Chapter One
Introduction

1.1 Background of the Study

Security practice is crucial peaceful living. In the old times, before the advancement of technology, security was a major concern due to invasions, robbery, and wars. According to history, security personnel in those days known as vigilante also served as police. The security responsibilities then require 100% human effort, having to go over an assign geographical area, restlessly and sleeplessly, to secure lives and properties. But today with technological advancements, people are able to live in security without the need for protection. The advancement in technology as relieved human a whole lot of security threats and stress [1, 2].

Meanwhile, the world is changing fast. Not only are we experiencing the Industrial Revolution 4.0, but also the Fourth Industrial Revolution that is marked by digitization and IoT (Internet of Things). The main purpose of IoT is to establish advanced connectivity of devices, systems, and services that supersede machine-to-machine (M2M) communications, supporting several domains, protocols, and applications[3].

Along with this digital transformation, another revolution is happening in the world which is related to how people live in metropolitan cities: implementing smart city initiatives, these initiatives focus on addressing urban challenges through empowering people to be more efficient, effective, and sustainable citizens within their communities, the continuously growing movement of smart cities is increasingly becoming a challenge to efficiently manage the city's resources and infrastructure, one of the primary aspects these challenges are the security systems, which includes the need for surveillance system. Advancement in today's technology have lead to newer and more efficient technologies for

surveillance, providing high-definition video with features like object recognition, persistent filming capability, intelligent alerting and machine learning analytic that help in catching the criminal element. It is also a growing trend in the world of law enforcement to use video surveillance coupled with license plate recognition software to gather information on criminal activities, providing a proactive rather than reactive police response[3, 4].

1.2 Statement of the Problem

In known smart environment surveillance technology, a real-time multicast viewing and system monitoring is faced with numerous challenges[10,13]. For example, the monitoring unit is usually centralized at a defined station, which limits extensive and close monitoring of the system, if there is consideration for an alternative monitoring unit, an IoT based remote streaming app is usually used, which sometimes experiences delay / interruption in transmission, due to error from the framework or internet connections. This method also consumes a lot of internet data, due to enormous data transmission and it allows limited number of users[14].

Furthermore, there has been an increase in insecurity and injustice across the nation, even regrettably, in the smart environment, due to insignificant and improper security protocols[1,2]. However, the implementation of an advance surveillance system, that will enable residents in a community to join forces with one another and contribute their own quota in securing their environment, lives and properties, through a surveillance system monitoring, is an area that has not been fully explored.

1.3 Aim and Objectives of the Study

This study aims to develop a surveillance system multicast for crime prevention and detection, within an enclosed geographical location, to enable residents in the community to join forces with one another and contribute their own quota in securing their environment, lives and properties, through a surveillance system monitoring.

The specific objectives are to:

i. develop a CCTV system, using an analogue camera and a digital video recorder, having a hard-drive, for data capturing and storage.
ii. design a decentralization system using a wireless video transceiver.
iii. integrate the objective one & two for a multicast surveillance system.
iv. evaluate the system.

1.4 Motivation of the Study

Motivation for this study is to reduce/eradicate internet data usage in surveillance system monitoring. There will not be any application development in this study, because the beginning of application development is an approach to internet data usage. Eradicating internet data usage in surveillance monitoring through multicast is a compelling concept that could revolutionize the way we approach remote viewing applications. The primary benefit of multicast is that it allows data to be transmitted to multiple recipients simultaneously, rather than sending individual streams to each recipient separately. This means that it is possible to reduce the amount of internet data used in remote viewing applications by sending a single video stream to multiple recipients at once.

By utilizing multicast, surveillance monitoring can significantly reduce internet data usage, which can translate into cost savings and more efficient use of resources. Moreover, multicast can improve the real-time monitoring capabilities of surveillance systems by reducing the latency associated with traditional data transmission methods.

One of the key advantages of multicast is that it can work over local area networks (LANs), which means that it is possible to reduce or eliminate the need for internet connectivity in remote viewing applications. This can be particularly useful in situations where internet connectivity is limited, unreliable, or costly[5].

However, implementing multicast in surveillance monitoring requires specialized equipment and network infrastructure, and it may not be suitable for all applications. It is also worth noting that using multicast over LANs may require additional security measures to protect against potential vulnerabilities.

Eradicating internet data usage in surveillance monitoring through multicast is an exciting concept that has the potential to significantly improve the efficiency and effectiveness of remote viewing applications. By utilizing multicast, organizations can reduce costs, improve real-time monitoring capabilities, and enhance overall security and privacy in surveillance operations, even in areas where internet connectivity is limited.

1.5 Significance of the Study

The need for a significant and proper surveillance system in the society cannot be over emphasized. the increase in crime rates and paramount insecurity in the society has brought eagerness to individual in joining forces with one another and government to tackle insecurity by providing the necessary resources and infrastructure. Take for instance, cultism, bullying, vandalism, theft and burglary are major issues in academic campuses, also terrorism across the nation. A stray footage could capture culprit identity or hideout at given event, there would be fast detection and proper action will be taken on time, because large number of people are monitoring the surveillance system.

This study will encourage transparency in law enforcement in the society, mitigate injustice, concrete evidence will be used against criminals and they will be brought to book for their wrong doings. Crooks will think twice about getting away with their crime.

1.6 Scope of the Study

Security practice is crucial peaceful living, this is a reflection of how the lack of proper and effective surveillance technology has taken away safety and security in the society. This study is focused on implementing an advanced surveillance system, which will multicast to several residents in a community or estate through a wireless video transceiver, for a proper surveillance system monitoring.

This study will not consider any internet protocols rather it will consider the radio frequency range to be used and its wavelength range and the matching Wi-Fi protocol. Considering the public privacy and control, read only data will be multicast, while the read and write data remains centralized at the main workstation. For experimental or result purposes, only the system prototype will be presented.

1.7 Limitation of the Study

In this study, we could not automatically differentiate between criminal related activities and normal human activities without the intervention of human, but can provide accurate video footage or data on-demand about an event for law enforcement and transparency in justice.

1.8 Operational Definition of Terms

1. **nLos:** Non-line of sight (NLOS) refers to the path of propagation of a radio frequency (RF) that is obscured (partially or completely) by obstacles, thus making it difficult for the radio signal to pass through.

2. **Algorithm:** is a procedure used for solving a problem or performing a computation. Algorithms act as an exact list of instructions that conduct specified actions step by step in either hardware- or software-based routines.
3. **Streaming:** is the ability of the user of a surveillance system to view the streaming live footage of that system over the internet on a device such as a Personal Computer, or a Smartphone.
4. **MAC Level Multicast Protocol:** unreliable wireless level is used for delivering the messages to the mobile homes.
5. **Multicast:** In computer networking, multicast is group communication where data transmission is addressed to a group of destination computers simultaneously. Multicast can be one-to-many or many-to-many distribution. Multicast should not be confused with physical layer point-to-multipoint communication.
6. **Wi-Fi:** is the wireless technology used to connect computers, tablets, smartphones and other devices to the internet. Wi-Fi is the radio signal sent from a wireless router to a nearby device, which translates the signal into data you can see and use.
7. **Optical Wireless Communications (OWC):** is a form of optical communication in which unguided visible, infrared (IR), or ultraviolet (UV) light is used to carry a signal.
8. **Frequency Range:** Mobile networks use radio communication which is carried out on a range of frequencies. These frequencies can range from 850 MegaHertz (MHz) to tens of GigaHertz (GHz).
9. **Spectrum or Frequency Spectrum:** is a range of frequencies that are available for any given service.
10. **Transceiver:** a transceiver is an electronic device which is a combination of a transmitter and a receiver, hence the name. It can both transmit and receive radio or optical waves for communication purposes.

11. **Decentralization:** is the allocation of resources, both hardware and software, to each individual workstation, or office location.
12. **Centralization:** computing exists when the majority of functions are carried out, or obtained from a remote centralized location.
13. **Computer Operation:** an elementary operation that a computer is designed and built to perform.
14. **Floating-point Flop:** an arithmetic operation performed on floating-point numbers; "this computer can perform a million flops per second".
15. **Operation:** data processing in which the result is completely specified by a rule (especially the processing that results from a single instruction); "it can perform millions of operations per second.
16. **Retrieval:** the operation of accessing information from the computer's memory.
17. **Storage:** the process of storing information in a computer memory or on a magnetic tape or disk.
18. **Storage Allocation:** The process of assigning memory space to computer programs and data.
19. **Data Encryption:** The process of converting plain text or data into an encoded format to prevent unauthorized access.
20. **Memory Access:** The process of reading or writing data from or to memory.
21. **Accumulator Register:** A special-purpose register in a computer's central processing unit (CPU) used to store intermediate results during arithmetic and logical operations.
22. **Screen Background:** The background image or color on a computer screen or display.
23. **Backup:** A copy of computer data stored separately from the original data to protect against data loss in the event of hardware failure or accidental deletion.

24. **Bulletin Board System:** A computer-based system that allows users to exchange messages and files, similar to an online forum.
25. **Memory Cache:** A high-speed component that stores frequently accessed data to reduce the time needed to access it from main memory.
26. **Central Processing Unit:** The part of a computer that performs most of the processing and controls the other parts of the computer.
27. **Information Processing System:** A system that processes data into meaningful information using hardware and software components.
28. **Computer Circuit:** A physical component that carries electrical signals and performs logical operations within a computer system.
29. **Computer Network:** A group of interconnected computers that can communicate and share resources.
30. **Magnetic Core:** A type of memory technology that uses small magnetic cores to store data.
31. **Dedicated File Server:** A computer system that is dedicated to storing and managing files for other computers on a network.
32. **Dialog Box:** A graphical user interface element that presents information or options to the user and requires a response.
33. **Dual Inline Package Switch:** A type of electronic switch used in computer hardware to control the flow of data.
34. **Disk Controller:** A hardware component that manages the transfer of data between a computer's disk drive and its main memory.
35. **Disk Drive:** A hardware component that reads and writes data to a computer's disk.
36. **Display Adapter:** A hardware component that translates signals from a computer into a form that can be displayed on a monitor.

37. **Dongle:** A small hardware device that is connected to a computer to provide additional functionality or security.
38. **Drive:** A hardware component that can read or write data to storage media, such as a disk or USB drive.
39. **File Server:** A computer system that is dedicated to storing and managing files for other computers on a network.
40. **Firewall:** A network security system that monitors and controls incoming and outgoing network traffic based on predefined security rules.
41. **Foreground:** The part of a computer display or user interface that is currently being used or viewed by the user.
42. **Video Encoders:** Devices that convert analog video signals into digital format for storage and transmission.
43. **Image Sensors:** Electronic devices that convert light into electrical signals to create digital images.
44. **CMOS:** Complementary Metal-Oxide-Semiconductor, a technology used in computer hardware, including memory chips and image sensors.
45. **CCD:** Charge-Coupled Device, a type of image sensor that converts light into electrical signals.
46. **Image Scanning:** The process of converting physical images into digital format using a scanner or other image capture device.
47. **Interlaced (popular for CCD applications):** A type of image scanning in which alternate lines of an image are scanned and then combined to create a complete image.
48. **Progressive (popular for CMOS applications):** A type of image scanning in which all lines of an image are scanned sequentially to create a complete image.

49. **Recorders:** Devices that are used to capture and store audio or video data, such as a digital voice recorder or a video camera.
50. **Optical Camera Communication:** is considered one possible solution towards achieving a ready-to-use Li-Fi system by utilizing the camera's properties
51. **Visible Light Communication:** visible light communication (VLC) is the use of visible light as a transmission medium
52. **Video Management Software:** A video management system (VMS) orchestrates a surveillance workflow by integrating with cameras, encoders, recording systems, underlying storage infrastructure, client workstations, gateway systems and analytics software, mainly by providing a single interface for video surveillance infrastructure management.
53. **Free-space Optical Communications:** is an optical communication technology that uses light propagating in free space to wirelessly transmit data for telecommunications or computer networking. "Free space" means air, outer space, vacuum, or something similar. This contrasts with using solids such as optical fiber cable.
54. **Erasable Programmable Read-only Memory:** is memory that does not lose its data when the power supply is cut off. The data can be erased and the chip reprogrammed by shining an intense ultraviolet (UV) light through a window designed into the memory chip.
55. **Charged Coupled Device:** is an integrated circuit containing an array of linked, or coupled, capacitors. Under the control of an external circuit, each capacitor can transfer its electric charge to a neighboring capacitor. CCD sensors are a major technology used in digital imaging.
56. **Media Access Control:** is a network data transfer policy that determines how data is transmitted between two computer terminals through a network cable.

57. **Infrared:** having a wavelength just greater than that of the red end of the visible light spectrum but less than that of microwaves. Infrared radiation has a wavelength from about 800 nm to 1 mm, and is emitted particularly by heated objects.

Endnotes

1. N. Chikodiri, & O. Olihe, *National Security and Sustainable Economic Development in Nigeria since 1999:* Implication for the Vision 20 2020, 4,. 2014, 129-142. https://doi.org/10.5901/jesr.2014.v4n5p129.

2. S. Zahurul, N. Mariun, I.V Grozescu, H. Tsuyoshi, Y. Mitani, M.L Othman, H. Hizam, & I.Z Abidin, *Future strategic plan analysis for integrating distributed renewable generation to smart grid through wireless sensor network: Malaysia prospect* **Renewable and Sustainable Energy Reviews**, 53, 2016, pp.978–992. doi:https://doi.org/10.1016/j.rser.2015.09.02.

3. K. Abid, H. Lakhlef, & A. Bouabdallah, *A survey on recent contention-free MAC protocols for static and mobile wireless decentralized networks in IoT*, **Computer Networks**, 201, 2021 p.108583. doi:https://doi.org/10.1016/j.comnet.2021.1085.

4. S. Silvana, B. Valerio, C. Davide, Biancone & Paolo, *Towards a hybrid model for the management of smart city initiatives,* **Cities**, 116, 103278, 2021, https://doi.org/10.1016/j.cities.2021.103278

5. P.P. Ray, *A perspective on 6G: Requirement, Technology, Enablers, Challenges and future road map,* **Journal of Systems Architecture**, 118, 2021 pp.102180, doi:https://doi.org/10.1016/j.sysarc.2021.102180.

6. I. Haroon, S. Mubarak & S. Ray, *Enhancing Camera Surveillance Using Computer Vision: a Research Note*, **Policing**, 41, 2018, 292-307, https://doi.org/10.1108/PIJPSM-11-2016-0158

7. P.W. Khan, Y.-C. Byun, & N. Park, *A Data Verification System for CCTV Surveillance Cameras Using Blockchain Technology in Smart Cities*, **Electronics**, 9(3), 2020, pp.484. doi:https://doi.org/10.3390/electronics9030484.

8. S. Sukhavasi, S. Elleithy, K. Abuzneid, A. Elleithy & Abdelrahman, *Human Body-Related Disease Diagnosis Systems Using CMOS Image Sensors*: *A Systematic Review* **Sensors**, 21, 2021, 2098, https://doi.org/10.3390/s21062098.

9. ITU-T Telecommunication Standardization sector of ITU, G.9991: *High speed indoor visible light communication transceiver – System architecture, physical layer and data link layer specification*, 2019, http://handle.itu.int/11.1002/1000/11830-en

10. G. Véronique, P. Nicolas, B. Sébastien, & M. Véronique, *"Outdoor Optical Wireless Communication: potentials, standardization and challenges for Smart Cities*", 2020, https://doi.org/10.1109/WOCC48579.2020.9114953.

11. P. Eric, The History, "*Policy Implications, and Knowledge Gaps of the CCTV Literature: Insights for the Development of Body-Worn Video Camera Research".*

International Criminal Justice Review, 31, 2018, https://doi.org/10.1177/1057567718759583.
12. A. Jabbari, K. Almalki, B.-Y Choi & S. Song, *ICE-MoCha: Intelligent Crowd Engineering using Mobility Characterization and Analytics*. **Sensors**, 19(5), 2019, p.1025. doi:https://doi.org/10.3390/s19051025.

13. M. Cailean, Dimian, & Mihai. *Impact of IEEE 802.15.7 Standard on Visible Light Communications Usage in Automotive Applications,* **IEEE Communications Magazine**, 2017, pp.2-7, https://doi.org/10.1109/MCOM.2017.1600206CM.

14. IEEE 802.15 WPAN™ Task Group 13 (TG13), *Multi-Gigabit/s Optical Wireless Communications,* [Online], 2020, http://www.ieee802.org/15/pub/TG13.html.

Chapter Two

Literature Review

2.1 Conceptual Review

This section covers the parts within the broad literature on surveillance technology, that are most relevant to this paper. One of it is the security and privacy debate, which has been at the headlines in recent years. The issue here is central effectiveness, as the basis for the argument is for the use of any given surveillance program must be that it is effective and manageable in increasing security. However, any concise judgment must put into consideration, the privacy intrusion of the program against its effectiveness.

The review of the literature can be classified into three categories:

i. Actual effectiveness

ii. Belief of effectiveness and

iii. Statements of effectiveness[1].

We searched for surveillance technology evaluations published from 2013 through 2022, to account for the time period since the last review. Five comprehensive search strategies were used to locate studies meeting the inclusion criteria for this review.

Searches of electronic bibliographic databases. In the bibliographic databases were searched using relevant key words; Criminal Justice p mAbstracts, CrimeSolutions.gov, National Criminal Justice Reference Service (NCJRS) Abstracts, Sociological Abstracts, Educational Resources Information Clearinghouse (ERIC), Google Scholar, Government Publications Office Monthly Catalogue (GPO Monthly), Psychology Information (PsychInfo), Proquest Dissertation and Theses Global, Rutgers Gottfredson Library grey literature database, and the Campbell Collaboration virtual library.

Our review also found that the effect of surveillance technology is heterogeneous across crime types, the largest or effect size was observed for robbery crimes. This finding is intriguing in light of prior research reporting that armed robbers find it more easy to rob its victims, in definite absence surveillance technology. Our findings suggest that despite such robbery rampage from robbers, CCTV cameras may help combat the incessant robbery attacks. Research has found that drug sellers adopt situational prevention techniques to avoid apprehension by police which can include activities such as the involvement of multiple sellers in single transactions, stash-spots to store drugs, and mediation schemes meant to obscure transactions. These processes can be quite complex and difficult for police officers to observe on the street[2]. In this sense, surveillance system may help disrupt drug selling through the elevated position and telescopic capacity of cameras, which affords the operators greater range of vision than street-level police officers, once observed such benefits within a surveillance system control room, with a police Lieutenant monitoring a camera and relaying the following information to undercover officers in the field via two-way radio: "The guys I saw selling on street 1 yesterday are now on street 2, they just served (sold drugs to) a guy in a white mercedez, the kid who made the actual transaction is wearing a leave green t-shirt, the other 2 dealers are on street 3, one is wearing a black shirt with black hat and a beard; the other one has a blue jacket with white t-shirt and thinner beard, they keep walking towards the suburb; I think that's where the stash of drugs is[3]."

Surveillance system was associated with significant reductions in both vehicle crime and property crime in general, with no significant effects observed for violent crime. Public safety agencies combatting violent crime problems may need to consider whether resources would be better allocated toward other crime prevention measures. For jurisdictions with existing surveillance systems, public safety agencies may need to make changes to their

existing strategies to effectively combat violence. Actively-monitored surveillance system, which can detect incidents of concern in real time, may be able to deploy police officers on-scene before a situation escalates into serious violence. This potential benefit of CCTV was observed in their systematic social observation of violent crime events recorded in their entirety i.e., the moments immediately prior to, during, and following the event on CCTV[4].

Most violent crime incidents were preceded by an "intervention opportunity," such as a fight, disorderly behavior, or drug transaction, providing probable cause for a police response. Researcher argued that while a police response would not have guaranteed the prevention of the subsequent violent crime, police officers being on-scene would have made the incident less likely to occur than the absence of police presence[4]. Indeed, research hypothesized that early intervention by police may help increase the certainty of crime punishment in CCTV target areas, ultimately generating crime reductions. It randomized controlled trial pairing active CCTV monitoring with directed police patrol supported this causal mechanism, finding that violent crime as well as social disorder significantly decreased. It should be noted, however, that actively-monitored CCTV systems require a greater commitment of resources than passive systems. This is especially the case if agencies wish to maintain current levels of active monitoring as surveillance systems expand, because high camera-to-operator ratios can negatively affect active monitoring practices[2,3,4]. Towards this end, police have increasingly integrated crime control technologies such as gunshot detection technology (GDT) in an attempt to maximize efficiency, given that operators cannot monitor all cameras in a system simultaneously, such technology is expected to better focus operator attention by identifying precisely when an operator should monitor a specific camera. However, there is no guarantee that such technology will increase surveillance technology effectiveness. Further research has it

found that the introduction of GDT in Newark, New Jersey, did not improve active monitoring practices of surveillance system. Given the high cost associated with technology, introducing additional camera operators and/or patrol officers into surveillance operations may be a more cost-effective measure than complementary crime control technologies[2,3,4]. For example, the costs of the additional camera operators, police officers, and patrol vehicles deployed in Newark's CCTV Directed Patrol Project were approximately $76,000. In contrast, ShotSpotter, the industry leader in GDT technology, reports that subscriptions for their service cost between $65,000 and $90,000 per square mile per year. In the case of Newark, which has ShotSpotter's GDT installed in a seven square mile area of the city, this translates to a yearly cost of between $455,000 and $630,000. At an average cost of about $6,897 per week ($75,873.07 / 11-week intervention period), conducting the CCTV Directed Patrol Project each week of the year (totaling $358,644) would cost between $96,356 and $271,356 less per year than GDT[2,3,4].

However, we must note that technology besides GDT can be used in an attempt to improve CCTV monitoring functions and may provide a more cost-effective solution. Recently, research explored the potential benefits that computer vison technology (CVT; also known as machine learning) can provide to surveillance system interventions. CVT applies mathematical algorithms to each frame of CCTV footage for the purpose of automating the detection of crime related events. Upon detection of an image of concern such as a weapon, fugitive vehicle, or physical behavior indicative of crime (e.g., a person repeatedly striking a vehicle window as if trying to break in), CVT alerts the CCTV operator who may have been monitoring a different camera at the time. Within a CVT-assisted CCTV scheme, the primary role of the human operator is shifted from the traditional role of manually mining video footage in search of criminal behavior to a supervisory role emphasizing assessment of detected images and response decision-making i.e., whether to report detected events to

the police[5]. This may bolster the efficiency of active CCTV monitoring, as research has shown the bulk of camera operator time is spent on activities other than camera monitoring. To date, little use of CVT has been made by law enforcement[5]. None of the evaluations we identified for potential inclusion in this review mentioned the use of CVT. As the use of CVT expands, researchers should conduct case-controlled evaluations to measure whether CVT improves the effectiveness and efficiency of surveillance technology. Even with further policy insights from an increase in evaluations of surveillance technology, there continue to be opportunities for further improvement in evaluation research. For one, randomized controlled experiments are a rarity in the study of surveillance technology. Research carried out the only randomized experiments of surveillance technology in public settings, it was noted that, because CCTV cameras are hard wired to physical structures and configured to wireless communications networks, moving locations after experimentation would require additional expenditures. Other crime prevention strategies, such as hot spots policing or body-worn cameras, do not present such difficulties and are more amenable to randomization[6].

Nonetheless, random assignment of CCTV cameras may be possible in certain cases. As argued by researcher, agencies could identify priority locations at the outset of a program and randomly select a subset of locations to receive cameras during the first phase of installation. In a waiting-list design, other priority sites could receive cameras in later installation phases, after completion of the experiment. Under this strategy, officials could simultaneously generate the most rigorous evidence of the effects of surveillance technology while still ensuring that all priority locations received CCTV (presuming that experimental results support the installation of more cameras). In this sense, there may also be a role for re-deployable CCTV cameras, meaning that experimental areas can be moved around[6].

2.1.1 Surveillance Retail Intelligence

Surveillance Retail Intelligence offers an artificial intelligence (AI) platform that reviews and analyzes brick and mortar store cameras in order to radically improve store operations[6]. Market intelligence collected from video surveillance system of customers is being used to analyse buying trends or metrics and enable improved strategies, e.g. what and how do people shop, what is the probabilities of they responding to calls to action within different store area, which lane do they traverse the most. Heat maps metrics could show the highs and lows of shopper rate at specific locations in a store, assisting stores to recognize peak buying times, preferred promotion types, and recruiting requirements for peak shopping periods[7].

Surveillance retail intelligence refers to the use of advanced surveillance technologies and data analytics to gather insights and improve decision-making in the retail industry. The technology involves the use of cameras, sensors, and other monitoring devices to capture data on customer behavior, preferences, and buying patterns. This data is then analyzed using advanced algorithms and artificial intelligence to provide insights that can be used to optimize operations and enhance the customer experience[7].

One of the main benefits of surveillance retail intelligence is its ability to improve customer experience. By monitoring customer behavior, retailers can gain a better understanding of what customers want and need, and adjust their operations accordingly. For example, if a store notices that a particular product is frequently being picked up but not purchased, they may choose to lower the price or place it in a more prominent location[9].

Surveillance retail intelligence can also be used to improve store layout and design. By analyzing data on customer traffic and movement patterns, retailers can optimize store layout and product placement to increase sales and improve the customer experience. For example, they may choose to place popular items near the entrance to encourage customers to make a purchase before leaving the store[7,8].

