A BLUEPRINT TO SECURING DELTA STATE UNIVERSITY ELECTRONICALLY IN THE CURRENT WAVE OF INSECURITY IN NIGERIA (OLEH CAMPUS AS A TEST BED)

Ufuoma Kazeem Okpeki[1], Efenedo Gabriel Ilori[2] , Oyubu Akpovi Oyubu[3]
[1,2,3,]Department of Electrical and Electronic Engineering, Delta State University Abraka, OlehCampus, Nigeria.

***Abstract*- Delta State University, Oleh Campus, like many tertiary institutions in Nigeria, faces security challenges including theft of equipment, vandalism, intrusion into restricted areas, and limited real-time monitoring capabilities. The Oleh Campus, relies on its key physical assets such as the generator houses in the Faculty of Engineering and the Faculty of Law, the e-library as well as the Provost's Office, to maintain academic functions, These assets are particularly important. This research, therefore, developed and implemented a Wireless Digital Surveillance Security System (WDSSS) to secure crucial assets of the University Oleh campus main assets electronically. The project utilized several materials, categorized into hardware components and software; the various hardware components were integrated to achieve the overall system functionality. On the hardware side, the following components were used, one 14 inches HP Laptop, four 1080p HD wireless IP cameras, with infrared night vision (up to 30m) with built in Wi-Fi connectivity capabilities, IP66 weatherproof rating, wide-angle lens (2.8 mm), onboard motion detection and solar powered. One dual-band Wi-Fi router (2.4 GHz/ 5GHz), one Techno smart phone, 4 – channel wireless network video recorder, four fabricated iron poles and bolts/nuts. The web-based application was implemented using MySQL (MY Structured Query Language). Html (Hypertext Markup Language, CSS (Cascading Style Sheet) and jQuery were used to design the web-user interface, PHP (Hypertext Preprocessor) was used as the server-side script language to link the interface and the database of the central control center. The system was designed, implemented and tested. The system worked perfectly in line with its designed specifications.**

***Keywords:* Security system, interfacing, modular, remote terminals**

I. INTRODUCTION

With the current wave of insecurity brewing across our nation Nigeria, abductions, communal crisis, herders and farmers crashes, arm resistances, vandalism and stealing. There is a clarion call for every State Government, heads of parastatals, establishments and institutions to take proactive measures to secure or protect her immediate environments against kidnapping and vandalism of key assets, staff and students

The sovereignty of a nation may be determined by their capacity to safeguard citizens and her resources against any attack, be it from within or outside the state territory. Therefore, security is the ability of state security mechanisms, which involves state and non-state actors to prevent or manage anxiety, uncertainty and harm that has the capacity to distort serenity and development (Abdulkarian & Saidatu-Lakmal, 2022). Challenges post by insecurity in Nigeria has assumed a formidable dimension that now requires multistate holders approach, at all levels of governance, parastatals, establishments and institutions. Security is a major concern in higher institutions due to increasing cases of theft, vandalism, unauthorized access, and destruction of valuable assets. Universities possess critical infrastructure such as administrative buildings, ICT centers, examination offices, libraries, laboratories, hostels, and power facilities that require constant monitoring.

Delta State University, Oleh Campus, like many tertiary institutions in Nigeria, faces security challenges including theft of equipment, vandalism, intrusion into restricted areas, and limited real-time monitoring capability (Esther Garge, 2015; Kumar & Singh, 2018).

The Oleh Campus, relies on its key physical assets such as the generator houses in the Faculty of Engineering and the Faculty of Law, the e-library as well as the Provost's Office, to maintain academic functions, These assets are particularly important, as the generator houses provide backup electricity to faculty buildings that cannot afford interruptions due to the frequent outages in Nigeria's power supply, while the Provost's Office contains important governance records and administrative systems essential for the daily operations of Oleh Campus. However, the traditional security measures currently utilized at these sites such as, perimeter barriers and the manual patrols have proven insufficient as a complete protection solution. Human surveillance is limited due to its restricted coverage, the potential for fatigue, and the inability to continuously and reliably document access events across various isolated areas simultaneously results to security breaches at these facilities and this reduces the chances for prompt action and accountability.

