International Journal of Engineering Trends and Technology
ISSN: 2231–5381 / https://doi.org/10.14445/22315381/IJETT-V72I7P123

Volume 72 Issue 7, 214-223, July 2024

Original Article

IoT Interoperable Surveillance System Using Wireless and Fiber Cable

Percy Okae[1], Isaac Adjaye Aboagye[1*], Nii Longdon Sowah[1], Eric Tetteh Ofoe[1], Margaret Richardson Ansah[1], Gifty Osei[1]

[1]*Department of Computer Engineering, University of Ghana, Accra, Ghana.*

[*]*Corresponding Author : iaaboagye@ug.edu.gh*

Received: 18 November 2023 Revised: 29 March 2024 Accepted: 01 July 2024 Published: 26 July 2024

Abstract *- The exponential growth of science and technology, together with the improvement of the standard of living of people, has made security and surveillance systems essential for our day-to-day activities. These demands have increased the usage of surveillance systems such as CCTVs from the comfort of our homes, schools, hospitals, and workplaces. There are presently many surveillance system implementations to meet these demands; however, these systems have low bandwidths, lack interoperability with Internet protocol surveillance devices from different vendors, and do not allow multiple users to access and interact with a single system. This study aimed to develop a video surveillance system by using a wireless network and optical fiber cable to provide a systematic approach to integrating internet protocol cameras into Web applications for video and data transmissions. The study adopted a waterfall model to create an application that will integrate different makes of security devices into one uniform system and subsequently deploy it as a Web application for easy access. The robustness of the developed system addressed the challenges of currently existing systems. By using optical fiber as the backbone, we improved CCTV surveillance in terms of transmission speed, footage quality, and general performance of the systems.*

Keywords *- Closed-Circuit Televisions, Internet Protocols, NVRs, Power over ethernet switches, Video surveillance systems, Web applications.*

1. Introduction

Surveillance refers to the systematic monitoring of individuals, groups, or environments to gather information, track activities, or manage security. It can be carried out through various methods, including the use of cameras, sensors, data collection, etc. In recent years, security systems have become essential to businesses, educational institutions, and homes owing to the growing rates of crime [1-3]. Manufacturers have been developing many types of security systems which include advanced internet protocol (IP) security cameras, door locking systems, and many others, with the intent of preventing unauthorized access to private properties. Traditionally, video surveillance is usually based on an Analog Video Recorder (AVR) to implement the monitoring system. The mobility of these systems is poor and also requires someone to guard the frontage of the monitoring equipment. Recently, Network Video Recorders (NVRs) have become available for purchase. These systems operate by encoding and processing video in cameras before transmitting it to NVR for storage or remote viewing [4]. The solution is beneficial to businesses with many locations since users can monitor multiple departments at once through the network. With the advent of information and communication technology and Internet Protocol, video surveillance technology has experienced different stages of innovation [5-8]. However, the lack of real-time alerts when an intrusion occurs for owners of existing security systems is an issue. Secondly, the differences in proprietary software and hardware of various brands are problematic when one wants to combine the hardware as well as the software from different proprietors to create a seamless surveillance system. Thirdly, the use of coaxial cables in surveillance systems has some disadvantages, such as cable distance, installation issues, quality of video or images, etc. [9-12]. Many existing IoT surveillance systems face limitations because of different standards, protocols, and architectures used in different IoT systems. This makes it difficult to integrate different systems and devices. This can lead to interoperability issues and make it difficult to achieve the full potential of IoT. The issue of interoperability presents a significant research gap. Fiber optic cables and wireless web surveillance systems can be deployed as long as system interoperability is implemented. In this research, a wired (fiber) and wireless Web Internet Protocol Surveillance System (WWIPSS) is developed to enable seamless interoperability of devices irrespective of the differences in both the software and the hardware. The focus of the research is to design a system that is capable of effectively functioning across different environments while

maintaining interoperability between components. This research will provide all stakeholders with a systematic approach for planning and creating web applications that will integrate any type of internet protocol security cameras for monitoring and securing lives and properties. The contributions of this research will include the following: propose a novel architecture for IoT systems that allows for interoperability between different devices and systems, achieve interoperability among different surveillance components regardless of their protocols or hardware specifications, and provide a case study of the architecture using a real-world IoT application.

This research has been structured into five major sections. Section one presents an introduction to the concept of surveillance. Section two will address research works related to this study, the proposed work, and the scope of the study. Section three deals with the proposed architecture of the systems as well as the integrated system. Section four is the design implementation as well as testing of the system. Section five presents the conclusions of the system implementation. It captures the challenges faced in the system design and implementation stages as well as recommendations for future works.

2. Literature Review

The literature review of existing works was done to establish the level of work done in surveillance system design and implementation. Zeliang Liu et al. [13] conducted a study on the Anti-Theft Technology of Museum Cultural Relics Based on the Internet of Things. In their research, they proposed a museum anti-theft scheme based on the Internet of Things (IoT) technology, which recognizes whether the cultural relics are within the safe zone through the passive RFID readers. Once stolen, the cultural relics will leave the effective RFID identification range, which results in immediate alarm, and then the system starts the anti-theft plan. Although the designed scheme of the system met the expected requirements, and the museum's anti-theft system based on IoT technology was achieved, the following challenges exist.

The detection accuracy of the hardware part of the system can be further improved to improve the safety of museum equipment. The RFID system has a limited recognition range, and signal strength may be affected if there is a certain volume of obstacle between the reader and the tag.Jayendra Kumar et al. [14] proposed a Real-Time Monitoring Security System integrated with Raspberry Pi and e-mail communication link. In their research, they proposed a system for smart door lock technique with Raspberry Pi using IoT by integrating a webcam and motion sensor with e-mail. The proposed system is a one-step (pin) authentication process which makes the system less secure. Also, there was no database to store data. Chia-Hsu Kuo et al. [15] presented research on an Image-based Intelligent Surveillance System with the Robust Universal Middleware Bridge Service. In this paper, they propose an Image-based Intelligent Surveillance System (IISS) integrated with the Universal Middleware Bridge Service (UMBS) for IP camera networking. The UMBS provides mechanisms related to manual system setting, automatic configuration, and management for improving the entire setting and installation procedures. The researchers could have combined the framework and application services with cloud computing. Also, they did not extend the UMBS for IP camera networking to a mobile platform. Ali Tekeoglu and Ali Şaman Tosun [16] Implemented an Experimental Framework for Investigating the Security and Privacy of IoT Devices. In this research, they proposed a framework for the investigation of security and privacy issues of IoT devices. The framework consists of four components: a testbed, a set of topics to be investigated, a set of experiments for each topic investigated, and a final report. The fundamental approach used in the framework is to capture layer 2 and layer 3 packets and to analyze the packets for various features.

