Application of Information and Communication Technology (ICT) in Curbing Insecurity Challenges in Nigeria.

Engr. Ibrahim M.I[1], Nura T.A[2], Ibrahim M[3], Ibrahim A[4]
[1, 3, 4] Computer Science Department
[2] Innovation Technology Department
[1, 2, 3,4] Jigawa State Institute of Information Technology, Kazaure.
[1]Email: ibrahimq7@gmail.com, Mobile: 08137167587.

ABSTRACT

This write-up would explores and dwell on modern techniques in which information and communication technology (ICT) can play a role in curbing insecurity in Nigeria. IT Governance, is the first step towards tackling insecurity in the country. The text will also highlight causes of the insecurity, modern IT enable solutions, services, tools and techniques such as surveillance technology, biometrics, data mining and profiling. If the nation would adopt these modern techniques and fully implement IT services in all sectors of economy, the challenges of all forms of insecurity such as kidnapping, insurgency, child trafficking and abuses, militancy, corruptions, armed robbery or unemployment would be reduced to minimal.

Key words: IT governance, Insecurity, Nigeria, Surveillance, Biometrics, Data mining

1. BACKGROUND TO THE STUDY:

The incessant challenges of insecurity has been claiming precious lives of citizenry over the years, the state of insecurity in the country is becoming worrisome. Felonies have rocks every geo-political zones of the nation with different act of crimes of militancy, kidnapping, armed robbery and insurgency (Hassan & Kabiru, 2013), despite various efforts by the government to reduce the menace.
The use of information and communication technology (ICT) in the provision of solution to human, social and industrial challenges has proven success in many places on this earth and therefore, this country should not be an exception. The recent installed surveillance cameras in Lagos and Abuja to monitored criminal acts, has not been successful due to the lack of underlying national ICT backbone infrastructure that would support the technology, poor positioning of the devices in the architectural design, above all analog system, instead of IP surveillance system.

1.1 Statement Of Problem:

Traditionally, we relied on intelligence gathering by government security agents (police, SSS, civil defense or soldiers), strict physical security at vulnerable facilities by security guards, vigilance on the part of citizens, which are grossly inadequate in tackling the current insecurity challenges. The solution to the nation's insecurity challenges lies in technologies implementation such as IP based surveillance, biometrics, data mining and profiling in relevant parastatals and government agencies to checkmate militancy and other criminal acts in the country.

1.2 Research Objective:

The objective of the study is to review the pervasive insecurity challenges in Nigeria, analyses of the trends and causes of incidences. It also analyses the key design consideration of an IP surveillance technology through the development of a prototype system.

2. METHODOLOGY:

In this research method, pre-existing data is going to be used and instruments that the researchers used to collect data include observations and document analysis from journal, report, articles, newsletters and diaries (Strauss & Corbin, 1998), in this approach, the data is in descriptive nature.
ConceptDraw and Edraw software's custom library will be use to design and defined the requirements of resilient IP surveillance system model that could be implemented and configured across the country. Particularly, most affected regions where insurgents, militants, kidnapping activities were prevalent.

2.1 Reviewed Work:

Information and communication technology is an excellent tool that can be used to monitor unlawful activities, nab criminals or impede them on their pathway (Ikeogu, 2014). With the aid of forensic detective tools when an individual perpetrate crime, the security analyst and law enforcement agents could use detective ICT tools to know who perpetrated a crime when where and how ?
An IP surveillance system is one of the technology that could be placed at strategic street junctions, public places such as shopping mall, religious centers, viewing centers, schools, hospitals, public houses and even recreational centers. In this study we will demonstrate a typical scenario of an IP based surveillance system that can be configured in strategic areas.

The surveillance technology provides means of monitoring the behavior of people for the purpose of influencing, managing or protecting them (David, 2007), it is very useful in maintaining social control, recognizing or monitoring crime scene and assisting in investigating criminals and insurgents activities, this makes it possible for security agencies to combat crime in real time.

