E-Intruders Monitoring & Criminal Evidence System in a Construction Site: A Proactive Approach to Mitigate Corrupt Practices in Project Finances and Contractual Relationships

[1]Yekini N.A, [2]Adigun J.O, [3]Okikiola F.M, [4]Hungbo A.A, [5]Ojo O.
[1]computer Engineering Dept' Yaba College of Technology
[2,3]computer Technology Dept' Yaba College of Technology
[4]quantity Surveying Dept' Yaba College of Technology

ABSTRACT

Insecurity in Nigeria has shown significant growth thereby showing the flaws in the security system of the nation. This has led to the citizens clamoring for a system that works in tackling the potential and future security threats. The perpetrators of the criminal are majorly the intruders. E-security monitoring and criminal evidence system is a globally recognized and trusted device that has the capability of providing security alternatives in society. This tool is seen as a means of cautioning intruder's activities which in return leads of less or no crime. This research work explores the influence of e-security intruder monitoring and criminal evidence system on the behavior of individuals and extends the discourse analysis to interpreting insecurity occurrences in our society to investigate and find meanings that construct social reality.

Keywords: **Insecurity, Intruders, Crime Prevention, E-Security, Criminal, Crime Evidence, Security System.**

Date of Submission: Feb 08, 2022 Date of Acceptance: Feb 18, 2022

I. INTRODUCTION

Security can be referred to as freedom from, or resilience against, the potential harm caused by others. While evidence, as broadly accepted, is anything presented in support of a statement because evident things can never be doubted. There are two generally known kinds of evidence: intellectual evidence, which is the obvious, and empirical evidence, which is proof [1]. A crime of any magnitude is an offence that deserves community condemnation, punishment, usually by way of fine or imprisonment. This is different from a civil wrong which is an action against an individual that requires compensation or restitution [2]. An e-security monitoring and criminal evidence system is a system that is mainly carried out using crime record systems like CCTV systems to monitor the interior and exterior of a property, thereby transmitting the signals to the display. According to [3], the methods of detection employed are dictated by the nature of the crime and the procedures permitted by the legal system. Most investigations start with careful, objective observations that are then collated, and matched against applicable law. If there is a reason to believe or assume that a crime has indeed been committed, more investigations are carried out using scientific methods and techniques [4].Most nations across the globe make use of a criminal record system that also serves as an investigation system. The system uses a comprehensive database of crimes committed and it makes it extremely easy for the police to investigate crimes. This is possible because the database can be queried based on different criteria such as type of crime, the surname of suspects, facial recognition, etc. The success of any platform depends on the trust and security that they maintain regarding users personal and payment data this is applicable to e-commerce as opined by [5]. No doubt that the opinion of the authors in the research work entitled Practical Security Testing of Electronic Commerce Web Applications could be justified based on integrity which can be link to criminal evidence if criminal activities takes place and also to put in place efforts for robust system to prevent security threat.

The rate of crime in Nigeria has led to significant security issues in the country security system. This has resulted in the citizens clamoring for a system that works in tackling security treat. Study shows that there is no computerized criminal record/monitoring system that enables the police to confirm past criminal records, get information of suspects, and keep criminal records based on different criteria to track down offenders. The manual method of investigating cases takes time, leaving cases pending and even neglected over time. Consequently, the perpetrators of the crime are not apprehended at the end of the day thereby making the police force investigation baselessly ineffective. This study, therefore, presents the design and implementation of Electronic Security monitoring and criminal evidence system in Yaba College of Technology.

II. LITERATURE REVIEW

Closed-circuit television technology was invented in 1942 by a German engineer named Walter Bruch. He designed and installed the first Black and white analog camera mainly for observing the launching of rockets. The surveillance cameras were used by the scientists from inside a bunker to observe the nuclear bomb testing without being exposed to the danger of the bomb launch. Scientists were able to learn the effect of nuclear weapons without encountering the aftermath danger [6]. Initially, CCTV was called Vericon and it worked entirely on wires until Marie Van Brittan Brown was granted the U.S. patent for home security. It was used in locations such as banks and the initial equipment was expensive, bulky, and provided an objectively poor picture quality, with the grainy footage [7]

A security camera is a planted video capturing equipment that records an individual's activities in real-time to detect and prevent crime from happening. It is a device that is used in capturing footage of homes, properties, banks and so on which can be viewed on smart phones, computers anywhere and can be monitored real-time when connected to the internet. Most widely used security cameras can detect motion and can equally record the activities detected and send an alert. Vision is the faculty of sight, and it is one of the most amazing abilities to have evolved [8]It can be an extremely sensitive tool of perception, yet it is also very vulnerable to adverse conditions. For several hours a day, for example, darkness renders our eyes near useless, yet, on a clear day, as the saying goes, we can see things miles away.