Using the framework, they investigated the security and privacy issues of many IoT devices, including HDMI sticks, IP cameras, activity trackers, smartwatches, and drones. There were various security and privacy issues in the devices used, ranging from simple issues such as passwords to more complex issues such as insecure mobile apps and web interfaces. The proposed framework could be applied to other IoT devices by just connecting them to access points and executing the experiments.

3. System Design and Development

The design of the proposed system will include the physical arrangement of network devices such as wireless intelligent routers, switches, Internet Protocol cameras, fiber optic cable, twisted pair cable, and mini servers for the installation of the web and database server. Secondly, applications such as MySQL, Java, HTML5, Apache, and PHP would be installed on a Windows or Linux platform to support the configuration of the system [17-19]. We interconnected and powered the IP cameras via the Power over Ethernet (PoE) switch. Electrical signals from the PoE switch were transmitted to the media converter, which converted the electrical signals to light signals and then transmitted over the optical fiber cable to the other receiving end for reconversion back into electrical signals. The electrical signals are then transmitted to the router, and then Network Video Recorder on the desktop for real-time monitoring of the captured video footage.

3.1. System Architecture (Optical Fiber and CAT6)

The physical design setup included our internet protocol cameras (IP cameras), PoE switches, routers, local network storage devices, fiber optic cables, twisted pair cables, connectors, network video recorder, media converter, PC, and a mobile device (mobile phone). The devices were

interconnected using a combination of fiber optic cable and CAT 6 cable. The PoE switch powered the IP cameras. These two devices were connected using the CAT 6 cable. The PoE switch was connected to the media converter using a CAT 6 cable. The media converter is connected to another media converter using a fiber optic cable, as shown in Figure 1a. The other end of the media converter is connected to the router and the Network Video Recorder (NVR) using a CAT 6 cable. It was then connected to the desktop monitor for real-time monitoring of the videos captured by the IP cameras. A different setup was designed using only CAT 6 cables. This is shown in Figure 1b. To ensure that there was a continuous transmission of signals, a continuity test was performed on the CAT 6 and fiber optic cables using a cable tester and a visual fault locator, respectively. Figures 1a and 1b below depict the architectural overview of the surveillance system with fiber optic cable and CAT 6 cable [20].

3.2. Architectural View of WWIPSS

The physical network is made up of local servers, wireless routers, Internet Protocol Cameras (IPC), local network storage, and backup devices. The WWIPSS web application development requires that system administrators install operating system software such as Windows Server 2016 or Windows 10 64-bit or Linux server and other applications on the local host empty shell computer, ensure that all network devices are configured with standard TCP and UDP protocols, configure all Internet Protocol cameras with static IP addresses, ensure that local storage and backup devices are configured to have automatic recovery capabilities, and to install Uninterruptible Power Supply (UPS) equipment to prevent power failures.

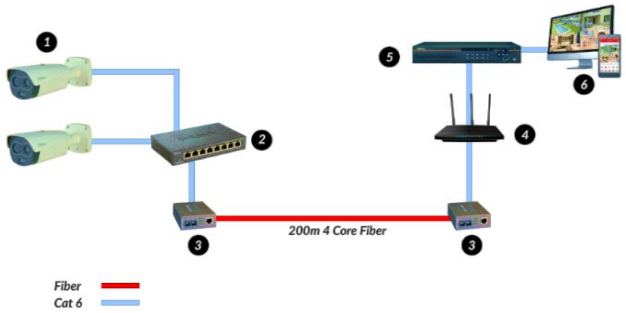

Fig. 1a Fiber Optic and CAT 6 surveillance system implementation

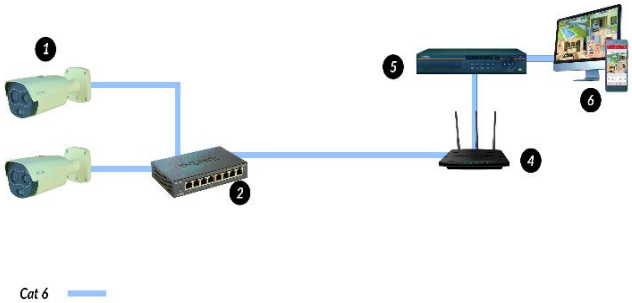

Fig. 1b CAT 6 surveillance system implementation

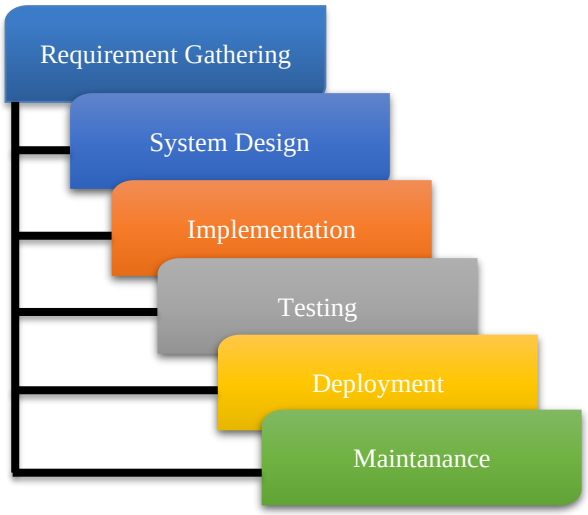

Fig. 2 Waterfall Model Diagram

The design of the proposed system will include the physical arrangement of network devices and applications such as MySQL, Java, HTML5, Apache, and PHP to support the configuration of the system. The system will be deployed, tested, and assessed to check for performance vis-à-vis existing systems. The waterfall model is a classical model used in the system development life cycle to create a system with a linear and sequential approach. This model is divided into different phases and the output of one phase is used as the input of the next phase. Every phase has to be completed before the next phase starts, and there is no overlapping of the phases [21-24]. Waterfall methodology includes features such as requirements gathering and analysis, system design, implementation, integration, system testing, system development, and system maintenance.

Figure 3 shows the architectural view of the wired (fiber) and wireless web internet protocol surveillance systems.

