LGJDX ISSN No: 1008-0562 Journal Of Liaoning Technical University Natural Science Edition

DEVELOPMENT OF SMART INTRUSION DETECTION AND ALARM SYSTEMS TO CURB VANDALIZATION OF INFRASTRUCTURE IN THE POLYTECHNIC ADMINISTRATIVE BUILDING

[1]Babalola, A.D, & [2]Olufemi, T.O. (Ph.D)
[1]Department of Computer Engineering, Federal Polytechnic, Ile-Oluji, Ondo State
[2]Department of Computer Science, West Midlands Open University Ikeja, Lagos State
Email: babalolaabayomi@gmail.com, tolubiks67@gmail.com

Abstract
This study investigates the development of an intelligent intrusion detection and alarm system to reduce infrastructure vandalism at the Polytechnic Administrative Building. This article emphasizes the critical need for improved security protocols in educational settings and proposes an innovative strategy that combines Internet of Things (IoT), machine learning, and blockchain technology. The system's frame work integrates the indoor and outdoor monitoring features, such as a 4k high-definition camera with an intelligent facial recognition detector and device with infrared sensor for unauthorized intruders. The main control systems analyze the images received from different camera locations on each floor and use machine learning techniques to identify and detect anomalies and potential security breaches and violations. The research also includes anti-tamper devices to protect the installed equipment. The analysis reveals that 10% of the data points fall into the category of anomalies, requiring critical attention. The analysis reveals a slight negative correlation between average and maximum motion, thereby unveiling intricate patterns in potential intrusion scenarios. This comprehensive campus security policy aims to minimize theft and damage while exhibiting the institution's commitment to using innovative technology for the safety and well-being of its community. The proposed approach offers a scalable and adaptive answer to evolving security problems in educational settings.
Keywords: Smart Intrusion Detection, IoT Security Systems, Machine Learning Algorithms, Vandalism Prevention, Blockchain Technology, Real-time Monitoring, Data Visualization in Security

1. Introduction

The Polytechnic operations depend on the integrity and functionality of both the academic and administrative security infrastructure built and controlled within the Polytechnic Administrative building. This infrastructure with the Polytechnic campus is essential focal points for research, teaching, and institutional administration. The importance of the infrastructure to the polytechnic community for learning, research and administrative purposes can also be endangered by the vandals and theft and this will in turn disrupt the smooth operation of the institutional activities and will cause more damages and make the institution incurred more cost in acquiring the infrastructure. The design and development of intelligent intrusion detection and alarm systems customized for the unique architecture of the Polytechnic Administrative building is essential for addressing this challenge. Employing advanced technologies like as blockchain, machine

learning, and the Internet of Things (IoT), these systems provide thorough real-time detection and alert methods to prevent unauthorized access. The Polytechnic's implementation of advanced security technologies offers a proactive approach to enhance security and sustain the functionality of academic and administrative sectors while preserving the integrity of its infrastructure.

1.2 Problem Statement and Justification

Developing sophisticated intrusion detection and alarm systems for the Polytechnic Administrative Building mitigates theft and damage, safeguarding essential Polytechnic assets. Utilizing IoT, machine learning, and blockchain technologies, which enable real-time monitoring and alerts for unauthorized access, these systems provide a proactive security solution. This not only deters possible invaders but also reduces the probability of property damage and theft. Implementing these systems aligns with the institution's duty to protect its staff, educators, and students by ensuring a secure environment that facilitates administrative functions, research, and education. The Polytechnic has made a significant investment in installing closed-circuit television to address the security challenges of the campus infrastructure. This will not only boost the confidence of the staff and students but also lead to a reduction in the number of security personnel. Lowering the personnel budget will also improve the security team's performance. The use of this technology demonstrates the seriousness of polytechnic management in ensuring life and property safety