Day-Night cameras are used color when enough light is present. When light levels are too low, they switch to black and white, which is more sensitive in low light conditions. Infrared (IR) cameras use color in the day and switch to black and white in low light conditions [9]. These cameras use IR light-emitting diodes (LEDs) to illuminate the environment in low-light conditions. Digital Video Recorder (DVR) – DVRs consist of a hard drive that stores CCTV video data.

Cameras connect to the DVR and the DVR can then display the camera video on a monitor in split-screen mode. It then Stores multiple videos and audio signals in digital format on a hard disk drive. DVRs can offer motion-detection-activated recording and remote viewing from anywhere in the world via internet access. CD, DVD, USB backup media can also be used (Herman, 2017). Because of its dependability and stability, stand-alone DVRs use the Linux operating system (Microsoft Windows often contains software glitches!) Some CCTV experts believe video surveillance should never be PC-based because of the lack of reliability. Digital Video Recorder Card – Used to convert Computer to DVR, CCTV storage unit is an electronic device that process signals received from CCTV cameras and save the data to storage media such as a hard drive or a cloud-based storage service

The Hard Disk Drive (HDD) device is used to store digital information. A CCTV monitor is an output device that is usually connected to a feed from a surveillance video recording device. Systems can be “future-proofed” to a certain extent by using a monitor with multiple inputs. The majority of DVR and NVR devices have a VGA connection, while others have HDMI or DVI connections. LCD PC Monitors connect to the VGA port on the DVR. If there is no VGA Port, a BNC to VGA converter cable is needed (Steven et al., 2018. According to [10] "homeowners in general like to keep an eye on things, whether it's knowing about specific incidents or simply seeing who just came to the front door." Security cameras are classified into two types: wired and wireless. Wireless security camera uses wi-fi to transmit footage captured to a cloud-based server over the internet. This helps an individual to view the footage in real-time on internet-enabled devices. Another thing to put into consideration is that there are many wireless cameras that are entirely not wireless because there is a need for them to be connected or plugged into an AC power by using a power cable. Nonetheless, some of them use batteries that can be recharged. Wireless security cameras are frequently referred to as "smart cameras" because they can be controlled by an app on your smartphone and can integrate with smart home devices and systems like Google Assistant, smart locks, smart speakers, and smart lights [11].In their research work entitled Networking CCTV Cameras & Passive Infra-Red Sensors for E-Classroom Monitoring System [12],it was opined that CCTV cameras can be used to monitor the classroom for security purpose and towards enhancing quality control in teaching and learning system.

III. METHODOLOGY

Security cameras, cables, Cloud Video Recording Equipment, storage Device, Aduino Intruder sensor, and Display unit are among the proposed system's components. Figure 1 depicts the simplified architecture and connection of the proposed system. There is a power unit that provides power to the Cloud DVR and camera so that they can function. The camera(s) capture activity within the surveillance area and transmit it to the DVR, which processes it and saves the captured data to the storage device embedded in as well as to the content online (cloud). The system administrator's password will control access to the stored captured audio and video. When the sensor detects an intruder, the camera will be activated. Figure 2 depicts the system's operation.