Another benefit of surveillance retail intelligence is its ability to improve inventory management. By tracking product movement and analyzing customer purchasing patterns, retailers can optimize their inventory levels to ensure that they have the right products in stock at the right time. This can help to reduce waste and prevent stockouts, improving both profitability and customer satisfaction[8,9].

Surveillance retail intelligence can also be used to improve store security. By monitoring customer behavior and identifying suspicious activity, retailers can improve loss prevention and reduce shrinkage. This can be particularly important in high-risk environments such as convenience stores and pharmacies[9].

Overall, surveillance retail intelligence is an important tool for retailers looking to improve customer experience, optimize operations, and increase profitability. By leveraging advanced surveillance technologies and data analytics, retailers can gain a deeper understanding of customer behavior and use this insight to make more informed decisions. As technology continues to evolve, surveillance retail intelligence is likely to become even more important in the retail industry[9].

2.1.2 Surveillance Security Behavior

Surveillance Security behaviors allow control over credentials, authentication, authorization, and auditing logs. These behaviors can be utilized, either by programming or

through configuration. Surveillance system utilized to research suicide find out that 83 percent of people attempting to jump in front of a train showed a noticeable specific behaviors[10]. It was later analysed from CCTV footage and now used to alert surveillance monitor watchers to potential suicides. Surveillance system networks are also used by researchers to determine and record crowd activities in public places and prevent anti-social behaviors. For example, cameras have been used at academic places for security, and to record bullying, cultism or playground incidents on video[7].

Surveillance security behavior refers to the use of surveillance technologies to monitor and influence human behavior in order to improve security. This approach involves using cameras, sensors, and other monitoring devices to gather data on human behavior, and then using this data to identify and respond to security threats.

One of the main benefits of surveillance security behavior is its ability to improve situational awareness. By monitoring the environment and gathering data on human behavior, security personnel can gain a better understanding of potential security threats and respond more quickly and effectively. This can help to prevent security incidents and reduce the impact of those that do occur.

Surveillance security behavior can also be used to influence human behavior in order to improve security. For example, the presence of cameras can deter potential criminals from committing crimes, and the use of signage and other cues can encourage people to behave in a certain way (such as avoiding certain areas or reporting suspicious activity). This approach can be particularly effective in high-risk environments such as airports, stadiums, and other public spaces.

Another benefit of surveillance security behavior is its ability to provide evidence in the event of a security incident. By recording video footage and other data, surveillance technologies can provide valuable evidence that can be used to investigate incidents and prosecute criminals. This can help to improve accountability and deter criminal activity in the future.

However, there are also some concerns associated with surveillance security behavior. One of the main concerns is the potential for privacy violations. As surveillance technologies become more advanced, there is a risk that they may be used to collect personal data and infringe on individual privacy. This can be particularly concerning in situations where the surveillance is carried out by private organizations rather than government agencies.

Overall, surveillance security behavior is an important tool for improving security in a wide range of settings. By monitoring human behavior and influencing it in a positive way, security personnel can help to prevent security incidents and reduce their impact. However, it is important to strike a balance between security and privacy, and ensure that surveillance technologies are used in a responsible and ethical manner[7,8,9].

2.1.2.1 Types of Security Measures

There are two types of security measures which are preventive and detective measures. The preventive measure is aimed at preventing the occurrence of an undesired event by use of barriers or other devices such as cameras for surveillance[6]. Detective measure is performed after an undesired event has occurred to detect who or what has caused such event in order to prevent it from happening again, which is the basis of this study. We are taking into consideration, a preventive and detective security measures by integrating a CCTV system with a 2.4Ghz optical wireless video transceiver to multicast in a smart environment[7,8].

Meanwhile, in consideration of the technological implementation for this study, Optical Wireless Communication (OWC) is considered as part of a solution, it usually make use of the unlicensed ultraviolet, infrared light or visible spectrum bands. For over a decade, researchers have been working on UltraViolet Communication (UVC) applications, basically in the circle of long-distance nonline-of-sight (nLoS) communications. UV band is specified from 100 to 400 nm (Nautical Mile) and is classified into three zones: UV-A (400 to 315 nm), UV-B (315 to 280 nm) and UV-C (280-100 nm)[5]. The three can damage the skin, the significance of their physiological effects depends on the wavelength (the smallest wavelength, the greatest effect).

Table 2.1 Frequency & Wavelength Range Analysis[6].

Band	Frequency range	Wavelength range
Extremely Low Frequency (ELF)	<3 kHz	>100km
Very Low Frequency (VLF)	3 to 30 kHz	10 to 100km
Low Frequency (LF)	30 to 300 kHz	1m to 10km
Medium Frequency (MF)	300 kHz to 3 GHz	100m to 1km
High Frequency (HF)	3 to 30 GHz	10 to 100m
Very High Frequency (VHF)	30 to 300 GHz	1 to 10m

Therefore, this technology needs to be avoided and it is not discussed in this study as part of a possible solution smart cities insecurity. Rather, the Radio Frequency for OWC will be implemented in this study, as it has been a major technology for wireless technology in past centuries, with no physiological effect on human[6]. Variations of OWC can be potentially employed in a diverse range of communication applications ranging from

optical interconnects within integrated circuits through outdoor inter-building links to satellite communications, using Wi-Fi protocols.

Table 2.2: Wi-Fi protocol Summary[4].

Protocol	Frequency	Signal	Maximum Data Rate
Legacy 802.11	2.4 GHz	FHSS or DSSS	2 Mbps
802.11a	5 GHz	OFDM	54 Mbps
802.11b	2.4 GHz	HR-DSSS	11 Mbps
802.11g	2.4 GHz	OFDM	54 Mbps
802.11n	2.4 GHz or 5 GHz	OFDM	600 Mbps (theoretical)
802.11ac	5 GHz	256-QAM	1.3 Gbps

Where:

FHSS = Frequency Hopping Spread

Spectrum, DSSS = Direct Sequence Spread Spectrum,

OFDM = Orthogonal Frequency Division Multiplexing,

HR = High-Rate, QAM = Quadrature Amplitude Modulation[4].

Table 1.2 shows summary of IEEE 802.11 protocol, if we see there, the Legacy 802.11 is the first Wi-Fi protocol developed in the series of IEEE 802.11 having the maximum data rate 2Mbps. After that, the next versions developed with increasing maximum data rate of Wi-Fi.

2.1.3 Video Surveillance Applications

The fact remains that video surveillance is such an effective system especially when one thinks of its widespread use attests to its low investment cost. We are going to be discussing several video surveillance applications in the next few paragraphs.

2.1.3.1 Crime Management

CCTV surveillance can deter potential criminals. When a crime does occur, video footage can help law enforcement to investigate and later provide evidence for prosecution in a law court. Used in conjunction with CCTV, audio, thermal and other types of sensors can alert officials to occurrences that are out of the ordinary, e.g. a fire or gun shots at a location. For businesses, CCTV cameras can detect and monitor in-house criminal activities. Prisons may use video surveillance to prevent drones from delivering drugs and other contraband to prisoners. Security cameras are able to monitor areas that are not easily accessible, e.g. rooftops[8,9].

Crime management refers to the efforts of law enforcement agencies and other stakeholders to prevent, detect, investigate, and respond to criminal activity. Effective crime management requires a combination of strategies and tactics, including intelligence gathering, community policing, technological solutions, and criminal justice system reforms[9].

One of the key components of crime management is prevention. This involves identifying risk factors and implementing strategies to address them before criminal activity occurs. Prevention efforts may include community outreach programs, public education campaigns, and targeted interventions aimed at reducing specific types of crime.

Another important component of crime management is detection. Law enforcement agencies rely on a variety of tools and techniques to identify criminal activity, including surveillance technologies, forensic analysis, and informants. Effective detection requires a combination of resources, expertise, and technology.

Once criminal activity has been detected, law enforcement agencies must investigate the crime and gather evidence to support a prosecution. This may involve conducting interviews, collecting physical evidence, and analyzing data to identify potential suspects. Effective investigation requires a combination of technical expertise and advanced analytical tools[10,12].

In addition to prevention, detection, and investigation, crime management also involves responding to criminal activity in a timely and effective manner. This may involve deploying law enforcement personnel to the scene of a crime, coordinating with other agencies to ensure a swift and coordinated response, and engaging with the community to address concerns and prevent future incidents.

Finally, effective crime management requires ongoing evaluation and improvement. Law enforcement agencies must constantly review their strategies and tactics to identify areas for improvement and make adjustments as needed. This may involve evaluating the effectiveness of specific programs, analyzing crime data to identify trends, and engaging with the community to gather feedback and input[12].

Overall, crime management is a complex and multifaceted endeavor that requires collaboration and coordination among a wide range of stakeholders. By implementing a

comprehensive approach that includes prevention, detection, investigation, response, and evaluation, law enforcement agencies can help to reduce crime and improve public safety.

2.1.3.2 Disaster Management

With CCTV cameras, emergency services and rescue teams are able to scrutinize and monitor events in real time to pass on a "situation" through video to disaster management teams, e.g. from inside a cave, burning building, or from an helicopter flying over a scene[8,9].

Disaster management refers to the process of preparing for, responding to, and recovering from natural or man-made disasters. The goal of disaster management is to reduce the impact of disasters on individuals, communities, and infrastructure.

Preparedness is a key component of disaster management. This involves identifying potential hazards and developing plans and procedures to mitigate their impact. Preparedness activities may include training and education programs, developing emergency response plans, conducting drills and exercises, and establishing communication protocols.

In the event of a disaster, response activities are critical to saving lives and reducing damage. Response activities may include search and rescue operations, providing emergency medical care, evacuating affected populations, and providing food, water, and shelter to those in need. Effective response requires a coordinated effort among emergency responders, government agencies, and community organizations[9].

Recovery activities focus on restoring normal operations after a disaster has occurred. This may involve rebuilding infrastructure, providing financial assistance to affected individuals and businesses, and providing counseling and other support services to those who have

been impacted. Recovery activities can be lengthy and complex, and require a sustained effort over time.

Disaster management also involves ongoing efforts to reduce the risk of disasters and their impact. This may include investing in infrastructure to make it more resilient to natural disasters, implementing early warning systems to alert individuals and communities of potential hazards, and conducting research to better understand the causes and impacts of disasters[10].

Effective disaster management requires a multi-disciplinary approach that involves collaboration among government agencies, emergency responders, community organizations, and the private sector. By working together to prepare for, respond to, and recover from disasters, communities can minimize the impact of disasters on individuals, families, and businesses[10].

2.1.3.3 City and Community Street Monitoring

CCTV Cameras at traffic lights, link bridges, and other places in cities, monitor people to collect the traffic statistics as well as footage for over speeding. IoT birth the AoT which is a Chicago initiative to gather real-time data, weather and environment, about the city. Some of the sensory nodes include CCTV security cameras that detailed the images they record, but, prior to protecting individuals' privacy, will not transmit or store these images. Basically, a limited figures are stored for use by senior researchers so as to "design and develop the computer vision software". The project has encountered with some restrictions from privacy watchdogs[8,9].

City and community street monitoring refers to the use of surveillance technologies to monitor public spaces, including streets, sidewalks, and other public areas. The goal of

street monitoring is to enhance public safety, prevent crime, and deter unwanted behavior in public spaces.

One of the key benefits of city and community street monitoring is that it can provide law enforcement agencies with valuable intelligence and evidence to support criminal investigations. Street monitoring systems can capture video footage of criminal activity, which can be used to identify suspects and prosecute criminals.

In addition to its role in law enforcement, street monitoring can also serve as a deterrent to criminal activity. The presence of surveillance cameras in public spaces can discourage individuals from engaging in criminal behavior, as they are aware that their actions are being recorded and may result in legal consequences.

Street monitoring can also be used to improve traffic safety and manage traffic flow in busy urban areas. Cameras can be used to monitor traffic patterns, identify areas of congestion, and adjust traffic signals to improve the flow of traffic.

Another important benefit of street monitoring is that it can enhance community safety and help residents feel more secure in their neighborhoods. By providing a visible presence of law enforcement and capturing evidence of criminal activity, street monitoring can create a sense of security among residents.

However, there are also concerns about the use of street monitoring, particularly in terms of privacy and civil liberties. Critics argue that widespread surveillance can be intrusive and may lead to a chilling effect on free speech and other civil liberties.

To address these concerns, it is important that street monitoring systems are designed and implemented in a way that is transparent and respects individual privacy rights. This may involve limiting the use of surveillance technologies to specific high-risk areas, ensuring that footage is only accessed by authorized personnel, and establishing clear guidelines for the retention and use of surveillance footage.

Overall, city and community street monitoring can play an important role in enhancing public safety and preventing crime. However, it is important that surveillance technologies are used in a way that balances the need for security with individual privacy and civil liberties.

2.1.3.4 Medical Monitoring and Diagnosis

There are approximately 43 facial muscles that shows people's thoughts and feelings. Some smart software identifies these expressions, e.g. anxiety or pain, from images more easily than people can. CCTV surveillance cameras can also monitor hospital patients, for instance identifying potential medical crises in children or the elderly, e.g. an epileptic or a stroke, or asthma attack[8,9].

Medical monitoring and diagnosis refer to the use of technology to gather and analyze health-related data, with the aim of identifying and diagnosing medical conditions.

One of the most common applications of medical monitoring and diagnosis is in the management of chronic medical conditions. Patients with conditions such as diabetes, hypertension, and heart disease may use medical monitoring devices to track their vital signs, such as blood glucose levels, blood pressure, and heart rate. This data can be

transmitted to healthcare professionals who can use it to monitor the patient's health and adjust their treatment plans as needed.

Another important application of medical monitoring and diagnosis is in the detection and diagnosis of medical conditions. Technologies such as magnetic resonance imaging (MRI), computed tomography (CT) scans, and ultrasound can be used to capture images of internal organs and structures, which can be used to identify abnormalities or injuries. Blood tests and other diagnostic tests can also be used to detect the presence of specific conditions or diseases.

Medical monitoring and diagnosis can also be used to support telemedicine, allowing healthcare professionals to remotely monitor and diagnose patients. This can be especially useful in remote or underserved areas where access to healthcare is limited.

In recent years, advances in machine learning and artificial intelligence have also enabled the development of medical diagnosis and monitoring systems that can analyze large amounts of health data to identify patterns and trends. This can be especially useful in predicting and diagnosing diseases before symptoms appear, allowing for earlier intervention and treatment[9].

However, there are also concerns about the potential risks and limitations of medical monitoring and diagnosis technologies. For example, there is a risk of false positives and false negatives, and there may be privacy concerns related to the collection and use of health data.

To address these concerns, it is important that medical monitoring and diagnosis technologies are rigorously tested and evaluated, and that patient privacy is protected through secure data storage and transmission.

Overall, medical monitoring and diagnosis technologies have the potential to revolutionize healthcare by improving the accuracy and speed of diagnosis, enabling earlier intervention and treatment, and facilitating remote healthcare delivery.

2.2 Methodological Frameworks

Video surveillance, or closed-circuit television (CCTV), has become a highly popular and prevalent method of preventing crime in public space in many countries across the world. Although it often dominates the policy focus, questions have been raised about its effectiveness and social costs, as well as how it compares to alternative surveillance measures. The review of theoretical and programmatic understanding of surveillance draws attention to other widely used surveillance measures that perform a crime prevention function in public places. These include security guards, improved street lighting, place managers e.g., bus drivers and parking lot attendants, and defensible space i.e., changes to the built environment. The article reviews the research evidence on the effectiveness of the full range of public area surveillance measures and examines related social costs. It also serves to broaden the view of public area surveillance beyond the current narrow focus on surveillance technology[7].

Forward searches of surveillance system evaluations, we used Google Scholar and Research Gates to conduct forward searches of all evaluation studies identified in the prior review as well as during our updated search. Through this process, we obtained all articles

that cited a study included in this updated review and manually reviewed the references sections.

Contacts with leading researchers. These search strategies identified new surveillance technology evaluations. Several studies did not meet the inclusion criteria and thus were excluded. This process resulted in the collection of new evaluations of surveillance technology that met the inclusion criteria. In considering these new evaluations alongside those included in the last review, the present review includes lots of evaluations, with many providing the requisite data to be included in the meta-analysis. Our approach allowed for the inclusion of both published and unpublished studies in the systematic review. Published reports accounted for is about 78.7% of the evaluations, with 21.3% reports coming from the grey literature.

Researcher did a systematic review, incorporate rigorous methods for locating, appraising, and synthesizing evidence from prior evaluation studies, using a similar level of reporting detail that characterizes high-quality reports of original research. In following this framework, we incorporated a rigorous approach to identify evaluation studies for inclusion in our review[8].

In this phase of approach, the usability attribute evaluation will be adopted, by recent research in this study. People At Center of Mobile Application Development (PACMAD) originated, by integrating the usability attributes developed, regularized by the International Organization for Standardization (ISO). This is a phase that review the PACMAD usability attributes, prior to developing the metric to measure usability of Surveillance System. Figure 2.1 below describes the most common usability evaluation

attributes based on Lillian-Yee-Kiaw W , ISO, with the recent integration of usability attributes in PACMAD model obtained from literature[9].

Figure 2.1: PACMAD UE Framework[9].

2.3 Review of Related Works

Scientific views was presented on the history of mankind and the current global threats, their dangers and nature. In particular, the existence of constructive ideas and destructive ideas influences their interests in global threats and the problem of protection from Them[10].

Manual searches of surveillance system evaluation study bibliographies, as our search progressed, we conducted manual searches of the references section of each study

identified for potential inclusion. For manual searches of other surveillance system study bibliographies, we conducted manual searches of the following theoretical articles, policy essays, qualitative studies, and literature reviews published in the last 9 years which reviews the CCTV and BWVC literature across four main areas of inquiry are:

i. Program effect and common outcome measures,

ii. Contextual factors influencing program effect,

iii. Intervention costs, and

iv. Implementation issues[8,10].

A research was carried out, on the effectiveness of surveillance cameras in reducing crime suffers from potential threats to causal certainty. This particular paper reviews seven studies that address some of these problems using the rigorous research designs of randomized and natural experiments. Included studies that reported changes in total crime found crime reductions ranging from 24 to 28% in public streets and urban subway stations, but its effectiveness in parking facilities or suburban subway stations are not commendable. Moreover, surveillance cameras may help reduce unruly behaviour in academic campuses, football stadiums and theft in supermarkets/mass merchant stores. These findings proved that video surveillance can reduce crime in several settings[11].

There was another research on surveillance technologies and crime control: understanding police detainees' perspectives on police body-worn video (BWV) and CCTV cameras[12].

Researcher presents the current state of the art and direction of research in computer vision aimed at automating the analysis of surveillance system images. It includes low level recognition of objects within the field of view of cameras, upon following those objects

over time and between cameras, as well as the interpretation of those objects' appearance and movements with regards to models of behavior (therefore intentions inferred). The potential ethical problems and some potential opportunities, in this case, such developments may pose if and when deployed in the real world are being presented, and suggestions being made as to the necessary new regulations which will be needed if such systems are not to further enhance the power of the surveilles against the surveilled[13].

The review that the fear of crime may have negative impact for health and wellbeing, is influenced by factors in the physical and social environment. This study aimed to review and harmonize qualitative evidence from the UK on fear of crime and the environment with the use of special methods of searching Eighteen databases, including crime, health and social science databases. Qualitative studies conducted in the UK which presented data on fear of crime and the environment were included. Quality was assessed using Hawker et al.'s framework. Data were harmonized thematically. The total of 40 studies were included in the review. Several factors in the physical environment are assumed to impact on fear of crime, including visibility and signs of abandon. However, factors in the local social environment appear to be more important as pioneer of fear of crime, including familiarity and social networks and, broader social factors appear to be of limited relevance. Certainly, there is considerable evidence for limitations on physical activity as a result of fear of crime, but less for mental health impacts[14].

Visible Light Communication has emerged as a prominent technology for wireless communication due to benefits such as license, bandwidth, coexistence and security. In addition, it was officially standardized by IEEE 802.15.7 in 2011[15]. However, it encounters certain challenges that can be term as criteria to develop a revised version. OCC operates in the same channel band as VLC with more benefits on receiver characteristic and it is party

to the standardization of issues in IEEE 802.15[16]. There are extensive research on OCC technologies, new spectrum targeting, multiple-input-multiple-output diversity, transmission access, and novel architectures with augmented reality user experience for the extended 5G wireless network[17].

Review of past studies gathered that a Media Access Control (MAC) and Physical (PHY) layer use light wavelengths from 10,000 nm to 190 nm in optically transparent media for OWC[18]. The standard is capable of transferring data rates up to 10 Gbit/s at distance in the range of 200 meters unrestricted nLoS. It is designed for point-to-point and point-to-multipoint communications in both non-coordinated and coordinated topologies. The standard is capable of transferring data rates sufficient to support video and audio multimedia services and at the same time considers mobility of the visible link, impairments due to noise and interference from sources like ambient light, compatibility with visible-light infrastructures and a MAC layer that houses visible links. The standard adheres to eye safety regulations applicable[19,20].

Scientific investigation shows the possible urban outdoor solution, to free up the RF spectrum for smart cities users, a single point of failure from machine malfunctions, purposeful or accidental human behavior, can make the whole framework stop working. They were able to come up with a solution of an IoT based blockchain technology[21].

There have been many articles written on the privacy concerns raised by the intersection of modern technology and government surveillance, some of the authors lay accusations on western democracies of falsifying the threat of terrorism to justify mass surveillance and also of exaggerating its role in preventing terrorist activity[23].

2.3.1 Surveillance Technology

Surveillance technology is an electronic device / system utilizing an electronic device, or similar technological tool designed, or primarily intended to collect audio, electronic, visual, location, thermal, olfactory, biometric, or similar information specifically associated with, or capable of being associated with, any individual or group[17,23,24].

Furthermore, a data verification system for CCTV surveillance cameras using Blockchain Technology was invented, the system ensures the authenticity of the stored recordings, allowing authorities to validate whether or not a video has been altered. It helps to distinguish fake videos from original ones and to make sure that surveillance cameras are authentic. This immutable ledger reduces the risk of copyright intrusion for law enforcement agencies and users by securing possession and identity[21].

In 2013, The U.S. Department of Homeland Security established a System Assessment and Validation for Emergency Responders Program to assist emergency responders making procurement decisions, the system serves basically as a security force booster, providing surveillance for a wide area, often time, than would be viable with security personnel alone. The system is often used to support complex security systems by integrating video coverage and security alarms for barriers, intrusion detection, and access control[25].

There are three classical model of surveillance processes, which are:

a) Capture and collation of data

b) Analysis and interpretation of data (to generate information)

c) Dissemination of information

2.3.2 Decentralization / Multicast

In computer networking, multicast is group communication where data transmission is addressed to a group of destination computers simultaneously. Multicast can be one-to-many or many-to-many distribution[26]. Multicast should not be confused with physical layer point-to-multipoint communication.

During data transmission in multicasting using IEEE 802.11n WLANs standard, the common two problems that usually occur is poor consistency and low data rate broadcast[20]. A new protocol was implemented to eradicate these problems which is cross layer optimisation[28].

Project REMP (Reliable Efficient Multicast Protocol), by Gopikrishnan R., is basically suggested for MAC level Multicast protocol for increasing reliability and efficiency. Vinod B Durdi, P. T. Kulkarni, and K. L. Sudha, developed methods to take care of resource allocation in cooperative wireless a sensor networks (CWSNs). The most challenging area of the CWSNs is the quality of service i.e. how to guaranty multimedia content delivery[26,28].

2.3.3 Optical Wireless Communication

Variations of OWC can be potentially employed in a diverse range of communication applications ranging from optical interconnects within integrated circuits through outdoor inter-building links to satellite communications.

OWC can be divided into five categories based on the transmission range:

Ultra-short Range: chip-to-chip communications in stacked and closely packed multi-chip packages.

Short Range: wireless body area network (WBAN) and wireless personal area network (WPAN) applications under standard IEEE 802.15.7, underwater communications.

Medium Range: indoor IR and VLC for wireless local area networks WLANs and inter-vehicular and vehicle-to-infrastructure communications.

Long Range: inter-building connections, also called free-space optical communications (FSO).

Ultra-long Range: Laser communication in space especially for inter-satellite links and establishment of satellite constellations[28,29].

Future research should continue to ensure the policy relevance of CCTV research. It is important to note that knowing whether a technology "works" is not enough for policymakers; the contextual and procedural aspects necessary to maximize effects are equally important when considering the adoption of a crime prevention technology. In recognition of this fact, the College of Policing developed the What Works Toolkit to summarize the research evidence on a variety of crime prevention strategies in a format that is easily interpreted by practitioners.18 The toolkit identifies five dimensions of programs that

are of interest to policy makers:

- Intervention effect,
- Causal mechanisms,
- Moderating factors
- Implementation issues, and
- Economic costs[35].

The College of Policing noted that Surveillance Technology meta-analyses have provided a great deal of evidence on the intervention's effect, causal mechanisms, and moderating factors, but have generated much less evidence on implementation issues and economic costs. In a sense, this is unsurprising given that the Toolkit focused on meta-anlyses that exclusively included studies incorporating crime as an outcome measure. In order to generate sufficient knowledge on implementation issues and economic costs associated with Surveillance Technology, researchers may need to conduct systematic reviews that

prioritize research directly focusing on these factors, irrespective of whether crime was directly tested in the evaluation.