2. Literature Review

Ajala et al. (2020), studied how to use the Internet of Things (IoT) to make smart homes safer. They created a special system that can detect when someone is trying to break into a house. This system uses sensors, GPS, cameras, alarms, and communication tools to spot intruders, take pictures, and send alerts to the homeowner right away. The system uses GPS, location tracking, and image recognition to make homes safer. It also uses sounds, lights, and water to scare away intruders. Even though this system works well, there's still a lot we don't know about how different IoT devices and systems can work together and handle a lot of users. Mitigating this deficiency could improve integration and standardization, resulting in more efficient IoT-based intrusion systems for smart villas. Mustafa et al. (2020) developed a novel intrusion detection system specifically designed for smart homes, highlighting real-time alerts and minimizing false alarms. Both studies emphasize the potential of IoT to enhance home security while highlighting

the necessity for additional study on system scalability and seamless integration across various IoT infrastructures to augment their efficacy.

Mohammed et al. (2020) also emphasized how their burglary and theft detection solution improves real-time reporting of security breaches by integrating fuzzy logic and SMS-based alert systems. To detect intrusions, their system utilizes a microcontroller-based accelerometer and a fuzzy inference system to process the data, thereby delivering timely notifications to the authorities. Similar to Ajala et al. (2020), their research can reduce crime rates, but it faces some challenges in terms of interoperability with other security equipment and infrastructure. Vinayakumar et al. (2019) utilized machine learning techniques and analysis, specifically deep neural networks, to establish a real-time intrusion detection system that detects cyberattacks on the security system. The results show that the performance outweighed other classifiers in detecting attacks and intrusions. Further studies on integration and scalability in cyber security, including smart homes and cities, can address the interoperability challenges. Kanthaseelan et al. (2021) conducted research on the application of computer vision and image processing in home security surveillance. They used recent technology to process the images generated from the surveillance camera, which in turn improved the security systems' performance. While the system was effective, it encountered challenges in optimizing its interface with various home automation and security frameworks. To achieve this fit, a robust, cohesive, and effective security system for both intruder detection and life and property safety management must be developed. The results showed that it is possible to scale an IoT-based intrusion detection system for seamless integration with diverse platforms with varying architectures. The evaluation reveals shortcomings in current research, emphasizing the need for thorough techniques to tackle scalability, standardization, and interoperability challenges in IoT security frameworks. Ajala et al. (2020), Mustafa et al. (2020), and Mohammed et al. (2020) conducted research that highlight the potential of utilizing IoT and advanced technologies inside machine learning algorithms, such as fuzzy logic and real-time alerts, to improve security systems. The amalgamation of the current security framework design with alternative platforms poses considerable difficulties. Recently, many platforms have embraced this framework for its efficacy in executing the specified security architecture. In 2019, scientists Vinayakumar and his team asserted that the application of machine learning, particularly deep neural networks, is crucial for managing large and complex datasets in intrusion detection systems. However, they

also stated that we require systems capable of evolving and adapting to emerging dangers while functioning well with other IoT devices. In 2021, Kanthaseelan and his colleagues discussed the application of image processing and computer vision for intruder detection and kid safety. The growth and popularity of Internet of Things (IoT) devices has produced an increase in interconnected systems; nevertheless, their efficacy is sometimes obstructed by issues of interoperability and scalability. Future research should emphasis the establishment of standardized protocols to enable seamless communication among various IoT devices. Establishing a standardized language for these devices can markedly enhance the effectiveness and efficiency of security systems, especially in extensive implementations such as smart cities and residences. This standardization will enhance data interchange and integration while strengthening the security framework of IoT networks, protecting sensitive information and mitigating potential vulnerabilities.

3. **Methodology**

The evaluation reveals shortcomings in current research, emphasizing the need for thorough techniques to tackle scalability, standardization, and interoperability challenges in IoT security frameworks. Ajala et al. (2020), Mustafa et al. (2020), and Mohammed et al. (2020) conducted research that highlight the potential of utilizing IoT and advanced technologies in machine learning algorithms, such as fuzzy logic and real-time alerts, to improve security systems. The amalgamation of the current security framework design with alternative platforms poses considerable difficulties. Recently, several platforms have embraced this framework for its efficacy in executing the previously outlined security architecture.