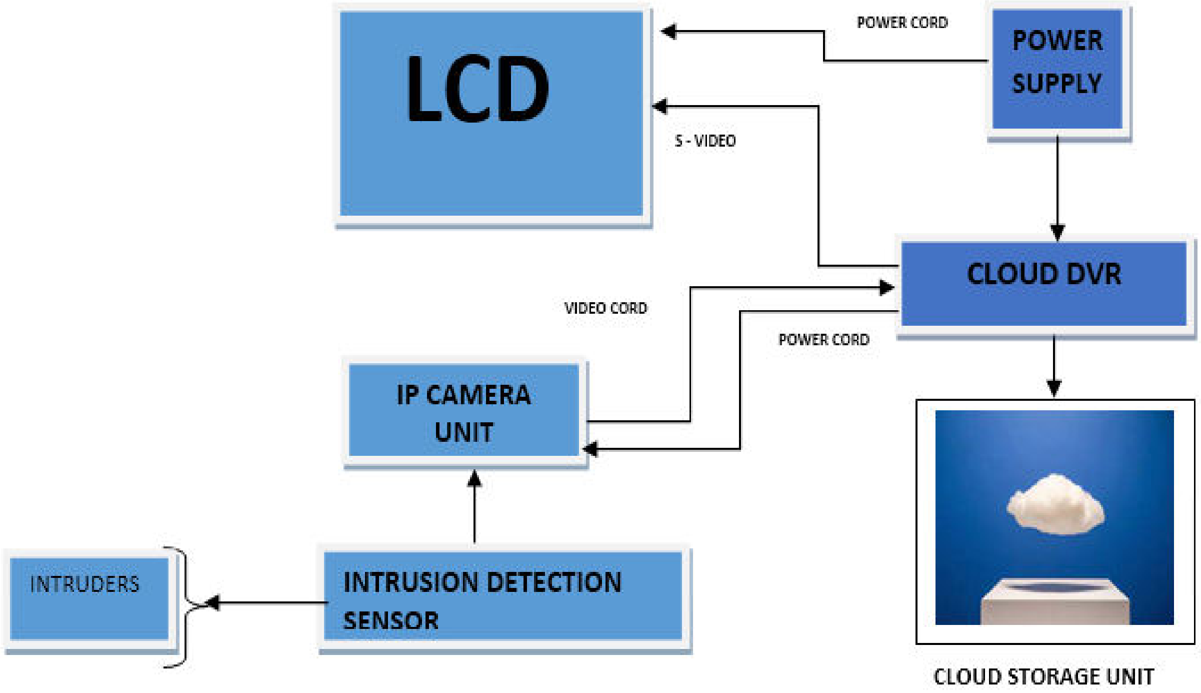

Figure 1: Simplified Architecture of Proposed E-Intruders Monitoring & Security System.

Figure 2 illustrate the flow of operation of the proposed system.

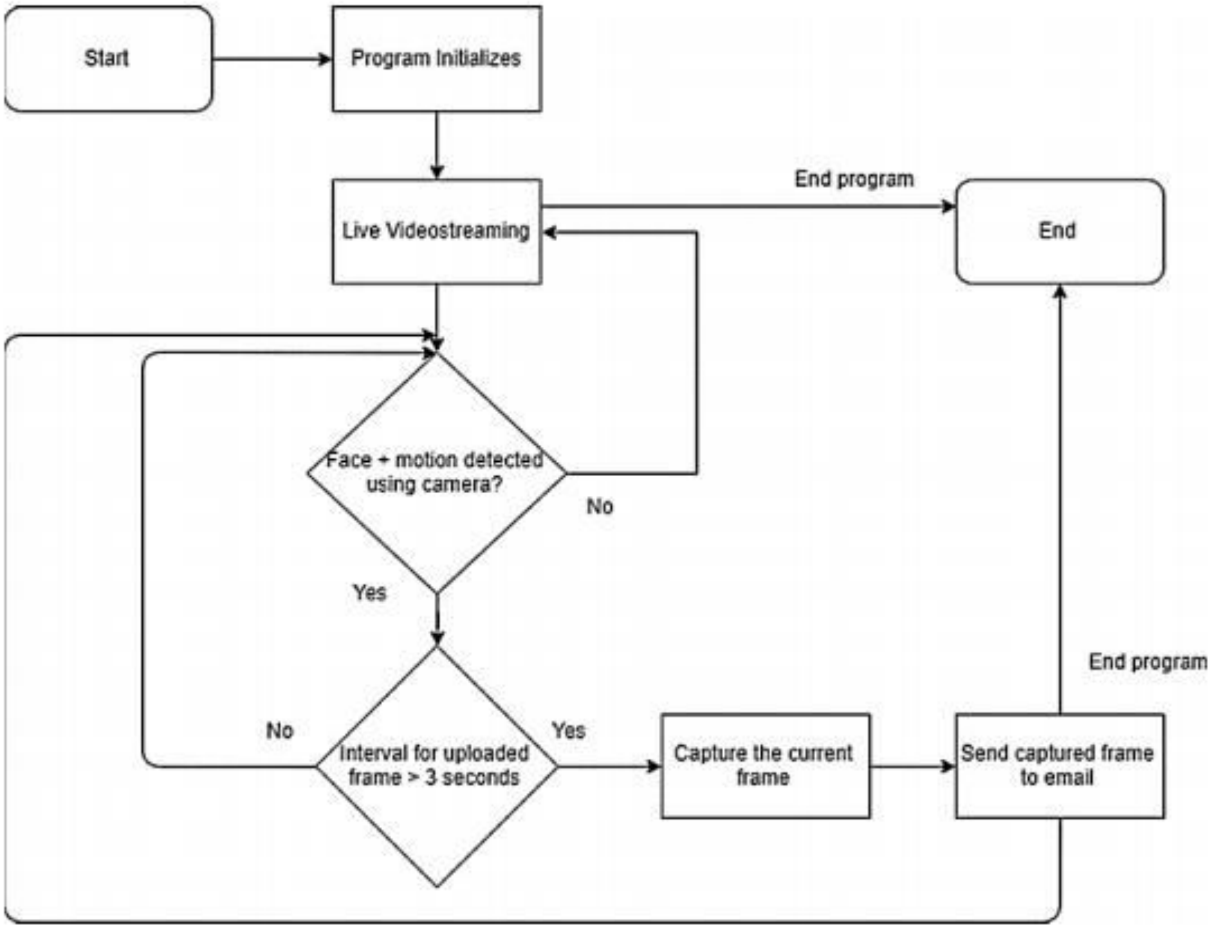
Start
Program Initializes
Live Videostreaming
End program
End
Face + motion detected using camera?
No
Yes
End program
No
Yes
Interval for uploaded frame > 3 seconds
Capture the current frame
Send captured frame to email

