sufficient degree of autonomy, via interaction with technology. This could be distributed in a house at affordable costs and with high reliability. The authors managed to incorporate moving object detection modules that could disregard shadows. OD-RGRSVS is designed to get rid of attempting to process irrelevant video footage in any form.

2.1.4. Closed Circuit Television

Closed-circuit television (CCTV) is simply the use of video cameras to transmit a signal to a specific place, on a limited set of monitors. It differs from broadcast television in that the signal is not openly transmitted, though it may employ point to point (P2P), point to multipoint, or mesh wireless links. The first CCTV system was installed by Siemens AG at Test Stand VII in Peenemünde, Germany in 1942, for observing the launch of V-2 rockets written by Dornberger, Walter, in 1954. Though almost all video cameras fit this definition, however, the term is most often applied to those used for surveillance in areas that may need monitoring such as banks, casinos, airports, military installations, and convenience stores.

Nevertheless, during the 1980s video surveillance began to spread across the country specifically targeting public areas. It was seen as a cheaper way to deter crime compared to increasing the size of the police departments. Some businesses as well, especially those that were prone to theft began to use video surveillance.

During the 1990s, digital multiplexing which allowed for several cameras at once to record and introduce time lapse and motion-only recording, increased the use of CCTV across the country and increased the savings of time and money. From the mid-1990s on, police departments across the country installed an increasing number of cameras in various public spaces including housing projects, schools and public parks departments. Following the September 11, 2001 attacks in the United States, the use of video surveillance has become a common occurrence in the country to deter future terrorist attacks (Yesil, 2006). In September 1968, Olean, New York was the first city in the United States to install video cameras along its main business street in an effort to fight crime (Robb, 1979). CCTV later became very common in banks and stores to discourage theft, by recording evidence of criminal activity. Their use further popularized the concept.

In recent decades, especially with general crime fears growing in the 1990s and 2000s, public space use of surveillance cameras has taken off, especially in some countries such as the United Kingdom.

In industrial plants, CCTV equipment may be used to observe parts of a process from a central control room, for example when the environment is not suitable for humans. CCTV systems may operate continuously or only as required to monitor a particular event. A more advanced form of CCTV, utilizing digital video recorders (DVRs), provides recording for possibly many years, with a variety of quality and performance options and extra features (such as motion-detection and email alerts). More recently, decentralized IP-based CCTV cameras, some equipped with megapixel sensors, support recording directly to network-attached storage devices, or internal flash for completely stand-alone operation. Surveillance of the public using CCTV is particularly common in many areas around the world including the United Kingdom, where there are reportedly more cameras per person than in any other country in the world (Lewis, 2009). There and elsewhere, its increasing use has triggered a debate about security versus privacy. This has remained relatively obsolete in the 21st century. This work will present a baseline discussion on video surveillance generation having established the CCTV scenario.

2.2 Baseline Video Surveillance Functions

According to a white paper (Cisco Systems inc., 2007), typical video surveillance systems, especially those found in higher-security environments such as airports, casinos, military sites, correctional facilities, and many corporate headquarters, have the basic system component functions shown in Fig.2.1.

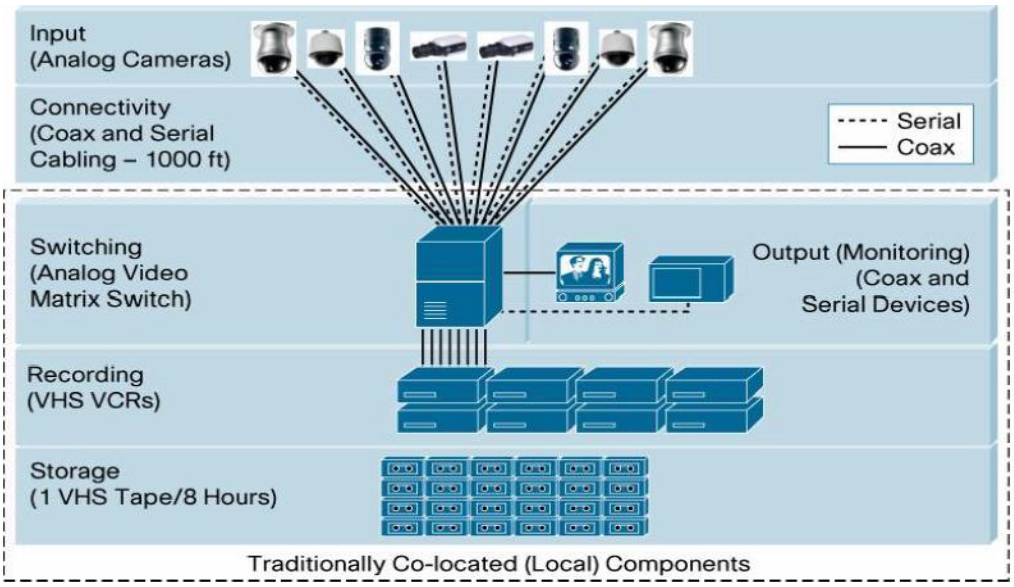


Figure 2.1. Basic Components of a Typical Video Surveillance System
(Courtesy: Cisco Systems, 2007)

Video surveillance system is generally associated with the following features;

i. Input devices: Cameras (fixed and/or pan tilt and zoom [PTZ]) that are available in either black and white or colour are covertly or openly deployed.

ii. Connectivity: Multiple, parallel cable plants are necessary to deploy video surveillance solutions: coaxial cables for NTSC/PAL (National Television System Committee/Phase Alternating Line) video transmission; low-voltage, ring-oriented RS-485 cable plants for serial PTZ command and control; and dedicated fibre-optic cabling for video transmission and PTZ command and control between buildings in a campus setting. Some installations convert the coaxial media to and from unshielded twisted pair (UTP) cabling or use wireless transmission systems, such as microwave.

iii. Switching (video stream management): Real-time central command and control monitoring of video streams is provided. Monitoring station personnel can direct a transmission or aggregation device (commonly referred to as a matrix switch) to switch from one camera feed to another in order to display the scene on a monitor.

Switching is traditionally supported by matrix switches that come in many sizes, scaling from tens of cameras to thousands of cameras.

iv. Monitoring: This involves the viewing of live video. In this case, the operators select the desired video feed and specify where the video is to be displayed. For larger installations, a special-purpose keyboard controls which camera video feed is displayed over an RS-232 connection that sends vendor specific or proprietary commands to the matrix switch. The requested video stream is delivered to the monitor over a coaxial connection that supports the analogue video signal (NTSC/PAL). Unlike a typical PC keyboard, the layout and operation of the video surveillance keyboard is specific to the video surveillance market. This special-purpose keyboard references cameras by simple numbering schemes (01 = camera1, 104 = camera104, etc.). In some installations, PCs can be used instead of special-purpose keyboards and displays but many operators prefer the special purpose monitoring stations and keyboard/joystick controls.

v. Recording: Independent from monitoring functions, recording in Fig.2.1 has been historically accomplished using video cassette recorders (VCRs) or, more recently, Digital Video Recorders (DVRs).

vi. Storage: Based upon regulatory and other organization requirements, recorded video may be archived for a few days, weeks, or months. This facilitates the investigation of events that may have occurred or need to be correlated with other events. Most manufacturers of cameras, fibre-optic transmission equipment, matrix switches, and monitoring keyboards have their own proprietary communications protocols and languages to interconnect these systems. This approach has locked the customer into a single-vendor solution, increasing equipment costs and decreasing the customer's ability to pick best-in-class solutions.

2.3 Video Surveillance System Evolution

With proprietary solutions, the video surveillance market has experienced less significant innovation compared to the open standards-based cloud industry. However, various technologies have been so compelling in their ability to solve significant video surveillance demands, such that this field has begun to evolve, catching up with many other systems and applications. This section presents a comprehensive review of video surveillance evolutions.

2.3.1 First-Generation Video Surveillance (Tier-1)

First-generation video surveillance systems are entirely analogue. Cameras are controlled and transmitted video in an analogue format. These video streams are aggregated, switched, and dispersed to monitoring displays using analogue matrix switching technology. The matrix switch also provides the video stream to VCRs for recording purposes. Figure 2.2 illustrates first- second- and third-generation video surveillance system deployments, which incorporate newer methods of video recording and storage.

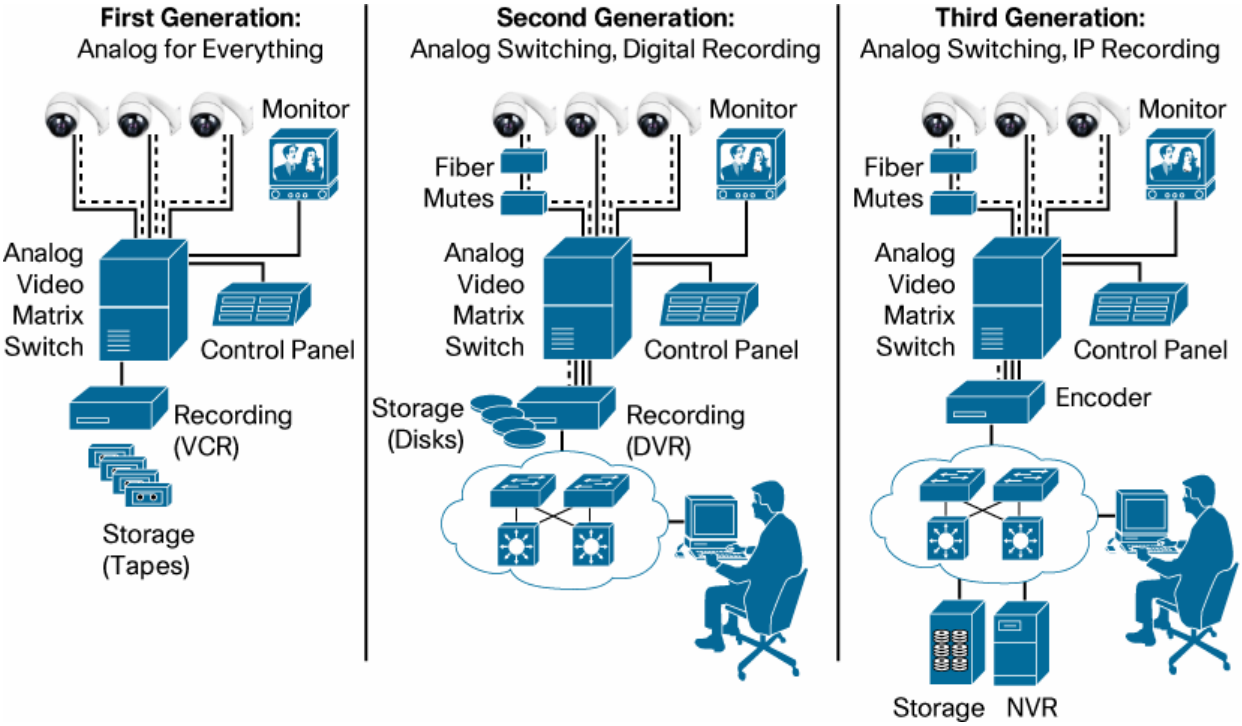


Figure 2.2: Video Surveillance Evolution
(Courtesy: Cisco Systems, 2007)

While the analogue devices provide basic monitoring and recording capabilities, they do have several operational drawbacks. For instance, the VCR-based recording does not facilitate simultaneous recording and playback of video; separate record and playback (review) components are required in order to record video during the investigation process. Moreover, the recording process is prone to human error: replacing blank media or ensuring that recording was activated, for example. From a reliability and system availability perspective, any failure of the recording system can go undetected for an extended period.

Storage and access are also issues. Because videos can be required for future investigation, tapes must be manually stored and indexed in VCR device. These consume a significant amount of space and power, and generate quite a bit of heat.

The viewing of live or recorded video is limited to specific operations and investigation centres. To review recorded video from a remote location requires the appropriate tape to be located and sent to the investigation centre. In virtually all cases, video surveillance system operations are based on proprietary signalling and format protocols; best-in-class multi-vendor component interoperability is not an option for video surveillance customers without extensive and costly customization.

2.3.2. Second-Generation Video Surveillance (Tier-2)

Second-generation systems are also based on camera (input), fibre or coaxial connectivity, with video switching provided by an video matrix switch. However, recording functions are enhanced. The second-generation systems primarily focus on addressing recording and storage problems. DVRs replace VCRs. DVRs convert the video feeds into a digital format and save the resulting digitized video on internal hard disk drives or on locally direct attached storage (for example, digital tapes, disk drives, or DVDs). Thus, many manual efforts associated with VCRs are eliminated or reduced in frequency. Additionally, the DVR's internal database reduces video retrieval time during investigations.

While DVRs offer longer operation life than VCRs, they can pose recording system availability problems. In the event of a DVR failure, the DVR has to be replaced, generally resulting in a loss of video, unless an N+1 redundancy was offered, and failover capability enabled to provide a form of resilience that ensures system availability in the event of component failure.

It must be noted that some DVRs use personal computer operating systems which can be subject to tampering and virus propagation. In this case, the DVRs must be included in a routine maintenance program with regular virus protection and security mechanism configuration. Moreover, since many DVRs fuse the software-based video stream/storage management value into a hardware- (vendor-) specific platform, a generic server/storage device with a considerably lower price may not be available.

Frequently, the DVR software is accessed and controlled by a vendor-specific user interface often running as a set of administrator and operator applications on a

personal computer (PC). As such, second-generation DVRs frequently require a PC viewing client. The use of client software offers some trade-offs; it can limit access to recorded video on a local basis, which may be desirable, but it also can impose problems In emergency situations where remote viewing, over an IP network may be helpful. Some DVRs can be accessed via a network-connected PC to further reduce the time associated with video archiving and retrieval. On-demand access to archived video accelerates evidence review and improves evidence control. It also saves time and effort; investigators do not have to travel to other facilities to perform investigations. To preserve remote-location WAN bandwidth, the video can be pulled over the network on an on-demand basis.

2.3.3 Third-Generation Video Surveillance (Tier-3)

As with first- and second-generation video surveillance deployments, third-generation deployments are primarily based on analogue camera (input), fibre or coaxial connectivity, and video switching is provided by an analogue video matrix switch. However, accessibility of live and recorded video is enhanced.

As observed, second-generation DVRs typically require video to be viewed by PC, which affects video surveillance operator efficiency. Some vendors, offer IP-to-analogue video gateway decoders (IP gateway decoders) as part of a third-generation video surveillance solution that allows operators to view recorded video from their analogue monitoring stations. By using familiar video surveillance PTZ (Pan,Tilt,Zoom) joystick controls, operators can select the video associated with a specific camera, rewind the video, and review it over analogue monitors. This enables faster response and investigation of events, eliminating the need for a PC and the associated delay.

Moreover, in multi-display environments, the operator can continue to monitor other camera video while investigating a recorded event. With interoperability interfaces, operators can use their preferred keyboard and joystick from one vendor while viewing video using another vendor’s cameras. When available, an IP gateway provides any-to-any vendor interoperability, and protects investments in analogue video surveillance cameras and monitoring stations.

Many third-generation systems frequently unbundle the DVR; discrete encoders or high-density, rack-mountable, chassis-based encoders provide the conversion from

analogue to digital and use the network to a greater extent. Thus recording becomes a separate function from video digital encoding.

Encoders serve as analogue-to-IP gateways and as a connection point to the network. The IP network transports the video streams to monitoring and recording locations. Encoders digitize analogue video; typically, they compress the digital video using various compression algorithms, including the same ones used for production-quality motion picture DVDs, and transmit the compressed digital video over a frame-based (Ethernet) or packet-based (IP) network.

Some encoders, such as IP Gateway Encoders, provide additional features that allow them to operate with a wide variety of analogue cameras. This gives video surveillance operators more control over their analogue vendor camera selection process by offering a greater degree of multivendor keyboard/camera interoperability. This aspect becomes even more important when PTZ cameras are used, many of which have proprietary camera control signalling. In this case, encoders can also be differentiated by the latency induced by the digitization and compression algorithm implementation. The lowest-latency, high-video-quality encoders generally have less than 200ms of latency. A lag of more than 200ms can be problematic for video surveillance operators using PTZ cameras—they commonly overshoot the intended item to monitor (zoom in too far or pass the given object). By introducing IP Gateway encoders which serve as hardware and digital signal processing (DSP) based platforms with high-quality, low-latency compression algorithm implementations; latencies are negligible for most operations environments.

Another benefit from unbundling the DVR and using encoders is that the recording (stream and storage management) function, sometimes referred to as a network video recorder (NVR), can be fully independent of storage. The NVR can be located anywhere on the network, often in the data centre with other server systems. Moreover, the NVR software can run on lower-cost common off-the-shelf (COTS) servers.

In the first and second generation deployments, surveillance cameras must be within 1000 feet of the recording device when connecting over coaxial cable, or require fibre connections for longer distances.

Now that encoding occurs in a separate device, the NVR can be located anywhere on the network—at an organization's headquarters, for example, or using servers in two data centres—to simplify management and increase availability. Physically separating the encoding device from the server has another advantage as well: the server no longer needs to devote compute cycles to managing video cards and compression.

In this research, it is observed that by moving to third-generation NVR technology, each server can manage over 32 cameras compared to the 8 to 16 they previously managed, reducing server hardware requirements to approximately 40 percent.

Many organizations have resorted to maintaining a separate database for each remote DVR. However, when using NVRs that can be deployed anywhere on the network, it is possible to centralize the CCTV database into fewer distinct geographic database environments that can be replicated back to the organization's central safety and security operations centre. This partitioning and semi-centralization of databases further simplifies video surveillance system management and reduces equipment costs and helps improve operational efficiency of the system.

An environment could be tasked with the responsibility of maintaining the video surveillance servers and storage, as well as protecting them along with other mission-critical servers. This allows security personnel to focus on security issues, not maintenance of storage devices. As a result, it is possible to reduce not only redundant capital infrastructure investment by using the network for transport and access of the video, but also optimize operational roles and responsibilities.

It should be recognized that this model of separate but complementary functional responsibilities is quite common in most organizations today.

NVR deployments offer several other advantages compared to second-generation deployments using DVRs. Recording and storage component availability is further increased—the failure of a storage device can be almost instantly remedied by having the NVR direct the video stream to another network-connected server or storage device. The use of superior long life(higher MTBF(mean time before failure)) storage devices also helps increase video surveillance system availability.

As mentioned, NVRs offer both video stream management and video stream storage management. Storage management can be an important factor for users with high 24-hour "record-everything" storage requirements. NVRs that can prune stored video

based on motion or other criteria (i.e. first in first out) can further minimize regular maintenance tasks and potentially reduce the amount of storage needed to meet long-term retention requirements.

The ability for the NVR to ingest IP video also enables IP camera video to be recorded in addition to the video coming from analogue video encoders. While IP cameras are discussed in greater detail in other Cisco documents and whitepapers, it should be recognized that IP cameras offer several advantages to analogue cameras and analogue encoders. These benefits include:

i. Compact, single video capture form factor (as compared to an analogue camera plus an encoder).
ii. No separate power source required when Power over Ethernet is provided by the IP network switch, which in many cases has battery back-up in the event of power failure.
iii Ease of deployment using wireless LAN technology.
iv Lower cost deployment using Category 5 structured cabling

2.3.4 Fourth-Generation Video Surveillance (Tier-4)

Collapsing video switching functions onto an existing Ethernet switched environment further reduces the complexity and lowers the cost of deploying video surveillance. It also provides video surveillance system owners with the flexibility to design solutions tailored to their unique requirements. Furthermore, as part of an open network, operators can create policies allowing the inherent value of the video, as a source of information, to be used by other safety and security applications, as well as other non-traditional business applications (Cisco Systems, 2007).

In this research, experience has shown that by converging various applications and technologies on the IP network and in operating a large global video surveillance system over the network, it is feasible to adopt such deployments in cloud computing context (which would be discussed subsequently). Fourth-generation video surveillance provides additional benefits and advantages over preceding generations as shown in Fig. 2.3. The framework expands and extends the capability of video surveillance gateways (enhanced encoders and decoders) and the NVR, which allows the matrix switch to be replaced by standard and typically lower-cost Ethernet switching platforms.

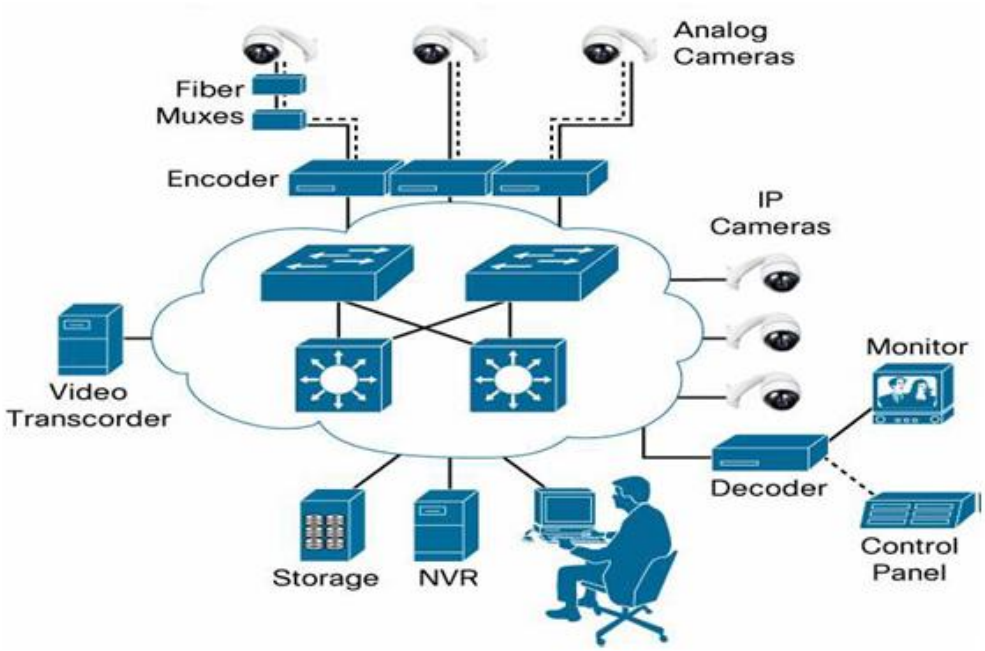


Figure 2.3: Fourth-Generation IP Network-Centric Video Surveillance

(Courtesy: Cisco Systems, 2007)

Considering Fig. 2.3, when used with PCs for monitoring and reviewing video, some NVRs offer matrix switch-like functions, allowing the matrix switch to be eliminated. The switching is provided by the network infrastructure with the video stream management provided by the NVR. Without the matrix switch, encoders can be either centralized in multiport configurations to support home-run cabling schemes or located closer to the camera. By situating the encoder closer to the camera, the encoder can use the pervasive IP network cabling infrastructure, further reducing the cost of redundant cabling infrastructure. For pre-existing long-range camera deployments, fibre multiplexers and distribution amplifiers can continue to coexist with encoders. Of course, for new deployments it may be possible to eliminate the need for fibre multiplexers and distribution amplifiers entirely, thereby further reducing deployment costs (Cisco Systems, 2007).

The On-Demand Real-Time GPS-Based Remote Security Video Sensing System (OD-RGRSVS) supported on video surveillance IP gateway encoders and IP Gateway decoders as well as services Platforms can provide true matrix switch functionality that supports not only analogue cameras and PCs but also the highly specialized video surveillance controllers and monitors. This true matrix switch capability provides full multivendor best of breed mix and match interoperability.

The OD-RGRSVS as a Video Surveillance Manager (VSM) which is designed to run on standard cloud based servers having virtual machine -driven Linux operating system provides a browser-based user interface to collect, manage, record / archive and distribute video from multiple third party video encoders and IP cameras. The Web interface enables cloud operators and other users to easily access live or recorded video using a PC, or various other browser equipped devices. As a result, the video can be viewed in remote and mobile environments on real time basis.

Additionally, the OD-RGRSVS Video Surveillance Manager (VSM) allows for easier integration with other network applications including third party command and control software. Moreover, much like analogue based systems, VSM video can be directed to digital video walls based on various pre-defined events.

Video surveillance system gateways convert or translate proprietary vendor-specific video signals and formats into a common format and then to the same or other vendor-specific formats. This level of interoperability provides the ability to share video information with other systems via the common format. This enables the integration of video surveillance with access control and intrusion detection without the need for a centralized server, which would represent a single point of failure. The ability to integrate, or unify the surveillance system with alarm systems would increase the effectiveness of security operations personnel and cut the expense of responding to false alarms.

For instance, with OD-RGRSVS (video surveillance), a security officer could determine that the source of a door-forced alarm was a gust of wind, not an intruder.

A common format for video and control signals that is transmitted across the IP network also provides the ability to add new functions such as video analytics anywhere in the network. Cloud based video analytics could offer the ability to automatically monitor surveillance video for violations. Therefore, the proposed OD-RGRSVS is a tool for remediation, prevention and early detection. No matter where IP surveillance camera is interfaced at the edge of the network, a common format enables the same video analytics program to be used or varied based on specific circumstances.

However, the efficacy of real-time monitoring of video is greatly diminished if major critical events are missed. One of the more interesting and promising benefits of OD-

RGRSVS is the ability for computer processing and analysis of video, also referred to as video analytics. By using a set of computer algorithms that scrutinize the change in the digital image at the pixel level by comparing one frame or image of video with the previous frame, the cloud based solution can identify movement, recognize objects or people as a grouping of related pixels, and determine the size of an object.

Video analytics can be used in a wide range of applications, not just to alert operators or investigators to an event, but also to highlight common patterns such as traffic flow of people or cars. Video analytics also create new opportunities for the use of video surveillance by non-traditional users, who are not generally focused on safety or security. These users may be in other parts of an organization, such as in marketing in the retail industry or manufacturing and production control. The OD-RGRSVS administrators can use analytics to trigger automated alarms and other responses. For example, by using video analytics, an IP video surveillance system can sense the presence of a bag left in its field of view and page security staff immediately. Casinos can monitor crowding around gaming tables and, when needed, alert the floor staff to quickly open another table. Retail businesses can monitor checkout areas to detect delays as well as understand customer movement for optimized product placement in a far less invasive manner.

Analyzing video can even help freight companies validate the movement of cargo and help to locate lost packages. Thus, video analytics can create new uses for video and transform it into a business tool that contributes to the productivity or sales growth of a business or organization.

In this work, the video analytics capability is embedded into Digital Signal Processors (DSPs) and microprocessors of IP video cameras, Digital Network Video Recorders as well as the dedicated remote storage server clusters of OD-RGRSVS. The flexibility of where video analytics can be deployed and who can use this new tool is enhanced when they are used on an IP network. The network provides the video to be analysed and generates reports that can be distributed anywhere the network goes.

However, the video analytics in general, may not always be accurate in identifying a given event; false alarms do occur. In some applications, the algorithms to identify certain items or events may not deliver acceptable accuracy for instance in facial recognition.

Consequently, by adding networking capability to existing video cameras, this could provide improved benefits, including:

- Improved ability for remote viewing and control. Anyone on the network can potentially see video from any camera connected to the network.
- IP storage makes it possible to store data in any geographic location.
- Greater ease of distribution. An image of a crime suspect, for example, can be immediately distributed to officials.
- The ability to connect to email and other communications systems so that alerts can be sent automatically. There is a growing industry trend towards replacing analogue CCTV with IP surveillance systems.

In most cases, the use of satellite and Global Positioning System (GPS) has facilitated surveillance processes. CCTV with IP surveillance systems (Tier 3/4) can be integrated with the GPS to reinforce its capability.

2.4 Overview of Global Positioning System (GPS)

The Global Positioning System (GPS) is a location determination network that uses satellites to act as reference points for the calculation of position information. The location based GPS is a space-based satellite navigation system that provides location and time information in all weather conditions, anywhere on or near the Earth where there is an unobstructed line of sight to four or more GPS satellites.

The system provides critical capabilities to military, civil and commercial users around the world. It is maintained by the United States government and is freely accessible to anyone with a GPS receiver. These man-made reference points can be viewed as aerial lighthouses that are visible to user equipment and can also transmit additional information that can provide extremely accurate location information to the GPS function within location determination devices. In the U.S. for instance, the police have planted hidden GPS_tracking devices in people's vehicles to monitor their movements, without a warrant. According to Thomas, 2009, court was asked to disallow warrantless GPS tracking.

Though in early 2009, this was seriously challenged in court on its legality. Several cities are running pilot projects to require parolees to wear GPS devices to track their movements when they get out of prison. Hilden (2002, April 16).

Also, mobile phones are also commonly used to collect geolocation data. The geographical location of a mobile phone (and thus the person carrying it) can be determined easily (whether it is being used or not) using a technique known as multilateration to calculate the differences in time for a signal to travel from the cell phone to each of several cell towers near the owner of the phone. BBC News ("Tracking a suspect by mobile phone", 2005).

Despite the fact that mobile phones with GPS features help track criminals, legal issues still hover around it. Joshua (2009, March 14). "Cell Phone Tracking Can Locate Terrorists - But Only Where It's Legal". FOX News. Retrieved 2009, March 14.

Essentially, the GPS project was actually developed in 1973 to overcome the limitations of previous navigation systems, integrating ideas from several predecessors, including a number of classified engineering design studies from the 1960s. GPS was created and realized by the U.S. Department of Defense (DOD) and was originally run with 24 satellites. It became fully operational in 1994. Roger L. Easton is generally credited as its inventor. Advances in technology and new demands on the existing system have now led to efforts to modernize the GPS system and implement the next generation of GPS III satellites and Next Generation Operational Control System (OCX) (GPS Advanced Control Segment, 2011, October 25).

The technology was exclusively meant for the military with less than 24 satellites. This has been however, declassified for public use as prompted by the take down of Korean Airline 007 by Russian Military jets when the commercial airliner drifted into Russian airspace in 1983. Since then, public use of the satellites for commercial purposes was allowed and by July of 1995, 24 satellites were in place, completing the full system, and orbiting earth at altitudes of approximately 11,000 miles. This is high enough to avoid the problems associated with land based systems, while providing accurate positioning 24 hours a day.

As GPS units are becoming smaller and less expensive, there are an expanding number of applications for GPS.

In transportation applications, GPS assists pilots and drivers in pinpointing their locations and avoiding collisions. Farmers can use GPS to guide equipment and control accurate distribution of fertilizers and other chemicals.

Recreationally, GPS is used for providing accurate locations and as a navigation tool for hikers, hunters and boaters. One could rightly quote that GPS has found its greatest utility in the field of geographic information systems (GIS). With some consideration for error, GPS can provide any point on earth with a unique address (its precise location). This GIS is basically a descriptive database of the earth (or a specific part of the earth). While the GPS shows the location point *P, Q, R,* the GIS shows the map of *P, Q, R* as an apple tree.

Hence, the GPS captures us "where" while GIS tells us the "what". These two technologies GPS/GIS have reshaped the way resources are located, organized, analyzed and mapped. This rather serves a significant interest in the proposed OD-RGRSVS by providing means of collecting client's location data.

2.5 Overview of Cloud Computing

Cloud computing is an information technology (IT) paradigm that enables ubiquitous access to shared pools of configurable system resources and higher-level services that can be rapidly provisioned with minimal management effort, often over the Internet (www.wikipedia.org). Cloud Computing refers to both the applications delivered as services over the Internet and the servers and system software in the datacentres that provide those services on demand (Alvarez & Humphrey (2012), Armbrust et al. (2009), Buyya, Yeo, & Venugopal (2009), Buyya & Ranjan (2010). It relies on sharing of resources to achieve coherence and economy of scale. Simply put, cloud computing is the delivery of computing services involving servers, storage, databases, networking, software, analytics and more, over the internet.

2.5.1 Cloud Services

Most cloud computing services fall into three broad categories: infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (Saas). These are sometimes called the cloud computing stack, because they build on top of one another. Knowing what they are and how they are different makes it easier to accomplish one's business goals.

2.5.2 Infrastructure-as-a-Service (IaaS)

This is the most basic category of cloud computing services. With IaaS, you rent IT infrastructure—servers and virtual machines (VMs), storage, networks, operating systems—from a cloud provider on a pay-as-you-go basis.

2.5.3 Platform- as -a-Service (PaaS)

Platform-as-a-service (PaaS) refers to cloud computing services that supply an on-demand environment for developing, testing, delivering and managing software applications. PaaS is designed to make it easier for developers to quickly create web or mobile apps, without worrying about setting up or managing the underlying infrastructure of servers, storage, network and databases needed for development.

2.5.4 Software-as-a-Service (SaaS) is a method for delivering software applications over the Internet, on demand and typically on a subscription basis. With SaaS, cloud providers host and manage the software application and underlying infrastructure and handle any maintenance, like software upgrades and security patching. Users connect to the application over the Internet, usually with a web browser on their phone, tablet or PC.

2.6 Cloud Deployments

Not all clouds are the same. There are three different ways to deploy cloud computing resources: public cloud, private cloud and hybrid cloud.

2.6.1 Public Cloud

Public clouds are owned and operated by a third-party cloud service provider, which deliver their computing resources like servers and storage over the Internet. Microsoft Azure is an example of a public cloud. With a public cloud, all hardware, software and other supporting infrastructure is owned and managed by the cloud provider. You access these services and manage your account using a web browser.

2.6.2 Private Cloud

A private cloud (also called enterprise or internal cloud) refers to cloud computing resources used exclusively by a single business or organisation. A private cloud can be physically located on the company's on-site datacenter. Some companies also pay third-party service providers to host their private cloud. A private cloud is one in which the services and infrastructure are maintained on a private network.

2.6.3 Hybrid Cloud

Hybrid clouds combine public and private clouds, bound together by technology that allows data and applications to be shared between them. By allowing data and

applications to move between private and public clouds, hybrid cloud gives businesses greater flexibility and more deployment options.

2.7 Characteristics of Cloud Computing

The National Institute of Standards and Technology's definition of cloud computing identifies "five essential characteristics":

On-demand self-service. A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

Broad network access. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

Resource pooling. The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.

Rapid elasticity. Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear unlimited and can be appropriated in any quantity at any time.

Measured service. Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

— National Institute of Standards and Technology(Peter Mell and Timothy Grance (September 2011).

2.8 Deployment of Surveillance Cameras

i. A network of cameras on city streets and other public spaces using on- demand cloud integration increases the chances of capturing a criminal on video and can generate an overwhelming amount of evidence on a server cluster.

ii. The cameras make some people feel more secure, knowing that bad guys are being watched. But privacy advocates and other citizens are uneasy with the idea that every public move they make is being monitored. Meanwhile, facial-recognition software and other technologies are making security-camera images more valuable to law enforcement. Now, software can automatically mine surveillance footage for information, such as a specific person's face, and create a giant searchable database. For instance, after the bombings at the Boston Marathon on April 15, 2013, Figure 2.4 shows the security-camera images of suspects in the deadly Boston Marathon bombings released by Federal Bureau on Investigation, (FBI). With this system, the security agents had to resort to a mountain of footage from government surveillance cameras, private security cameras and imagery shot by bystanders on smart phones. FBI quickly released the blurry shots of the two suspects, taken by a department store's cameras in three days.

Figure 2.4: Surveillance camera images of suspects
(Source: FBI Deadly Boston Marathon bombings of April 15, 2013)

iii. Quick Tracking leverage- Compare their quick turnaround with the 2005 London bombings, when it took thousands of investigators weeks to parse the city's CCTV footage after the attacks. The cameras, software and algorithms had come a long way within eight years (i.e. 2005 - 2013).

2.8.1 Internet Protocol (IP) Camera

An Internet protocol (IP) camera, is a type of digital video camera commonly employed for surveillance, and which unlike analogue closed circuit television (CCTV) cameras can send and receive data via a computer network and the Internet. Although most cameras that do this are webcams, the term "IP camera" or "netcam" is usually applied only to those used for surveillance. In terms of operating mode, IP cameras can be grouped into two kinds;

- Centralized IP cameras, which require a central Network Video Recorder (NVR) to handle the recording, video and alarm management.
- Decentralized IP cameras, which do not require a central Network Video Recorder (NVR), as the cameras have recording functionality built-in and can thus record directly to digital storage media, such as flash drives, hard disk drives or network attached storage.

2.8.2 Analogue Versus IP Surveillance Systems

The cabling involved in analogue systems can be tapped and erroneous video material can be fed into the wire or recorded at will without any intrusion alarm being raised. Compared to analogue systems, IP systems are much more difficult to compromise, as encryption requires two nodes that agree on exactly what is being sent and received, and interruptions to this data stream will automatically trigger alarms and alerts. Any type of additional data (sound, graphics, applications, event triggers etc.) can also be sent through the encrypted network. Thus, one-way or two-way audio requires only microphones and speakers at the end points when used with appropriate digital cameras that support audio capabilities. This means that it is very easy to deploy audio alongside video data. Analogue systems on the other hand, cannot handle single channel audio or two-way sound channels without added cabling and expenses.

Yet another benefit is the storage systems used within IP surveillance networks. They are much easier to configure and more reliable. The surveillance camera backup and storage systems are server based RAID (Redundant Array Independent Disks) systems that are connected to uninterruptible power supplies (UPS) just like any other network, and capable of capturing and storing terabytes of data and images simultaneously.

Any network administrator can manage these servers without having any additional training. Another benefit of this server based technology used in IP based surveillance networks is that the cameras are able to record during playback. Analogue systems however require proprietary recording and backup systems that add significant component, maintenance, and training costs as the system grows. In addition, analogue tape based recording systems require ongoing replacement tapes.

Also, IP surveillance data such as captured by the system discussed in this work can be securely viewed at anytime and anywhere from a standard web browser like Internet Explorer. This simply cannot be done with analogue systems that are relegated to the local redundant cabling infrastructure that has been established.

Another aspect of the above mentioned flexibility is that additional cameras can easily be added at one time , whereas analogue systems mostly require increments of 8, 16 or 24 additional cameras. The fact that several cameras can be supported on the same IP infrastructure makes adding additional cameras cost effective. There are various models to accomplish such task applying broadband solutions (Fig. 2.5).

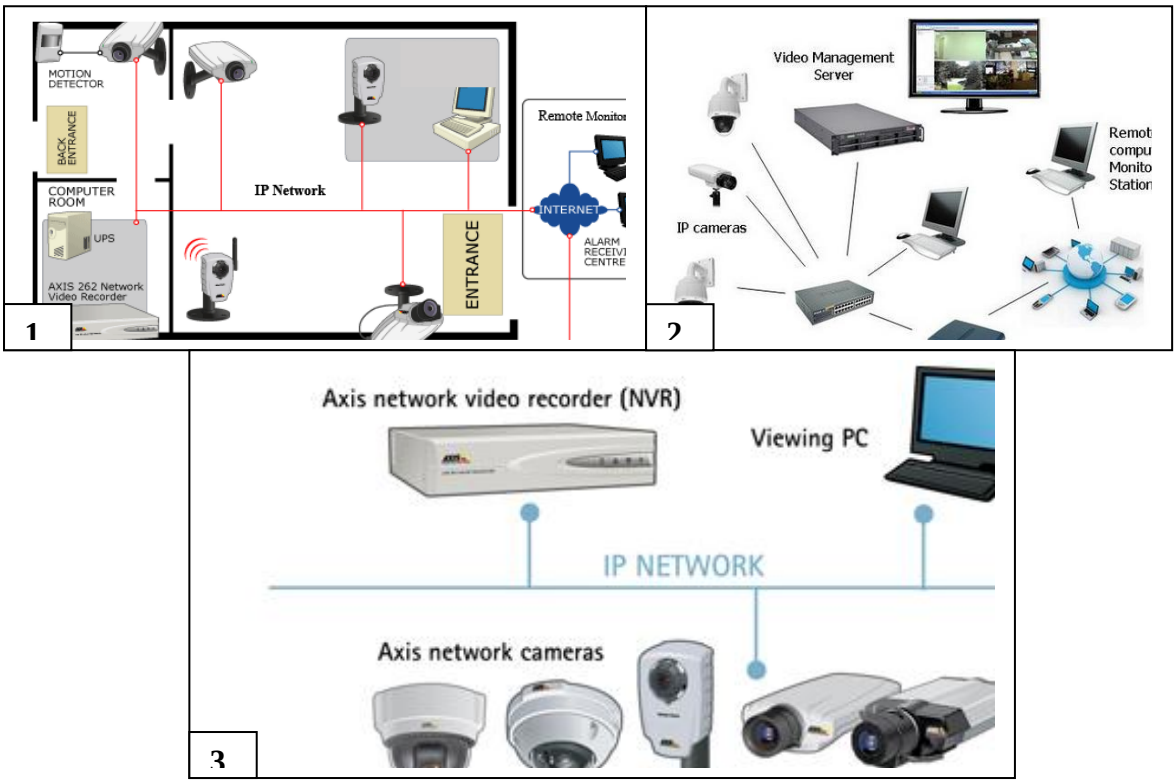


Figure 2.5: IP video surveillance camera connection

(Source: www.axis.com & www.kintronics.com)

Typical switches and routers available today simply segregate traffic for larger scale video applications. With proper network design, installations with 250,000 to 500,000 CCTV cameras are common to accomplish such tasks, and some organizations use more than 1,000,000 cameras at a time. Such could be applied in simultaneous surveillance of stock Exchange Trading Halls.

2.8.3 Benefits of the Real-Time IP Video Surveillance

- **Flexibility**: Surveillance systems that use IP cameras can be reconfigured to meet one's ever-changing needs. This feature is beneficial especially when a new client location needs to be monitored.
- **Theft Prevention**: Prominently mounted security cameras help deter theft.
- **Remote Monitoring**: Adding an NVR to one's surveillance system allows for the broadcasting of one's footage over the internet with ease. One can have a real-time view of any desired location at any time and from anywhere.
- **Ease of use:** It is quite easy and snappy to setup and manage a system of IP cameras . It takes just to mount the cameras and start recording, unlike CCTV cameras that require power tools and technicians.