3.1 The System Architecture

By integrating physical and cybersecurity measures, the intrusion detection and alert system enhances the performance of the security apparatus. It uses sensors such as infrared barrier sensors, an intelligent camera with face detection, and a microphone to detect an intrusion (fig 3.1). The system utilizes a centralized control system to process and analyze the collected data, employing a machine learning model to set off an alarm and dispatch SMS alerts when an intrusion occurs. There is also remote monitoring for remote access control and intervention based on authorized access. The system is scalable and always updated in case of security threats.

LGJDX
ISSN No: 1008-0562
Journal Of Liaoning Technical University
Natural Science Edition

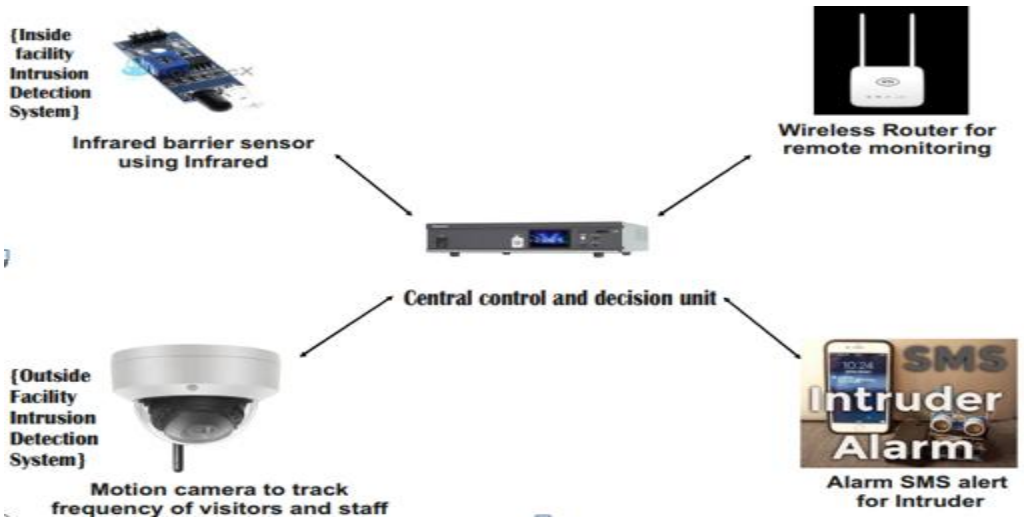

Figure 3.1 shows specified intrusion layout and security system architecture

3.1.1 Outdoor Facility

The external security system includes a sophisticated bullet camera with facial recognition technology to detect personnel entering the administrative building. The technology identifies regular staff members by monitoring their visit frequency and alerts for unknown individuals as potential invaders. This feature improves the building's security by identifying unauthorized access or suspicious behavior, ensuring that only authorized individuals are recognized, and facilitating the detection and response to intrusions.

3.1.2 **Indoor facility**

The security system incorporates both inside and outdoor surveillance elements for thorough protection. The indoor system incorporates an embedded device engineered to detect human motion using an infrared sensor. Upon motion detection, it notifies the security unit and activates an alarm. The SMS module is been link with the microcontroller to generate alert in case of abnormality (Fig3.2.). The external surveillance system comprises infrared barrier sensors

positioned around the structure. These sensors project an imperceptible beam that, upon interruption, transmits a signal to the control unit. The system features a camera at the main entrance that records photos upon detecting motion. Vibration sensors and microphones are incorporated to identify attempts of forcible access, such as metal cutting. The microprocessor in the outdoor system receives information from infrared sensors and interacts through a Controller Area Network (CAN), facilitating long-distance data transmission and enabling simultaneous connections to numerous sites. The system incorporates a Raspberry Pi to augment processing performance, facilitating rapid input processing from several sensors. Data transfer and connection with the central control unit utilize Ethernet protocols, guaranteeing rapid and dependable connectivity for monitoring and reaction.