Figure 2: Software operation of the system

IV. IMPLEMENTATION & TESTING

This entails the layout and connection of all the components that made up this system by putting them together and testing their interrelationships thereby showing the desired outcome. Figures 3, 4, and 5 show the connection test of the hardware part of the system.

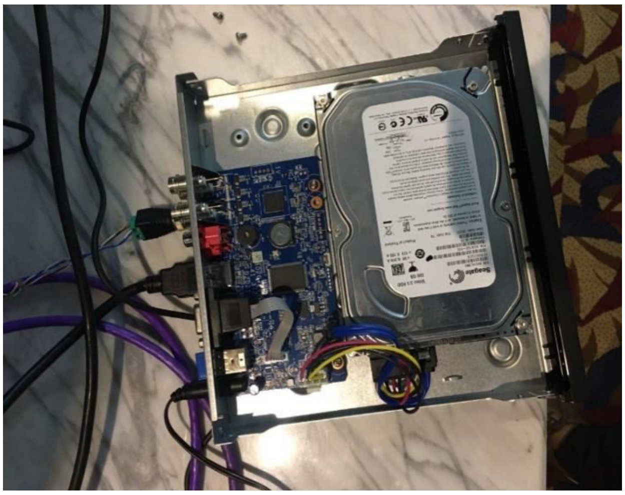

Figure 3: Connection of Hard disk with the DVR

Figure 3 depicts the connection of the hard disk to the Digital Video Recorder so that recorded images can be saved for future reference and use. A hard drive is an essential component of any CCTV system. Its settings are critical for the quality and dependability of camera video recordings. HDDs used for monitoring, on the other hand, operate under conditions that differ from those found in PCs. Data is continuously recorded in CCTV systems and accounts for more than 90% of the disk load.