Information and communication technology when properly deploy and adopt can provide solutions of the incessant security challenges of kidnapping, militancy, armed robbery, and pervasive corruptions (Nadabo, 2013). Even though, some places in the country have implemented CCTV technology but it has not yield positive result (LeakTimes, 2015).

In this research paper, resilient and key design considerations of IP-based surveillance system is going to be illustrated, a system type that would ensure and provide ideal insecurity solution when implemented according to recommended technical specifications. IT-governance is the application of ICT to strengthen governance — the use of Information technology in the operations of all public and private sectors in the country. If thoroughly and widely implemented across the nations not confined within few cities or agencies.

IT-governance would not only assist in tackling insecurity, but also aid in reduction of corruptions, unemployment and hunger, and hence a fully implemented e-government service sectors would efficiently work to facilitate both public and private sector developments, and thus encourage foreign investments in every sectors of economy. (Oketola, 2010), observed that the ICT industry can help establish criminal database with exciting agency-specific graphical user interfaces (GUI) for use by law enforcement agencies and security forces. With information and communication technology, law enforcement or security agents could easily track and locate kidnappers, within a domain of a particular network using a mobile tracker (Arsenault, 2014). And every mobile number in used, in this country shall be uniquely identified as belonging to an identified person in Nigeria, and keep repository and databases of their subscribers.

3. CAUSES OF INSECURITY IN NIGERIA:

Ikeogu (2014), observed that - rising insurgency is as a result of citizens' perceived injustice, due to imbalance in public administrations, and pervasive corruption in our day to day businesses interactions. The issue of idleness among youths is the major contributing factor, an axiom of "whom you know or have" is playing a greater role in the employment process in both public and private sectors, where an individual could not secured job until you know somebody or somehow connected, procedures and selections criteria are no longer practicable in most recruitment processes (Sunday, Emma, & Nwokwu, 2015).

Similarly, (Akinola, 2014), observed- weak educational systems and growth misconduct in academia, too much love of power and competition of political offices, greediness and intolerance, transnational crimes and indiscipline in the electoral process, deliberate denial of employee gratuity and other entitlements, lawlessness among citizens particularly the elites class are major contributors to current security challenges in the country.

3.1 IP Surviellance Network Syestm:

A typical hypothetical system model of an IP surveillance system would be illustrated here,design concepts and key network consideration involve in building resilient and scalable CCTV surveillance network. An IP video surveillance system includes components, such as cameras, encoders/decoders, data storage, video management software, and network equipment (Weidner, 2011).
When faced with complex network design, understanding the key network ingredients will help us identify the most important elements we need to focus on, in order to tackle the complexity of the network and design a solution that will meet the objective of the implemented surveillance system in the country.

The devices would be configured and installed in strategic places and known vulnerable areas (such as motor parks, markets, religious centers), the below figure shows a typical IP surveillance system and the key network elements require to set-up an IP surveillance network system.