2.9 Limitations of Existing System

There are drawbacks to remote videography. A system of camera, lens, recorder, and power source can cost thousands of dollars, which when multiplied over a large sample of areas could be prohibitive to some research budgets. Surveillance systems usually include a bulky recorder and power source, and often there can be mechanical or electrical problems (Mc Quillen & Brewer, 2000). For successful operation, it is critical to provide and sustain electrical power to each system even in remote locations.

Privacy Concerns**:** This is mostly an issue for business owners. Employees can be offended by the presence of cameras in the breakroom and the backroom. A hidden video surveillance camera can cause problems in court if illegal behavior is recorded by the system.

Limited Storage Capacity: Today, huge amounts of video footage have to be stored locally many a time which often leads to automatic overwrite coupled with capture of irrelevant footage of which only a small amount of data may be useful in the

conventional video surveillance systems. Various kinds of sensors often leads to false alarm events being generated instead of only when there is an actual breach.

2.10 Application Areas

- **Asset Protection:** Large organizations, including utilities such as gas, water, and electric pipelines, railways, airports and mines have essential equipment and assets that need monitoring from time to time. These industries face threats from thieves, vandals, intruders, terrorists, and even natural disasters. Remote real-time video monitoring is an ideal tool in these cases.
- **Access Control:** Many sites and buildings need secure perimeters filter the entrants, giving access to authorized ones and keeping out intruders.
- **Home:** Most home owners today want to do everything possible to protect their homes from theft.
- **Polling Boots:** Incidents of tampering with election/voting materials during elections in Nigeria is a common event. Human agents are usually sent to monitor polling centres. The real-time security system discussed here is an effective substitute since polling locations can be viewed in real-time if monitored and transmitted by this equipment.
- **Education:** Educational campuses often deal with vandals, intruders and thefts.
- **Day/Night Care Institutions:** Day/Night Care sites, including kindergartens and retirement homes require surveillance security systems to monitor the activities in their institutions.
- **Cellular Transmission Towers:** Cellular and transmission towers are often unmanned, and located in remote areas hence need regular monitoring.
- **Construction:** Construction sites attract thieves and vandals, therefore monitoring is necessitated.
- **Street Surveillance:** Some neighborhoods are notorious and well known robbery locations.
- **Parking Lots:** These are well known locations for theft and vandalism, and many a time, car owners are made to park at their own risks.
- **Military:** Intruders need to be kept away from military facilities and there is the need to guard against attacks.

2.11 Advantages of IP Cloud-Based Surveillance System

- IP location based surveillance via a single network cable allows users to communicate with what they see.
- Higher image resolution: IP cameras have a resolution of at least 640x480 and can provide multi-megapixel resolution and High Density TeleVision (HDTV) image quality at 30 frames per second.
- Flexibility: IP cameras can be moved around anywhere on an IP network (including wireless).
- Distributed intelligence: with IP cameras, video analytics can be placed in the camera itself allowing scalability in analytics solutions.
- Transmission of commands for PTZ (pan, tilt, zoom) cameras via a single network cable.
- Encryption & authentication: IP cameras offer secure data transmission through encryption and authentication methods such as WEP(Wired Equivalent Privacy), WPA(Wifi Protected access), WPA2(Wifi Protected access2), TKIP(Temporal key Integrity Protocol, and AES (Advanced Encryption System).
- Remote accessibility: live video from selected cameras can be viewed from any computer, anywhere, and also from many mobile smart phones and other devices.
- IP cameras are able to function on a wireless network. Initial configuration has to be done through a router; after the IP camera is installed it can then be used on the wireless network. These cameras are used in navigation purpose in defence forces
- PoE - Power over Ethernet. These IP cameras have the ability to operate without an additional power supply. They can work with the PoE-protocol which gives power via the ethernet cable

2.12 Disadvantages of the New System

- High initial cost per camera, and the cloud infrastructure
- High network dependence and bandwidth requirements: A typical surveillance camera with resolution of 640x480 pixels and 10 frames per second (10 frame/s) in MJPEG mode requires about 3Mbit/s. Also, availability of GSM network and internet service is imperative.

- Technical barrier: Most security systems including both CCTV and IP camera systems may require a professional technician to install the system, although a competent person can install an IP camera very easily, depending on make.
- As with a NDVR system, if the video is transmitted over the public Internet rather than a private IP LAN, the system becomes open to a wider audience of hackers and hoaxers. Criminals can hack into a CCTV system to observe security measures and personnel, thereby facilitating criminal acts and rendering the surveillance counterproductive.

2.13 Cloud-Based Remote Storage Paradigm Shift

Leveraging on an on-demand cloud storage backend is important because video captures especially high-definition videos are bandwidth intensive, so the applicability of cloud technology for data storage and real time provisioning is very essential.

The virtual machines (VMs) on the cloud facilitate the sharing of resources on the cloud storage offering a high performance quality of service (QoS) index for the surveillance service.

Through cloud-based remote backup, this presents an opportunity to leverage on the scale of the cloud to build a resilient disaster recovery solution without having to invest in hardware, complex software licensing or new skilled personnel. Cloud-based backup offers an intrinsic benefit over onsite alternatives in that the physical storage is generally far removed from users and their source data.

2.14 Benefits of Cloud Based Remote Backup

Cloud-based remote backup offers benefits in four main areas: cost, risk, flexibility and quality. These are discussed below.

i. By backing up data in the cloud, the proposed OD-RGRSVS can reduce and simplify their cost structures while offloading some of their risks to a service provider.

ii. By leveraging the elasticity of cloud computing, the OD-RGRSVS becomes more agile in responding to changing circumstances. This can run on a dedicated

Service Level Agreement (SLA), outsourcing cloud provider. In this case, relying on the provider's core competency could help to achieve better backup services.

iii. Cost: The most obvious benefits of cloud computing have to do with cost. Cloud-based remote backup can mean a significant reduction in upfront capital expenditures because there is no need to purchase extensive hardware infrastructure or software licenses. Instead, the organization can align its costs with actual usage.

iv. Risk: Remote backup can offload risk from the customer to the service provider. By contractually stipulating provisions for data protection and disaster recovery that are tied to specific indemnities in the event of service failures, risks could be further mitigated.

v. Remote backup also reduces the likelihood of under-provisioning data storage. Cloud computing offer elastic resource allocation and unlimited data retention, making it less likely that storage capacity will ever be exhausted.

vi. Since cloud providers typically undergo very strict security audits by employing best-available security procedures and solutions, they keep those solutions up to date based on Service level Agreements (SLAs). To meet up with such agreements, a lot of research is ongoing. For example, Onoja, A.A, Babasola, O.L., Moyo, Edwin and Ojiambo, Viona (2018), published on the Application of Queuing Analysis in modeling Optimal Service level.

increase overall data security, segregation of data, using an extended private in-housing internal network is optimal. For this purpose, a lot of research is ongoing

vii. Flexibility: A cloud infrastructure adds considerable flexibility and agility to an enterprise architecture. The scalable, elastic storage capacity afforded by a cloud service means that rapid data growth is easily accommodated. Flexibility also comes in the form of speed of execution vis-à-vis QoS.

Similarly, data restoration can take place on demand, supporting excellent recovery time objectives (RTOs). A globally replicated cloud infrastructure can facilitate data access from anyplace using any device at any time, which contributes to greater user flexibility and productivity.

viii. Quality: Quality of service (QoS) is clearly a major concern. Cloud computing via its service providers offers great economies of scale and

specialization. There are developed rigorous processes and procedures to maximize uptime and optimize performance. They run best-available software to monitor and manage the infrastructure, using excellent expertise.

A cloud model for OD-RGRSVS is perceived as a revolutionary intervention. As a result, users would often receive more frequent and timelier updates on its rollout.

In this research, high-performance, robust connectivity is vital for remote backup of surveillance image because it relies on the network to transport and store data. The connection is generally dedicated to backup, so it is possible to plan in isolation. The network infrastructure for the entire OD-RGRSVS architecture must be evaluated while taking backup requirements into consideration.

When it comes to remote backup, poor network planning can manifest in two ways. First, insufficient network capacity may mean that a backup cannot run in a reliable and timely manner, leaving some data unprotected at least for a period of time.

Secondly, the backup may encroach on the network needs of other potentially mission-critical applications and cause their failure. The only way to understand the full network requirements of the organization is to take inventory of the application type for storage, the users, and then map out the application storage paradigm.

2.15 Storage Virtualization

In this research, step storage virtualization is the precursor to remote backup because it offers many benefits and helps achieve location independence for the data that may eventually move to the cloud. The technology presents a logical space for data storage and handles the process of mapping it to the actual physical location. Virtualization via Virtual Machines (VMs) redirects incoming requests based on a logical disk location and translates them into new requests referencing a physical disk location. This abstraction makes storage consolidation much easier because it is possible to migrate data without disrupting access. The host only knows about the logical disk, so the physical data can be moved or replicated to another location without affecting the operation of any client.

Also, resource pooling can increase utilization. The physical storage is logically aggregated into pools. As a result, additional storage systems can be added as needed and the virtual storage space will scale up transparently. This allows for optimal storage solutions.

Finally, storage virtualization can act as a centralized console for managing all volumes in the environment. Multiple dispersed and independent storage devices appear as a single monolithic storage device. In summary, storage virtualization offers several benefits that stand on their own merits. But optimized efficiency, centralized management and storage abstraction are also key factors in facilitating a smooth migration to the cloud.

2.16 Multiserver Queue (M|M|c) Model

Queues are fundamental in the analysis of packet traffic in communication networks in respect of real-time requirements, delays, resource management. Multisever queue systems are characterized as Markovian queue model denoted by M|M|c. The model describes a system where arrivals to the service facility form a single queue and are governed by a Poisson process, with 'c' number of servers, and exponentially distributed job service times. It represents a stochastic process whose state space is set to {0,1,2,3,….}, where the values correspond to the number of jobs (also referred to as customers, users, clients, or calling population) in the system including any currently in service.

It is important at this juncture to introduce the concept of Kendall's notation which helps define the multiserver queue model being discussed.

In Kendall's notation, a queuing system is defined by **a/b/c/n** where

a = type of arrival process = M (Poisson process)

b= service time distribution = { M exponential; D deterministic; G general

c = number of servers

n = maximum number of customers allowed in the system.

2.16.1 Characteristics of M/M/c Queue Model

M/M/c queue is a multiserver queue model generally characterized as follows;

- Arrivals occur at rate, λ according to a Poisson process.
- Service times are exponentially distributed with mean service rate μ. If there are less than *c* jobs, some of the servers will be idle. If there are more than *c* jobs, the jobs queue in a buffer.
- The buffer is of infinite size, so it can contain infinite number of customers.
- Jobs are processed under First In First Out (FIFO) i.e. First Come First Served (FCFS) queue discipline.
- The average proportion of time which each of the servers is occupied, ρ *is* the utilization factor for the service system given by; $\rho = \frac{\lambda}{c\mu}$. It is required that this value is less than 1 for the system to be stable.

Fig. 2.6 represents M/M/c queuing model with arrival rate λ and service rate μ.

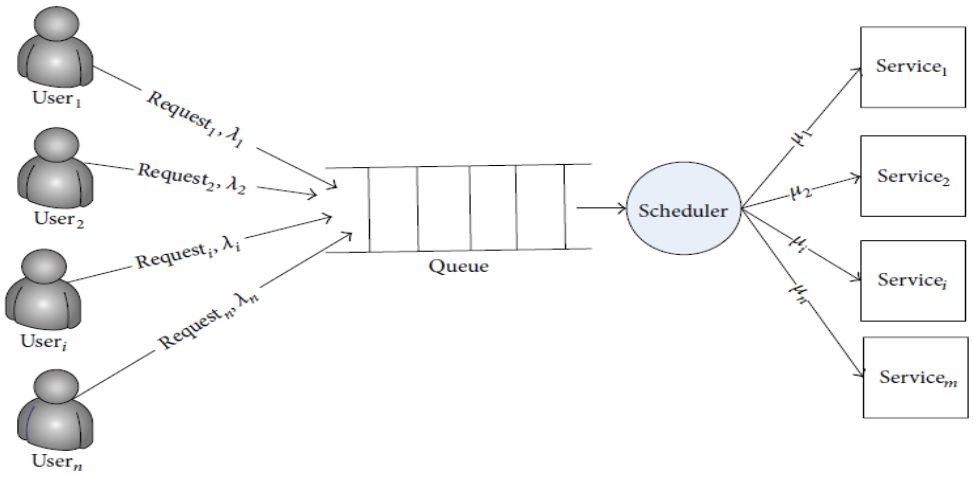


Figure 2.6: Queuing performance model in cloud computing

(Courtesy: Vetha S. & Vimala Devi K., 2017)

A state transition diagram of a Poisson process to a multiservice facility can be represented as a Markov Chain.

2.17 Markov Chain

A Poisson process can be modeled as a continuous time Markov chain (CTMC) with transition state diagram as shown in Fig. 2.7. A Markov process is known for exhibiting the property of being memoryless as it consists of states and probabilities where the probability of moving from one state to another depends only on the current state and not on the previous state.

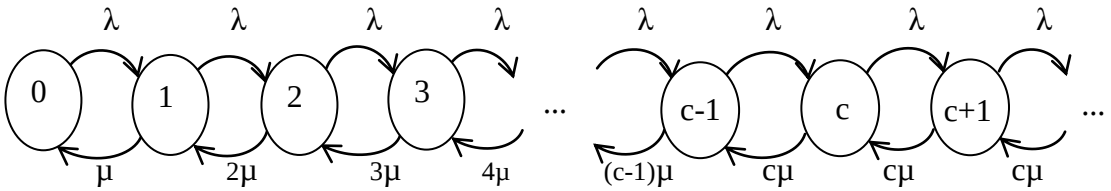


Figure 2.7: Continuous time Markov chain

(Source: www.wikiwand.com)

It is important at this juncture to refer to M/M/1 model which is a single server queue model with utilization factor $\rho = \frac{\lambda}{\mu}$.

In M|M|c queues however, the arrival rate remains same as M|M|1 queues but the service rate depends on the number of servers, c. If there are n jobs in the system, the service rate, μ_c will be ;

$$\mu_c = \begin{cases} (n\mu) & n \leq c \text{ for } n=1,2,3,....c \\ (c\mu) & n > c \text{ for } n=c, c+1,.... \end{cases}$$

This implies that as soon as the number of jobs exceeds c, i.e. n>c, the service rate becomes cμ as shown in the state transition diagram (Fig. 2.7).

2.18 Littles Law

Little's Law is a theorem that determines the average number of items in a stationary queuing system based on the average waiting time of an item within a system and the average number of items arriving at the system per unit of time. It is stated as follows;

$$N_s = \lambda * W_s \qquad (2.1)$$

Where N_s = average no. of customers in the service facility

λ = average arrival rate

W_s = average waiting time (i.e. time spent in the system)

Equation (2.1) is applicable to all queuing systems under steady state condition.

2.19 Review of Related Literature

In this section, various research efforts will be highlighted comprehensively with the intent of establishing obvious research gaps.

Romanca, Szekely, Cocorada, and Grama (2007) developed a video surveillance system for controlling the access in a building with results obtained at the installation. The system uses an IP video camera (NC 1200) connected at a building LAN. The IP camera used allows the visualisation of images by Internet connection but, for recording images, admits only manual command from the human operator that supervises the entrance. The camera has embedded the function of sending an instant picture by e-mail or on a FTP (File Transfer Protocol) server if the system disposes any of these two facilities. An, application which was created automatically causes the system to start recording images when a motion is detected in the supervised space. The application has the advantage of saving the image frames directly on the monitoring computer and eliminates the constraint to have an online server (FTP or e-mail) and also that permits no modification of the camera firmware, being installed only on the monitoring computer.

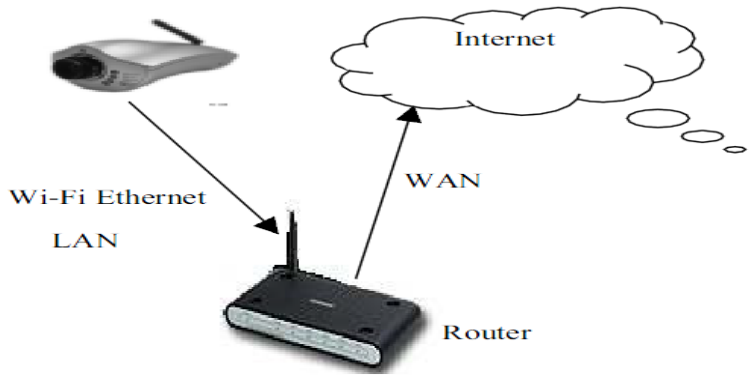


Figure 2.8: LAN Based NC1200 camera connection

(Source: ACTA TECHNICA NAPOCENSIS Electronics and Telecommunications, 2007)

The authors concluded that their system has advantage of using a cheap IP camera combined with the original application for entrance surveillance as shown in Fig.2.8.

Rodríguez-Silva, Gonz'lez-Castano, Adkinson-Orellana, and Gonz'lez-Martinez (2012) proposed a cloud-based video surveillance system with emphasis on storage. They analyzed the storage requirements of a traditional surveillance system and justified their choice of a cloud-based storage model as an alternative to that of traditional approach. OD-RGRSVS also addresses the optimization aspect of video transmission and cloud storage and proposes an efficient cloud storage.

Terrissa, Radhia, and Bréthé (2016**)** proposed a cloud ROS-based architecture according to cloud computing principles, where the robot can be considered as a service in the cloud. The authors defined and implemented three kinds of services: Robotic Software as a Service (RSaaS), Robotic Platform as a Service (RPaaS) and Robotic Infrastructure as a Service (RIaaS). According to them, an obvious next step is to share cloud resource with artificially intelligent software and hardware. Therefore, the robots should be able to benefit massively of this resource which is nearly infinite in the cloud.

Valentín et al.(2017) presented a paper on cloud-based architecture for smart video surveillance capable of acquiring a video stream from a set of cameras connected to the network, process that information, detect, label and highlight security-relevant events automatically, store the information and provide situational awareness in order to minimize response time to take the appropriate action. According to the authors, they implemented a prototype which consists of a set of cameras connected to the network, a couple of desktop computers for pre-processing and a processing system implemented on FIWARE.

Singh & Patil (2010) discussed an efficient proposal to upgrade an existing Camera based Surveillance Architecture for security and Administration in Fig. 2.9. Their renewed approach was essentially based upon RFID (Radio Frequency Identification) technology by utilizing RFID tags and their readers as basic components. Unlike camera-based surveillance systems, the RFID based approach can monitor and administer a quarter not only within some region of visibility but can efficiently do the same for locating the individuality. This approach emphasizes not only on overcoming the demerits of observation-based supervision, but it presents easier and

effective monitoring methodologies using radio waves and their usable features in security and administration for areas with consumer pour out.

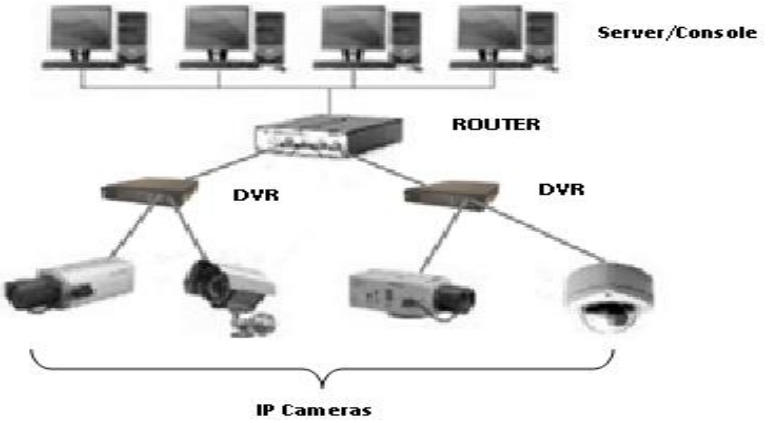


Figure 2.9: IP Camera Surveillance System
(Source: Kintronics Information technology)

As shown in Fig. 2.10, their dynamic RFID system consists of a reader and one or more tags. The reader's antenna is used to transmit radio frequency (RF) energy. Depending on the tag type, the energy is harvested by the tag's antenna and used to power up the internal circuitry of the tag. The tag then modulate the electromagnetic waves generated by the reader in order to transmit its data back to the reader. Their reader receives the modulated waves and converts them into digital data. In the case of the parallax RFID Reader Module, correctly received digital data is sent serially through the S_{OUT} pin (Harriton & Lowford, 2006).

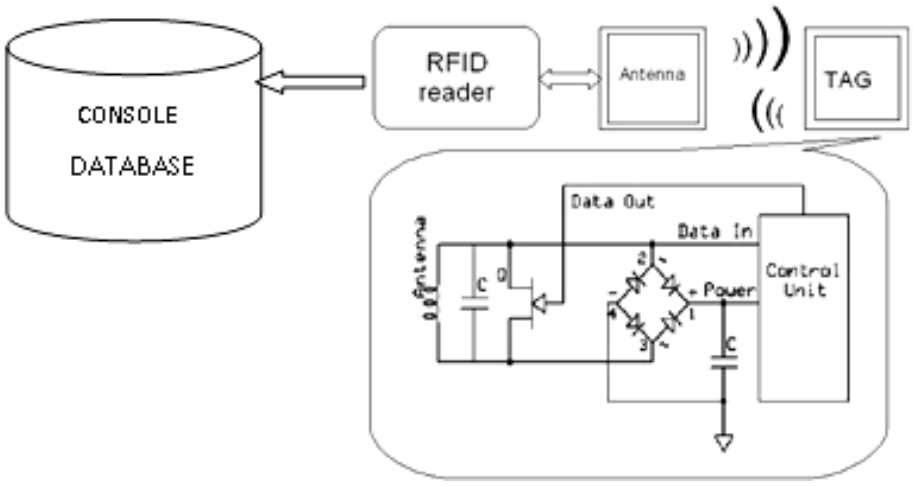


Figure 2.10: Dynamic Surveillance RFID mechanism
(Harriton & Lowford, 2010)

Fan & Yibo (February 2009) presented a new video encryption scheme for H.264/AVC (also known as MPEG-4 part 10 or AVC (for latest Advanced Video Coding), and also the hardware design of encryption module. Similarly, a new novel scheme for digital video encryption was proposed by Chandra et al. (2012). The authors gave a method to generate an encrypted video by encrypted video-frame. It is a matrix computation scheme which uses a concept of Video-frame and XOR operation.

Usman et al. (2017) tried to address limitations of the existing schemes for secure exchange of media files between the mobile devices and the clouds in terms of memory support, processing load, battery power, and data size. They proposed a secure, lightweight, robust, and efficient scheme for data exchange between the mobile users and the media clouds. The proposed scheme considers High Efficiency Video Coding (HEVC) Intra-encoded video streams in unsliced mode as a source for data hiding. The proposed scheme aims to support real-time processing with power-saving constraint in mind, using Advanced Encryption Standard (AES) as a base encryption technique. The results of the proposed scheme outperforms AES-256 by decreasing the processing time up to 4.76% and increasing the data size up to 0.72% approximately. The proposed scheme can readily be applied to real-time cloud media streaming.

Tian et al. (2008) developed a large scale data analysis and management Smart surveillance systems that uses automatic image understanding techniques to extract information from the surveillance data. Their current version includes two components: (1) Smart Surveillance Engine (SSE) which provides the front end video analysis capabilities; (2) Middleware for Large Scale Surveillance (MILS) which provides data management and retrieval capabilities. These two components in conjunction with the IBM DB2 and IBM WebSphere Application Server support the following features: Local Real-Time Surveillance Event Notification (LRTSEN), Web Based Real-Time Surveillance Event Notification (WBRTSEN), and Web Based Surveillance Event Statistics (WBSES). Their Smart Surveillance Engine (SSE) is a C++ based framework for performing real-time event analysis. This engine is capable of supporting a variety of video/image analysis technologies and other types of sensor analysis technologies.

Diao et al. (2017) carried out a Study on Data Security Policy Based on Cloud Storage. The purpose of the paper is to achieve data security of cloud storage and to formulate corresponding cloud storage security policy. They combined the study with the results of existing academic research by analyzing the security risks of user data in cloud storage and approach a subject of the relevant security technology, which based on the structural characteristics of cloud storage system.

Broaddus et al. (2009) described a novel scalable approach for the management of a large number of Pan-Tilt-Zoom (PTZ) cameras deployed outdoors for persistent tracking of humans and vehicles, without resorting to the large fields of view of associated static cameras. The system, Active Collaborative Tracking – Vision (ACT-Vision), is essentially a real-time operating system that can control hundreds of PTZ cameras to ensure uninterrupted tracking of target objects while maintaining image quality and coverage of all targets using a minimal number of sensors. The system ensures the visibility of targets between PTZ cameras by using criteria such as distance from sensor and occlusion. Also, it consists of two primary components, namely the Tracker Node and ACT-Vision Manager (AVM). Fig. 2.11 shows the high-level block diagram of the data flow. The goal of the ACT-Vision System is to automatically control individual PTZ cameras to follow a particular target, or a set of targets, and also optimize the arbitration of *N* PTZ cameras to maintain visibility. This allows an operator using the visualization GUI to select a single target, or a collection of targets, with a mouse which relays this information to ACT-Vision Manager.

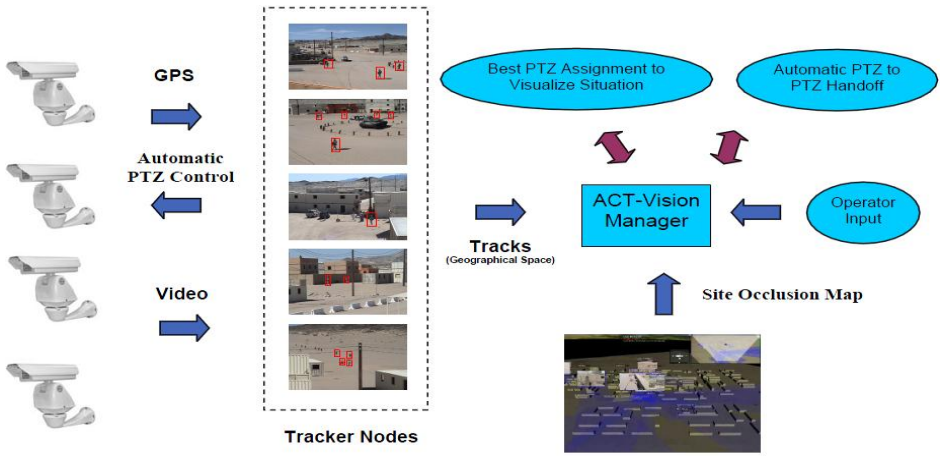


Figure 2.11: Block diagram of the ACT-Vision System
(Courtesy: Broaddus et al. (2009)

Rajkumar (2011) proposed a mobile video surveillance paradigm that encompasses both video acquisition and image viewing, addressing both computer-based and mobile-based surveillance. It is based on JPEG 2000 still image compression format and supports still image creation on the basis of motion detection technique which enables efficient utilization of resources.

Hossain (2014) proposed a framework for a Cloud-Based Multimedia Surveillance System. The author also designed and analyzed a prototype surveillance system in the context of the proposed surveillance framework. The paper finally reports that cloud-based multimedia surveillance system can effectively support the processing overload, storage requirements, ubiquitous access, security, and privacy in large-scale surveillance settings. The paper finally reported that cloud-based multimedia surveillance system can effectively support the processing overload, storage requirements, ubiquitous access, security, and privacy in large-scale surveillance settings.

Wang (2013) made a review on intelligent multi-camera video surveillance. The paper reviews the recent development of relevant technologies from the perspectives of computer vision and pattern recognition. The covered topics include multi-camera calibration, computing the topology of camera networks, multi-camera tracking, object re-identification, multi-camera activity analysis and cooperative video surveillance both with active and static cameras. Detailed descriptions of their technical challenges and comparison of different solutions are provided. It emphasizes the connection and integration of different modules in various environments and application scenarios.

Mitrea et al. (2014) proposed a classification-based automated surveillance system for multiple-instance object retrieval task with the main purpose, to keep track of a list of persons in several video sources, using only few training frames (Fig. 2.12).

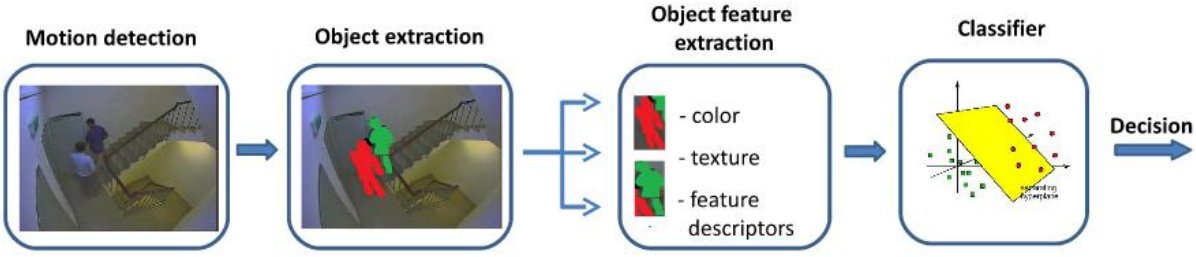


Figure 2.12: The proposed classification-based automated surveillance system (Courtesy: Mitrea et al. (2014)

The authors discussed the perspective of designing appropriate motion detectors, feature extraction and classification techniques that would enable attainment of high categorization accuracy, and low percentage of false negatives.

Rajpoot and Jensen (2016) presented a thesis on Enhancing Security and Privacy in Video Surveillance through Role-Oriented Access Control Mechanism. They presented a taxonomy of video surveillance and broadly categorized the areas under surveillance into Publicly Accessible and Private (Fig.2.13).

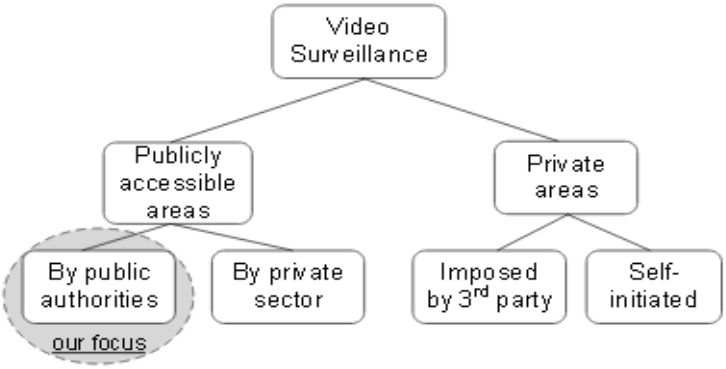


Figure 2.13: Taxonomy of video surveillance system

(Courtesy: Rajpoot & Jensen, 2016)

Rajpoot (2016) later developed a hybrid access control model which combines role–based access control (RBAC) and attribute-based access control (ABAC) models aimed at enhancing security and privacy in large scale video surveillance. He used an approach that provides a mechanism that not only takes information about the current circumstances into account during access control decision making but is also suitable for applications where access to resources is controlled by exploiting the contents of resources in the access control policy.

Kalra and Singh (2015) made a review of metaheuristic scheduling techniques in cloud computing. The authors pointed out that One of the important research issues which need to be focused for its efficient performance is scheduling which focuses to map tasks to appropriate resources that optimize one or more objectives. In the paper, they provided an extensive survey and comparative analysis of various scheduling algorithms for cloud and grid environments based on three popular metaheuristic techniques: Ant Colony Optimization (ACO), Genetic Algorithm (GA) and Particle Swarm Optimization (PSO), and two novel techniques which include League Championship Algorithm (LCA) and BAT algorithm. According to the authors,

different scheduling algorithms have focused on diverse optimization criteria, and most of the authors have focused on reduction of makespan and execution cost whereas others have given significance to response time, throughput, flow time and average resource utilization. They also noted that recent research efforts are done in the direction of energy-aware scheduling as data centers have become energy-hungry and a major source of CO_2 emissions, adding that the challenge is to reduce energy consumption of data centers without degrading performance and violating SLA constraints.

Guoqing and Zhenchun (2017) catalogued data infrastructures for remote sensing big data into six (6) classes based on the features such as basic service unit, distributivity, heterogenity, space-time continuation and on-demand processing, and designed architectures for all the 6 classes of data infrastructures. According to them, data infrastructures for remote sensing big data will provide PaaS (platform-as-a-service) and SaaS (software-as-a-service) services for developing much more remote sensing data analysis applications with the architecture designs and implementation technologies.

Moganarangan, Babukarthik, Bhuvaneswari, Saleem Basha & Dhavachelvan (2016) pointed out the important role of cloud computing in scientific application, where on-demand facility of virtualized resources is provided as a service with the help of virtualization without any additional waiting time. According to them, energy consumption is reduced for job scheduling problems based on makespan constraint which in turn leads to significant decrease in the energy cost, but there is an increase in complexity for scheduling problems mainly because the application is not based on makespan constraint. The authors then proposed a new hybrid algorithm combining the benefits of ACO (Ant Colony Optimization) and cuckoo search algorithm. The algorithm focused on the voltage scaling factor for reduction of energy consumption. Their result showed that the performance of the hybrid algorithm considerably increased from 45 tasks onward when compared to ACO algorithm.

Chi, Zhang, Du and Liu (2013) put forward a distributed storage module based on image blocks organization to settle the problems existing in the application of cloud storage for remote sensing data. The authors claimed as follows; i. the inefficient problem of distributed file system in massive image blocks storage was solved. ii. In the combination of the module and HDFS, the efficient distributed storage and

retrieval of image data were implemented, and the ability of spatial data access of the remote sensing data cloud storage was enabled. iii. As built upon distributed file system, the storage system has a good scalability to meet the requirements of data growing.

iv. The experiment and analysis showed that the storage system could maintain a high throughput and stability under multiple concurrent connections.

Puthal, Nepal, Ranjan and Chen (2017) proposed a Dynamic Prime Number Based Security Verification (DPBSV) scheme for big data streams. The scheme is based on a common shared key that updated dynamically by generating synchronized prime numbers. The common shared key updates at both ends, i.e., source sensing devices and Data Stream Manager (DSM), without further communication after handshaking. Theoretical analyses and experimental results of their DPBSV scheme show that it can significantly improve the efficiency of verification process by reducing the time and utilizing a smaller buffer size in DSM.

Yang et al. (2016) carried out a study on how to map the heterogeneous virtual machine requests to the heterogeneous physical machines in cloud computing platform. They first designed a video surveillance cloud platform architecture which could be seamlessly integrated with the video surveillance systems that comply with the ITU standard. They also proposed a multi-resource virtual machine allocation algorithm named Dominant Resource First Allocation (DRFA) aimed at resource optimization in heterogeneous cloud computing environment. By computing the dominant resource under multiple resource dimensions, their proposed DRFA algorithm can make full advantage of the heterogeneous physical resources. The authors finally implemented the cloud platform and developed some typical video surveillance services on the cloud platform. Their experimental results show that their resource allocation approach outperforms Other Widely Used Approaches.

2.20 Summary of Review of Related Literature/Research Gaps

Related works reviewed so far show that in era of big data, data continues to get bigger by the day in conformity to Internet of Things (IoT), Internet of Everything (IoE), and Internet of NanoThings (IoNT). Security and surveillance mandates are constantly increasing – longer retention terms, as well as higher frame rates and

resolutions. Due to these changes, more video data is being collected and stored than ever before, and the amount of data will continue to increase over time. From the reviews, authors hardly discussed video traffic without making reference to the associated enormous data volume and consequent bandwidth requirements, processing and storage. The importance of efficient management of video footage which is normally automatically stored, indexed, and recalled for a wide variety of needs, including: real-time or near-real-time security review, federal and state compliance requirements, evidence, either for prosecution or for liability defense, forensic investigation, and training/performance review cannot be overemphasized. As a result, video surveillance systems have migrated from being manually controlled by human operator (to record footage and store locally), such as the video surveillance system developed by Romanca et al. (2007) for controlling the access in a building. Video surveillance now goes with automated instantaneous capture with cloud storage.

Also, many works focused on data encryption and security such as Fan and Yibo's (2009) video encryption module and that of Chandra et al. (2012). Mahmood and Jensen (2016) also focused on data security and privacy enhancement, while Puthal et al. (2017) equally sought to develop a verification scheme for big data streams in line with security and privacy.

The reviews also show that a lot of research towards energy efficiency in the cloud is ongoing. Moganarangan et al. (2016) proposed a new hybrid algorithm combining the benefits of ant colony optimization (ACO) and cuckoo search algorithm. The algorithm focused on the voltage scaling factor for reduction of energy consumption.
The trend of literature in the area of cloud based video surveillance shows that all efforts are geared towards enhancement, expansion and optimization of cloud resources for a better life in readiness for internet of everything. OD-RGRSVS presents remote sensing as a service (RSaaS) with efficient optimization algorithm via proper load balancing techniques through computation of network traffic payload to improve video capture and storage efficiency. This enables the system to yield acceptable throughput values. OD_RGRSVS is also designed to address video surveillance storage limitation problem by incorporating on-demand capability via GSM control giving zero tolerance to irrelevant video processing. This form of

control makes it possible to provide remote video surveillance as a service (RVSaaS) to subscribers and drastically relieve the entire video surveillance infrastructure nodes of undue overhead costs.

In summary, most of the reviewed works clearly reveal that current security video surveillance systems are often subjected to undue video capture and storage, being triggered by sensors especially motion detectors. This necessitates development of OD-RGRSVS which is activated on-demand by valid GSM signal to process only relevant video data. This activation mechanism makes it possible to drastically reduce the amount of processed video data, and consequently, the storage requirements.

CHAPTER THREE

METHODOLOGY AND SYSTEM DESIGN

3.1 Methodology

A set of systematic techniques were used in this research. The techniques were basically prototyping followed by quantitative research approach.

3.1.1 Prototyping

Prototyping involves designing and building a miniature model of the system. This was carried out by laying out the modular design of the entire system which would be presented shortly.

3.1.2 Quantitative Research

Quantitative Research is an approach that involves generation of data meant to be subjected to formal quantitative analysis. It encompasses three classes which include; inferential, experimental, and simulation approaches. Out of the three classes of quantitative research, simulation approach was adopted in this work which involved development of mathematical models to characterize the cloud storage server clusters and conceptualize involved network traffic and overall traffic payload. This involved using queuing theory to present the analytical model of the system as a multiserver queue network modeled as a Markov chain.

The discrete event engine of Riverbed modeler 17.5 academic edition was used in the simulation to generate the data used in the system performance analysis.

Simulation approach involves the construction of an artificial environment within which relevant information and data can be generated. This permits an observation of the dynamic behavior of a system (or its sub-system) under controlled conditions. Given the values of initial conditions, parameters and exogenous variables, a simulation is run to represent the behavior of the process over time. Simulation approach can also be useful in building models for understanding future conditions. (Daniel & Sam, 2010).

3.1.3 Network Simulation Platform

A cloud network model which involved setting up network devices including the servers was created. Network traffic was also created, and the link and node statistics of the study were chosen. Simulation runs were carried out considering performance metrics such as network latency (sec), point-to-point throughput (packets/sec) and point-to-point utilization. Results were viewed and analysed, with optimal results presented through graphs.

At the beginning, a baseline scenario was setup by creating the network topology and network devices through the cloud control panel interface. This setup involved selection of the operating system and configuration of the servers (used to store surveillance images remotely from smart devices and other network devices) via the flavor section. Successful creation and provisioning of cloud storage servers cause it to display the status 'running' which indicates readiness and availability for remote connection. Video surveillance cameras were set up and configured accordingly.

The scenario was duplicated with changes made to link and node object attributes. Each time there was a change in the attributes, simulation run was carried out and the results were compared with the previous. Optimal values for the desired metrics were subsequently obtained using ten (10) IP cameras at the client side, while at the server storage cluster, six (6) servers were deployed at the primary storage cluster, and six (6) servers at the secondary storage cluster.

3.1.4 Research Outline

- Architecture for the proposed OD-RGRSVS was designed
- Hardware Prototype was designed and built
- mathematical characterization for the server clusters were developed and the system was modeled as a Poisson arrival process.
- An on-demand cloud model was developed (using the simulation tools of Riverbed modeler 17.5 academic edition).
- Data were generated from the discrete event simulation.
- Performance analysis was carried out and results were obtained.
- Validation of results using Cloud Analyst on CloudSim simulator.

3.2 Information Gathering

Sources of information used in carrying out this research were mainly the internet, magazines and research articles, text books on surveillance systems and network queuing models, video editing, IP technology. Oral information was also obtained from ICT consultants and experts who have gotten reasonable hands-on practical experience in the field over the years.

3.3 Analysis of Existing Systems

Existing video surveillance systems, some of which have been described in section 2.18 of chapter two in this dissertation (under *Summary of Related Literature*) feature the following;

- being triggered by motion, which makes the systems often capture irrelevant video feeds.
- The video coding standard of some existing systems was MPEG2, MPEG4, and H.263 instead of H.264 compression format which compresses across frames and consumes less bandwidth and storage.
- Some of the systems did not take advantage of IP technology. Even the IP based ones had storage limitations, being not cloud-based and lacks on-demand structure.
- The video surveillance system developed by Romanca et al. in 2007 incorporated IP cameras and allowed visualization of images by internet connection but, for recording images, admits only manual command from the human operator (who supervised the entrance) for video recording.
- Although some recent existing video surveillance systems are based on IP technology, the implementation and performance study lacks proper balance of cost efficiency.

