SIMS: SMART IOT-BASED MONITORING SYSTEM WITH CCTV SURVEILLANCE, RFID-BASED INVENTORY MANAGEMENT, AND WIRELESS ALARM SYSTEMS

Edmon O. Fernandez
Electonics Engineering Department
edmon_fernandez@tup.edu.ph

Angela Denise P. Alcantara
Electronics Engineering Department
angeladenise.alcantara@tup.edu.ph

Alvin Kenneth A. Cabanlit
Electronics Engineering Department
alvinkenneth.cabanlit@tup.edu.ph

Ma. Celine V. Grecia
Electronics engineering Department
maceline.grecia@tup.edu.ph

Reynald B. Minguez
Electronics Engineering Department
reynald.mingues@tup.edu.ph

Vincent Paulo D. Soriano
Electronics Engineering Department
vincentpaulo.soriano@tup.edu.ph

***Abstract*- In an era marked by rapid technological advancement, the integration of Internet of Things (IoT) solutions has transformed various aspects of modern living. This abstract introduces the Smart IoT-Based Monitoring System (SIMS), a comprehensive and versatile system designed to enhance security, inventory management, and alarm systems through a combination of cutting-edge technologies. SIMS incorporates CCTV surveillance, offering real-time monitoring and surveillance capabilities to ensure the safety and security of diverse environments, such as residential spaces, industrial facilities, and commercial establishments. This component employs high-definition cameras and advanced video analytics for improved situational awareness and proactive threat detection. Furthermore, SIMS integrates Radio-Frequency Identification (RFID) technology for efficient inventory management. By employing RFID tags and readers, the system automates inventory tracking, reducing human error and streamlining stock control processes. This facilitates real-time inventory visibility, aiding businesses in optimizing supply chains and minimizing operational costs.**

Keywords: Internet of Things, security systems, CCTV Surveillance

I. INTRODUCTION

Security is one of the topmost concerns of every corporation, establishment, community, and even of a single household. In the past decades, there has been a vast number of continuous research discoveries that concentrate on improving and ensuring the safety of a particular locale. There are various security devices and systems that cater to the need for the preservation of safety. For instance, the installation of CCTV cameras in different locations for 24-hour monitoring, the use of home security doorstep alarms to prevent burglary or unauthorized access, and the exploitation of other innovative means to secure properties and resources to look after a specific place.

Similarly, educational institutions like the Technological University of the Philippines- Manila experience the challenge of guaranteeing the safety of its facilities and valuable possessions. For the past years, the establishment has encountered damage and loss of properties particularly in its laboratory facilities. Today, the TUP College of Engineering Room 5 has several newly-acquired and expensive engineering apparatuses that demand improved supervision and safekeeping. Thus, the incitement of the plan to build up an Internet of Things-based security and control system, which can give authorized users a moment update about the room, send an electronic warning lest of emergencies and provide remote access to the network of devices inside.

II. RELATED STUDIES

IoT-based Smart Home Security System with Alert and Door Access Control using Smart Phone

In 2016, S. Anwar et al. , developed a low-cost system to monitor the home remotely using a smartphone. The system could detect an intruder and capture his image using a PIR motion sensor and PiCamera, respectively. Also, the system comprises a relay driver to control the electromagnetic door lock, and a loudspeaker system to enable voice alert. All these devices are interconnected to a Raspberry Pi set up for storage of the captured image in an SD card. For the sending of email notification to the user, SMTP software was used. The python script is the command language adopted for SMTP software and other devices like the door lock. For the voice alert, the user sends a Linux command through the Internet, which stimulates the voice alert. SSH Client is used to transmit the instruction, which is implemented on the android platform using JavaScript.[1]

Physical Security and Its Importance

All individuals have possessions that are important enough to be secured and preserved. In a more comprehensive outlook, organizations have relatively more abundant assets to supervise and protect. At present, properties can be in the form of digital information or material goods. However, most organizations focus on "technology-oriented security countermeasures" to defend their assets from cyber-attacks (Harris, 2013), while unknowingly overlooking how equally critical the safety of physical assets is. In view of this, the importance of physical security is thoroughly discussed in a literary journal by