3.3. Use Case Diagram

In modeling the proposed system, the use case diagrams are employed to describe the concept of developing the WWIPSS. The use case diagrams will show all stakeholders the various activities and roles they will play in the proposed system. The Figures below show examples of Use Case diagrams by the users of the proposed system. The Executive Director (Figure 4a), after successfully logging in to the WWIPSS, can update all users' credentials, watch live streaming videos via a Web browser on Mackintosh desktops and wireless smart televisions both in the office and at home, and will be able to select and download any video from the system locally. A branch manager (Figure 4b) will have the ability to watch streaming videos, update personal profiles, and download recorded videos after logging on to the web portal of the proposed system. However, in instances where credential details are forgotten, a branch manager is expected to contact the administrator for a user account update.

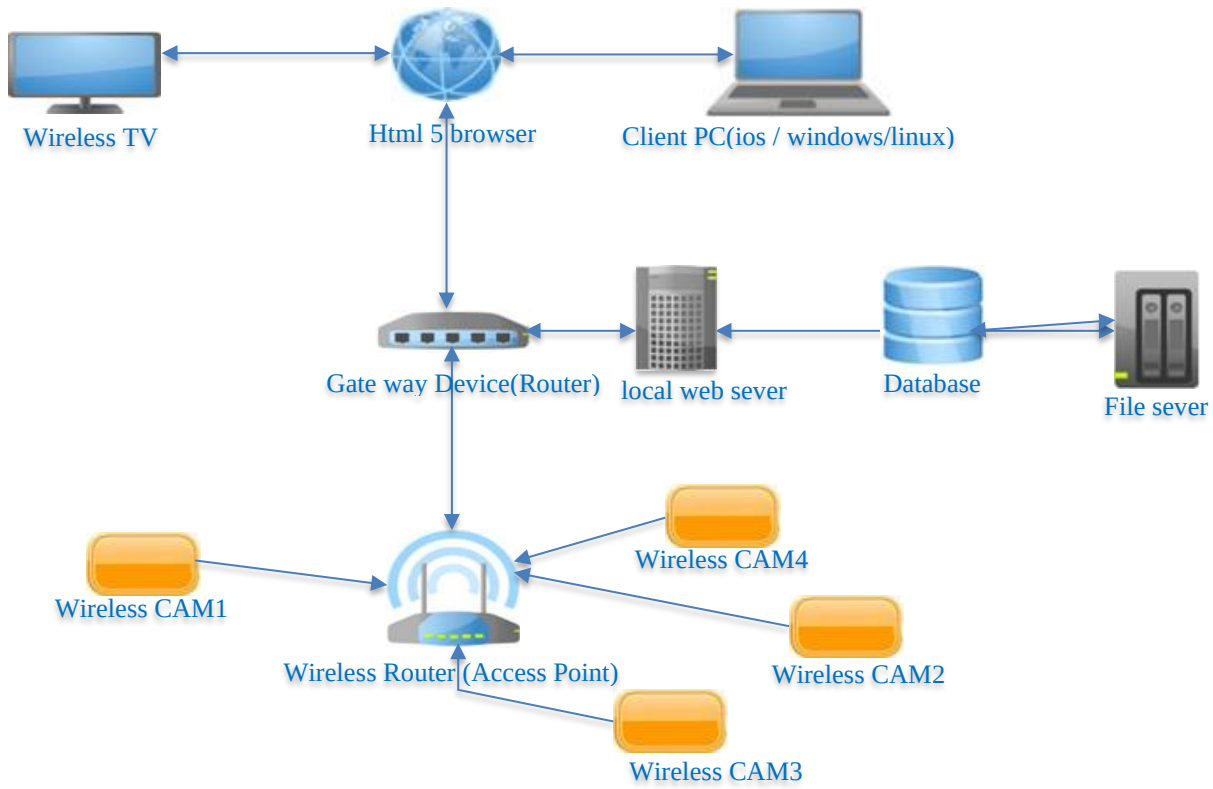

Fig. 3 Architectural view of WWIPSS

An administrator (Figure 4c) of the proposed system will perform the role of a systems and database manager. Firstly, the administrator will have the ability to create all user credentials locally at the backend server or update the database of the system by logging on to the portal online. Secondly, the administrator will perform other functions like creating backups and downloading reordered footage, etc.

Therefore, the administrator will be required to have an extended understanding of data management.A chief security officer has almost the same privileges as an administrator. This may include watching live streaming videos, updating personal profiles, downloading recorded videos, and creating backups after logging in to the Web portal of the proposed system. However, this user will be limited by not having the ability to create and update other user credentials.

3.4. Flowchart Diagram of the Proposed System

The diagram below illustrates the activities of the Executive Director, an advanced user who has an administrative privilege. Upon connecting to the WWIPSS web application administrator's interface, it is expected that the user logs in successfully with an authorized password.

Secondly, the user should be able to update all user passwords, watch live streaming, play, and download previously recorded videos. However, if the actor's password is incorrect, the system will not authorize a successful login.

