Web Based Surveillance System in Nigeria
Osodeke Charles Efe, Prof. Gloria Chukwudebe, Dr. Emmanuel Ekwonwune, Oladimeji Biodun S.

Department of Computer Science, Imo State University Owerri Imo State Nigeria,
Dean School of Computing and Information Science, Federal University of Technology Owerri,
Department of Computer Science, Imo State University Owerri,
PhD. Student Department of Computer Science, Imo State University Owerri Imo State Nigeria.

ABSTRACT: This work was motivated by the fact that the technology used by thieves and robbers for stealing in our society has improved exponentially, hence the need for the surveillance techniques to also improve with the changing technology. Thus, that has led to the design of sophisticated Video Surveillance System. The objective of this study is to design model video surveillance software that will monitor the firms day-to-day activities alert the system administration of suspicious action and generate a comprehensive report of all day to day activities of the firm. The methods used to gather data are the observation and interview methods, which were guided by software engineering methodology called Structural System Analysis and Designed Method (SSADM). We succeeded in designing model software for video surveillance system, capable of monitoring a system.

KEYWORDS: surveillance, data surveillance, surveillance, detection, Biometric, etc

I INTRODUCTION
Surveillance is the monitoring of the behaviour, activities, or other changing information, usually of people for the purpose of influencing, managing, directing, or protecting them. This can include observation from a distance by means of electronic equipment or interception of electronically transmitted information; and it can include simple, relatively no- or low-technology methods such as human intelligence agents.

The word surveillance comes from a French phrase for "watching over"; "sur" means "from above" and "veiller" means "to watch".

The objective of most video surveillance systems was originally security, however in practice they are being used for other purposes. Video Surveillance System is motion detection software that monitors your home, office, or any premise. The system records action triggered by motion or noise as it happens. You can view activities monitored by your camera. Video surveillance technology is not as expensive or difficult to acquire as it used to be. A new trend in video surveillance is driving down the price even further. Now you can transform your webcam and personal computer into a fully functioning video surveillance system simply by configuring the Motion Detection Software. The system will send immediate message notification along with a photo directly in your system as soon as motion or noise intrusion is detected. You can customize alerts like video and audio recording, taking snaps with date and time, sounding alarms etc. Automatically upload recorded video, audio and snaps to the server.

Surveillance is very useful to governments, Schools and law enforcement to maintain social control, recognize and monitor threats, and prevent/investigate criminal activity. With the advent of programs such as the Total Information Awareness program, technologies such as high speed surveillance computers and biometrics software, and laws such as the Communications Assistance For Law Enforcement Act, governments now possess an unprecedented ability to monitor the activities of their subjects.

However, many civil rights and privacy groups, such as the Electronic Frontier Foundation and American Civil Liberties Union, have expressed concern that by allowing continual increase in government surveillance of citizens we will end up in a mass surveillance society, with extremely limited, or non-existent political and/or personal freedom. Fears such as this have led to numerous lawsuits.

Surveillance cameras are video cameras used for the purpose of observing an area. They are often connected to a recording device or IP network, and may be watched by a security guard or law enforcement officer. Cameras and recording equipment used to be relatively expensive and required human personnel to monitor camera footage, but analysis of footage has been made easier by automated software that organizes digital video footage into a searchable database, and by video analysis software (such as VIRAT and HumanID). The amount of footage is also drastically
reduced by motion sensors which only record when motion is detected. With cheaper production techniques, surveillance cameras are simple and inexpensive enough to be used in home security systems, and for everyday surveillance.

II SIGNIFICANCE OF STUDY

The current CCTV (Surveillance system) use in Nigeria is a standalone system; which means if you get hold of the system you can destroy the files. This means that if a suspect or a criminal locates the source or location of the system; he or she can destroy the system and there will be no evidence to as who, when and how the crime was committed. The system design is very expensive for the lower class income earners. With the present CCTV the amount of acquisition, installation and maintenance is on the high side for an average Nigeria who hardly receive his or her salary at the end of the month. So there is need to upgrade to a cheaper and better platform.