David Hutter, entitled Physical Security and Why It Is Important, in 2016. [2]

Security and Alarm Systems

In 2012, Mansour Assaf et al. developed a home control and security system based on Field Programmable Gate Array (FGPA), where the user interacts directly with the system through a web-based interface. It allows the user to monitor the entry points of his house and receive an alerting email in the event of any breach. Additionally, the system can send control demands some appliance like the air-conditioning units and obtain feedback from different peripherals. [3]

IoT-based Home Security and Automation System

In 2016, Kodali et al. concentrated on creating a prototype that would secure a house from any unauthorized access. The user can receive alerts over voice calls in his/her mobile phone if there is a presence of an intruder. The team used a TI-CC3200 Launchpad board that comes with an embedded micro-controller and an on-board Wi-Fi shield. The prototype does not require a smartphone connected to the internet for access and control functionalities to the appliances at home. The system works as the PIR sensor detects motion. Only then will the Launchpad alert the user through a phone number coded in the program. Every appliance has an assigned number for remote control. For example, digit number 1 is assigned for the lights. In case of intrusion, turning them on could warn that intruder that he is being watched.[4].

CCTV Surveillance System

CCTV is top-of-mind technology when it comes to security systems. CCTV is a situational crime prevention (SCP) scheme where degrees of formal surveillance are amplified within a defined area (Cornish & Clarke, 2003; Welsh & Farrington, 2009)[5]. A study by Piza et. Al, in 2019, exhibits a 40-year systematic review of CCTV surveillance using meta-analysis. The results of this review disclose that CCTV is correlated with a substantial and modest decline in crime. Although the most significant and unswerving effects of CCTV were observed in car parks, the review also provides evidence of considerable crime reductions within other settings, especially residential areas. This systematic review is beneficial to this project for it authenticates the efficiency of visual protection systems and adds support to the continued use of CCTV systems.[6]

School-based Crimes

This project aims to develop the security system of a particular room in an educational establishment. Thus, it is just fitting to take account of crime statistics of schools, starting from petty misconducts like vandalism, damaging or defacing of school properties to more serious offenses like burglary, felony, and theft. In a whitepaper written by Tom Stiles, he fairly concurs with the idea of integrating new technologies with present security systems in order to better guard campuses and other private institutions. As the executive director of Identification Systems Group, he made a strong point on the custom of ID Badging. Identification cards are used to visually recognize people entering/leaving a particular place. The wearing of IDs is required in most school campuses, which could empower the deployed ID registration systems. Furthermore, he mentioned the implementation of other identifications and safety systems as well, like door access control systems, video surveillance systems, and electronic tracking systems.

III. METHODOLOGY

A. Software Development

RFID Detection

As mentioned before, the existing school IDs of the faculty members and students will be brought into play. Two units of RFID readers will be installed (one at the entrance and one inside the room). The entrance RFID reader is responsible for room access profiling, while in-house RFID reader will take on the tracking and inventory-keeping of available equipment.

Image Processing

In this feature, OpenCV will be used for the image processing to be used as a people counter. Upon entering the area, the system will start accessing surveillance data to start the counting process.

Development of a MySQL Database for Access and Control

In this project, MySQL will be employed to manage the database. The streamlining of multiple processes or doing multitasking is a lot of work for physical systems, and it will require more computing power. Thus, the use cloud computing technology to process gathered data, control smart switches, and display statistical and informative data is of great contribution.The database will be used to store surveillance data from the CCTV system to document in-and-out access history, to record any irregular activity (lost instruments, fire detection, etc.), to transmit commands (smart switch controls), and to send room availability notifications.

Operational and Testing Procedure

The competence and effectiveness of this project will be based on three factors, namely, the functionality, accuracy, and integrity of the system. To ensure a state-of-the-art product, the researchers would like to conduct a series of tests before deploying the system to see if it responds to every control and process that is being run, following the right order of commands. Some of the systems need specialized planning and methodical installation; thus, the purpose of this section is to highlight the pre-installation quality check procedure.

