

Design and Construction of An Integrated Smart Surveillance Network Using Perimeter Intrusion Dictation (PID) and AI Cameras

Amadi Christopher Chidi¹, Opara Felix Kelechi², Nkwachukwu Chukwuchekwa³, Anyalewechi Chika⁴, Nnamdi Henry Ifeanyi⁵

Department of Computer Engineering, Michael Okpara University of Agriculture Umudike, Abia State, Nigeria¹

Department of Electrical and Electronics Engineering Federal University of Technology Owerri, Imo State, Nigeria^{3,4}

Department of Computer Engineering, Michael Okpara University of Agriculture Umudike, Abia State, Nigeria⁵

amadi.christopher@mouau.edu.ng¹,

Abstrak

Kata Kunci:

Pengawasan Cerdas,
Deteksi Intrusi Perimeter
(PID), Kamera AI, Desain
Jaringan Pengawasan

Makalah ini membahas desain dan konstruksi jaringan pengawasan pintar yang mengintegrasikan deteksi intrusi perimeter (PID) dengan kamera AI. Pengaturan mencakup sistem deteksi gerakan, platform otentikasi, sistem peringatan, dan panel kontrol aplikasi web. Inti dari desain ini adalah Raspberry Pi, diprogram dengan Python, yang bekerja bersama sensor PIR dan kamera untuk mendeteksi gerakan dan menangkap gambar. Selain itu, ada pembaca/kartu RFID untuk otentikasi, modem USB untuk melakukan panggilan telepon, dan menghubungkan perangkat ke internet, memungkinkannya mengirim gambar penyusup mana pun langsung ke email pemiliknya. Bel alarm juga merupakan bagian dari sistem, dan panel kontrol aplikasi web dapat diakses melalui Wi-Fi Raspberry Pi untuk pengelolaan yang mudah. Sistem ini diuji dalam berbagai skenario, termasuk otentikasi pengguna dan deteksi penyusup, dan bekerja seperti yang diharapkan.

Abstract

Key Word:

Smart Surveillance,
Perimeter Intrusion
Detection (PID), AI
Cameras, Surveillance
Network Design

This paper discusses the design and construction of a smart surveillance network that integrates perimeter intrusion detection (PID) with AI cameras. The setup includes a motion detection system, an authentication platform, an alert system, and a web application control panel. At the heart of this design is a Raspberry Pi, programmed with Python, which works alongside a PIR sensor and a camera for detecting motion and capturing images. Additionally, there's an RFID reader/card for authentication, a USB modem for making phone calls, and connecting the device to the internet, allowing it to send images of any intruder directly to the owner's email. An alarm buzzer is also part of the system, and the web application control panel can be accessed via the Raspberry Pi's Wi-Fi for easy management. The system was tested under various scenarios, including user authentication and intruder detection, and it performed as expected.

Copyright © 2025 Amadi Christopher Chidi, Opara Felix Kelechi, Nkwachukwu Chukwuchekwa, Anyalewechi Chika, Nnamdi Henry Ifeanyi

This work is licensed under an **Attribution-ShareAlike 4.0 International (CC BY-SA 4.0)**

INTRODUCTION

Video surveillance systems popularly known as Closed-circuit television (CCTV) have been around since the 20th Century. One of the first recorded applications for closed circuit television system (CCTV) was in 1942 when it was used to view the launch of V2 rockets in Germany (Mesnik, B., 2016). Traditionally, the system consists of cameras attached to monitor screens. CCTV systems are installed to give an overview of a large area to a limited number of operators (Nalini M and Kiran, 2017). In times past, security personnel will have to constantly watch multiple screens in a room all day in order to detect intrusion or review hours of stored footage of intrusion that took place when the security personnel was unavailable (Sheshai.S. S, 2016). With advancements in technology, many improvements have been made to video surveillance systems making them smarter. Today, video surveillance systems have found their applications in various sectors in our society. These devices have been a key component in ensuring security at airports, banks, prisons, schools, residential areas, to mention a few (Ovseník, L.et al,2010) Criminal activities are becoming very dexterous nowadays, through intelligent and novel methods criminals are maneuvering to succeed in their activities in residential apartments. The need for safety of life and property cannot be over emphasized and with the rising costs of security installations, a cost-effective alternative is always a welcomed option (Nosiri et al, 2018).