Lastly, researchers should expand the focus of Surveillance Technology evaluations to include more outcome measures than crime prevention. While crime prevention is obviously an important consideration, police departments also largely invest in Surveillance Technology, for its ability to detect and identify offenders for investigatory purposes. Despite this potential benefit of the technology, a body of research on the investigatory benefits of Surveillance Technology has yet to develop. To our knowledge, represent the only case-controlled tests of Surveillance Technology's effect on on-scene offender apprehension and retroactive criminal investigations, respectively. The field would benefit from an increased evidence-base on the effect of Surveillance Technology on such outcomes[36].

2.4 Summary of Gaps in Literature Reviewed

After critical review of past studies, it was gathered that most of the surveillance system are IoT based centralized system, which is expensive, not user friendly and increases the venerability of system breach to attackers.

The review of related literature is in Table 2.3 below

AUTHORS WITH DATES	PAPER TITLE	PROBLEM SOLVED	METHOD USED	LIMITATION
Prince Waqas Khan Yung-Cheol Byun Namje Park 2020	A Data Verification System for CCTV Surveillance Cameras Using Blockchain Technology in Smart Cities	Crime prevention and examinations in smart cities	IoT combined but blockchain-based	A single point of failure from machine malfunctions, purposeful or accidental human behavior, can make the whole framework stop working
Amanda Thomas, Eric Piza Brandon C. Welsh David P. Farrington 2011	The Internationalization of CCTV Surveillance: Effects on Crime and Implications for Emerging Technologies	Crime prevention and policing across the world	Systematic review methods with meta-analytic techniques	The standard of the system proposed is tedious to implement which slowed down its implementation in several countries
Ammar Gharaibeh, Mohammad A. Salahuddin, Sayed Jahed Hussini, Student and Ala Al-Fuqaha, 2017	Smart Cities: A Survey on Data Management, Security, and Enabling Technologies	The projects aimed at offering new data and access to increase the efficiency of the city services and to reduce the consumption of esources	Object Level Frame comparison methodology was used with Machine learning algorithm was used.	The main challenge faced is that the data generated by smart city applications are voluminous, which sometimes results to deadlocks

Neeraj Kaushik Dr. Teena Bagga 2021	Smart Cities Using IoT	The use of IoT to maintain E-governance, smart transport, smart waste management, smart water management, smart energy management to make a smart city	These IoT technologies; Sigfox, Ingenu, Lora, weightless, and RPMA were considered	Network requirement for each smart section differs

Endnotes

1. Shen B, *Research on Video Remote Transmission Technology Based on FPGA.* IOP Conference Series: Materials Science and Engineering, 382, 2018, https://doi.org/10.1088/1757-899X/382/4/042031.

2. E. I. Piza, & V. A Systma, *Exploring the Defensive Actions of Drug Sellers in Open-air Markets: A Systematic Social Observation,* **Journal of Research in Crime and Delinquency**, 53. 2016, pp.36-65, https://www.researchgate.net/journal/Journal-of-Research-in-Crime-and-Delinquency-0022-4278.

3. Z. Shu, M.Z.Q. Chen, & Q. Hui, *Advanced Mathematical and Numerical Methods in Control and Optimization for Smart Grids* **Mathematical Problems in Engineering**, [online] 2019, p.e2074019. doi:https://doi.org/10.1155/2019/2074019.

4. P Eric, C. Joel & K. Leslie. *CCTV as a Tool for Early Police Intervention: Preliminary Lessons from Nine Case Studies.* **Security Journal**, 30, 2017, https://doi.org/10.1057/sj.2014.17.

5. I. Haroon, S. Mubarak & S. Ray, *"Enhancing Camera Surveillance Using Computer Vision":* a research note, **Policing**. 41, 2018, pp.292-307, https://doi.org/10.1108/PIJPSM-11-2016-0158.

6. P. Eric, The History, *Policy Implications, and Knowledge Gaps of the CCTV Literature: Insights for the Development of Body-Worn Video Camera Research,* **International Criminal Justice Review**, 31, 2018, https://doi.org/10.1177/1057567718759583.

7. Z. Zhang, S. Qian, Q. Zhang, & L. Li, *Advanced Concrete Technology and Its Structural Applications,* **Advances in Civil Engineering**, 2022, pp.1–4. doi:https://doi.org/10.1155/2022/9781273.

8. P.W. Khan, Y.-C. Byun, & N. Park, *A Data Verification System for CCTV Surveillance Cameras Using Blockchain Technology in Smart Cities*, **Electronics**, 9(3), 2020, pp.484. doi:https://doi.org/10.3390/electronics9030484

9. Z. Lv, K. Ota, J. Lloret, W. Xiang, & P. Bellavista, *Complexity Problems Handled by Advanced Computer Simulation Technology in Smart Cities 2021*. **Complexity**, 2022, pp.1–3. doi:https://doi.org/10.1155/2022/9847249.

10. I.-H. Lee, J.-B. Kim, H. Jung, S.-C. (Sean) Kwon, & E. Kurniawan, (2019). *Advanced Wireless Technology for Ultrahigh Data Rate Communication*, **Wireless Communications and Mobile Computing**, 2019, pp.1–2. doi:https://doi.org/10.1155/2019/9790853.

11. P.-C. Chiu, K.-W. Su, T.-Y. Ou, C.-L. Yu, C.-Y. Cheng, W.-C. Hsiao, M.-H. Shu, & G.-Y Lin, , *An Adaptive Location-Based Tracking Algorithm Using Wireless Sensor Network for Smart Factory Environment.* **Mathematical Problems in Engineering**, [online] 2021, p.e4325708. doi:https://doi.org/10.1155/2021/4325708.

12. Y. Luo, *Construction of Smart Higher Education Teaching Resources Using Data Analysis Technology in Unbalanced Data Environment,* **Journal of Environmental and Public Health**, 2022, pp.1–12. doi:https://doi.org/10.1155/2022/2130623.

13. S. Zhu, C. Zhou, & Y. Wang, *Highly Efficient Multicast over Surface Wave in Hybrid Wireless-Optical On-Chip Networks for IoT HPC,* **Wireless Communications and Mobile Computing**, [online] 2022, p.e3882894. doi:https://doi.org/10.1155/2022/3882894.

14. M. Yadav, K. Singh, A.S. Pandey, A. Kumar, & R. Kumar, *Smart Communication and Security by Key Distribution in Multicast Environment,* **Wireless Communications and Mobile Computing**, [online] 2022, p.e1011407. doi:https://doi.org/10.1155/2022/1011407.

15. R. Agrawal, N. Faujdar, C.A.T. Romero, O. Sharma, G.M. Abdulsahib, O.I. Khalaf, R.F. Mansoor, & O.A Ghoneim, *Classification and Comparison of AdHoc Networks: A review*. **Egyptian Informatics Journal**, [online] 24(1), 2023, pp.1–25. doi:https://doi.org/10.1016/j.eij.2022.10.004.

16. W. Tan, Y. Fen, & Q. Yuan, *Optimization of Historic Building Survey Technology under Artificial Intelligence Wireless Network Technology Environment*. **Wireless Communications and Mobile Computing,** 2021, pp.1–12. doi:https://doi.org/10.1155/2021/6408772.

17. S. Narejo, B. Pandey, D. Esenarro vargas, C. Rodriguez, & M.R. Anjum, *Weapon Detection Using YOLO V3 for Smart Surveillance System*, **Mathematical Problems in Engineering,** 2021, pp.1–9. doi:https://doi.org/10.1155/2021/9975700.

18. X. Cui, *Explore the Application Effect of Wireless Networks in Smart Clothing Based on Artificial Intelligence Technology,* **Wireless Communications and Mobile Computing**, 2022, pp.1–9, doi:https://doi.org/10.1155/2022/6937128.

19. IEEE 802.15 WPAN™ Task Group 13 (TG13), *"Multi-Gigabit/s Optical wireless Communications,"* [Online]. Available: http://www.ieee802.org/15/pub/TG13.html, 2020.

20. S. Bhattacharjee, T. Acharya, & U. Bhattacharya, *Cognitive radio based spectrum sharing models for multicasting in 5G cellular networks: A survey,* **Computer Networks**, [online] 208, 2022, p.108870. doi:https://doi.org/10.1016/j.comnet.2022.108870.

21. A. Ibnu Febry Kurniawan, Taufiq Asyhari, F. He, & Y. Liu, *Mobile computing and communications-driven fog-assisted disaster evacuation techniques for context-aware guidance support: A survey.* 179, 2021, pp.195–216. doi:https://doi.org/10.1016/j.comcom.2021.07.020.

22. Y.-S. Chen, C.-K. Lin, & Y.-W Kan, *An Advanced ICTVSS Model for Real-Time Vehicle Traffic Applications*, **Sensors**, 19(19), 2019, p.4134. doi:https://doi.org/10.3390/s19194134.

23. A. Ali, A. Ali, F. Masud, M.K. Bashir, A.H. Zahid, G. Mustafa, & Z. Ali, *Enhanced Fuzzy Logic Zone Stable Election Protocol for Cluster Head Election (E-FLZSEPFCH) and Multipath Routing in wireless sensor networks.* **Ain Shams Engineering Journal,** [online] 2023, p.102356. doi:https://doi.org/10.1016/j.asej.2023.102356.

24. R. Xu, S.Y. Nikouei, D. Nagothu, A. Fitwi, & Y. Chen, *BlendSPS: A BLockchain-ENabled Decentralized Smart Public Safety System,* **Smart Cities**, 3(3), 2020, pp.928–951. doi:https://doi.org/10.3390/smartcities3030047.

25. United State Department of Homeland Security; *Prepared by Space and Naval Warfare Systems Center Atlantic.* CCTV Technology Handbook 2013

26. D. Vinod, K. Prahlad & K.L. Sudha, *Robust Video Transmission over Wireless Networks Using Cross Layer Approach,* **Journal of Industrial and Intelligent Information**, 1, 2013 97-101. https://doi.org/10.12720/jiii.1.2.97-101.

27. M. Kim, K.L. Man, & N. Helil, *Advanced Internet of Things and Big Data Technology for Smart Human-Care Services*. **Journal of Sensors**, 2019, pp.1–3. doi:https://doi.org/10.1155/2019/1654013.

28. X. Yuchen, W.P. Guan, W. Shangsheng, L. Jingyi, L. Zeyang, L. Manxi, *The Optical Bar Code Detection Method Based on Optical Camera Communication Using Discrete Fourier Transform.* **IEEE Access**, 2020, pp.1-1, https://doi.org/10.1109/ACCESS.2020.3006752.

29. K. Abid, H. Lakhlef, & A. Bouabdallah, *A survey on recent contention-free MAC protocols for static and mobile wireless decentralized networks in IoT,* **Computer Networks**, 201, 2021, 108583, doi:https://doi.org/10.1016/j.comnet.2021.108583.

30. A. Matthew, *The Value of CCTV Surveillance Cameras as an Investigative Tool: An Empirical Analysis***. European Journal on Criminal Policy and Research**, 2017, 23, https://doi.org/10.1007/s10610-017-9341-6.

31. B. Anthony, W. David & T. Brandon, *Focused Deterrence Strategies and Crime Control: An Updated Systematic Review and Meta-Analysis of the Empirical Evidence,* **Criminology & Public Policy**, 2018, 17. https://doi.org/10.1111/1745-9133.12353.

32. J. Zhao, *Construction of College Chinese Mobile Learning Environment Based on Intelligent Reinforcement Learning Technology in Wireless Network Environment,* **Wireless Communications and Mobile Computing**, 2022, pp.1–10. doi:https://doi.org/10.1155/2022/5164430.

33. H. Du, & Y. Zhang, *Ensemble Learning-Based Multi-Cues Fusion Object Tracking in Complex Surveillance Environment,* **Computational Intelligence and Neuroscience**, [online] 2022, p.e9165744. doi:https://doi.org/10.1155/2022/9165744.

34. W. Wang, X. Chen, G. Zhang, J. Qian, P. Wei, B. Wu, & H. Zheng, *Precision Security: Integrating Video Surveillance with Surrounding Environment Changes,* **Complexity**, 2018, pp.1–10. doi:https://doi.org/10.1155/2018/2959030.

35. J. Shane, T. Nick & B. Kate, *Introducing EMMIE: An evidence rating scale to encourage mixed-method crime prevention synthesis reviews,* **Journal of Experimental Criminology**, 2015, 11, https://doi.org/10.1007/s11292-015-9238-7.

36. P. P Ray, *A perspective on 6G: Requirement, Technology, Enablers, Challenges and Future Road Map.* **Journal of Systems Architecture,** 118, 2021, doi:https://doi.org/10.1016/j.sysarc.2021.102180

Chapter Three

Methodology

3.1 Research Approach

The approach used in this study is the development of technical artifacts (use of experiments), with a quantitative investigation of phenomena. A purposive sampling technique was implemented to assume transmission frequency range and wavelength range within tested location. Purposive sampling theory suggests, it is implemented where the insight quality is sufficient to offer valid information into the investigation[1].

The purpose of the above approach was to help for crime prevention and detection, within an enclosed geographical location, enabling residents in the community to join forces with one another and contribute their own quota in securing their environment, lives and properties, through a surveillance system monitoring. An alpha pre-test was conducted before the experiment, followed by a beta post-test[2]. This implies the process of integrating the hardware devices to give the required output and connectivity, such as, power supply test, 12v 5watts Direct Current was supplied into the system and there was an interference in communication, another is the absence of storage device (hard-disk), which result to an error message "No storage device installed", then the error was fixed by installing a storage device, which gave the expected result[3,4].

Table 3.1 below illustrates the alpha pre-test, experiment and beta post-test

Table 3.1: The alpha pre-test, experiment and beta post-test.

Sequence	Alpha Pre-test	Experiment	Beta Post-Test
Control apparatus	Tested usability of the System, observed some inhibitions	No experiment	Tested usability of the System, observed some inhibitions
Experiment apparatus	Tested usability of the System, observed some inhibitions	Integrated the system for multicast	Tested usability of the System, observed some inhibitions

Source: [1]

3.2 System Design

3.2.1 Surveillance Technology

Surveillance technology is an electronic device / system utilizing an electronic device, or similar technological tool designed, or primarily intended to collect audio, electronic, visual, location, thermal, olfactory, biometric, or similar information specifically associated with, or capable of being associated with, any individual or group[6].

There are three classical model of surveillance processes, which are:

d) Capture and collation of data

e) Analysis and interpretation of data (to generate information)

f) Dissemination of information

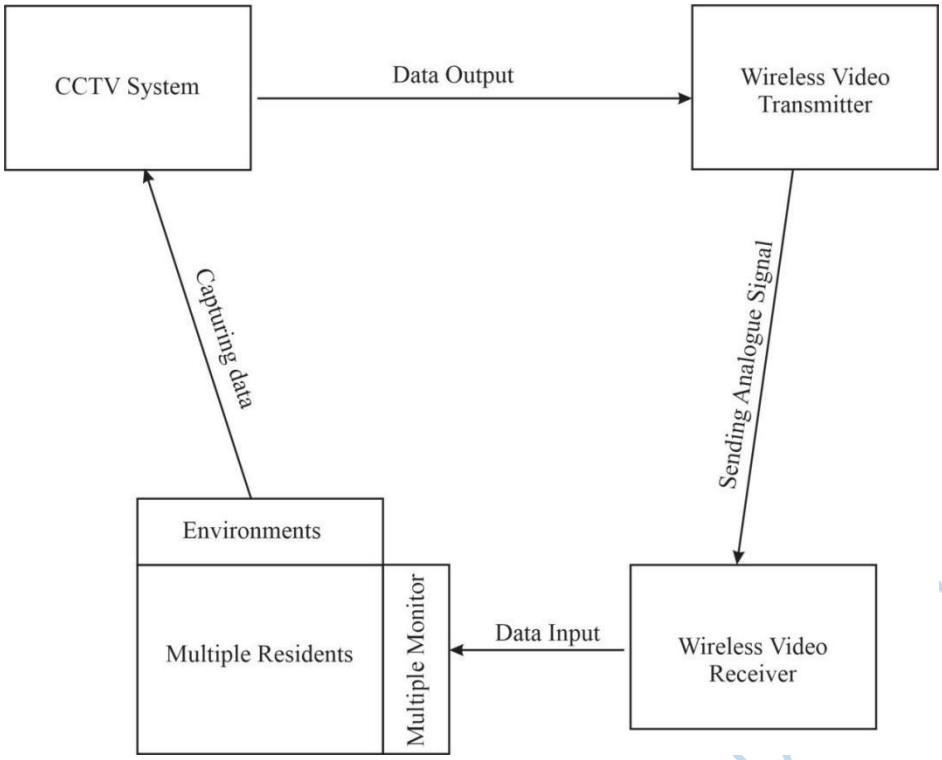


Figure 3.1: Proposed Surveillance System Multicast Conceptual Diagram

Source: [1]

Where: CCTV System is setup to capture data and store with proper and required equipment

Integrate a Wireless Video Transmitter

Signal sent to the Wireless Video Receiver

Wireless Video Receiver is plugged to monitors for Multicast

Surveillance technology crucial to human living and is applicable in several human day to day activities such as: Transportation, Health Care, Waste Management, Smart Water, e-governance, CCTV Surveillance System etc[7,8].

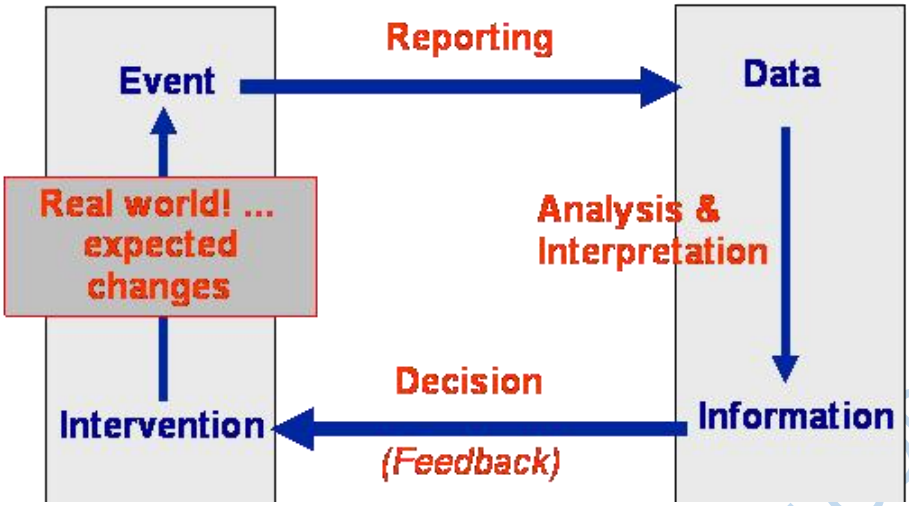


Figure 3.2: A typical Surveillance System Cycle.

Source: [2]

This is a typical surveillance life cycle, showing how the data collected is considered an information for decision making, which requires an intervention, creating an event for a report.

Furthermore, looking a CCTV surveillance system, it is the commonly use surveillance technology globally for security improvement and enhancement.

Basic CCTV System Specifications are:

a) CCTV Cameras

b) Digital or Network Video Recorder

c) Monitor

Analog and digital CCTV systems work quite differently but modern CCTV networks use conversion software and hardware to convert analog to digital. This process is called retrofitting.

The traditional CCTV Surveillance system comprises:

- One or more cameras (analog or digital), each with a lens equipped with an image sensor
- A recorder – Either a standard video tape recorder for analog systems, or a Digital Video Recorder (DVR) or Network Video Recorder (NVR) for digital systems
- Cables – Either Cat5 for digital or coaxial RJ59 for analog
- One monitors to which the images are transmitted through cable or more which images are transmitted through internet.

3.2.1.1 Basic CCTV Architectural Diagram

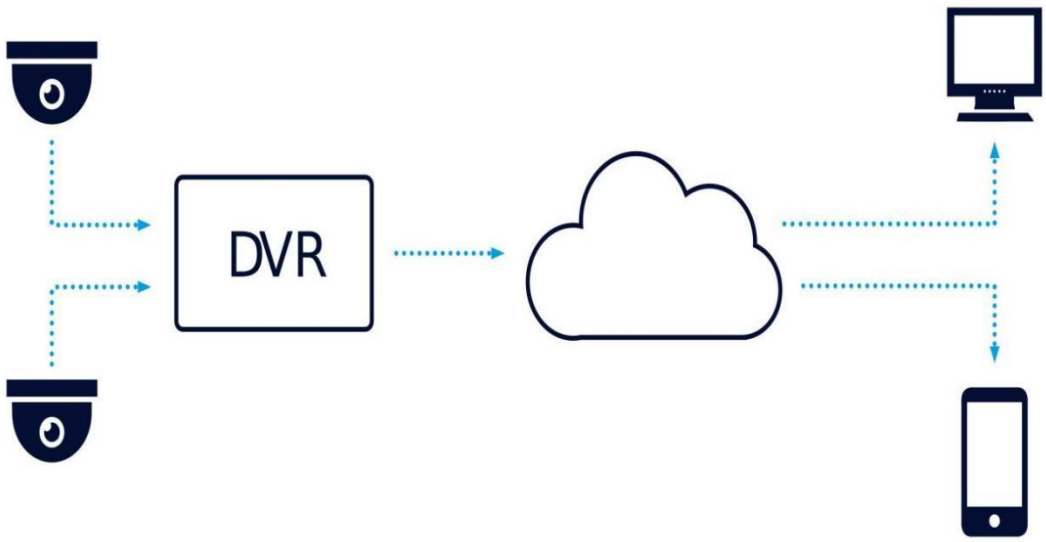


Figure 3.3: Basic CCTV surveillance system architecture.

Source: [3]

Camera(s) records image**s** through the lens using image sensors with the help of DVR, these images (and often audio too) are transmitted to the recorder, either wirelessly or by cable. Recorders may use analytical software and other smart technologies to scan the data and send automated alerts to either humans, or other systems and devices. This Video Management Software records, stores and analyzes video feeds. The software is often self-

learning, using machine learning algorithms that utilize functionality like motion detection, face recognition, people counting, etc. Monitor(s) can be passively (through software) or actively (by people) monitored. CCTV networks can, and should, themselves be monitored[8,9].

CCTV security recording systems are commonly integrated with new and existing devices, with the wide variety of CCTV cameras on the market, and new advances in technology being made all the time, there is a lot to learn about CCTV Surveillance system due to its broad discovery possibilities, which is the reason for this study, a wireless video transmitting module will be developed and integrated with the CCTV system for an uninterrupted multicast[8,9].

3.2.1.2 CCTV Cameras Implementation

IP camera is a type of digital video camera that receives control data and sends image data via the Internet. Unlike analog CCTV (Close-Circuit Television) cameras, they require no local recording device, but only a local area network. Some IP cameras require a NVR (Network Video Recorder) to handle the recording, video and alarm management, where some IP Cameras are standalone, which can operate without an NVR, as the camera is able to record directly to a SD Card (if the Camera supports an SD Card). IP cameras are Digital and connect via Cat5 (Networking) Cable or WiFi. The resolution of IP cameras is measured in Megapixels. It provides Plug & Play Ease of Use.

The basic and well recognized type of IP Camera is the Pan and Tilt, which requires the user input to move the camera to wherever he wishes to look into. But a new type of IP Camera is steadily emerging called the Fish-Eye IP Camera which has no moving parts.

3.2.1.3 Video Recorder

There are two main types of recording systems in the market. The first being the DVR which is cheaper and easier to setup. The second being the NVR which is fairly more expensive and requires some technical knowledge.

DVR (Digital Video Recorder) are mostly wired. Special equipment is needed to make it wireless.

DVR uses analogue cameras which need a two-core cable for signal. Usually coax cables are used and u need an additional cable for power.

NVR systems run either via ethernet cables or wireless. Higher picture quality (720p, 1080p) can be achieved by NVR compared to DVR.

NVR cables are ethernet if you go with the wired option. Also there are PoE (Power over Ethernet) meaning both power and signal can be sent through one ethernet cable. You could also opt in for wireless at the time of purchase.

NVR uses IP cameras as those type of cameras work on a network using ethernet cables or WiFi.

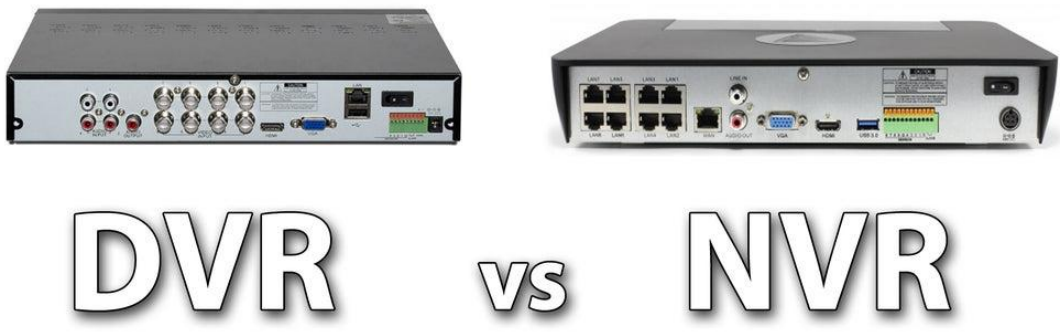


Figure 3.4: Typical DVR & NVR diagram

Source: [9]

The larger the HDD, the further you can playback. The higher the quality of the camera, the lesser you can playback as it takes more space. In my estimate an 8 channel 1080p NVR with a 1TB HDD will give you roughly a week of playback. Probably lesser cos the quality is high.