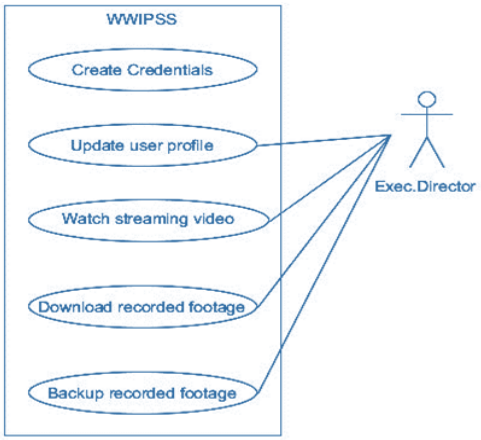

Fig. 4a Use case diagram for executive director

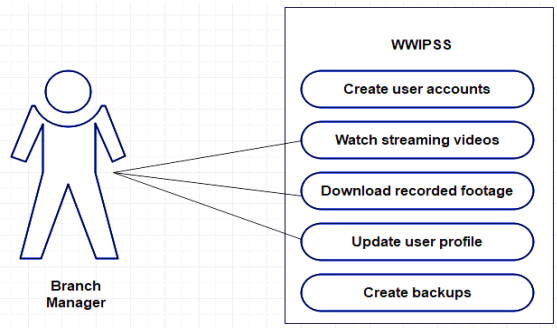

Fig. 4b Use case diagram for branch manager

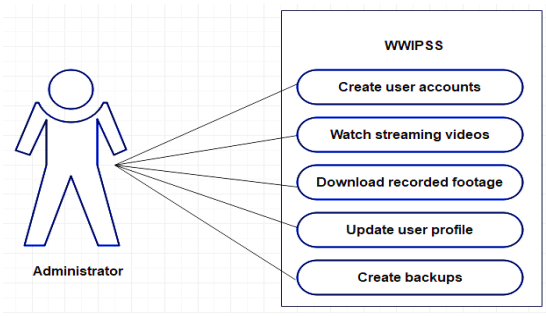

Fig. 4c Use case diagram for web administrator

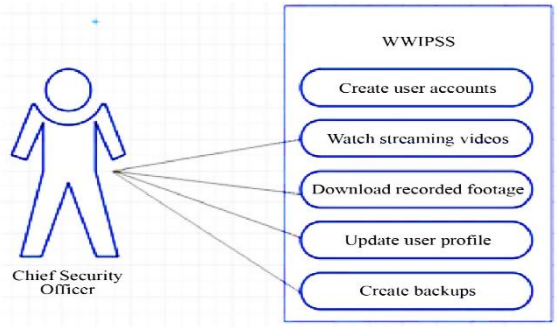

Fig. 4d Use case diagram for chief security

Figure 6 shows the activities of the Web Administrator. Upon connecting to the WWIPSS web administrator's interface, it is expected that the user logs in successfully with an authorized password. Also, the actor can update all user passwords, watch live streaming, play, and download previously recorded videos. However, if the user's password is incorrect, the system will not allow him or her to log in. Figure 7 above explains the activity of a branch manager and the chief security. Upon connecting to the WWIPSS web application user's interface, it is expected that the actor logs in successfully with an authorized password. Further, the user can update his or her passwords, watch live streaming and play and download previously recorded videos. However, if the actor's password is incorrect, the system will not allow him or her to log in. With network and system storage functions, users of the proposed system should be able to backup and restore data when there is a need to. This will aid recovery processes in times of system failures.

4. Implementation and Testing

4.1. Physical Networks Setup

There was a complete physical network setup for CAT 6 and Fiber optic cables [25]. Fiber optic splicing was performed to meet the required fiber length. During splicing, it was ensured that attenuation was minimal. The whole system powered after the setup was complete. Electrical signals from the camera via a PoE switch were transmitted to the media converter, which converted the electrical signals to light signals and transmitted them over the optical fiber cable to the other receiving end for reconversion back into electrical signals. All the network devices were configured to the standard TCP and UDP protocols. Also, the IP cameras were configured with static IP addresses as well as the local storage and backup devices to have recovery capabilities. An Uninterrupted Power Supply (UPS) was provided. The EZStation software was used for the surveillance system implementation because it provides a simple user interface for the management of the IP cameras, NVR, access control as well as security for real-time monitoring of users and administrators. The NVR also provided an interface to configure the IP addresses of the cameras, subnet masking, port usage, and gateway for transmission [26, 27].