3.4 The Proposed System (Global Concept)

An On-Demand Cloud-Based Real-Time Remote Sensing (OD-RGRSVS) system which is activated either by phone call or SMS has been proposed in this research work. It is based on GSM and IP technology which enables the system to render video surveillance coverage with remote storage on-demand. It also deploys GPS (Global Positioning System) technology to acquire location data of subscribers stored in the database at the control (base) station. The system is essentially composed of a master control station which could be signaled for service request at any time by any

subscriber from any location round the globe. Some other control stations (sub-control stations) are wirelessly connected to the master control station, and each sub-control station is linked to a number of clients under its coverage. This description matches the conceptual block diagram of the proposed OD-RGRSVS as shown in Fig.3.1.

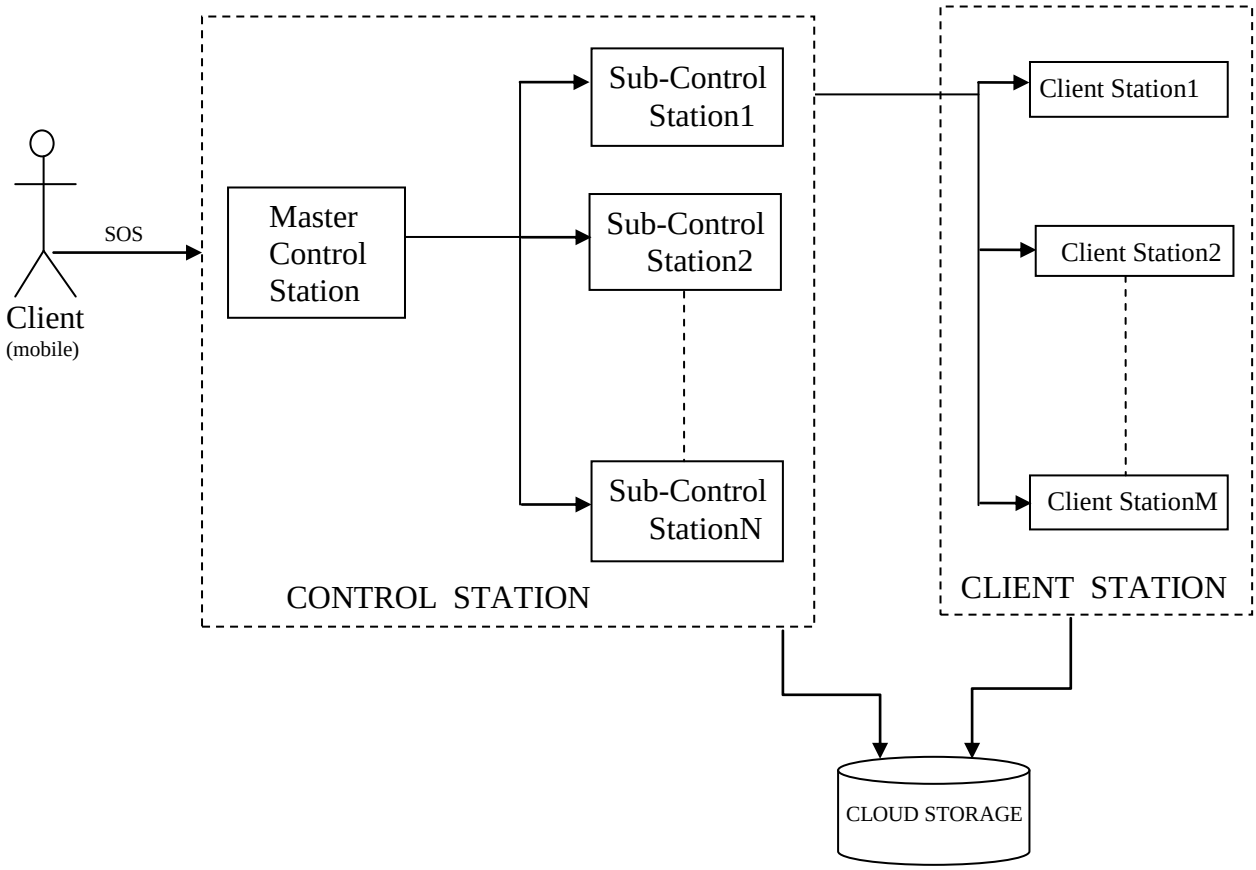


Figure 3.1: Conceptual Model of OD-RGRSVS.

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 Control Station (CS) in charge of the client's location as depicted in Fig.3.1. The CS in turn sends service activation signal to the corresponding client station and triggers surveillance action over the area for instantaneous video capture into the cloud network. It is important to note that the description so far characterizes a distributed system which is conceptual in the context of this research.

3.5 Distributed Processing

The global system block diagram (Fig.3.1) features distributed processing by having a centralized control station and distributing the work to multiple control substations. Such distributed layout gives room for scalability and expansion as the network grows.

3.5.1 Parallel Architectures

Modern parallel processing architectures have evolved into two broad categories, based upon the architectural differences; these are shared and distributed memory systems. Shared memory parallel systems link multi processors on a common memory and system bus. Whilst processing is distributed amongst the available processors, each processor still shares core services, such as memory, disk and operating system resources/functions. Communication between processors is achieved via shared or common memory between one or more processing elements. Shared memory systems include small to large-scale parallelism such as a dual or quad processing systems (Pentium or SPARC) and the Connection Machine. Modern systems of this type implement Symmetric Multi-Processing (SMP) and used a thread based model for parallel processing. SMP machines generally incorporates multi processors with a single unit/machine. Distributed parallel processing system includes a much broader spectrum of machines and devices and is open to a wider scope of interpretation. Distributed parallel systems involve linking a set of processing elements that have a certain level of autonomy with respect to memory and other system resources. Processing elements are connected to other processing elements via dedicated point to point links or a common communication bus. Parallel systems of this type include a transputer parallel sub-system where a network of transputers (each with their own memory) are linked to a host system which provides some shared resources, i.e. User Input / Output, disk / file access and operating system functions. Inter-processes communication is achieved using a message passing model where information / data is sent between communicating processors via the inter-process links or communications bus.

However, distributed parallel systems have adopted a much broader interpretation especially with the increase of computer / local area networks (LANs). In this sense a distributed system can include single processor machine connected via a common interface / LAN to provide a parallel processing cluster, a resource that can be

exploited as a virtual machine. Each individual machine in a cluster is an independent system in its own right, with total control over system resources including memory, disk etc.). The adoption of distributed or cluster computing has brought parallel processing to a wider audience so that benefit can be achieved without the need of expensive high performance specialized parallel processing equipment, this is especially true in the case of GIS.

3.5.2 Distributed Workstation Cluster

Distributed computing is well establish in the business and commercial sector, mainly due to the introduction of networks, operating systems and distributed databases. The scene is thus set for the benefit of distributed computing to be applied to GIS. The main advantage of using a cluster is that many organizations already have a network of fast processor machines (e.g. Pentium PC-based workstation). A network of uni-processor machines can be exploited as a non-specialized distributed parallel processing resource and significant speed-up can be achieved with only a few machines. A parallel cluster of machines (or workstations) can provide an overall system that is powerful, scalable and well structured (Bell, 1991).

A parallel cluster can connect machines of varying speeds, architecture and capabilities and can include specialized hardware. Clusters are generally classified into two categories, homogenous or heterogeneous. Homogenous networks connect machines of the same architecture and are therefore much simpler to support and organize in terms of data and application programs. Heterogeneous networks, on the other hand, link machines of different architecture (vendors) which introduces new issues when designing a distributed system, the main factor being a coherent and understandable set of protocols for process creation and communication.

3.5.3 Distributed Cluster Implementation

In developing a distributed system, attention must be paid to either reducing or synchronizing inter-process communication and thus circumvent any communication bottlenecks.

3.5.4 Single Master Node/Sub-Control Model

In single master node/sub control model (Fig.3.2) the master control station communicates with all other control stations, including sending initial configuration parameters, distributing the computation workload and collating results.

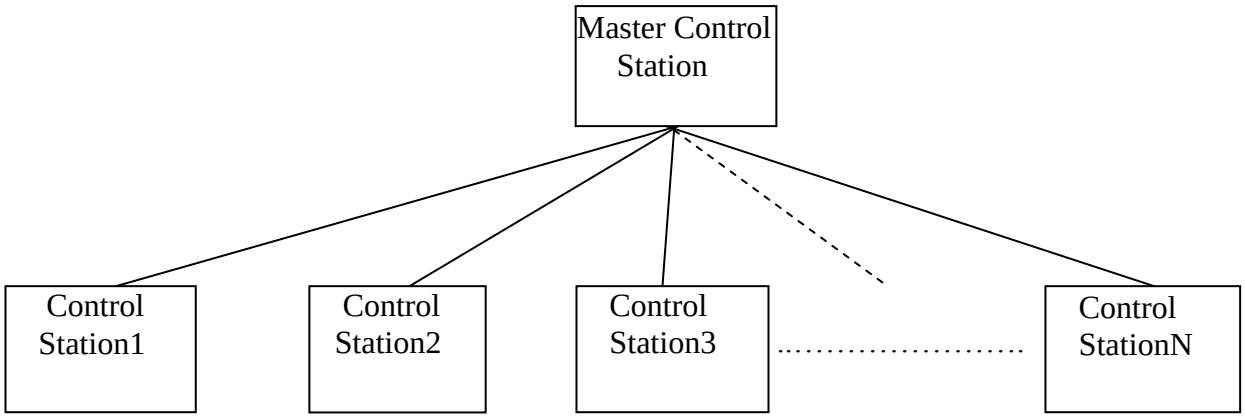


Figure 3.2 Single Master Node / Sub-Control Model

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. However, as the number of processing nodes increases extra communication (sub-master nodes) could be introduced to share the communication burden (Fig. 3.3).

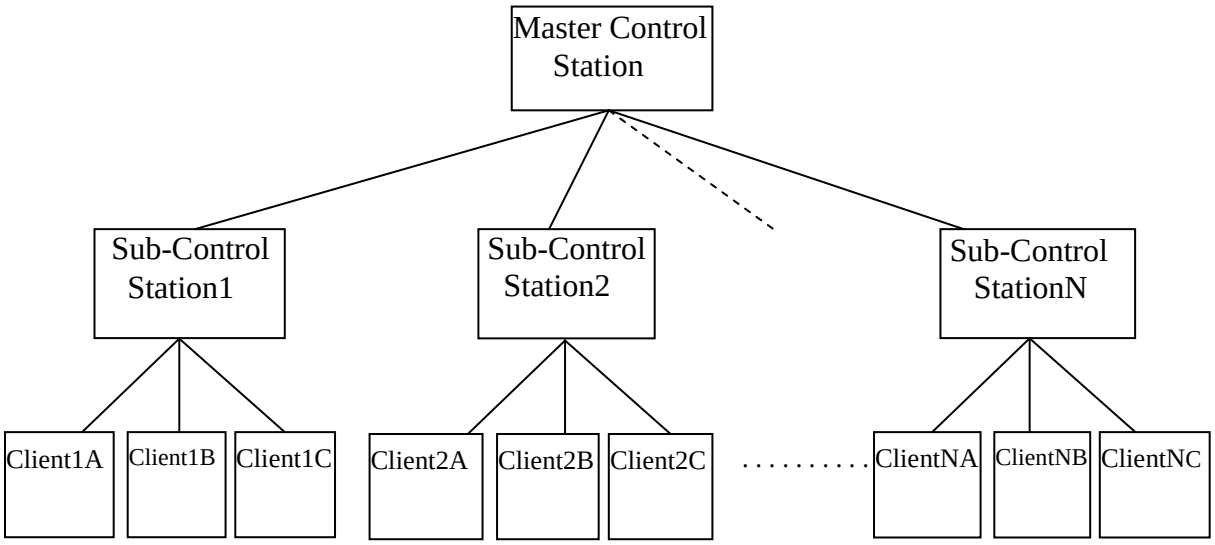


Figure 3.3: Single Master Node / Sub-control Model with Client Links

When and how these extra nodes are added depends upon the number of processing nodes, the channel capacity, and the data management strategy.

3.6 OD-RGRSVS IP Video Surveillance System

The OD-RGRSVS IP surveillance is a form of digitized and networked version of closed-circuit television (CCTV). Video surveillance cameras are mounted at all client locations with infrared capability for night vision and used for video capture whenever valid service request is received from client.

3.6.1 Architecture of On-Demand Cloud Based Real-Time Remote Sensing System (OD-RGRSVS).

The system architecture is shown in Fig. 3.4. It comprises a registered client who could send in a request for service in an SOS signal in form of SMS or phone call from an arbitrary location.

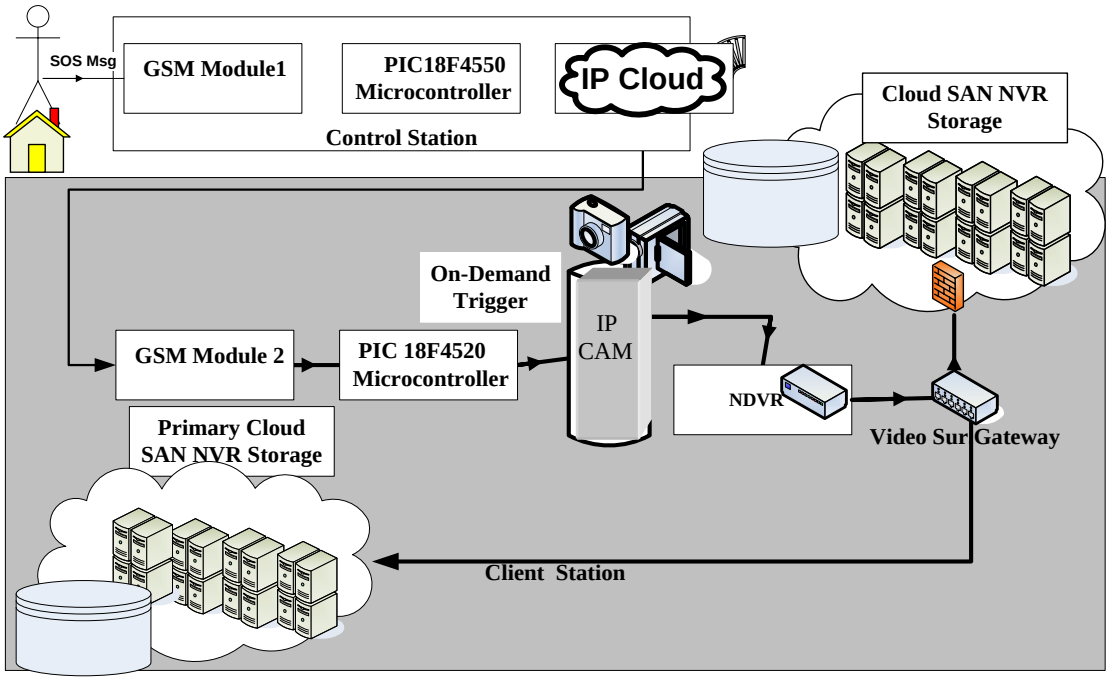


Figure 3.4: Network Architecture of On-Demand Real-Time GPS-Based Remote Security Video Sensing System (OD-RGRSVS)

In the system architecture, a client sends a request for service via a control station in charge of the client which triggers surveillance action over the area for which the location must have been registered and stored in the EEPROM (Electrically Erasable Programmable Read Only Memory) of the microcontroller.

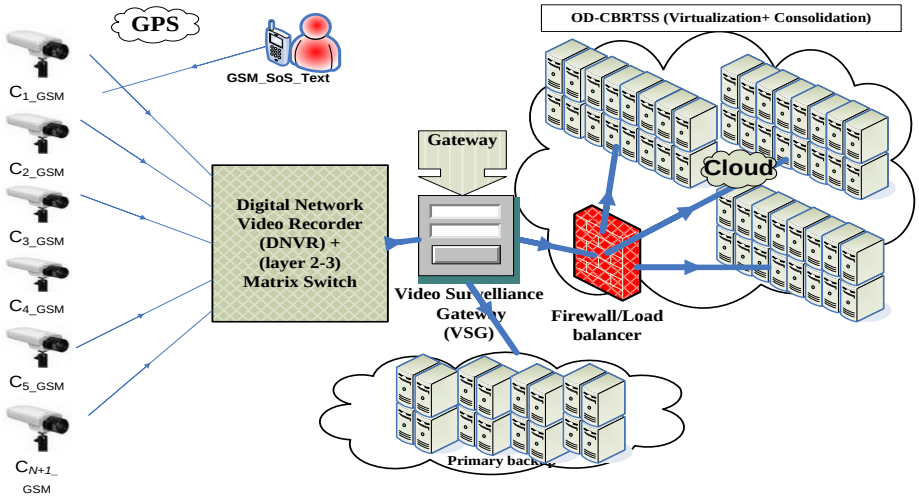


Figure 3.5: Cloud based on-Demand IP Surveillance System Architecture

In Fig.3.5, the Network XL-8 channel NVR NW3808XL is a software program that records video in a digital format to a disk drive, USB flash drive, SD memory card or other mass storage device. The NVR contains no dedicated video capture hardware. However, its software is typically run on a dedicated device, usually with an embedded operating system. To help support increased functionality and serviceability, standard Linux operating system was used with standard Intel processors and video management software. It was typically deployed as a backend to the location cluster IP video surveillance system. Upon being triggered in the network, the video captured snapshots are encoded and processed at the camera, for storage by the cloud based NVR. This is then streamed to the NVR for storage or remote viewing. Using the cloud computing paradigm makes it easy to set up, and can be accessed through a web browser, and allow the user to be notified by email if an alarm is triggered. The features include;

> Up to 4/8/16 channel 1080P cameras real-time live view

> H.264/MJPEG dual codec decoding

> Max 120fps@1080p, 240fps@720p,480fps@D1 preview & recording

> HDMI / VGA simultaneous video output

> All channel synchronous real-time playback, GRID interface

> Support Multi-brand network cameras

> 3D intelligent positioning with Dahua PTZ camera

> Support 2 SATA HDDs up to 8TB, 2 USB2.0

> Support IPC UPnP, 4 PoE ports

> Multiple network monitoring via web viewer

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.
- The ability to compress content 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.

3.6.2 IP Network-Centric Video Surveillance

Cisco systems proposed recommendations on how to build third- and fourth-generation video surveillance systems in a white paper - Cisco Systems Inc.(2007). IP Network-Centric Video Surveillance. Pp.1-14. 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.

3.7 Hardware Design Layout

The hardware design is conceptually made up of subsystems which comprise a **master control station** (or base station) wirelessly linked to **client stations** (sometimes referred to as sub-control stations in this dissertation). Each control station is in turn, connected to a number of client stations within its service domain as shown in Fig.3.6.

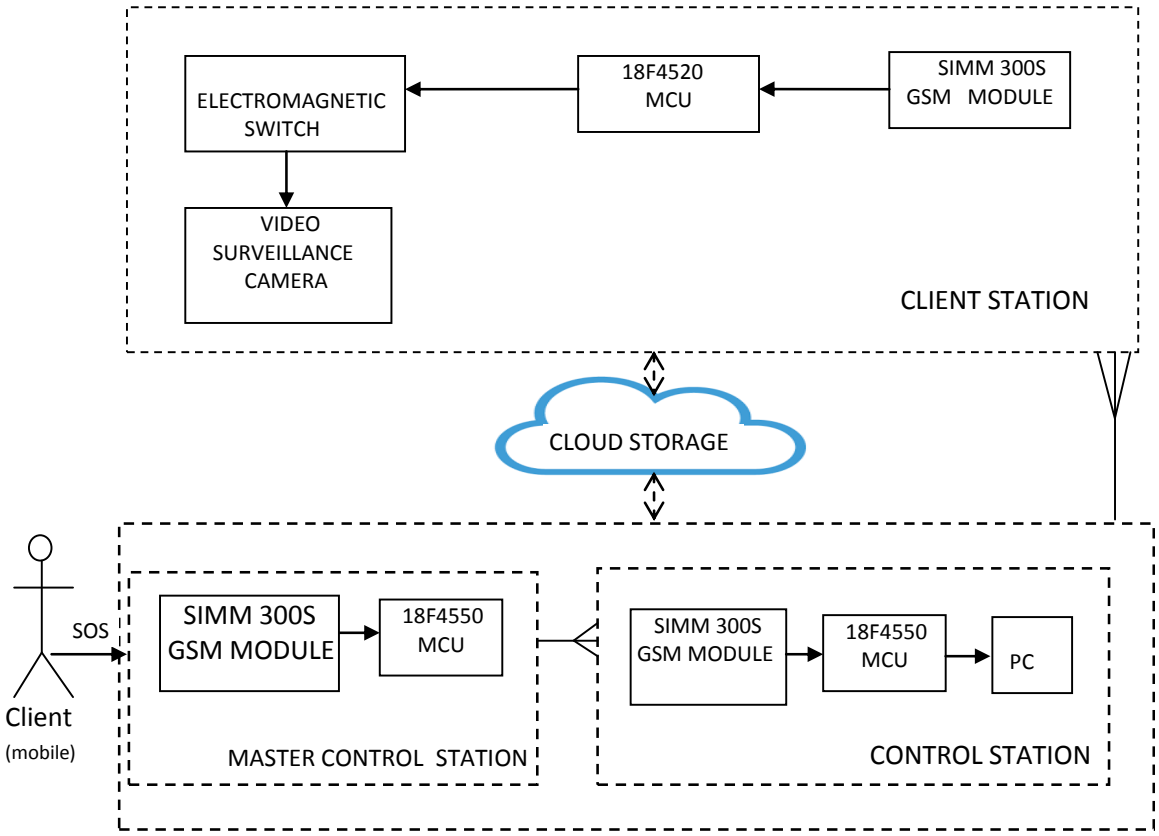


Figure.3.6: Block diagram layout of the on-demand real-time system modules
(Conceptual Model Block diagram Layout)

Arrival of requests (via the base station) for on-demand video processing service conforms to M/M/1 queue model while the end storage follows M/M/c queue model with multiple servers comprising primary and secondary backups.

This work focused on performance analysis of the OD-RGRSVS based on results obtained from the simulation platform using multiple service facility. Reference was therefore made to M/M/1 queue while characterization for the storage server clusters was handled as a multiserver queue model.

The diagram in Fig.3.37 represents traffic arrival rate λ_n, and service rate $\mu_{n,}$ of events with c parallel servers as service facilities.

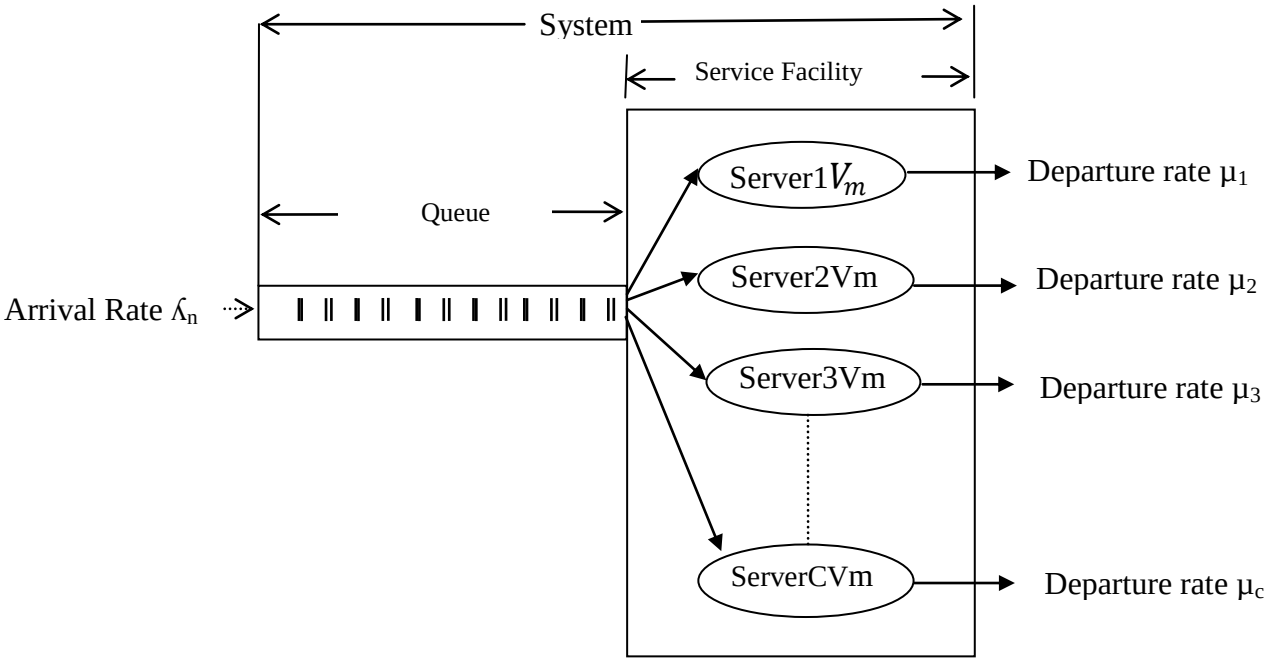


Figure 3.7: system model for storage with C parallel servers

3.8 Characterization of On-Demand Machines

The cloud server cluster, SV_m used in the simulation platform consists of physical and virtual storage servers denoted as S and V_m respectively. The server cluster is given by;

$$S_nV_{mT} = S_1(V_{m1}) + S_2(V_{m2}) + S_3(V_{m3}) \ldots\ldots + S_n(V_{m+1}) \quad (3.1)$$

Let $y = S_nV_{mT}$

$S_1 = a_0$; $S_2 = a_1$; $S_3 = a_2$; $S_4 = a_3$; ..... $S_n = a_k$;

$V_{m1} = X^m$; $V_{m2} = X^{m+1}$; $V_{m3} = X^{m+2}$; $V_{m4} = X^{m+3}$; ..... $V_{mn} = X^{m-k}$

Hence, the total physical server storage matrix is given by;

$$S_{nT} = \begin{pmatrix} S_{11} & S_{12} & S_{13} & S_{14} & S_m \\ S_{21} & S_{22} & S_{23} & S_{24} & S_m \\ S_{31} & S_{22} & S_{23} & S_{24} & S_m \end{pmatrix} \quad (3.2)$$

While total Virtual machine matrix is given by;

$$V_{mT} = \begin{pmatrix} V_{m11} & V_{m12} & V_{m13} & V_{m14} & V_{mk} \\ V_{m21} & V_{m22} & V_{m23} & V_{m24} & V_{mk} \\ V_{m31} & V_{m32} & V_{m23} & V_{m34} & V_{mk} \end{pmatrix} . \quad (3.3)$$

Now, the series solution to cloud server cluster is given by;

$$Y = a_0X^m + a_1X^{m+1} + a_2X^{m+2} + a_3X^{m+3} + \ldots\ldots\ldots + a_kX^{m+k} \quad (3.4)$$

Or

$$Y = \sum_{k=0}^{\infty} a_kX^{m+k} \quad (3.5)$$

Differentiating equation (3.5) yields;

$$\frac{dy}{dx} = \sum_{k=0}^{\infty} ak(m+k)\, X^{m+k-1} \quad (3.6)$$

Again, differentiating equation (3.6) yields;

$$\frac{d^2y}{dx^2} = \sum_{k=0}^{\infty} a_k\,(m+k)(m+k-1)X^{m+k-2} \quad (3.7)$$

But $\frac{d^2y}{dx^2} + \frac{dy}{dx} + y = 0$ (3.8)

By substituting (3.5), (3.6) and (3.7) into (3.8), we obtain;

$$Y = \sum ak(m+k)(m+k-1)X^{m+k-2} + \sum ak(m+k)\, X^{m+k-1} + \sum ak\, X^{m-k}$$

$$Y = ak\sum_{k=0}^{\infty}[(m+k)(m+k-1)X^{m+k-2} + (m+k)X^{m+k-1} + X^{m-k}] \quad (3.9)$$

Equation (3.9) characterizes the cloud server model.

3.9 Model Definition For On-Demand Video Surveillance Event

- Arrivals occur at rate λ according to a Poisson process.
- Service times are exponentially distributed with mean service rate μ. If there are less than *c* jobs, some of the servers will be idle. If there are more than *c* jobs, the jobs queue in a buffer.
- The buffer is of infinite size, so it can contain infinite number of customers.
- Jobs are processed under First In First Out (FIFO) i.e. First Come First Served (FCFS) queue discipline.
- The average proportion of time which each of the storage servers is occupied, ρ *is* the utilization factor for the service system given by; $\rho = \frac{\lambda}{c\mu}$. It is required that this value is less than 1 for the system stability
- The end storage conforms to M/M/c queue model.

3.9.1 Probability Density Function of Video Traffic Event

From probability theory, the probability density function of an exponential random variable such as request for service and/or video traffic event at the end storage is given by;

$$f(t; \lambda) = \begin{cases} e^{-\lambda t} & \text{for } t > 0 \\ 0 & \text{for } t < 0 \end{cases}$$

The cumulative distribution function of the exponential random variable is given by;

$$F(t) = \begin{cases} 1 - e^{-\lambda t} & \text{for } t \geq 0 \\ 0 & \text{for } t < 0 \end{cases}$$

The probability mass function of Poisson distribution which describes the probability of ***k*** events occurring at a time interval is given by;

$$P(\lambda; k) = \frac{\lambda^k e^{-\lambda}}{k!} \qquad (3.10)$$

Where λ = average number of events in an interval (i.e. event rate or rate parameter)

e = 2.71828 (Euler's number) equals the base of the natural logarithm, while k takes values 0,1,2,3,…..

We refer to Poisson transition diagram presented as continuous time Markov chain discussed in chapter 2, section 2.17 (Fig. 2.7) and use it to generate a transition rate matrix (generator matrix, stochastic matrix, or Markov matrix) which is used to describe the transitions of the Markov chain used to represent video sensing traffic events. The matrix, A, is given by;

$$A = \begin{bmatrix} -\lambda & \mu & 0 & 0 & 0 & 0 & 0 \\ \lambda & -(\mu+\lambda) & \mu & 0 & 0 & 0 & 0 \\ 0 & \lambda & -(2\mu+\lambda) & 2\mu & 0 & 0 & 0 \\ 0 & 0 & \lambda & -(3\mu+\lambda) & 3\mu & 0 & 0 \\ & & & & \ddots & & \\ 0 & 0 & 0 & 0 & \lambda & -(n\mu+\lambda) & n\mu \end{bmatrix}$$

In modeling of queue networks, one typically tries to obtain the equilibrium distribution of the network. Using the matrix, the steady state probabilities of the queuing system can be solved.

In order to determine the long term average system performance measures, we need to consider the steady state condition i.e. when the traffic flow into each state equals flow out of the state.

Let the steady state probability distribution vector $p = (P_0; P_1; P_2; P_3; \ldots P_n)^t$

Under steady state condition, $A*P = 0$.

i.e.

$$\begin{bmatrix} -\lambda & \mu & 0 & 0 & 0 & 0 & 0 \\ \lambda & -(\mu+\lambda) & \mu & 0 & 0 & 0 & 0 \\ 0 & \lambda & -(2\mu+\lambda) & 2\mu & 0 & 0 & 0 \\ 0 & 0 & \lambda & -(3\mu+\lambda) & 3\mu & 0 & 0 \\ & & & \cdot & & & \\ & & & & \cdot & & \\ & & & & & \cdot & \\ 0 & 0 & 0 & 0 & \lambda & -(n\mu+\lambda) & n\mu \end{bmatrix} \begin{bmatrix} P_0 \\ P_1 \\ P_2 \\ P_3 \\ \cdot \\ \cdot \\ \cdot \\ P_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ \cdot \\ \cdot \\ \cdot \\ 0 \end{bmatrix}$$

By law of conservation, the normalization equation is given by;

$P_0 + P_1 + P_2 + P_3 + \ldots\ldots + P_n = 1.$

We generate the steady state equations from the generator matrix as follows;

$$\lambda P_0 = \mu P_1 \qquad (3.11)$$

$$(\mu + \lambda)P_1 = \lambda P_0 + \mu P_2 \qquad (3.12)$$

$$(2\mu + \lambda)P_2 = \lambda P_1 + 2\mu P_3 \qquad (3.13)$$

$$(3\mu + \lambda)P_3 = \lambda P_2 + 3\mu P_4 \qquad (3.14)$$

Similarly,

$$(n\mu + \lambda)P_n = \lambda P_{n-1} + n\mu P_{n+1} \qquad (3.15)$$

Solving the system of linear equations to find the probabilities, $P_0, P_1, P_2, P_3, \ldots\ldots P_n$ yields performance measures for the queue model.

From (3.11), $\lambda P_0 = \mu P_1$

$$\therefore P_1 = \frac{\lambda}{\mu} P_0 \qquad (3.16)$$

Equation (3.16) represents the probability that only a single job is in the system.

For the purpose of this queue model with c>1, the balance equations are obtained expressing all probabilities in terms of P_0 as follows;

$$P_1 = \frac{\lambda}{\mu_c} P_0$$

From (3.12), $(\mu + \lambda)P_1 = \lambda P_0 + \mu P_2$

Substituting P_1 in (3.16) into (3.12) gives;

$$P_2 = \frac{\lambda}{\mu_c} P_1 = \left(\frac{\lambda}{\mu_c}\right)^2 P_0 \qquad (3.17)$$

Similarly, from (3.13),

$(2\mu + \lambda)P_2 = \lambda P_1 + 2\mu P_3$

$$P_3 = \frac{\lambda}{\mu_c} P_2 = \left(\frac{\lambda}{\mu_c}\right)^3 P_0 \qquad (3.18)$$

$$P_4 = \frac{\lambda}{\mu_c} P_3 = \left(\frac{\lambda}{\mu_c}\right)^4 P_0 \qquad (3.19)$$

By induction, from (3.16), (3.17), (3.18), and (3.19), the probability that there are n jobs in the system is given by;

$$P_n = \frac{\lambda}{\mu_c} P_{n-1} = \left(\frac{\lambda}{\mu_c}\right)^n P_0 \qquad (3.20)$$

By Chapman-Kolmogorov equation, (3.20) can be rewritten as ;

$$P_n = \begin{cases} \left(\frac{\lambda^n}{\mu(2\mu)(3\mu)\ldots(n\mu)}\right)P_0 & \text{For } n < c \\ \left(\frac{\lambda^n}{\mu(2\mu)(3\mu)\ldots(c\mu)(c\mu)}\right)P_0 & \text{For } n \geq c \end{cases} \qquad (3.21)$$

Equation (3.21) gives;

$$P_n = \begin{cases} \left[\frac{1}{n!}\left(\frac{\lambda}{\mu}\right)^n\right]P_0 & \text{For } n \leq c \\ \left[\frac{1}{c!}\left(\frac{\lambda}{\mu}\right)^n\left(\frac{1}{c^{n-c}}\right)\right]P_0 & \text{For } n > c \end{cases} \qquad (3.22)$$

Let $\frac{\lambda}{\square} = \rho$

Equation (3.22) becomes;

$$P_n = \begin{cases} \frac{\rho^n}{n!} P_0 & \text{For } n \leq c \\ \left[\frac{\rho^n}{c!}\left(\frac{1}{c^{n-c}}\right)\right] P_0 & \text{For } n > c \end{cases} \qquad (3.23)$$

The steady state probabilities of the various states of the video sensing facility so obtained can then be used to analyze various performance measures of the queue model.

3.10 Performance Measures

In order to carry out performance rating of the queue model, we consider what happens when a stream of packets arrive at the system in respect of response time, throughput and server utilization.

We apply Little's law to determine the number of packets/users/requests in the system, server's throughput and the average response time under steady state conditions. The law states as follows;

$$N_s = \lambda * W_s \qquad (3.24)$$

Where N_s = average no. of customers in the service facility

λ = average arrival rate

W_s = average waiting time (i.e. time spent in the system)

In the multiserver system with c servers, no queue is formed until all the servers get busy. Packets queue up when they arrive and find all the servers busy. If there are n jobs in the system, then n-c represents the number of jobs in the queue at any time instant.

The long term average number of packets in the queue, N_q, is given by;

$$N_q = \sum_{n=c}^{\infty} (n - c) P_n. \qquad (3.25)$$

Where P_n is the probability of having n jobs in the system.

Let j = n-c which implies that n= c+j

$$\Rightarrow \quad N_q = \sum_{n=c}^{\infty} jP_n \tag{3.26}$$

From (3.20), P_n can be rewritten as;

$$P_n = \left(\frac{\lambda}{\mu} + \frac{\lambda}{2\mu} + \cdots + \frac{\lambda}{c\mu}\left(\frac{\lambda}{\mu}\right)^j\right)P_0$$

$$= \frac{\rho^c}{c!c^j}\rho^j P_0 \tag{3.27}$$

Combining (3.26) and (3.27) ;

$$N_q = \sum_{j=0}^{\infty} j\left(\frac{\rho^c}{c!c^j}\rho^j\right)P_0 \tag{3.28}$$

Which can be rewritten as;

$$N_q = \left(\frac{\rho^{c+1}}{(c-1)!(c-\rho)^2}\right)P_0 \tag{3.29}$$

Having determined the number of jobs in the queue, N_q in (3.29), the waiting time in the queue, W_q can be determined using Little's formula as follows;

.

$$W_q = \frac{N_q}{\lambda} \tag{3.30}$$

3.10.1 The Cloud facility Response Time

The long term average system response time (or sojourn time), $E[W_s]$, which is the expected mean response time in the system equals sum of expected waiting time in the queue, $E[W_q]$ and time spent in service, $\frac{1}{\mu}$. That is;

$$E[W_s] = [W_q] + \frac{1}{\mu} \tag{3.31}$$

3.10.2 The Cloud Facility Throughput

The long term average service facility throughput, $E[T_p]$ is related to the expected average number of packets in the system, $E[N_s]$, and the expected average waiting time in the system, $E[W_s]$ as follows;

$$E[T_p] = \frac{E[Ns]}{E[Ws]} \quad (3.32)$$

From (20), the expected average number of packets in the service system, $E[N_s]$, is deduced as follows;

$$E[N_s] = \lambda E[W_s] \quad (3.33)$$

$$\Rightarrow \lambda = \frac{E[Ns]}{E[Ws]} \quad (3.34)$$

Equation (3.34) shows that λ corresponds to the actual system throughput compared with (3.32).

The expected average number of packets in the system, $E[N_s]$, (which is the long term average workload on the facility) equals the sum of expected average number of packets in the queue, $E[N_q]$ and the number of packets being served.

$$\text{Thus, } E[N_s] = E[N_q] + \rho \quad (3.35)$$

$$\text{Also, from (3.21), } E[W_s] = W_q + \frac{1}{\mu}$$

Therefore, the expected average throughput of the cloud service facility, $E[T_p]$ is given by;

$$E[T_p] = \frac{E[Nq] + \rho}{E[Wq] + \frac{1}{\mu c}} \quad (3.36)$$

Where μ_c is the service rate of the multiserver queue model.

The importance of (3.36) is that the network throughput values need be monitored at any point in time to maintain acceptable quality of service and improve performance by either adding more service facilities or otherwise.

3.10.3 Service Facility Utilization

At any point in time, it is expected that the cloud server utilization factor (which is the traffic intensity) $\rho = \frac{\lambda}{\mu} < 1$ to maintain stability, according to ***operational law***. If the

traffic intensity is greater than 1, the system becomes unstable. This is applicable to the single server case.

For the purpose of this video sensing storage event model where c>1, the traffic intensity, $\rho = \frac{\lambda}{c\square}$.

3.10.4 Input/Output Parameters

The analytical queue model was defined using three input parameters which include; arrival rate, λ, service rate, μ, and number of servers, c.

The outputs include; resource utilization, ρ, and the number of jobs waiting in the queue, N_q, and waiting time in the queue, W_q. We then use simple formula to convert number-of-customers-waiting N_q into time-a-customer-waits W_q, i.e. $N_q = \lambda W_q$. This relationship holds for jobs in the queue. The relationship for the entire system is deduced in a similar fashion, i.e. $N_s = \lambda W_s$ to include both jobs in the queue and jobs being served.

3.10.5 Determination of Capacity

If the capacity of the service facility is increased (by increasing the number of servers, c, or by increasing the service rate, μ), it results in increased cost of providing that capacity. This will lead to jobs waiting less which implies decrease in cost of job waiting time. This suggests that one should look at the total cost, C_T which is the sum of cost of providing service, C_s and cost of customer waiting, C_w in order to make decision about how much capacity to provide. Determination of capacity is a trade-off between cost of service capacity and cost of jobs waiting.

A major objective of network provider is system optimization whereby minimization of network response time (latency) and C_T are targeted while maximizing throughput and total profit. This has led to development of various queue models with strategies to consider customer behaviors for better network performance predictions. Som & Seth (2018) developed a set of multiserver queuing systems with encouraged arrivals, reneging, retention and feedback customers. According to them, customers often get attracted by lucrative deals and discounts offered by firms, so the authors integrated incentives in the models to make the system attract more patronage.

3.11 Prototype Hardware

The prototype hardware of OD_RGRSVS was designed and built using a control station (or base station) which served as the master control station, and a client station as shown in Fig. 3.8.

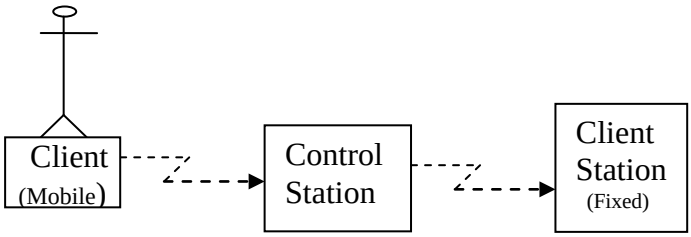


Figure 3.8: Block diagram of the major prototype modules.

The block diagram shows that a client with a mobile handset can call the control station from any arbitrary location requesting for his/her fixed station (client station) to be monitored. The control station validates the request with the client database stored in the EEPROM of the microcontroller.