Recording capacity is a function of disk space (channels x resolution x frame rate). If you get 1 week at 30fps, dropping to 15fps (still quite usable) would give you two weeks of playback.

3.2.2 CCTV Integration System

As discussed earlier, CCTV recording systems are commonly integrated with new and existing devices. With the traditional CCTV surveillance system, a wireless video transceiver module will be integrated with the CCTV system for an uninterrupted multi-streaming[8].

3.2.3 Wireless Video Transceiver

A transceiver is a combination transmitter/receiver in a single package. While the term typically applies to wireless communications devices, it can also be used for transmitter/receiver devices in cable or optical fiber systems[6,8]. The transceiver module is developed on 2.4Ghz frequency, with a PCB Antenna; which is a transducer converting current waves into EM waves in a high-frequency PCB. PCB antennas convert current in high frequency into EM waves that propagate into the air. There are two PCB antennas in a high-frequency PCB. They are embedded into the PCB as the etched copper structure. The transmission ranges from 200 meters up to 20 kilometers. Even in highly disturbed industrial environments, this will serve an effective system of tightening the security with

number of video channels, combined with a highly effective wireless video transmission module. In addition, the time required to carry out monitoring is reduced, with unlimited transmission possibilities. With well thought-out solutions, the wireless video transmitting module are adapted to all types of CCTV system in every standard, from IP, to AHD, 720dpi, 1080 dpi up to 4 and 8k. They can be installed outside and indoors, for several meters and several dozen km of wireless range, sending data from the DVR/NVR to several monitors[10].

Table 3.2.: Wireless Video Transceiver Specifications

Power Supply	DC12V-24V
Consumption Current	200mA
Tx Channel	1 to many
Output Power	200mW
Unobstructed Effective Range	150 ~ 200 m
Operating temperature	-10°c ~ +50°c

Source: [5]

The proposed device has two parts integrated, the first part is transmitter and second one is receiver. The device receiver can be plugged in any monitor using AV or HDMI port. The Wireless Video Transceiver works on the concept of Internet Protocol (IP) multicast for Local Area Network. IP multicast allows to broadcast a single information to all the devices connected over a same Local Area Network (LAN). At present, the protocol IEEE 802.11g for WLANs is also providing a maximum data rate of 54Mbps, we can see in table 1.2. Such a high transmission rate makes broadcasting of visual signals through Wi-Fi possible. In this device VT, for the discovery of same type of applications and making links

between transmitter and receivers, Network Service Discovery (NSD) is used. It searches, all VT that are available over the one WLAN. NSD makes link of transmission by exchanging the keys, so that only those receiver can see visual signals from the transmitting source.

3.2.4 System Architecture

We have earlier illustrated the concept of the basic CCTV system, also the Wireless Video Transceiver concept and specifications. Moving forward, we need to depict a conceptual model that defines the structure, behavior, and more views of a system. Below Illustrates an architecture description that is a formal description and representation of the system. The experiment apparatus is the sample unit (Table 3.1) that is exposed to one or more experimental stimulus; Thus, a user would be able to view the cast data from the transmitting source.

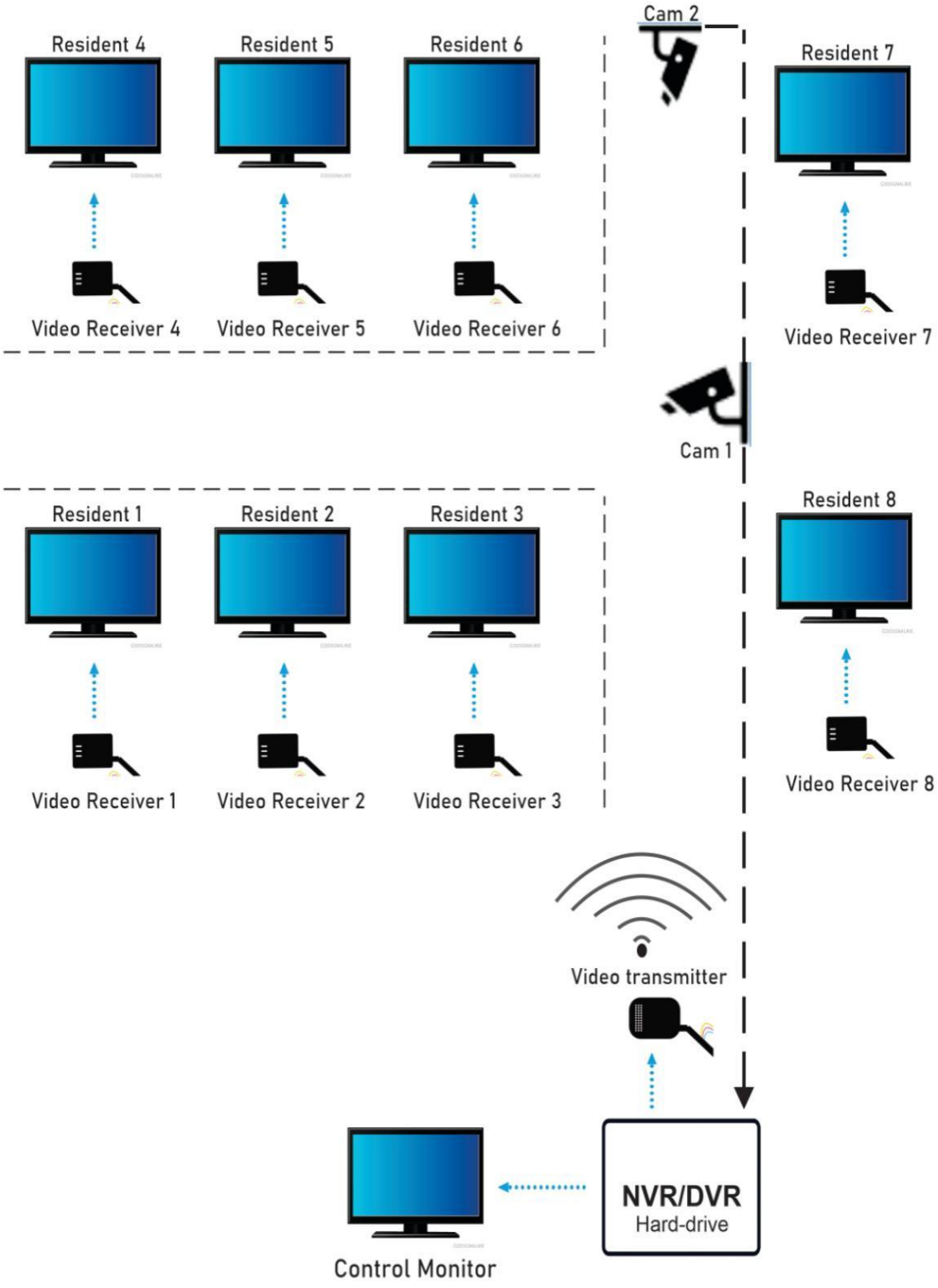


Figure 3.5: System Architecture

The above figure (3.4) depict the structure, behavior, and more views of a system.

Where: Cam 1 and Cam 2 are set to capture footage in the community and send it for storage and multicast to the DVR.

The Video Transmitter to be integrated with the DVR sending signal to the Receivers that is connected with several residents monitors.

In this phase of approach, the usability attribute evaluation will be adopted, by recent research in this study. People At Center of Mobile Application Development (PACMAD) originated a model[14], by integrating the usability attributes developed by[3], the International Organization for Standardization (ISO). This phase will review the PACMAD usability attributes, prior to developing the metric to measure usability of Surveillance System. Figure 3.4 below describes the most common usability evaluation attributes based[3], with the recent integration of usability attributes in PACMAD model obtained from literature.

Figure 3.6: PACMAD UE Framework

Source: [9]

3.3 Requirements Specification

In this section, we are going to be considering the requirement specifications, which lays out functional and non-functional requirements, and it may include a set of use cases that describe user interactions that the system must provide to the user for perfect interaction, as well as system development life cycle that explains the process for planning, creating, testing, and deploying an information system, the concept applies to a range of hardware and software configurations, as a system can be composed of hardware only, software only, or a combination of both. Furthermore, we are going to be considering requirements analysis of the system, which focuses on the tasks that determine the needs or conditions to meet the new or altered project, taking account of the possibly conflicting requirements of the various stakeholders, analyzing, documenting, validating and managing system requirements. Functional specification which are documents that specifies the functions that a system or component must perform will be included, and lastly the system model that presents a framework for implementation of specific activities[11].

3.3.1 System Development Life Cycle

The system development life cycle works like an assembly line, where each phase of the process needs to be completed before moving on to the next. This helps us produce high-quality systems that match expectations, meet deadlines and fulfill all requirements.

Surveillance systems can be complex SDLC helps us focus on one phase at a time and simplify the development process. We chose agile from the variety SDLC methodologies or models, to help develop systems throughout the life cycle phases.

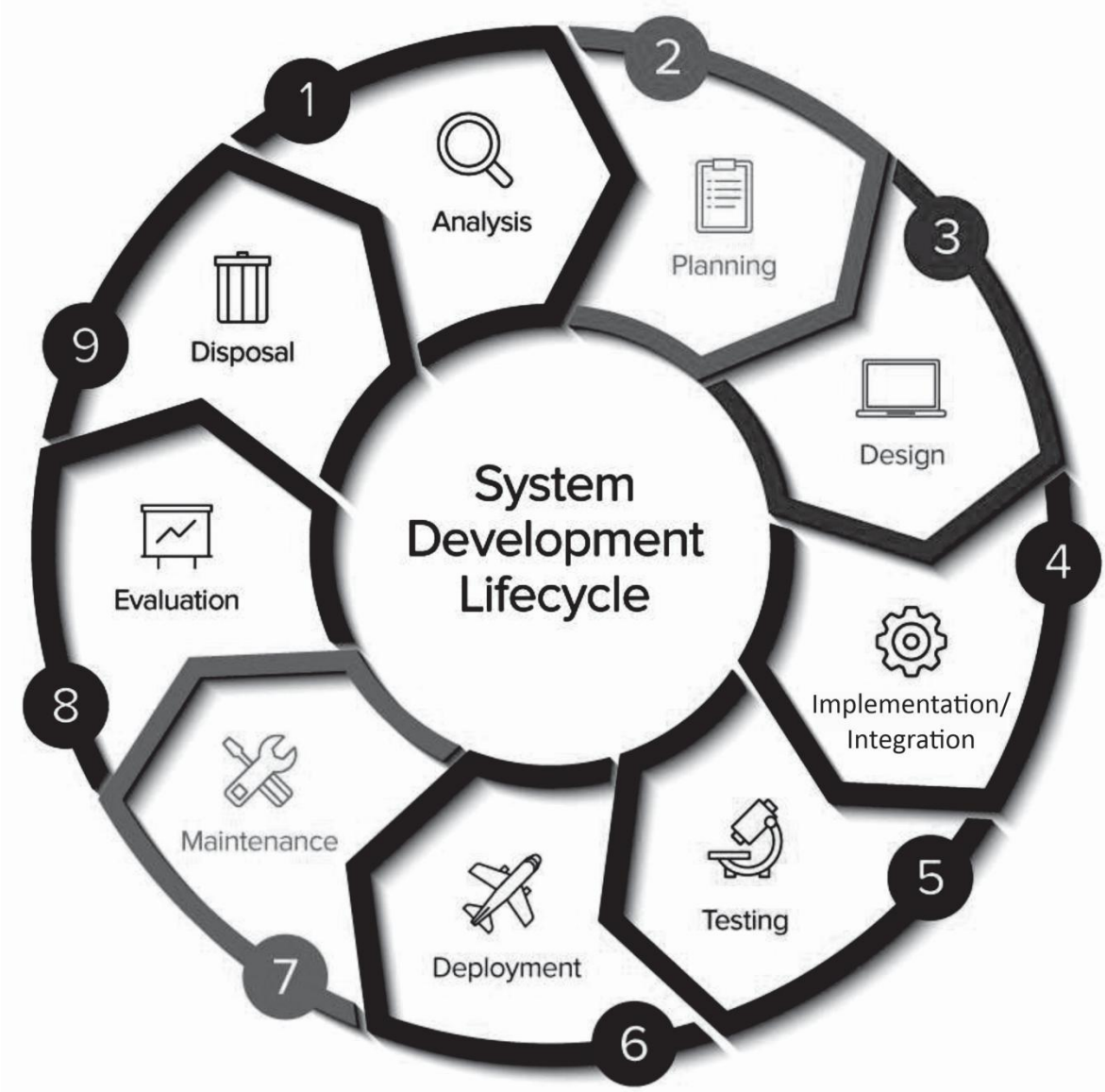


Figure 3.7: Agile SDLC model

Source: [8]

With the model shown at above figure (3.5), explains, we reach a milestone at the implementation and integration level (4) and the deliverable is at the deployment stage (6). We will do our evaluation by collecting feedback and act upon the feedback for disposal.

3.3.2 Implementation and Evaluation Model

Furthermore, we presents a framework for Quality implementation and evaluation of activities using Donabedian's Structure, it is one of the most effective methods of ensuring customer satisfaction. The QIE model consists of policy, provider competency, and performance and accountability, to guide this experimental initiative, which is one of the methods implemented in this study to achieve the expected result. The QIE model is shown in figure (3.7) below:

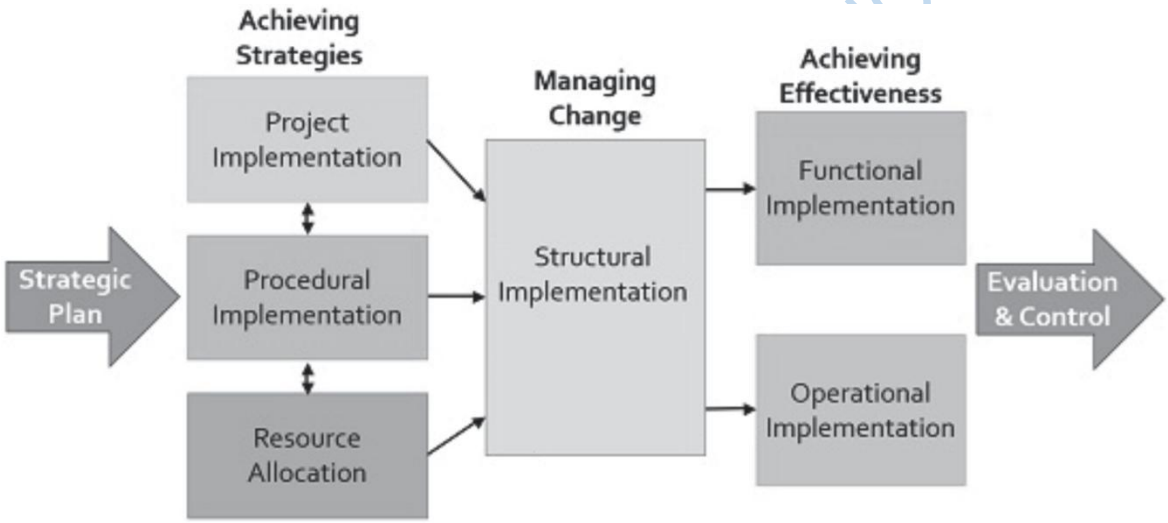


Figure 3.8: Quality Implementation and Evaluation model

Source: [7]

From our strategic plan to the evaluation & control.

First stage of achieving strategies consist of project implementation, procedural implementation and resource allocation. Managing change could be achieved through the structural implementation and achieving effectiveness goes with functional implementation and operational implementation.

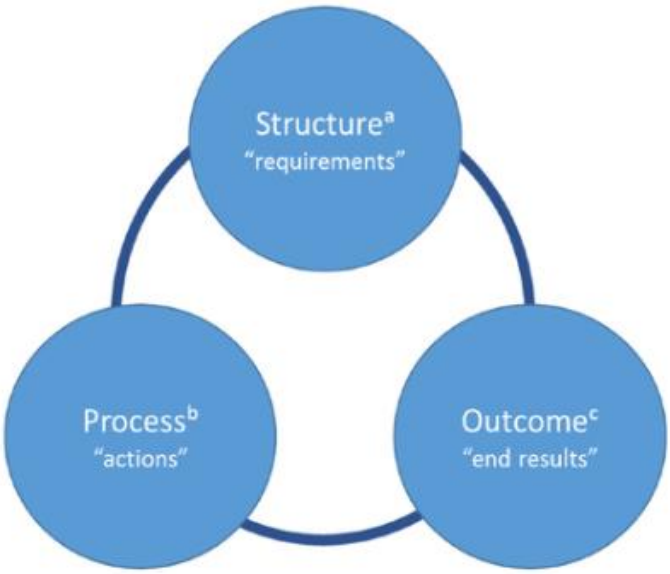


Figure 3.9: Donabedian Structure-Process-Outcome framework

Source: [9]

a. What the system needs to have to be user friendly and more effective

b. The actions in giving and receiving adequate security

c. End result as a consequence of providing adequate security

3.3.3 Use Case

However, there is need to define the roles users will be playing in the system, the use case. Use cases can be valuable tools for understanding the system's ability to meet the needs of end users. When designing the system, we enhance the development efforts by thinking through the system practical use operations, the assertion is that the system use must be as flexible as possible, for a lame man to operate. The diagram representation of this scenario is seen in Figure (3.9) below

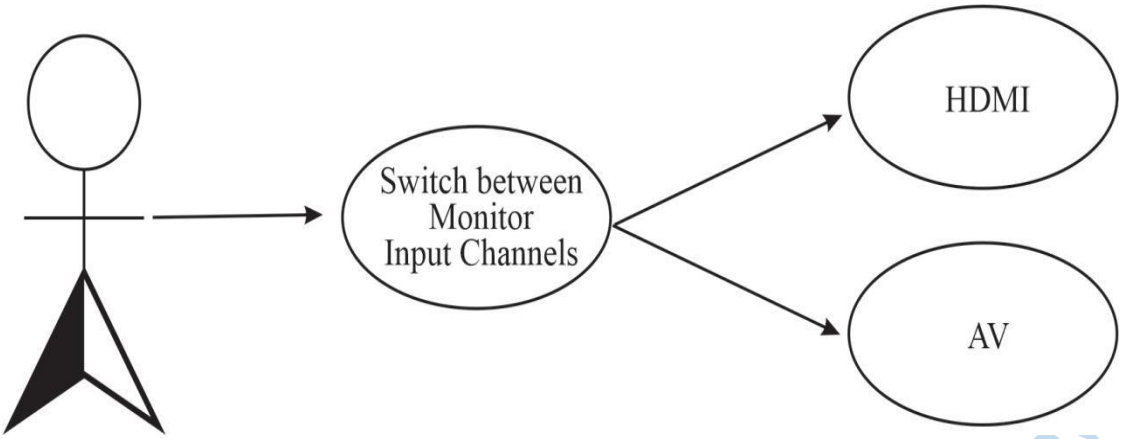


Figure 3.10: UML use case

Source: [9]

The use case of the system is flexible for a lame man. Put on the monitor, control switch between the monitor channels in which the wireless video transceiver is plugged, then you have the view.

3.4 Research Methods

It was earlier discussed in this chapter, several types and specification of CCTV surveillance devices like; Analogue, AHD and IP cameras, DVR, NVR, BNC Connectors, Coaxial Cable etc.

3.4.1 CCTV System Development

The number one objective of this study is to develop a CCTV system using an analogue camera and a digital video recorder, having a hard-drive, for data capturing and storage.

The method to achieve this objective is practically mounting cameras at the required angles to capture video signals, encode and send it as an analogue signal through an RG59 coaxial

cable to the DVR, which is then shown on a CCTV monitor and record it as a digital file for surveillance, security, and protection use.

There are 2 specifications of both analogue and cameras which are:

1. Indoor Camera
2. Outdoor Camera

Depending on the space at the which the camera needs to be fixed for surveillance purposes, indoor cameras will be used for indoor purpose as its called and the outdoor camera will be used for outdoor spaces.

Figure 3.11 Analogue Indoor Dome Camera

Source: [8]

Figure 3.12 Analogue Outdoor Bullet Camera

Source: [8]

The cameras shown in the above figures (Figure 3.10 and 3.11) are built according to the specification of their purpose, the indoor which is used indoor only and the outdoor bullet water proof for outdoor use, both cameras has infrared sensor in it which enables motion detection and night vision.

Moving on to the RG59 coaxial cable which is responsible for the communication between the camera and the DVR (the camera send video signals through RG59 coaxial cable in analogue signals to the DVR) with the help of BNC connectors. The coaxial cable is also attached with a power cable which powers the cameras.

Figure 3.13 RG59 Coaxial Cable

Source: [8]

As shown in Figure 3.10 above, the coaxial cable is made up of soft copper and hard cores on inside. It was also attached with a power cable, which is positive and negative black and red colour.

Figure 3.14 BNC Connectors

Source: [8]

BNC Connectors facilitates connections between the camera and DVR BNC ports for swift communications.

Moving forward, to the DVR which is a consumer electronics device designed for recording video in a digital format within a mass storage device such as hard disk drive or any other storage device.

Figure 3.15: Digital Video Recorder

Source: [8]

This is an 8 channels DVR, if we observe to the left, there are 8 ports which accommodates connectivity of 8 cameras. Followed by the BNC video out and audio out port. There is also VGA output port and HDMI output port. The next is the audio in port. Looking at the second to the last contains the POE port for network connectivity and USB ports and lastly, we have the power adapter.

3.4.2 Decentralization / Multicast

The objective 2 is to design a decentralization system using a wireless video transceiver. Xolbekova Mavluda et al. (2021) declared that every surveillance system must be designed to meet all privacy policy possible, whereas, Sakpere Wilson (2017) argued that an absolute privacy is difficult to achieve in a smart environment. To maintain a balance here, only the read-only data will be decentralized, read and write data remains centralized at the main workstation[1,15].

Moving on, the variations of OWC can be potentially employed in a diverse range of communication applications ranging from optical interconnects within integrated circuits through outdoor inter-building links to satellite communications.

Using Long range OWC enables inter-building connections, also free-space optical communications, as it known that the smallest wavelength, the greatest effect[16].

Table 3.3 IEEE 802.11 Frequency Range Analysis

Band	Frequency range	Wavelength range
Extremely Low Frequency (ELF)	<3 kHz	>100km
Very Low Frequency (VLF)	3 to 30 kHz	10 to 100km
Low Frequency (LF)	30 to 300 kHz	1m to 10km
Medium Frequency (MF)	300 kHz to 3 GHz	100m to 1km
High Frequency (HF)	3 to 30 GHz	10 to 100m
Very High Frequency (VHF)	30 to 300 GHz	1 to 10m

Source[18]

Wi-Fi is a family of wireless network protocols, based on the IEEE 802.11 family of standards, which are commonly used for local area networking of devices and Internet

access, allowing nearby digital devices to exchange data by radio waves. These are the most widely used computer networks in the world, used globally in home and small office networks to link desktop and laptop computers, tablet computers, smartphones, smart TVs[18,19].

Table 3.4 Wi-Fi Protocol Summary

Protocol	Frequency	Signal	Maximum Data Rate
Legacy 802.11	2.4 GHz	FHSS or DSSS	2 Mbps
802.11a	5 GHz	OFDM	54 Mbps
802.11b	2.4 GHz	HR-DSSS	11 Mbps
802.11g	2.4 GHz	OFDM	54 Mbps
802.11n	2.4 GHz or 5 GHz	OFDM	600 Mbps (theoretical)
802.11ac	5 GHz	256-QAM	1.3 Gbps

Source: [16]

Where:

FHSS = Frequency Hopping Spread

Spectrum, DSSS = Direct Sequence Spread Spectrum,

OFDM = Orthogonal Frequency Division Multiplexing,

HR = High-Rate, QAM = Quadrature Amplitude Modulation.

Source:[16]

Table (void) shows summary of IEEE 802.11 protocol, if we see there, the Legacy 802.11 is the first Wi-Fi protocol developed in the series of IEEE 802.11 having the maximum data rate 2Mbps. After that, the next versions developed with increasing maximum data rate of Wi-Fi[16,17].

A wireless video transmitter solves the problem of allowing to send an AV signal wirelessly across rooms or through walls.