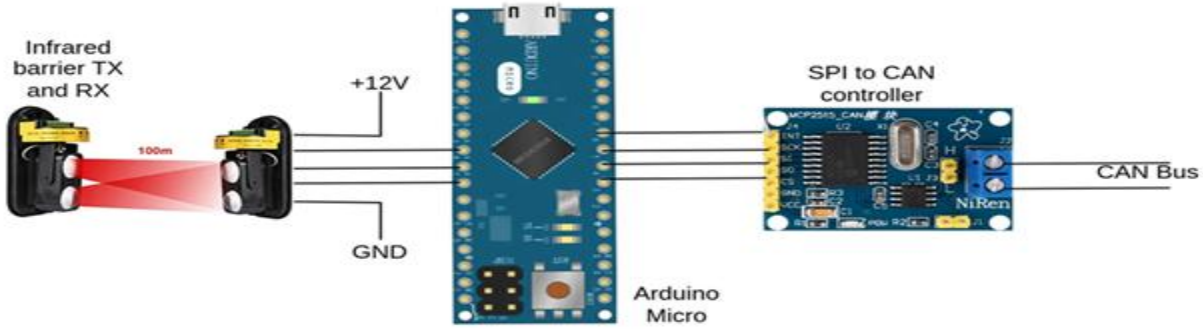

Figure 3.2: Outdoor monitoring unit

3.2 In-Facility Intrusion Detection System

The security system incorporates both inside and outdoor surveillance elements for thorough protection. The indoor system incorporates an embedded device engineered to detect human motion using an infrared sensor. Upon motion detection, it notifies the security unit and activates an alarm. The SMS module is been link with the microcontroller to generate alert in case of abnormality. The external surveillance system comprises infrared barrier sensors positioned around the structure. These sensors project an imperceptible beam that, upon interruption, transmits a signal to the control unit. The system features a camera at the main entrance that records photos upon detecting motion. Vibration sensors and microphones are incorporated to identify attempts of forcible access, such as metal cutting. The microprocessor in the outdoor system receives information from infrared sensors and interacts through a Controller Area Network (CAN), facilitating long-distance data transmission and enabling simultaneous connections to numerous sites. The system incorporates a Esp32 microcontroller with flask

application on the server to augment processing performance, facilitating rapid input processing from several sensors. Data transfer and connection with the central control unit utilize Ethernet protocols, guaranteeing rapid and dependable connectivity for monitoring and reaction.

Figure 3.3 shows: The ground view and middle floor view of designated building

Figure 3.4: Middle Floor and the general view designated building

3.3 **Interfacing of the Cameras with Display unit**

The system consist of four cameras connected in parallel to each other in each the building floor, the output cable of cameras were directly linked with PoE switch through port 1through4 and network cable were used to connect the switch via display unit and microcontroller, where the

processing and decision were been taking place for surveillance every activities in each floor and display the information at control room, has been described in Figure3.5