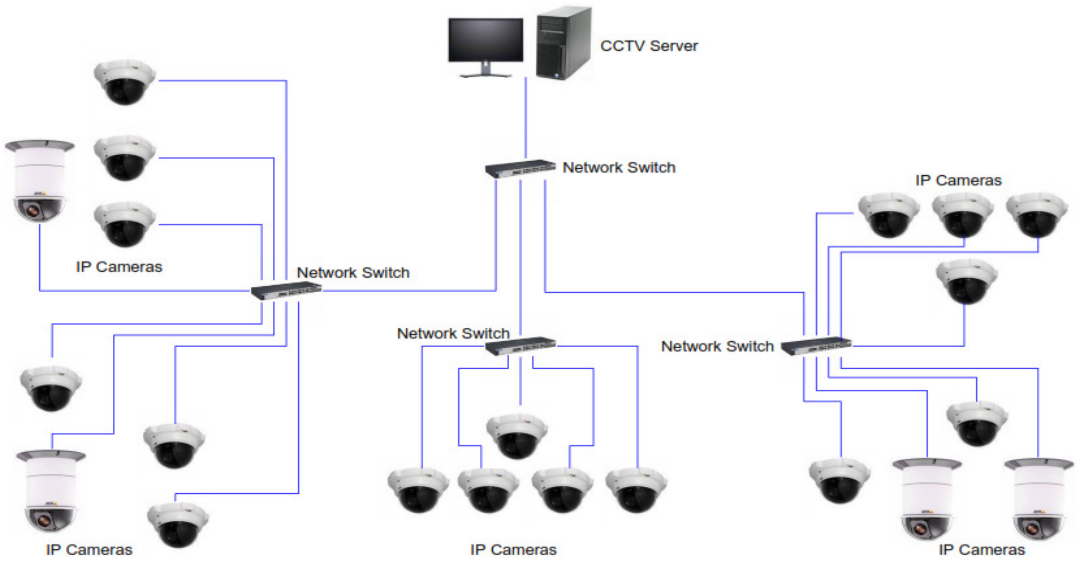

Figure 1: Schematic Design of an IP Surveillance Network

4. KEY DESIGN CONSIDERATIONS:

To realize the full benefits of IP video surveillance and prevent failure, it's important to design and build a resilient network that is capable of meeting the current and future requirements (scalable and future-proof surveillance network). A resilient surveillance network is a network that functions reliably, the first and most important step to a robust network design is understanding the nature of deployment environment/coverage area, as well as collecting and analyzing network requirements (Weidner, 2011). These requirements are the benchmark to measure the success of the implemented system. Surveying the deployment environment and coverage perimeter will determine the type and number of network cameras, as well as other network components to be configured in the network.

Some of the considered key requirements are sufficient bandwidth, should there be any downtime due to broken links or device failure (recovery time must be 70ms), video archiving every 24 hours, and 365 days a year (Walters, 1995). The design also take into consideration bandwidth utilization will increase time to time, averagely, every 12 months by 10%. The demand for video quality is the major driver of the network bandwidth consumed by a surveillance system, the higher the video quality, the more bandwidth and data storage required, a video is basically a stream of images or frames. The quality of each image is closely related to its resolution, the frame rate is the number of frames taken in a specific time span (Weidner, 2011). Higher resolution and frame rate increase required network bandwidth and storage space. To save space and increase transmission efficiency, a video normally is compressed before being transported on a network.

Compression efficiency varies greatly depending on the selected compression algorithm. There are about three main video compression algorithms in used today, these are: Motion JPEG, MP-4, and H.264 (Krone, 2013). Motion JPEG, MP-4 were the most common, now some manufacturers have begun to incorporates H.264 algorithms in their products, each of these employs different algorithms to reduce the amount of data transferred and stored in a network video system.

4.1 Comparison Of Analog And Ip Surveillance System:

In this section, we are going to compare the features of analog system that has been highlighted in the background to this study and IP surveillance system. An analog CCTV system uses dedicated point-to-point analog coaxial from the camera location to the viewing or recording station, whereas; IP-Surveillance uses the IP network technology as the backbone for transporting stream of frames (Krone, 2013). In an IP-Surveillance application, digitized video and/or audio streams can be sent to any location even around the world if desired via a wired or wireless IP network, enabling video monitoring and recording from anywhere with network access.

While an analog video system uses coaxial cabling as illustrated in figure 2, for the data delivery which is only 1- way data communication to the DVR (analog-digital conversion), in an IP video system the camera itself is capable of streaming digital video, therefore, no need of A-D conversion. The camera is network device, so the cabling used is usually ethernet cabling (as shown in figure 3), this network connection allows for allows for 2-ways communications between users in the network and the cameras, the camera streams the video signals directly to the NVR (Krone, 2013). The main reason IP cameras is getting popularity in the world as illustrated in the global market indices (Crouwel, 2014), it can captured and delivered video in much higher resolution than analog systems, other benefits includes using and working with existing network infrastructure.