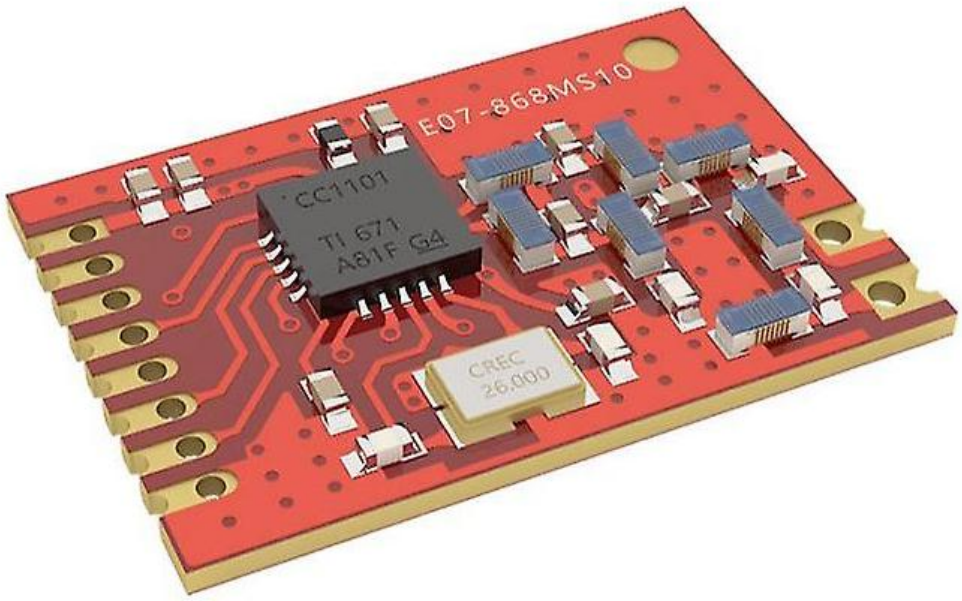


Figure 3:16 Wireless Transceiver Module Architecture

Source: [17]

Table 3.5 Wireless Video Transceiver Module Specification

Power Supply	DC12V-24V
Consumption Current	200mA
Tx Channel	1 to many
Output Power	200mW
Unobstructed Effective Range	150 ~ 200 m
Operating temperature	-10°c ~ +50°c

Source: [19]

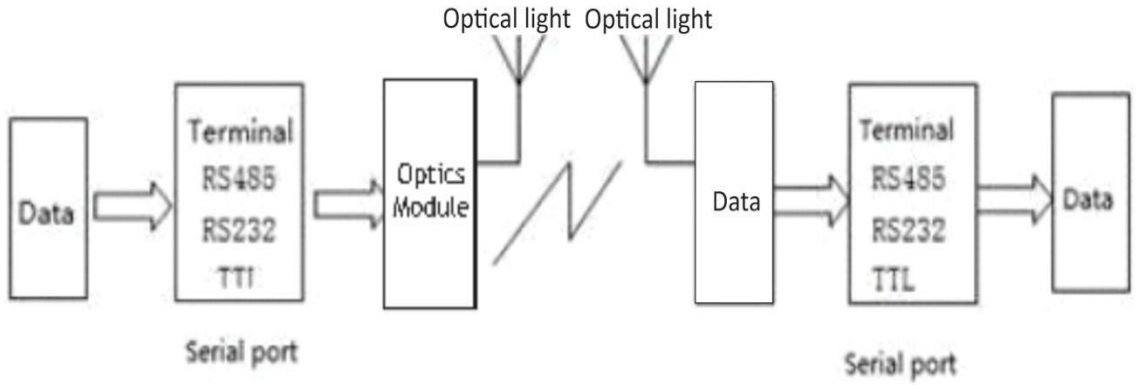


Figure 3:16 Wireless Video Transceiver Data Transmission Sequence

Source: [17]

The experiment apparatus as the sample unit Table (3.1) was exposed to one or more experimental stimuli. The control apparatus (the developed application), on the other hand, was the sample unit that was not exposed to any experimental stimulus and yet identical to the experiment apparatus[5,22]. In this study, the experimental stimulus refers to the manipulation of the application's code for the improvement of the navigation app. Any differences observed between the control apparatus and experiment apparatus, on one hand, and between the pre-test and post-test, on the other hand, are attributed to the effect of the experimental stimulus. The experiment is considered successful if the post-test outcome is more favourable than the pre-test[2,20]. The integration of the 2 system enables a Multicast Surveillance Technology System, which is shown in below figure 3.17

Figure 3.18: Research Display Result

Source: (Researcher's Fieldwork, 2023**)**

Endnotes

1. W. E. Sakpere, *A Near Field Communication Framework for Indoor Navigation: Design and Deployment Considerations.* Master's Thesis, Cape Peninsula University of Technology. 2015, http://digitalknowledge.cput.ac.za/xmlui/handle/11189/3628

2. W. Ajayi, Software Testing and quality assurance (CSC 714), Lead City University, 2022

3. W. Lillian, Y. Kiaw, L. Sook-Ling, L. Siong-Hoe & C. Leow. *Usability Factors Predicting Continuance of Intention to Use cloud e-learning Application,* **Heliyon,** 5, 2019, https://doi.org/10.1016/j.heliyon.2019.e01788.

4. D.R. Monette, T.J. Sullivan, C.R. Dejong, & T.P. Hilton, *"Applied Social Research: A Tool for the Human Services,*" 9th ed., 2014, ISBN 10: 128507551X ISBN 13: 9781285075518.

5. E, Babbie, *"The Practice of Social Research,"* 14th ed., 2014, ISBN: 978-1-305-10494-5, https://lms.su.edu.pk/download?filename=1606930922-earl-babbie-the-practice-of-social-research-cengage-learning-2014.pdf&lesson=47225

6. A. Stuart & K. Steven, "*The American Heritage Student Science Dictionary,*" Second Edition, 2014.

7. S.S. Dhillon, M.S. Vitiello, & E.H. Linfield, *The 2017 Terahertz Science and Technology Roadmap* In: **Journal of Physics D, Applied Physics**, Vol. 50, No. 4, 2017, 043001, 04.01, https://doi.org/10.1088/1361-6463/50/4/043001

8. P. Eric, W. Brandon, F. David & T. Amanda, *CCTV Surveillance for Crime Prevention, A 40 - Year Systematic Review with Meta - Analysis*. **Criminology & Public Policy**, 18, 135-159, 2019, https://doi.org/10.1111/1745-9133.12419.

9. United State Department of Homeland Security; *Prepared by Space and Naval Warfare Systems Center Atlantic.* CCTV Technology Handbook 2013

10. S. Muhammad, S. Simon, S. Marlindia & M. Lisa, *"2.4 GHz Wireless Data Acquisition System for FIToplankton ROV," 2018,* 189-193. https://doi.org/10.1109/ICoICT.2018.8528795.

11. Digital Evidence Section Forensic Scientist Manager, "*Technical Procedure for DVR Analysis*", Version 5, 2018 https://forensicresources.org/wp-content/uploads/2019/07/Video-DVR-Analysis-Procedure-06-13-2018.pdf

12. Wikipedia, Donabedian model, 2023, https://en.wikipedia.org/wiki/Donabedian_model

13. Cine Gears Incorporation, "*Ghost Eye Eireless HDMI/SDIVIDEO Transmission System User Manual", 2020*

14. R. Harrison, D. Flood & D. Duce, *"Usability of Mobile Applications: Literature Review and Rationale for a New usability model,"* **Journal of Interaction Science**. 2013 1. https://doi.org/10.1186/2194-0827-1-1.

15. U.M. Xolbekova and A.M. Tajibayev, *"Security, international peace and religious tolerance and foreign policy -as an important priority in the appeal."* Teachers department of "Social Sciences" of Jizzakh Polytechnic InstituteJizzakh, Uzbekistan. vol. 2, 2021, 175-194. https://doi.org/13.1219/ICoICT.2021.8768272

16. G. Véronique, P. Nicolas, B. Sébastien, & M. Véronique, *"Outdoor Optical Wireless Communication:"* potentials, standardization and challenges for Smart Cities, 2020 https://doi.org/10.1109/WOCC48579.2020.9114953.

17. M. Kashef, M. Abdallah, & N. Al-Dhahir, *"Transmit Power Optimization for a Hybrid PLC/VLC/RF Communication System,"* IEEE Transactions on Green Communications and Networking. pp.1-1, 2017, https://doi.org/10.1109/TGCN.2017.2774104..

18. A.M. Cailean, & M. Dimian, *"Impact of IEEE 802.15.7 Standard on Visible Light Communications Usage in Automotive Applications,"* IEEE Communications Magazine. PP. 2-7, 2017, https://doi.org/10.1109/MCOM.2017.1600206CM.

19. IEEE 802.15 WPAN™ Task Group 13 (TG13), *"Multi-Gigabit/s Optical Wireless Communications,"* 2020, [Online]. Available: http://www.ieee802.org/15/pub/TG13.html.

20. J. Nielsen, "Usability 101: *Introduction to usability",* 2012, available at: www.nngroup.com/articles/usability-101-introduction-to-usability.

21. R. Ismail, N. Fabil, & A. Saleh, *"Extension of PACMAD Model for Usability Evaluation Metrics Using Goal Question Metrics (Gqm) Approach*." Journal of Theoretical and Applied Information Technology. 2015, 79, https://www.researchgate.net/publication/325484529_Extension_of_pacmad_model_for_usability_evaluation_metrics_using_goal_question_metrics_Gqm_approach/citation/download.

Chapter Four

Implementation and Evaluation

4.1 Implementation

In this section, we present the results of our implementation in figures (graphs and diagrams), tables and written text. The figures and tables presents the complete results in numerical, visual or graphical terms, while the written text helps the reader to focus on the most important aspects of the results and to interpret them.

The result advance the concept of surveillance implementation outcomes, distinguished from surveillance service system outcomes. Implementation outcomes is known as the effects of deliberate and purposive actions to implement new practices, and services[1]. Implementation outcomes have three important functions, which are;

- First, serve as indicators of the implementation success.
- Second, they are proximal indicators of implementation processes.
- And third, they are key intermediate in relation to service system in effectiveness and quality of surveillance research.

Because crime intervention or surveillance system will not be effective if it is not implemented well, implementation outcomes serve as necessary preconditions for attaining subsequent desired changes in surveillance system or service outcomes.

Therefore, to present the implementation and evaluation proper, there are some pre-conditions that need to be met for an effective implementation and evaluation. They include ensuring all required implementation equipment and tools are available and properly placed, as well as ensuring a proper source of power for all the equipment and tools. Hence, the results are presented under the following four stages:

1. Background information, so that the reader can place our results in the context of other research.
2. Tables and/or figures presenting our results. These are located and identified through numbers (for example, 'Table 1') and captions.
3. Text accompanying and referring to the tables or figures, describing the aspects of the results we are focusing on.
4. Comments on the results. For example, generalisations arising from the results, explanations of possible reasons for the results or a comparison of the results with other studies.

4.1.1 Background Information

The first objective of this study is to develop a CCTV system using an analogue camera and a digital video recorder, having a hard-drive, for data capturing and storage. The method to achieve this objective is object detection, this practically involves mounting cameras at the required angles to capture video signals, encode and send it as an analogue signal through an RG59 coaxial cable to the DVR, which is then shown on a CCTV monitor and recorded as a digital file for surveillance, security, and protection use.

4.1.2 Integration of the Hard Disk

Moving forward, the DVR shown in Figure 4.1, which is a consumer electronics device designed for recording video in a digital format within a mass storage device such as hard disk drive or any other storage device.

Figure 4.1: Digital Video Recorder

Figure 4.1 is a 4-channel DVR. To the left, there are 4 ports that accommodate the connectivity of 4 cameras, followed by the BNC video-out and audio-out ports. There is also the VGA output ports and HDMI output port. The next is the audio-in port. Looking at the second to the last, it contains the POE port for network connectivity and USB port. Lastly, we have the power adapter port. The DVR would display "No Signal" and "HDDs are not found", if other devices are not yet integrated into it, as shown in Figure 4.2.

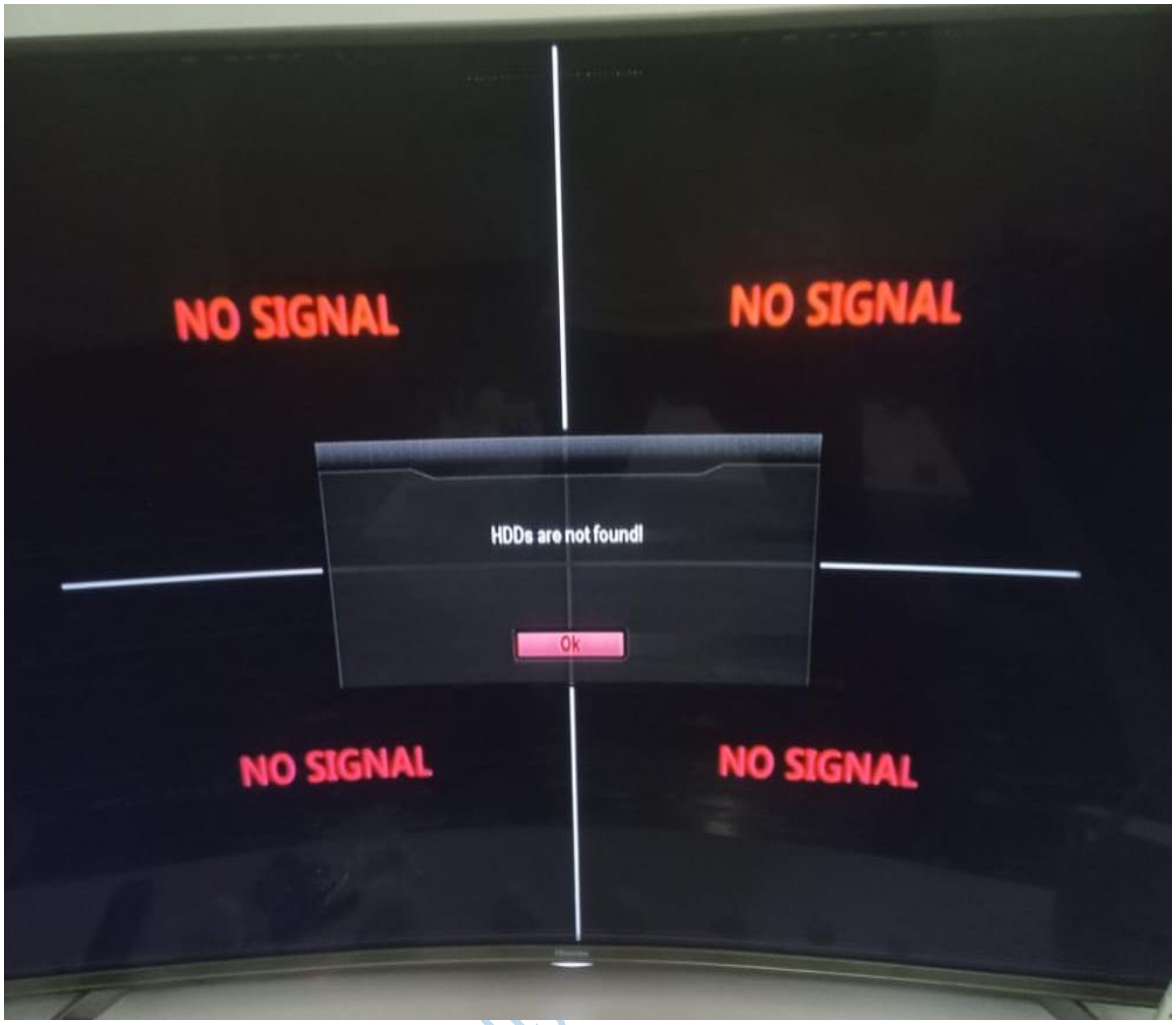


Figure 4.2: Display Result for the DVR without Hard-drive

Figure 4.3 shown, is the internal hardware of the DVR consisting of the motherboard and having Serial Peripheral Interface that could accommodate other peripheral devices needed.

Figure 4.3: Internal Hardware of DVR

This hard drive, shown in figure 4.4, is a 500GB HDD to be integrated with the DVR as the main storage device. The uses magnetism to store and retrieve digital information. The device consists of a stack of rotating magnetic disks, or platters, that are coated with a magnetic material and read/write heads that move across the platters to read and write data. Each platter has a magnetic surface that is divided into concentric circles called tracks, and each track is further divided into sectors. The read/write heads move across the platters in order to read and write data by creating and detecting changes in the magnetic field of the platters.

The internal hardware is shown in Figure 4.3 was integrated with the HDD shown in Figure 4.4. The after integration is shown in in Figure 4.5.

Figure 4.4: Hard Drive

Furthermore, by integrating a storage device, depending on the intended storage size. The hard drive can be integrated with the DVR, and the result of the integration is shown in Figure 4.5

Figure 4.5: Internal Hardware after the Hard drive integration

The hard disk, is a magnetic storage medium for a computer. Hard disks are flat circular plates made of aluminum or glass, and coated with a magnetic material. Hard disks for personal computers can store terabytes (trillions of bytes) of information. Data are stored on their surfaces in concentric tracks. A small electromagnet, called a magnetic head, writes a binary digit (1 or 0) by magnetizing tiny spots on the spinning disk in different directions and reads digits by detecting the magnetization direction of the spots. A computer's hard drive is a device consisting of several hard disks, read/write heads, a drive motor to spin the disks, and a small amount of circuitry, all sealed in a metal case to protect the disks from dust. In addition to referring to the disks themselves, the term hard disk is also used to refer to the whole of a computer's internal data storage. Beginning in the early

21st century, some personal computers and laptops were produced that used solid-state drives (SSDs) that relied on flash memory chips instead of hard disks to store information[2].

Figure 4.6: Display Result after HDD's integration

4.1.3 Integration of the CCTV Camera

Now, our DVR is good to accept communications from the camera, we proceed to the integration of the CCTV camera. This step will conclude the first objective. The two specifications of CCTV cameras, which are analogue and network, share common classifications that include:

- Indoor Camera
- Outdoor Camera

Depending on the space the camera needs to be fixed for surveillance purposes, indoor cameras will be used for indoor purpose and the outdoor camera will be used for outdoor spaces.

Figure 4.7: Analogue Indoor Dome Camera

The camera shown in Figure 4.7 is built according to the specification of its purpose. The indoor camera, which is used indoor only, has infrared sensor in it that enables motion detection and night vision.

The RG59 coaxial cable is responsible for the communication between the camera and the DVR (the camera send video signals through RG59 coaxial cable in analogue signals to the DVR) with the help of BNC connectors, BNC Connectors facilitate connections between the camera and DVR BNC ports for swift communications. The coaxial cable is also attached with a power cable which powers the cameras. The coaxial cable is made up of soft copper and hard cores on the inside. It was also attached with a power cable, which is positive (red) and negative (black). The result after integration of the CCTV camera with the DVR is shown in Figure 4.8. This concludes the first objective.

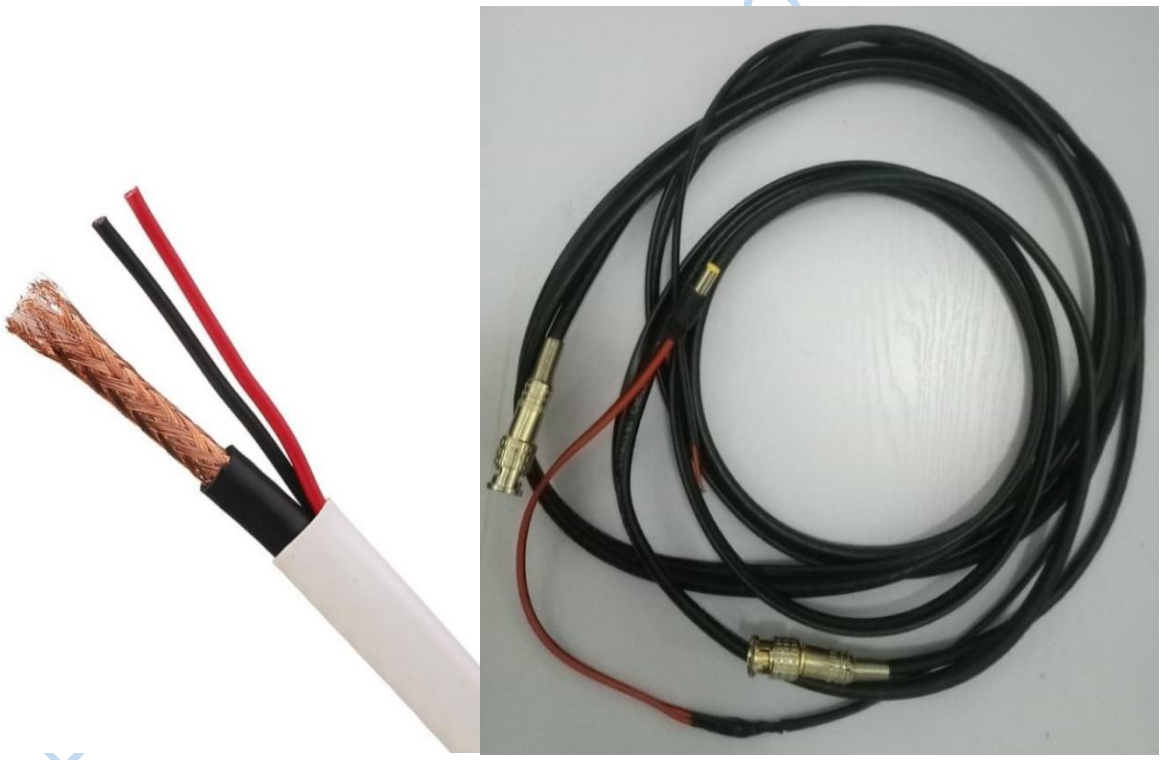


Figure 4.8: RG59 with BNC Connector Coaxial Cable

Figure 4.9: Display result of first objective

After the implementation of the first objective, using the applicable methods, we have our result in figure 4.9. Camera 1 is shown with its time stamp, which is recorded into the storage device integrated with the DVR.

4.1.4 Design of a Decentralisation System

The second objective is to design a decentralization system using a wireless video transceiver. Researchers declared that every surveillance system must be designed to meet all privacy policy possible. Whereas, some, argued that an absolute privacy is difficult to achieve in a smart environment[1,2]. To maintain a balance here, only the read-only data will be decentralized. The read and write data remains centralized at the main workstation.

Moving on, the variations of OWC can be potentially employed in a diverse range of communication applications ranging from the optical interconnects within integrated circuits through outdoor inter-building links to satellite communications.

Using Long range Optical Wireless Communication enables inter-building connections and free-space optical communications, as it is known that the smallest wavelength has greatest effect[3].

Table 4.1 Frequency Range Analysis

Band	Frequency range	Wavelength range
Extremely Low Frequency (ELF)	<3 kHz	>100km
Very Low Frequency (VLF)	3 to 30 kHz	10 to 100km
Low Frequency (LF)	30 to 300 kHz	1m to 10km
Medium Frequency (MF)	300 kHz to 3 GHz	100m to 1km
High Frequency (HF)	3 to 30 GHz	10 to 100m
Very High Frequency (VHF)	30 to 300 GHz	1 to 10m

Source: [1]

Wi-Fi is a family of wireless network protocols, based on the IEEE 802.11 family of standards, which are commonly used for local area networking of devices and Internet access, allowing nearby digital devices to exchange data by radio waves[7]. These are the most widely used computer networks in the world, used globally in home and small office networks to link desktop and laptop computers, tablet computers, smartphones, smart TVs[8].

Where: FHSS = Frequency Hopping Spread Spectrum,

DSSS = Direct Sequence Spread Spectrum,

OFDM = Orthogonal Frequency Division Multiplexing,

HR = High-Rate,

QAM = Quadrature Amplitude Modulation.

Table 4.2: Wi-Fi Protocol Summary

Protocol	Frequency	Signal	Maximum Data Rate
Legacy 802.11	2.4 GHz	FHSS or DSSS	2 Mbps
802.11a	5 GHz	OFDM	54 Mbps
802.11b	2.4 GHz	HR-DSSS	11 Mbps
802.11g	2.4 GHz	OFDM	54 Mbps
802.11n	2.4 or 5 GHz	OFDM	600 Mbps (theoretical)
802.11ac	5 GHz	256-QAM	1.3 Gbps

Source: [2]

Table 4.2 shows the summary of IEEE 802.11 protocol, if we see there. The Legacy 802.11 is the first Wi-Fi protocol developed in the series of IEEE 802.11 having the maximum data rate 2Mbps[4,5]. After that, the next versions were developed with increasing maximum data rate of Wi-Fi.

The IEEE 802.11 protocol is used in the wireless video transmitter implementation in this study, The invention of wireless video transmitter solves the problem of sending AV signal wirelessly across rooms or through walls.

Figure 4.10 Wireless Video Transmitter Module

Figure 4.10 is a wireless video transmitter with Serial Peripheral Interface. The wireless video transmitter uses Wi-Fi protocol to communicate wirelessly by sending digital signal to with the receiver. The receiver is shown in the figure 4.11.