A lot of technologies for surveillance and monitoring have been in existence but none seems to be heterogenous in its operation. Some of these technologies include closed-circuit television (CCTV), perimeter intrusion detectors (PIDs), drone camera systems, radio frequency identification tags (RFID) and lots more. To adequately monitor a given area or environment, an integrated and also an adaptive system would go a long way to mitigate several security loopholes and mitigate intrusion.

Surveillance videos are becoming part of every aspect of life activities, from banks to executive buildings as well as monitoring of traffic, organizations and schools Anas et al., (2022). Surveillance systems are employed in school to prevent examination malpractice and immoral activities. So, surveillance cameras are mainly deployed in the exam halls, laboratories and libraries. The capability of surveillance system is far beyond how it is currently used in the school campuses. Campuses have diverse set of individuals which makes it hard to monitor and control. Riots and protests frequently arise in Nigerian campuses due to the difference in religion and culture. Example is Deborah's case (13-may-2022) in Shehu Shagari Collage of Education, Sokoto State of Nigeria as a result of blasphemy. Also, Lukman (23-nov-2022) in Sultan Abdulrahman Collage of Health Technology, Gwadabawa, Sokoto State of Nigeria as a result of theft accusation. And that of Michael Okpara University of Agriculture (Feb 10, 2024) which was as a result of increased school fees and students' protest. These cases usually reach the authorities very late when things are already out of control. Surveillance system can be used to trace and penalize the perpetrators of such events.

Systems developed to mitigate unauthorized access such as the Intrusion Detection Systems (IDS) serve as vital security safeguards, shielding network infrastructures from cyber-attacks by identifying unauthorized access and harmful actions. Since their emergence in the mid-80s, they have undergone substantial advancements to stay on par with the growing complexity of computer-related crimes (Delamore, 2015). During the World war II, various mechanical and electrical devices were developed for military use to secure perimeters. These included tripwires, pressure-sensitive Figures, and rudimentary alarm systems. After the war, some of the technology developed for military purposes found applications in civilian security. Simple electric fence systems became more common. Shortly after, the use of electronics and sensors advanced PIDS technology. Infrared sensors and microwave systems were introduced to detect intrusions. These early systems had limitations in terms of false alarms and reliability. Significant improvements were made in PIDS technology, including the use of digital signal processing (DSP) to reduce false alarms. More advanced sensors like passive infrared (PIR) and dual-technology sensors were developed. Up till date, PIDS technology has continued to evolve with the integration of advanced software, networking, and communication capabilities. Modern PIDS can use CCTV cameras, fiber optic sensors, and intelligent analytics to provide more accurate and real-time intrusion detection. IDS can be categorized into network intrusion detection (NIDS) and prevention (IPS) systems, which analyze network traffic for signs of malicious activity using signature and statistical anomaly detection as well as heuristic behavioral analysis (Niksefat 2017). Such systems have the capability to identify and potentially avert attacks and malicious actions that conventional security measures like firewalls may miss (Aljanabi M., Ismail M.A., Ali A.H., 2021).

Review of Related works

A Passive Infrared (PIR) sensor is a device that detects infrared radiation (IR) from objects in its field of view. Several surveys related to smart surveillance systems and artificial intelligence cameras were reviewed in the course of the study.

Lee & Chuah in 2018, developed a smart indoor home surveillance monitoring system using raspberry pi, a Passive Infra-Red PIR sensor and a webcam. Motion in the room triggered the PIR sensor which captured images of any intruder and using internet connectivity from a wireless network the images are sent to the owners Dropbox Cloud storage which was then followed by an email and an SMS notification (Lee & Chuah in 2018). The observed shortfall in the system is that the system lacked intruder authentication which inadvertently made the owner appear as an intruder in his own premises. The PIR sensor was the only means of intruder detection which made the system prone to false alerts, another flaw to the surveillance system.