The introduction of Video surveillance with web storage application system in the security system of Nigeria will go a long way to overcome the security issues facing most organizations in Nigeria. However, there are many wonderful reasons to consider a video surveillance system in your environment; this include:

1. Reduce and prevent theft
2. It carries out real time monitoring
3. Resolve Business disputes
4. Provides evidence for investigation
5. it leads to employees productivity, etc

III LITERATURE REVIEW

This chapter explains Video Surveillance, Surveillance, motion detection and object monitoring systems. It review other authors work on surveillance system. Until the mid-eighties, the deployment of CCTV systems had largely been limited to private spaces (Hempel 2001)[7]. The appearance of these systems in settings typically considered ‘public’ is a more recent phenomenon; and, it is one which occurred with considerable alacrity in many countries. A diverse array of aims and objectives have motivated the introduction of CCTV into public spaces including: public safety, deterrence, enhanced detection and increased response times. In the contemporary context, the predominant uses of CCTV in public spaces are in the management of risks, traffic jams, fire, accidents and crime prevention (Hempel 2001).

Video surveillance or closed-circuit television (CCTV) has become widely used in many parts of the world. Although its potential applications include detecting, investigating, and reducing fear of crime, empirical research has mainly focused on its use in crime prevention (Welsh & Farrington, 2008)[19]. The most frequently cited mechanism through which video surveillance may deter crime is its potential effect on the perceived certainty of punishment (Piza, Caplan, Kennedy, & Gilchrist, 2015)[13]. However, there are methodological problems associated with demonstrating a causal relationship between surveillance cameras and crime (Stutzer & Zehnder, 2013)[1]. It requires, among other things, the use of a control condition to estimate the counterfactual situation in which video surveillance was not introduced. Unfortunately, evaluations of public area surveillance interventions have often used weak research designs, sometimes lacking controls entirely (Welsh, Peel, Farrington, Elffers, & Braga, 2011)[18].

IV ORIGIN OF SURVEILLANCE

In recent years, with the latest technological advancements, off-the-shelf cameras became vastly available, producing a huge amount of content that can be used in various application areas. Among them, visual surveillance receives a great deal of interest nowadays. Until recently, video surveillance was mainly a concern only for military or large-scale companies. However, increasing crime rate, especially in metropolitan cities, necessitates taking better precautions in security-sensitive areas, like country borders, airports or government offices. Even individuals are seeking for personalized security systems to monitor their houses or other valuable assets.

Old-fashioned security systems were vastly relying on human labour instead of system hardware. As a result, detection and assessment of threat was limited with the concentration of the human operator. Additionally, area under surveillance may be too large to be monitored by a few operators and number of cameras may exceed their monitoring capability. This situation forces the use of more personnel, which makes it even a more expensive task in an era of technological equipment’s’ being much cheaper than the human resource.
The sole answer for this increasing demand for personal and societal security is automation. The vast amount of data acquired from video imagery should be analyzed by an intelligent and useful autonomous structure. This intelligent system should have the capacity to observe the surrounding environment and extract useful information for subsequent reasoning, like detecting and analyzing the motion, or identifying the objects entering the scene. Besides, monitoring should be done 24-hours-a-day, without any interruption. This sort of a system will achieve the surveillance task more accurately and effectively, saving a great amount of human effort.

V VIDEO SURVEILLANCE

Video surveillance applications are interested in the real-time observation of humans or vehicles in some environment (indoor, outdoor, or aerial), leading to a description of the activities of the objects within the environment. A complete video surveillance system typically consists of foreground segmentation, object detection, object tracking, human or object analysis, and activity analysis.

KidRooms [1996][10] surveillance is a tracking system based on “closed world regions.” These are regions of space and time in which the specific context of what is in the regions is known. These regions are tracked in real-time domains where object motions are not smooth or rigid and where multiple objects are interacting. It was one of the first multi-persons; fully automated, interactive, narrative environment ever constructed using non-encumbering sensors.