The rise of Internet Protocol (IP) camera technology offers universities around the globe a practical, scalable, and cost-effective way to address these security vulnerabilities (Akinola & Adeyemi, 2021). . An IP camera is a digital device that connects to a network to capture, encode, and transmit video data, allowing authorized individuals to access live footage in real time from any connected device, (Okae et al., 2024; Zhang et al., 2020). This research, therefore, developed and implemented a Wireless Digital Surveillance Security System (WDSSS) to secure crucial assets of the University Oleh campus main assets electronically. The project utilized several materials, categorized into hardware components and software; the various hardware components were integrated to achieve the overall system functionality. On the hardware side, the following components were used, one 14 inches HP Laptop, four 1080p HD wireless IP cameras, with infrared night vision (up to 30m) with built in Wi-Fi connectivity capabilities, IP66 weatherproof rating, wide-angle lens (2.8 mm), onboard motion detection and solar powered. One dual-band Wi-Fi router (2.4 GHz/ 5GHz), one Techno smart phone, 4 – channel wireless network video recorder, four fabricated iron poles and bolts/nuts. The web-based application was implemented using MySQL (MY Structured Query Language). Html (Hypertext Markup Language, CSS (Cascading Style Sheet) and jQuery were used to design the web-user interface, PHP (Hypertext Preprocessor) was used as the server-side script language to link the interface and the database of the central control center. The system was designed, implemented and tested. The system worked perfectly in line with its designed specifications.

II. REVIEW OF PAST WORKS

The need for securing organizations, institutions, homes and properties has been a concern since prehistoric times when early humans sought to protect themselves and their belongings from external threats. The Internet of Things (IoT) has become an engine room for several technologies, as a result, it is possible to connect smart physical devices and enable smart decision making across wide range of applications. **Sarika and Mena (2022),** investigated the framework of ICT in providing security in our environments. Their findings showed that the IoT network environment can provide various ranges of security on the communities.

The intelligent community security system (ICSS) is becoming one of the biggest applications of the IoT. The purposes of the ICSS are proportion of invasion, automatic property management, real-time environment surveillance and quick response to accidents. **Jihong and Yang, (2011),** described the basic characteristic and architecture of the IoT and introduced an intelligent model to realize a practical and intelligent community management system. Their findings showed that the system can improve the community security automatically. With monitoring, measurements, data collection and analysis, the IoT benefits environmental sustainability such as resource management, energy efficiency and security government, **Yu-Yang et al (2022**) established IoT infrastructure for environmental monitoring, that provide information for improving life quality, and to prevent natural disaster. Their findings showed that the data collected from different sensor areas analyzed and applied in practice can smartly conveniently increase environmental sustainability, social security and economy efficiency.

Egbe (2025) developed and optimized a real-time campus security surveillance system using Arduino and CCTV, claiming that intrusion detection and real-time alerts can be enhanced with embedded monitoring and automation. The study implemented a scalable concept where sensors and embedded control support surveillance operations, aiming to improve detection and response in critical areas. The reported outcome emphasized improved monitoring capability and real-time alerting compared with passive CCTV setups. The main gap is that Arduino-based architectures may face limitations in large scale video analytics, false alarm control, and integration with professional VMS/NVR platforms, and the study provides limited discussion on network design, storage retention, and long-term maintainability typical in real university infrastructures.

Sharma et al., 2025), They used Deep learning to transforms traditional CCTV into proactive, intelligent surveillance. Systematic review synthesizing four decades of empirical evidence on CCTV and AI technologies. Deep learning boosts detection quality but raises ethical/privacy issues requiring governance frameworks. High level review lacked practical architecture and implementation case studies.

Ehiagwina et al. (2024), detailed the development of a reliable and secure wireless CCTV camera network for the main administration building at Federal Polytechnic Offa, Nigeria, published in the Engineering and Technology Journal. Their system interconnected multiple wireless IP cameras via vendor software to a 16-channel monitor that displayed feeds from eight well-chosen locations. This study is geographically and contextually aligned with the current project, providing robust support for the proposed implementation at DELSU and
affirmed its technical feasibility within Nigerian institutions.

Cob-Parro et al. (2021) presented a smart video surveillance system using edge computing to detect, count, and track people in real time using embedded hardware and computer vision.