3.11.1 Control Station Prototype

The control station is equipped with SIM 300S GSM modules which serves as a transceiver (Fig.3.9). All request signals from clients who could send request from any arbitrary location are received by the GSM module connected to PIC 18F4550 MCU (Microcontroller Unit) via a voltage level converter. The MCU validates the signal by making reference to registered clients' database stored in the EEPROM of the MCU. If the request is valid, the MCU alerts the GSM module to trigger the client station for surveillance action. As a control measure, the control station sends commands to client stations with the prefix) "**CLX**", where X represents the clients location number.

The microcontroller is connected to the PC via USB (Universal Serial Bus). The PC is essentially used for client database management which would be discussed subsequently.

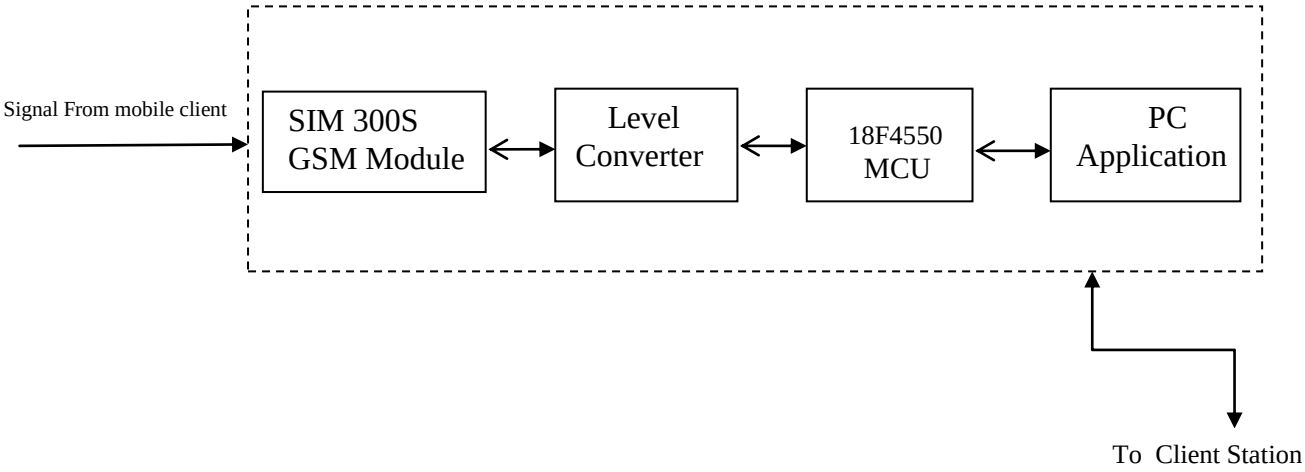


Figure 3.9: Control Station block diagram

3.11.2 Client Station Prototype

The fixed location (client station) of each subscriber (mobile client) to this system is similarly equipped with SIM 300S GSM module for receiving commands from the control station. It uses PIC18F4520 MCU since it does not require PC interface. The client station is always powered ON but the cameras are activated to capture only when triggered by the microcontroller which must have received command from the GSM module. This automated control was achieved by the firmware in the microcontroller which was written in embedded C-language in MPLAB Integrated Development Environment (IDE). A block diagram of the client station is shown in Fig.3.10.

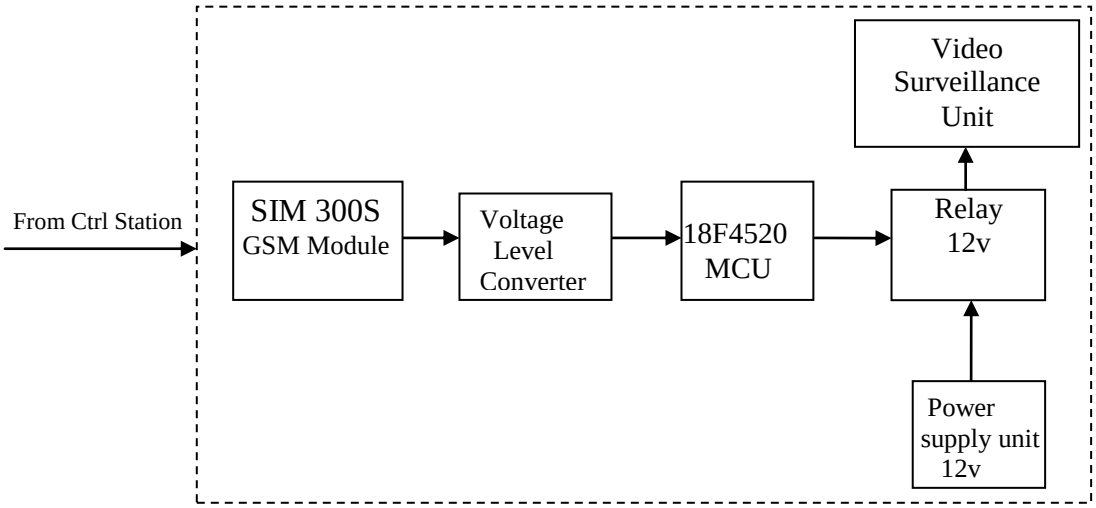


Figure 3.10: Client Station block diagram

The client station receives commands via SIM 300S GSM module connected to 18F420 MCU with a simple transistor-pair level converter in between. The MCU activates the 12v relay circuit which is connected to power both the surveillance camera and the DVR since each of them is powered by 12v supply.

3.12 Essential Prototype Hardware Subsystems

3.12.1 GSM Module

A snapshot of SIM 300S GSM module is shown in Fig. 3.11. It can accept any GSM network operator SIMM (Single Inline Memory Module) card and acts just like a mobile phone with its own unique phone number. The advantage of this module is that its RS232 port can be used to communicate and develop embedded applications such as SMS control, data transfer, remote control and logging.

Figure 3.11: Snapshot of SIM 300S GSM Tx/Rx Module

The GSM module can either be connected to PC serial port directly or to any microcontroller. It can be used to send and receive SMS or make/receive voice calls. It can also be used in General Packet Radio Service (GPRS) mode to connect to the internet and do many applications for data logging and control. In GPRS mode, you can also connect to any remote File Transfer Protocol (FTP) server and upload files for data logging. The modem is a highly flexible plug and play quad band GSM modem for direct and easy integration to RS-232 applications. SIM 300S GSM modules were used in the design and implementation of the prototype. A SIMM (Single Inline Memory Module) module was interfaced to PIC 18F4550 at the control

station, while another one was interfaced to PIC18F4520 at the client end. The microcontrollers feature USART (Universal Synchronous and Asynchronous Receiver Transmitter) capabilities.

3.12.2 Power Supply Unit

Most of the gadgets such as the cameras in the system are powered by 12v, while some that go on 5v such as the GSM module were aided by LM7805 voltage regulator as shown in Fig. 3.12.

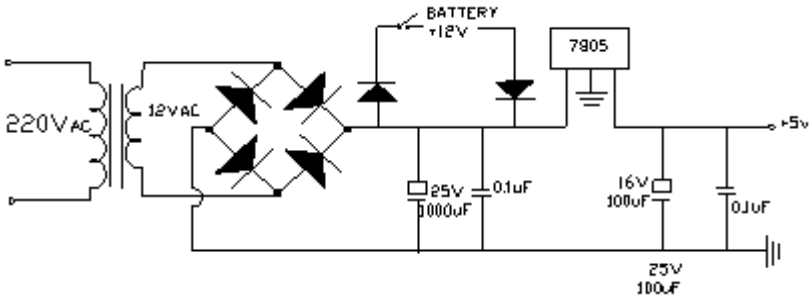


Figure 3.12: Power supply unit

The entire system is terminally connected to 220V ac (alternating current) which is passed through a 12V step down transformer (Fig.3.12). The output is rectified to give 12V dc (direct current) required to switch the relay circuit that powers the servomotor at the client station. The microcontroller units and GSM modules are powered by 5v supplied by 7805 voltage regulator.

3.12.3 PIC 18F4520 Microcontroller Pin Diagram

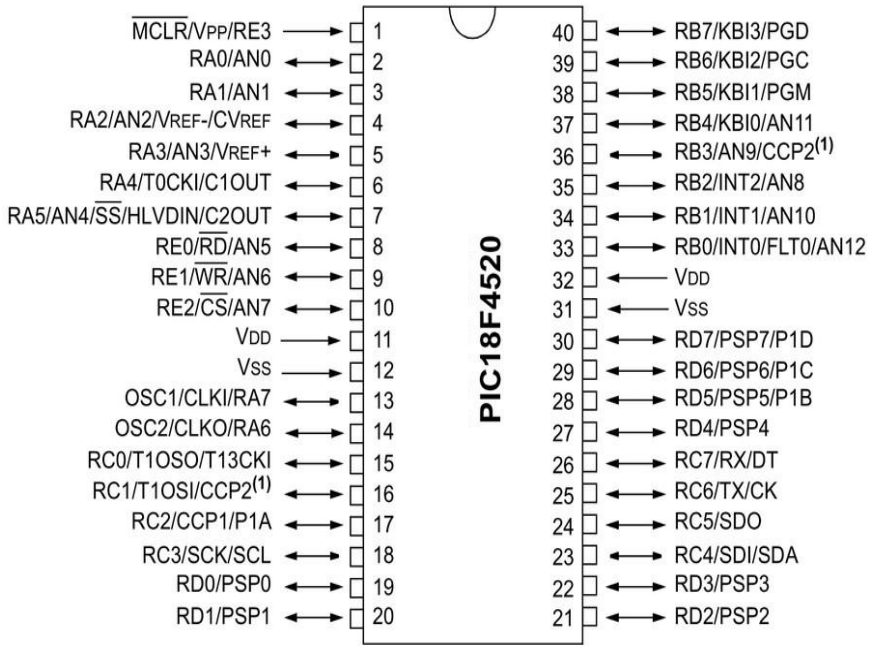


Figure 3.13: PIC18F4520 Microcontroller Pin Diagram

The features of PIC 18F4520 Microcontroller whose pin diagram is shown in Fig.3.13 include;

- 40-pin Low Power Microcontroller
- Flash Program Memory: 32 kbytes
- EEPROM Data Memory: 256 bytes
- SRAM Data Memory: 1536 bytes
- I/O Pins: 36
- Timers: One 8-bit / Three 16-Bit
- A/D Converter: 10-bit Thirteen Channels
- PWM: 10-bit Two Modules (PWM stands for Pulse Width Modulation)
- Enhanced USART: Addressable with RS-485, RS-232 and LIN Support
- MSSP: SPI(Serial Peripheral Interface) and I²C(Inter-Integrated Circuit) master and Slave Support (MSSP stands for Master Synchronous Serial Port)
- External Oscillator: up to 40MHz
- Internal Oscillator: 8MHz

The 40-pin version of 18F4520 MCU (Fig. 3.13) was found fit as it possesses features suitable for data transmission and Reception via the Tx pin 25 and Rx pin 26 respectively, and the I/O pins werer sufficient for all the necessary data tansfers.

3.12.4 PIC 18F4550 Microcontroller Pin Diagram

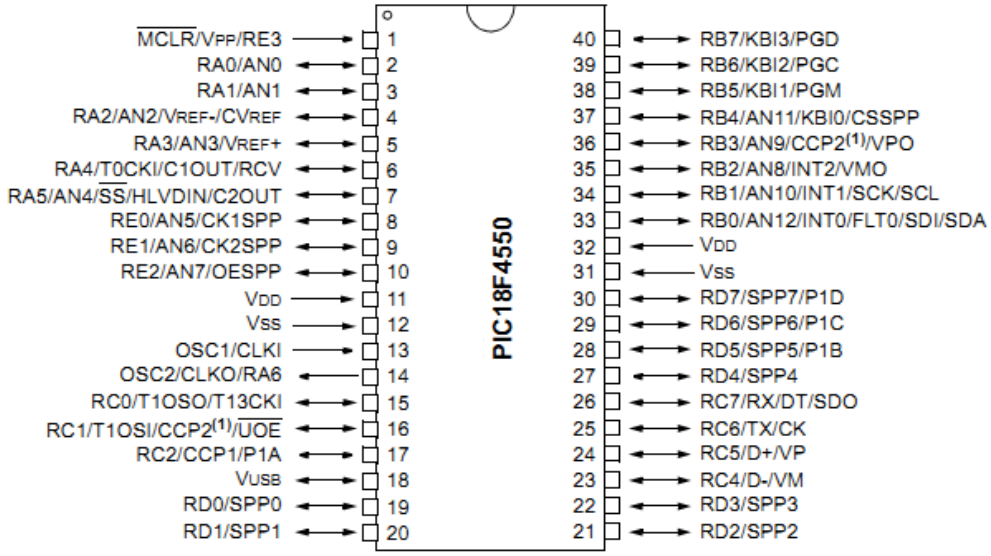


Figure 3.14: PIC 18F4550 microcontroller pin diagram

PIC 18F4550 microcontroller unit (Fig. 3.14) was used at the control station for ease of interfacing to PC via pin 18 (V_{USB}) which is a full speed universal serial bus (USB) not found in PIC 18F4520 microcontroller unit used at the client station. It also has RAM capacity of 2048 bytes which is higher than the 1536 bytes capacity of the client station 18F4520 unit.

3.13 Prototype Hardware Design

Each of the control and client station modules of which the prototype is composed consists of microcontrollers and GSM modules which were procured from the market. GSM modules were connected to the microcontrollers via two-transistor pair voltage level converters. This was done because the microcontroller uses TTL logic level, while GSM module uses serial interface referred to as RS232 standard which is a different scheme for logic levels, hence the need for a level converter in between.

3.13.1 RS232 Communication

The motive behind RS232 Communication is to send and receive data between two devices using RS232 standard. RS232 is serial interface which implies that data is transferred bit by bit at a time, requiring only a single wire to send data and another one to receive data, including a common wire (GND) required between two separate circuitry to enable current flow. Data is transmitted through the Tx line and received

via Rx. So a total of three wires are required for communication. RS232 can be used to communicate between a variety of devices like the MCU (Micro Controller Unit) and a GSM module or a PC. The PIC18F4550′s USART serves as the control microcontrollerr, transmitting data at a specified data rate (9600bps, 115200bps etc.) In this work, a PIC18F4550 MCU was connected to the GSM module (Fig.3.11), and a Windows HyperTerminal program on PC was used to test the link. A terminal program is used to send and receive text data. So any text sent by the MCU will be visible on terminal screen and any key press made on the PC keyboard would be sent over RS232 to the MCU. This configuration is the simplest setup to test and understand RS232 communication. The Terminal can be replaced with one's own PC end software for sending and receiving data. The same functions that we use here to communicate with PC can be used to send/receive data to/from other devices also. But modern PCs do not have a serial port, so one could use a USB to serial converter. The PIC MCU uses TTL logic level i.e. a logic 1 represents 5v and logic 0 is 0v, but RS232 (now EIA232) standard uses a different scheme for logic levels, hence the need for a level converter in between. MAX232 IC is often used for this conversion purpose.

When a MAX232 IC receives a TTL level to convert, it changes a TTL logic 0 to between +3 and +15 V, and changes TTL logic 1 to between -3 to -15 V, and vice versa for converting from RS232 to TTL.

However, a simple low-cost, transistor-pair voltage level converter was used to implement this conversion as shown in (Fig. 3.15).

3.13.2 Transistor Based RS232 Level Converter

By RS232 standard, a logic high (1) is represented by a negative voltage which ranges from -3v to -25v, while a logic low (0) represents a positive voltage within +3v to +25v range.

On most PCs, these signals swing from -13v to +13v. The more extreme voltages of an RS232 signal helps to make it less susceptible to noise, interference and degradation. This implies that RS232 signal can travel longer distances than the TTL counterparts.

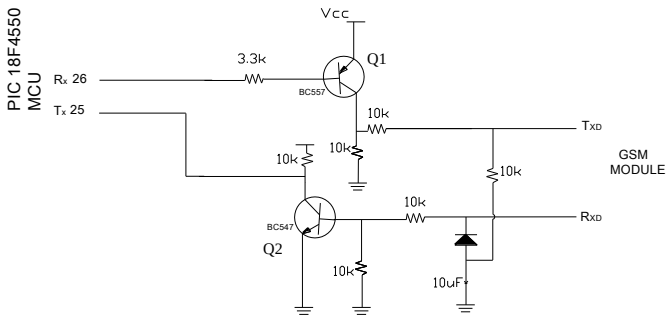


Fig 3.15 Two-Transistor Voltage Level Converter

In the circuit diagram of Fig. 3.15, two small signal transistors which include BC547 (NPN) and BC557 (PNP) transistors were used. For an application that requires only transmitter circuit, the transmitter section of the circuit could be used with the GND signal connected to it. The transmitter circuit uses PNP transistor, BC557. While in mark state, the Tx RS232 signal is logic '1', Q1 turns off. Tx RS232 signal then provides the negative voltage to Rx RS232. For space state, Tx control signal then becomes logic '0', which turns on Q1, the approximately +5V is then fed to Rx control signal. With this method, while sending data is being made, Tx control signal must be stable at -9V, say. Some applications not only need transmitter, but also receiver. The circuit at the lower symmetry is a simple inverter circuit that converts RS232 level back to TTL logic. When PC sends data to Tx pin, logic '1' is -9V, say, Q2 turns off, Rx (TTL) is approximately +5V. The start bit makes Tx to approximate +9V, Q2 then turns ON, Rx (TTL) then becomes approximately 0V. The circuit can be used for half duplex transmission.

The PIC18F4550 chip has in-built USB transceiver which provides for interfacing to PC. The conversion actually serves for the GSM modules, one at the control station (Fig. 3.15a) and the other at the client station(Fig. 3.15b).

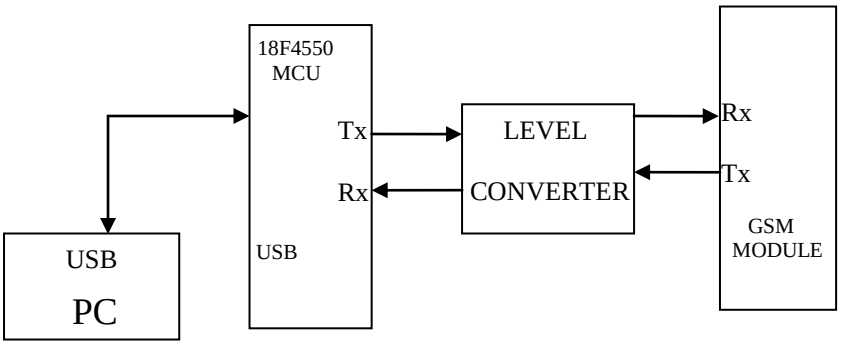


Figure 3.15a: Control Station using 18F4550 with PC interface

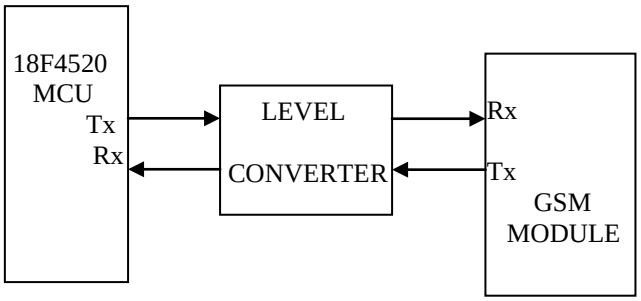


Figure 3.15b: Client Station using 18F4520 without PC interface

However, a prototype of the surveillance system was built using a control station and a client station in order to curtail equipment costs.

3.13.3 Relay Interfacing with Microcontroller

Digital ICs cannot provide the necessary current and voltage to turn ON a Relay, hence, a relay driver circuit is required in the prototype OD-RGRSVS. The basic function of the driver circuit is to provide the necessary current to energize the relay coil. Generally relay coils operate from 5V to 24V and require about 25mA to 100mA current to energize the coil, the current required to turn ON a relay is referred to as "PULL IN" or "HOLDING" current. This PULL IN current depends upon the Relay used. The simplest form of relay driver circuit consists of an NPN or a PNP transistor. Almost all the digital circuits can provide enough base current to turn ON a transistor.

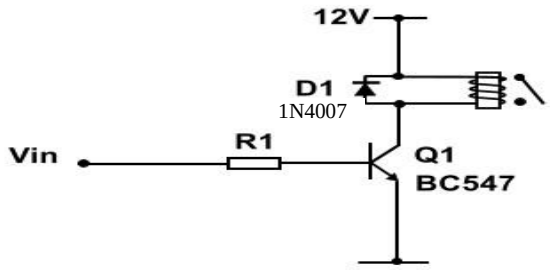


Figure 3.16: Relay driver circuit

An NPN transistor BC547 is being used to drive the relay (Fig.3.16). The relay has a 12V coil i.e. it can be turned ON only when the operating voltage i.e. the Vcc is 12V. The resistor R1 is used to set the base current for the transistor, the value of R1 is such that when the input voltage, Vin is applied, the transistor is driven into saturation, and the relay is energized. It is important that the transistor is driven into saturation so that the voltage drop across the transistor is minimum thereby dissipating very little power. Now we have to calculate the value of R1. Suppose the relay requires a PULL IN current of 80mA, so the collector current has to be at least 80mA. The minimum DC current gain of BC547 is 100, so the minimum base current should be;

$$I_B = I_C/H_{fe} = 80/100 = 0.8mA$$

So the minimum base current is 0.8mA (Fig.3.14). But to be on the safe side i.e. just to make sure that the transistor is in saturation region, we approximately double this value to say 1.5mA. Now, if the Vin is switching from 0V to 12V, the base resistor, R1 is given by;

$$R1 = \frac{Vin - V_{BE}}{I_B}$$

Where V_{BE} is the bias voltage.

Vin = 5V, V_{BE} = 0.6, and I_B =1.5mA

$$R1 = \frac{5 - 0.6}{1.5 \times 10^{-3}} = 2.933k\Omega.$$

This implies that 2.933KΩ resistor could be used to provide base current of 1.5mA, which is sufficient to turn ON the relay and activate it. So we can use 3.33KΩ as the base resistance R1, which is the approximate value of resistor commonly available in the market. A diode (1N4007) is connected across the relay coil; this is done so as to

protect the transistor from damage due to back electromotive force generated in the relay's inductive coil. When the transistor is switched OFF the energy stored in the inductor is dissipated through the diode and the internal resistance of the relay coil.

3.14 Instruction Cycle of MCU and Oscillator Frequency

The relationship between the oscillator frequency of the PIC microcontroller and the instruction cycle duration is a very crucial subject requiring proper consideration.

PIC microcontroller uses 4 clock cycles to perform a single instruction. The frequency of PIC microcontroller, F_{pic} is therefore related to the frequency of crystal oscillator F_{cry} by the equation;

$$F_{pic} = \frac{Fcry}{4} \qquad (F_1)$$

As we used 20MHz crystal oscillator, it is equivalent to clock rate of 0.2µs obtained by substituting the value of crystal into equation (F1) as follows;

F_{pic} = 20MHz/4 = 5MHz. i.e 4 pulses = 1 operation

Now, $F_{pic} = \frac{1}{T}$ where T is the period, and $T = \frac{1}{F}$

This implies that $T = \frac{1}{5x10^6} = \frac{1x10^{-6}}{5} =$ 0.2µs is equivalent to one cycle

The question now is; if one cycle takes 0.2µs to complete, how many cycles can run in one second? This question would be answered as we consider the microcontroller throughput.

3.15 PIC18F4520 Throughput

Nowadays, the throughput of modern processors are measured in Million Instructions Per Second (MIPS). When designing a PIC project, the first thing to consider is the oscillation clock source and frequency of the PIC. The PIC will internally divide the clock input frequency by 4 in order to execute the program instructions. Since the PIC takes 0.2µs to complete 1 cycle, the throughput in MIPS is determined as follows;

1 cycle = 0.2µs = 0.2 x 10^{-6}s

?cycles = 1s

Let the number of cycles be X

X per second = $\frac{1}{0.2 \times 10^{-6}}$ = 5MIPS.

3.16 System Communication Test

The GSM module was configured and tested by using the MS-Windows HyperTerminal, setting the baud rate to 9600 bps.

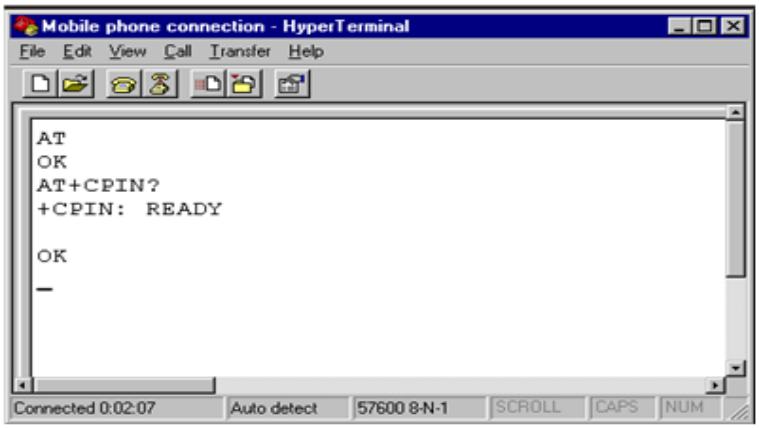


Figure 3.17: GSM module communication test response using Hyper Terminal.

On typing “AT” and pressing “Enter” , it displayed “OK”. It was also checked for password requirement using the AT + CPIN command and it displayed READY (Fig. 3.17).

Further communication tests were carried out by sending and reading text messages to and fro the modules using AT commands issued from the PC terminal, after which the GSM modules were connected to the control and client circuits respectively.

3.17 How The Control And Client Stations Work

The control station circuit is connected to a GSM module and embedded with PIC 18F4550 MCU interfaced to PC terminal which provides the GUI for client database management. The control station is always switched ON.

The client station circuit is connected to a GSM module but this time embedded with PIC 18F4520 MCU which requires no interfacing to PC terminal.

When the client station is powered up, the microcontroller initializes the peripheral ports and delays for 5seconds to enable the GSM module start the SIMM card and acquire network. The DVR connected to client station taps 12volts from the client station circuit to get powered up (See Appendix D). When a valid command is received from the control station in form of phone call or SMS, the microcontroller interprets the command (which it acquires from the GSM module) powers up the

DVR to start recording for the specified period of time. If the duration is not stated, the default period of 15 minutes is implemented.

Appendices B and C contains the full schematic diagrams of the client station and the control station respectively. Snapshots of the prototype hardware are found in Appendix D.

3.17.1 Control Station Operation Flow Chart

An operation flowchart of the control station prototype is shown in Fig. 3.18. The flowchart presents how the prototype of the control station works. The process automation and control is achieved using the embedded C-language codes stored in the PIC16F4550 microcontroller which is a component of the control station. This way, the firmware handles communication between the control station and the client station. (See Appendix F for the C-language code listing).

As soon as the system is powered ON, the microcontroller gets initialized with other modules and verifies the signal for client subscription validity, using the client's location and subscription data stored in the database which resides in the EEPROM of the control station microcontroller. If the signal is valid, the request is processed and executed.

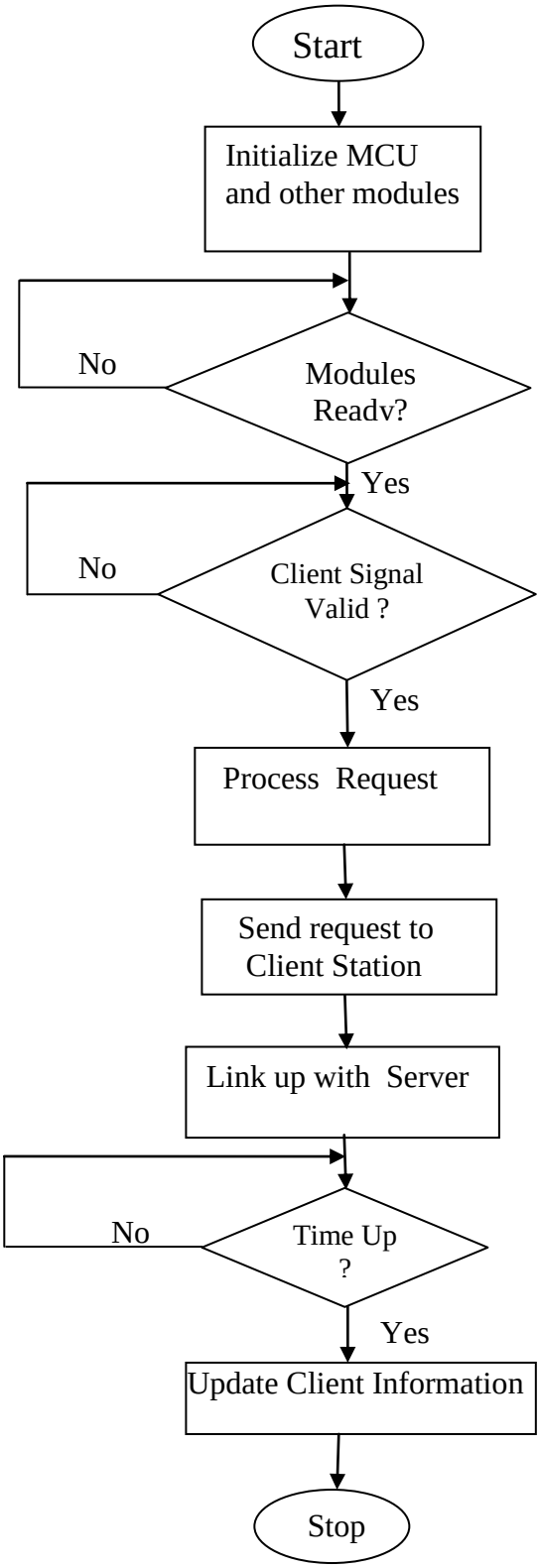


Figure 3.18: Control Station prototype operation Flowchart

3.17.2 Client Station Operation flowchart

The client station flowchart (Fig. 3.19) presents how the prototype of the client station works. When the system is powered up, the MCU and other modules initialize. The system checks whether the modules are ready or not. If ready, valid signal from control station is checked for. If any valid signal is detected, cameras are activated and recording is initiated for as long as requested.

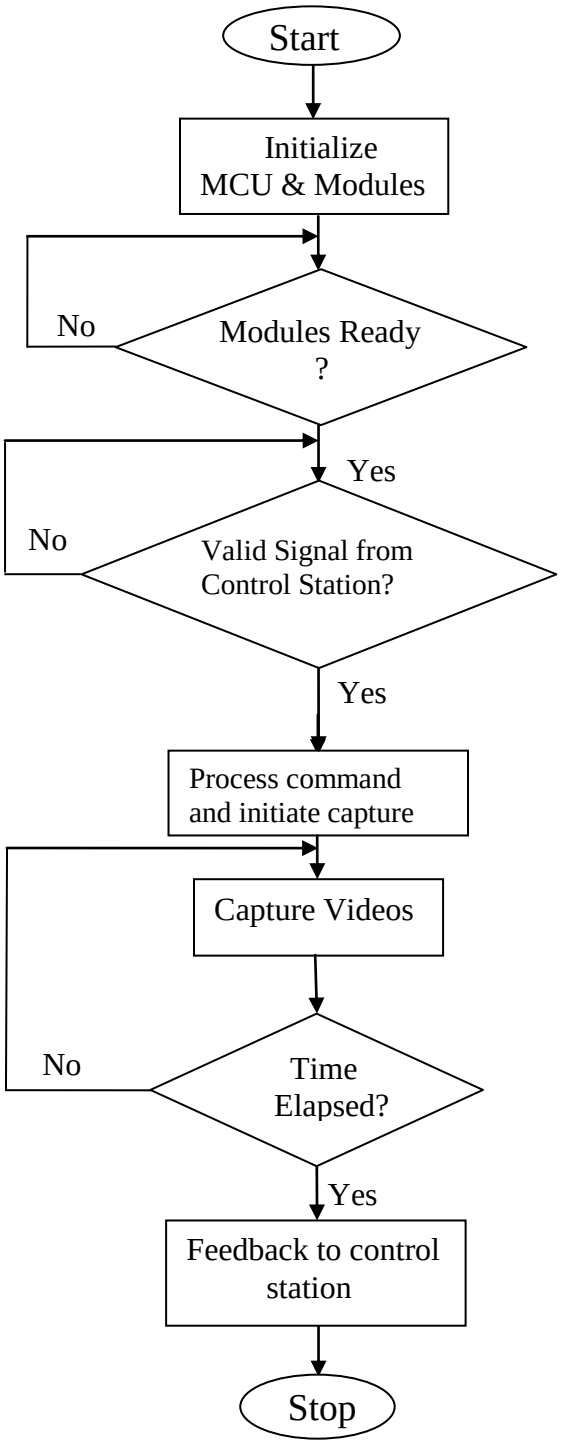


Figure 3.19: Client Station Operation Flowchart

3.18 Data Analysis

Major types of data involved were;

Location data: this includes the longitudinal and latitudinal coordinates of locations being monitored which were supplied by the GPS. Each location data was assigned a unique location number associated with the client's registered SIMM number. This actually refers to the client station GSM module number.

Client data: this includes fields such as phone number, name, address, camera identification number etc. relevant to the subscribers in client database (Table 3.1).

Event trace file: Refers to data extracted from the discrete event tool of Riverbed modeler which was used during the simulation. These were exported to Microsoft Excel worksheets and the data sets were plotted and analyzed to obtain results. (See Appendix E for the simulation datasets). The details of performance analysis of the network traffic will be discussed in chapter four.

3.18.1 Client Subscription Data/Module

In a global sense, the database of all the subscribers are stored in a database. This comprises all clients from all the continents of the world ; Africa (AFR), North America (NAM), South America (SAM),), Antarctica (ANT), Asia (ASI), Australia (AUS), and Europe(EUR).

The first record in the Geographical Zone (geog_zone) field of table 3.1 i.e. AFR_NG_EN_CS1 for example reflects that the client location is Africa in Nigeria , and in Enugu under Control Station1.

Table 3.1: Client Sample Database

Client_Name	Phone_No	Subscr_No	Geog_Zone	Ar-Code	Long.	Lat.	Cam_No.
Madona_Hosp	07056419866	00001	AFR_NG_EN_CS1	001	7316695	6273112	DVR1_CAM1
1st_Avesuites	07034213222	00002	AFR_NG_EN_CS1	001	7296970	6287485	DVR1_CAM2
Shoprite_Enu	08145667191	00003	AFR_NG_EN_CS1	001	7297492	6275486	DVR1_CAM3
Army_82div	08023421780	00004	AFR_NG_EN_CS1	001	7306470	6276981	DVR1_CAM4
Newline_Com	08064515115	00005	AFR_NG_EN_CS1	001	7310142	6291968	DVR1_CAM5
Nwokolo_Brt	08033224496	00006	AFR_NG_EN_CS1	001	7310030	6291963	DVR1_CAM6
Obiefuna_Ben	08199312212	00007	AFR_NG_EN_CS1	001	7311116	6291945	DVR1_CAM7

Relevant data about the clients such as the client's name, phone number, subscription number, area code, geographical zone, including longitude and latitude which are location data supplied by the GPS. The camera number enables one to identify each camera in the system at any time and is used in conjunction with the client's geographical zone to know which location to watch at any point in time.
The clients round the globe are grouped into seven (7) geographical zones by continent as shown in table 3.2.

Table 3.2: Continent Database

Continent	Continent_Area_Code
Africa (AFR)	01
North America (NAM)	02
South America (SAM)	03
Antarctica (ANT)	04
Asia (ASI)	05
Australia (AUS)	06
Europe(EUR)	07

From a global coverage point of view, each subscriber is associated with a continent, country, state, and control station.

Table 3.3: African Countries Database

Country	Country_Area_Code
Algeria	01
Angola	02
Benin	03
-	-
-	-
Zimbabwe	61

3.19 Business Model for On-Demand Real-Time Video Surveillance

The business model was developed using a prototype of the control station, and also a client station. As already stated, request for service are sent by clients to the control station either by phone call or by SMS.The prototype of the control (base) station was equipped with PIC18F4550 microcontroller module which provides for USB (Universal Serial Bus) interface to PC (Personal Computer). Client's location data were pre-stored in the EEPROM (Electrically Erasable Programmable Read Only Memory) of the microcontroller. The control station was connected to a PC via USB connection and a GUI (Graphical User Interface) application designed using VB.NET was used to manage the client data in the EEPROM (The VB.NET source code is found in Appendix H).

3.19.1 EEPROM Database Storage

The EEPROM of the PIC18F4550 microcontroller is usually made up of 256bytes of memory. Location number of clients with their corresponding phone numbers were stored in the EEPROM which could take 20 locations at the backend and about 18 locations at the front end. A mapping for the content of the EEPROM is represented in table 3.4.

Table 3.4: Client Database Storage map in EEPROM

Location	1	2	3	4	5	6	7	8	9	10	11
1	*	*	*	*	*	*	*	*	*	*	*
2	*	*	*	*	*	*	*	*	*	*	*
3	*	*	*	*	*	*	*	*	*	*	*
4	*	*	*	*	*	*	*	*	*	*	*
5	*	*	*	*	*	*	*	*	*	*	*
.	.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.	.
20	*	*	*	*	*	*	*	*	*	*	*

Clients location number which occupies one byte of space is stored in the first column, while the phone numbers (11 bytes) takes 11 columns to the right as shown in table 3.4.

The system was designed to allow for change of both base and client station numbers in case the need arises. These are flexibly updated at the control station via the GUI application. It is important to note that both the base and client station numbers occupy their own memory in the EEPROM.

3.19.2 Base Station Input Interface

The input interface enables one to edit client database via a PC terminal at the control station. The data is then processed and the results are used to activate surveillance camera procedure as discussed in chapter three. A GUI (Graphical User Interface) framework which connects the control station to the PC for customer database operations as shown in Fig.3.20 was designed using Visual Basic.NET.

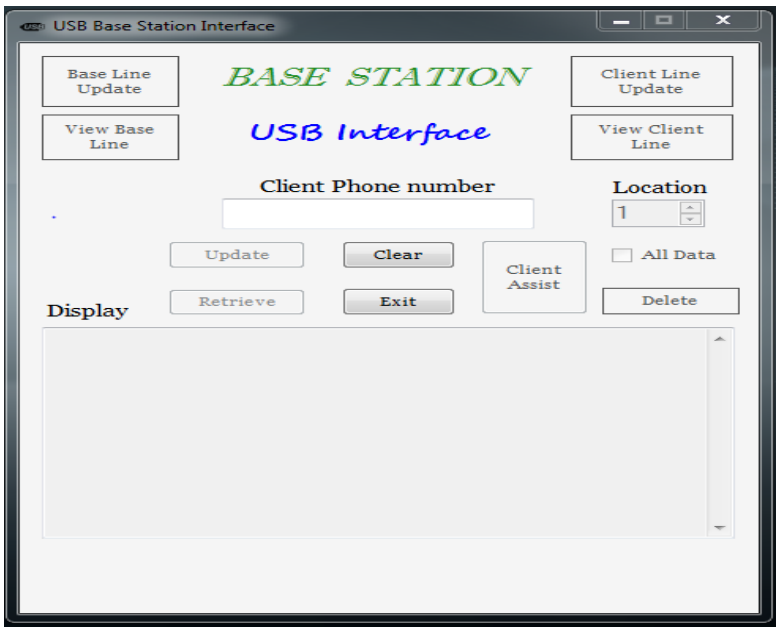


Figure 3.20: Base Station GUI for Client database

Client's subscription data are stored in the EEPROM (256 bytes) of the base station microcontroller with the corresponding location data. Clients data updates are carried out via the ***update*** button of the GUI (Fig. 3.20). Subscriber's data are called up via the ***Retrieve*** button when the client phone number must have been entered. If the '***All Data'*** box is checked before clicking the *retrieve* button, this causes all data in the

database to be displayed on the screen. The ***Location*** pointer points at the location of each subscriber, but when a client wishes to send request with unregistered phone number, the ***Client Assist*** button is used to manually send the clients request by a base station staff who must verify that he is a registered client. The ***Clear*** button when clicked clears all entries, while the ***Exit*** button enables one to quit the application.

3.19.3 Base Station Input Interface Testing

Communication was tested between the control station and the PC by connecting the control station to the USB port of the PC. When the based station is connected to the PC, the message "*Base Station Connected*" is displayed at the status bar of the base station GUI window and the relevant buttons become activated as shown in (Fig.3.21). The SIMM card of the base station can be changed and updated via the "Base Line Update" button if the need occasionally arises and clients must be notified accordingly. "*Client Line Update*" is used similarly in case of change of client location SIMM card.

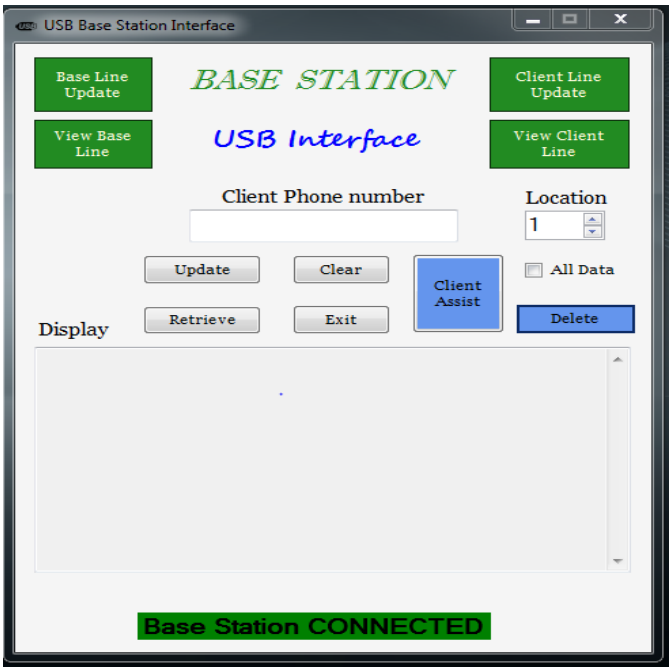


Figure 3.21: The Graphical User Interface of the base station connected to PC

A maximum of eleven integers are allowed at the client phone number field. The retrieve button calls up to the screen the entries at the database. Checking the "*All Data"* checkbox causes all entries in the database to be displayed on the screen.