Rehg et al. [1997][9] developed Smart Kiosk to detect and track people in front of a kiosk. It uses both colour information, face detection, and stereo information for detection. However, when people are very close to the kiosk, it can only track a single person.

Olson[2011][17] developed a general purpose system for moving object detection and event recognition. They detected moving objects using change detection and tracked them using first-order prediction and nearest-neighbour matching. It is designed for indoor surveillance and it cannot handle small motions of background objects. It is a single person tracking system.

The distributed surveillance system consists of a collection of mobile and stationary sensor systems designed to detect, classify and track moving objects in the environment in real-time. Object Video VEW (Video Early Warning) product detects objects in real-time video and determines basic activity information such as object type (human, vehicles, etc) object trajectory, and interactions with other objects. Recently, Duque et al. [2007][3] presented a video surveillance system (OBSERVER) that detects and predicts abnormal behaviours aiming at the intelligent surveillance concept.

VI TYPES OF SURVEILLANCE

A COMPUTER SURVEILLANCE

The vast majority of computer surveillance involves the monitoring of data and traffic on the Internet. In the Nigeria for example, under the Nigeria Communication Commission Act, all phone numbers are required to be available for unimpeded real-time monitoring by Federal law enforcement agencies.

There is far too much data on the Internet for human investigators to manually search through all of it. So automated Internet surveillance computers sift through the vast amount of intercepted Internet traffic and identify and report to human agents.

Computers can be a surveillance target because of the personal data stored on them. If someone is able to install software, such as the FBI's Magic Lantern and CIPAV, on a computer system, they can easily gain unauthorized access to this data. Such software could be installed physically or remotely.

B TELEPHONE SURVEILLANCE

The official and unofficial tapping of telephone lines is widespread. In Nigeria for instance, the Nigeria Communication Commission (NCC) requires that all telephone and VoIP communications be available for real-time wiretapping by Federal law enforcement and intelligence agencies.

Human agents are not required to monitor most calls. Speech-to-text software creates machine-readable text from intercepted audio, which is then processed by automated call-analysis programs.
Law enforcement and intelligence services in the United Kingdom and the United States possess technology to activate the microphones in cell phones remotely, by accessing phones’ diagnostic or maintenance features in order to listen to conversations that take place near the person who holds the phone. Mobile phones are also commonly used to collect location data. The geographical location of a mobile phone (and thus the person carrying it) can be determined easily even when the phone is not being used, 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.

C    CAMERA SURVEILLANCE

Surveillance cameras are video cameras used for the purpose of observing an area. They are often connected to a recording device or IP network, and may be watched by a security guard or law enforcement officer. Cameras and recording equipment used to be relatively expensive and required human personnel to monitor camera footage, but analysis of footage has been made easier by automated software that organizes digital video footage into a searchable database, and by video analysis software.

![Surveillance Camera](source: Gil-Jiménez P.,2007)[6]

D    BIOMETRIC

Biometric surveillance is any technology that measures and analyzes human physical and/or behavioural characteristics for authentication, identification, or screening purposes. Examples of physical characteristics include fingerprints, DNA, and facial patterns. Examples of mostly behavioural characteristics include gait (a person's manner of walking) or voice.

Facial recognition is the use of the unique configuration of a person's facial features to accurately identify them, usually from surveillance video.

Another form of behavioural biometrics, based on affective computing, involves computers recognizing a person's emotional state based on an analysis of their facial expressions, how fast they are talking, the tone and pitch of their voice, their posture, and other behavioural traits. This might be used for instance to see if a person is acting "suspicious.

Facial thermographs are in development, which allow machines to identify certain emotions in people such as fear or stress, by measuring the temperature generated by blood flow to different parts of their face. Law enforcement officers believe that this has potential for them to identify when a suspect is nervous, which might indicate that they are hiding something, lying, or worried about something.