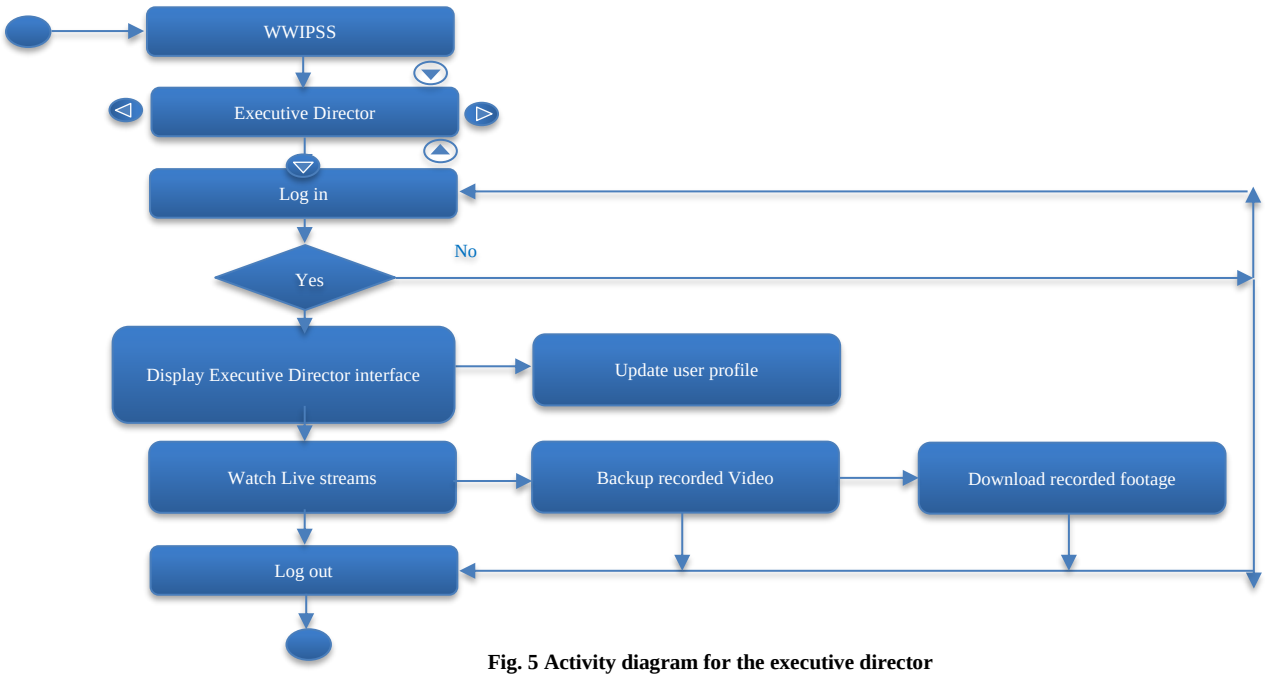

Fig. 5 Activity diagram for the executive director

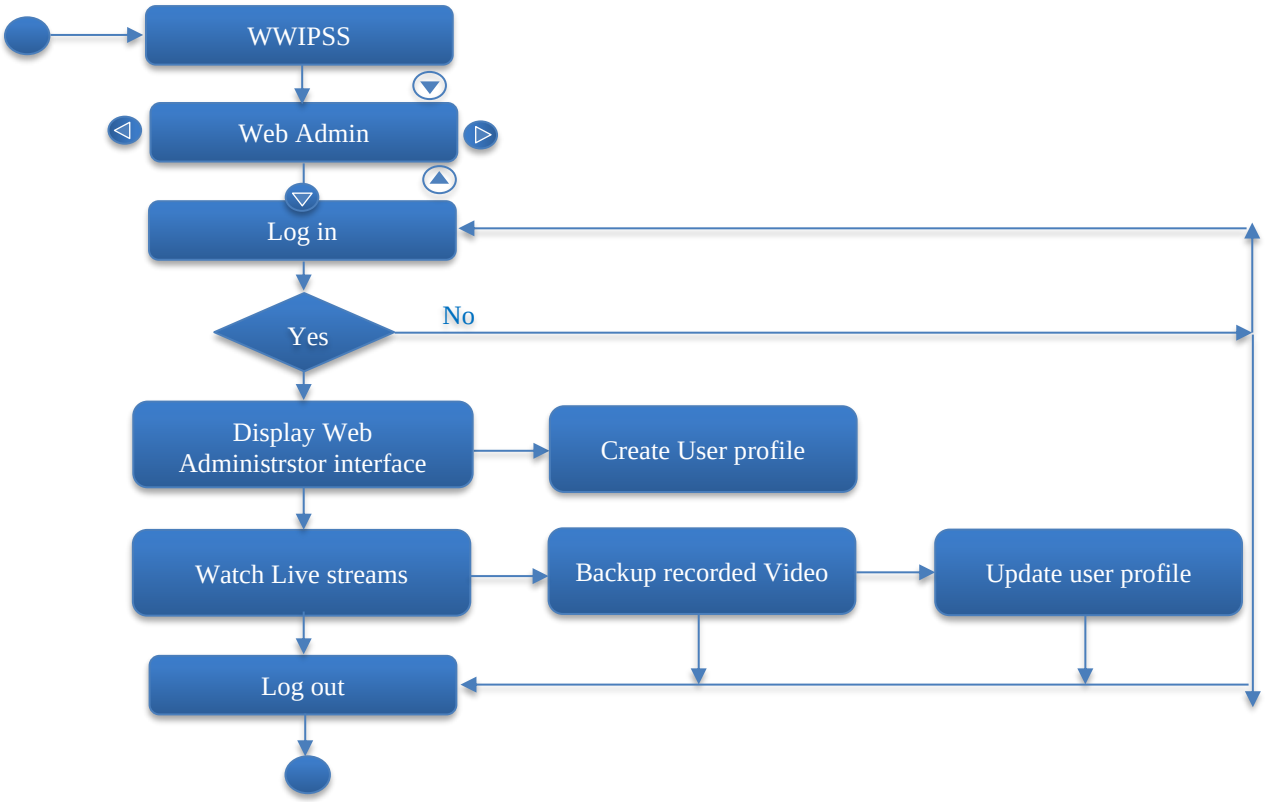

Fig. 6 Flow diagram for the Web Admin

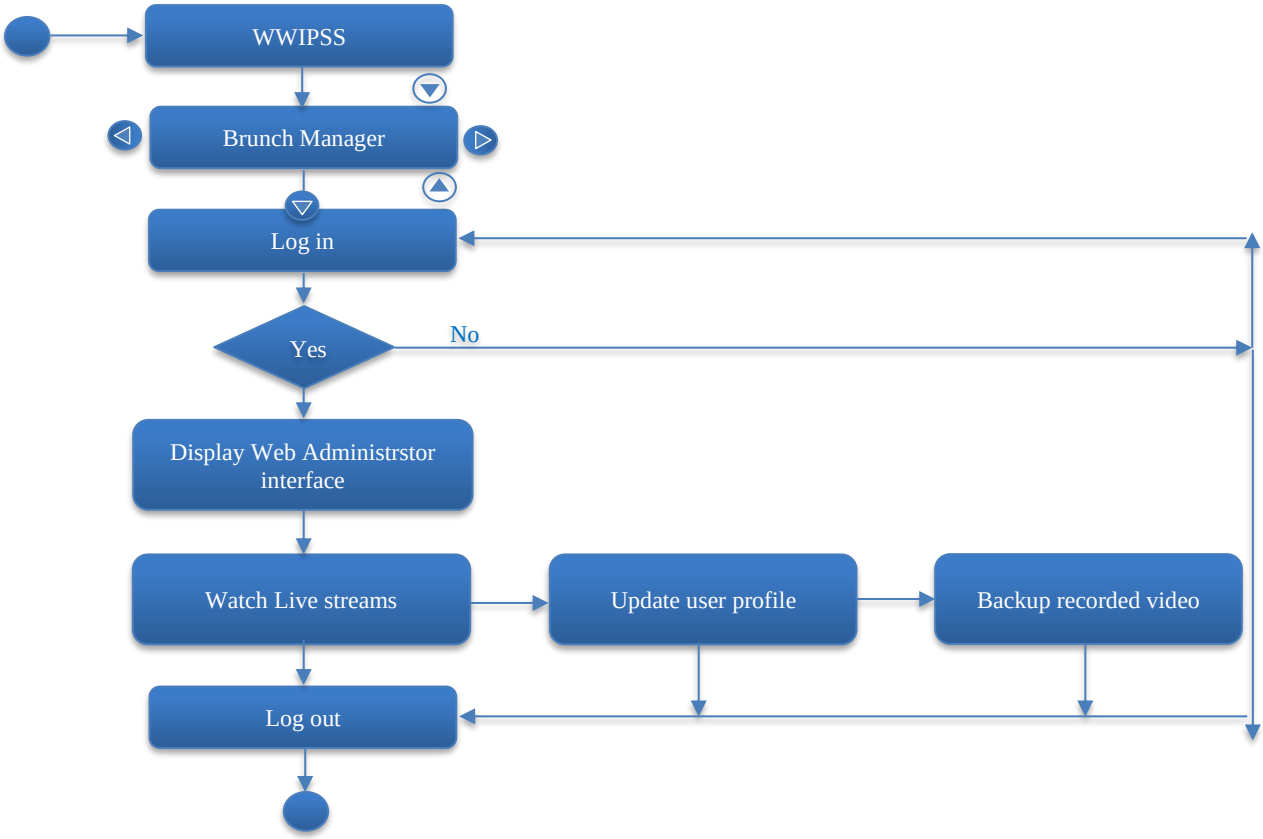

Fig. 7 Flow chart diagram for the branch manager and chief security

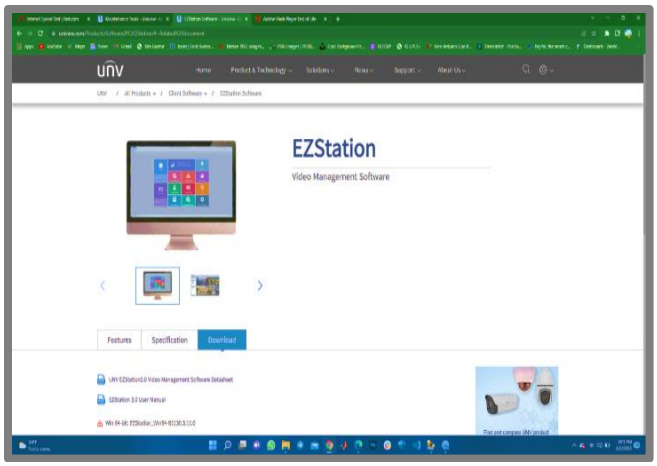

Fig. 8 Homepage of EZStation

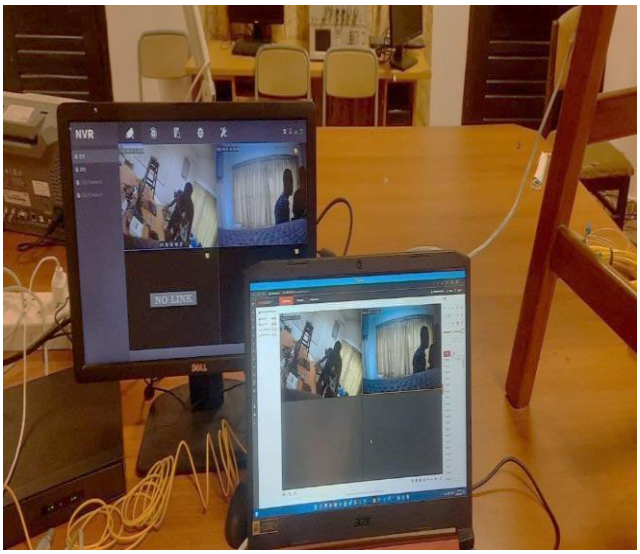

Fig. 9 Image of actual system implementation

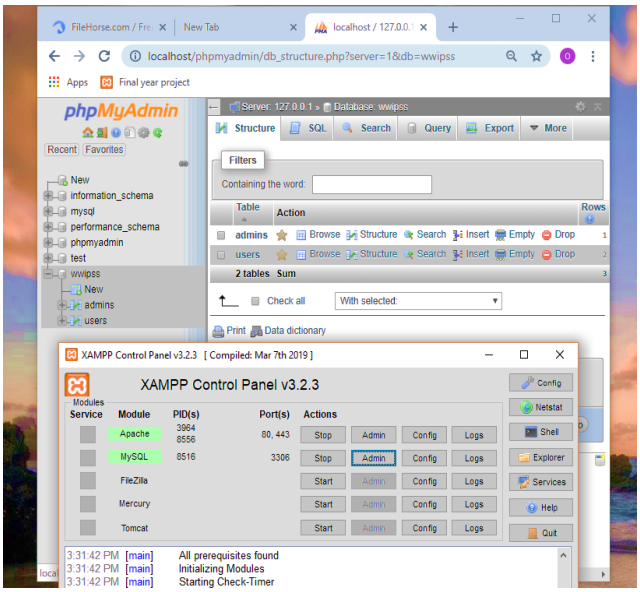

Fig. 10 Web and database server interface

4.2. Practical Results for CAT6 Implementation

Two cameras were used for the testing. The ping results in camera 1 had 0% data loss when four packets were sent. The approximate round trip times in milli-seconds for minimum, maximum, and average were 1 ms, 3 ms, and 1 ms, respectively, when four packets were sent over the IP address of 192.168.10.8 with 32 bytes of data. The ping results in camera 2 had 0% data loss when four packets were sent. The approximate round trip times in milli-seconds for minimum, maximum, and average were 0ms, 2ms, and 1ms, respectively, when four packets were sent over the IP address of 192.168.10.100 with 32 bytes of data. It was observed that there was an increase in transmission delay and packet loss as the distance increased in the case of the CAT 6 setup. Also, the transmission speed decreased gradually as the distance increased. These factors affected the quality of signals received.

4.3. Practical Results for Fiber and CAT6 Implementation

Two cameras were used for the testing. The ping results in camera 1 had 0% data loss when four packets were sent. The approximate round trip times in milli-seconds for minimum, maximum, and average were 1ms, 1ms, and 1 ms, respectively, when four packets were sent over the IP