For authentication purposes, the base station was designed to send the string "**CLX**" as prefix to client station number, so that client station recognizes such

calls as base station calls requesting for prompt surveillance video coverage, where X stands for client station location number.

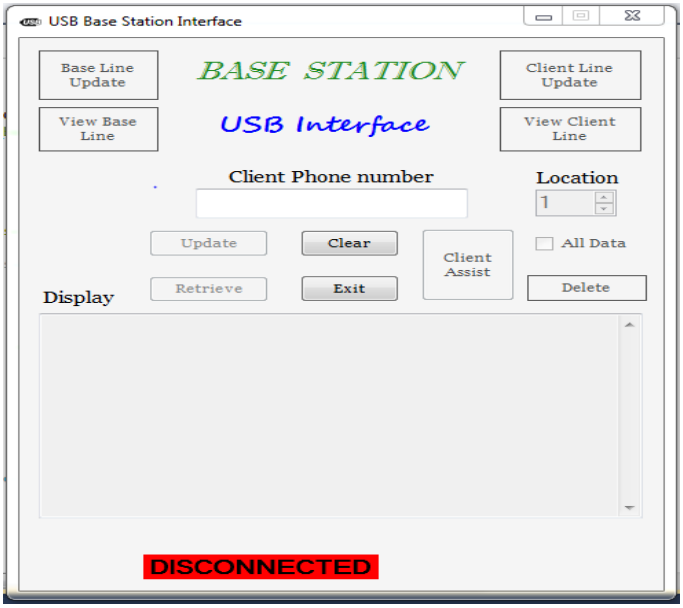


Figure 3.22: The Graphical User Interface of the base station disconnected from PC

When the base station USB connector is disconnected from the PC, the base station window displays 'DISCONNECTED' and the buttons are inactive as shown in Fig.3.22.

Figure 3.23: Control station connected to PC

A snapshot of the Control station prototype connected to PC is shown in Fig.3.23. The GUI window for the VB.Net application is displayed as soon as the application is launched as could be seen on the desktop.

3.19.4 Client Service Charge

A sample table for client service charge is shown in Table 3.5. Request for service from clients were categorized according to duration of request such that charges increase with duration.

Table 3.5: Client Service Charge Sample

REQUEST_CLASS	DURATION			AMOUNT	
	HOURS	MINS	SECS	US_D ($)	NAIRA (₦)
101A	0.25	15	900	30	9000
201B	0.50	30	1800	50	15000
301C	1.00	60	3600	70	21000
401D	2.00	120	7200	90	27000
501E	6.00	360	21600	110	33000
601F	12.00	720	43200	130	39000

3.19.5 Components of the Surveillance Service Tariff

A number of factors could be considered as constituents of the surveillance tariff which include but are not limited to:

Standing charges: these are fixed charges that are used to pay for the cost of the connection to the server and the equipment to monitor that customer's or service connection. They are usually charged on a monthly basis.

Surveillance charges: these charges are variable according to request for service duration and are used to pay for the upkeep of the equipment deployed to render video capture and route the data instantly to a secure remote storage location. However, the charges are per camera.

Storage costs: client's video feeds are stored for a default minimum duration after which the client either moves the video footage to his own server or request for extended storage duration at a fee.

The above component charges put together, gives the total surveillance charge. These are however, subject to amendment at any time with proper notification to subscribers

3.19.6 Client Station Output Interface

Surveillance video feeds stored in the cloud servers are used for predictive analytics. The stored information can be displayed to the user after a request is made by the user. The user can remotely view videos of interest captured by cameras connected to the user's network DVR from anywhere in real-time or otherwise using a PC or mobile phone from any location at any time. However, in order to carry out all forms of viewing, the network dvr, router, and the computer have to be set.

3.19.7 DVR Connections Using Monitor

A UK-Link cloud DVR model UK-8004 was typically used in this prototype. Video feeds captured by surveillance cameras could be locally viewed on a monitor (i.e. video display unit of a pc) by connecting the camera to the dvr via an AV (audio video) cable(Fig.3.24a) with BNC-to-AV connectors at the camera port and dvr port respectively. Alternatively, the dvr is connected to the camera using RG59 cable with each end terminated with a male BNC connector (Fig.3.24b and c). The VGA (video graphics array) port of the DVR is then connected to that of the monitor using a VGA-to-VGA (signal) cable.

Figure 3.24a: Audio Video Cable

Figure 3.24b: RG59 Cable terminated with BNC connectors

Figure 3.24c: BNC Connectors

The DVR is powered using a 12v DC output plug connected to the back panel of the DVR. The power supply plug is then connected to the outlet. On switching ON the Power button, the DVR beeps and the "Power" light is on and the system starts up. From the menu items which is displayed on right clicking the mouse, the default IP address of the DVR is viewed and noted from the network option. The setup Wizard is then used to configure the basic parameters, such as, device name, language, date

and time. A live control bar as shown in Fig.3.25 usually pops up when the mouse is right-clicked. The buttons on the bar points to the DVR settings. The hard drive of the DVR is formatted to save video files locally if desired.

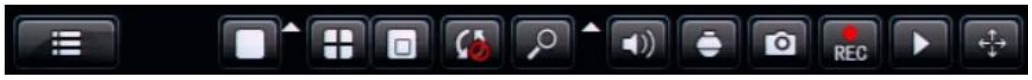


Figure 3.25: Live control bar

3.19.8 DVR Setup For Local Network View Using Laptop

The connection of DVR to laptop is similar to the connections to ordinary monitor via VGA ports as already described. However, a network DVR has a LAN (Local Area Network) port which the normal PC monitor does not have. The DVR can simply be accessed from the laptop by using a crossover cable to link the DVR to the laptop. The laptop IP address is configured to be in the same IP address range with the default IP address of the DVR. On typing the IP address of the DVR in the address bar of Internet Explorer (IE) browser, the DVR opens.

Another way of accessing the DVR is by using a router. In this case, the default IP address of the DVR is changed to the IP range of the router. The static IP address setting of the DVR must be changed to DHCP (Dynamic Host Communication Protocol) to enable the router dynamically assign a new IP address to the DVR. The DVR can then be accessed via Internet Explorer from the laptop.

In order to view the IP addresses of all the network items connected to the LAN, one could download, install and run an IP scanner software which detects and displays the IP addresses of all network devices in the LAN.

Access to surveillance videos via DVR from the pc is alternatively made through a central monitoring station software called *CMSclient* which comes with the DVR software package.

3.19.9 DDNS Setup for New DVR.

In general, configurations for DDNS online for a series of new UK Link DVR including UK-8004 which was typically used to setup this prototype can be handled in two main parts – one part is for ***setting*** while the other is for ***viewing.***

Settings are done for the DVR, the router and the computer one after the other.

3.19.10 DVR Settings

Setting the DVR involves setting a static IP address, ports, and DDNS for the DVR as follows;

Open the DVR and connect all wires (which include USB mouse, LAN cable, BNC, VGA).

The next step is to Set the ports and LAN IP as follows;

Open the Main Menu

Select ‘Advanced Setting’→Network (Fig. 3.26)

When the Network menu opens,;

Set the “Web Port” as “88”
Set the “Media Port” as “89”
Set “Network Type” as “STATIC”

Figure 3.26: Advanced Setting window

Set “IP Address”as: 192.168.1.88
Set “Subnet Mask”as: 255.255.255.0
Set “Gateway”as: 192.168.1.1
Set “Preferred DNS Server”as: 8.8.8.8
Set “AlternateDNS Server”as: 8.8.4.4 (also you can leave it as default)
Click “Apply” as shown in Fig. 3.27.

Figure 3.27: Network settings

3.19.11 Setting DDNS for DVR

The steps to setup free DDNS for DVR are as follows;

Go to ‘Main Menu’

Click Advanced Setting→DDNS”, enable the DDNS function, then select “leadingdvr.com” in the “DDNS Type”. Click “Apply” (Fig. 3.28).

The outlined steps enables one to obtain a free DDNS.

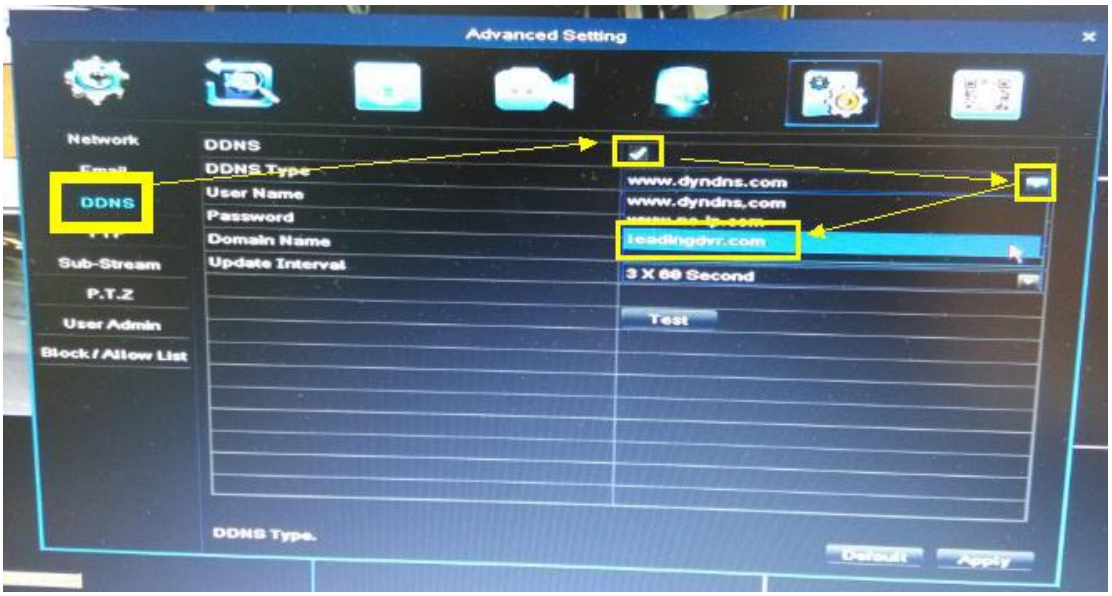


Figure 3.28: DDNS Setting

The next step is to set the username and password so that one would be able to log in from a remote location. While still in the Advanced Setting window, set username and password as shown in Fig. 3.29.

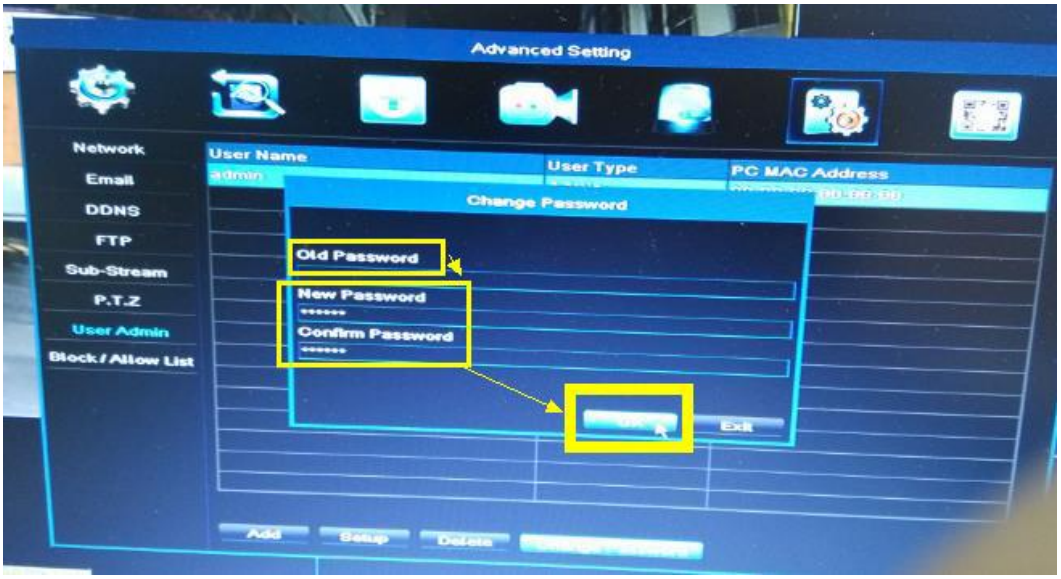


Figure 3.29.: Username and Password Setting

Now we are done with settings for the DVR and that of the router comes next.

3.19.12 Router Settings

In order to access the router, open IE browser and type "192.168.1.1" in the address bar. Go to "Forwarding→Virtual Servers→Add New" (Fig.3.30).

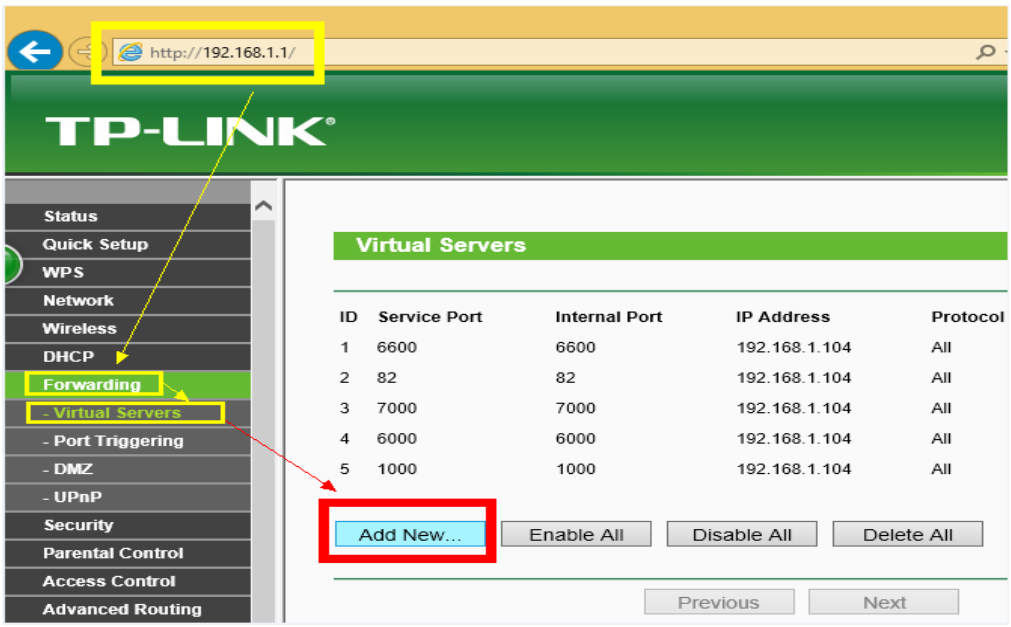


Figure 3.30: Port Forwarding window

Add port “88”in “Service Port”, put “192.168.1.88”in “IP Address”, select “All”in “Protocol”, then click “Save” (Fig. 3.31).

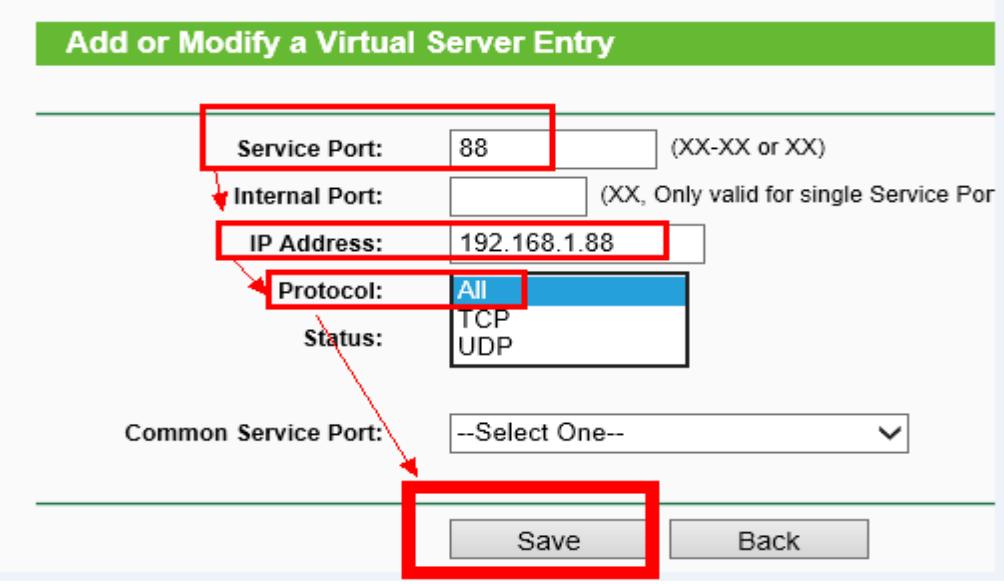


Figure 3.31: Add or Modify virtual server entry

Same way to forward port “89” to “192.168.1.88” (Fig. 3.32).

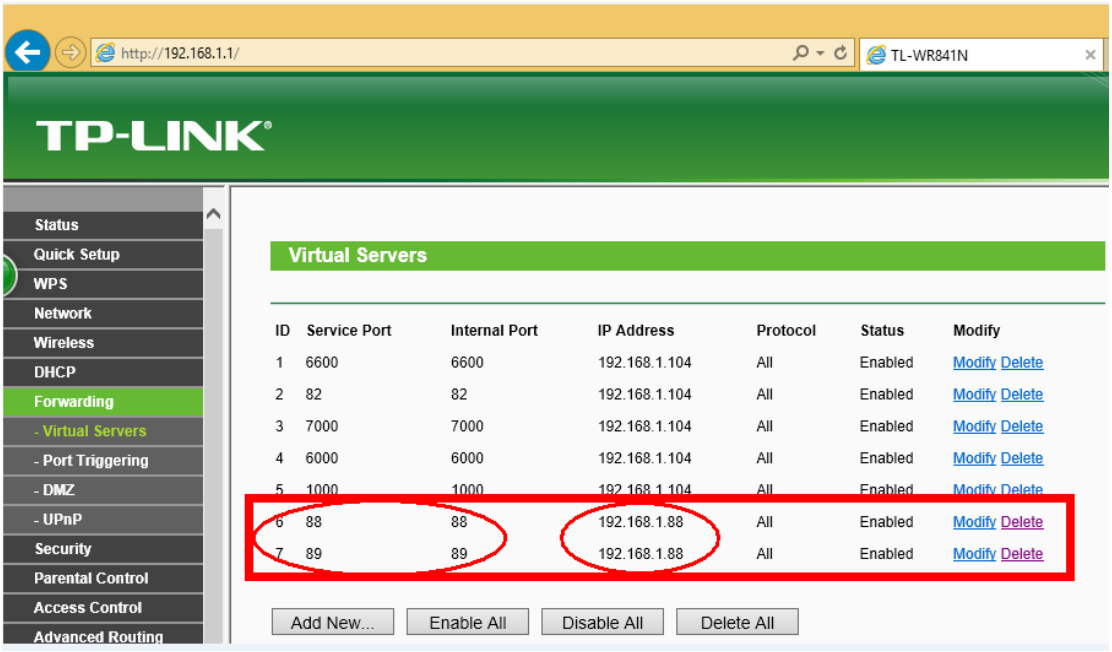


Figure 3.32: Forwarded ports 88 and 89 window

Now we have finished all configurations on DVR and router. The next step is to set the computer by installing the required plug-in.

3.19.13 Computer Setting

Computer setting involves installing the Computer Plug-in

In order to install the plug-in for computer, Open IE browser, type http://192.18.1.88 in the address bar to visit the DVR. Tips from the DVR requesting to install the plug-in would appear. Just download and install it.

After installing the plug-in, one could start viewing the DVR on Local network, on remote computer and remote mobile (Android/iPhone).

3.19.14 Local Network Viewing

In order to view the video feeds of surveillance cameras connected to a 4 Channel UKLINK DVR model 8004 which was essentially used in this prototype, the following steps were taken;

Install CMSclient

Launch the CMSclient software to see login window appear as shown in Fig.3.33.

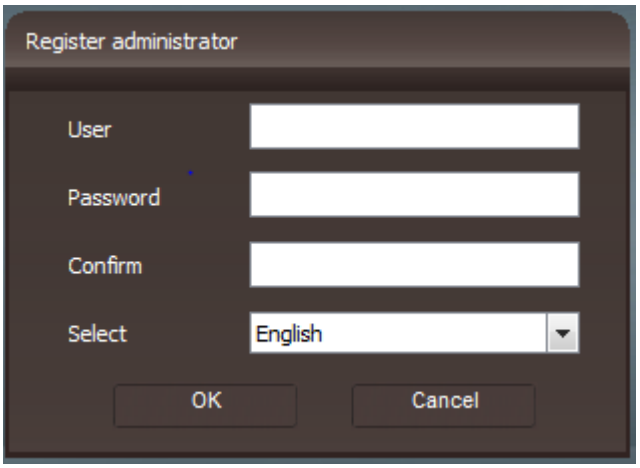


Figure 3.33: CMSclient LOGIN window

Log in using username and password.

The default username is admin and the default password is 00000000 (i.e eight zeros). One can always change the username and password of choice such that could be easily remembered.

Cick **login** to see a device list window appear.

Right click on *Device List* to add device in an *Add Device* window (Fig.3.34) which appears.

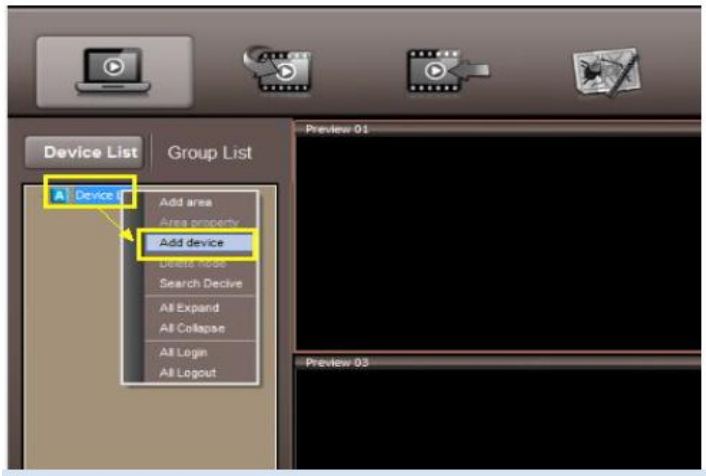


Figure 3.34: Device List window

On clicking Add Device , the Device Property window (Fig.3.35) opens.

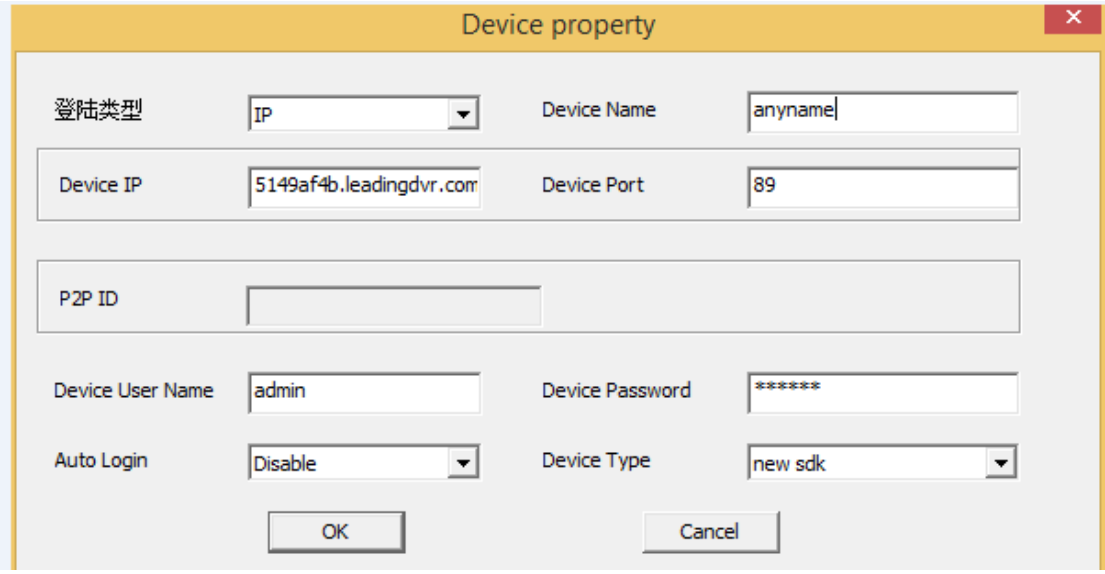


Figure 3.35 ： Device Property window

Select P2P as login type.

Put the device name eg. Mydvr or the IP address of the DVR.

Put in the value for the P2P ID (This is copied exactly as it is with case sensitivity considered).

Enable either manual or auto login and begin to view the videos.

3.19.15 Remote Viewing

In order to view the DVR from Android mobile phone, one has to take the following steps;

- Install VIDEODEFENCEV2 from Google playstore in the Android phone
- After installation, launch the application
- Click device
- Click the + icon to open device info
- Type-in device name e.g. mydvr or any name of your choice
- Put username and password i.e *admin* and 00000000 (eight zeros) respectively.
- Scroll back up the screen and click register type
- Select QR code. Scan the code by aligning the QR code within the frame and clicking the code

When the code is captured, click Done.

The UID is captured and displayed .

- Click the leftmost top icon to see a window display Live, Device, Image, Remote, Local, Push Setting

Click Live to see channels window as shown in Fig. 3.36a. The Live videos then appear as shown in Fig.3.36b

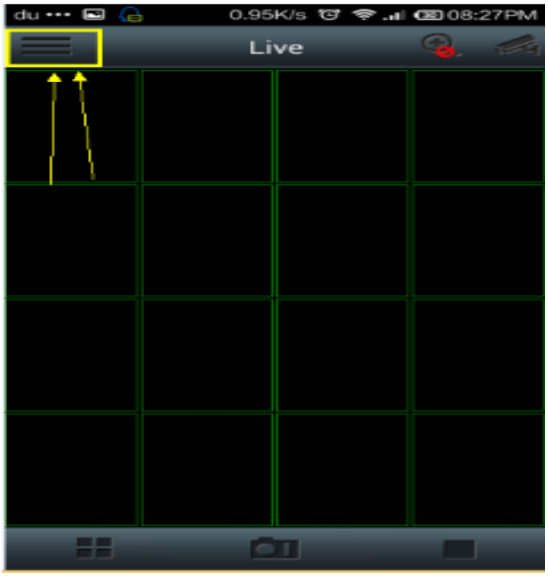


Figure 3.36a: Channels Window

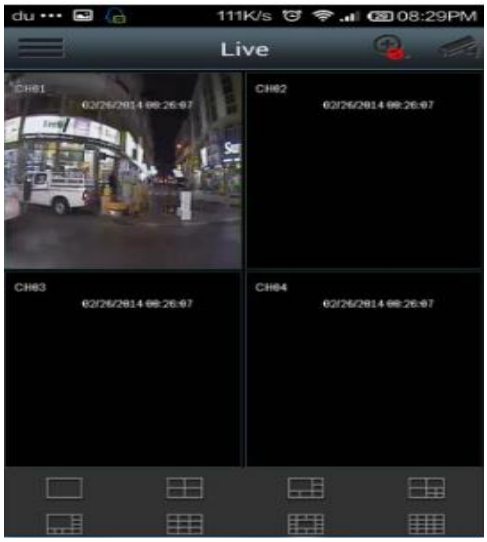


Figure 3.36b: Remote view of videos

On the top right corner of the screen, click the camera icon

Mydvr icon is immediately displayed showing the UID.

Check the box by the top right corner of the screen and click *Start Preview*

This displays the video feeds of the cameras connected to the DVR as shown in Fig. 3.36b.

3.20 System Flowchart For On-Demand Cloud-Based Real-Time Remote Security Video Sensing System

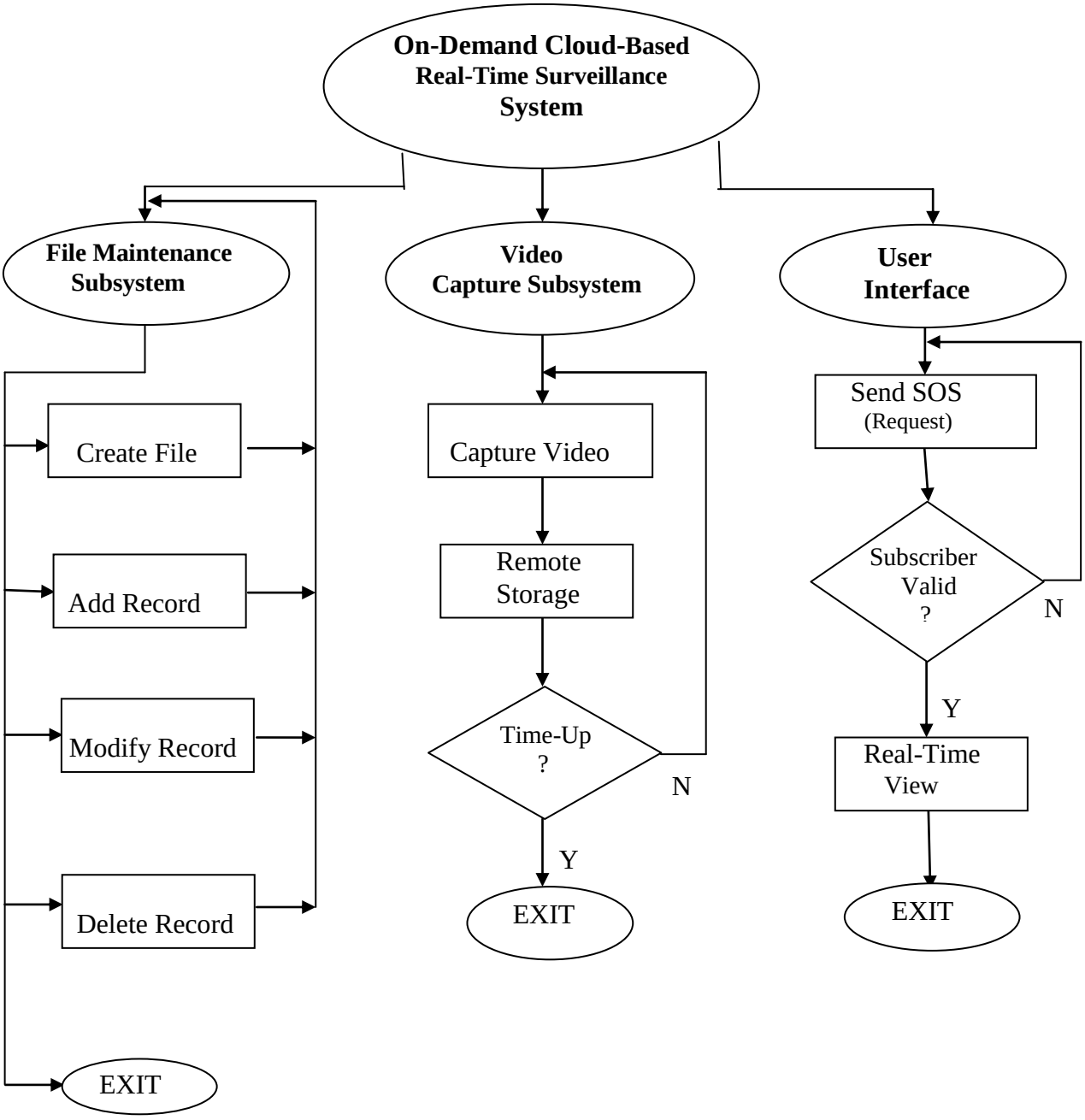


Figure 3.37: OD-RGRSVS system flowchart

A flowchart of the entire system depicting the operations of the subsystems that constitute the OD-RGRSVS is shown in Fig.3.37. It is composed of; the *file maintenance* subsystem which is handled at the base station for client data manipulation, the *video capture* subsystem which takes care of the real-time surveillance action with remote storage, and the user interface which enables users to send request for surveillance service and access the video from anywhere.

3.21 Choice of Programming Language

A number of programming and scripting languages were utilized in carrying out this work. They include; embedded C-language in MPLAB Integrated Development Environment (IDE), and VisualBasic.NET.

Micro coding for PIC 18F4550 and 18F4520 MCUs which were used in the control station and client's station respectively was carried out in embedded C-Language with MPLAB IDE as the source code editor using microchip C18 compiler. PIC kit2v2.6 by Microchip was used to drive the PIC programming device. A graphical user interface (GUI) for PC connection to the control station was developed using Visual Basic.NET (VB.NET).

3.21.1 MPLAB Integrated Development Environment (IDE)

MPLAB IDE is a Windows based Operating System (OS) software that runs on a PC to develop applications for Microchip microcontrollers and digital signal controllers. It is called an Integrated Development Environment, or IDE, because it provides a single integrated "environment" to develop code for embedded microcontrollers.

MPLAB IDE is designed to work with many Microchip and third party language tools. These tools take your application code (written in assembly, C or BASIC language) and turn it into executable code that may be programmed on your selected Microchip device.

Two major features of MPLAB IDE are; projects and workspaces. A project contains the files needed to build an application (source code, linker script files, etc.) along with their associations to various build tools and build options, while a contains information on the selected device, debug tool and/or programmer, open windows and their location and other IDE configuration settings. The best way to set up a project and its associated workspace is by using the Project Wizard. This will set up one project in one workspace.

To set up more advanced applications, the project and workspace could be set up manually. You can take advantage of the workspace setup and open multiple projects in one workspace. Also, you can tailor each project in a multiple-project workspace to create one part of a larger application (concurrent projects). MPLAB IDE supports the use of numerous assemblers and compilers for building code in several

programming languages. Microchip provides free assemblers and linkers for PIC MCU and dsPIC DSC(Digital Signal Controller) devices, as well as compilers (free student/academic/demo editions and for-purchase full versions). Third parties provide additional coverage with language tools for assembly, C and BASIC languages. It contains additional features to aid in code debugging and general support.

PIC programming device was used in writing codes to the microcontroller, driven *by* PICkit 2 Programmer Software ***v2.****61* by Microchip**.** This tool enables one to select the proper device family and carry out read, write, erase and other relevant operations such as importation of hex files.

3.22 System Modeling and Simulation Using Riverbed Modeler

This section focuses on the implementation and validation of the OD-RGRSVS involving simulation with Riverbed Modeler 17.5 for the network performance analysis. First, the system assumptions and specifications will be outlined. Consequently, a step by step procedure will be highlighted to show the results from the test bed setup with the Riverbed Modeler 17.5 whose home screen shot is shown in Fig.3.38.

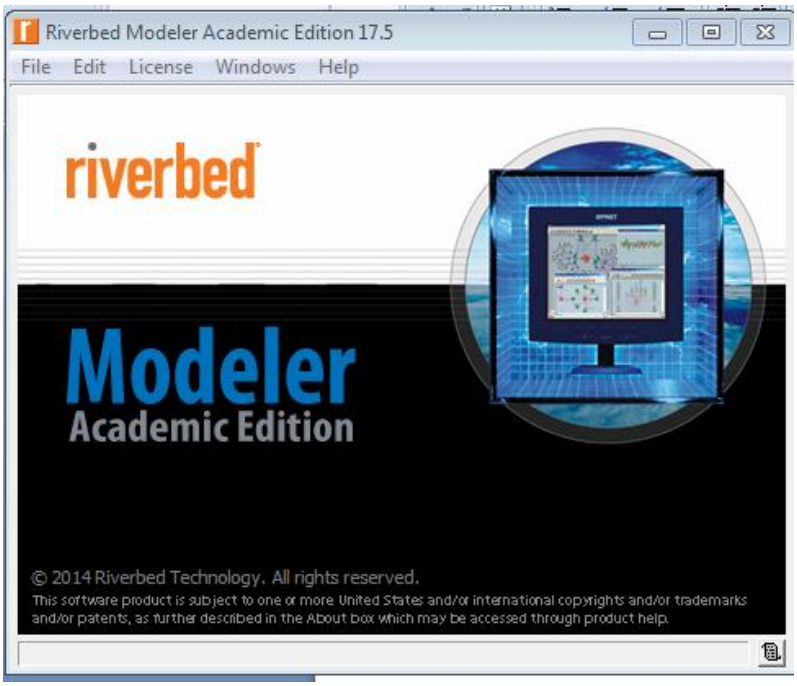


Figure 3.38: Riverbed Modeler 17.5 home page

3.22.1 Software Requirements

The requirements to run the proposed system for optimal performance are listed below and any computer that meets these requirements can install the system without any problem;

- Microsoft windows vista or windows7 while using Linux Redhat for production deployment.
- Apache server version 1.3.14 & above
- PHP version 4.1.0
- MYSQL version 4.1.0
- All browser compatible

  Operating system requirements;
- Adequate temporary space for paginations to virtual memory
- 64-bit and 32-bit compatible
- Windows 7/Server 2007 and Linux Redhart.

3.22.2 Hardware Requirements

The minimum hardware requirements include:

- Server Monitor
- 4GHz Processor
- 4GB of RAM
- 1TB of available hard-disk space
- 1.5 GB of swap space
- 400 MB of disk space in the /tmp directory

3.23 Implementation Framework/Cloud Server Creation

The following steps were used to set up a Cloud Server through the Cloud Control Panel interface.

1. Log in to the Cloud Control Panel. The Cloud Servers list opens by default.
2. Click the **Create Server** button.
3. In the **Details** section, enter a name for your server in the **Server Name** field (Fig. 3.39).

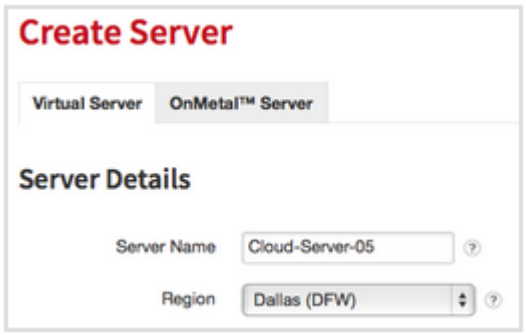


Figure 3.39: Cloud server creation

4. From the Region list, select the region in which you want to create the server.
5. In the **Image** section, select which operating system to use as shown in Fig.3.40.

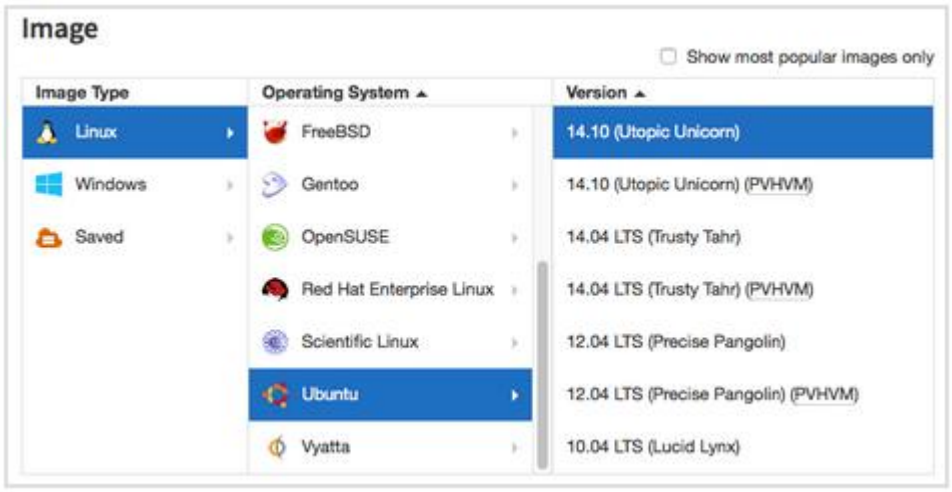


Figure 3.40: Server OS selection

6. In the Flavor section, choose the appropriate configuration for the server as shown in Fig. 3.41

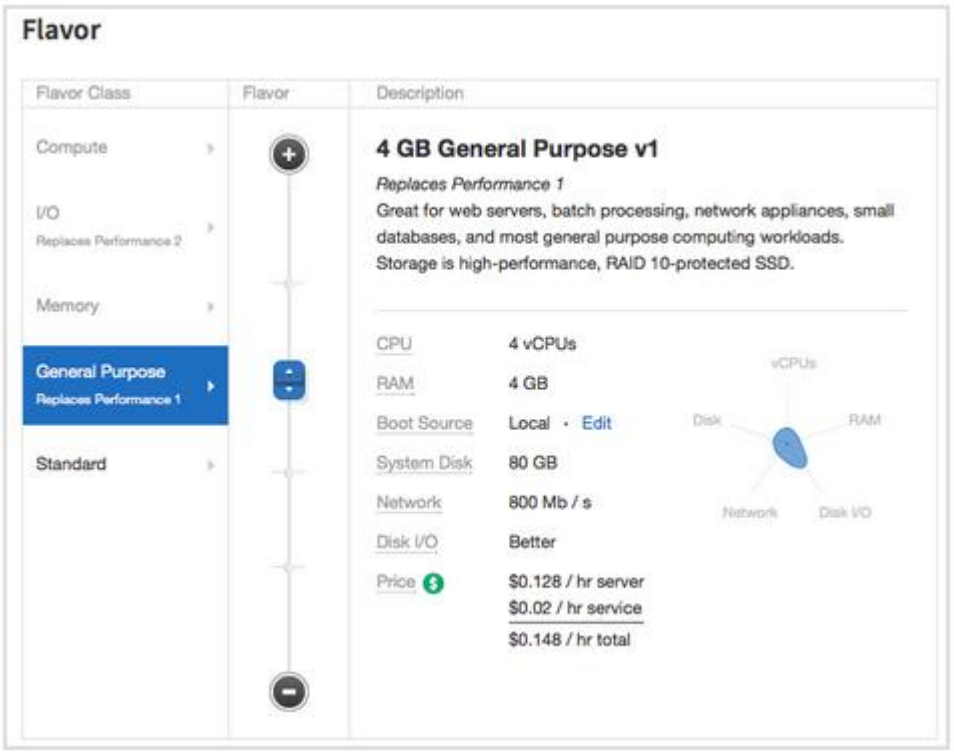


Figure 3.41: Server Image Creation

7. Optionally assign a public key to the server by selecting an existing key as shown in Fig. 3.42.

- To assign an existing public key, under Advanced Options, select a public key from the drop down list.