A Motion Detector Security System for Indoor Geolocation was developed by (Nosiri et al, 2018) EE. This project focused on developing a security system used indoors at the entrances of homes. It has a motion detection module, video capturing module, SMS notification module and a web server module. The system was able to detect motion (intruder), activate the embedded camera to take frames of video after motion was sensed and store the video on a web server with an SMS alert to the notify the owner. Also, the shortfall observed in the system is that the system did not also have an authentication module meaning the owner could be seen as an intruder and in the absence of internet connectivity, the owner would not be alerted since the SMS notification module uses internet.

Moreso, Ashwin and Guddeti (2020), demonstrated a Hybrid Convolutional Neural Network to analyze students' body postures, gestures and facial expressions to investigate engagement. Three states of student's engagement were examined: boredom, engaged and neutral. Rashmi et al. (2021), proposed an automatic system, that monitors the students' activities, such as the actions of sleeping, eating, using phone, discussion and being engage. The aim of this study is to localize and recognize multiple actions of the students in an image frame.

In 2013, an Access Control of Door and Home Security by Raspberry Pi through Internet was developed by (Nasimuzzaman et al). This made use of a PIR sensor, an LCD, Wi-Fi camera, raspberry pi and a Wi-Fi dongle. When the PIR sensor detects motion, the Wi-Fi camera is activated to take a photo and email the attachment to the respective email and at the same time generate a tweet to notify the administrator about the visitor with pictures. The administrator could see the visitor

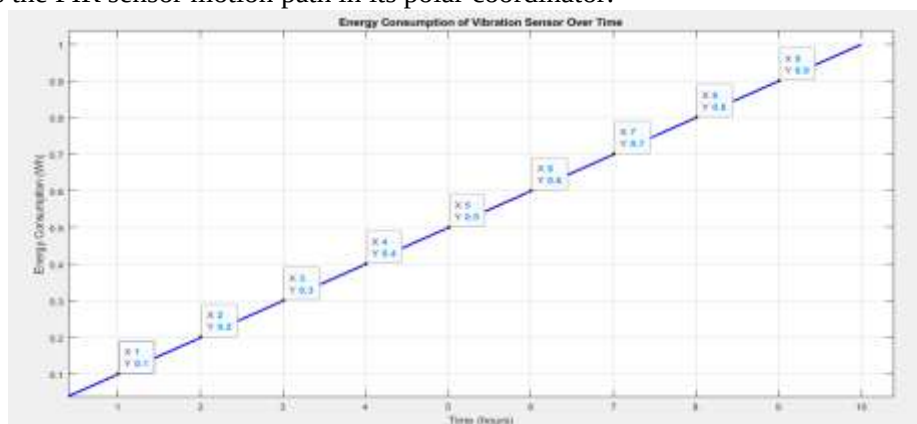
and notify the visitor via tweets and the visitor can view on the screen or he can send a command via twitter to unlock the door. The owner has no way of verifying himself, so when he gets to his door an image of him is also taken and if there is power failure, he would not have access to his apartment because of the magnetic lock. Live Streaming Motion Detection Camera Security System with email notification using Raspberry Pi was developed by (Angela & Gidveer) [8]. This security system made use of raspberry pi as the main controller, a PIR sensor and a webcam for motion. The PIR sensor and the camera detect motion, sound an alarm, save the images and send them to the owner's email. The LAN connection enables the raspberry pi to connect to the internet. It also makes use of an android application to activate and deactivate the system. Using LAN connection for internet access requires an external peripheral like a router or another computer with internet connectivity. The above systems present cost-effective alternatives to home surveillance but has its drawback or limitation centered on no satisfactory or non-existing authentication and cumbersome internet access. This work seeks to address some of these issues.