address of 192.168.10.8 with 32 bytes of data. The ping results in camera 2 had 0% data loss when four packets were sent. The approximate round trip times in milli-seconds for minimum, maximum, and average were 0ms, 1ms, and 0ms, respectively, when four packets were sent over the IP address of 192.168.10.100 with 32 bytes of data. It was observed that the transmission delay, packet loss, and transmission speed for the fiber and CAT 6 setup performed far better than as the distance increased. The quality of pictures and videos obtained from the Fiber and CAT 6 setup had a higher resolution as compared to that of only the CAT 6 setup.

4.4. Web and MySQL Database Server Installation

We installed my-php and Contra_Cam streaming server software. Consequently, any web administrator can access the local host system by using a local IP address or its Domain Name Service (DNS). Specific to this work, the local host was http://localhost/dashboard/ or http://127.0.0.0. To effectively manage the proposed Web application server, the Web and database administrators need to ensure that all application servers are installed, configured, and tested to meet the requirements of users. They must also cross-examine the responsiveness and effectiveness of these systems. Finally, administrators will need to change or update the system specification only when it is significant. The streaming server is used to capture, save, and share live videos for all IP cameras within the Web application. It is recommended that the network administrators check and install all internet protocol cameras, configure and test all connections to the wireless router devices, set up and install the streaming server, and connect and access the local host address of the streaming with the required credentials.