Their approach combined a designed embedded architecture with real-time detection and tracking algorithms, demonstrating that meaningful analytics can run on edge-class hardware for surveillance tasks. The results highlight that edge devices can support real-time monitoring functions without requiring heavy centralized computing. The key limitation for "securing key assets" is that people counting/tracking alone may not directly capture asset-specific threat scenarios (e.g., unauthorized access into restricted labs, tampering with electrical infrastructure), and a campus solution still needs policy-based zone rules, alert prioritization, evidence export procedures, and cyber security controls.

Akpan etal, (2015), presented techniques for configuring, interfacing, and networking wireless IP cameras for real-time security surveillance, proposing three implementation routes: vendor software access, web-browser access, and MATLAB/Simulink access. Their methodology compared practical access and interfacing options for IP cameras and demonstrated that real-time monitoring can be achieved through multiple integration approaches.

Cusack and Tian (2017) looked into the cybersecurity risks associated with current IP surveillance systems at the 15th Australian Information Security Management Conference. They employed various attack methods to examine a representative commercial IP camera and DVR system. Their findings highlighted that the continued use of default manufacturer credentials a common error in real-world settings led to unauthorized access without requiring advanced skills, with 70% of authentication tests resulting in valid credentials. This research serves as a crucial foundation for the cybersecurity strategy of the proposed DELSU system, emphasizing the necessity for mandatory credential changes prior to deployment.

Sultana and Wahid (2019), proposed IoT-Guard, a fog-based video surveillance system for real-time security management, published in IEEE Access. Their design introduced fog computing nodes to reduce bandwidth needs for continuous high-resolution video streaming, allowing real-time alerts while minimizing data transmission.

Bose et al. (2023), they designed and tested an IoT-based smart IP camera system aimed at monitoring examination halls in an institutional setting, detailed in Springer's Advances in Intelligent Systems and Computing series. Their system utilized IP cameras linked through a dedicated cloud service for real-time remote surveillance accessible via web browsers and smart phones, with video recording stored in the cloud at 30–35 frames per second. This project demonstrated that comprehensive monitoring solutions could be implemented in institutions using simultaneous mobile and web access, affirming the core functional needs of the proposed system.

III. MATERIALS AND METHOD

The framework design and implementation of the Wireless Digital Surveillance Security System (WDSS) based on the IoT technology. The project utilized several materials, categorized into hardware components and software; the various hardware components were integrated to achieve the overall system functionality. On the hardware side, the following components were used, one 14 inches HP Laptop, four 1080p HD wireless IP cameras, with infrared night vision (up to 30m) with built in Wi-Fi connectivity capabilities, IP66 weatherproof rating, wide-angle lens (2.8 mm), onboard motion detection and solar powered. One dual-band Wi-Fi router (2.4 GHz/ 5GHz), one Techno smart phone, 4 – channel wireless network video recorder, four fabricated iron poles and bolts/nuts.

The web-based application was implemented using MySQL (MY Structured Query Language). Html (Hypertext Markup Language, CSS (Cascading Style Sheet) and jQuery were used to design the web-user interface, PHP (Hypertext Preprocessor) was used as the server-side script language to link the interface and the database of the central control center.

In view of the security concerns at Delta State University Oleh Campus that this research tend to resolve, it is desirable that an effective digital surveillance mechanism be put in place to provide a real-time monitoring that will mitigate any attempt by criminals to vandalize the university properties in this key areas that are vulnerable to theft and vandalism due to their isolated locations (1) The Provost office, (2) Engineering faculty workshop, (3) E-Library building, (4) Generator house.

A. System Architecture and Implementation

The designed system adopts a wireless star topology in which all four IP cameras are connected to a central Wi-Fi router, which feeds its encoded video stream to the Network video recorder (NVR). The NVR then outputs to the Center Information Processing System (CIPS) with IoT capabilities, in the security control room. The software section entails the software design and implementation to create a more intuitive Web-based dashboard using the capabilities of the IoT platform for effective monitoring. The four solar powered IP cameras were mounted on fabricated iron poles and strategically placed in the designated areas to be protected in the campus. All other components were properly connected and integrated in the network infrastructure. The NVR will continuously record all streams and make them accessible for remote viewing through the mobile app over the internet. Users accounts were created for security personnel and administrators with specific access rights assigned based on job responsibilities to log into the app and access live and recorded video streams. A block diagram illustrating the connections between these components is provided in Figure 1 and Figure 2, the system Architecture