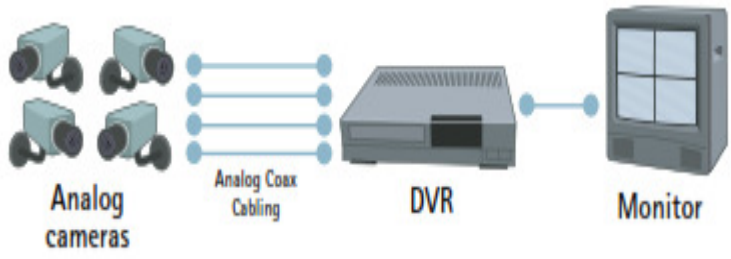

Figure 2: Analog Surveillance System

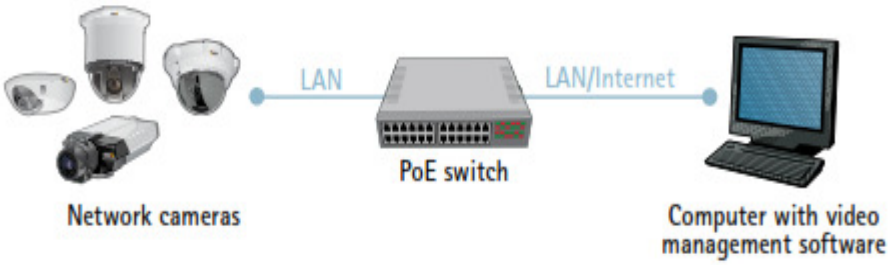

Figure 3: An IP surveillance System

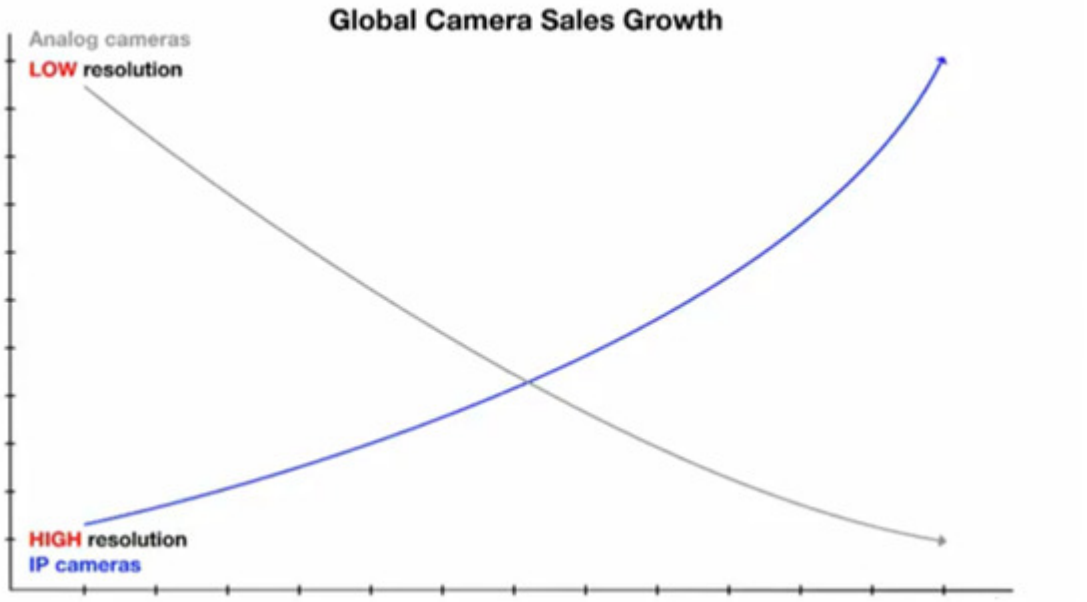

Figure 4: IP cameras popularity ↑, Analog cameras ↓

5. DISCUSSION:

With digital CCTV technology, we can set up a large-scale IP video surveillance across the nation, in strategic points and vulnerable places (such as motor parks, religious centers, retail outlets, and educational centers). The technology would assist security agents to monitor high-quality video feeds and control multiple surveillance cameras in real time from a remote location. Security agents like mobile police, civil defense, army or SSS can take advantage of the wireless cameras portability and easily move around the cameras to different locations to watch crime hotspots, it would restrain gangs from criminal acts and serve as a tool for detecting and investigating crimes.