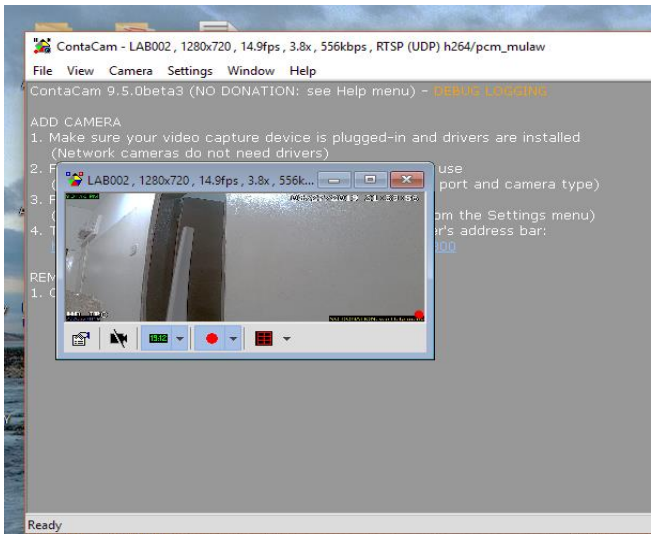

Fig. 11 The local host interface of the streaming server

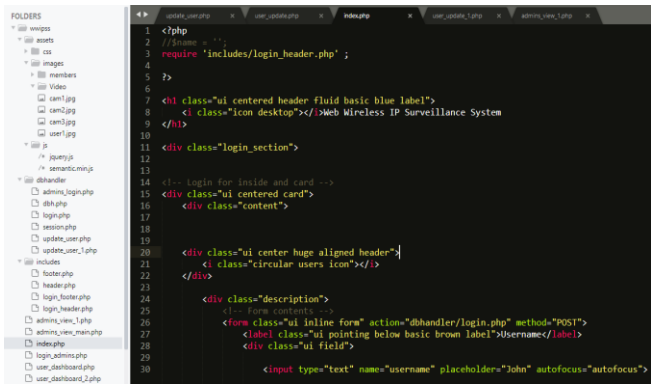

Fig. 12 Using a text editor to manage the WWIPS backend

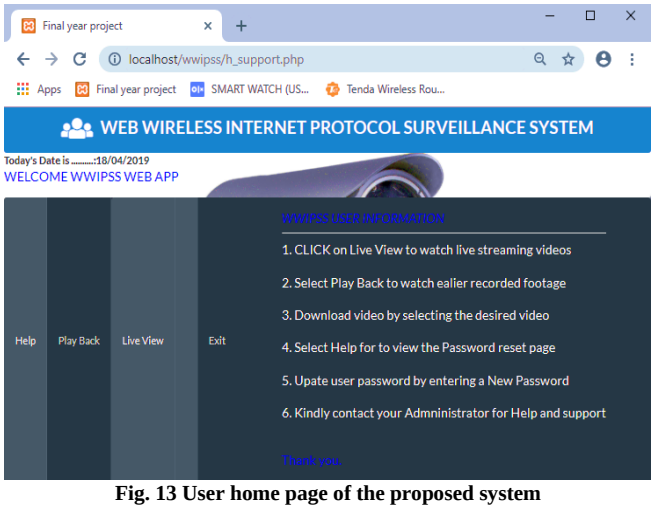

Fig. 13 User home page of the proposed system

4.5. Backend Server Managing and Scripting

In configuring the backend servers, a Web text editor was installed. This facilitated an effective process of managing the logical architecture of the Web application. To integrate the IP cameras into WWIPSS, the Web administrator will test connections to the streaming server by using an authorized login credential. Furthermore, the administrator shall create a hyperlink between the Web and the streaming server. This will contain the local host Internet protocol addresses of all cameras on the local area network (LAN). The user interface of WWIPSS Web applications will give authorized users the privilege of accessing and monitoring all Internet Protocol cameras (IPC) within a given local area network (LAN). Users shall connect the application by using the local host address or its domain name service (DNS) and their login credentials. A successful login will connect an authorized user to the WWIPPS home page where users can select activities such as Live View to watch live streaming video, Play Back to play previously recorded footage, "Help" to help view the user password update page, and "Exit" to log out.

The user live view page will connect actively authorized stakeholders to all IPCs within a selected LAN. WWIPSS applications shall provide Internet protocol camera customization. This implies that users will be involved in the implementation process. The playback page of the proposed system will give users the capability of watching earlier recorded footage from a secured area. This will include actions such as selecting a specific video with its date and time. Users will also have the opportunity to download selected footage. The administrator's page will grant advanced users the attribute of managing and maintaining the proposed surveillance application. It will include multimedia features such as playback, home, and live streaming activities. Administrators will be privileged to change all users' passwords. The link to the administrator's login page will be connected to the WWIPSS user login page where users with administrative credentials only may be authorized to login. The WWIPSS administrator home page will be used by all system administrators of the proposed application to effectively manage and monitor all live IPCs. A successful login will grant an authorized administrator the ability to change any user's password, watch live streaming video, and instantly playback or download selected footage.

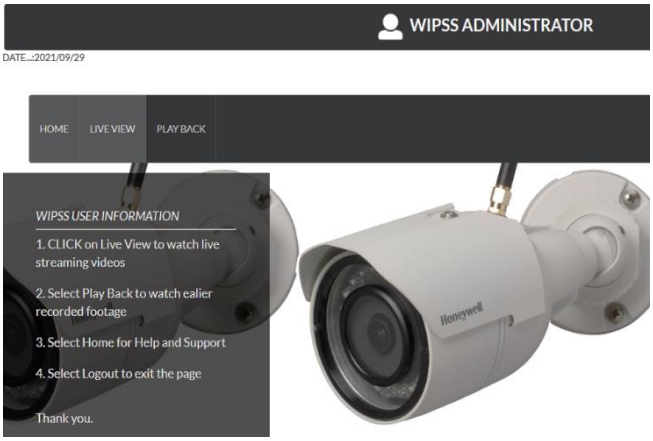

Fig. 14 WWIPSS administrator home page

Securing the system is very important. A biometric finger scanner was installed at the entrance of the server room. burglar alarms and smoke detectors were also included. These will help deter and monitor unwanted physical access. Passwords and passcodes of users and systems will be frequently changed to forestall intrusion. Likewise, backup storage devices and processes will be properly initiated and monitored. Firewall was installed to protect the WWIPS from threats and network attacks.

5. Conclusion

This research was conducted to improve the performance of the surveillance systems, bandwidth utilization, and link Internet protocol surveillance devices from different vendors. The implementation of the fiber as the backhaul helped to improve signal integrity due to its unlimited bandwidth, low latency, and reduced attenuation caused by twisted pair cables. Results from simulated and actual implementation showed that our system worked well in terms of bandwidth utilization, signal quality, and attenuation.

The average latency for the fiber optic setup was far better than the all CAT 6 setup. Signal quality was also better for the fiber optic setup. Also, a wireless Web Internet Protocol Surveillance System (WWIPSS) was developed that enabled the interoperability of devices from different vendors to communicate and share resources.

Fiber optic cables used help to increase the distance of the physical connection without any effect on the signal integrity. The fiber backhauls also provided better security than coaxial cables. The system met all the projected objectives and the project was holistically tested and implemented on the campus of the University of Ghana.

Funding Statement

This research was self-funded.

Acknowledgements

The authors are grateful to the BANGA Africa Project for editing the research.