Figure 3.42: Public key assignment

- Select the public key from the list and continue with the next step.

8. To add a new public key, click Manage SSH Keys (*SSH stands for* Secure Shell *which is a cryptographic network protocol that provides administrators with a secure way to access a remote computer*) and perform the following steps:
    1. On the SSH Keys page, click Add Public Key
    2. If you are adding a public key, give your new public key a name.

3. In the Region field, confirm or select the region in which the key will be used.
4. Paste the public key into the Public Key field.
5. Once the Key Name, Region, and the Public Key are entered, click Add Public Key. as shown in Fig. 3.43

Figure 3.43: Add public key

6. Confirm that the key is listed in the SSH Key list for your new server.
7. As needed, create a new network and select the PublicNet and ServiceNet options.
8. Click Create Server. This can then be used to store the surveillance images remotely from smart devices.

At this stage, the server is built. After it is provisioned, the server displays the status running and is now available for remote connection. Specific remote connection instructions for server are displayed on the side bar located at the right of the Cloud Control Panel.

3.24 Simulation Platform.

All the simulations were run on a Del Inspiron 1464, Intel ® Core ™, i5 CPU, 2.4GHz with 4G RAM under a Microsoft Windows 7 ultimate edition environment. On this platform, all the experiments were implemented in Riverbed IDE. As shown in Fig. 3.44, ten (10) IP surveillance cameras were linked to NVR integrated switch board. The On-demand traffic was linked with the network gateway which also backup captured snapshots before storing them in the remote server clusters. The network expands and extends the capability of video surveillance gateways (enhanced

encoders and decoders) and the NVR, which allows the matrix switch to be replaced by standard and typically lower-cost Ethernet switching platforms. In the design, the request inter-arrival time follows an exponential distribution. The service rate also follows exponential distribution, and the service rate mean is maintained.

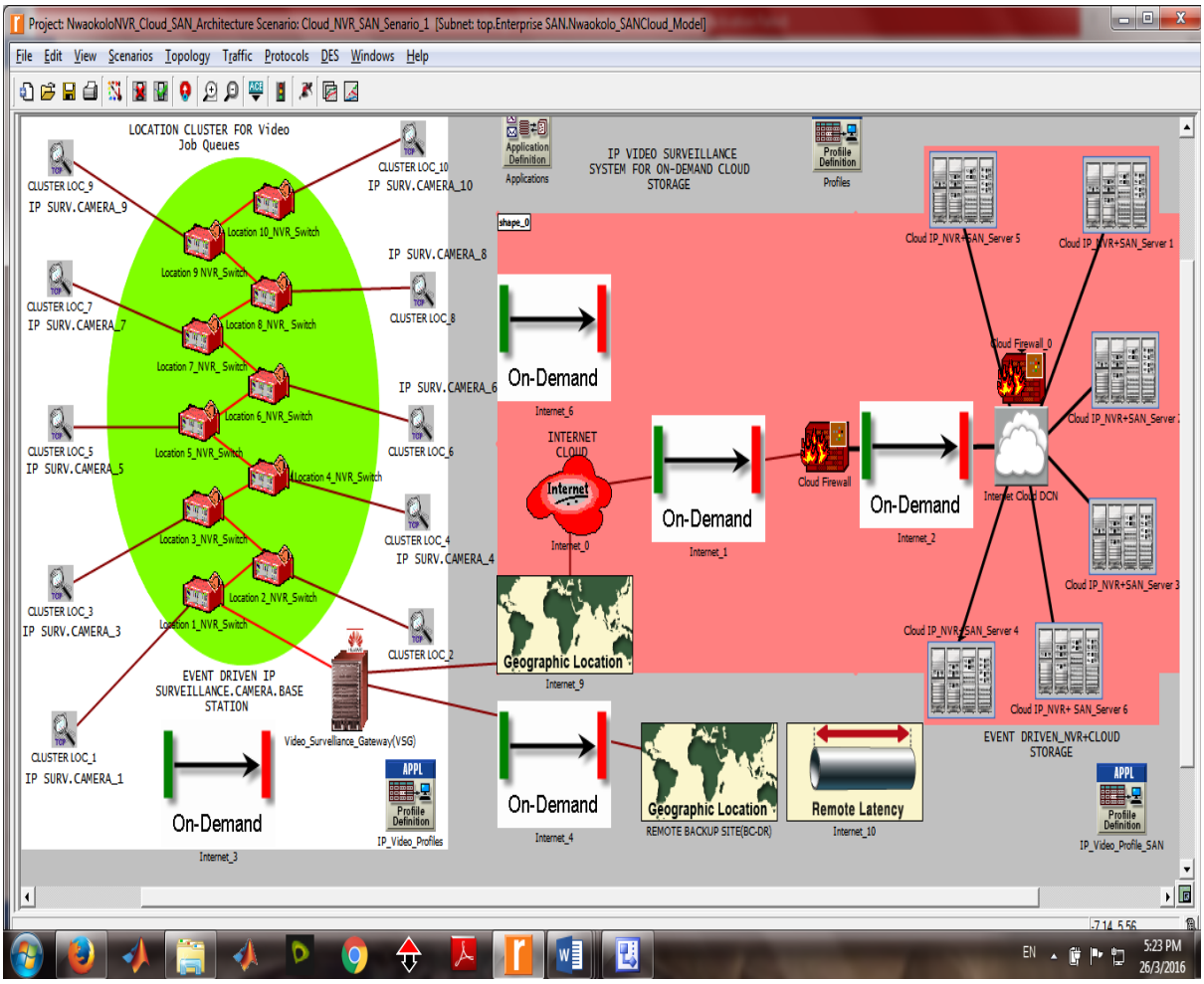


Figure 3.44: OD-RGRSVS Implementation Testbed

From the system test bed shown in Fig.3.44, the NVR supports a web browser-based graphical user interface and is complemented with video transcoding capabilities. This makes the video surveillance monitoring and viewing highly flexible.

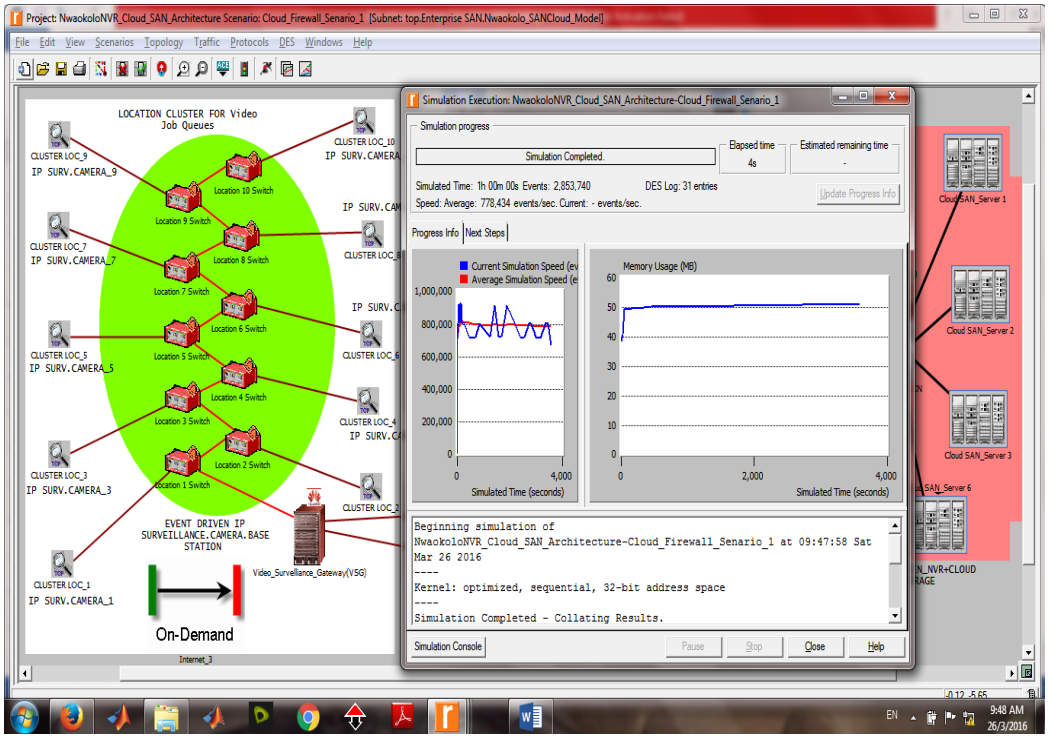


Figure 3.45: OD-RGRSVS Test Mode

Figure 3.45 shows the OD-RGRSVS test mode where the discrete event trigger traffic was configured and executed for test verifications. The trace file compilation window is shown depicting the current thread and the average simulation threads as well as the memory usage. This has implication on the accuracy of the expected result, so a careful adjustment was made to accommodate simulation hardware. Successful test mode results show the workability of the system in a live scenario.

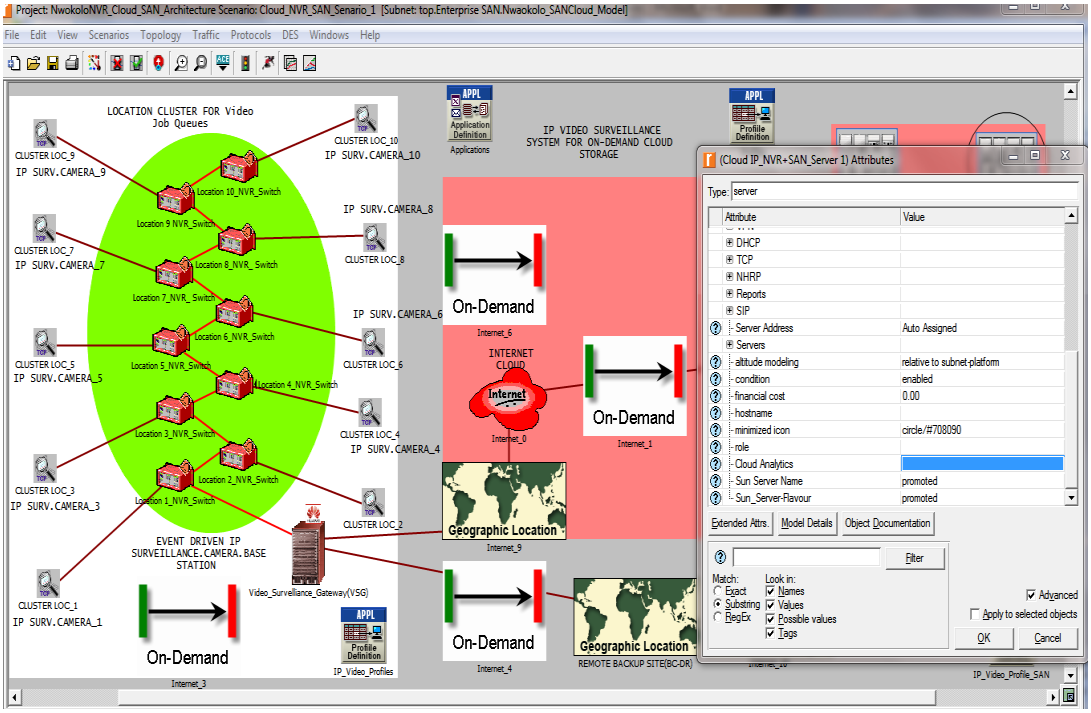


Figure 3.46: Cloud Analytics configuration for On-Demand Storage (Secondary Backup)

Server attributes which are secondary backup configurations are setup in this scenario (Fig.3.46) for cloud analytics. The cloud IP_NVR SAN server attribute window is shown where the cloud analytics and the virtualization capabilities previously highlighted were configured. All the computing entities for a good server workload optimization are managed via this interface window. The implication of this backend design is that the server services fabric enables consolidation of services onto its common storage platform. This can be deployed on hardware, on software in the cloud environment. This reduces operational overhead by standardizing management as well as enabling deployment processes that support continuous delivery efforts, (i.e., sustained service rates). By sharing compute service resources and leveraging fine-grained multi-tenancy of the cloud zone, the cost of individual services is dramatically reduced, enabling the application interface to take advantage of services that are beneficial to their security, reliability, and performance.

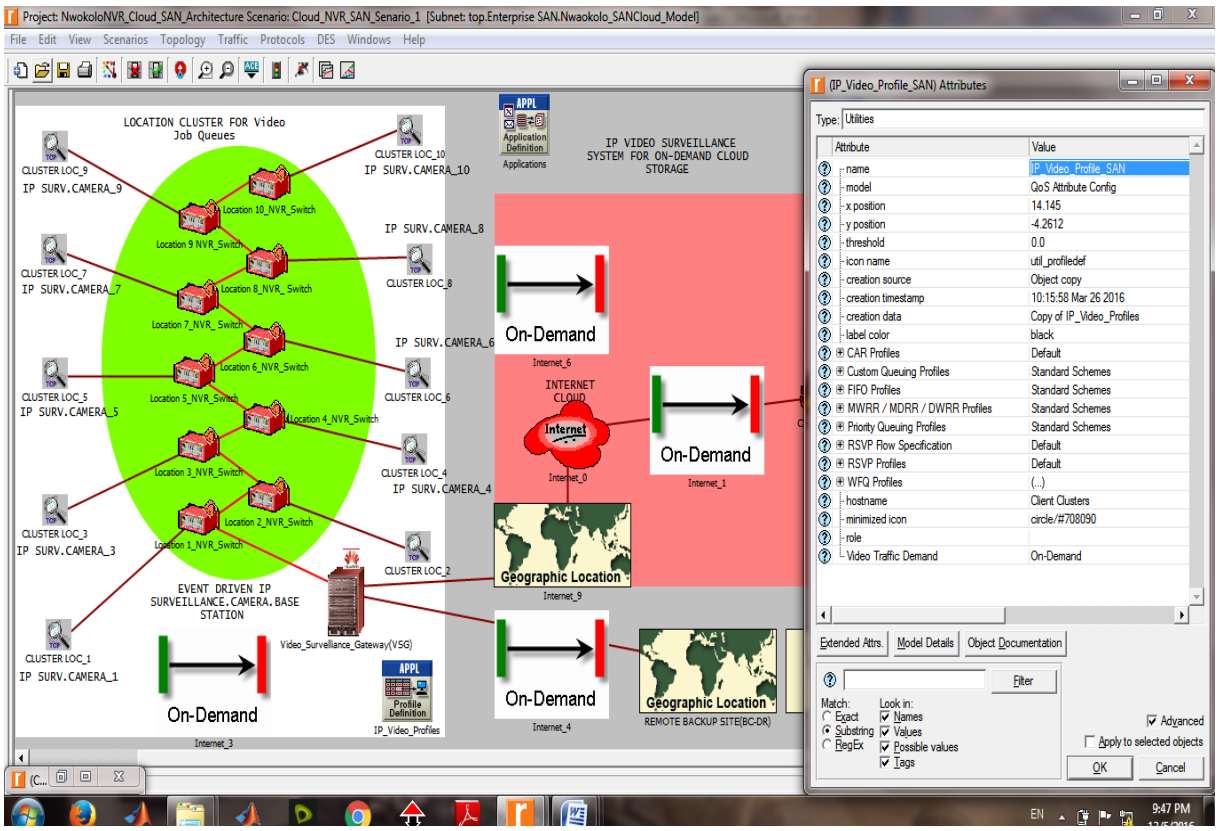


Figure 3.47: Cloud queuing configuration policies for on-demand storage (secondary backup)

Fig.3.47 is a scenario for cloud queuing configuration to keep track of sources of camera footage, time, and traffic demand. This hybrid infrastructure approach, including cloud resources, for IoT deployments not only allows service providers to distribute their IoT applications and services when it makes sense, but also provides global fault tolerance to the overall system. Depending on how the disaster recovery infrastructure is designed, this can be an active site, a hot standby, a leased hosting space, a cloud provider, or some other contained compute location. As soon as that IoT server, application, or even location starts to have trouble, a service provider can seamlessly maneuver around the issue and continue to deliver its services to the devices.

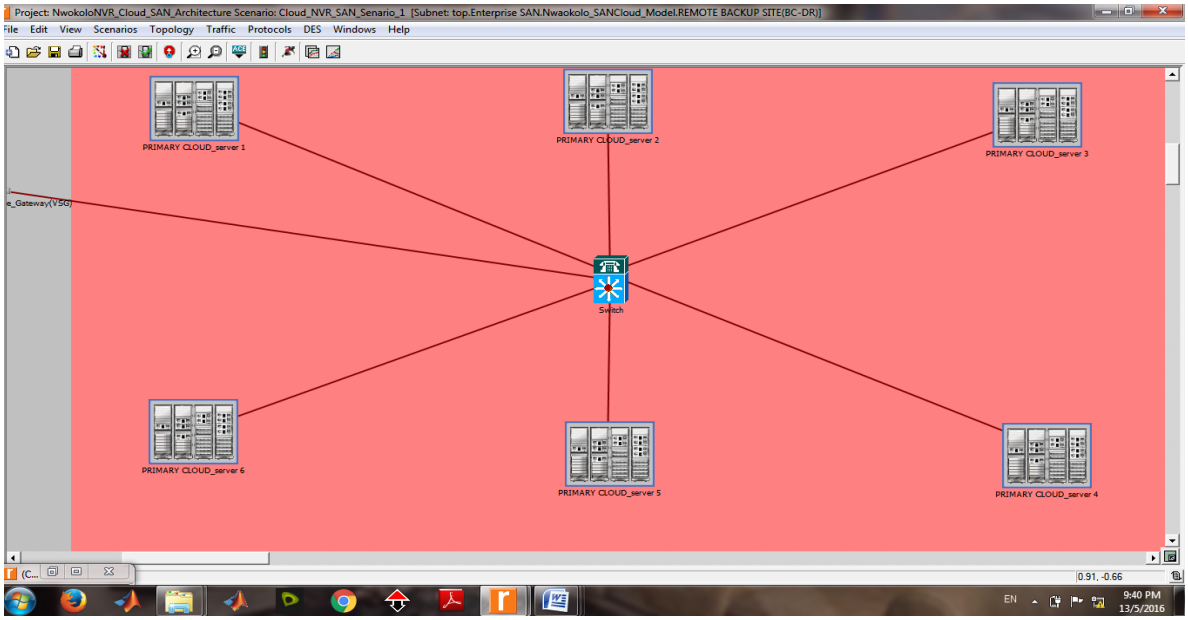


Figure 3.48: Cloud On-Demand Storage (primary Backup)

Figure 3.48 shows the cloud On-Demand storage designated as the primary backup. This is very vital since availability is paramount objective. The individual primary server interfaces with the NVR which supports web-browser-based graphical user interface that complements video transcoding capabilities and video surveillance monitoring. The simulation runs were concluded using six (6) primary cloud servers managed by network switch linked to a video surveillance gateway.

3.25 Optimization Algorithm for OD-RGRSVS

(1) **Input**: IP Surveillance request list, NVR_calls, server cluster list

(2) **Output**: server number; process jobs &store

(3) ***For*** server in server cluster list ***DO***

(4) (t) = getvalue(snapshot arrival number)

(5) Lq = getvalue$L$ (Store in NVR)

Post (surveillance gateway filter)
Compute Traffic payload T_p

(6) ***End***

(7) ***For*** server in backup server list ***DO***

(8) Function value = distribute Traffic payload T_p
Traffic payload T_p

(9) ***End***

(10) Scheduler schedules the request to the selected load balance & Firewall;

(11) Server Scheduler schedules the request to the selected server

(12) Get the index of the first function value

(13) Process job task and enforce Active storage

(14) Schedule for predictive analytics.

(15) ***End***

In the optimization algorithm of section 3.25, the input captures are read and processed while executing storage of captured snapshots. The algorithm is further expanded using the flowchart in Fig. 3.49.

The flowchart depicts the on-demand video surveillance behaviour. The location cluster is first initialized with event arrival = zero. As soon as event arrival occurs, the IP network video recorder engine is invoked to take video surveillance record routed to IP gateway with firewall and load balancing features. The system then checks for validity of the location cluster. If cluster is not valid, control is transferred back to location cluster initialization, but if valid, captures and stores redundant image copy, sets the IP cloud and the virtual machine servers with proper configurations. Surveillance traffic data is processed, structured and stored in readiness for big data analytics which yields resultant data that are harnessed for decision routine.

3.25.1 Behavioral Flowchart for OD-RGRSVS Simulated Model

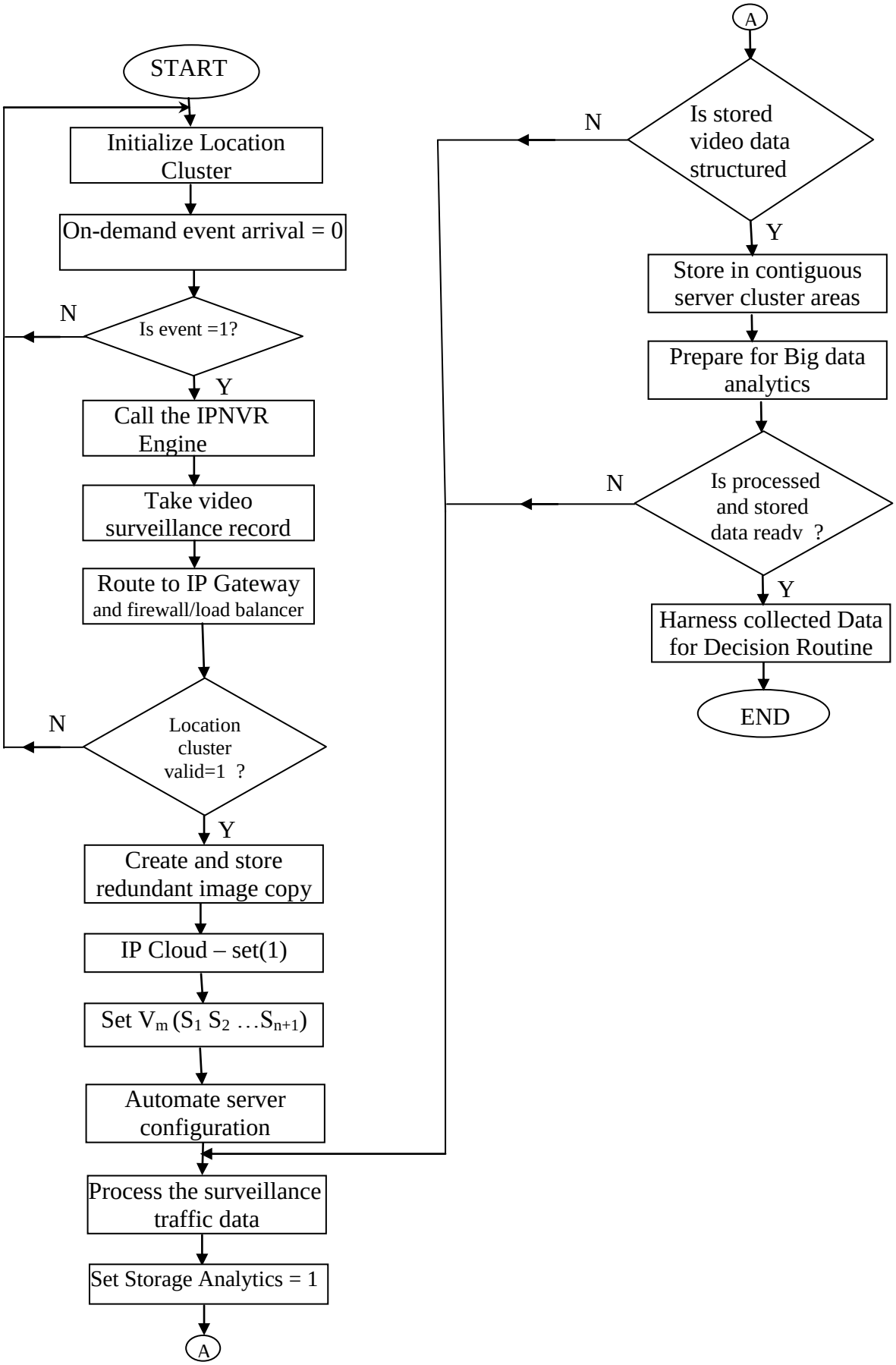


Figure 3.49: OD-RGRSVS Behavioral Flowchart

CHAPTER FOUR

RESULTS AND DISCUSSION

4.1 System Performance Analysis

This section presents a detailed performance analysis of the network traffic. After implementing Fig. 3.44, an optimization method known as Priority Queue of synthesis was leveraged on. In order to compare and analyze the performance of optimization strategy, two distinct procedures were applied in the primary and secondary server clusters for the storage of the image snapshots. First, the classical Priority Queue of shorter service time first (SSTF) was used as the test metric. On the other hand, the First-In, First Out (FIFO) queuing policy was used. The Priority Queue block used in the first case to implement queuing policies was a fair optimization strategy. The influence of On-demand surveillance computing on QoS using some selected metrics from the event driven engine such as on-demand latency, throughput and resource utilization are briefly analyzed below.

4.1.1 On-Demand Latency Behaviour

The latency profiles of both the primary and secondary storage are shown in Fig.4.1. Owing to closeness of the primary storage domain to the NVR surveillance cameras, it took smaller time frame to process and store the captured event. The primary backup took about 0.002secs while the secondary backup took about 0.01secs delay, which characterises a state-of-the-art high speed network with latency far less than 1 second.

Technically, frame rate (which refers to the number of frames per second (fps)) is a measure of latency from one frame to the next. This implies that the higher the frame rate, the lower the frame latency, and vice versa. It is important to note that this frame rate setting is client-side. Actually, the higher the frame rate, the more accurately one would be able to see things on the screen. However, there are trade-offs because higher frame rates demands more storage pixels. Moreover, excessive frame rate settings could cause a computer system to overheat or display blue screen.

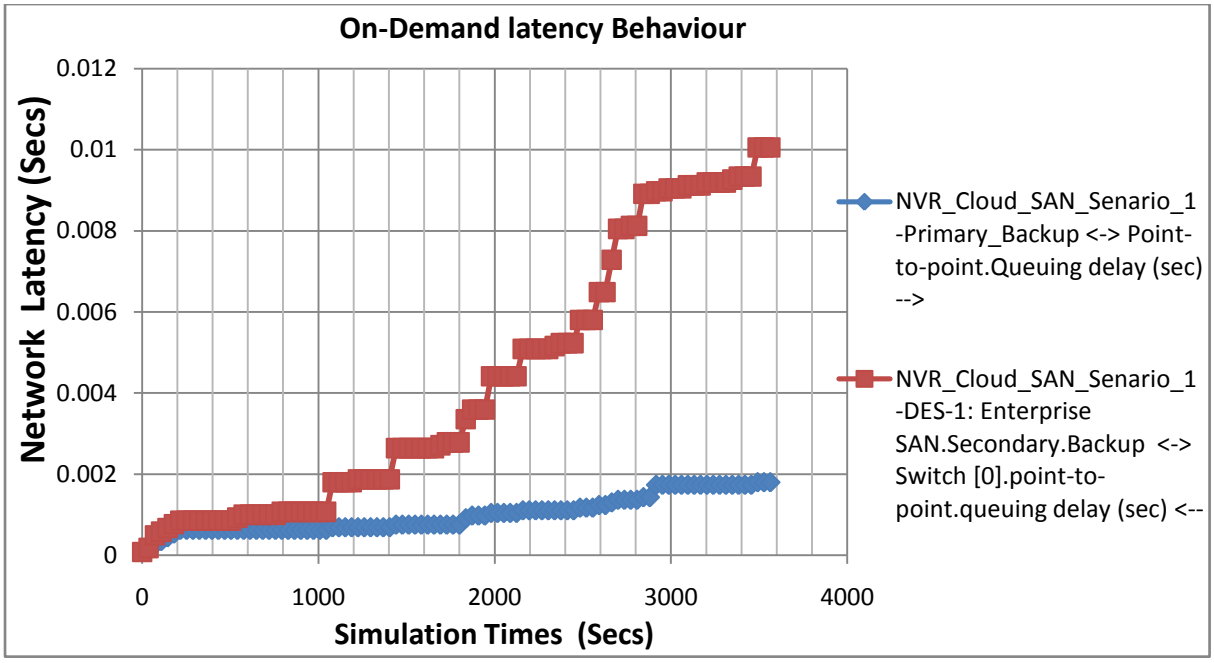


Figure 4.1: On-demand Latency profile

Most video analytics vendors suggest the optimal frame rate for current captures should not be more than 15 fps. CCTV Camera Pros which is a US veteran owned business that was founded in the year 2006 by Greg Bond and Mike Haldas, for example, recommends 7.5 fps - 15 fps as the most popular range of recording frame rate used in video surveillance systems. However, frame rate above 15 frames per second could be excessive and would lead to higher overall network latency value at the expense of satisfactory QoS. There is also very little difference in the movement of an object between frames sent and analysed every 1/15 of second compared to that of every 1/30 of a second.

4.1.2 On-demand Throughput Behavior

A literal throughput trend in the network being discussed is illustrated in Fig. 4.2. The network offers an increased reliability, higher system availability, greater utility (any camera to any monitoring or recording device for any application, anywhere), increased accessibility and mobility, and the ability to enhance other building management system capabilities through improved interoperability. An elastic curve starting from 40packets/sec was observed which grew to a stable state at 100 packets/sec. With the network, a common format for video and control signals that is transmitted across the IP network also provides the ability to add new functions such as video analytics anywhere in the network. This Video analytics offer the ability to

automatically monitor surveillance video for violations (that is, package left alone, presence after building closure, going in the wrong direction). Therefore, it is a tool for prevention and early detection. No matter where this function is deemed best to run; whether at the edge of the network, embedded in the camera, in the encoder, or centralized in monitoring centre. A common format enables the same video analytics program to be used or varied based on specific circumstances.

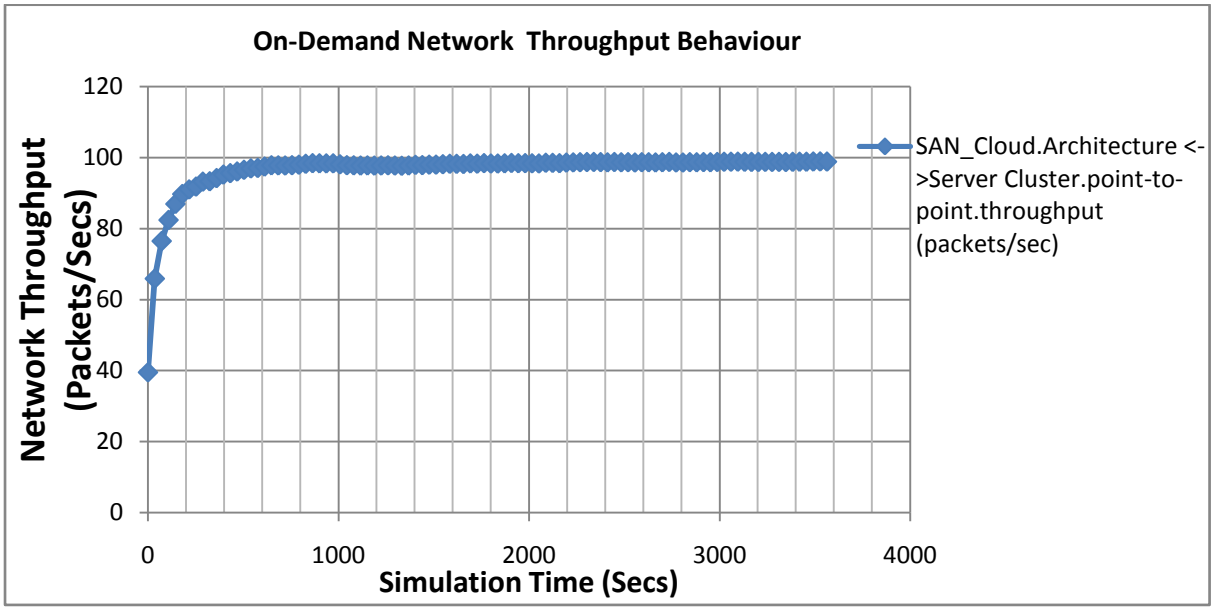


Figure 4.2: On-demand throughput profile

Given current server CPU performance, it would be more desirable to analyze more video streams than to waste CPU cycles on images with very little difference between them. With virtualization algorithms on the surveillance cameras (which scrutinizes the change in the digital image at the pixel level by comparing one frame or image of video with the previous frame), these cameras can identify movement, recognize objects or people as a group of related pixels, and determine the size of an object. As a result, the cloud servers can alert operators or generate alarms based on specific events, such as people entering the field of view, the direction of an object, or the removal of an item from the field of view. Fig. 4.3 shows a similarity response trend in both primary and secondary storage domains. Both offer good throughputs which are 900packets/sec (primary) and 1100packets/sec (secondary) over time. (See Appendix E for the simulation datasets).

4.1.3 On-demand Throughput Behavior with Virtualization

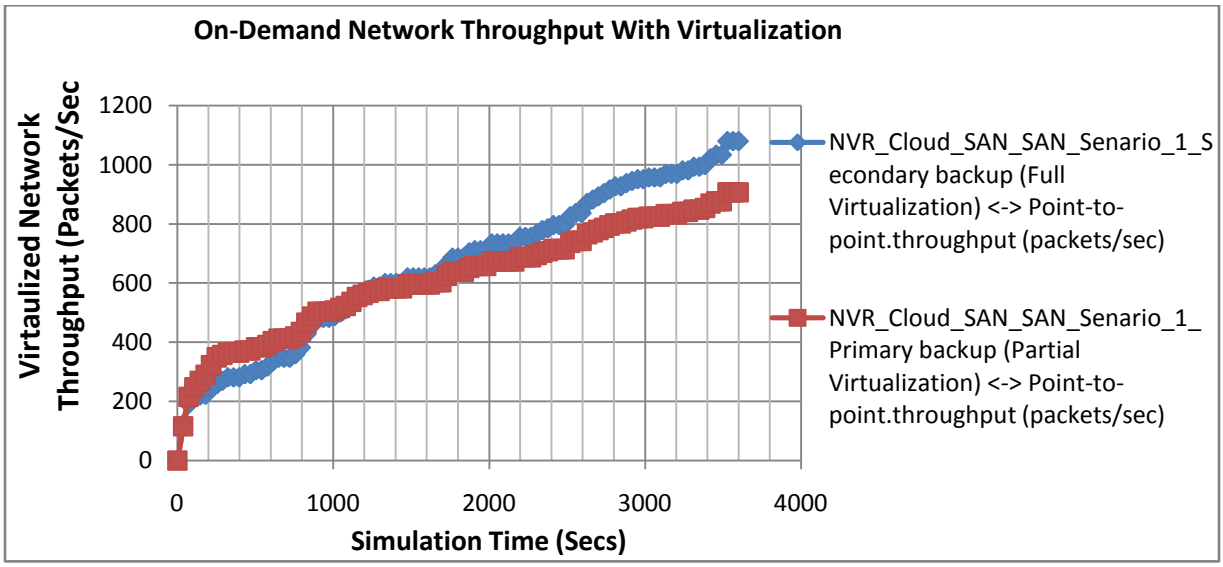


Figure 4.3: On-demand throughput profile with virtualization

The probability of on-demand trigger is always less than or equal to one, i.e.100% as shown in Fig. 4.4. This implies that there will virtually always be event trigger. The IP surveillance network cloud houses the video analytics capabilities embedded into DSPs (Digital Signal Processor) which also run on chipsets deployed in devices such as cameras and NVRs. They also run on the dedicated server clusters of Fig. 4.7. The flexibility of where video analytics can be deployed and who can use this new tool is enhanced when on the IP network. The network provides the video to be analyzed and generate reports that can be distributed anywhere the network goes.

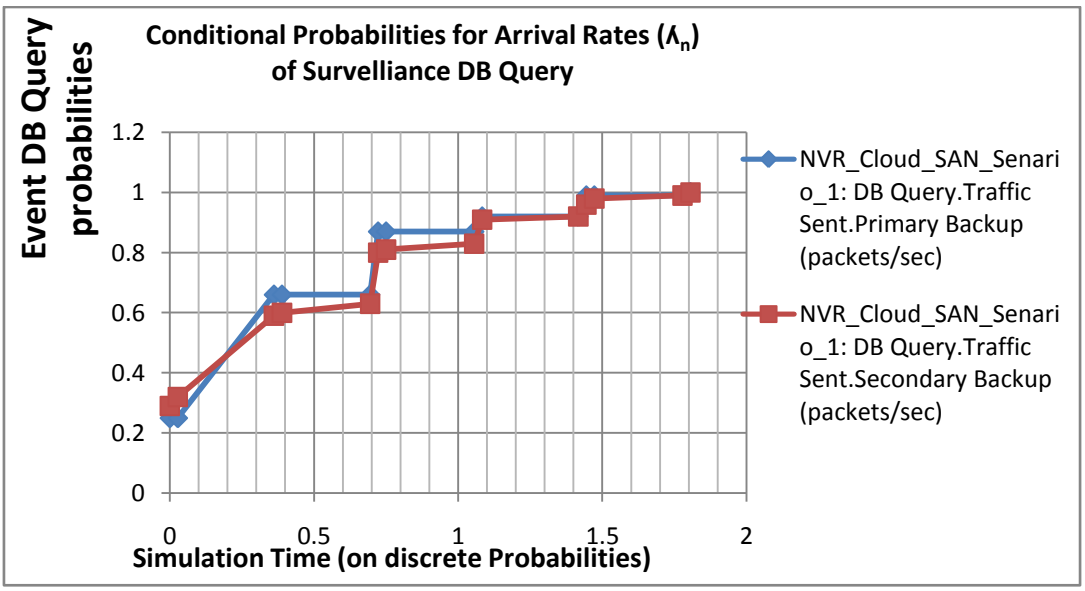


Figure 4.4: On-demand query probabilities

4.1.4 Resource Utilization Behaviour

It could be observed from Fig.4.5 that the backup literally has low utilization rates less than 15% during off peak period and not more than 35% at peak times. This underutilization is usually a deliberate action at cloud datacenters aimed at ensuring that the system does not collapse on-demand due to concerns about Service Level Agreement (SLA) violations that may result from resource contention as server utilization increases. The obtained low utilization rates at the storage cluster implies that the type of servers used and their configuration optimizes power consumption. It is also rational and necessary to keep the utilization rates as low as possible because, as a public cloud provider, one must guarantee as much isolation as possible in a public infrastructure so that one greedy user would not be allowed to make another nice user's life miserable by violating utilization requirements as well as the SLAs of critical workloads.

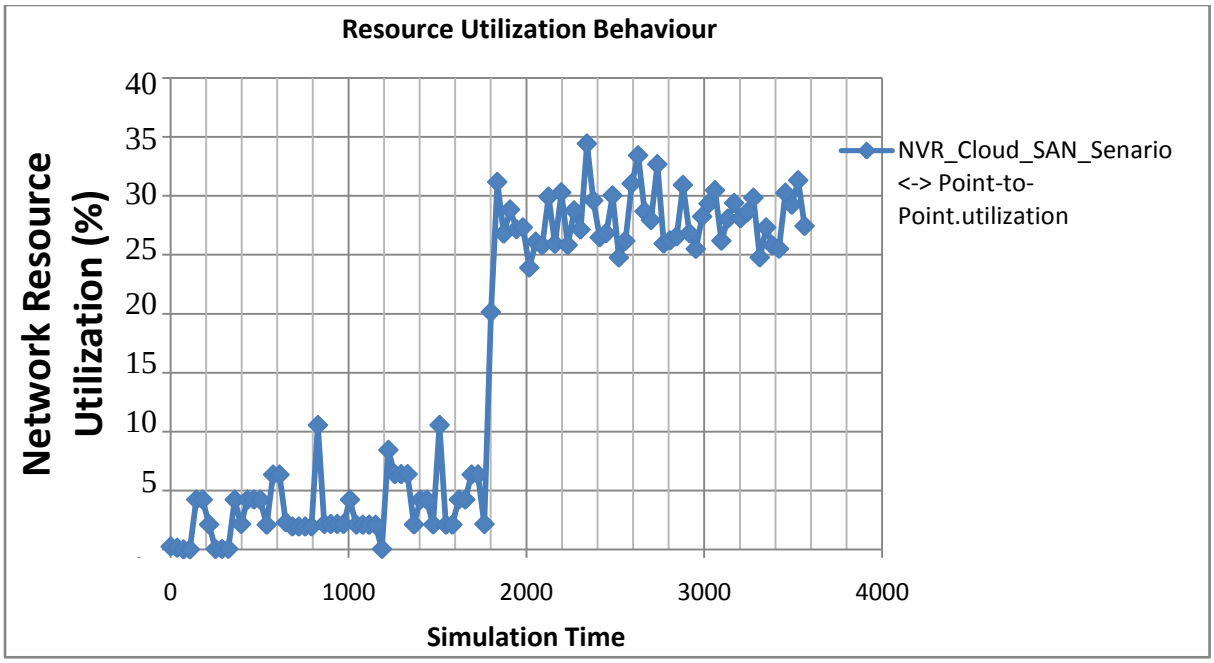


Figure 4.5: On-demand resource utilization profile

The simulation data sets (Appendix E) were generated by the modeler, after careful configuration of the network in the DES application and object configuration palette environment, and successful simulation.