First on the list is to run a test for the CCTV system, including the connection stability between the server and the mobile application. Here, the researchers would like to see if the surveillance footage can be viewed on the mobile application, as well as if the image processing for counting people is continuous while displaying real-time surveillance.

Next is the functionality of the RFID system. As we know it, RFID technology corresponds to the use of electromagnetic fields. With this, the researchers would want to make certain that the RFID readers are smart enough to identify whether the detected radio waves are real or just some random radio waves. The researchers would also want to observe how fast the RFID antennas can work on different detection operations, such as blind spots and alarm protocols.

Further, the testing of installed sensors in the system is also a must. In this case, the researchers are expecting a 95-100% functionality and accuracy rating from the sensors to prove that they will work as intended. This includes experimenting with the smart response, which will inform and notify the mobile users of the system during predetermined incidents.

Then comes the functionality of the mobile application. This comprises a stress test to see if the system can manage network traffic. Plus, bug testing for the mobile application. This includes functionality testing, communication error testing, missing command errors, syntactic errors, handling errors, calculation errors, and control flow errors. The researchers expect to get an average rating of 90–95% so that patches to fix errors can be applied.

Lastly, the test for the security of the system itself will also be done. The researchers themselves would like to perform security breaches to look for loopholes and identify weak points in the network so that countermeasures can be executed. The results of the following tests will be evaluated statistically, and expects to get an average of 90% confidence throughout the working system.

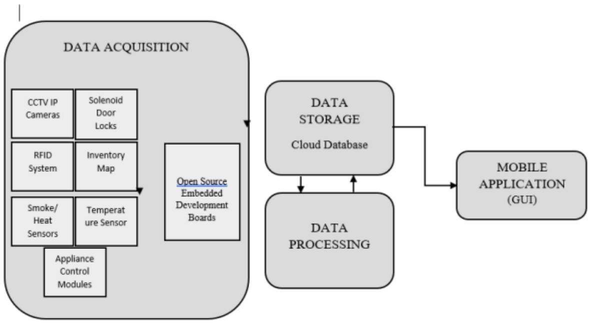


Figure 1 Network System Block Diagram

B. Hardware Design

The representation below denotes the physical characteristics of the system proposed in the study. It comprises the proposed security and control systems. Because this project is a system of systems, the following illustrations show the individual systems as well.

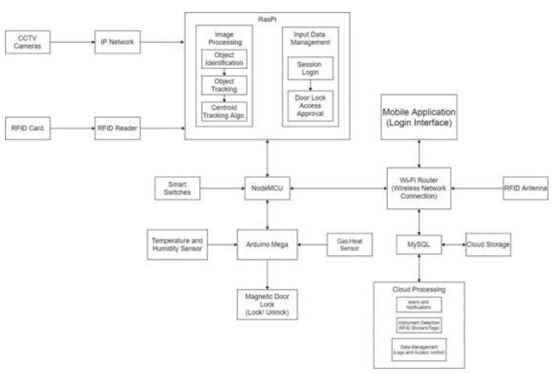


Figure 2 Project Flow Diagram

C. Design Considerations

The proposed network of systems will be installed in and around the TUP-COE Room 52. In the intent of preserving the physical integrity and aesthetics of the room, the proponents will use modular circuits and easy-to-install devices. All sensors/detectors will work with open-source embedded development boards like Arduino and NodeMCU, to send input data wirelessly to the router. The control of some appliances will be done by connecting mechanism modules along electrical wires or in utility boxes. The RFID readers will be installed at the entrance and inside the room to keep track of the occupants and equipment borrowers' information. School RFID tags of students and faculty members will be registered to the system, while modified RFID tags will be attached to each equipment. The surveillance system, unlike everything else, will require IP cables running in the walls of the room for the supply of power and transmission of the video signal into the Digital Video Recorder located in a secured room. Additionally, the gathered data from some of these systems, like CCTV footages will be sent to a local hard drive to keep the data physically documented. Above all, the systems mentioned will possess an independent power supply, especially for the electronic modules to continue operating even after school hours.