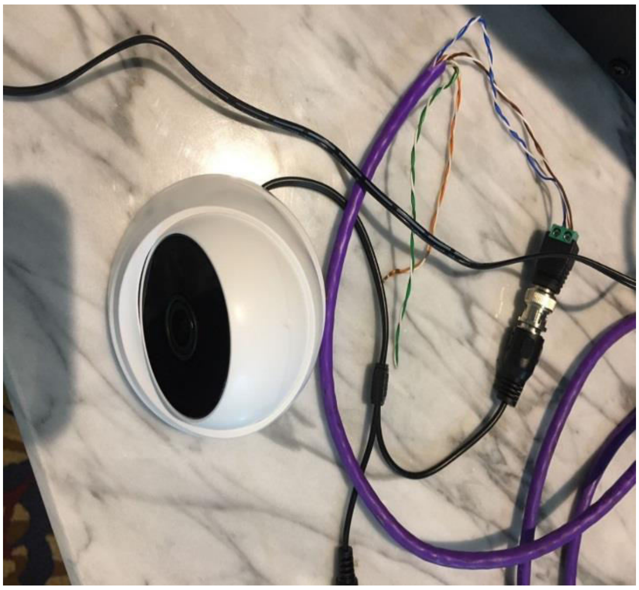

Figure 4: Connection of BNC connector to the Security Camera

Figure 4 shows the connection of connector to the port of the dome camera and that of the DVR so that images can be viewed on the monitor screen. The coaxial side of the cable carries the video signal from your security camera to the DVR. For the coaxial cable, BNC connectors are needed to install the cable into the camera and into the DVR.

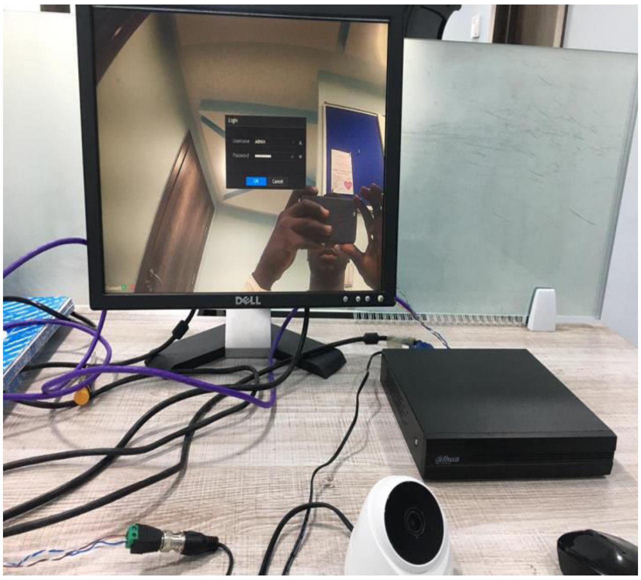

Figure 5: Connection of all Components

Figure 5 shows the successful interconnection of all components. Connection of security camera to the DVR using BNC connector and the connection of the DVR to the screen to display the recorded images. A couple of screenshots below shows the results of the interface, it's functioning seamlessly.

The DVR stores the security video/images on a hard drive. The vast majority of security cameras in use today capture analog images. After compression, the DVR converts these analog signals to digital and stores them on the hard drive. DVRs can handle multiple camera inputs. You can view all these images and videos at a time or one by one, depending on your preference.

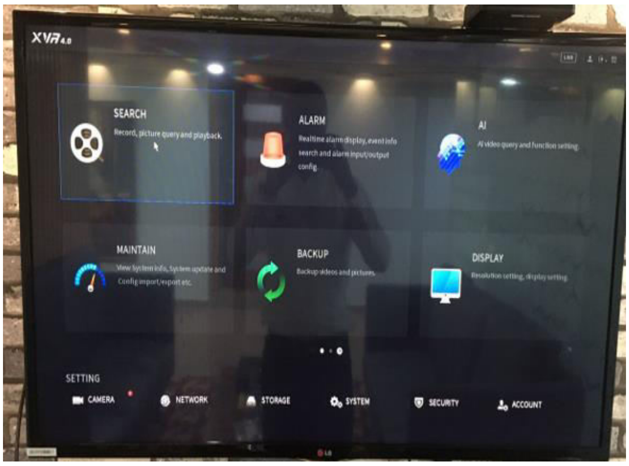
XVR 4.0
SEARCH
Record, picture query and playback.
ALARM
Realtime alarm display, event info search and alarm input/output config.
AI
AI video query and function setting
MAINTAIN
View System info, System update and Config import/export etc.
BACKUP
Backup videos and pictures.
DISPLAY
Resolution setting, display setting
SETTING
CAMERA
NETWORK
STORAGE
SYSTEM
SECURITY
ACCOUNT

Figure 6: Interface Layout

Figure 6 depicts the system's layout display. It shows the various icons set up for easier interfacing with the system to enable users to easily carry out desired modifications and enhance a user-friendly experience with the system.