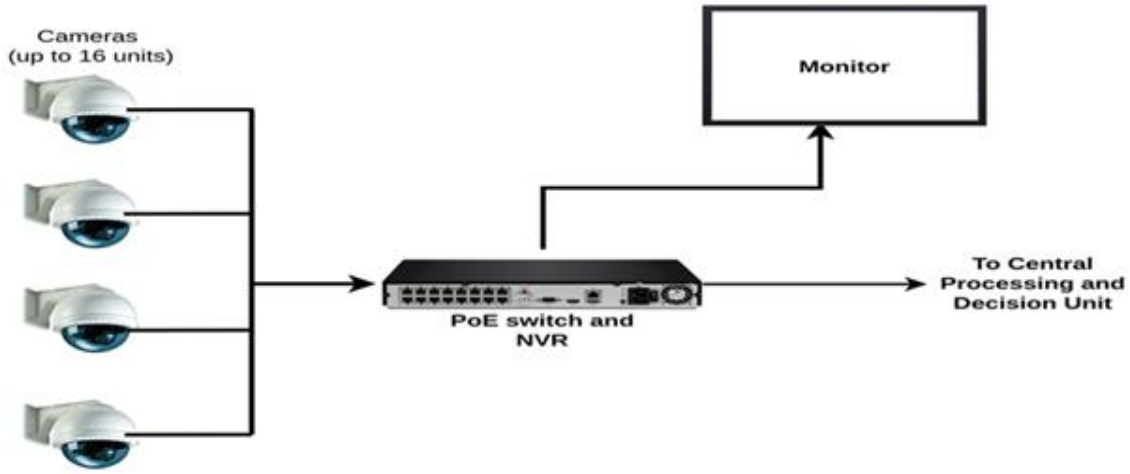

Figure3.5 shows the wired network camera connection model diagram

3.3.2 Anti-tamper systems for Removable units

To enhance the security of detachable units such as batteries, cameras and NVR, an anti-tamper system will be employed to prevent unauthorized removal. This system uses electronic switches, mounted securely with screws or suction pads, that trigger alarms when tampering is detected. The alarm signals are then sent to security personnel, ensuring the safety and integrity of critical equipment. At the core of this design is a reflective IR sensor, positioned to create a continuous optical path between the IR LED and receiver. When tampering occurs, the IR sensor sends a signal to an ATtiny85 microcontroller, which then communicates over a Controller Area Network (CAN) bus. Each protected unit is assigned a unique ID, enabling the connection of multiple anti-tamper boards within the same system. These boards are linked to a Raspberry Pi Pico, a low-cost, high-performance microcontroller capable of managing multiple inputs. This anti-tamper system is integrated with the facility's broader security infrastructure, including the camera and Network Video Recorder (NVR) system. When tampering is detected, the NVR system can activate cameras to capture real-time footage, providing visual evidence of the incident. The central control system, connected via an SPI to Ethernet converter, allows seamless communication and coordination between all security components, ensuring comprehensive protection of both removable units and the facility shows in figure 3.6 below.

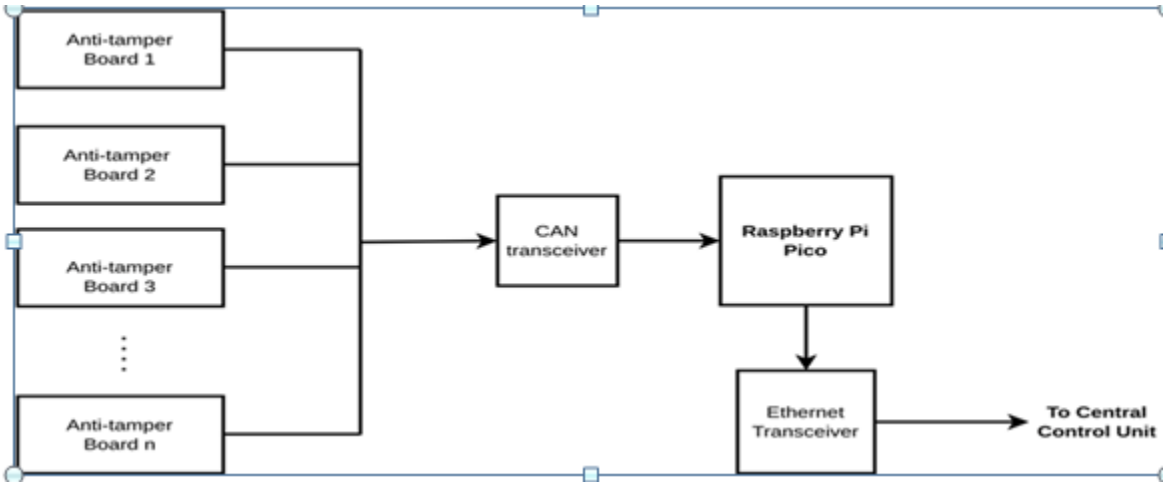

Figure 3.6 shows the network diagram of the Anti-tamper system

3.3.3 Central Control and Decision Unit

As they manage data from dozens of sensors and monitoring devices, security keypads allow intelligent applications to communicate with the heart of the home security system, which forms the central control unit. This includes a network switch for switching signals, a router for external communication, and a Linux-firmware-based computer to even perform demanding calculations. This structure allows a system to analyze and act on real-time information in other words, decide whether or not it should sound the alarm bells. Linux-based and capable of running security scripts, the system is also able to communicate via SOS signals directly over mobile networks to neighboring base stations for a swifter reaction in case something unfortunate may happen and its owners need help. The unit controls and monitors the processes of multiple production stations to ensure all operations are centralized, ultimately playing a vital role in securing the facility from potential threats.