E    CORPORATE SURVEILLANCE

Corporate surveillance is the monitoring of a person or group's behaviour by a corporation. According to the American Management Association and the ePolicy Institute that undertake an annual quantitative survey about electronic monitoring and surveillance with approximately 300 U.S. companies, “more than one fourth of employers have fired workers for misusing e-mail and nearly one third have fired employees for misusing the Internet”. More than 40% of the companies monitor e-mail traffic of their workers, and 66% of corporations monitor
Internet connections. In addition, most companies use software to block non-work related websites such as sexual or pornographic sites, game sites, social networking sites, entertainment sites, shopping sites, and sport sites.

VII SOUSVEILLANCE

This is the practice of avoiding surveillance or making surveillance difficult. Developments in the late twentieth century have caused counter surveillance to dramatically grow in both scope and complexity, such as the Internet, increasing prevalence of electronic security systems, high-altitude (and possibly armed), large corporate and government computer databases.

sousveillance is the practice of the reversal of surveillance on other individuals or groups. Counter-surveillance can be used in applications to prevent corporate spying or to track other criminals by certain criminal entities. It can also be used to deter stalking methods used by various entities and organizations.

sousveillance is inverse surveillance, involving the recording by private individuals, rather than government or corporate entities.

VIII SOUSVEILLANCE CASES

According to the United Nations Interregional Crime and Justice Research Institute Imrohoroglu et al. (2006)[2], people victimized by property crime (as a % of the total population) varied between 14.8% in New Zealand to 12.7% in Italy, 12.2% in U.K., 10% in U.S., 3.4% in Japan and 31.7% in Nigeria. The possible explanations for cross country differences are many, ranging from distinct definitions of crimes and different reporting rates (percentage of the total number of crimes actually reported to the police), to real differences in the incidence of crime and even to different cultural aspects. It can even be contributed to democracy as explained by Lin (2007)[8], whereby compared to non-democratic governments, democratic government punish major (minor) crime more (less) and hence this crime rate is lower (higher).

No matter how we look at it, it is still an utmost important subject due to its large impact on a psychological aspect as well as economical aspect. Its pernicious effects on economic activities and more generally on the quality of life of people contribute to the emerging fact that crime is merging as a priority in policy agendas worldwide. The relationship between crime and development is a very crucial economic issue. Crime can hinder growth in a country. Higher crime rates have been found to reduce both domestic and foreign investment (Boba, R. 2005)[14] and have been linked to lower job creation and sales growth (Skogan 1984)[15]. Due to the complexity of the phenomenon and lack of consensus among policy makers or scholars, research on this issue continues to be conducted in many areas.

A. OWERRI ZENITH BANK ROBBERY

The armed robbers trailed a customer who came in to deposit a huge sum of money to the Zenith bank branch located along Wetheral Road, opposite Dan Anyiam Stadium in the owerrri city of imo state. On reach, the robbers engaged in a gun battle with police as they shot aimlessly. One of the thieves was gunned down when he tried entered the gate post.

The thieves try to make away with the money but engaged with the Police in a shootout. On Arrival, the operatives engaged the four armed robbers that arrived the bank with an ash colour Toyota Camry in a shootout. At the end of the shootout, three Police men sustained various degrees of gunshot injuries.

It was with the help of the cctv camera the police were able to trace the thieves and were eventually apprehended. (Naijanews, 2017)[11]

B. OFFA ROBBERY CASE

Robbers attacked two banks and a police station, killing 15 people including nine police officers in Offa, central Nigeria.

Late Thursday afternoon, “a gang of robbers’ invaded police and bank headquarters in Offa,” Ajayi Okasanmi, police spokesman in Kwara State, told AFP.