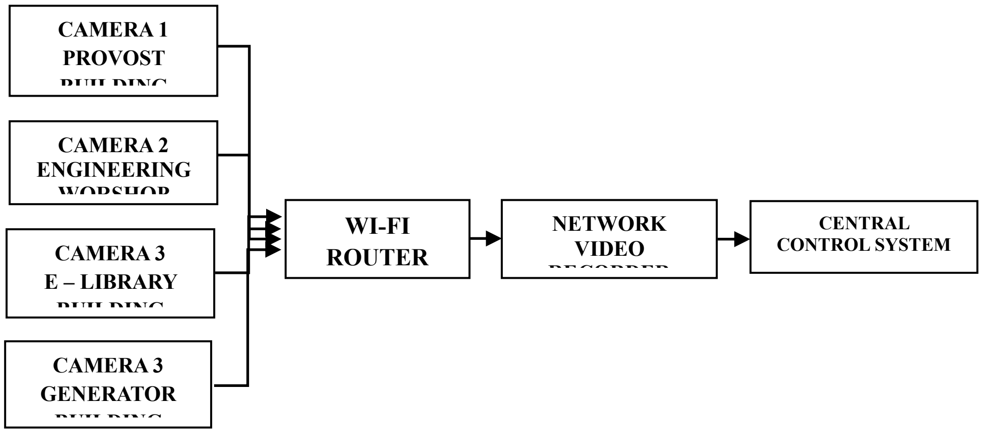

Figure 1 Block diagram of a Wireless digital surveillance security system

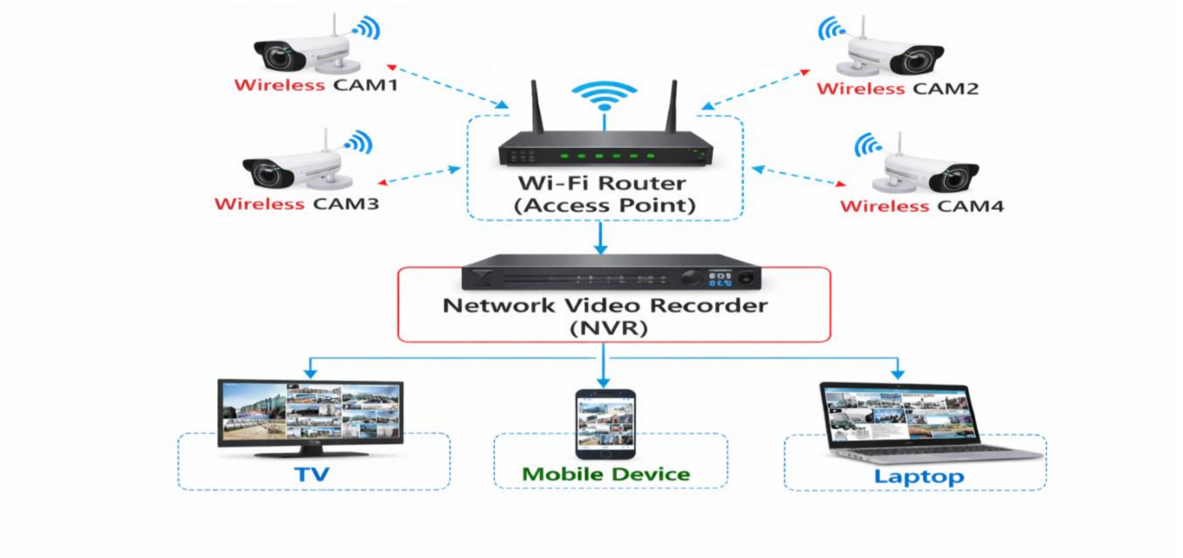

Figure 2: System Architecture

B. *Remote Access Integration for Authorized Personnel*

A mobile monitoring application compatible with the NVR brand, such as gDMSS Plus or Hik-Connect was installed in smart phones of authorized security personnel and a university top management staff. This enables live viewing and playback from any location with an internet connection, using password-protected accounts. Only designated personnel are granted access credentials, ensuring that remote monitoring capability does not become a security liability.