Moreso, Ashwin and Guddeti (2020), demonstrated a Hybrid Convolutional Neural Network to analyze students' body postures, gestures and facial expressions to investigate engagement. Three states of student's engagement were examined: boredom, engaged and neutral. (Rashmi et al., 2021), proposed an automatic system, that monitors the students' activities, such as the actions of sleeping, eating, using phone, discussion and being engage. The aim of this study is to localize and recognize multiple actions of the students in an image frame.

RESEARCH METHODS

The smart surveillance Network is designed to detect the presence of an individual entering a premises. When motion is detected by both the PIR sensor and the Artificial intelligence camera, images are taken, saved and sent to the control room. The system offers levels of authentications to the assumed intruder after which if no authentication success is recorded the system notifies the owner in the control room via SMS alert and an email containing photos of the intruder.

In practice, the system offers two authentication windows, The RFID authentication and the Passcode. The first of which is an initial period of 10 seconds from the period a motion/ human presence is detected and confirmed by both the PIR sensor and the A.I camera connected together using a Rasberry Pi. PIR sensors are widely used for motion detection in security systems, automatic lighting, and other applications (Biswa, 2014). The physics of infrared radiation, sensor sensitivity, and the geometry of detection as shown in Figure shows the PIR sensor motion path in its polar coordinator.



Graph of Energy Consumption by the vibration sensor in 10 hrs duration of unit test

PIDS and Motion Detection Unit and the associated Blackbody Radiation Models

Objects emit infrared radiation according to their temperature. The radiation emitted by an object can be approximated using Planck's Law for blackbody radiation (Biswa, 2014). However, for many practical purposes, the Stefan-Boltzmann Law is more convenient:

$$P = \sigma \epsilon A T^4 \quad (3.1)$$

Where:

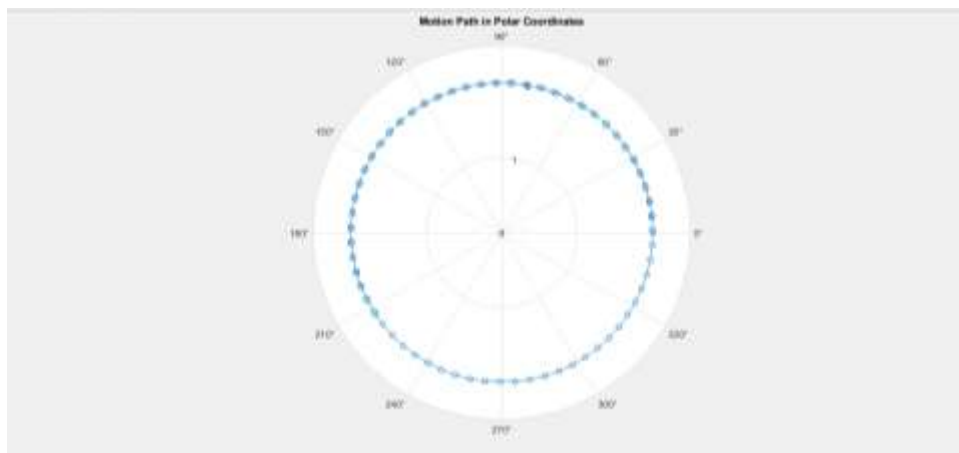
P = the power radiated by the object (W).

σ = the Stefan-Boltzmann constant ϵ is the emissivity of the object (dimensionless, ranges from 0 to 1) = $5.6 \times 10^{-8} \text{ W m}^{-2} \text{ K}^{-4}$

A = the surface area of the object (m^2).

T = the absolute temperature of the object (K).