He added that the police officers had been attacked by surprise, without however detailing the precise circumstances under which the victims had been killed.
With the help of the cctv camera, it was observed that it would have been worse if the police had retaliated forcefully, but we would have endangered the lives of civilians at the scene of the attacks, in the commercial district of Offa, a locality of about 100,000 inhabitants in Kwara State. (Newsexpress, 2018)[12]

C HOUSE HELPS: WEIGHING THE ODDS

Usually, a married woman, especially one that works in an office or far from home, starts toying with the idea of engaging the services of a house-help when she becomes a mother. As the babies arrive one after the other and she is also saddled with the never-ending household chores, her predicament stares her squarely in the face. Her maternity leave is over and she has to resume work, but there is no help in sight, then she begins to grasp the full import of the saying that “a good housemaid is like gold.”

Generally, it is many women’s ardent desire to excel both at the home front and in their careers. And so, they strive to put in their very best in these two areas. But realistically, it is not an easy thing for a woman to maintain a clean house, care for the children and then perform optimally in her career. With modern-day living and all its possible and impossible demands, it could be a herculean task combining all these and desiring to come up tops.

So, in tackling this knotty issue, families have devised various methods suitable to their circumstances and needs. While some have resorted to engaging the services of house-helps, albeit reluctantly, others, who feel uncomfortable with the idea of harbouring a total stranger all in the name of a helper, have sought to overcome the challenge employing other tactics. These could be in the form of having relatives live with them. But in the situation, where this is not available, it poses a huge problem. More often than not, however, people opt to settle for house-helps, who would be easy to control, as their services are paid for.

Interestingly, engaging the services of a house-help is not always a fallout of urgent necessity. To some people, the idea has come to be viewed as a sort of status symbol; to show that the family is buoyant enough to afford such luxury or that ‘madam has arrived.’ In such cases, the madam in question merely uses the house-help as an escort when attending public functions, whereby she walks elegantly into a gathering with the house-help in tow, carrying the baby and her bags.

But like everything else in life, the act of engaging the services of house-helps brings in its trail certain advantages and disadvantages. While some women feel that the disadvantages far outweigh the advantages and would thus go to any length to avoid hiring house-helps and somehow find a way to cope, others just cannot do without them.

To this category of women, it is far better to condone the excesses and vices associated with house-helps than suffer the pains. In recent time, however, there have been growing concerns over the threat some house-helps pose to families, especially the little children in the household. There is an increase in the rate at which some house-helps reportedly unleash terror, brutality and hatred, leading to distrust and insecurity on the part of their employers. Events happening around reveal that many families, especially mothers, whether single or otherwise, have today lost their sleep, privacy, properties, children and other valuables to sheer negligence or nonchalant attitude of maids. (Guardian, 2015)[5]

IX KNOW THE ENEMY

Security pros should take a moment to re-think their assumptions about their facility's enemies. Don't overlook the obvious. Don't spend too much time on the esoteric. Shake up your thinking to improve threat assessments and subsequent response planning. Security novices should also remember to take the time to understand the various enemies they could be facing. Planning effectively depends on knowing who you're up against.

According to Stephen (2002)[16] do you know who your enemies are? When setting up security plans, do you envision fighting off groups of armed international terrorists? If so, you may be making a big mistake. You're more likely to face threats closer to home, and your security plans will be flawed until you know your enemies.

Whether experienced in threat assessments and security planning or not, it's impossible to mount an effective defense without knowing the enemy. Following is a guide to the five broad categories of aggressors, a “rogue's gallery of bad guys” who may be targeting a facility. Their acts can range from crimes such as burglary, embezzlement or fraud, to “low-intensity conflict threats” such as unconventional warfare.
A CRIMINALS

Consider criminals by their degree of sophistication: unsophisticated, sophisticated and organized groups. While they share the common objective of stealing valuable assets, what they target, the quantities they seek, their efficiency and the finesse of their actions vary significantly. In some cases, vandals and activists may be included under this category.