C. *Administrator:*

An administrator of the wireless digital surveillance security system will serve as 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 in to the portal online. Secondly, the administrator will perform other functions like creating backups and downloading reordered footage, or reviewing recorded videos.

The administrator should be a person with extended understanding of the computer and data management. A chief security officer has almost the same privileges as an administrator. However, he will be limited by not having the ability to create and update other user credentials or accounts.

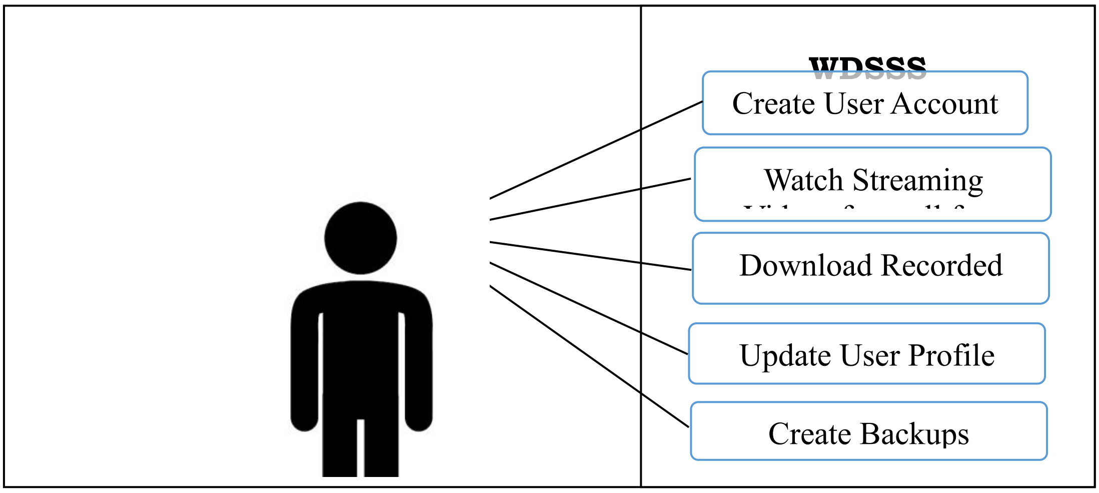

Figure 3: A use case diagram for web administrator

D. Flowchart Diagram of the System

The diagram below illustrates the activities of the Administrator, an advanced user who has an administrative privilege.

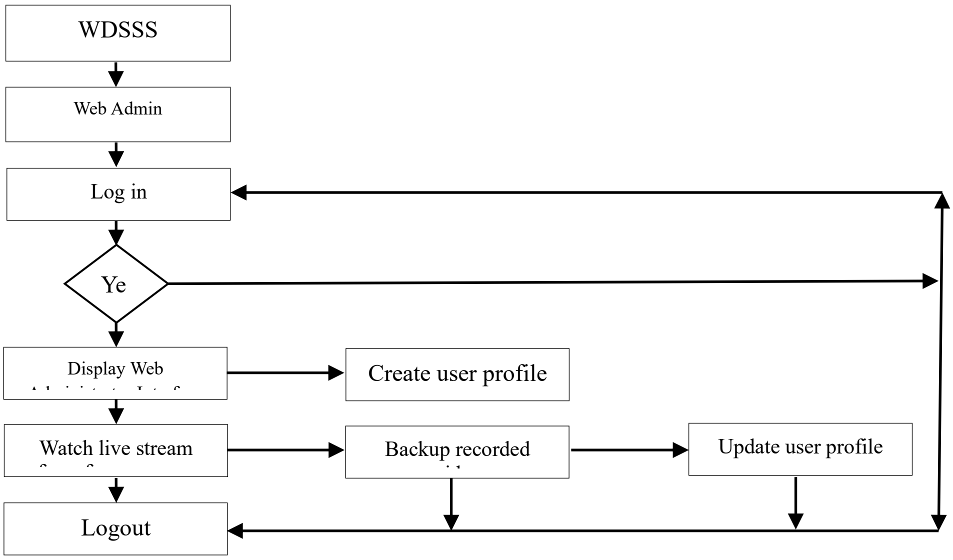

Figure 4: flow chart diagram

Figure 3 shows the activities of the Web Administrator. Upon connecting to the WDSSS web administrator's interface, it is expected that the user logs in successfully with an authorized password. Also, he 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.