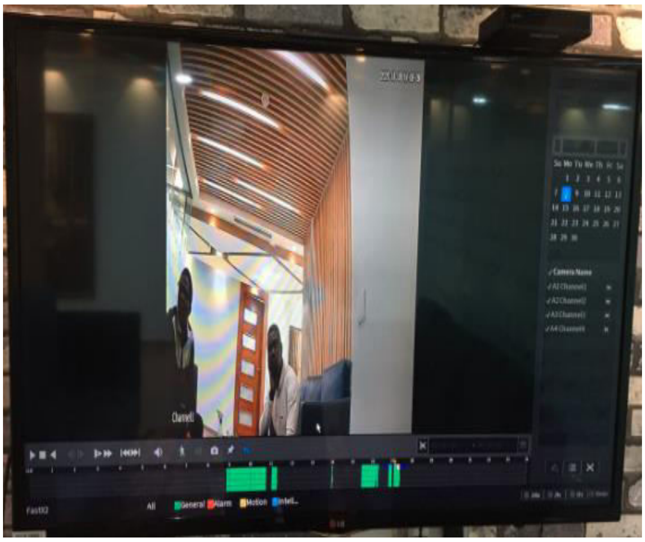

Figure 7: Captured Image

Figure 7 shows the image captured while test running the system functionality.

V. CONCLUSION

This work is based on strategically placing cameras and observing the camera's output on monitors somewhere. Because the cameras communicate with monitors and/or video recorders via private coaxial cable runs or wireless communication links, they are labeled "closed-circuit" to indicate that access to their content is restricted to those who can see it by design. Previously, older CCTV systems relied on small, low-resolution black-and-white monitors with no interactive capabilities. However, this design work includes features such as color, high-resolution displays, and the ability to zoom in on an image or track something (or someone). When necessary, the system saves the recorded intruder activities in the cloud as criminal evidence.

REFERENCES

[1] Abeer S. J. (2015) “Designing A Digital System for the Security of a Building Based on Behavioral Tracking”, University of Technology, Computer Science Department, 2015.

[2] Bui D. C, et.al, (2013) “Real-time Zoom Tracking for DM36x-based IP Network Camera”, Journal of Korea Multimedia Society, vol. 16, no. 1, pp 1261-1271, 2013.

[3] Elizabeth L. K. (2011) “The cons of analog cameras”, available at http://ipvideomarket.info/report/cctvsurveillance.htm August 2011. Retrieved 13, January 2022.

[4] Farhan T. (2016)"understanding and planning of CCTV security systems", Life safety & security, 2016.

[5] P. Raghu Vamsi, Agrah Jain (2021) Practical Security Testing Of Electronic Commerce Web Applications: Int. J. Advanced Networking and Applications Volume: 13 Issue: 01 Pages: 4861-4873(2021) ISSN: 0975-0290

[6] Herring T. (2015) "The history of CCTV", available https://herringtechnology.com/news/the- history-of-cctv/, 2015. Retrieved December 31, 2022.

[7] Jea H. S, Hong R. K. (2013) “A new IP-based Multi-Channel Elevator Video Surveillance System”, The Transactions of the Korean Institute of Electrical Engineers, vol. 62, no. 4, pp 164-168, 2013.

[8] Jong W. C. (2012) “A Study on the Network Based DVR(NVR)-GUI Design”, Journal of Digital Interaction Design, vol. 11, no. 3, pp 49-62, 2012.

[9] Joseph Q. (2013) “Overview of IP Camera Technology Report” pg 12-14, 2013

[10]Louis F. (2001) "Encryption and Cryptosystems in Electronic Surveillance: A Survey of the Technology Assessment Issues", 2001

[11]Moon W. (2008) "Electronic Security Systems", University Press, Cambridge UK, 2008, pg 66-75

[12]Oloyede Adetokunbo Olamide., Yekini Nureni Asafe., Onadokun Isaac Olawale., & Akinyele Okedola Akinleye (2027). Networking CCTV Cameras & Passive Infra-Red Sensors For E-Classroom Monitoring System: Proactive Approach To Quality Assurance In Education System. Int. J. Advanced Networking and Applications Volume: 08 Issue: 05 Pages: 3213-3219 (2017) ISSN: 0975-0290