B VANDALS AND ACTIVISTS

While the degree of damage they seek to cause will vary with their sophistication and motivation, they typically cause destruction to achieve publicity, notoriety and a reputation. These groups are typically made up of protesters who are politically or issue-oriented. They may act out of frustration, discontent or anger against the actions or stated position of a company in regard to a particular issue. They may also be acting for or against other social or political groups. Their selection of targets will vary based on the risk associated with attacking them.

C EXTREMISTS

Often fanatical in their political beliefs, extremists take radical, violent actions to gain support for their beliefs or causes.

D PROTESTERS

This group is considered a threat only when violent. While lawful protests are a fact of life, protesters must be taken into account in security planning and threat assessments. Typically, significant protective measures beyond basic crowd control are not normally needed to address their actions. However, there is the possibility that extremists or vandals/activists in the crowd will incite violence.

E TERRORISTS

As recent events illustrate, terrorists are almost always ideologically, politically or issue-oriented. They commonly work in small, well-organized groups (cells). They are sophisticated, skilled with tools and weapons and possess an efficient planning capability.

X CRIMINOLOGICAL THEORY AND ITS APPLICATION TO VIDEO SURVEILLANCE

According to the routine activity theory of criminology, criminal incidents occur when three spheres converge. The three factors that are necessary to enable prohibited behaviour are:
1. The motivated offender
2. a suitable target, and
3. Absence of a capable guardian.

In the Nigeria Security system, the offender exists as a result of religious or political ideology. Preventing the motivated offender becomes a huge undertaking that involves the tireless efforts of diplomats, mediators and religious leaders. In crime control, minimizing the potential for motivated offenders requires social service intervention. Drug and alcohol rehabilitation, anger management, behavioural modification, employment services, etc. become issues that the broad-thinking criminal justice professional must engage in order to reduce the number of motivated offenders. Unlike the intangible ideologies and the social service concerns, reducing suitable targets can be an observed accomplishment. Hardening potential targets usually requires changing the physical structure or improving the visible security measures surrounding the structure. The number of critical infrastructure locations continues to multiply and the cost of hardening the targets is astronomical. Since the process of target-hardening is a never-ending process, the likelihood of reasonably reducing the number of suitable targets remains slim.

Capable guardianship endures as the sphere that public safety professionals can influence most effectively and efficiently. This particular realm of the routine activity theory purports that communities possessing active oversight tend to be victimized by less criminal activity. Capable guardianship within the neighbourhoods of our cities has been left to the supervision provided by parents, concerned adults and law enforcement. Technological advances have dramatically changed the capable guardian sphere for Nigeria security threats. CCTV surveillance of public areas can supplement or possibly replace human supervision in the terrorist prevention model.

Most criminologists assert that the pool of motivated offenders will always exist and that attention needs to be directed towards minimizing suitable targets for crime and increasing the level of capable guardianship. The cost and success of hardening the variety of potential terrorist targets can make the mission of neutralizing this sphere unreasonable. This
The author presents the belief that the most effective and efficient manner of exercising the routine activities theory of criminology to Nigeria security is by using CCTV surveillance as capable guardianship.

**XI CONCLUSION**

In order to have effective surveillance system, several methods have been proposed and developed by many researchers. During our survey it is seen that Nigerian are still working with standalone surveillance system and this is associate with the problem of accessing your properties or evaluating your employees in your absence. Web based surveillance system is considered to be the most effective method of surveillance; which means with or without your presence the system will function effectively

Compare to the normal CCTV system; if a suspect have access to the system since is a standalone it is possible to destroy the evidence or the system. Web based surveillance system is hereby recommended for safety of human, data and properties.

**REFERENCES**

[8] Hsu-Fen Lin (2007); Knowledge sharing and firm innovation capability: an empirical study
[11] Naijanews (2017); Chilling CCTV Footage of the Zenith Bank Owerri Robbery Attack That Left 5 People Dead Surfaces
[16] Stephen Bungay (2002); Knowing Your Enemy: Information and Commitment Problems in Civil Society