E. Chief Security Officer Use Case Scenario

A chief security officer has almost the same privileges as an administrator. However, he will be limited by not having the ability to create and update other user credentials or accounts. The use case scenario is given in Figure 5

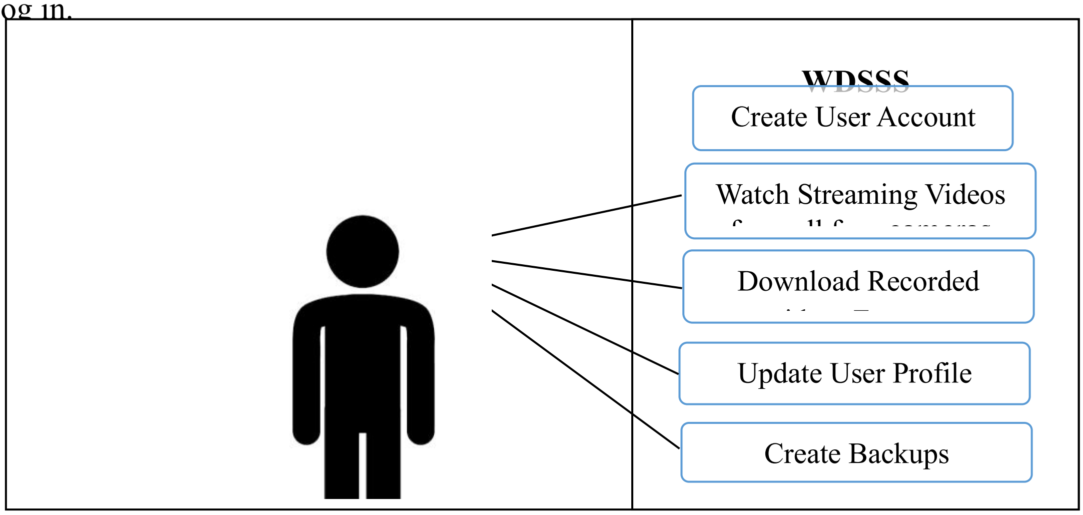

Figure 5: A use case scenario

F. Chief Security Activities Flowchart

Figure 5 above explains the activity of the chief security. Upon connecting to the WDSSS 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 his 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