To improve the detection perimeter of the PIR sensor used in this work, the surface area must be adjusted accordingly. The PIR Motion Sensor Path in Polar Coordinates is shown in Figure



PIR Motion Sensor Path in Polar Coordinates

Modelling and Simulation of the Vibration Sensing Unit over time (the vibration sensor and parameter dynamics)

The model of the vibration Sensor parameters according to its datasheet from the manufacturer (e.g., accelerometer, piezoelectric sensor), such as sensitivity, natural frequency and damping ratio was developed based on its mass (m), damping coefficient (c), and its stiffness (k) (Lévesque, 2014). In creating the differential mathematical model, equations 1, 2, and 3 were simulated using MATLAB code. For the sensor used in this work, a second-order system was considered for a simple accelerometer:

$$m\ddot{x} + c\dot{x} + kx = F(t) \quad (3.2)$$

Where m is the mass, c is the damping coefficient, k is the stiffness, and (t) is the external force.

For the Transfer Function of the accelerometer:

$$H(s) = \frac{\text{Output}(s)}{\text{Input}(s)} \quad (3.3)$$

Equation 3 represents the transfer function for the accelerometer:

$$H(s) = \frac{\omega_n^2}{s^2 + 2\zeta\omega_n s + \omega_n^2} \quad (3.4)$$

Where ω_n is the natural frequency and ζ is the damping ratio.

From equation (1), the Vibration sensor simulation Matlab input parameters and code that were used were as follows:

The sampling frequency (Fs) was set at 1000 Hz and the cutoff frequency (fc) was 100 Hz,

Nyquist Frequency: For a sampling frequency (Fs) of 1000 Hz, the Nyquist frequency was 500 Hz.

Normalized Cut-off Frequency: The cut-off frequency must be divided by the Nyquist frequency. For a cut-off frequency of 100 Hz, the normalized cut-off frequency the normalized cutoff frequency was then calculated thus:

should be (Lévesque, 2014):

$$f_c = \frac{\text{cutoff frequency}}{\text{Nyquist frequency}} = \frac{100}{500} = 0.2 \quad (3.5)$$

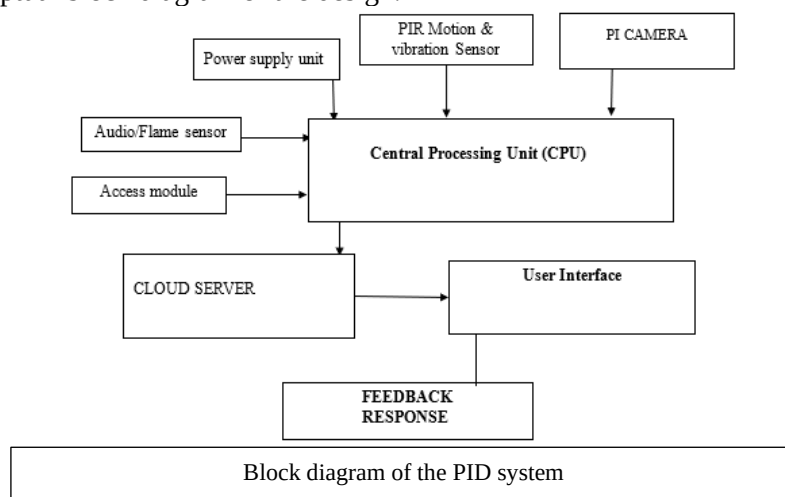
MATLAB Butter Function: The butter function requires the cut-off frequency to be within the range (0, 1), representing the fraction of the Nyquist frequency.

```
>> % Parameters
Fs = 1000; % Sampling frequency in Hz
T = 1; % Duration in seconds
t = 0:1/Fs:T-1/Fs; % Time vector

% Generate random noise
noise_signal = 0.1 * randn(size(t)); % Generate Gaussian white noise
% Design a low-pass filter
fc = 100; % Cut-off frequency in Hz
normalized_fc = fc / (Fs / 2); % Normalize the cut-off frequency
[b, a] = butter(4, normalized_fc); % 4th-order Butterworth filter
% Apply the filter to the white noise
filtered_noise = filter(b, a, noise_signal);
% Compute FFT of the filtered noise signal
N = length(filtered_noise); % Number of samples
Y_filtered = fft(filtered_noise); % Compute the FFT
f = (0:N-1)*(Fs/N); % Frequency vector
amplitude_filtered = abs(Y_filtered)/N; % Amplitude spectrum
% Plot filtered noise signal in time-domain
figure;
plot(t, filtered_noise);
xlabel('Time (s)');
ylabel('Amplitude');
title('Time-Domain Filtered Noise Signal');
grid on;
% Plot frequency spectrum of the filtered noise signal
figure;
plot(f, amplitude_filtered);
xlabel('Frequency (Hz)');
ylabel('Amplitude');
title('Frequency Spectrum of Filtered Noise Signal');
```