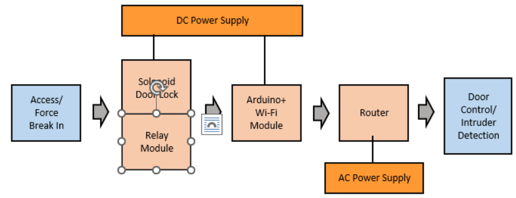


Figure 3 Door Lock System Overview

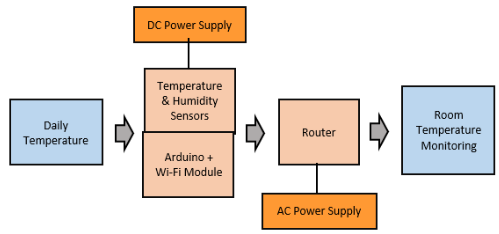


Figure 4 Temperature/Humidity System Overview

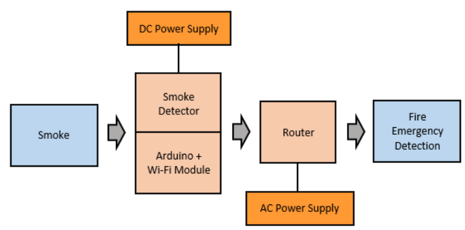
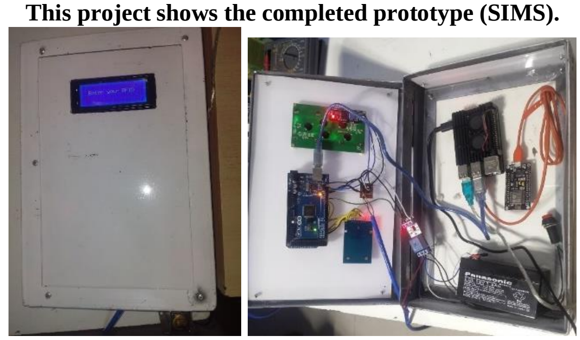


Figure 5 Smoke Detection System Overview

IV. TESTING AND DATA ANALYSIS

This project shows the completed prototype (SIMS).

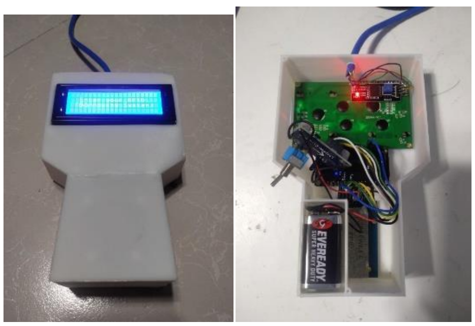


Figures 6 and 7 Front and inside view of the front panel of SIMS.

Figures 6 and 7 show the actual front panel's front and inside view. The prototypes' dimensions are measured at 8.3 inches x 2 inches x 12 inches. The frame is made with steel and chassis are made from acrylic. The front panel is installed with a 12V battery that serves as backup power for any power outage.

Figures 8 and 9 Smoke detectors and Temperature/humidity sensors of SIMS.

Figures 8 and 9 show the actual smoke detectors and temperature or humidity sensors. The prototype's dimensions are measured at 4 inch in diameter and 2.1 inch in height. It is 3D printed PLA+ plastic for the chassis.



Figures 10 and 11 Actual front and inside view of the borrower's device of SIMS.

Figures 10 and 11 show the actual borrower's device RFID. It is 3D printed PLA+ plastic for the chassis.

Figure 12 Actual 3d view of enrollment device of SIMS.

Figure 12 shows the actual enrollment device. It is 3D printed PLA+ plastic for the chassis.