In the U.S, places like Texas and Dallas, IP-based CCTV surveillance systems have been impressive, report from Dallas security department revealed a twelve percent (12%) drop in crimes and a nine percent(9%) increase in arrests in the first year after implementation of the system (Abshire & Eiserer, 2008). Others ICT tools are biometrics, determining and profiling, biometrics is a technology that stores, measure, and analyses physiological and behavioral characteristics of human being for authentication, identification or screening purposes (Johnson & Williams, 2007). For example, information for uniquely recognizing human being based upon one or more intrinsic physical traits such as fingerprints, iris scan, facial patterns, and DNA.

Nigerian immigration and custom services could similarly, use biometric measurements such as fingerprints to identify illegal immigrants, reports has shown most of insurgents were immigrants from bordering countries.so, software application such as Automated Fingerprint Identification System (AFIS) or Biometric Access System(BioAccSys), investigators can collect a set of finger prints at a crime scene electronically using a mobile device and then compare them against a database of millions citizens fingerprints within few minutes (FBI, 2014). Federal, state, and local level relevant agencies like NPC, NIS, should equally gathered data, when they issued birth certificates, identification cards or e-passports. Thus, government and security agencies now have citizens and immigrants databases of digital biometric data at their fingertips to search for and identify suspects or when the need arises. In some cases, DNA samples(body fluids such as blood) could be analyze and used by investigators to track and identify criminals, its more information rich, with better distinguishing characteristics than other biometric identifiers (Arsenault, 2014).

Another vital ICT tool is data mining and profiling technique, that could be used to collect and analyze crimes data, then routinely generate security report, this would help to understand trends (Johnson, 2004) and gain better intelligence about crimes and effective resource utilization. The process of data mining and profiling is simply the collection of crimes data into a single repository or data warehouses, where data mining algorithms like apriori, ID3 and C4.5 decision tree algorithms are applied to discover trends and pattern of crimes incidences (Quinlan, 1993). The use of analytics platforms like HADOOP, would also assist in implementing “Broken Windows Theory” of criminology that monitoring and policing crimes hotspots and public places may stop further vandalism and escalation into more serious crimes (Kelling & Coles, 1996).

Therefore, these techniques could assist security agencies, to generates clear metrics and validate the effectiveness of enforcement tactics, and rapidly respond to emerging crime trends like armed robbery, kidnapping or child trafficking.

6. CONCLUDING REMARKS:

The major issue facing the nation law-enforcement agencies and security operatives is lack of modern IT enable tools for monitoring crimes and data collection, intelligence gathering and analyzing the growing volumes of crime data. Advancement of information technologies with tools such as data mining analytics, CCTV surveillance, biometrics and DNA sampling tools are increasingly evolving and accessible to security operatives and the law enforcement agencies, installing and running these modern IT enable services often cost less than recruiting and training security personnel. Automated security systems are also less prone to errors than human investigators.

This research paper focus on discussing factors that causes insecurity in Nigeria, modern IT enable techniques were also highlighted using IP CCTV surveillance, biometrics and DNA sampling, and crime analysis tools using different analytics software suit, which can assist law enforcement to easily analyze crime dataset, identify actionable patterns and trends, and hence efficiently handle crime investigation and security issues.