Flowchart Diagram for Chief Security Officer

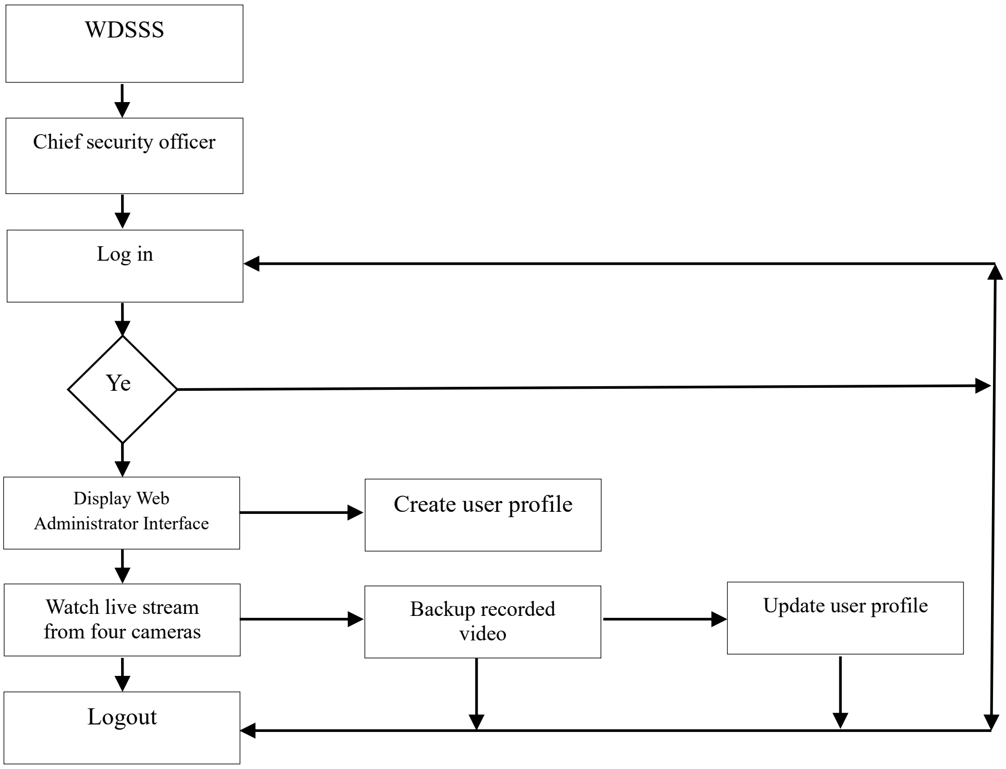

Figure 6: flowchart for chief security officer

G. *The Benefits of the Wireless Digital Surveillance Security System*

The primary objectives of the digital surveillance security system are stated as follows;

1. Proactive incident detection and response
2. Enhancing security for the university staff, student and assets
3. Data management – reviews of recorded video over time will equipped the chief security officer for proper prosecution of offenders in courts.

IV. .RESULTS AND DISCUSSIONS

Upon completing the physical network setup and the system powered. 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 EZ Station 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. On completion of the system installations, devices configuration and integrations, the system was thoroughly tested and evaluated on the following performance criteria.

• **Video Quality:** Footage from each camera were reviewed in the days and at nights for a period of two to five days to confirm that images are sharp enough to identify individuals and detect incidents clearly.

Shown in figure 7 is footage from the four IP cameras.

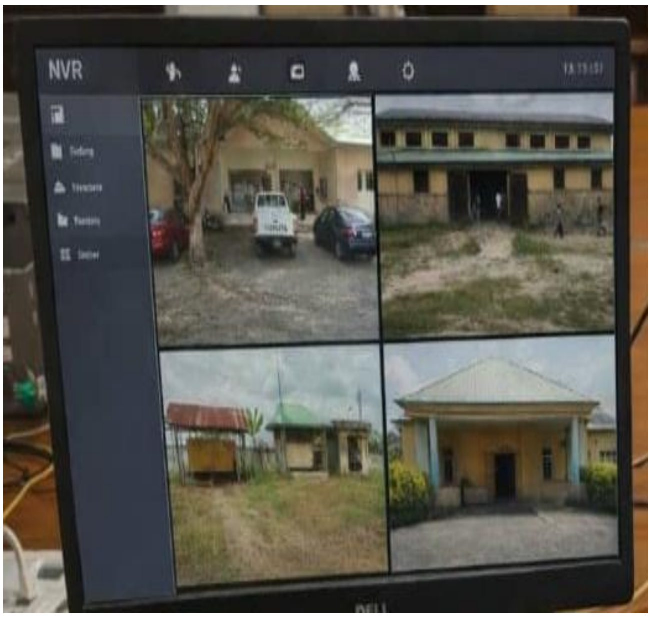

Figure 7: live footage from the four cameras

• **Wireless Stability:** Signal strength at each camera locations were measured and the video streams monitored over several days to check for drops or interruptions in transmission.

• **Recording Reliability:** The NVR were observed over an extended period to confirm continuous, uninterrupted recording with no data loss or storage errors.

• **Motion Detection Accuracy**: Controlled tests were conducted to verify that motion alerts are triggered correctly, and settings adjusted to minimize false alarms caused by environmental factors.

• **Remote Access Performance**: The mobile app was tested on both Wi-Fi and mobile data to evaluate the quality and responsiveness of the live stream outside the campus network.

• **Power Backup:** The mains power was switched off to confirm that the UPS keeps the system running for the required minimum of two hours without any loss of recording.

The developed wireless digital surveillance security system (WDSSS) performed excellently in line with the designed specifications in all the performance criteria's.

V. CONCLUSION

This Wireless Digital Surveillance Security System is developed and implemented to secure Delta State University, Oleh Campus key assets against theft and vandalism, Also to give staff sense of protections. The system was holistically tested and implemented in the campus of the University Oleh..

Funding Statement

The research was funded by Tertiary Education Trust Fund (TETfund) of Nigeria.

Acknowledgement

The authors are grateful to Delta State University and TETfund of Nigeria for funding this research.