4. Results

The study's findings will focus on the deployment of an intelligent intrusion detection and alarm system aimed at improving security in the Polytechnic Administrative Building. The system will be integrated with IoT, machine learning, and blockchain technology to enable real-time monitoring and warning capabilities. These findings are crucial for identifying illicit activities and preventing theft or vandalism. While it effectively connected motion data, the inverse

correlation between average and maximum motion indicated its inadequacy in anticipating intrusion scenarios will be analysed.

Using the 3D scatter plot to present a detailed perspective on motion data with the following axes:

i. **X-axis**: Dataset ID
ii. **Y-axis**: Average Motion
iii. **Z-axis**: Maximum Motion

The result obtained in this plot (Figure.4.1), blue dots indicate normal data points, whereas red triangles mark anomalies—those exceeding two standard deviations from the mean in either average or maximum motion. This visualization effectively reveals the correlation between average and maximum motion across datasets, helping to pinpoint irregular patterns or outliers that may suggest potential intruder activity.

Analysis of Anomalies:

i. Mean Average Motion of Anomalies: 143.08
ii. Overall Mean Average Motion: 101.88
iii. Mean Maximum Motion of Anomalies: 149.02
iv. Overall Mean Maximum Motion: 105.67

Anomalous data points constitute 10.00% of the total dataset. This discrepancy highlights the significant deviation of anomalous motion from typical values, aiding in the identification of unusual activity.

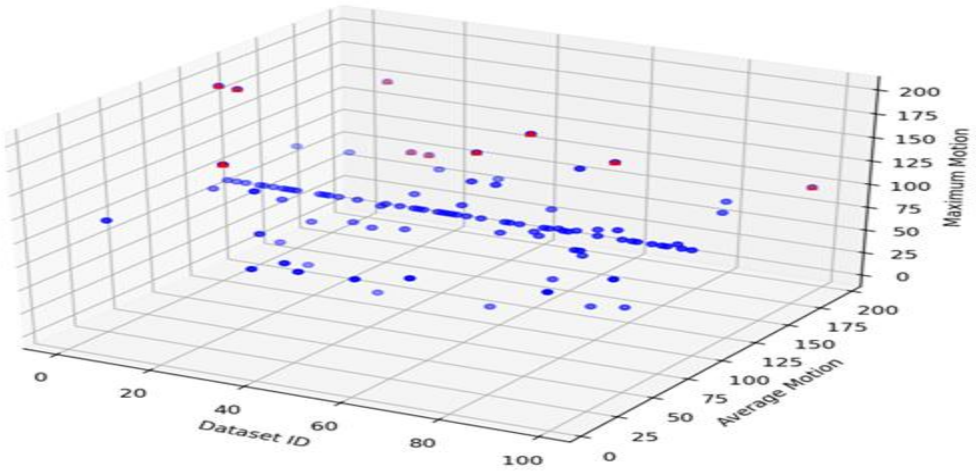

Figure 4.1: shows 3D Visualization of motion Data with Anomalies Highlighted

Data visualization aid in detection of an intelligent alarm system alarming to prevent theft and vandalization occurring within the Administrative building at Polytechnic. The pair plots shown Figure 4.2 payoff is seen only when plotting across the different security metrics and finding insights in, or uncovering relationships between motion, access points, or timestamps. By plotting these relationships, the pair plot enables us to see groups or patterns that might suggest alternative types of behavior, potentially indicative of intrusions. For example, the odd motion behaviors or logins to abnormal hours may imply some unauthorized activity. Such visual insights help the ID system to raise anomalies and alarms for effective working of overall intrusion detection system, When developing a smart intrusion detection and alarm system to prevent theft and vandalism attacks at the Polytechnic Administration's facility, understanding motion patterns is crucial as it enables the reliable identification of security breaches. The average motion and maximum motion exhibit a weak negative correlation, with the correlation coefficient from a motion data analysis being approximately -0.0805. This indicates that having a higher average motion is not a reliable predictor of maximum motion. A low R2 value of 0.0065 also tells us that the linear model accounts for very little of the variance in the data, so we establish almost no linear dependence between average and maximal movement as shown in Figure 4.3. Moreover, the p-value is not statistically significant, indicating that this correlation could be casual and there might not be any meaningful connection at all.