References

[1] Kirstie Ball, "Workplace Surveillance: An Overview," *Labor History*, vol. 51, no. 1, pp. 87-106, 2010. [CrossRef] [Google Scholar] [Publisher Link]

[2] Milan Adameka, Michaela Barinova, and Tomas Havir, "Software for CCTV Systems Design," *MATEC Web Conference, 20th International Conference on Circuits, Systems, Communications and Computers (CSCC 2016)*, vol. 76, pp. 1-7, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[3] Mohamad Kashef, Anna Visvizi, and Orlando Troisi, "Smart City as a Smart Service System: Human-Computer Interaction and Smart City Surveillance Systems," *Computer in Human Behaviour*, vol. 124, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[4] Gurlove Singh, and Amit Kumar Goel, "Face Detection and Recognition System Using Digital Image Processing," *2020 2nd International Conference on Innovative Mechanisms for Industry Applications*, Bangalore, India, pp. 348-352, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[5] N. Boonma et al., "Image Recorder Server with IP Camera and Pocket PC," *2nd International Science, Social-Science, Engineering and Energy Conference 2010:Engineering Science and Management, Procedia Engineering*, vol. 8, pp. 182-185, 2011. [CrossRef] [Google Scholar] [Publisher Link]

[6] Mohammad Mehedi Hassan, M. Anwar Hossain, and Muhammad Al-Qurishi, "Cloud-Based Mobile IPTV Terminal for Video Surveillance," *16th International Conference on Advanced Communication Technology*, Pyeongchang, Korea (South), pp. 876-880, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[7] Moon Sun Shin et al., "Design and Implementation of IoT-Based Intelligent Surveillance Robot," *Studies in Informatics and Control*, vol. 25, no. 4, pp. 421-432, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[8] Bojie Sheng et al., "Partial Discharge Pulse Propagation in Power Cable and Partial Discharge Monitoring System," *IEEE Transactions on Dielectrics and Electrical Insulation*, vol. 21, no. 3, pp. 948-956, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[9] Wen-Tsuen Chen et al., "Design and Implementation of a Real Time Video Surveillance System with Wireless Sensor Networks," *VTC Spring 2008 - IEEE Vehicular Technology Conference*, Marina Bay, Singapore, pp. 218-222, 2008. [CrossRef] [Google Scholar] [Publisher Link]

[10] J. Logeshwaran et al., "The Role of Integrated Structured Cabling System (ISCS) for Reliable Bandwidth Optimization in High Speed Communication Network," *ICTACT Journal on Communication Technology*, vol. 13, no. 1, pp. 2635-2639, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[11] Hongwei Wang, F. Richard Yu, and Hailin Jiang, "Modeling of Radio Channels With Leaky Coaxial Cable for LTE-M Based CBTC Systems," *IEEE Communications Letters*, vol. 20, no. 5, pp. 1038-1041, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[12] Madhusmita Sahu, and Rasmita Dash, "Study on Face Recognition Techniques," *2020 International Conference on Communication and Signal Processing*, Chennai, India, pp. 0613-0616, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[13] Zeliang Liu et al., "Study on the Anti-Theft Technology of Museum Cultural Relics Based on Internet of Things," *IEEE Access*, vol. 7, pp. 111387-111395, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[14] Jayendra Kumar et al., "Real-Time Monitoring Security System Integrated with Raspberry Pi and E-Mail Communication Link," *2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, Noida, India, pp. 79-84, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[15] Chia-Hsu Kuo, and Huan-Ming Hsu, "Image-Based Intelligent Surveillance System with the Robust Universal Middleware Bridge Service," *Life Science Journal*, vol. 12, no. 7, pp. 76-87, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[16] Ali Tekeoglu, and Ali Şaman Tosun, "An Experimental Framework for Investigating Security and Privacy of IoT Devices," *2016 First International Conference: Intelligent, Secure, and Dependable Systems in Distributed and Cloud Environments*, Vancouver, BC, Canada, pp 63-83, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[17] Zhonghong Xu, Lingjun Yang, and Sanxing Cao, "Design and Implementation of Mobile Lightweight TV Media System Based on Android," *2016 7th IEEE International Conference on Software Engineering and Service Science*, Beijing, China, pp. 730-733, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[18] Zhaohua Zheng, Jieren Cheng, and Jinlian Peng, "Design and Implementation of Teaching System for Mobile Cross-Platform," *International Journal of Multimedia and Ubiquitous Engineering*, vol. 10, no. 2, pp. 287-296, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[19] Serena Pastore, "The Platform as a Service (PaaS) Cloud Model: Opportunity or Complexity for a Web Developer?," *International Journal of Computer Applications*, vol. 81, no. 18, pp. 29-37, 2013. [Google Scholar] [Publisher Link]

[20] Junchan Li et al., "Pattern Recognition for Distributed Optical Fiber Vibration Sensing: A Review," *IEEE Sensors Journal*, vol. 21, no. 10, pp. 11983-11998, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[21] Henoch Juli Christanto, and Yerik Afrianto Singgalen, "Analysis and Design of Student Guidance Information System through Software Development Life Cycle (SDLC) and Waterfall Model," *Journal of Information Systems and Informatics*, vol. 5, no. 1, pp. 259-270, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[22] Nur Hidayati, and Sismadi, "Application of Waterfall Model In Development of Work Training Acceptance System," *INTENSIF: Jurnal Ilmiah Penelitian Dan Penerapan Teknologi Sistem Informasi*, vol. 4, no. 1, pp. 75-89, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[23] Shravan Pargaonkar, "A Comprehensive Research Analysis of Software Development Life Cycle (SDLC) Agile & Waterfall Model Advantages, Disadvantages, and Application Suitability in Software Quality Engineering," *International Journal of Scientific and Research Publications*, vol. 13, no. 8, pp. 120-124, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[24] C. Fagarasan et al., "Agile, Waterfall and Iterative Approach in Information Technology Projects," *IOP Conference Series: Materials Science and Engineering*, vol. 1169, pp. 1-10, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[25] Juliano Pimentel, and Jawad Arif, "Communication Network Optimization for Subsea Processing Fields Development," *2019 Petroleum and Chemical Industry Conference Europe (PCIC EUROPE)*, Paris, France, pp. 1-8, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[26] V.A. Akpan, R.A.O. Osakwe, and S.A. Ekong, "Configuration, Interfacing and Networking of Wireless IP-Based Camera for Real-Time Security Surveillance Systems Design," *African Journal of Computing & ICT*, vol. 8, no. 2, pp. 107-114, 2015. [Google Scholar]

[27] Xinzhuo Li et al., "Design Optimization of Substation Video Monitoring Based on Transparent Transmission Principle," *2023 IEEE International Conference on Control, Electronics and Computer Technology*, Jilin, China, pp. 1450-1455, 2023. [CrossRef] [Google Scholar] [Publisher Link]