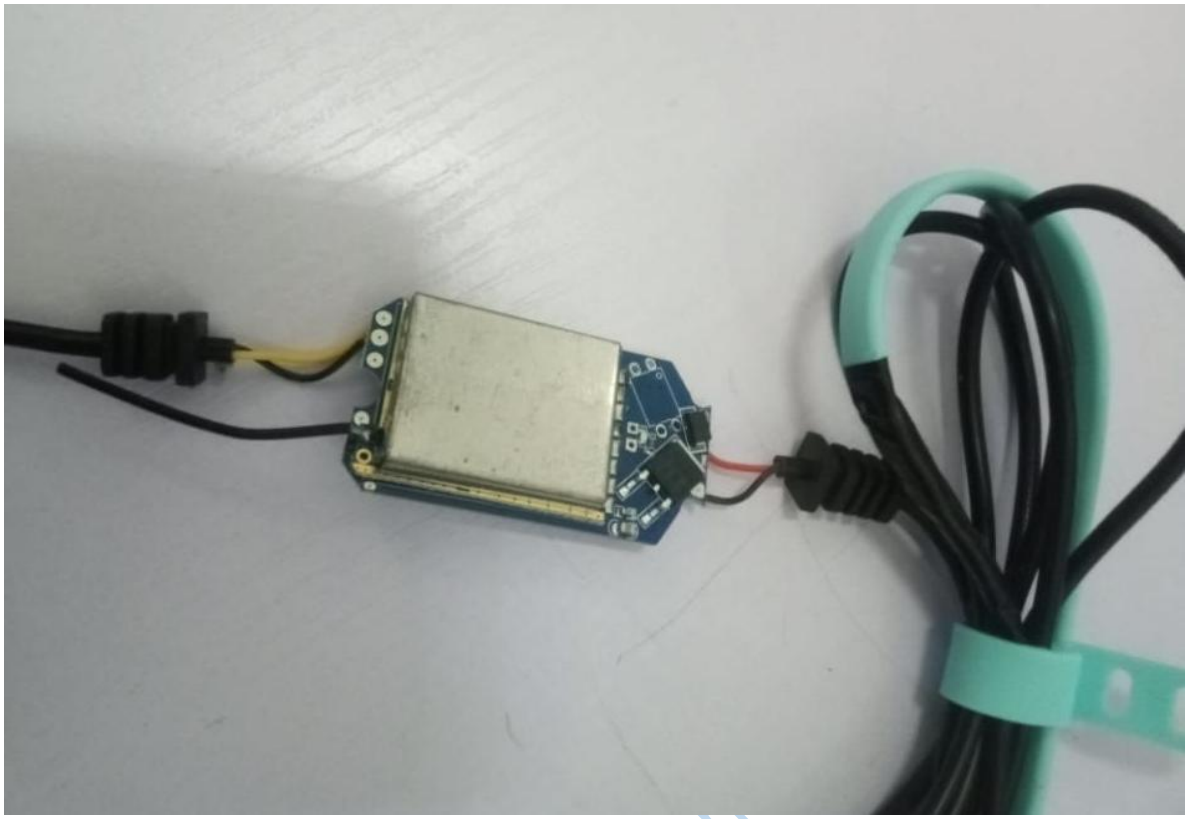


Figure 4.11 Wireless Video Receiver Module.

The wireless video receiver module requires a source of power which was initially taken from the TV USB port, but there were lots of interference due to insufficient power voltage supply. Hence, An alternative power supply was considered, which is the 12V power supply box. The power box has a regulator to sufficiently supply the required power for the devices, unless there is a device that requires a voltage lower than 12V. The result is shown in Figure 4.12.

Figure 4.12 USB Power source display result

The discussed devices eliminate the use of internet data to communicate with the help of Wi-Fi protocols. Our research deepens on the use of Wi-Fi protocols for network communications, without the need for internet data. The wireless video transmitter device specification is stated in Table 4.3.

Table 4.3 Wireless Video Transceiver Module Specification (IEEE 802.15 WPAN™ Task Group 13 (TG13)

TITLE	DESCRIPTION
Power Supply	DC12V-24V
Consumption Current	200mA
Tx Channel	1 to many
Output Power	200mW
Unobstructed Effective Range	150 ~ 200 m
Operating temperature	-10°c ~ +50°c

The wireless video transmitter requires a Direct Current of 12V to 24V, which mean the DVR power IC does not have enough capacity to power the transmitter, so we created an alternative power source for the device, with the use of case power supply box, which was later integrated with the DVR. The Power Supply Box is shown in figure 4.13

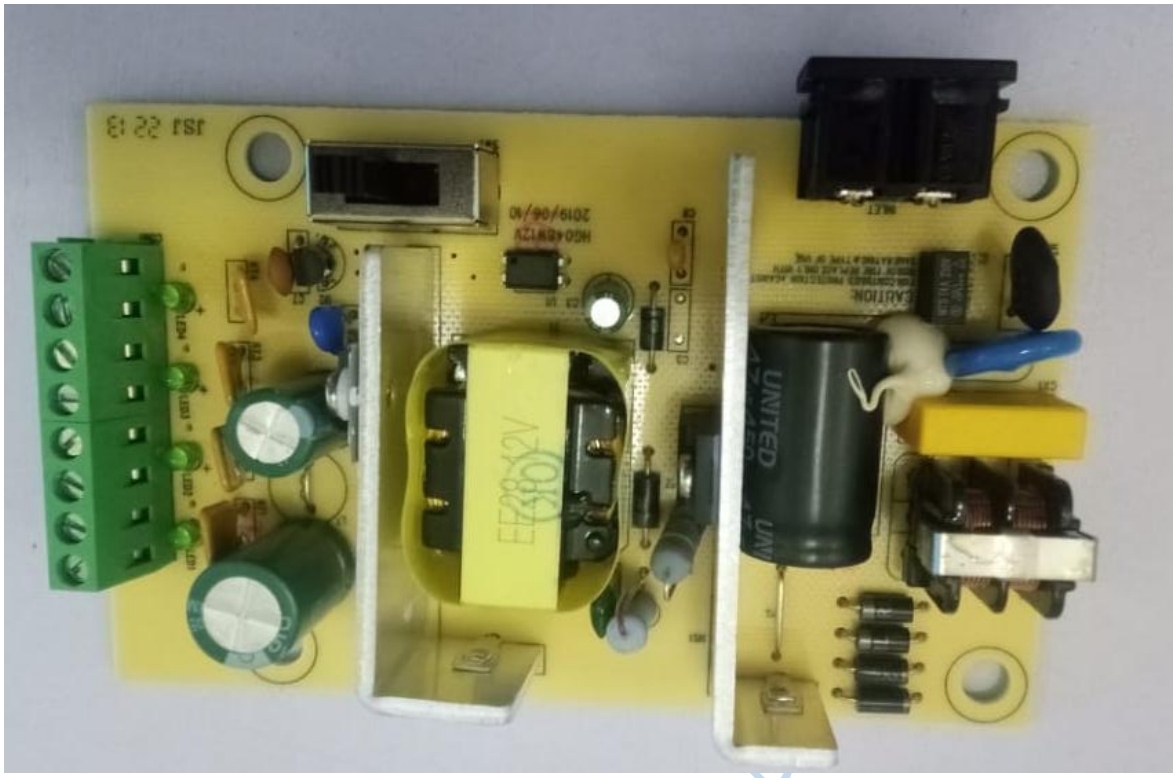


Figure 4.13: 12V Power Supply Box

The power supply box receives an Alternating Current (AC), passing through the converter which converts the current to a Direct Current (DC), with the help of stepdown transformer, then we have a DC output port.

Moreover, with all our implementations and integrations, the first three, have been accomplished. The final internal hardware integration and display results are shown in the figures that follow. The internal hardware integration diagram for power supply is shown in figure 4.14

Figure 4.14: Alternative Power Supply Integration

Figure 4.15 show the final hardware integration result while figure 4.16 shows the final Display result.

Figure 4.15: Final Internal Hardware integration Diagram

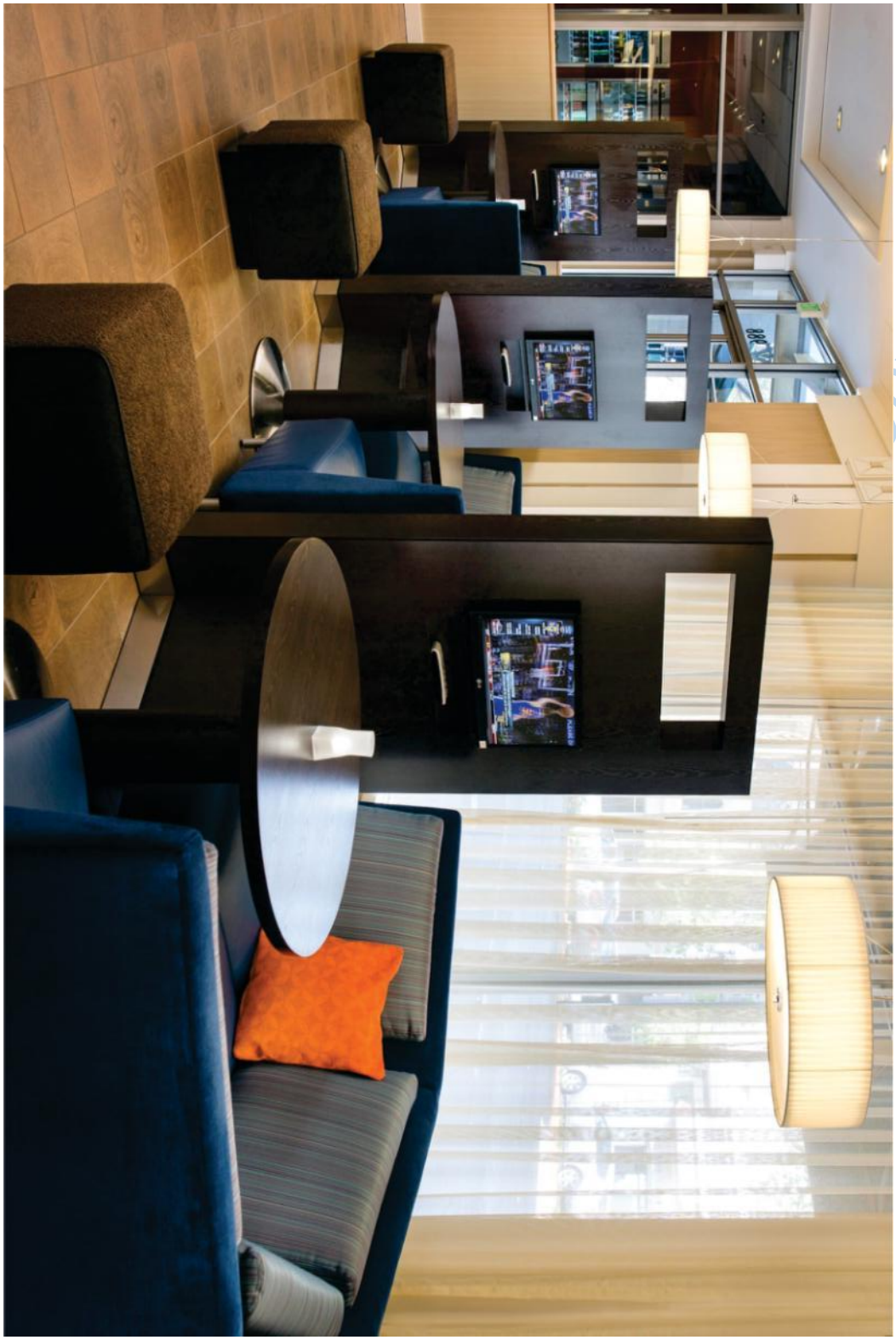


Figure 4.16: Final Display of the implementation Research Result

4.2 Evaluation

Due to the significance of the results, there is a need to analyse and interpret the research results. The significance of the results are explained and emphasized to relate the output to the research statement of the problem.

In known smart environment surveillance technologies, a real-time multicast viewing and system monitoring is faced with numerous challenges[7,8]. For example, the monitoring unit is usually centralized at a defined station, which limits extensive and close monitoring of the system. If there is consideration for an alternative monitoring unit, an IoT based remote streaming app is usually used, which sometimes experiences delay / interruption in transmission, due to error from the framework or internet connections. This method also consumes a lot of internet data/due to enormous data transmission, and it allows limited number of users[9].

Furthermore, there has been an increase in insecurity and injustice across the nation. Regrettably, even in the smart environment, due to insignificant and improper security protocols[1,10]. However, the implementation of an advanced surveillance system, which will enable residents in a community to join forces with one another and contribute their own quota in securing their environment, lives and properties, through a surveillance system monitoring without the use of internet data, is an area that has not been fully explored.

Therefore, we utilized resources, equipment, literatures, and academic knowledge to develop a surveillance system multicast for crime prevention and detection, within an enclosed geographical location.

We developed a CCTV system using an analogue camera and a digital video recorder, the system has a hard-drive, for data storage, in an approach to design a decentralization

system using a wireless video transceiver, then we Integrated the whole objective and we have a CCTV surveillance wireless multicast system, without the use of internet data.

4.2.1 System Evaluation

The system to be evaluated is the CCTV surveillance multicast which consist of cameras, DVR and wireless video transceiver aimed for crime prevention and detection, in public areas, such as parks, streets, and public buildings. Here are some evaluation key factors to put into considerations:

- Camera quality
- DVR functionality
- Wireless video transceiver performance

4.2.1.1 Camera Quality

The quality of the cameras used in the system is critical to the effectiveness of the surveillance system. High-resolution cameras (the higher the resolution, the clearer the image will be, but 1080p or higher is generally recommended for most applications) with good low-light sensitivity and wide-angle lenses used are important features to consider.

4.2.1.2 DVR Functionality

The DVR have adequate storage capacity to store the video footage captured by the cameras. The compression format used by the camera can affect the image quality and the amount of storage space required. H.264 or H.265 compression formats are options of use, which offer good image quality while minimizing storage requirements. It also has the ability to record continuously or on motion detection, and to allow remote access to the recorded footage. The DVR have recording compatibility of MJPEG, MPEG-4, H.264 and

H.265. The DVR must be compatible with the cameras being used. This includes support for the video format used by the cameras, as well as the number of channels and resolution supported

4.2.1.3 Wireless Video Transceiver Performance

The wireless video transceiver has sufficient frequency range and bandwidth to transmit video signal at 25Mbps from the DVR to multiple user monitors simultaneously, allowing for real-time monitoring, without significant signal loss or interference. The video transceiver has a good balance of range, signal quality, and latency, which minimizing interference and power consumption. Additionally, it has built-in security features that protects unauthorized access to the video signal.

The signal strength evaluation:

dB = 10lg(A/B)

if power value A is 100 mW and power value B is 10 mW, 10lg(100/10) equals to 10 dB, indicating that power value A is 10 dB greater than power value B. If power value A changes to 10000 mW, the calculation result changes to the following: 10lg(10000/10) = 30 dB.

System setup analysis:

- Camera Setup: Install cameras in the designated areas where surveillance is required.
- Camera Feed: The cameras capture live video footage of the monitored areas and send it to the recording device.
- Recording: The recording device saves the video footage in real-time or periodically based on the set interval.

- Storage: The recorded footage is saved on a storage device for later retrieval.
- Monitoring: The live footage and recorded footage can be monitored by the security personnel through a monitor or remotely using a network connection.
- Multicast: The live footage is casted into multiple users monitor for human supervision
- Alerts: The system can be configured to send alerts to the security personnel in case of any suspicious activities.
- Analysis: The recorded footage can be analyzed to detect any unusual or suspicious activities, and necessary action can be taken accordingly.
- Retrieval: The recorded footage can be retrieved for review or investigation purposes if required.
- Maintenance: Regular maintenance and updates of the system should be carried out to ensure the proper functioning of the CCTV surveillance system.

4.2.2 Performance Evaluation

The method used for performance evaluation is showed in figure 4.14 with reference to VCA. The GT and AR files are organized in cell arrays whose row number indicates the object while the columns contain: the list of frames in which the object is present (vectors long as the number of frames of the track) and bounding-box coordinates (top-left and bottom-right). The other inputs are the thresholds used for spatial and temporal overlap, which are set to 15%. Starting from this information, the performance of the CCTV Surveillance Multicast system has been compared with an open-source tool called i-SPY. The videos selected to evaluate system performance are taken from a camera installed on a real location. The alarms was tested also in the scene, events of interest have been simulated, together with light changes, shadows and object intersections[11].

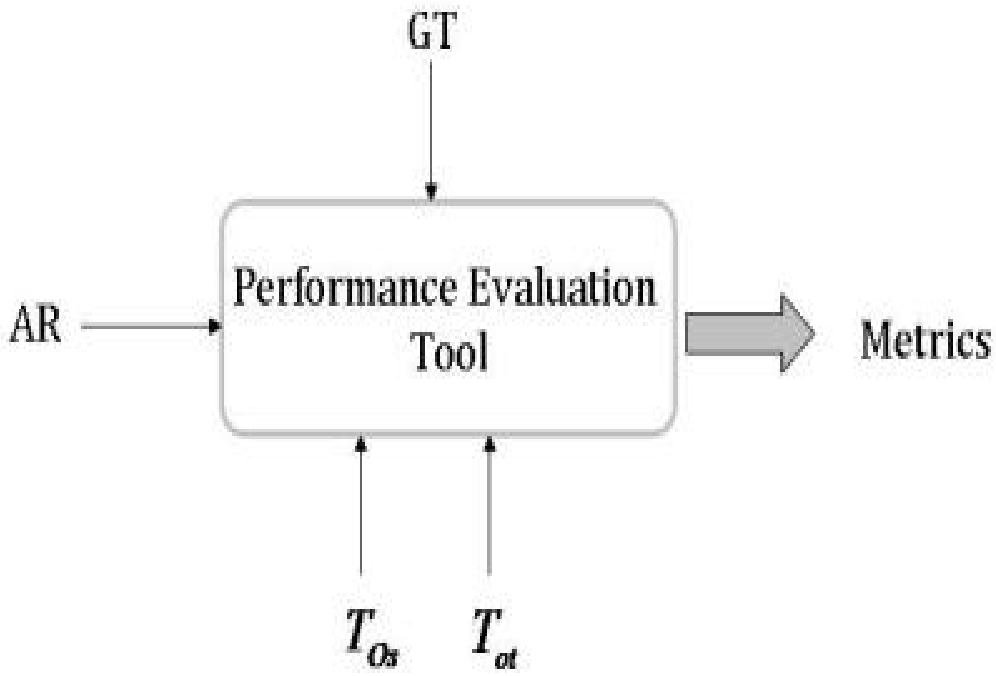


Figure 4.17 Tool for performance evaluation

In both VCA systems, the same Min and Max threshold have been configured for the objects to detect. Furthermore, the same background elaboration area (Figure 4.14) has been set, excluding the zones which could be potentially prone to problems (e.g. windows, doors, etc.). The video stream has been analysed for a time of 1 minute at a frame rate of 10 fps.

For the object-based analysis, the following metrics have been considered.

True Positive (TP): Number of frames where both GT and AR agree on the presence of one or more objects, and the bounding boxes of one or more objects coincide.

False Negative (FN): Number of frames where GT contains at least one object, while AR either does not contain any object or none of the AR objects fall within the bounding box of any GT object.

False Positive (FP): Number of frames where AR contain at least one object, while GT either does not contain any object or none of the GT objects fall within the bounding box of any system object.

False Alarm Track (FAT). We consider a system track as a false alarm if the system track meets any of the following conditions:

– A system track j does not have temporal overlap larger than with any GT track i.

– A system track j does not have sufficient spatial overlap with any GT track although it has enough temporal overlap with GT track i.

Track Fragmentation (TF): Fragmentation indicates the lack of continuity of system track for a single GT track. We allow multiple associations between GT tracks and AR tracks, therefore fragmentation is measured from the track correspondence results[11,12].

Table 4.1: Performance Indices

Performance Index	Description
$FAR = \frac{FP}{TP+FP}$	Percent of false alarms
$PP = \frac{TP}{TP+FP}$	Percent of true positive
$FNR = \frac{FN}{FN+TP}$	Rate of false negative
$FI = \frac{TP}{FRAGM}$	Ratio of TP and objects detected by the system.
$FM = \frac{OBJ_{AR}-FP}{MERGE}$	Evaluates the merging of blobs in the system

Figure 4.18: Background Area Selection

4.2.2.1 Motion Detection Evaluation

Bearing the limitations of motion detection in surveillance systems in mind, our objective is to find error metrics which evaluate the segmentation quality, the amount of spa tial errors as function of the foreground-background contrast and to assess the effects of morphological processing on the detection results. For motion detection ground truth is generated using real image sequences with superimposed computer-generated humans. The foreground-background contrast is varied by generating individual video sequences where each sequence has a distinct foreground gray level intensity (16 variations in total). The background was recorded using a hikvison outdoor bullet camera. Each video sequence consists of 1340 frames, 24-bit RGB images with a pixel resolution of 640x480 (Figure 4.15). The generation procedure was performed using Discreet 3DSMax 3.0 with the Character Studio plugin.

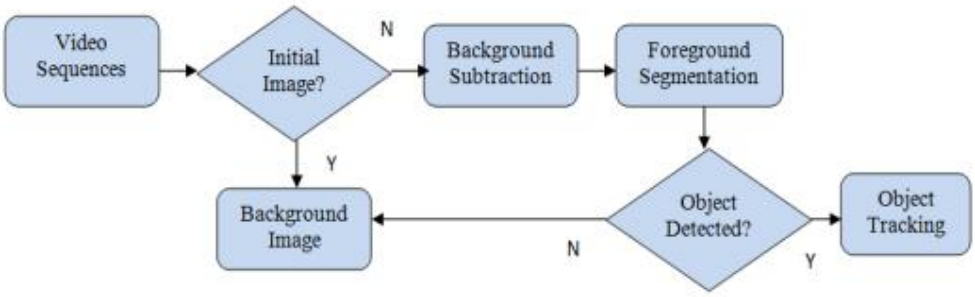


Figure 4.19: General Flowchart for Moving Object Detection

4.2.3 Population under Surveillance

The population under surveillance would depend on the specific location and purpose of the CCTV system. It could include all individuals who enter the monitored public areas.

4.2.3.1 Public Privacy Importance

As discussed earlier that every surveillance system must be designed to meet all privacy policy possible, and there was an argument that an absolute privacy is difficult to achieve in a smart environment. We have maintained a balance by decentralizing read only data, the read and write data access remains centralized at the main workstation.

4.2.4 Period of Data Collection

The period of data collection depends on the specific objectives of the system. For example, data collection for monitoring compliance with social distancing guidelines might begin at the start of an infectious disease outbreak and continue until the outbreak is contained.

Information collected:

The information collected by the CCTV surveillance system would include visual data captured by the cameras, as well as any additional data such as time and location stamps.

Provider of CCTV surveillance information:

The provider of CCTV surveillance information would typically be the organization or entity responsible for operating the system.

Transfer of information:

The information captured by the CCTV system would typically be transferred electronically, either in real-time or as recorded footage.

Storage of information:

The information captured by the CCTV system would be stored electronically, typically on a server or cloud-based platform.

Data analysis:

Data analysis would be conducted by trained personnel, either manually or using automated software.

Frequency of reports:

The frequency of reports would depend on the specific objectives of the system and the frequency of data collection. Reports might be disseminated daily, weekly, or on an as-needed basis.

Distribution of reports:

Reports would typically be distributed to stakeholders such as public health officials, law enforcement, or other relevant organizations.

Usefulness:

The usefulness of the CCTV surveillance system would depend on the specific objectives of the system and the accuracy and completeness of the data collected. If the data is reliable and used effectively, the system could be useful for detecting and preventing criminal activity or monitoring compliance with public health guidelines. The entities that could use the data to make decisions and take actions could include public health officials, law enforcement, and other relevant organizations. CCTV surveillance multicast is a useful tool for enhancing security in public spaces. However, it should be used with caution and with consideration for privacy concerns. The effectiveness of the system also depends on the quality of the hardware, software, and human resources used to operate and monitor it.

Simplicity:

The simplicity of this system depend on the specific components and operation of the system, but it is designed to be user-friendly and easy to operate.

Flexibility:

Thus systems is flexible, allowing for customization and adaptation to different geographical location surveillance needs . However, the flexibility may be limited to the specific hardware and software used and the specific objectives of the system

Acceptability:

The use of CCTV surveillance multicast is generally accepted, particularly in public areas where security is a concern. However, it may not be accepted in private spaces due to privacy concerns.

Sensitivity:

CCTV surveillance multicast has the potential to capture sensitive information and infringe on individual privacy. Therefore, sensitivity should be taken into consideration when installing and using the system.

Predictive value positive:

CCTV surveillance multicast can have a high predictive value positive, meaning that it can effectively identify potential threats and criminal activity. However, this depends on the quality of the cameras, the expertise of the operators, and the availability of analytics tools.

Representativeness:

CCTV surveillance multicast can provide a representative view of the monitored area, but this depends on the number and placement of cameras. Blind spots and inadequate camera placement can limit the representativeness of the system.

Timeliness:

CCTV surveillance multicast can provide real-time monitoring and quick response to potential threats. However, delays in transmission or response time may occur due to technical limitations or human error.

Endnotes

1. U.M. Xolbekova and A.M. Tajibayev, *"Security, International Peace and Religious Tolerance and Foreign Policy -as an Important Priority in the Appeal."* Teachers Department of "Social Sciences" of Jizzakh Polytechnic InstituteJizzakh, Uzbekistan. vol. 2, 2021, 175-194. https://doi.org/13.1219/ICoICT.2021.8768272

2. W. E. Sakpere, *"A near Field Communication Framework for Indoor Navigation: Design and Deployment Considerations."* Master's Thesis, Cape Peninsula University of Technology. 2015, http://digitalknowledge.cput.ac.za/xmlui/handle/11189/3628

3. D.R. Monette, T.J. Sullivan, C.R. Dejong, & T.P. Hilton, *"Applied Social Research: A Tool for the Human Services,"* 9th ed., 2014, ISBN 10: 128507551X ISBN 13: 9781285075518.