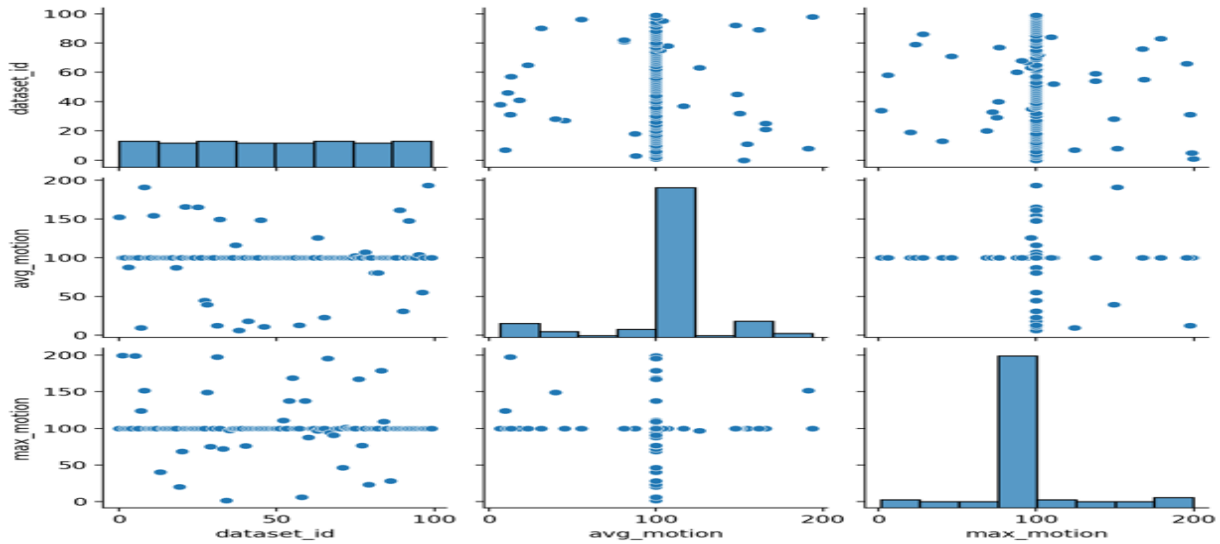

Figure 4.2 shows: Pair plots matrices among the security cameras

LGJDX
ISSN No: 1008-0562
Journal Of Liaoning Technical University
Natural Science Edition