Network utilization is the ratio of current network traffic (video/data streams) to the maximum traffic that the NVR-port or even VSG port can handle vis-à-vis the cloud

network. By monitoring network utilization, this reveals the state of the network - busy, normal or idle. From the datasets obtained, this made it easy to monitor the network utilization, so as to find out any bottleneck for possible network performance improvement. This could be used to inquire why the network utilization is low, or how network utilization could be increased.

At some points from the datasets, it was observed that the network was not stable for the traffic broadcast/multicast. At some other time, it was busy or idle. This could be used to plan for on-demand task scheduling by the various devices such as CPU on the network, or one could use '***optimize network devices'*** to either reduce or increase network utilization for predictive analytics.

4.1.5 Discussions

A prototype of OD-RGRSVS was designed and built using the following components; GSM modules (SIM 300), voltage Level Converter, Outdoor digital surveillance camera, H.264 DVR; 4-Channel, PIC microcontrollers 18F4520 at the client station, and 18F4550 at the control station, and a simplified power supply unit.

The cloud server cluster was modeled to offer optimal QoS throughput, network latency and resource utilization on point-to-point basis, such that users are enabled to access the video of their desired monitored resource on a handset or laptop from anywhere.

While no two video surveillance deployments are identical, the developed on-demand real time surveillance could be migrated to a large-scale, network-centric third- and fourth-generation video surveillance deployment which could have a mix of analogue and IP cameras. Such IP network-centric video surveillance could offer the following benefits;

- Reduced storage requirements because it has the intelligence to store video only if request is made by subscribers, i.e. on-demand response.
- Reduced number of servers as they can now support nearly double the number of cameras they did previously because they no longer need to devote compute cycles to video encoding owing to virtualization and consolidation.
- Improved video quality: At four frames per second, the ability to recognize faces is vastly improved.

- Gained ability to unify CCTV system with other security systems, such as alarm detection and access control systems.
- Reduced false alarms in areas covered by video surveillance cameras .
- Less time required to investigate incidents; Security operations centre and other authorized safety and security personnel can view stored or real-time video surveillance from any camera around the world, responding more quickly and appropriately to incidents.
- Investigation is further accelerated because investigators can retrieve more video at one time.
- Reduced maintenance costs; Cloud based IT has economies of scale and spends less time monitoring and maintaining servers than when physical security team maintained the dedicated servers
- Increased security; The cloud NVR based system is more secure. Network protection and virus definitions are implemented as soon as they become available.
- Return on investment. The system could pay for itself more than once by enabling the safety and security department to apprehend thieves and then recover the stolen property.
- Business continuity and backup recovery in the system offers 24/7 operation with 99.9% service availability, hence, near zero down time.

4.2 Evaluation of Objectives

1. A hardware prototype of OD-RGRSVS made up of a client station and a control station was designed and built. The schematic diagram of the client station is shown in Appendix B, while that of control station is shown in appendix C.

2. A miniature business model was developed by means of the control station prototype interfaced to PC. A GUI application was developed using VB.NET for base station interface to PC and visualization of client data resident in the EEPROM of the control station microcontroller unit. The application GUIs are shown in Fig. 3.20 - Fig.3.22.

3. Mathematical characterizations were developed for the following;

i. Cloud storage clusters comprising physical and virtual storage servers (section 3.8).

ii. Requests to the system as a Poisson process (section 3.9)

4. An optimization algorithm was developed for instantaneous data capture and transmission into the cloud (section 3.25).
5. Simulation of OD-RGRSVS was carried out to provide precise information on the throughput, latency and resource utilization (section 4.1).

4.3 Research Validation

In order to validate this research work, a java-based CloudAnalyst software which runs on CloudSim simulator was used because of its ability to handle multi-layer cloud models.

CloudSim has the following basic properties;

- Provides controlled and a repeatable environment to create and simulate cloud entities.
- Can be extended to include user defined policies for cloud.
- Provides changeable infrastructure modeling, changeable network architecture, federated cloud support.
- Provides virtual machine provisioning, host provisioning, network provisioning and application provisioning.

A limitation of CloudSim is lack of GUI feature which led to the use of CloudAnalyst simulator in this research work to extend the CloudSim feature.

CloudAnalyst is simply a CloudSim-based visual modeller for analysing cloud computing environments and applications as depicted in Fig.4.6.

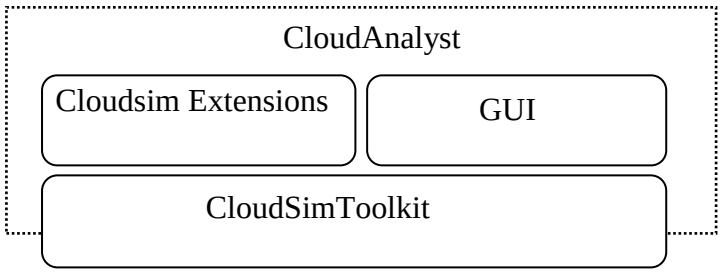


Figure 4.6: CloudAnalyst on CloudSim

4.3.1 Features of CloudAnalyst Simulator

There are many existing tool-kits which can also be used for simulation environment and can help in studying the performance of scalable applications which are available on the Internet.

CloudAnalyst features a GUI, with a level of visualization capability, which makes it an easy to use tool and better than just a tool-kit. It separates simulation setup environment exercise and supports the modeler to focus on the parameters used for simulation purposes rather than the programming technicalities only. It also supports a modeller to perform simulations continually by modifying the parameters easily, quickly and in very less time (Jeong & Park, 2012). The graphical user interface simulation output results of CloudAnalyst enables the results to be examined more proficiently and also quickly helping in getting over any problems dealing with the accuracy and performance of simulations.

Some of the features of CloudAnalyst are summarized as follows:

Usage Simplicity : CloudAnalyst is easy to set up as it comes with the java package and only requires one to simply double-click on the icon. Execution of simulation experiment is the main key feature of CloudAnalyst tool.

GUI based Output: GUI based output which comprises tables (consisting of rows and columns), graphs and charts are highly desired to review a number of results which are obtained at the time of Cloud Analyst simulation. Such GUI based presentations help in understanding and identifying the important outlines of the parameters and also helps in their comparison.

Repeatability: CloudAnalyst provides room to repeat the experiments which is a very significant requirement of any simulator. With CloudAnalyst simulator, if one experiment having some parameters, on simulation, produces some results, same results would be obtained each time the same simulation is executed with same parameters.

Ability to Save the Results: CloudAnalyst also has the option to save the results. This is helpful as we can save the experiment (along with the set of all input parameters and values taken during simulation) as a file on the system (PC) or other media. The results can also be exported to PDF format.

4.3.2 Setting up a Simulation in CloudAnalyst

To set up simulation in CloudAnalyst, the following steps were taken;

i. Definition of user bases –User Base entities are used to define the users of the application, their geographic distribution, and other properties such as the number of users, the frequency of usage and the pattern of usage such as peak hours. This is done in the Main tab of the 'Configure Simulation' screen.

ii. Definition of data centers – Using the Data Centers tab of the Configuration screen defines the data centers to be used in the simulation, including all the hardware and accounting aspects of the data centers.

iii. Allocation of Virtual Machines for the application in Data Centers – Once the data centers have been created, virtual machines are allocated in them for the simulated application using the Main tab of the Configurations screen. Multiple types of virtual machines could be allocated in the same data center during this step.

iv. Review and adjustment of the advanced parameters in the Advanced tab of the Configuration Screen.

v. Review and adjustment of the network latency and bandwidth matrices on the Internet Characteristics screen.

4.3.3 CloudAnalyst Simulation Scenario

The CloudAnalyst tool is used to analyze the various load balancing algorithms. To implement the various algorithms, the environment was simulated by taking 5 user bases and a data center, having 5 virtual machines. Each simulation was run for one hour, and average peak users were considered as 1000, while average off-peak users were considered to be 100 in each user base. Service broker policy used for simulation was closest data center. The simulation configuration screenshot is shown in Fig. 4.7, while configuration for the internet characteristics is shown in Fig.4.8.

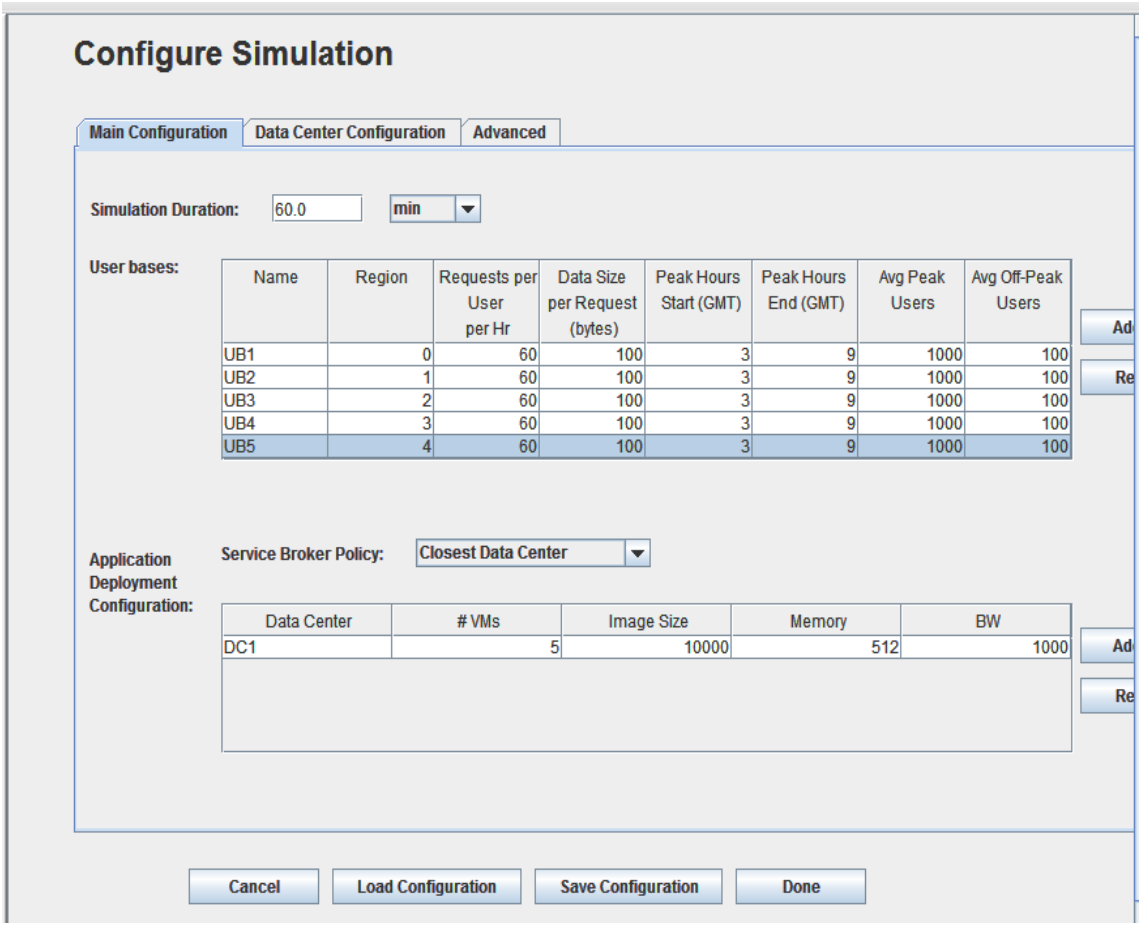


Figure 4.7: CloudAnalyst Simulation Configuration

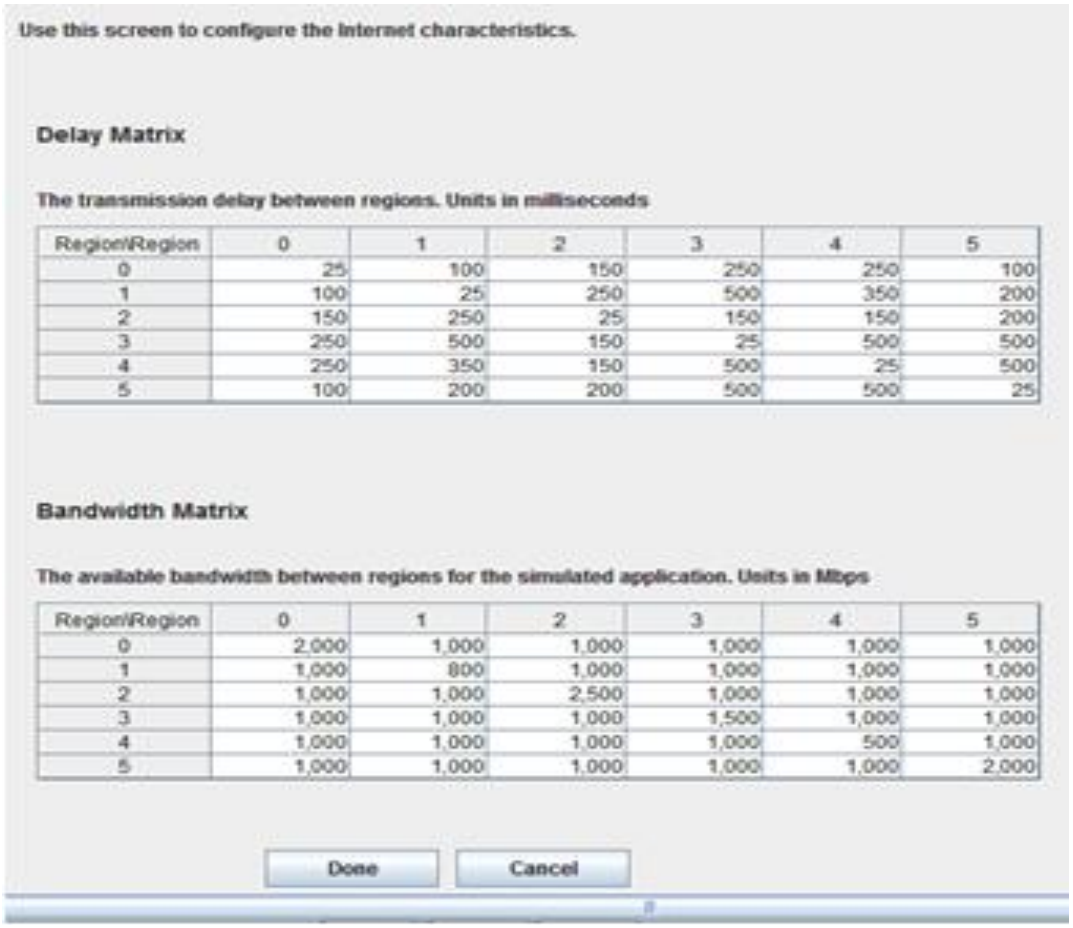


Fig. 4.8: Internet Characteristics Configuration screenshot

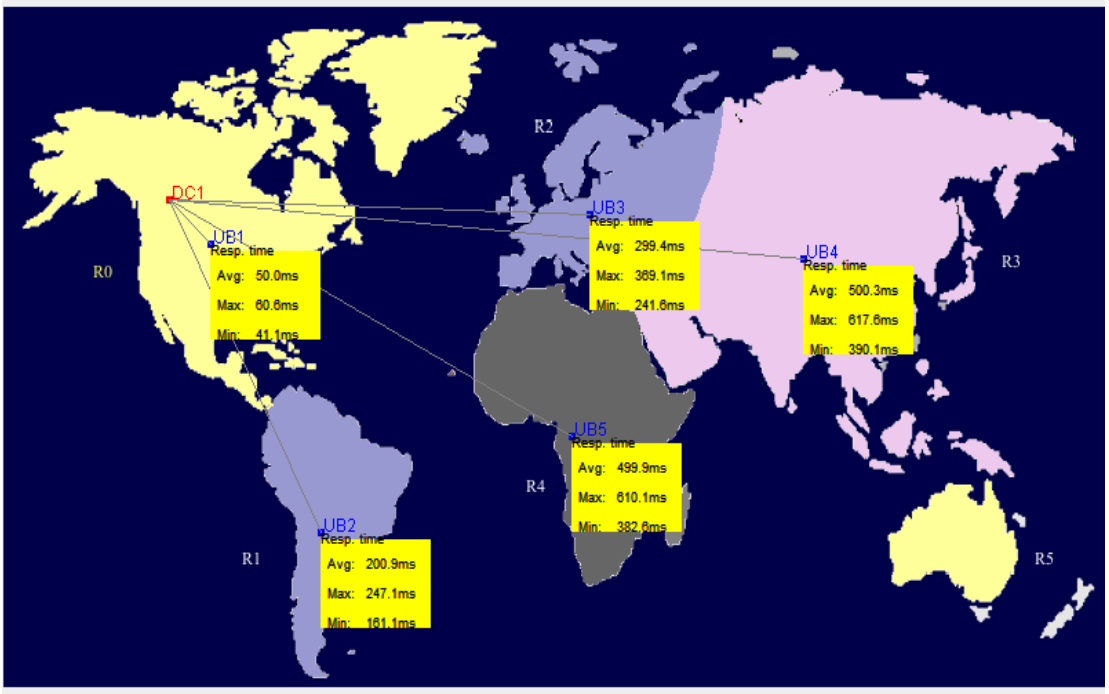


Figure 4.9: Simulation output screen using a datacenter and 5 user bases

Results of the Simulation Completed at: 12/11/2018 03:25:13

Overall Response Time Summary

	Avg (ms)	Min (ms)	Max (ms)
Overall response time:	310.50	41.11	617.61
Data Center processing time:	0.32	0.02	0.86

Response Time by Region

Userbase	Avg (ms)	Min (ms)	Max (ms)
UB1	50.03	41.11	60.61
UB2	200.88	161.11	247.11
UB3	299.42	241.61	369.12
UB4	500.33	390.11	617.61
UB5	499.87	382.60	610.12

Fig.4.10: Simulation screenshot in cloud analyst with 5 user bases

Further simulation runs were carried out until 10 user bases were used with results obtained and analysed. A screenshot for the simulation using a datacenter and 10 user bases is shown in Fig.4 .11.

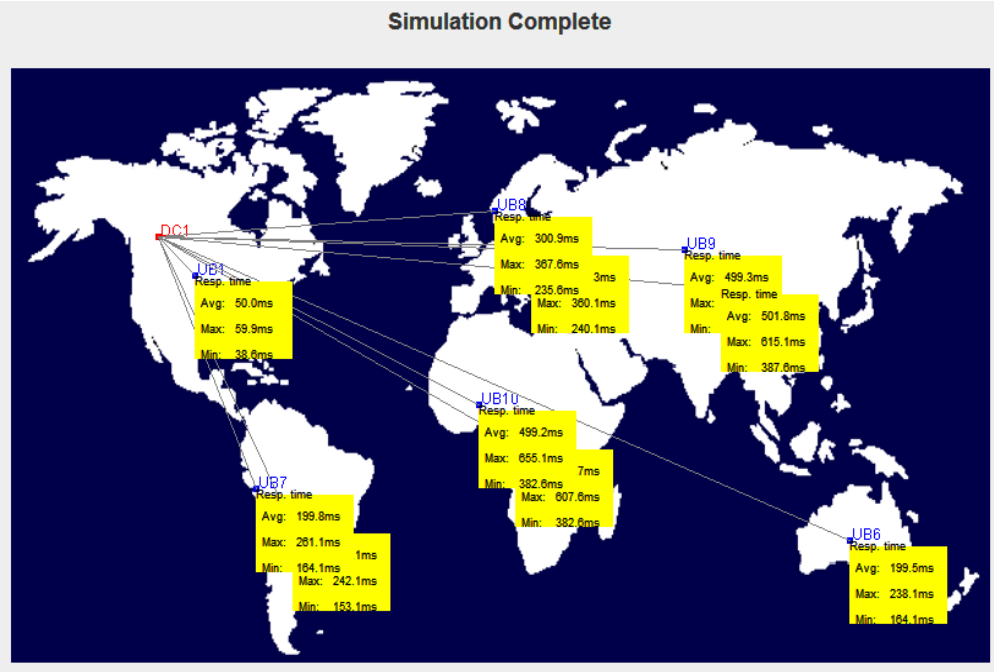


Figure 4.11: Simulation scenario using a datacenter and 10 user bases

Results of the Simulation Completed at: 12/11/2018 03:36:06

Overall Response Time Summary

	Avg (ms)	Min (ms)	Max (ms)
Overall response time:	280.03	38.61	655.11
Data Center processing time:	0.29	0.01	0.86

Response Time by Region

Userbase	Avg (ms)	Min (ms)	Max (ms)
UB10	499.00	382.62	655.11
UB1	50.03	38.61	59.86
UB2	200.01	153.12	242.12
UB3	299.41	240.09	360.11
UB4	501.62	387.61	615.12
UB5	200.69	153.12	243.11
UB6	49.98	41.11	60.86
UB7	199.84	164.12	243.11
UB8	300.97	235.62	367.61
UB9	499.71	387.62	625.11

Fig.4.12: Simulation result in cloud analyst with 10 user bases

4.3.4 CloudAnalyst Simulation Results

It was observed that User bases nearer the data center encountered shorter response time. From the result screenshot of Fig.4.10 when 5 user bases were used, UB1 being closest to the data center resulted in average response time of 50.03ms. This result is comparable to the response time of 2ms for obtained for the primary backup which had a shorter distance than the secondary backup that gave 10ms when Riverbed modeler was used. Even when the number of user bases was increased to ten in CloudAnalyst, as shown in Fig. 4.12, no significant variation in the result was obtained due to convergence that gave optimal results. The overall response time was found to be 280.03ms, which is acceptable for satisfactory QoS.

CHAPTER FIVE

FINDINGS, CONCLUSION AND RECOMMENDATION

5.1 Summary of Findings

During the simulation, output performance measures obtained from the data analysis revealed that the primary backup being closer to the video sensing gateway resulted in lower latency values than the secondary backup. Typically, the primary backup took about 0.002secs while the secondary backup took about 0.01secs delay.

Furthermore, it was observed that application of storage virtualization improved the overall network throughput (Fig. 4.2 and 4.3).

5.2 Contributions to Knowledge

In this work, the following are the contributions to knowledge;

1. Development of an on-demand video surveillance system that is automatically activated by means of valid GSM signal.
2. Formulation of mathematical characterization for the cloud storage cluster as well as video traffic arrivals to the system as a Poisson process.
3. Development of a unique Business Platform to manage database of subscribers to the remote security video sensing system.
4. Development of On-Demand Cloud Based Real-Time Remote Sensing (OD-RGRSVS) for satisfactory QoS which provides precise information on network performance analysis metrics such as latency, throughput, and resource utilization.

5.3 Conclusion

A miniature model of OD-RGRSVS activated by only valid GSM signal to eliminate processing of undesired video footage has been designed and built. This work has developed OD-RGRSVS as a future-poof video sensing system for processing only relevant video footage with remote cloud storage accessible via the online platform in addition to, saving files on an NVR or DVR hard drive. This has been achieved using Riverbed modeling software for simulation runs. The cloud-based system offers several advantages over saving all surveillance video feeds on an NVR, including the ability to access videos from anywhere and a larger storage capacity than the available NVR. The developed cloud storage is easy to use and requires minimal equipment. In

this case, any device with an internet connection which can send the video files to the cloud storage service is required.

One thing to consider when using the cloud storage is the amount of upstream bandwidth available on the network. If the video files are especially large, the upload process could slow down the network while uploading them. With the developed system, an NVR with a cloud service enables one to upload videos on a schedule and allows for selection of the best time to upload the files so the impact on the network is minimal. This could be nights, early mornings, weekends, or whenever works best for the user.

The system is very cost effective considering cloud storage and can benefit the surveillance system in many ways:

i. Video files are easily accessible from anywhere using either a computer, smart phone, or tablet.

ii. Files are not just stored locally, so even if a user equipment is damaged or stolen, the videos remain safe.

iii. Many companies choose to save videos for long periods of time, especially in case of accidents in the workplace; cloud storage makes it easier to keep those files without taking up limited space on a hard drive.

iv. Cloud storage can also be used as a backup for an NVR or hard drive even if it is not the main storage solution

This work has opened up a new frontier for promoting cloud based video surveillance systems with precise information on network latency, throughput and server resource utilization within the confines of acceptable QoS.

5.4 Recommendations

For improvement on OD-RGRSVS, the following measures are recommended;

i. Deployment of High Efficiency Video Coding (HEVC), also known as H.265 and MPEG-H Part 2, which offers about double the data compression ratio at the same level of video quality, or substantially improved video quality at the same bit rate is recommended instead of Advanced Video Coding (AVC) i.e. H.264 or MPEG-4 Part 10.

ii. Use of advanced encryption standard algorithm to secure video streaming protocols, and make strong camera access credentials needs to be explored.

iii. The investigation of privacy protection in video surveillance using transform-domain video scrambling in the MPEG-4 compressed video needs to be carried out.

iv. The impact of video compression on processing and storage efficiency given the cloud computational complexity should further be explored.

v. As there is shift towards getting everything onto the web - Internet of Things (IOT), there is need to cover every area or feature of interest under surveillance in order to deter crime, since crime deterred is crime prevented. This demands promulgation of a policy that seeks to lower the cost of IP cameras to make them easily affordable.

REFERENCES

Alvarez, A.R. & Humphrey, M. (2012). "A Model and Decision Procedure for Data Storage in Cloud Computing, Preliminary version". In P*roceedings of the IEEE/ACM International Symposium on Cluster, Cloud, and Grid Computing (CCGrid'12),* May 13-16, Ottawa Canada.

Armbrust M., Fox A., Griffith R., Joseph A.D., Katz R.H., Konwinski A., Lee G., Patterson D.A., Rabkin A., & Zaharia M. (2009). Above the Clouds: A Berkeley View of Cloud Computing. Technical Report No. UCB/EECS-2009-28, University of California at Berkley, USA.

Broaddus, C., Germano, T., Vandervalk, N., Divakaran,A., Wu, S. & Sawhney, H. (2009). " ACT-Vision: Active Collaborative Tracking for Multiple PTZ Cameras", Multisensor, Multisource Information Fusion: Architectures, Algorithms, and Applications, Proc. of SPIE Vol. 7345, 734505.

Buyya R. & Ranjan R. (2010). Federated Resource Management in grid and cloud computing Systems. *Journal of Future Generation Computer Systems, 26(5),* 1189–91.

Buyya R., Garg S.K., Calheiros R.N. (2011). SLA- oriented resource provisioning for cloud computing: challenges, architecture, and solutions. In: Proceedings of the International Conference on Cloud and Service Computing, vol. 17, No.5; pp.71–9.

Buyya R., Yeo C.S., and Venugopal S. (2009). Market-oriented cloud computing: vision, hype, and reality for delivering IT services as computing utilities. *JFuture Gener Comput Syst Arch*, *25*(6), 599–616.

Buyya R., Yeo C.S., Venugopal S. and Brandic I. (2009). Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility. *Future Generation Computer Systems, 25*(6), 599–616, Elsevier Science, Amsterdam, The Netherlands.

Chandra, M.A., Purwar, R., & Rajpal, N. (2012). A Novel Approach of Digital Video Encryption. *Int'l Journal of Computer applications,49*(4), 38-42.

Chi, Z., Zhang,F., Du, Z. & Liu, R. (2013). Cloud storage of massive remote sensing data based on distributed file system. Published in: Signal Processing, Communication and Computing (ICSPCC), August, 2013 IEEE International Conference **.** ISBN Information: INSPEC Accession Number: 13899051.

Cisco Systems Inc.(2007). Cisco Systems IP Networkcentric Video Surveillance. [White paper] (prod-white-paper0900aecd804a3e89.pdf). Pp1-15.

Cucchiara R., Grana C., Prati A., & Vezzani R. (2005). Computer vision system for in-house video surveillance. IEE Proceedings - *Vision, Image and Signal Processing. Vol.152,* Issue 2.

Daniel, P.S. & Sam, A.G. (2010). Research Methodology. Kalpaz Publications C-30, Satyawati Nagar, Delhi-110052. ISBN: 978-81-7835-900-7.

Diao, Z., Wang, Q., SU, N., & Zhang, Y. (2017). Study on Data Security Policy Based On Cloud Storage. IEEE 3rd Int'l Conference on High Performance and Smart Computing (HPSC), and IEEE int'l conference on intelligent data and security (ids). Pp 145-149.

Dornberger, Walter (1954). *V-2*, Ballantine Books.ASIN: B000P6L1ES, P.14

Giacomo, C., Grazia Lo S., Marcin Wozniak., & Robertas D. (2016). A Clustering Based System for Automated Oil Spill Detection by Satellite Remote Sensing. ICAISC (2) 2016: 613-623

GPS Advanced Control Segment (OCX). (2011, October 25). Losangeles.af.mil. (Factsheets). Retrieved November 6, 2011.

Guo, H., Huang Q., Li X., Sun Z.,& Zhang, Y. (2013). "Spatiotemporal analysis of urban environment based on the vegetation–impervious surface–soil model". *Journal of Applied Remote Sensing. 8. 084597.* Bibcode:2014JARS....8.4597G. doi:10.1117/1.JRS.8.084597.

Guoqing, L. & Zhenchun, H. (2017). Data Infrastructure for Remote Sensing Big Data: Integration, Management and On-Demand Service. *Journal of Computer Research and Development, , 54*(2): 267-283.

Harriton,G. & Lowford, J. (2006). "RFID and Privacy", ISBN 1-895-060-73-7.

Hilden, J. (2002, April 16). "What legal questions are the newchip implants for humans likely to raise?". *CNN.com (FindLaw)*. Retrieved March 17, 2009.

Hossain, M.A.(2014). Framework for a Cloud-Based Multimedia Surveillance System. *International journal of wireless sensor networks,* 10(5). https://doi.org/10.1155/2014/135257

Introduction to Video Surveillance Systems Over the Internet Protocol (October 2003). [White Paper] SPRA951A

Jeong, H-Y and Park, J.H. (2012). An Efficient Cloud Storage Model For Cloud Computing Environment. GPC 2012, 370–376.

Joshua, M. (2009, March 14). "Cell Phone Tracking Can Locate Terrorists - But Only Where It's Legal". FOX News. Retrieved March 14, 2009.

Kalra, M. and Singh, S. (2015). A review of metaheuristic scheduling techniques in cloud computing. *Egyptian Informatics Journal, 16*(3), 275-295.

Lewis, P. (2009). "Every step you take: UK underground centre that is spy capital of the world". *The Guardian*, March 2, 2009.

Lewis, S.B., DeSimone, P., Titus, K., Fuller, M.R. (2004). A Video Surveillance System for Monitoring Raptor Nests in a Temperate Rainforest Environment. *Northwest Science, Vol.78*, No.1.

Liu J.G., & Mason, P. J. (2009). *Essential Image Processing for GIS and Remote Sensing. Wiley-Blackwell. p. 4. ISBN 978-0-470-51032-2.*

Mahmud, A.R. and Zarrinbashar, E. (2008). Intelligent GIS-Based Road Accident Analysis and Real-Time Monitoring Automated System Using WiMAX/GPRS. *Int'l Journal of Engineering, 2*(1).

Mitrea, C.A., Mironică, I., Ionescu, B., & Dogaru, R. (2014). Multiple instance-based object retrieval in video surveillance: Dataset and evaluation. Intelligent Computer Communication and Processing (ICCP), 2014 IEEE International Conference. Pp 171-178.

Moganarangan, N., Babukarthik, R.G., Bhuvaneswari, S., Saleem Basha, M.S., Dhavachelvan P. (2016). A novel algorithm for reducing energy-consumption in cloud computing environment: Web service computing approach. *Journal of King Saud University - Computer and Information Sciences, 28*(1), 55-67.

Morgan, M.J. (2009, August 4). The Impact of 9/11 on Politics and War: The Day that Changed Everything?. Palgrave Macmillan. P.222. ISBN0- 230-60763-2.

Onoja, A.A, Babasola, O.L., Moyo, Edwin & Ojiambo, Viona (2018). The Application of Queuing Analysis in modeling Optimal Service level. *International Journal of Scientific and Engineering Research, 9.* DOI -10.14299/ijser.2018.01.002.

Peter Mell & Timothy Grance (September 2011). The NIST Definition of Cloud Computing (Technical report). National Institute of Standards and Technology: U.S. Department of Commerce. doi:10.6028/NIST.SP.800-145. Special publication 800-145.

Puthal, D., Nepal, S., Ranjan, R., & Chen, J. (2017). A dynamic prime number based efficient security mechanism for big sensing data streams. *Journal of Computer and System Sciences, 83*(1), 22-42.

Radio Waves “see” Through walls. *Science Daily* (Oct. 12, 2009).

Engineering Group, University of Utah.

Rajkumar, P. (2011). Motion Detection Based Interactive Surveillance Systems for Mobile Clients. International Conference on Information and Network Technology, IACSIT Press, Singapore. Pp.177-181.

Rajpoot, Q.M. (2016). Enhancing Security and Privacy in Large-Scale Video Surveillance through Role-Oriented Access Control Mechanism. Technical University of Denmark. PhD_2016_399.

Rajpoot, Q.M. & Jensen, C.D. (2014). Security and Privacy in Video Surveillance: Requirements and Challenges. 29th IFIP International Information Security Conference (SEC), Morocco. Springer, IFIP Advances in Information and Communication Technology, AICT-428, pp.169-184, 2014, ICT Systems Security and Privacy Protection.

Rajpoot, Q. M. & Jensen, C. D. (2016). Enhancing Security and Privacy in Video Surveillance through Role-Oriented Access Control Mechanism. Kgs. Lyngby: Technical University of Denmark. (DTU Compute PHD-2016; No. 399)

Robb, G.C. (1979). " Police Use of CCTV Surveillance: Constitutional Implications and Proposed Regulations". University of Michigan. *Journal of Law Reform. P. 572.*

Rodriguez-Silva, D.A., Gonz'lez-Castano, F.J., Adkinson-Orellana, L., & Gonz'lez-Martinez, D. (2012). Video surveillance based on cloud storage. Proceedings of the IEEE 5th International Conference on in Cloud Computing (CLOUD '12)2012991992 Google Scholar.

Romanca, M., Szekely, I., Cocorada, S., & Grama, I. (2007). IP Camera Surveillance System with Automated Recording. *ACTA Technica Napocensis- Electronics and Telecommunication. 48*(3).

Schott, John Robert (2007). Remote sensing: the image chain approach *(2nd ed.). Oxford University Press. p. 1. ISBN 978-0-19-517817-3.*

Schowengerdt, Robert A. (2007). Remote sensing: models and methods for image processing (3rd ed.). *Academic Press. p. 2. ISBN 978-0-12-369407-2.*

Singh, I., & Patil, H. (2010). “RFID: Dynamic Surveillance Approach”, *International Journal of Computer Science Issues (IJCSI), 7*(3), 24- 28.

Som, B. K., & Seth, S. (2018). M/M/C/N Queuing Systems With Encouraged Arrivals, Reneging, Retention And Feedback Customers. *Yugoslav Journal Of Operations Research, [S.L.], 28*(3) P. 333–344.

Staff (August 2007). "CCTV". Borough Council of King's Lynn & West Norfolk. Retrieved 2008.

Terrissa, L.S., Radhia, B., & Bretheé,J. (2016**).** ROS-Based Approach for robot as a service in cloud computing. The 2nd Conference on Computing Systems and Applications, December 13-14, At Ecole Polytechnique Militaire, Algiers, Algeria https://www.researchgate.net/publication/311583610.

Thomas, C. (March 4, 2009). "Court Asked To Disallow Warrantless GPS Tracking". *Information Week*. Retrieved March 18, 2009.

Tian Y., Brown, L., Hampapur, A., Lu, M., Senior, A., & Su, C. (2008). "IBM Smart Surveillance System (S3): Event Based Video Surveillance System with an Open and Extensible Framework", *Special Issue of Machine Vision and Applications Journal.*

"Tracking a suspect by mobile phone" . *BBC News*. August 3, 2005. Retrieved March 14, 2009.

Usman, M., Ahmad J.M., & He, X. (2017). Cryptography-Based Secure Data Storage and Sharing Using HEVC and Public Clouds. *Elsevier: Information Sciences, 387* Pp. 90 – 102

Valentin, L. et al. (2017). A cloud-based architecture for smart video surveillance. *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences, Volume XLII*-4/W3, 2017 . 2nd International Conference on Smart Data and Smart Cities, 4–6 October 2017, Puebla, Mexico.

Vetha S. & Vimala Devi K. (2017). Dynamic Resource Allocation In Cloud Using Queuing Model. *Journal of Industrial Pollution Control 33*(2) Pp. 1547-1554.

Vision;IEE Proceedings, Image and Signal Processing, Volume:152, Issue:2, 8th April 2005.

Wang, X. (2013). Intelligent multi-camera video surveillance: A review. The Chinese University of Hong Kong. Pattern Recognition Letters 34 (2013) 3–19.

Yang, X., Zhang, H., Ma H., Li, W., Fu, G., & Tang, Y. (2016). Multi-resource Allocation for Virtual Machine Placement in Video Surveillance Cloud. International Conference on Human Centered Computing. HCC 2016: Human Centered Computing. Pp 544-555.

Yesil, B. (2006). “Watching Ourselves - Video surveillance, urban space and self- self-responsibilization”. *Cultural Studies. Vol 20*(4-5), 400-416.

APPENDIX A: RESEARCH PAPER PUBLICATIONS

Inyiama, H.C., & Nwokolo, C.P. (2011). Automated Movement Monitoring and Control Using Geo-Referenced Trajectory Tracking and Analysis. Nigeria Society of Engineers (NSE), Awka Branch Annual Lecture. Scoa Heritage, Nigeria.

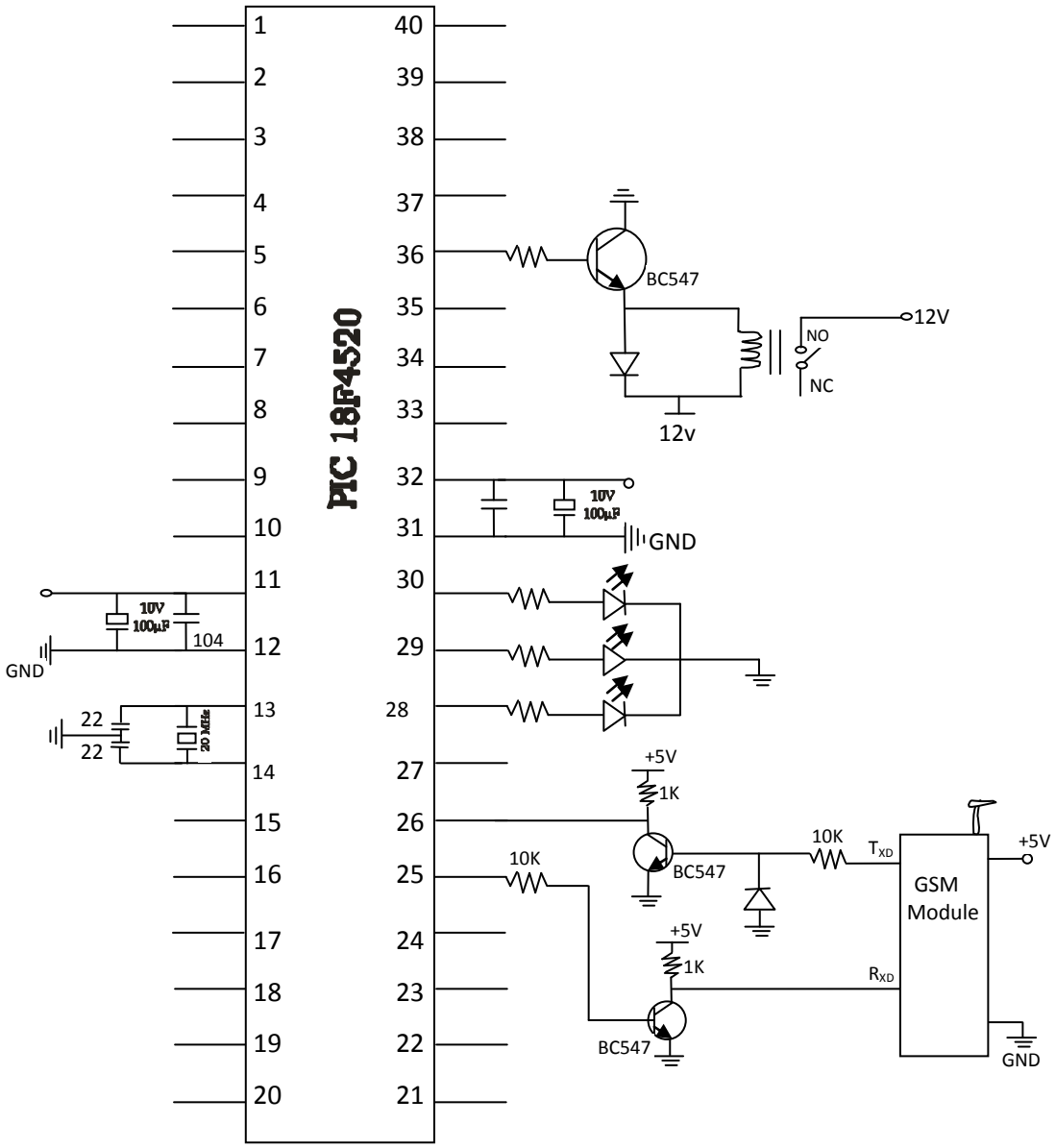
Nwokolo, C.P., & Inyiama, H.C. (2015). Client identification model for GPS- based On-demand real-time video surveillance security system. *International Journal of Research of Engineering and Computer Science (IJECS),4*,(9).