Pseudo code for Vibration Sensor Response graph of the PIDS

The block diagram for the PIDS, outlines the flow and interaction between different components to create a comprehensive AI-based adaptive perimeter intrusion detection system and identifies potential intrusions in real-time using the Short Message Service (SMS) and GPS as the notifying media. Figure shows the high-level conceptual block diagram of the design.



The block diagram of the dual authentication system using RFID and a password keypad consists of interconnected modules that work together to verify a user's identity. The primary components include an Arduino Uno microcontroller, an RFID reader, a keypad, an LCD, a servo motor, and a buzzer. These components collectively form the backbone of the security system, providing both RFID card and password-based access control.

The Arduino Uno acts as the central processing unit, managing signals from both the RFID reader and the keypad. The RFID reader detects and reads data from RFID tags, capturing each tag's unique identification (UID) when presented. This UID is then sent to the Arduino, which compares it against a pre-stored list of

authorizedUIDs. Simultaneously, the keypad is used to enter a passcode, which is also verified by the Arduino. For successful entry, both the RFID UID and the entered password must match the pre-configured authorized data.

An LCD is connected to the system to provide visual feedback. It shows prompts for users to scan their RFID tag or enter a password, as well as status messages indicating successful or failed authentication attempts. When the correct RFID and password are verified, the Arduino sends a signal to the servo motor, which rotates to unlock or open the secured access point, such as a door. The buzzer provides audible feedback, emitting a sound to indicate authentication status, either a positive tone for successful access or a negative alert for a failed attempt

RESULTS AND DISCUSSION

Design Implementation

The security system was designed and implemented to enhance surveillance, intrusion detection, access control, and audio-based security monitoring. The project utilized a Raspberry Pi Camera for real-time video surveillance, an ESP32 microcontroller for processing and communication, a vibration sensor for perimeter intrusion detection, an audio sensor for sound-based alerts, a fingerprint sensor for access control, a buzzer for alarm notifications, a display unit for system feedback, and a router for internet-based monitoring.

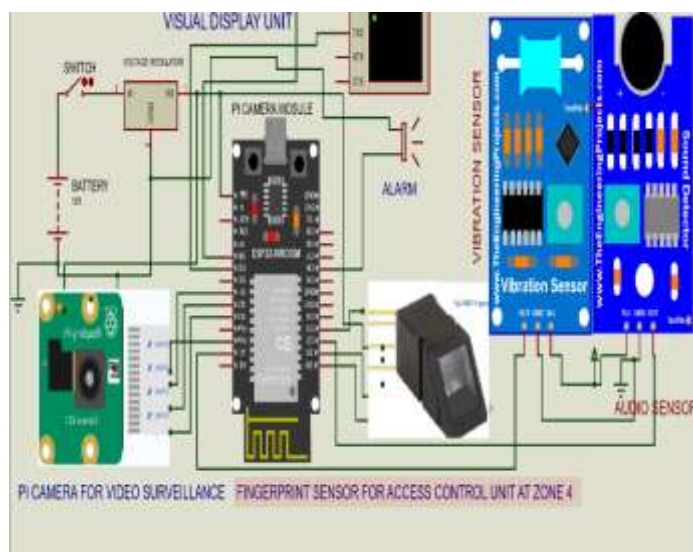
The system was powered by a 12V battery, regulated to supply appropriate voltage levels to each component. The Raspberry Pi Camera was strategically installed to provide live surveillance, transmitting video feeds to a central monitoring unit through the ESP32 module. The vibration sensor was deployed at key access points to detect unauthorized movement or force applied to secured areas. When triggered, the system activated an alarm and sent real-time alerts to security personnel.