4. A.M. Cailean, & M. Dimian, *"Impact of IEEE 802.15.7 Standard on Visible Light Communications Usage in Automotive Applications,"* IEEE Communications Magazine. PP. 2-7, 2017, https://doi.org/10.1109/MCOM.2017.1600206CM.

5. IEEE 802.15 WPAN™ Task Group 13 (TG13), *"Multi-Gigabit/s Optical Wireless Communications,"* 2020, [Online]. Available: http://www.ieee802.org/15/pub/TG13.html.

6. Cine Gears Incorporation, *"Ghost Eye Wireless hdmi/sdivideo Transmission System user manual",* 2020.

7. G. Véronique, P. Nicolas, B. Sébastien, & M. Véronique, *"Outdoor Optical Wireless Communication:"* potentials, standardization and challenges for Smart Cities, 2020 https://doi.org/10.1109/WOCC48579.2020.9114953.

8. K. Prince Waqas, B. Yungcheol & P. Namje, *"A Data Verification System for CCTV Surveillance Cameras Using Blockchain Technology in Smart Cities,"* Electronics, 2020, 9-484. https://doi.org/10.3390/electronics9030484.

9. S. Sukhavasi, S. Elleithy, K. Abuzneid, A. Elleithy & Abdelrahman, *"Human Body-Related Disease Diagnosis Systems Using CMOS Image Sensors:"* A Systematic Review. Sensors, 21, 2021, 2098, https://doi.org/10.3390/s21062098.

10. N. Chikodiri, & O. Olihe, "*National Security and Sustainable Economic Development in Nigeria since 1999:"* Implication for the Vision 20 2020, 2014, 4. 129-142. https://doi.org/10.5901/jesr.2014.v4n5p129.

11. H. Glasl, D. Schreiber, N. Viertl, S. Veigl, & F.D. Gustavo, "*Video based Traffic Congestion Prediction on an Embedded System,"* 2008, 950 - 955. https://doi.org/10.1109/ITSC.2008.4732555.

12. X. Wu, Y. Ou, H. Qian, & Xu, Yangsheng, "*A Detection System for Human Abnormal Behavior,*" 2005, 1204 - 1208, https://doi.org/10.1109/IROS.2005.1545205.

Chapter Five

Conclusion

5.1 Summary of Results

We need to presents the key information about the most important outcomes of this study, including the best effect. Security is crucial to peaceful living, (both the preventive and detective measures), this cannot be over emphasized. As said by researchers, that every surveillance system must be designed to meet all privacy policy as possible, whereas, others argued that an absolute privacy is difficult to achieve in a smart environment. We have maintained a balance, by decentralizing, the read-only data using Wi-Fi protocols,

which is free from internet data usage, and is also cheaper to implement. This security system needs to be adopted in every part of this country and the world as a whole.

Focusing on the development and implementation of a multicast surveillance system using optical wireless transceiver technology. The system is designed for use in smart environments, such as smart cities, where it can be used to monitor public spaces and enhance public safety.

The study finds that the use of optical wireless transceiver technology allows for the transmission of high-quality video data over long distances, making it ideal for use in large-scale surveillance systems. The multicast approach used in the system allows for the simultaneous transmission of data to multiple recipients, improving the efficiency and effectiveness of surveillance.

The study also finds that the system is highly scalable, allowing for the addition of new cameras and receivers as needed. The use of smart algorithms for video analysis enables the system to automatically detect and alert authorities to potential security threats, improving response times and minimizing false positives.

Overall, the study concludes that the use of optical wireless transceiver technology and the multicast approach is highly effective in enhancing the efficiency and effectiveness of surveillance systems in smart environments. The study provides important insights into the development and implementation of advanced surveillance technologies, with potential applications in various settings, including smart cities, transportation, and critical infrastructure.

5.1.1 Conclusions

In conclusion, the integration of surveillance technology multicast through optical wireless transceivers in smart environments marks a significant leap forward in enhancing security and efficiency. This innovative approach not only enables seamless and high-quality data transmission but also minimizes the limitations associated with IOT based surveillance system multicast. By harnessing the power of optical wireless transceivers, smart environments can benefit from real-time, reliable, and secure surveillance data dissemination to multiple destinations simultaneously. Moving forward, continued research and development in this field hold the potential to revolutionize the way we perceive and implement surveillance technology, making our smart environments safer, smarter, and more interconnected than ever before.

5.1.2 Recommendations

Based on the limitations of the current system, it is recommended that further research be conducted on the development of a robotic AI camera that can differentiate between normal human activities and criminal activities. This camera should be designed to learn and understand human activities with the help of machine learning algorithms, allowing it to identify suspicious behavior and alert authorities in real-time.

However, before the development and deployment of such a system, it is important to consider the ethical and privacy implications of using AI in surveillance and security. There should be clear guidelines and regulations in place to ensure that the system is used responsibly and transparently, with appropriate safeguards to protect individual rights and freedoms.

Additionally, the performance and accuracy of the robotic AI camera should be thoroughly tested and evaluated before it is implemented in real-world settings. This will help to ensure that the system is effective in identifying criminal activities and minimizing false positives.

Overall, the recommendation is to explore the potential of using robotic AI cameras in surveillance and security to improve the accuracy and reliability of criminal activity detection, while ensuring that ethical and privacy considerations are addressed.

5.2 Contribution to Knowledge

In October, 2021, there was a total shutdown of telecommunication network for about a month, in a bid to launch an offensive and disrupt bandits' operations in some parts of Nigeria. Although, telecommunications shutdown was seemingly effective in the first few days of the shutdown in Zamfara, it appears bandits have adapted to the situation. Reports had it that they now adopt Thuraya satellite phones to bypass the ban on telecommunications network. They circumvent networks, still communicate and wreak havoc despite the network suspension and claims of success by the military – while the masses suffer. If this research is being implemented in communities or by the government, there is definitely going to be a smooth operation of this system while the telecommunication network is down. Terrorists, bandits, or culprits will be tracked down with no interruption[12].

The lives of the vulnerable people whom the government seeks to protect were further endangered in the above attack scenarios – as bandits carried out their nefarious activities unrestrained. Can the victims place a distress call in such precarious situations? It even becomes worrisome to receive warning calls to escape impending attacks. No doubt, the

mobile phone shutdown further fuels insecurity. Shutting down telecommunications networks is therefore a counterproductive strategy – and no longer effective. Telecommunications suspension is no longer effective. Further suspension of telecommunication networks is not the panacea to the insecurity challenges; rather, it inflicts pain on the masses who need network to foil attacks and report suspicious movements. It is high time security operatives restrategised. We strongly suggest that there should be no further shutdown in telecommunication network for counter terrorism without the implementation of this study within the masses. Imagine watching on your TV, any harmful coming towards your dwelling, proper measures could have been taken to safe lives and properties.

There were highlights of limitation of the current system used for surveillance and security, namely its inability to automatically differentiate between normal human activities and criminal activities. This highlights the need for more advanced technologies, such as robotic AI cameras, that can learn and understand human activities with the help of machine learning algorithms.

The contribution to knowledge lies in identifying the potential of using AI and machine learning algorithms to enhance the accuracy and reliability of criminal activity detection. By training a system to recognize specific patterns of behavior, it is possible to improve the effectiveness of surveillance and security measures, thereby enhancing public safety.

The development of a robotic AI camera that can differentiate between normal human activities and suspicious behavior has the potential to revolutionize surveillance and security systems. This technology could be used to monitor public spaces, identify

potential threats, and alert authorities in real-time. In doing so, it could significantly improve the safety and security of communities around the world.

The contribution to knowledge, therefore, lies in the identification of a specific area of research, namely the development of a robotic AI camera for surveillance and security purposes, and the potential impact that such a system could have on public safety. This research could inform future development and implementation of advanced surveillance and security technologies that are effective, efficient, and ethically responsible.

5.3 Suggestion for Further Studies

This system could not automatically differentiate between normal human activities and criminal activities, robotic Artificial Intelligence camera, that will learn human activities with the help of machine learning is recommended for a future study.

This study suggests that there is a system that is not able to distinguish between normal human activities and criminal activities automatically. This means that the current system is limited in its ability to identify and flag criminal behavior in real-time. It also means that there is a higher chance of false positives, where innocent individuals are wrongly flagged as potential criminals.

To address this limitation, it is suggested that a robotic artificial intelligence (AI) camera be developed. This camera would be able to learn and understand human activities through machine learning. Machine learning is a subset of AI that involves training a computer system to learn from data and improve its performance over time without being explicitly programmed.

A robotic AI camera would have the potential to provide more accurate and reliable surveillance, as it would be able to differentiate between normal human activities and suspicious behavior based on its learning from data. It could also be programmed to identify specific criminal activities and alert authorities in real-time.

The use of AI in surveillance and security is becoming more common, and it is likely that we will see the development of more advanced AI cameras in the future. However, there are also concerns about the ethical and privacy implications of using such technologies. It is important to ensure that these technologies are developed and used in a responsible and transparent manner, with appropriate safeguards in place to protect individual rights and freedoms.

Bibliography

Book

Ajayi D., Software Testing and quality assurance (CSC 714), Lead City University, 2022

United State Department of Homeland Security; Prepared by Space and Naval Warfare Systems Center Atlantic. *CCTV Technology Handbook 2013*

Conference Proceeding

Anthony B., David W. & Brandon T., *"Focused Deterrence Strategies and Crime Control: An Updated Systematic Review and Meta-Analysis of the Empirical Evidence.*" Criminology & Public Policy, 2018, 17. https://doi.org/10.1111/1745-9133.12353.

Shen B., '*Research on Video Remote Transmission Technology Based on FPGA".* IOP Conference Series: Materials Science and Engineering. 382, 2018, 042031, https://doi.org/10.1088/1757-899X/382/4/042031.

Ebook

Stuart A. & Steven K, "*The American Heritage Student Science Dictionary,*" Second Edition, 2014.

Babbie E., *"The Practice of Social Research,"* 14th ed., 2014, ISBN: 978-1-305-10494-5, https://lms.su.edu.pk/download?filename=1606930922-earl-babbie-the-practice-of-social-research-cengage-learning-2014.pdf&lesson=47225

IEEE 802.15 WPAN™ Task Group 13 (TG13), "Multi-Gigabit/s Optical Wireless Communications," [Online]. 2020 Available: http://www.ieee802.org/15/pub/TG13.html

ITU-T Telecommunication Standardization sector of ITU, G.9991: *High speed indoor visible light communication transceiver – System architecture, physical layer and data link layer specification*, 2019, http://handle.itu.int/11.1002/1000/11830-en

Monette D.R., Sullivan T.J., Dejong C.R., & Hilton T.P., *"Applied Social Research: A Tool for the Human Services,"* 9th ed., 2014, ISBN 10: 128507551X ISBN 13: 9781285075518.

Nielsen J., "Usability 101: *introduction to usability",* 2012, available at: www.nngroup.com/articles/usability-101-introduction-to-usability.

Welsh, B.C. ; van der Laan, P.H. ; Hollis, M.E. / Systematic reviews and cost-benefit analyses: toward evidence-based crime policy. Experimental criminology. Prospects for advancing science and public policy. editor / B.C. Welsh ; A.A. Braga ; G.J.N. Bruinsma. New York : Cambridge University Press, 2013. pp. 253-276 https://research.vu.nl/en/publications/systematic-reviews-and-cost-benefit-analyses-toward-evidence-base.

Willis M., *"Police detainee perspectives on CCTV. Trends & issues in crime and criminal justice no. 538"*. Canberra: Australian Institute of Criminology. 2017

Xolbekova U.M., and Tajibayev A.M., "Security, international peace and religious tolerance and foreign policy -as an important priority in the appeal." Teachers department of "Social Sciences" of Jizzakh Polytechnic InstituteJizzakh, Uzbekistan. vol. 2, 2021, 175-194. https://doi.org/13.1219/ICoICT.2021.8768272

Journal

Abid K., Lakhlef H., & Bouabdallah A., *A survey on recent contention-free MAC protocols for static and mobile wireless decentralized networks in IoT,* **Computer Networks**, 201, 2021, 108583, doi:https://doi.org/10.1016/j.comnet.2021.108583.

Adebisi O., Adejumobi I., Durodola F. & Jim H. *Development of a microcontroller based automobile speed limiting device and alarm control system.* **International Journal of Electrical and Computer Engineering (IJECE)**. 13(1), 2023 195-206, https://doi.org/10.11591/ijece.v13i1.pp195-206.

Agrawal R., Faujdar N., Romero C.A.T., Sharma O., Abdulsahib G.M., Khalaf O.I., Mansoor R.F., & Ghoneim O.A, *Classification and comparison of ad hoc networks: A review*. **Egyptian Informatics Journal**, [online] 24(1), 2023, pp.1–25. doi:https://doi.org/10.1016/j.eij.2022.10.004.

Alexandra G., Willis M., Taylor E. & Lee M., *Surveillance technologies and crime control: Understanding police detainees' perspectives on police body-worn video (BWV) and CCTV cameras (Criminology Research Grants, No. CRG 31/14-15).* Report to the Criminology Research Advisory Council. Canberra City, Australia: Australian Institute of Criminology. 2017 https://www.aic.gov.au/publications/tandi/tandi538

Algethami N, Redfern S. A Robust *Tracking-by-Detection Algorithm Using Adaptive Accumulated Frame Differencing and Corner Features.* **J Imaging**, 6(4): 2020 pp.25. doi: 10.3390/jimaging6040025. PMID: 34460727; PMCID: PMC8321033.

Ali A., Ali A., Masud F., Bashir M.K., Zahid A.H., Mustafa G., & Ali Z., *Enhanced Fuzzy Logic Zone Stable Election Protocol for Cluster Head Election (E-FLZSEPFCH) and Multipath Routing in wireless sensor networks.* **Ain Shams Engineering Journal,** [online] 2023, p.102356. doi:https://doi.org/10.1016/j.asej.2023.102356.

Ammar G., Hussini S.M., Khreishah S., Khalil A., Guizani I., Al-Fuqaha M. & Ala, Smart Cities: *"A Survey on Data Management, Security and Enabling Technologies",* IEEE Communications Surveys & Tutorials. 2017, pp.1-1, https://doi.org/10.1109/COMST.2017.2736886.

Anthony B., David W. & Brandon T., *Focused Deterrence Strategies and Crime Control: An Updated Systematic Review and Meta-Analysis of the Empirical Evidence,* **Criminology & Public Policy**, 2018, 17. https://doi.org/10.1111/1745-9133.12353.

Bhattacharjee S., Acharya T., & Bhattacharya U., *Cognitive radio based spectrum sharing models for multicasting in 5G cellular networks: A survey,* **Computer Networks**, [online] 208, 2022, p.108870. doi:https://doi.org/10.1016/j.comnet.2022.108870.

Braga, Anthony & Weisburd, David & Turchan, Brandon, Focused Deterrence Strategies and Crime Control: An Updated Systematic Review and Meta-Analysis of the

Empirical Evidence. **Criminology & Public Policy**, 2018, 17. 10.1111/1745-9133.12353.

Cailean M., Dimian, & Mihai. *"Impact of IEEE 802.15.7 Standard on Visible Light Communications Usage in Automotive Applications,* **IEEE Communications Magazine***",* 2017, PP. 2-7, https://doi.org/10.1109/MCOM.2017.1600206CM.

Chen Y.-S., Lin C.-K., & Kan Y.-W, *An Advanced ICTVSS Model for Real-Time Vehicle Traffic Applications*, **Sensors**, 19(19), 2019, p.4134. doi:https://doi.org/10.3390/s19194134.

Chikodiri N. & Olihe O., *National Security and Sustainable Economic Development in Nigeria since 1999:* Implication for the Vision 20 2020, 2014, 4. 129-142. https://doi.org/10.5901/jesr.2014.v4n5p129.

Chiu P.-C., Su K.-W., Ou T.-Y., Yu C.-L., Cheng C.-Y., Hsiao W.-C., Shu M.-H., & Lin G.-Y, *An Adaptive Location-Based Tracking Algorithm Using Wireless Sensor Network for Smart Factory Environment*. **Mathematical Problems in Engineering**, [online] 2021, p.e4325708. doi:https://doi.org/10.1155/2021/4325708.

Cui X., *Explore the Application Effect of Wireless Networks in Smart Clothing Based on Artificial Intelligence Technology,* **Wireless Communications and Mobile Computing**, 2022, pp.1–9, doi:https://doi.org/10.1155/2022/6937128.

Du H., & Zhang Y., *Ensemble Learning-Based Multi-Cues Fusion Object Tracking in Complex Surveillance Environment,* **Computational Intelligence and Neuroscience**, [online] 2022, p.e9165744. doi:https://doi.org/10.1155/2022/9165744.

Durdi V. B, Kulkarni P. T., & Sudha K. L., *Robust Video Transmission over Wireless Networks Using Cross Layer Approach*, **Journal of Industrial and Intelligent Information,** Vol. 1, No. 2, 2013, pp. 97-101doi: 10.12720/jiii.1.2.97-101

Glasl H., Schreiber D., Viertl N., Veigl S., & Gustavo F.D., "*Video based Traffic Congestion Prediction on an Embedded System,"* 2008, 950 - 955. https://doi.org/10.1109/ITSC.2008.4732555.

Gopikrishnan R., **International Journal of Computer Science and Mobile Computing**, Vol.3 Issue.2, February- 2014, pg. 811-814, https://ijcsmc.com/docs/papers/February2014/V3I2201499a57.

Haroon I., S. Mubarak & S. Ray, *"Enhancing camera surveillance using computer vision":* a research note, **Policing**. 41, 2018, pp.292-307, https://doi.org/10.1108/PIJPSM-11-2016-0158.

He C. & Chen C., *"A Review of Advanced Transceiver Technologies in Visible Light Communications. Photonics".* 2023, 10-648. https://doi.org/10.3390/photonics10060648.

Hyungjin L., & Pamela W., *"Crime-Reduction Effects of Open-street CCTV: Conditionality Considerations."* Justice Quarterly, 34, 2016, 1-30, 10.1080/07418825.2016.1194449.

Ismail R., Fabil N., & Saleh A., *"Extension of pacmad model for usability evaluation metrics using goal question metrics (Gqm) approach*." **Journal of Theoretical and Applied Information Technology.** 2015, 79, https://www.researchgate.net/publication/325484529_Extension_of_pacmad_model_for_usability_evaluation_metrics_using_goal_question_metrics_Gqm_approach/citation/download.

Kalvein R., Wirawan, Hendrantoro G., Affandi A., & Hua-An Zhao, *A New Scheme for Evaluating Video Transmission over Broadband Wireless Network* , **Future Wireless Networks and Information Systems**, LNEE 143, 2012 pp. 335–341, Springerlink.com © Springer-Verlag Berlin Heidelberg.

Khan P.W., Byun Y.-C., & Park N., *A Data Verification System for CCTV Surveillance Cameras Using Blockchain Technology in Smart Cities*, **Electronics**, 9(3), 2020, pp.484. doi:https://doi.org/10.3390/electronics9030484

Kim M., Man K.L., & Helil N., *Advanced Internet of Things and Big Data Technology for Smart Human-Care Services*. **Journal of Sensors**, 2019, pp.1–3. doi:https://doi.org/10.1155/2019/1654013.

Lee I.-H., Kim J.-B., Jung H., Kwon S.-C. (Sean), & Kurniawan E., *Advanced Wireless Technology for Ultrahigh Data Rate Communication*, **Wireless Communications and Mobile Computing**, 2019, pp.1–2. doi:https://doi.org/10.1155/2019/9790853.

Lillian W., Kiaw Y., Sook-Ling L., Siong-Hoe L. & Leow C., *"Usability factors predicting continuance of intention to use cloud e-learning application,"* **Heliyon** 5, 2019, https://doi.org/10.1016/j.heliyon.2019.e01788.

Luo Y., *Construction of Smart Higher Education Teaching Resources Using Data Analysis Technology in Unbalanced Data Environment,* **Journal of Environmental and Public Health**, 2022, pp.1–12. doi:https://doi.org/10.1155/2022/2130623.

Lv Z., Ota K., Lloret J., Xiang W., & Bellavista P., *Complexity Problems Handled by Advanced Computer Simulation Technology in Smart Cities 2021*. **Complexity**, 2022, pp.1–3. doi:https://doi.org/10.1155/2022/9847249.

Matthew A., The Value of CCTV Surveillance Cameras as an Investigative Tool: An Empirical Analysis. **European Journal on Criminal Policy and Research**, 2017, 23, 10.1007/s10610-017-9341-6.

Michelle C., & Wolter P., *"The effectiveness of surveillance technology: What intelligence officials are saying, The Information Society",* 34, 2018, 88-103. https://doi.org/10.1080/01972243.2017.1414721.

Nam-Tuan L., Hossain A., Jang M., Min Y, *"A Survey of Design and Implementation for Optical Camera Communication. Signal Processing":* Image Communication, 2017, 53. https://doi.org/10.1016/j.image.2017.02.001.

Narejo S., Pandey B., Esenarro vargas D., Rodriguez C., & Anjum M.R., *Weapon Detection Using YOLO V3 for Smart Surveillance System*, **Mathematical Problems in Engineering,** 2021, pp.1–9. doi:https://doi.org/10.1155/2021/9975700.

Piza E. I, Joel C. & Leslie K., *CCTV as a tool for early police intervention: Preliminary lessons from nine case studies.* **Security Journal**, 30, 2017, https://doi.org/10.1057/sj.2014.17.

Piza E. I, The History, *Policy Implications, and Knowledge Gaps of the CCTV Literature: Insights for the Development of Body-Worn Video Camera Research,* **International Criminal Justice Review**, 31, 2018, https://doi.org/10.1177/1057567718759583.

Piza E. I., & Systma V. A, *Exploring the Defensive Actions of Drug Sellers in Open-air Markets: A Systematic Social Observation,* **Journal of Research in Crime and Delinquency**, 53. 2016, pp.36-65, https://www.researchgate.net/journal/Journal-of-Research-in-Crime-and-Delinquency-0022-4278.

Ray P. P, *A perspective on 6G: Requirement, Technology, Enablers, Challenges and Future Road Map.* **Journal of Systems Architecture,** 118, 2021, doi:https://doi.org/10.1016/j.sysarc.2021.102180

Sakpere W.E., *"A near field communication framework for indoor navigation: design and deployment considerations."* Master's Thesis, Cape Peninsula University of Technology. 2015, http://digitalknowledge.cput.ac.za/xmlui/handle/11189/3628

Shane J., Nick T. & Kate B., Introducing EMMIE: *"An evidence rating scale to encourage mixed-method crime prevention synthesis reviews.*" Journal of Experimental Criminology, 2015, 11, https://doi.org/10.1007/s11292-015-9238-7.

Shane J., Nick T. & Kate B., *Introducing EMMIE: An evidence rating scale to encourage mixed-method crime prevention synthesis reviews,* **Journal of Experimental Criminology**, 2015, 11, https://doi.org/10.1007/s11292-015-9238-7.

Shu Z., Chen M.Z.Q., & Hui Q., *Advanced Mathematical and Numerical Methods in Control and Optimization for Smart Grids* **Mathematical Problems in Engineering**, [online] 2019, p.e2074019. doi:https://doi.org/10.1155/2019/2074019.

Silvana S.S., Valerio B., Davide C., Biancone & Paolo. "*Towards a hybrid model for the management of smart city initiatives",* Cities, 116, 103278, 2021, https://doi.org/10.1016/j.cities.2021.103278.

Sukhavasi S.B., Elleithy K., Abuzneid S., & Elleithy A., *CMOS Image Sensors in Surveillance System Applications. Sensors,* 2021, 21, 488, https://scholarworks.bridgeport.edu/xmlui/handle/123456789/4413

bSukhavasi S.B., Elleithy K., Abuzneid S., Elleithy A. & Abdelrahman, *"Human Body-Related Disease Diagnosis Systems Using CMOS Image Sensors*:' A Systematic Review. **Sensors**, 21, 2021, 2098, https://doi.org/10.3390/s21062098.

Tan W., Fen Y., & Yuan Q., *Optimization of Historic Building Survey Technology under Artificial Intelligence Wireless Network Technology Environment*. **Wireless Communications and Mobile Computing,** 2021, pp.1–12. doi:https://doi.org/10.1155/2021/6408772.

Ahmad, F., Ramachandrapura, S., Manattayil, J. and Raghunathan, V. (2020). *Path-Loss Optimized Indoor Laser-Based Visible Light Communication System for Variable Link Length Gigabit-Class Communication*. **IEEE Photonics Journal**, 12(4), pp.1–12. doi:https://doi.org/10.1109/jphot.2020.3014216.

Nguyen T., Islam A., Hossan T. & Jang Y. M., *Current Status and Performance Analysis of Optical Camera Communication Technologies for 5G Networks*, in ***IEEE Access***, vol. 5, 2017, pp. 4574-4594, doi: 10.1109/ACCESS.2017.2681110.

El Majdoubi, D., El Bakkali, H., Sadki, S., Maqour, Z. and Leghmid, A. *The Systematic Literature Review of Privacy-Preserving Solutions in Smart Healthcare Environment,* **Security and Communication Networks**, 2022, pp.1–26. doi:https://doi.org/10.1155/2022/5642026.