7. CONTRIBUTION TO KNOWLEDGE:

Job creations is a critical tool to reduce insecurity in the country, most act of terrorism, violent behavior, kidnapping, or robbery is perpetrated by unemployed populace, therefore, these group of people need to be engaged with employment opportunities offered by Information and communication Technology services. IT centers should be build all over the nation where unemployed graduates can be engaged, with modern businesses of developing computer programs and assembling, mobile software applications, repairs and maintenance of computers accessories and network installations. On the other hand, public office administrators, traditional institutions, clergies, have to put hands together and fulfill their communal duties responsibly. They should promote the habits of working to serve their community not their good self. restructuring and sanitizing our educational system is paramount from primary to tertiary level, and incorporate mandatory IT subjects in the curricula in all disciplines to enable graduates compete with their global counterparts, prepared them for self-employment with evolving modern-IT enable businesses.
.

REFERENCES:

1. Abshire, R., & Eiserer, T. (2008). Surveillance Cameras in Dallas Area Work to Counter Crime. Dallas: Dallas Morning News. Retrieve from: http://www.mobilitytechzone.com/news/2008/03/22/3341737.htm Accessed Date: 19/10/2014.
2. Alademoko, D. (2013). e-government and national security. Osun State: Information Nigeria. Retrieve from: **http://www.informationng.com/2013/05/ict-can-be-used-in-tackling-insecurity-ncs.html** Accessed Date: 17/10/2014.
3. Akinola, W. (2014). Insurgency:The Five-Way Solution. Lagos: VanguardNewspaperNigeira. Retrieve from:
4. Arsenault, C. (2014). U.S Police Track CellPhones without Warrants. New York: Aljazeera.
5. David, L. (2007). An Overview of Surveillance Studies. Cambridge: Cambridge Polity Press.
6. Hassan, T., & Kabiru, I. (2013). Nigeria: Security Retains Top Spot in 2014 National Budget. Abuja: Dailytrust.
7. Hornby, A. (2005). Oxford Advanced Learners. U.K: Oxford University Press.
8. Ikeogu, M. (2014). Information Technology Can Solve Nigeria's Security Problems. effurun: Thepointernewsonline.
9. Johnson, P., & Williams, R. (2007). Internationalising New Technologies of Crime Control. EU: Policing and Society.
10. Johnson, S. (2004). Philadelphia Police Department: COMPStat Process. New York : ppdonline.
11. Kelling, G., & Coles, C. (1996). Fixing Broken Windows: Restoring Order and Reducing Crime in Our Communities . New York: The New York Times.
12. Krone, J. (2013). Ten Reasons To Switch From Analog Cameras And DVRs To IP Cameras And NVRs. New York: Jameson.
13. LeakTimes. (2015). CCTV Scam: Reps Investigate ZTE, Chinese Firm. Lagos: Leak Times Nigeria.
14. Nadabo, S. (2013). Insecurity in Nigeria: Causes and Resolutions. Jigawa: Nigeriavillagesquare.
15. NPC. (2014). Nigeria over 167 million population: Implications and Challenges. Nigeria: National Population commission Nigeria.
16. Oketola, D. (2010). Tackle national insecurity with ICT. Lagos: Nigerianbestforum Retrieve
17. from:http://www.nigerianbestforum.com/generaltopics/tackle-national-insecurity-with-ict-experts-tell-fg/ Accessed Date: 15/10/2015
18. Poulsen, K. (2007). Firsthand Reports from California Wildfires Pour Through Twitter. California: Wired Blog Network.
19. Oketola, D. (2010). Tackle national insecurity with ICT. Lagos: Nigerianbestforum.
20. Quinlan. (1993). Programs for Machine Learaning. California: MorganKaufmann.
21. Rahim, S., SunTie, Begum, A., & Sahar, G. (2005). ICTs Infrastructure Model for Crime Monitoring and Control. Pakistan: IEEE.
22. Strauss, A., & Corbin, J. (1998). Basics of Qualitative Research Techniques and Procedures for Developing Grounded Theory. London: Sage Publications.