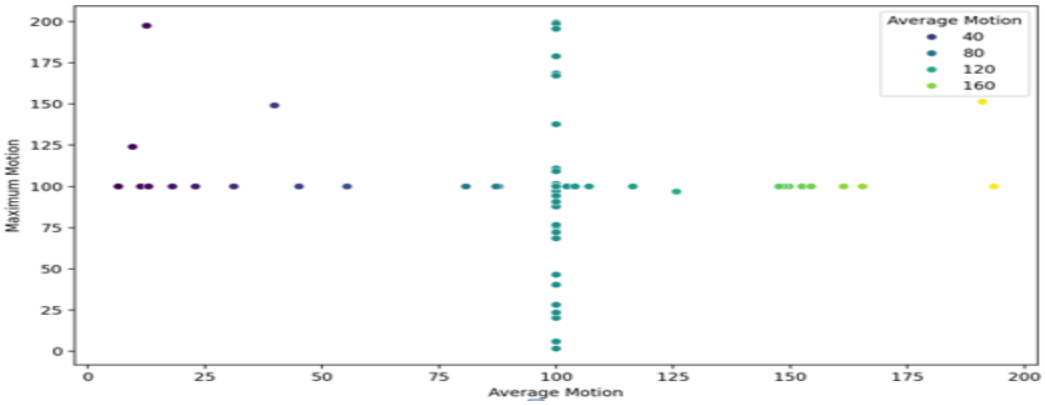

Figure 4.3: Relationship between Average Motion and Maximum motion

5 Conclusion

The Polytechnic Administrative Building now has a sophisticated intrusion detection and alarm system that we created that incorporates Internet of Things devices. This system represents a substantial enhancement in campus security, integrating an IoT-based methodology, machine learning algorithms, and blockchain technology to tackle the principal concerns of theft and vandalism. The study's notable findings encompass the full integration of inside and outside monitoring functionalities to deliver a holistic security solution. This encompasses the utilisation of high-definition cameras, sophisticated facial recognition technology, and infrared sensors to improve intruder detection. Furthermore, machine learning algorithms aggregate data from many sources to swiftly detect anomalies and risks. The incorporation of tamper devices improves the security of the equipment. The data analysis indicated that roughly 10% of the points were anomalies, validating the system's precise identification of anomalous conduct. Nevertheless, the evidence for a correlation was tenuous, and a negative correlation between average and maximum motion suggested a significant probability of potential incursion scenarios. The implementation of this advanced security system not only reduces the risk of burglary and vandalism but also underscores Copper Spring's commitment to use state-of-the-art technology for community safety.

6. Recommendations

It is therefore recommended that the Polytechnic deploy the smart intrusion detection and alarm system first in phases starting from high-risk zones of the administrative building where below 70% will allow for further customization before a complete scale out. Create a process for service updating the system software and machine learning algorithms periodically, so that the

system is even more efficient to respond to new situations of security threats. Due to this, effective staff training is needed for the operation of the system and maintenance while maintaining seamless integration with current security protocols thereby enforcing a unified security framework. Fail-safe methods of data protection must be implemented for privacy and regular monitoring of the performance of the system carried out to determine what needs to be improved in order to ensure that it is maintained with time. The scalability planning must extend the system to other buildings on campus based on lessons learned from this implementation. Collaboration between IT, Security Staff and Administration to make sure the system is meeting the needs of all parties involved and integrating your system with local law enforcement and other emergency services for faster response times in case of a serious security breach. Finally, hold some user awareness programs for students and staff to promote cooperation and understanding of the new measures in security. By following these steps, the Polytechnic can ensure that the system works most effectively to protect the academic community.

References

Ajala, J., & Saini, G., (2020). Cloud-IOT Based Smart Villa Intrusion Alert System. 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), 1326-1329. https://doi.org/10.1109/ICRITO48877.2020.9198022.

Mustafa, P., Asraf, S., & Idrus, S. (2020). Implementation of Intrusion Detection System for Smart Home. Journal of Physics: Conference Series, 1529. https://doi.org/10.1088/1742-6596/1529/3/032077.

Mohammed, I., Ikerionwu, C., & Chinenye, C. (2020). Re-engineering Real-time Intrusion and Burglary Detection using Fuzzy Technique. International Journal of Computer Applications. https://doi.org/10.5120/ijca2020920079.

Vinayakumar, R., Alazab, M., Soman, K., Poornachandran, P., Al-Nemrat, A., & Venkatraman, S. (2019). Deep Learning Approach for Intelligent Intrusion Detection System. IEEE Access, 7, 41525-41550. https://doi.org/10.1109/ACCESS.2019.2895334.

Kanthaseelan, K., Pirashaanthan, P., A.A.P, J., Sivaramakrishnan, A., Abeywardena, K., & Munasinghe, T. (2021). CCTV Intelligent Surveillance on Intruder Detection. International Journal of Computer Applications. https://doi.org/10.5120/IJCA2021921035.

Park, J., Chen, J., Cho, Y., Kang, D., & Son, B. (2019). CNN-Based Person Detection Using Infrared Images for Night-Time Intrusion Warning Systems. *Sensors (Basel, Switzerland)*, 20. https://doi.org/10.3390/s20010034.

LGJDX
ISSN No: 1008-0562
Journal Of Liaoning Technical University
Natural Science Edition