Wang W., Chen X., Zhang G., Qian J., Wei P., Wu B., & Zheng H., *Precision Security: Integrating Video Surveillance with Surrounding Environment Changes,* **Complexity**, 2018, pp.1–10. doi:https://doi.org/10.1155/2018/2959030.

Xu R., Nikouei S.Y., Nagothu D., Fitwi A., & Chen Y., *BlendSPS: A BLockchain-ENabled Decentralized Smart Public Safety System,* **Smart Cities**, 3(3), 2020, pp.928–951. doi:https://doi.org/10.3390/smartcities3030047.

Yadav M., Singh K., Pandey A.S., Kumar A., & Kumar R., *Smart Communication and Security by Key Distribution in Multicast Environment,* **Wireless Communications**

and Mobile Computing, [online] 2022, p.e1011407. doi:https://doi.org/10.1155/2022/1011407.

Yuchen X., Guan W.P., Shangsheng W., Jingyi L., Zeyang L., Manxi L., *The Optical Bar Code Detection Method Based on Optical Camera Communication Using Discrete Fourier Transform.* **IEEE Access**, 2020, pp.1-1, https://doi.org/10.1109/ACCESS.2020.3006752.

Xiao Y., Guan W., Wen S., Li J., Li Z. and Liu M., *The Optical Bar Code Detection Method Based on Optical Camera Communication Using Discrete Fourier Transform*, in **IEEE Access**, vol. 8, 2020, pp. 123238-123252, doi: 10.1109/ACCESS.2020.3006752.

Zhang, Z., Qian, S., Zhang, Q. and Li, L., *Advanced Concrete Technology and Its Structural Applications,* **Advances in Civil Engineering**, 2022, pp.1–4. doi:https://doi.org/10.1155/2022/9781273.

Zhao J., *Construction of College Chinese Mobile Learning Environment Based on Intelligent Reinforcement Learning Technology in Wireless Network Environment,* **Wireless Communications and Mobile Computing**, 2022, pp.1–10. doi:https://doi.org/10.1155/2022/5164430.

Zhu S., Zhou C., & Wang Y., *Highly Efficient Multicast over Surface Wave in Hybrid Wireless-Optical On-Chip Networks for IoT HPC,* **Wireless Communications and Mobile Computing**, [online] 2022, p.e3882894. doi:https://doi.org/10.1155/2022/3882894.

Electronic Sources (Internet)

Torr M., "*Defining the Fourth Industrial Revolution: Where IOT fits and the potential*", Microsoft Library, 2016, https://news.microsoft.com/europe/features/defining-the-fourth-industrial-revolution-where-iot-fits-and-the-potential/

Wikipedia, Donabedian model, 2023, https://en.wikipedia.org/wiki/Donabedian_model

Digital Evidence Section Forensic Scientist Manager, "*Technical Procedure for DVR Analysis*", Version 5, 2018 https://forensicresources.org/wp-content/uploads/2019/07/Video-DVR-Analysis-Procedure-06-13-2018.pdf

Magazine Article

Cine Gears Incorporation, "*ghost eye wireless hdmi/sdivideo transmission system user manual", 2020*

Appendix

Appendix A: Images of the system implementation

Plate A: A picture of the assembled Digital Video Recorder (DVR)

Plate B: 2 types of Video Recorder

Plate C: Outdoor Bullet Camera

Plate D: RG59 Connection cable with power

Plate E: Outdoor Bullet Camera

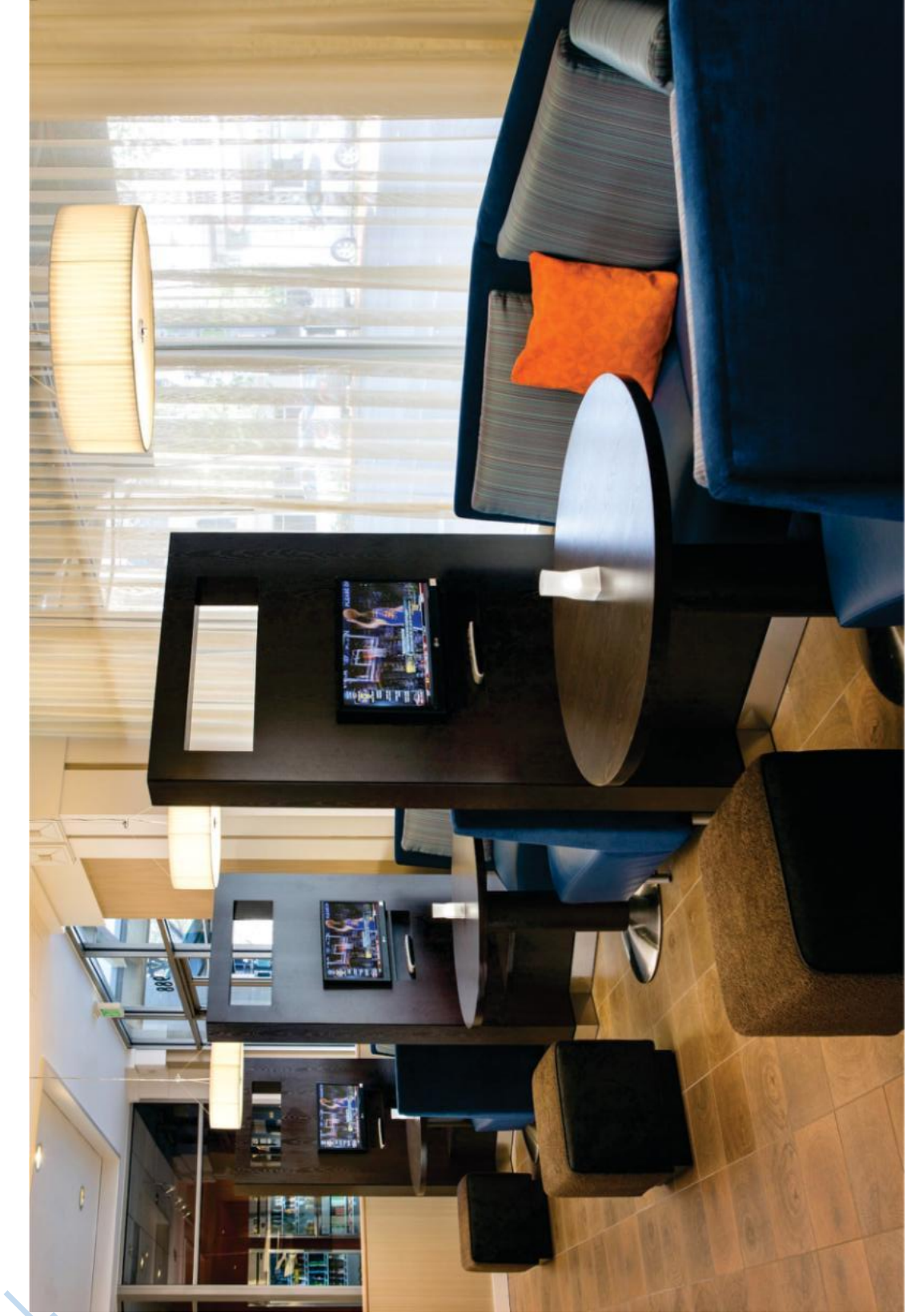


Plate F: Front and Back view of the DVR after final integration

Plate G: Display Result without a storage device

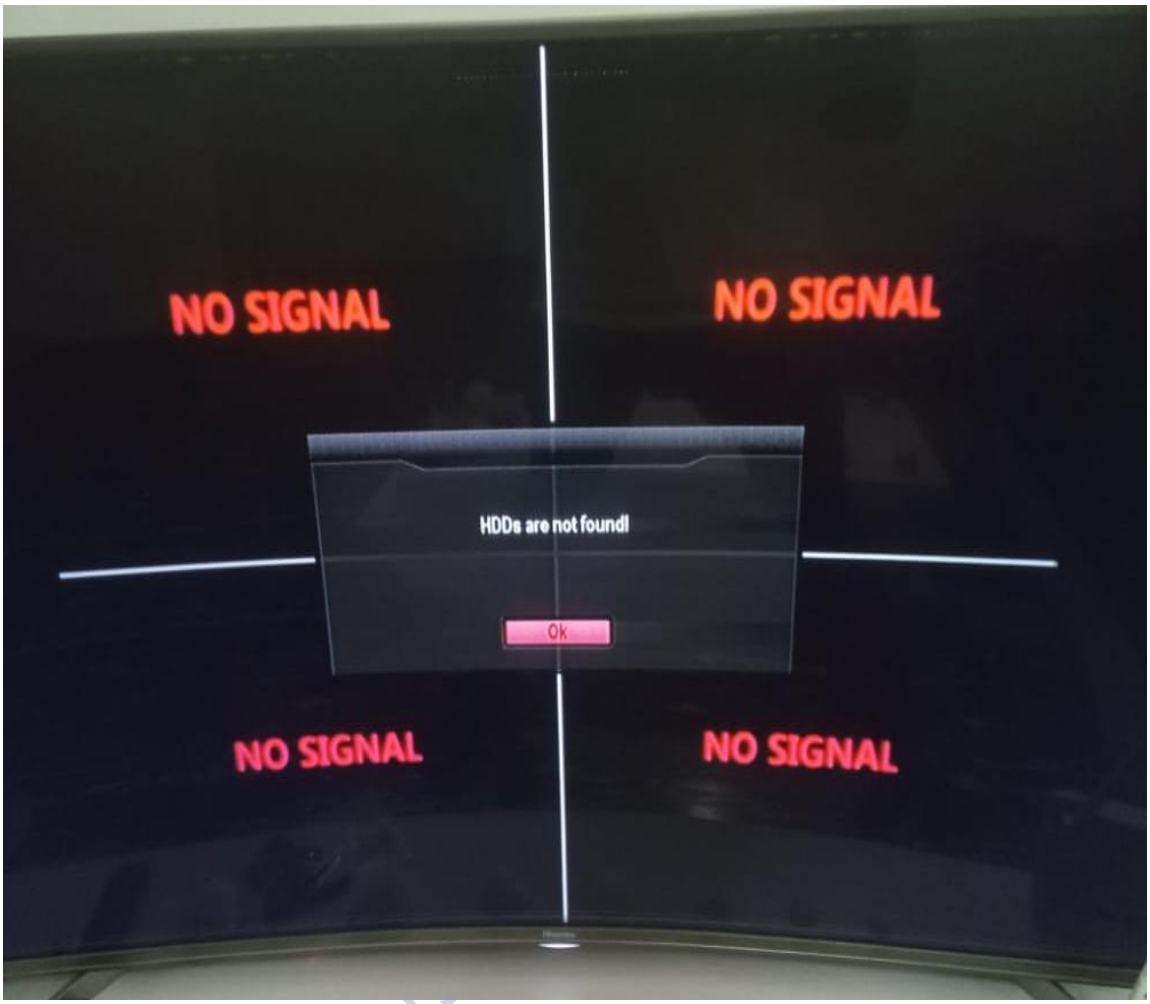


Plate H: DVR internal hardware before integration

Plate I: Hard-Drive

Plate J: Wireless Transceiver Module

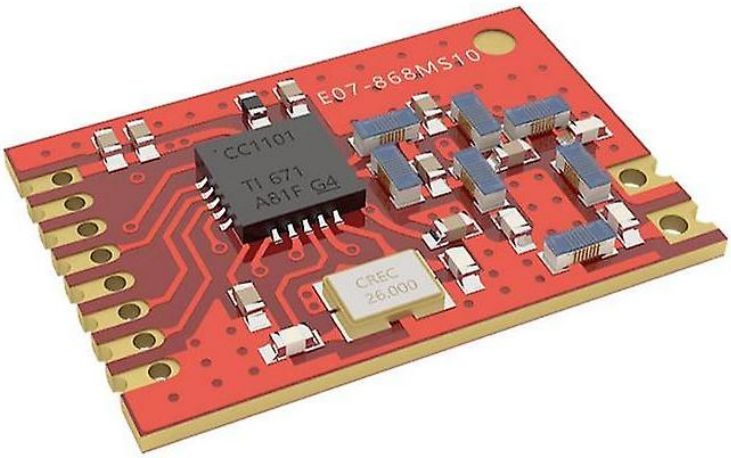


Plate K: Display Result after hard-drive integration

Plate L: Hard-drive integration with the DVR

Plate M: Wireless data receiver

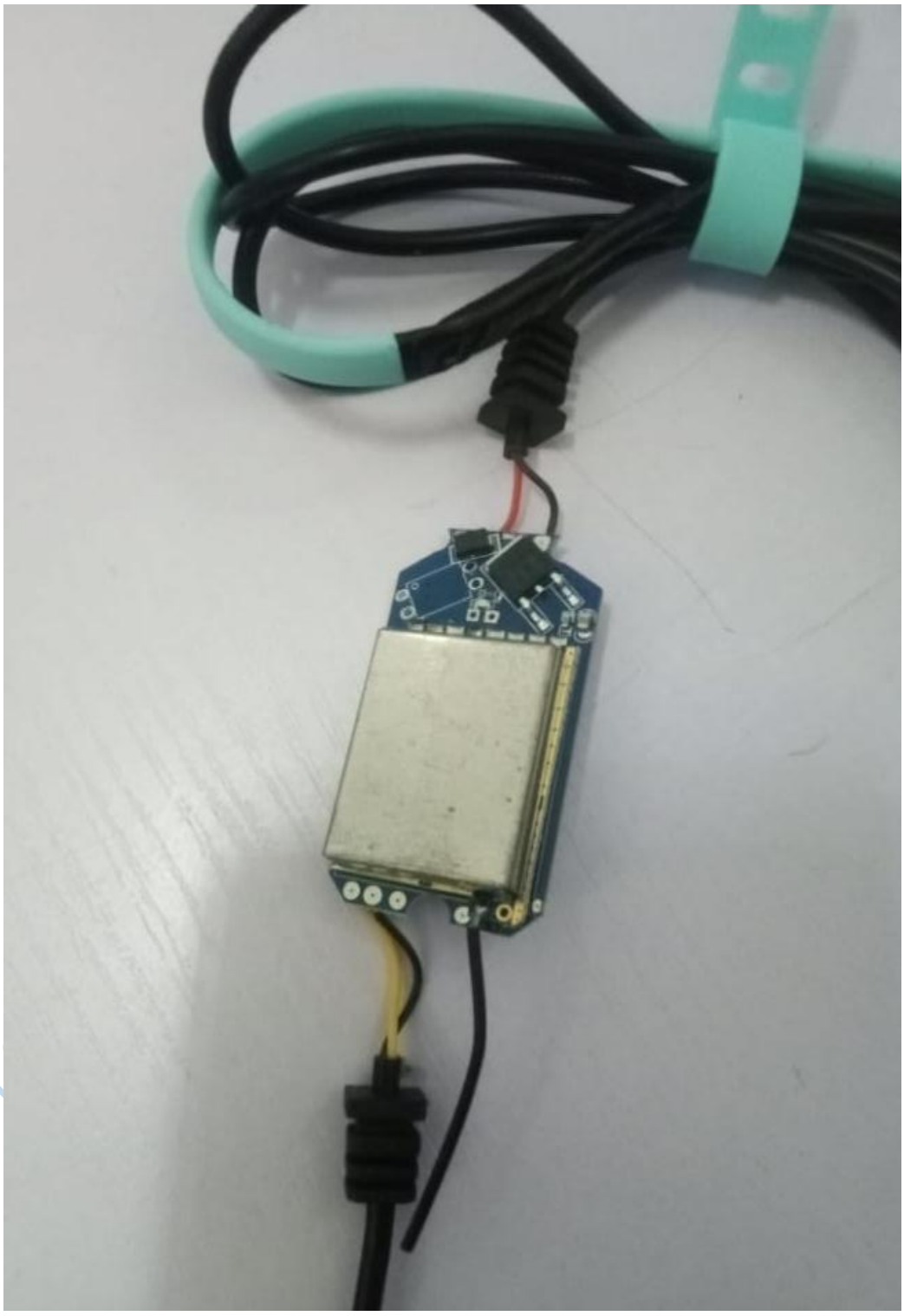


Plate N: Insufficient power supply output result

Plate O: Power Supply unit

Plate P: Hardware view after Hard-drive and power supply integration

Plate Q: Performance Evaluation

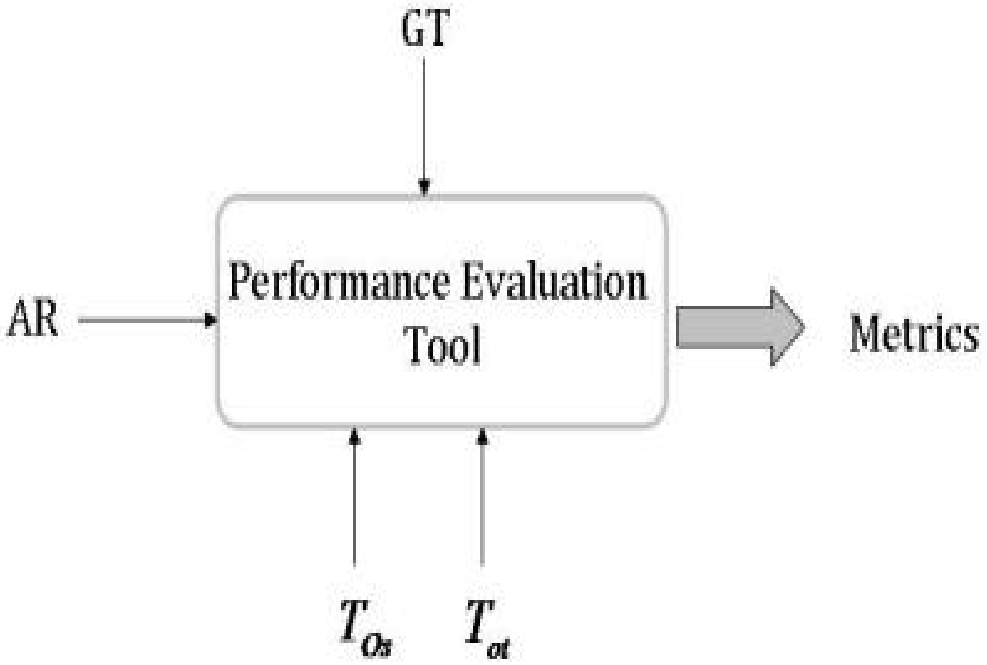
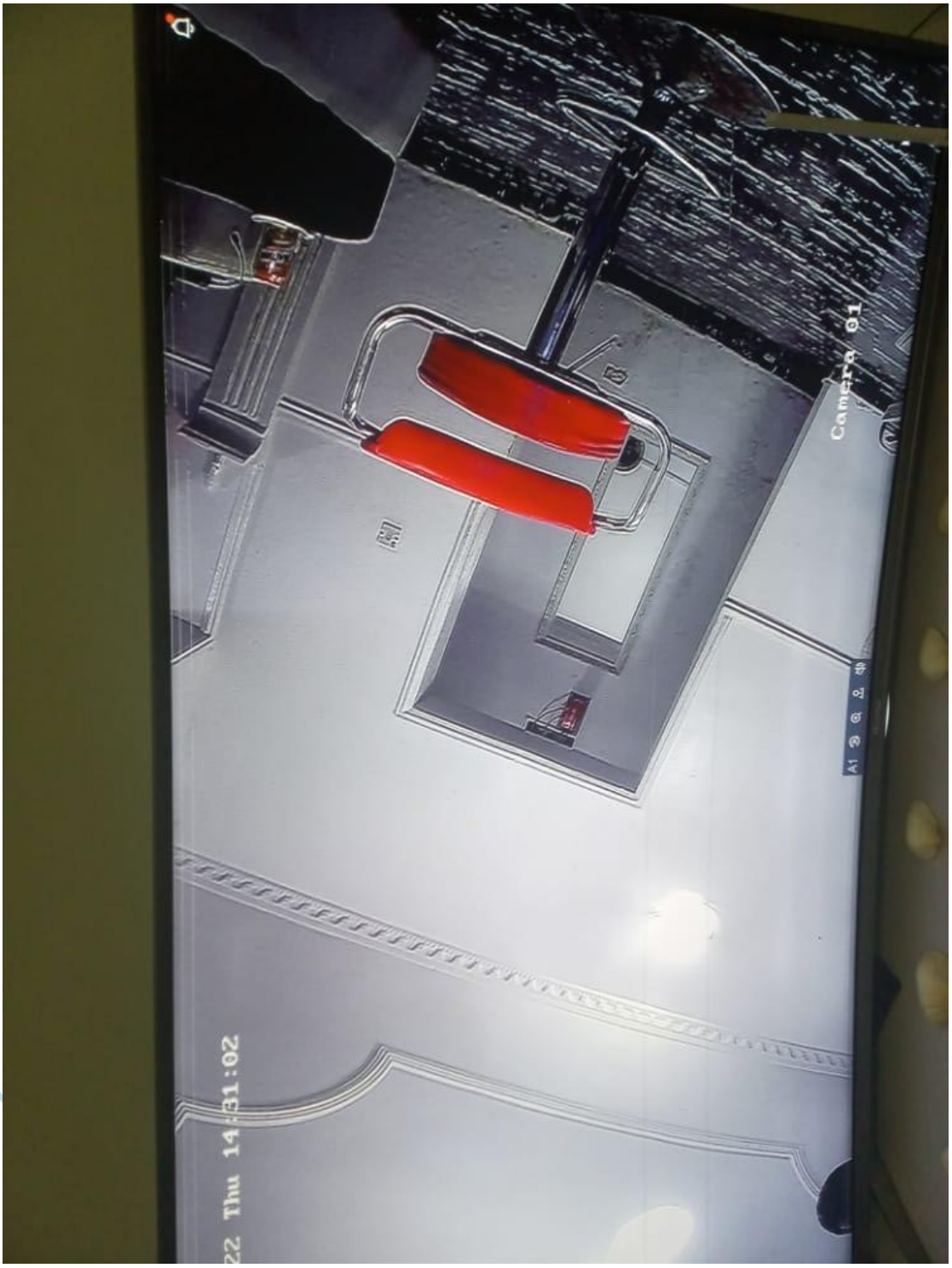


Plate R: Image censing setting

Plate R: Indoor dome CCTV camera

Plate S: Wireless data transmitter

Plate T: DVR final Integration display



Bio-data

Personal Data:

Surname: FAKUNLE

Other Names: ISRAEL OLUWAGBEJAMIJA

Date of Birth: 16 July, 1989

Gender: Male

Local Government Area: Obokun

State of Origin: Osun State

Nationality: Nigerian

Marital Status: Single

Religion: Christianity

Next of Kin: Elizabeth Y. Adeniyi

Contact:

Residential Address: Plot 4, Omorinre Johnson, Lekki Phase 1, Lagos

Postal Address: Same as above.

Email Address: heezyboss@gmail.com

Mobile No: +234 813 441 2128

Educational Background:

Institutions attended with Dates and Qualification:

Lead City University, Toll Gate, Ibadan, Oyo State: 2021 till date (MSc. Computer and Information Science)

The Polytechnic, Ibadan, Oyo State: 2015 -2017

Tower Polytechnic, Ibadan, Oyo State: 2011- 2013

West African School Certificate / Make Hay International College, Ibadan, Oyo State 2000-2006

Primary School Leaving Certificate/ Make Hay International Nursery and Primary School, Ibadan, Oyo State: 1990 -1999

Professional Qualifications

Nil

Certifications

Full Stack Developer	2020
Professional CCTV Installation and Configuration	2019
Desktop Publishing / Graphic Design	2007

Work Experience with Dates

- Siren Computer Institute (Instructor), Osogbo, Nigeria. 2017 & 2018
- PHCN (Computer Analyst), Ibadan, Nigeria 2019-2020
- Oshinubi & Associates Legal Practitioners, (Software Engineer) Ibadan, Nigeria 2010-2012
- Sqreems Lounge & Bar, (IT Manager), Ibadan, Nigeria 2013-2016
- Tek-Experts Microsoft Affliate (Microsoft Dynamics Support Engineer), VI, Lagos Nigeria 2020-2021
- 7th Breed Consult (Lead Strategist) 2018-

Published Journal Articles

Skills

- Web analysis and design

- Software engineering
- Web development
- Ability to work under duress

Referees

1. **Dr. Wilson Sakpere**

   Department of Computer science

   Lead City University, Ibadan, Oyo State.

   08159582869

2. **Elizabeth Adeniyi**

   Head of Marketing,

   Standard Alliance Insurance

   08038333008

3. **Ayodeji Johnson**

   Chief Executive Officer

   Mr. Johnson Furniture & Interior Decor.

   07018557168

Signature _____ Date _____

The University Compliance Certification

This is to certify that this thesis by Israel Oluwagbejamija FAKUNLE with Matriculation Number LCU/PG/002520 in the department of Computer Science, Faculty of Natural and Applied Science, Leas City University, Ibadan is in full compliance with the approved University's format and style.

…… Signature

……. Date:

Israel Fakunle Thesis LCU LIB3RARY

ORIGINALITY REPORT

15%	18%	15%	14%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.researchgate.net Internet Source	7%
2	onlinelibrary.wiley.com Internet Source	4%
3	www.emeraldinsight.com Internet Source	2%
4	www.instructables.com Internet Source	2%

Exclude quotes	Off	Exclude matches	< 2%
Exclude bibliography	On		