Iteration Number	Measured Temperature (S1)	Measured Humidity (S1)	Measured Temperature (S2)	Measured Humidity (S2)	Actual Temperature (°Celcius)	Actual Humidity (% Relative Humidity)	Average of Measured Temperature	Average of Measured Humidity	Percentage Error	Performance Accuracy	Remarks
1	35.8	63.4	35.1	62.2	34.8	50	35.45	62.8	2%	98%	GOOD
2	36.4	62.2	35.4	61.6	34.5	49	35.9	61.9	4%	96%	GOOD
3	36.8	61.5	35.6	61.2	33.1	53	36.2	61.35	9%	91%	GOOD
4	37.1	60.7	35.7	61.1	32.9	54	36.4	60.9	11%	89%	GOOD
5	37.3	59.8	35.8	61.1	32.9	55	36.55	60.45	11%	89%	GOOD
									7%	93%	

Table 1 Temperature/humidity alarm system data

The table above shows the data regarding the accuracy of the alarm system detection. It is composed of sensors 1 and 2. The actual data is measured using temperature and humidity reading device which serves as actual data reference for the device readings. In the table we can see that the readings have a percentage error of 7%, here it is considered acceptable and will be purely based on the environmental conditions of the time wherein the actual measurements took place. The following data results in a 93% accuracy of the overall device.

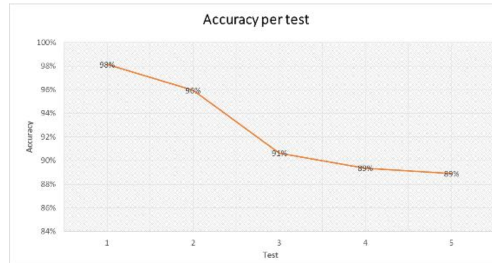


Figure 6 Temperature and humidity detection accuracy per test graph

The graph in figure 6 shows the accuracy of the devices measured over the series of tests. It is observed that through time that devices are activated the results are showing a decrease in accuracy which can be improved by upgrading the temperature/humidity sensors power management to eliminate the factors affecting the reading of the device.

Iteration Number	Actual Number of People Present	Number of People Reflected on the Mobile App	Percentage Error	Detection Accuracy	Time difference between data is presented by the mobile application VS direct image processing (Theoretical)	Time difference between data is presented by the mobile application VS direct image processing (Experimental)	Percentage Error	Performance Accuracy
1	3	2	33%	67%	15	20	33%	67%
2	3	3	0%	100%	15	20	33%	67%
3	3	1	67%	33%	15	30	100%	0%
4	3	3	0%	100%	15	20	33%	67%
5	3	1	67%	33%	15	40	167%	-67%
			Detection Accuracy:	67%			Response Time Rating:	27%

Table 2 People counter table

Table 2 shows the data of people counter. The test includes number of people present within the secured area and measures its detection capability and the mobile application's response to the detected number of people. 5 Tests were conducted to calculate the devices capability to process its detection capability. During the tests, out of 3 people, 2 tests detected the correct amount of people present, 1 test detected 2 people and 2 tests detected only 1 person. This resulted for a detection accuracy of 67%.

The 6th and 7th column are the tests for the system's response time to display the correct number of people detected which resulted to 27%.

Iteration Number	Actual Number of Equipment	Number of Items Detected	Detection Accuracy	SMS Alert after Detection (sec) (Theoretical)	SMS Alert after Detection (sec) (Experimental)	Percentage Error	Performance Accuracy	Remarks
1	1	1	100%	1.5	2	25%	75%	GOOD
2	1	1	100%	1.5	2	25%	75%	GOOD
3	1	1	100%	1.5	3	50%	50%	GOOD
4	1	1	100%	1.5	2	25%	75%	GOOD
5	1	1	100%	1.5	3	50%	50%	GOOD
		Detection Accuracy Rating:	100%			Response Time Rating:	65%	

Table 3 device UHF RFID-based object detection

The table above shows the accuracy of UHF RFID-based object detection capability of the system with 1 device. The data shows that 1 device detection can be detected accurately but shows a significant delay within the systems response resulting to a 1 to 2 second delay.