Nwokolo, C.P.,& Inyiama, H.C. (2016). Business model for on-demand GPS-based real-time video surveillance security system. *The International Journal Of Engineering And Science (IJES), 5*(2), 7-15.

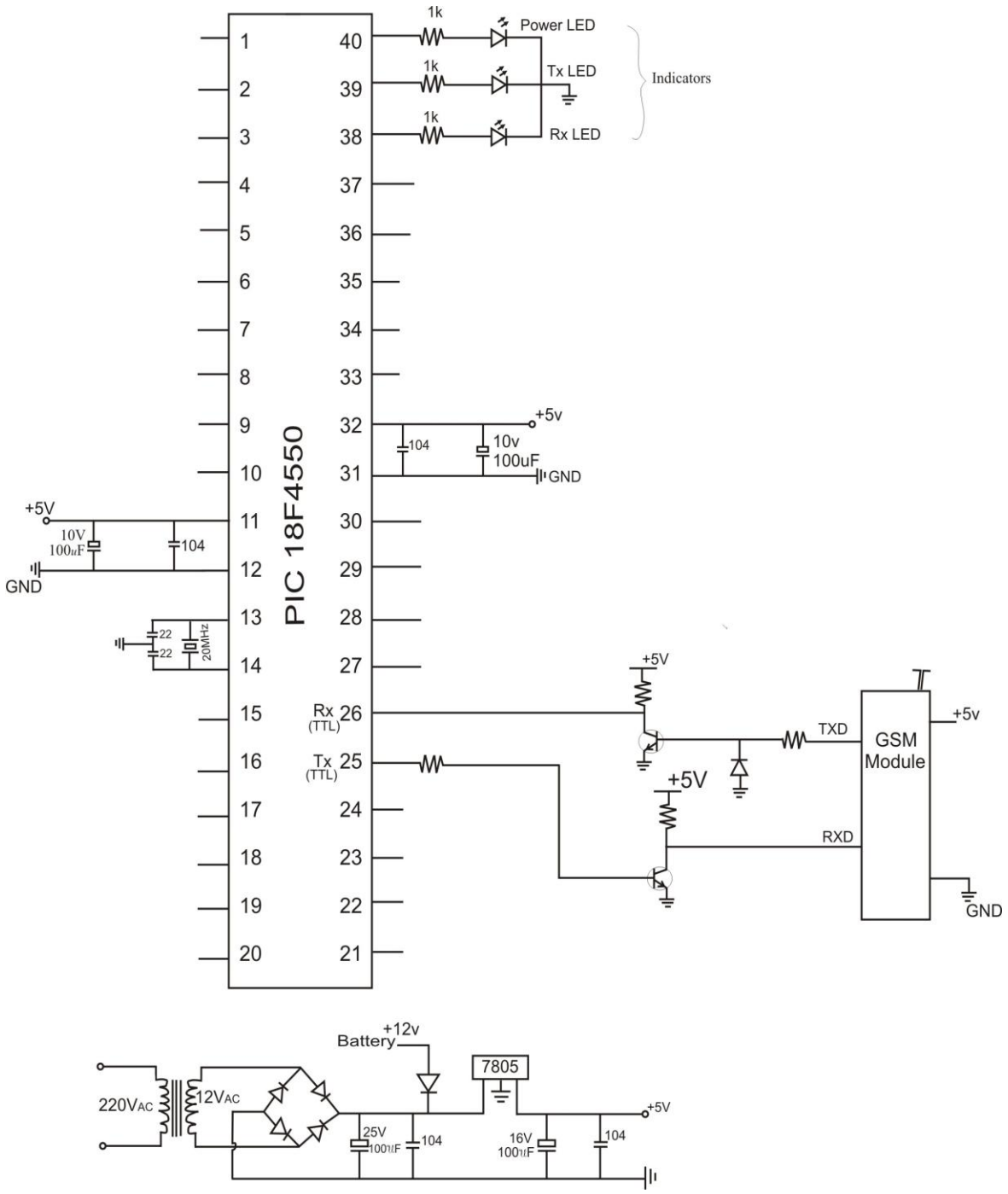
Nwokolo, C.P., & Inyiama, H.C. (2017). Quality of Service Evaluation in On-Demand Cloud-Based Video Surveillance. IEEE Nigercon Conference Proceedings. CP_142. Papers_532-537. Federal University of Technology (FUTO), Owerri Imo State, Nigeria.

Nwokolo, C.P., Inyiama, H.C., & Obiora-Dimson, I.C. (2018). Design and Simulation of GSM-Based On-Demand Video Surveillance with Cloud Storage. Accepted for publication on 16th April,2018. *Journal of Engineering and Applied Sciences*, Nnamdi Azikiwe University, NAU, Awka.

APPENDIX B: CLIENT STATION SCHEMATIC DIAGRAM

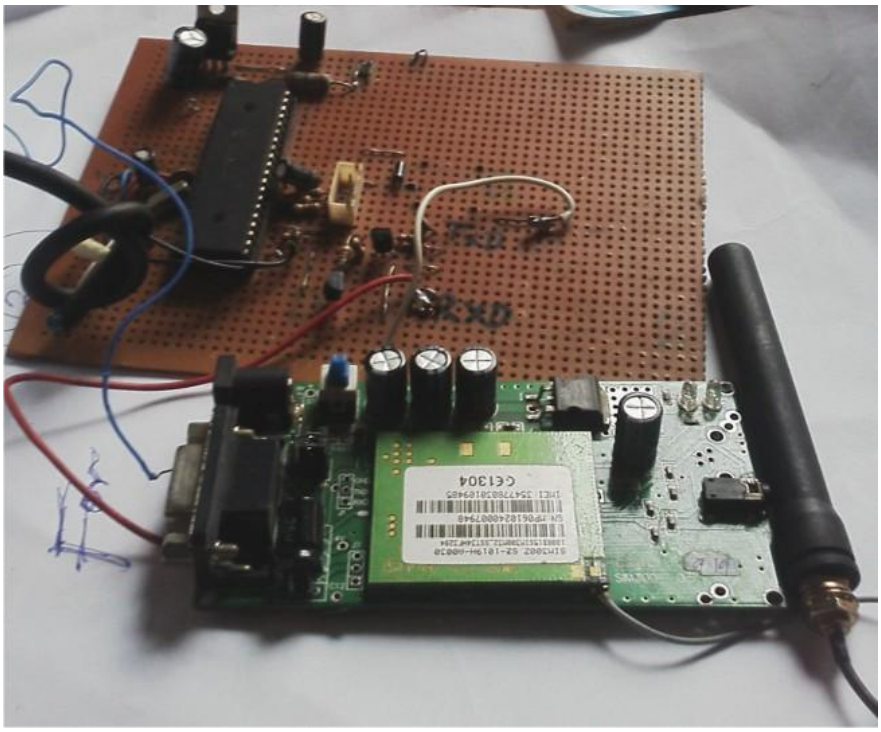


APPENDIX C: CONTROL STATION SCHEMATIC DIAGRAM



Control Station Schematic Diagram with power supply unit.

APPENDIX D: PROTOTYPE HARDWARE SNAPSHOTS



Control station circuit with SIM300 GSM Module

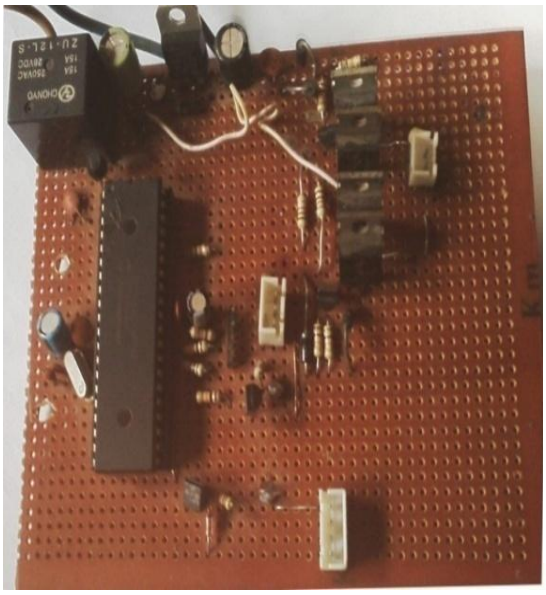


Figure 3.21a : Client station circuit on a circuit board

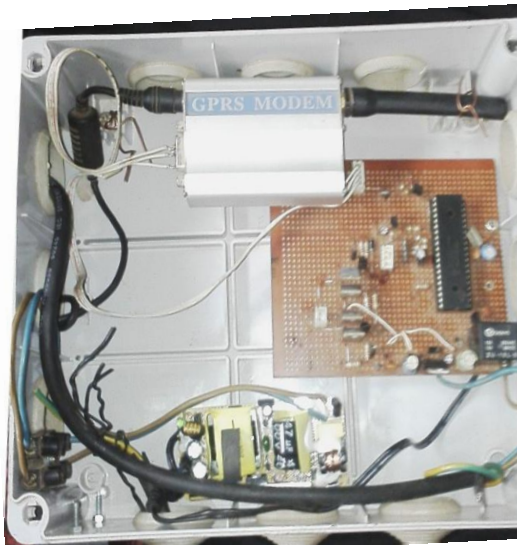


Figure 3.21b: Client station circuit connected to GSM module mounted on the base of the casing.

Fig.3.22 is a snapshot of the client station with a surveillance camera base resting on the client station prototype casing.

Figure 3.22: Client station with surveillance camera

Client station connected to a DVR

APPENDIX E: SIMULATION DATASETS

Network Utilization Dataset

Time (sec)	NVR_Cloud_SAN_Senario <-> Point-to-Point.utilization
0	0.024966667
36	0.014328889
72	0.00076
108	0.001013333
144	0.423051111
180	0.422957778
216	0.21216
252	0.003682222
288	0.003682222
324	0.004728889
360	0.422593333
396	0.215604444
432	0.422386667
468	0.423608889
504	0.421586667
540	0.209755556
576	0.634737778
612	0.634737778
648	0.229217778
684	0.194466667
720	0.194466667
756	0.194466667
792	0.194466667
828	1.055175556
864	0.215602222
900	0.215602222
936	0.215602222
972	0.215602222
1008	0.422393333
1044	0.209744444
1080	0.209457778
1116	0.209457778
1152	0.209457778
1188	0.00428
1224	0.844484444
1260	0.639046667
1296	0.639046667
1332	0.639046667
1368	0.211624444
1404	0.4224
1440	0.422517778
1476	0.211733333

Network Utilization Dataset contd.

Time (sec)	NVR_Cloud_SAN_Senario <-> Point-to-Point.utilization
1512	1.05586
1548	0.209946667
1584	0.209946667
1620	0.423088889
1656	0.423088889
1692	0.635515556
1728	0.635515556
1764	0.215626667
1800	2.014051992
1836	3.117454093
1872	2.678785296
1908	2.883538228
1944	2.716255719
1980	2.732066773
2016	2.390393798
2052	2.610592406
2088	2.579530859
2124	2.99283222
2160	2.591953738
2196	3.02916081
2232	2.582891441
2268	2.875896419
2304	2.713725409
2340	3.442378603
2376	2.96013732
2412	2.647277724
2448	2.682793523
2484	3.003250256
2520	2.476392609
2556	2.617689885
2592	3.103769036
2628	3.34329502
2664	2.868185978
2700	2.793099027
2736	3.268044625
2772	2.594946833
2808	2.621663153
2844	2.654256034
2880	3.092020509
2916	2.683878057
2952	2.549605672
2988	2.824455171

Network Utilization Dataset contd.

Time (sec)	NVR_Cloud_SAN_Senario <-> Point-to-Point.utilization
3024	2.93346251
3060	3.046924344
3096	2.618857951
3132	2.805261939
3168	2.938902102
3204	2.809392444
3240	2.858256417
3276	2.983448207
3312	2.477292437
3348	2.731800716
3384	2.579343336
3420	2.550637973
3456	3.025602042
3492	2.923971986
3528	3.131326527
3564	2.743978435
3600	2.743978435

Conditional Probabilities for Arrival Rates (λ_n) of Surveillance DB Query

DES Time (Secs)	NVR_Cloud_SAN_Senario_1: DB Query.Traffic Sent.Primary Backup (packets/sec)	NVR_Cloud_SAN_Senario_1: DB Query.Traffic Sent.Secondary Backup (packets/sec)
0	0.25	0.29
0.027778	0.25	0.32
0.361111	0.66	0.59
0.388889	0.66	0.6
0.694444	0.66	0.63
0.722222	0.87	0.8
0.75	0.87	0.81
1.055556	0.87	0.83
1.083333	0.92	0.91
1.416667	0.92	0.92
1.444444	0.99	0.96
1.472222	0.99	0.98
1.777778	0.99	0.99
1.805556	1	1
1.805556	1	1

On-Demand Throughput with Virtualization

Time (sec)	NVR_Cloud_SAN_SAN_Senario_1_Secondary backup Point-to-point.throughput (packets/sec)	NVR_Cloud_SAN_SAN_Senario_1_ Primary backup Point-to-point.throughput (packets/sec)
0	0	0
36	122	116
72	191	215
108	215	248
144	219	269
180	222	290
216	242	322
252	257	349
288	269	357
324	281	365
360	281	365
396	281	365
432	292	372
468	292	372
504	305	383
540	305	383
576	317	391
612	335	404
648	347	412
684	347	412
720	347	412
756	359	420
792	382	435
828	428	466
864	458	487
900	482	503
936	482	503
972	482	503
1008	488	508
1044	500	516
1080	511	523
1116	532	537
1152	555	553
1188	566	560
1224	577	567
1260	588	574
1296	588	574
1332	600	582
1368	600	582

On-Demand Throughput with Virtualization contd.

Time (sec)	NVR_Cloud_SAN_SAN_Senario_1_Secondary backup Point-to-point.throughput (packets/sec)	NVR_Cloud_SAN_SAN_Senario_1_ Primary backup Point-to-point.throughput (packets/sec)
1404	600	582
1440	600	582
1476	619	596
1512	619	596
1548	619	596
1584	619	596
1620	619	596
1656	630	603
1692	630	603
1728	664	625
1764	686	639
1800	686	639
1836	686	639
1872	704	652
1908	711	658
1944	711	658
1980	711	658
2016	734	673
2052	734	673
2088	734	673
2124	734	673
2160	734	673
2196	756	688
2232	756	688
2268	756	688
2304	767	695
2340	779	703
2376	785	708
2412	796	715
2448	796	715
2484	796	715
2520	826	736
2556	837	743
2592	837	743
2628	871	765
2664	882	772
2700	893	780
2736	904	787
2772	916	795
2808	927	802

On-Demand Throughput with Virtualization contd.

Time (sec)	NVR_Cloud_SAN_SAN_Senario_1_Secondary backup Point-to-point.throughput (packets/sec)	NVR_Cloud_SAN_SAN_Senario_1_ Primary backup Point-to-point.throughput (packets/sec)
2844	927	802
2880	938	809
2916	945	815
2952	951	820
2988	951	820
3024	957	825
3060	957	825
3096	957	825
3132	969	833
3168	969	833
3204	969	833
3240	981	841
3276	981	841
3312	993	849
3348	993	849
3384	999	854
3420	1022	869
3456	1034	877
3492	1034	877
3528	1080	907
3564	1080	907
3600	1080	907
3600	1080	907

On-Demand Network Throughput

Time (sec)	SAN_Cloud.Architecture <->Server Cluster point-to-point.throughput (packets/sec)
0	39.48945777
36	65.89062728
72	76.46315843
108	82.39703668
144	86.91662179
180	89.69447175
216	90.99240274
252	91.78748088
288	93.1837637
324	93.28720188
360	94.19018388
396	95.17291558
432	95.58407787
468	96.04084377
504	96.51398412
540	96.91730682
576	97.04202033
612	97.42571742
648	97.78946186
684	97.76523892
720	97.7168766
756	97.80907931
792	97.94180412
828	98.20964804
864	98.38499583
900	98.34697807
936	98.31777358
972	98.33643578
1008	98.0560512
1044	97.81124001
1080	97.77502667
1116	97.70885713
1152	97.74819393
1188	97.69699895

On-Demand Network Throughput contd.

Time (sec)	SAN_Cloud.Architecture <->Server Cluster point-to-point.throughput (packets/sec)
1224	97.72442336
1260	97.78079888
1296	97.71307383
1332	97.64307358
1368	97.73400759
1404	97.90608346
1440	97.83392985
1476	97.96329498
1512	97.96533704
1548	98.08862841
1584	98.21116375
1620	98.19228007
1656	98.1553097
1692	98.31394651
1728	98.23887502
1764	98.39824306
1800	98.28595272
1836	98.27587965
1872	98.34609201
1908	98.44502634
1944	98.37385206
1980	98.39746123
2016	98.34527096
2052	98.30072995
2088	98.49945209
2124	98.46930675
2160	98.3821015
2196	98.5487665
2232	98.60094175
2268	98.64952065
2304	98.70698494
2340	98.728254
2376	98.68174793
2412	98.61585881
2448	98.70833649

On-Demand Network Throughput contd.

Time (sec)	SAN_Cloud.Architecture <->Server Cluster point-to-point.throughput (packets/sec)
2484	98.6293576
2520	98.65782725
2556	98.56721981
2592	98.64939251
2628	98.64393759
2664	98.58297938
2700	98.65459261
2736	98.73254421
2772	98.57668993
2808	98.56111615
2844	98.66930532
2880	98.63270907
2916	98.68953579
2952	98.64555323
2988	98.7191637
3024	98.77850983
3060	98.78868698
3096	98.80629559
3132	98.77383252
3168	98.73751141
3204	98.73010706
3240	98.75174331
3276	98.73382298
3312	98.73989428
3348	98.7119023
3384	98.76407816
3420	98.78483366
3456	98.78534869
3492	98.85006214
3528	98.8687779
3564	98.83514851
3600	98.83514851

On-Demand Latency Datasets

Time (sec)	NVR_Cloud_SAN_Senario_1-Primary_Backup <-> Point-to-point.Queuing delay (sec)	NVR_Cloud_SAN_Senario_1-DES-1: Enterprise SAN. Secondary.Backup<- > Point-to-point.queuing delay (sec)
0	0.0000848	0.00008208
36	0.00018941	0.000179769
72	0.00026205	0.000491438
108	0.00035325	0.000582638
144	0.00044445	0.000673838
180	0.00053565	0.000765038
216	0.00062685	0.000856238
252	0.00062685	0.000856238
288	0.00062685	0.000856238
324	0.00062685	0.000856238
360	0.00062685	0.000856238
396	0.00062685	0.000856238
432	0.00062685	0.000856238
468	0.00062685	0.000856238
504	0.00062685	0.000856238
540	0.00062685	0.000928238
576	0.00062685	0.001000238
612	0.00062685	0.001000238
648	0.00062685	0.001000238
684	0.00062685	0.001000238
720	0.00062685	0.001000238
756	0.00062685	0.001000238
792	0.00062685	0.001072238
828	0.00062685	0.001072238
864	0.00062685	0.001072238
900	0.00062685	0.001072238
936	0.00062685	0.001072238
972	0.00062685	0.001072238
1008	0.00062685	0.001072238
1044	0.00062685	0.001072238
1080	0.000691535	0.00179922
1116	0.000691535	0.00179922
1152	0.000691535	0.00179922
1188	0.000691535	0.00179922
1224	0.000691535	0.00187122
1260	0.000691535	0.00187122
1296	0.000691535	0.00187122
1332	0.000691535	0.00187122
1368	0.000691535	0.00187122
1404	0.000691535	0.00187122
1440	0.000755935	0.002640266

On-Demand Latency Datasets contd.

Time (sec)	NVR_Cloud_SAN_Senario_1-Primary_Backup <-> Point-to-point.Queuing delay (sec)	NVR_Cloud_SAN_Senario_1-DES-1: Enterprise SAN. Secondary.Backup<- > Point-to-point.queuing delay (sec)
1476	0.000755935	0.002640266
1512	0.000755935	0.002640266
1548	0.000755935	0.002640266
1584	0.000755935	0.002640266
1620	0.000755935	0.002640266
1656	0.000755935	0.002640266
1692	0.000755935	0.002712266
1728	0.000755935	0.002784266
1764	0.000755935	0.002784266
1800	0.000755935	0.002784266
1836	0.000913104	0.003355199
1872	0.000980304	0.003590399
1908	0.000980304	0.003590399
1944	0.000980304	0.003590399
1980	0.001044704	0.004413599
2016	0.001044704	0.004413599
2052	0.001044704	0.004413599
2088	0.001044704	0.004413599
2124	0.001044704	0.004413599
2160	0.00110939	0.005085532
2196	0.00110939	0.005085532
2232	0.00110939	0.005085532
2268	0.00110939	0.005085532
2304	0.00110939	0.005085532
2340	0.00110939	0.005157532
2376	0.00110939	0.005229532
2412	0.00110939	0.005229532
2448	0.00110939	0.005229532
2484	0.00117499	0.005799932
2520	0.00117499	0.005799932
2556	0.00117499	0.005799932
2592	0.001239676	0.006489393
2628	0.001239676	0.006489393
2664	0.001304076	0.00728263
2700	0.001368762	0.00804663
2736	0.001368762	0.00804663
2772	0.001368762	0.00811863
2808	0.001368762	0.00811863
2844	0.001433447	0.008907284
2880	0.001433447	0.008907284
2916	0.001739047	0.008973418

On-Demand Latency Datasets contd.

Time (sec)	NVR_Cloud_SAN_Senario_1-Primary_Backup <-> Point-to-point.Queuing delay (sec)	NVR_Cloud_SAN_Senario_1-DES-1: Enterprise SAN. Secondary.Backup<- > Point-to-point.queuing delay (sec)
2952	0.001739047	0.008973418
2988	0.001739047	0.009045418
3024	0.001739047	0.009045418
3060	0.001739047	0.009045418
3096	0.001739047	0.009117418
3132	0.001739047	0.009117418
3168	0.001739047	0.009117418
3204	0.001739047	0.009189418
3240	0.001739047	0.009189418
3276	0.001739047	0.009189418
3312	0.001739047	0.009189418
3348	0.001739047	0.009261418
3384	0.001739047	0.009333418
3420	0.001739047	0.009333418
3456	0.001739047	0.009333418
3492	0.001803447	0.010052125
3528	0.001803447	0.010052125
3564	0.001803447	0.010052125

APPENDIX F

SOURCE CODE IN EMBEDDED C-LANGUAGE FOR CONTROL STATION COMMUNICATION WITH CLIENT STATION

// **Control Station _Client Station Communication via PIC microcontroller and GSM modules using Microchip MPLAB IDE**

```
unsigned char atcTest[] = "AT";                    // Every AT command starts with "AT"
unsigned char atcEcho[] = "ATE0";                  // Disable command echo
unsigned char atcTxtmode[] = "AT+CMGF=1";          // TXT messages
unsigned char atcMsgPhonenumber[] = "AT+CMGS=\"\atcMsgPhonenumber";";
//("AT+CMGS=\"08036807599\";");
//const char atc4[] = "AT+CMGR=1";                 // Command for reading message from
location 1 from inbox
//const char atc5[] = "AT+CMGD=1,4";               // Erasing all messages from inbox

unsigned char text_Location[] = "      DATABASE LOCATION:  ";
unsigned char Read_Buffer[64] absolute 0x500;
unsigned char Write_Buffer[64]absolute 0x540;
unsigned char num,FLAG = 0,k,rec_data,address,address_hold, tag;
unsigned int cnt,kk;
unsigned char gsm_response[20];

sbit RequestPin  at  RB4_bit;

sbit RequestSW  at  RB7_bit;
sbit RequestFlag  at FLAG.B0;
sbit USB_Connected_Flag at FLAG.B2;

char i;                          // Loop variable
void UART1_Write_Text_Newline(unsigned char msg[])
{
 UART1_Write_Text(msg);
 UART1_Write(10);
 UART1_Write(13);
}
```

```
void sendSMS(unsigned char msg[]){                    //routine for sending SMS msg.
  UART1_Write_Text_Newline(atcMsgPhonenumber);
  Delay_ms(100);
  //check for > and send text msg

  UART1_Write_Text(msg);
  UART1_Write(0X1A);    //ctrl Z
  Delay_ms(100);
}

void Requestdetect_GSM(){
       RequestFlag = 1;   //Metal Alarm
    }
    if(RequestPin == 0){
      RequestFlag = 1;
    }
}

//****************************************
  void CheckStatus(){
   if(RequestFlag ==1){
    //send  to the numbers in EEPROM in succession
          address = 0;
         do{
          address_hold =  address;
          address_hold =  address_hold * 20;
    //first number from EEPROM       // atcMsgPhonenumber[10 to 20]                //10 to
20 replaces the phonenumber for messaging

           for(cnt=0;cnt<11;cnt++){
             atcMsgPhonenumber[cnt + 10] = EEPROM_Read(cnt+ address_hold);
             Delay_ms(20);
           }
```

```
            Delay_ms(1000);
            address++;
          }while(address < 4);
       RequestFlag = 0;
  }
  else if(RequestFlag == 1){
        address = 0;
         do{
           address_hold =  address;
           address_hold =  address_hold * 20;
     //first number from EEPROM       // atcMsgPhonenumber[10 to 20]                  //10 to
20 replaces the phonenumber for messaging

            for(cnt=0;cnt<11;cnt++){
              atcMsgPhonenumber[cnt + 10] = EEPROM_Read(cnt+ address_hold);
              Delay_ms(20);
            }

            Delay_ms(1000);
            address++;
          }while(address < 4);
       RequestFlag = 0;
       //while(!HID_Write(&Write_Buffer,64));
  }
}
 //****************************************
void clear_buffer(unsigned char buffer[])
{
 unsigned char i = 0;
 for(i=0; i<64; i++){
    buffer[i] = '\0';
 }
}
```

```
void RetrieveData(){
     for(cnt=0;cnt<11;cnt++)
 {
//  Write_Buffer[cnt] = Read_Buffer[cnt];
  Write_Buffer[cnt] = EEPROM_Read(cnt+ address_hold);
  Delay_ms(20);
 }
  for(cnt=0;cnt<25;cnt++){
    Write_Buffer[cnt+11] = text_Location[cnt];
  }
  address = address_hold + 11;
  Write_Buffer[36] = (EEPROM_Read(address)+ 1);
  if(Write_Buffer[36]> 57){          //>9in ascii, write 10
    Write_Buffer[36] = 49;
    Write_Buffer[37] = 48;
  }

  Delay_ms(100);
// Write_Buffer[1] = Read_Buffer[11];
 while(!HID_Write(&Write_Buffer,64));
 }
//***************************************
 void interrupt()
{
 //USB_Interrupt_Proc();
 if(PIR2.USBIF){
  USB_Interrupt_Proc();
  USB_Connected_Flag = 1;
   }

 TMR0L = 100;            //Reload Value
 INTCON.TMR0IF = 0;       //Re-Enable Timer-0 Interrupt
}
```

```
//*****************************************
void main()
{
 PORTB = 0;
 PORTA = 0;
 PORTC = 0;
 PORTE = 0;
 TRISA = 0;
 TRISE = 0;
 TRISB = 0XFF;
 address = 0;
 tag = 0;
 k=0;
 UART1_Init(9600);
 Delay_ms(100);
 //UART1_Write_Text("USB Test Program");

 ADCON1 = 0x0F;                 // Configure AN pins as digital
 CMCON  = 7;                    // Disable comparators
 TRISB = 0xFF;
 TRISC = 0x80;

 INTCON = 0;
INTCON2 = 0b00000101;//0xF5;
INTCON3 = 0xC0;
RCON.IPEN = 0;
PIE1 = 0;
PIE2 = 0;
PIR1 = 0;
PIR2 = 0;
T0CON = 0x47;
TMR0L = 100;
INTCON.TMR0IE = 1;
```

```
T0CON.TMR0ON = 1;
INTCON = 0xE0;
//RCIE_bit = 1; //enable interrupt for serial receive
//UART1_Write(10);
//UART1_Write(13);
//UART1_Write_Text_Newline("Data is Ready to be Received from the PC");
USB_Connected_Flag = 0;
IDLEIE_bit = 1;
Hid_Enable(&Read_Buffer,&Write_Buffer);
Delay_ms(2000);

//*************************
//GSM module initialization
//*************************

UART1_Write_Text_Newline(atcTest);
Delay_ms(1000);
UART1_Write_Text_Newline(atcEcho);
Delay_ms(1000);
UART1_Write_Text_Newline(atcTxtmode);
Delay_ms(1000);

 start:
loop_second:

clear_buffer(Read_Buffer);
clear_buffer(Write_Buffer);
if(USB_Connected_Flag == 1){
while(Hid_Read() == 0)
{
 //CheckAlarm();              //check for alarm trigger while waiting for usb communication
}

//^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
```

```
//READ DATA FROM USB AND STORE IN EEPROM AS PHONE NUMBER AND
LOCATION USING 20BYTES PER PERSON(0-19;20-39;40-59)
//^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
  ///*
 //get the address of phone number to store in EEPROM. 1= location 0; 2= loc1, 10 = loc9
  //by 20 for other parameters plus phone number
  address_hold = Read_Buffer[11];
  address_hold = address_hold - 48;          // convert ascii to decimal value

 if(Read_Buffer[12] == 'U'){
  //update button response
  for(k=0; k<12; k++){
   // GIE_bit = 0;
     EEPROM_Write(address, Read_Buffer[k]);
     address++;
     Delay_ms(50);    //crucial delay to avoid EECON clash
  }
    //GIE_bit = 1;
    Write_Buffer[60]  = 1;       //notify application that database is updated
    while(!HID_Write(&Write_Buffer,64));
    clear_buffer(Write_Buffer);
   Delay_ms(1000);
 }

else if(Read_Buffer[12] == 'R') {                 //Respond to retrieve button only
 //Retrieve button response
 if(Read_Buffer[13] == 0){                     //if checkbox not checked
    RetrieveData();
 }
 else if(Read_Buffer[13] == 1){                 //ckeckbox checked to list all data
      Read_Buffer[11] = 0;

     do{
       address_hold = Read_Buffer[11];
```

```
      address_hold = address_hold * 20;
      address = address_hold;
      RetrieveData();
      Read_Buffer[11] = Read_Buffer[11]+1;      //repeat listing
    }while(Read_Buffer[11] < 4);
  }
 }
 if(PIR2.USBIF == 0)USB_Connected_Flag = 0;   //
}
else{
  RE0_bit = ~RE0_bit;
  Delay_ms(500);
}
goto loop_second;
 Delay_ms(1000);
Hid_Disable();
}
```

APPENDIX G

EMBEDDED-C- LANGUAGE CODE FOR CLIENT STATION RESPONSE

```
#define GSM_OK  7

sbit LED_PWR at RD7_bit;
sbit LED_RX at RD6_bit;
sbit LED_TX at RD5_bit;

sbit RELAY   at  RB3_bit;           //DVR power


unsigned char FLAG,gsm_state, responseCmd, tmp,i = 0;

unsigned char txt[6];
unsigned char len_txt[9];
unsigned char txt1[6]="32769";
sbit responseOK at FLAG.B0;

unsigned int len, balance = 0;


void interrupt(void){

    if(RCIF_bit == 1){
      tmp = UART1_Read();
      switch (gsm_state) {
     case  0: {

             if (tmp == '*')               // We have '*', it could be "correct cmd"
               gsm_state = 1;

             break;
            }
```

```
case  1: {
        if (tmp == '*') {

          gsm_state = 2;
        }
        else
          gsm_state = 0;
        break;
       }
case 2: {
        if (tmp == 'C') {
           gsm_state = 3;
        }
        else
           gsm_state = 0;
          break;
        }

case 3: {
        if (tmp == 'L'){
          gsm_state = 4;
          //gsm_state = 0;
        //  responseCmd = 1;
        }

        else
          gsm_state = 0;
        break;
       }
case 4: {
        if (tmp == '1') {
          gsm_state = 5;
        }
        else
```

```
            gsm_state = 0;
           break;
          }

    case 5: {
           if (tmp == '*')
            gsm_state = 6;
           else
            gsm_state = 0;
           break;
          }
    case 6: {
           if (tmp == '*' )
            gsm_state = 0;
            responseCmd = 1;                    //**CL1** found.
           break;
          }
       default: {
           gsm_state = 0;
          }
   }
}
}

void main() {

  PORTD = 0;
  PORTC = 0;
  PORTB = 0;
  PORTA = 0;

  TRISD = 0;
  TRISC = 0;
  TRISC.B7 = 1;
```

```
TRISB = 0;
TRISA = 0b00000111;

ADC_Init();

UART1_Init(9600);
Delay_ms(5000);

UART1_Write_Text("AT");
UART1_Write(0x0D);
UART1_Write(0x0a);
Delay_ms(1000);

UART1_Write_Text("ATE0");
UART1_Write(0x0D);
UART1_Write(0x0a);
Delay_ms(2000);
//LED_PWR = 1;


    UART1_Write(0x0D);
    UART1_Write(0x0A);
     Delay_ms(5000);


 UART1_Write_Text("ATH");
 UART1_Write(0x0D);
 UART1_Write(0x0A);
 Delay_ms(1000);

 UART1_Write_Text("AT+CLIP=1");
 UART1_Write(0x0D);
 UART1_Write(0x0A);
 Delay_ms(1000);
```

```
UART1_Write_Text("AT+CMGF=1");
UART1_Write(0x0D);
UART1_Write(0x0a);
Delay_ms(1000);
UART1_Write_Text("AT+CPMS=\"SM\"");
UART1_Write(0x0D);
UART1_Write(0x0a);
Delay_ms(1000);

UART1_Write_Text("AT+CNMI=1,2,0,0,0");
UART1_Write(0x0D);
UART1_Write(0x0a);
Delay_ms(1000);

responseCmd = 0;

  UART1_Write_Text("AT+CMGL=\"ALL\"");
UART1_Write(0x0D);
UART1_Write(0x0a);
Delay_ms(1000);

     GIE_bit  = 1;
     Delay_ms(200);

     UART1_Write_Text("AT");
     UART1_Write(0x0D);
     UART1_Write(0x0A);
     //wait for OK and break

 while(1){
       //UART1_Write_Text("AT+CMGL=\"ALL\"");
      UART1_Write_Text("AT+CMGR=1");
        UART1_Write(0x0D);
```

```
            UART1_Write(0x0A);
            Delay_ms(1000);

      if(responseCmd){

        responseCmd = 0;

        Delay_ms(500);

        RELAY = 1;                  //power recording
        Delay_ms(10000);
        RELAY = 0;

        UART1_Write_Text("AT+CMGD=1,4");
        UART1_Write(0x0D);
        UART1_Write(0x0A);
        Delay_ms(1000);
      }
    }
}
```

APPENDIX H

SOURCE CODE IN VB.NET FOR CONTROL STATION INTERFACE TO PC

’Application for Base Station interface to PC terminal

```
Imports System
Imports System.Threading
Imports System.Runtime.InteropServices

Module HIDDLLInterface
    ' this is the interface to the HID controller DLL - you should not
    ' normally need to change anything in this file.
    '
    ' WinProc() calls your main form 'event' procedures - these are currently
    ' set to..
    '
    ' MainForm.OnPlugged(ByVal pHandle as long)
    ' MainForm.OnUnplugged(ByVal pHandle as long)
    ' MainForm.OnChanged()
    ' MainForm.OnRead(ByVal pHandle as long)

    ' HID interface API declarations...
    Declare Function hidConnect Lib "mcHID.dll" Alias "Connect" (ByVal pHostWin
As Integer) As Boolean
    Declare Function hidDisconnect Lib "mcHID.dll" Alias "Disconnect" () As
Boolean
    Declare Function hidGetItem Lib "mcHID.dll" Alias "GetItem" (ByVal pIndex
As Integer) As Integer
    Declare Function hidGetItemCount Lib "mcHID.dll" Alias "GetItemCount" () As
Integer
    Declare Function hidRead Lib "mcHID.dll" Alias "Read" (ByVal pHandle As
Integer, ByRef pData As Byte) As Boolean
    Declare Function hidWrite Lib "mcHID.dll" Alias "Write" (ByVal pHandle As
Integer, ByRef pData As Byte) As Boolean
    Declare Function hidReadEx Lib "mcHID.dll" Alias "ReadEx" (ByVal pVendorID
As Integer, ByVal pProductID As Integer, ByRef pData As Byte) As Boolean
    Declare Function hidWriteEx Lib "mcHID.dll" Alias "WriteEx" (ByVal
pVendorID As Integer, ByVal pProductID As Integer, ByRef pData As Byte) As
Boolean
    Declare Function hidGetHandle Lib "mcHID.dll" Alias "GetHandle" (ByVal
pVendoID As Integer, ByVal pProductID As Integer) As Integer
    Declare Function hidGetVendorID Lib "mcHID.dll" Alias "GetVendorID" (ByVal
pHandle As Integer) As Integer
    Declare Function hidGetProductID Lib "mcHID.dll" Alias "GetProductID"
(ByVal pHandle As Integer) As Integer
    Declare Function hidGetVersion Lib "mcHID.dll" Alias "GetVersion" (ByVal
pHandle As Integer) As Integer
    Declare Function hidGetVendorName Lib "mcHID.dll" Alias "GetVendorName"
(ByVal pHandle As Integer, ByVal pText As String, ByVal pLen As Integer) As
Integer
    Declare Function hidGetProductName Lib "mcHID.dll" Alias "GetProductName"
(ByVal pHandle As Integer, ByVal pText As String, ByVal pLen As Integer) As
Integer
    Declare Function hidGetSerialNumber Lib "mcHID.dll" Alias "GetSerialNumber"
(ByVal pHandle As Integer, ByVal pText As String, ByVal pLen As Integer) As
Integer
```

```
    Declare Function hidGetInputReportLength Lib "mcHID.dll" Alias
"GetInputReportLength" (ByVal pHandle As Integer) As Integer
    Declare Function hidGetOutputReportLength Lib "mcHID.dll" Alias
"GetOutputReportLength" (ByVal pHandle As Integer) As Integer
    Declare Sub hidSetReadNotify Lib "mcHID.dll" Alias "SetReadNotify" (ByVal
pHandle As Integer, ByVal pValue As Boolean)
    Declare Function hidIsReadNotifyEnabled Lib "mcHID.dll" Alias
"IsReadNotifyEnabled" (ByVal pHandle As Integer) As Boolean
    Declare Function hidIsAvailable Lib "mcHID.dll" Alias "IsAvailable" (ByVal
pVendorID As Integer, ByVal pProductID As Integer) As Boolean

    ' windows API declarations - used to set up messaging...

    Public Declare Function CallWindowProc Lib "user32" Alias "CallWindowProcA"
(ByVal lpPrevWndFunc As Integer, ByVal hwnd As Integer, ByVal Msg As Integer,
ByVal wParam As Integer, ByVal lParam As Integer) As Integer
    Public Declare Function SetWindowLong Lib "user32" Alias "SetWindowLongA" _
                                          (ByVal hwnd As Integer, ByVal nIndex
As Integer, ByVal dwNewLong As Integer) As Integer

    Delegate Function SubClassProcDelegate(ByVal hwnd As Integer, ByVal msg As
Integer, ByVal wParam As Integer, ByVal lParam As Integer) As Integer
    Public Declare Function DelegateSetWindowLong Lib "USER32.DLL" Alias
"SetWindowLongA" _
                                           (ByVal hwnd As Integer, ByVal attr
As Integer, ByVal lval As SubClassProcDelegate) As Integer


    ' windows API Constants
    Public Const WM_APP As Integer = 32768
    Public Const GWL_WNDPROC As Short = -4

    ' HID message constants
    Private Const WM_HID_EVENT As Decimal = WM_APP + 200
    Private Const NOTIFY_PLUGGED As Short = 1
    Private Const NOTIFY_UNPLUGGED As Short = 2
    Private Const NOTIFY_CHANGED As Short = 3
    Private Const NOTIFY_READ As Short = 4

    ' local variables
    Private FPrevWinProc As Integer ' Handle to previous window procedure
    Private FWinHandle As Integer ' Handle to message window
    Private Ref_WinProc As New SubClassProcDelegate(AddressOf WinProc)
    Private HostForm As Object

    ' Set up a windows hook to receive notification
    ' messages from the HID controller DLL - then connect
    ' to the controller
    Public Function ConnectToHID(ByRef targetForm As Form) As Boolean
        Dim pHostWin As Integer = targetForm.Handle.ToInt32
        FWinHandle = pHostWin
        pHostWin = hidConnect(FWinHandle)
        FPrevWinProc = DelegateSetWindowLong(FWinHandle, GWL_WNDPROC,
Ref_WinProc)
        HostForm = targetForm
    End Function

    ' Unhook from the HID controller and disconnect...
    Public Function DisconnectFromHID() As Boolean
        DisconnectFromHID = hidDisconnect
        SetWindowLong(FWinHandle, GWL_WNDPROC, FPrevWinProc)
    End Function
```

```
    ' This is the procedure that intercepts the HID controller messages...

    Private Function WinProc(ByVal pHWnd As Integer, ByVal pMsg As Integer,
ByVal wParam As Integer, ByVal lParam As Integer) As Integer
        If pMsg = WM_HID_EVENT Then
            Select Case wParam

                ' HID device has been plugged message...
                Case Is = NOTIFY_PLUGGED
                    HostForm.OnPlugged(lParam)

                    ' HID device has been unplugged
                Case Is = NOTIFY_UNPLUGGED
                    HostForm.OnUnplugged(lParam)

                    ' controller has changed...
                Case Is = NOTIFY_CHANGED
                    HostForm.OnChanged()

                    ' read event...
                Case Is = NOTIFY_READ
                    HostForm.OnRead(lParam)
            End Select

        End If

        ' next...
        WinProc = CallWindowProc(FPrevWinProc, pHWnd, pMsg, wParam, lParam)

    End Function
End Module
```