The audio sensor was configured to detect specific sounds such as forced entry, breaking glass, or distress calls. Upon detection of any predefined sounds, the system triggered an immediate alert, ensuring a swift security response. Access control was reinforced using a fingerprint sensor, which authenticated registered users before granting entry. When a valid fingerprint was scanned, the ESP32 activated a relay mechanism to unlock doors, while unauthorized attempts set off an alarm and logged the event for security review.

The display unit provided real-time feedback on access status and security events, allowing security personnel to monitor system activity efficiently. The ESP32 controller managed all data processing and communication, ensuring seamless integration of the various security components. The router facilitated internet connectivity, enabling remote monitoring and alert notifications.

The implementation of this security system significantly enhanced security measures, providing automated monitoring, rapid intrusion detection, and efficient access control. The system's ability to operate in real-time ensured that security personnel received instant notifications and live video feeds, allowing for immediate responses to potential threats. This project successfully demonstrated the effectiveness of a smart, technology-driven security solution tailored to the needs of the institution.

Figure shows the circuit diagram for the PID system



Screenshot showing the design network display module with images



Screenshot showing the design network display module with images

CONCLUSION

In this project, we developed a smart home surveillance system that features a motion detection setup using a PIR sensor and an AI camera. It also includes an RFID-based authentication system, a web application control panel, and an alert system that notifies you through phone calls and emails. The heart of the system is a Raspberry Pi, which facilitates quick communication between all the components. We connected the AI camera, a USB network modem, the PIR sensor, an RFID reader, an LED, and a buzzer. After running various test scenarios, we found that the system performed well, proving to be a convenient and cost-effective alternative for home security surveillance.

REFERENCE

- Anas, A., Bagiwa, M. A., Roko, A., Buda, S., Yaldu, Z. Y., Bello, A. M. & Ainu, H. A. (2022). *An inter-frame forgery detection technique for surveillance videos based on analysis of similarities*. SLU journal of science and technology, 4(1&2), 15-26
- Aljanabi M., Ismail M.A., & Ali A.H.(2021). *Intrusion Detection Systems, Issues, Challenges, and Needs*. International Journal of Computational Intelligence Systems. 2021
- Ismail, L.; & Materwala, H. (2019). *A Review of Blockchain Architecture and Consensus Protocols: Use Cases, Challenges, and Solutions*. Symmetry 2019, 11, 1198.
- Mesnik, B. (2016). The History of Video Surveillance. Retrieved from <https://kintronics.com/the-history-ofvideo-surveillance>
- Nalini M., Kiran G.V (2017). Automatic Surveillance System Using Raspberry Pi and Arduino, International Journal of Engineering Sciences & Research Technology, 6(5), 635-640.
- Nasimuzzaman C., Shiblee, N., Sarker S., (2013), Access Control of Door and Home Security by Raspberry Pi through Internet. International Journal of Scientific and Engineering Research, 4(11), 550-558.
- Nosiri O.C., Akwiwu-Uzoma C.C., Nmaju U.A., Elumeziem C.H. (2018). Motion Detector Security System
- Niksefat S., Kaghazgaran P., & Sadeghiyan B.(2017). *Privacy issues in intrusion detection systems: A taxonomy, survey and future directions*. Computer Science Review. Aug;25:69–78.
- Ovseník, L., Kolesárová A., Turán J. (2010). Video Surveillance Systems, Acta Electrotechnica et Informatica, 10 (4), 46–53.
- Rashmi, M., Ashwin, T. S., & Guddeti, R. M. R. (2021). *Surveillance video analysis for student action recognition and localization inside computer laboratories of a smart campus*. Multimedia Tools and Applications, 80(2), 2907–2929.
- Sheshai.S.S (2016), Raspberry PI Based Security System, University of Nairobi, Kenya.