REFERENCES

1. Abdulkarin and Saidatulakmal, (2022), "Growth and Fiscal Effects of Insecurity on the Nigerian Economy. The European Journal of Development Research. Vol. 35, Pg. 743-76
2. Akinola,O S. & Adeyemi, A. A. (2021). Design and implementation of a real-time video surveillance system for security applications. International Journal of Engineering Research and Technology, 10(3), 45–52.
3. Akpan, V. A., Osakwe, R. A. O., & Ekong, S. A. (2015). Configuration, interfacing, and networking of wireless IP-based camera for real-time security surveillance systems design. African Journal of Computing & ICT, 8(2), 107–114.
4. Bose, S., Ghosh, S., Dhang, S., Karmakar, R., Dey, P., & Acharyya, A. (2023). IoT-based smart Internet Protocol camera for examination monitoring. In S. Bhattacharyya, G. Das, S. De, & L. Mrsic (Eds.), Recent Trends in Intelligence Enabled Research: Proceedings of DoSIER 2022. Advances in Intelligent Systems and Computing (Vol. 1446). Springer. https://doi.org/10.1007/978-981-99-1472-2_21
5. Cusack, B., & Tian, Z. (2017). Evaluated IP surveillance camera vulnerabilities. In C. Valli (Ed.), Proceedings of the 15th Australian Information Security Management Conference (pp. 25–32). Edith Cowan University. https://ro.ecu.edu.au/ism/202/

6. Cob-Parro, A. C., Losada-Gutiérrez, C., Marrón-Romera, M., Gardel-Vicente, A., & Bravo-Muñoz, I. (2021). Smart Video Surveillance System Based on Edge Computing. Sensors, 21(9), 2958. https://doi.org/10.3390/s21092958

7. David Egbe, O. ., Fraser Anwaitu (Ph.D), E. ., & Memoye Kepeghom (Ph.D), O. . (2025). Development And Optimization Of A Real-Time Campus Security Surveillance System Using Arduino And Cctv Camera. BW Academic Journal. Retrieved from https://bwjournal.org/index.php/bsjournal/article/view/2569

8. Ehiagwina, F. O., Kadiri, K. O., Yekeen, S. A., Azanubi, J. O., & Mustapha, K.O. (2024). Design and implementation of a reliable and secure wireless CCTV camera network for the main administration building, Federal Polytechnic Offa. Engineering and Technology Journal, 9(9), 5007–5011. https://doi.org/10.47191/etj/v9i09.04

9. Esther George (2015), "The Effects of Insecurity and Poverty on Human Development at the Muncipal Level in Northern Nigeria". Journal of Engineering Trends in Economics and Management Science,Vol. 6,No7

10. Jihong L. and Yang L. (2011), "Application of Internet of Things in Community Security Management". 2011 Third International Conference on Computational Intelligence, Communication System and Networks. Researchgate.

11. Kumar, R., & Singh, P. (2018). Smart surveillance monitoring system using CCTV and IoT. International Journal of Computer Applications, 179(19), 1–5.

12. Okae, P., Aboagye, I. A., Sowah, N. L., Ofoe, E. T., Ansah, M. R., & Osei, G.(2024). IoT interoperable surveillance system using wireless and fiber cable. International Journal of Engineering Trends and Technology, 72(7), 214–223. https://doi.org/10.14445/22315381/IJETT-V72I7P123

13. Sarika C. and Meena G (2022), "Internet of Things: Protocols, Applications and Security. Procedia Computer Science 215: 274-288. Doi:1016/;proc.2022

14. Sharma, M. L., Kumar, S., Ghosh, S., Alam, S., Firdos, S., & Joshi, K. (2025). Advanced surveillance and detection systems using deep learning. International Journal for Research in Applied Science & Engineering Technology (IJRASET), 13(11).

15. Sultana, T., & Wahid, K. A. (2019). IoT-Guard: Event-driven fog-based video surveillance system for real-time security management. IEEE Access, 7, 134881–134894. https://doi.org/10.1109/ACCESS.2019.2941978

16. Yu-Yong L. Tza-Yin C., Wen-Ray S. (2022), IoT for Environmental Management and Security Governance: An Integrated Project in Taiwan. Sustainability 2022. 14(1), 217, https://doi.org/10.3390/su14010217

17. Zhang, Y., Wang, L., & Zhao, H. (2020). Intelligent video surveillance systems: A review of technologies and applications. IEEE Access, 8, 151234–151248.