Iteration Number	Actual Number of Equipment	Number of Items Detected	Detection Accuracy	SMS Alert after Detection (sec) (Theoretical)	SMS Alert after Detection (sec) (Experimental)	Percentage Error	Performance Accuracy	Remarks
1	2	2	100%	3	5	40%	60%	GOOD
2	2	2	100%	3	8	63%	38%	GOOD
3	2	2	100%	3	5	40%	60%	GOOD
4	2	1	50%	3	1	100%	0%	GOOD
5	2	2	100%	3	8	63%	38%	GOOD
		Detection Accuracy Rating:	90%			Response Time Rating:	39%	

Table 4 devices UHF RFID-based object detection

The table above shows the accuracy of UHF RFID-based object detection capability of the system with 2 devices. The data shows that 2 devices detection wherein out of 5 tests only 1 test has detected 1 device, this gives a detection accuracy of 90%. The response time of the system to process took a significant amount of time. This is mainly due to the processing power of the device.

Iteration Number	Actual Number of Equipment	Number of Items Detected	Detection Accuracy	SMS Alert after Detection (sec) (Theoretical)	SMS Alert after Detection (sec) (Experimental)	Percentage Error	Performance Accuracy	Remarks
1	3	2	67%	9	9	100%	0%	GOOD
2	3	3	100%	9	15	40%	60%	GOOD
3	3	1	33%	9	9	100%	0%	GOOD
4	3	2	67%	9	9	100%	0%	GOOD
5	3	3	100%	9	20	55%	45%	GOOD
Detection Accuracy Rating:			**73%**			Response Time Rating:	**21%**	

Table 5 devices UHF RFID-based object detection

The table above shows the accuracy of UHF RFID-based object detection capability of the system with 3 devices. The data shows a significant decrease in performance. Out of 5 tests only 2 accurately detected the 3 devices which gives a total of 73% detection accuracy rating. The response time it took to detect the 3 devices took a significantly longer time than the previous tests. This proves that processing power is the main factor affecting the devices response in detection.

V. CONCLUSION

Based on the gathered data, outcomes of the tests conducted and the analysis of findings the following statements were inferred:

1. The system only utilized 4 GB RAM, 1.5 GHz. Quad- Core Raspberry Pi, which turned out to be insufficient if all subsystems were activated simultaneously. It can manage to continue operating, with an apparent compromise in the processing speed. Hence, the decrease in accuracy rating.
2. The prototype was deployed at an alternative location, which became a limiting factor in terms of internet speed. The project, being an IoT-enabled system of systems, purely depends on its connection to the internet. Thus, the decline in its precision rating.
3. Wireless devices require wireless supply of power. The alarm modules in this project only used 9V batteries, which easily depletes over time. This also incurs periodical battery change.
4. The entire system is designed to be implemented at TUP-COE Room 52, including the back-up power supply. But due to unforeseen events, the researchers used an alternative location, compromising quite a few features of the study.

REFERENCES

[1] Anwar, S., & Kishore, D. (2016). "IOT based Smart Home Security System with Alert and Door Access Control using Smart Phone." Volume 5(12), 504–509.

[2] Hutter, D. (2016). “Physical Security and Why It Is Important.” SANS Institute InfoSec Reading Room. Retrieved from https://www.sans.org/reading-room/whitepapers/physical/physical-security-important-37120

[3] Assaf, M. H., Mootoo, R., Das, S. R., Petriu, E. M., Groza, V., & Biswas, S. (2012). "Sensor-based home automation and security system." In IEEE International Instrumentation and Measurement Technology Conference (I2MTC), 2012

[4] Kodali, R. K., Jain, V., Bose, S., & Boppana, L. (2016). "IoT-based smart security and home automation system." In 2016 International Conference on Computing, Communication and Automation (ICCCA) (pp. 1286–1289). https://doi.org/10.1109/CCAA.2016.7813916

[5] Cornish, D. B., & Clarke, R. V. (2003). "Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention." Crime Prevention Studies, 16, 41-96.

[6] Welsh, B. C., & Farrington, D. P. (2009). "Public area CCTV and crime prevention: An updated systematic review and meta-analysis." Justice Quarterly, 26(4), 716–745. https://doi.org/10.1080/07418820802506206

[7] Piza, E. L., Welsh, B. C., Farrington, D. P., & Thomas, A. L. (2019). "CCTV surveillance for crime prevention: A 40-year systematic review with meta-analysis." Criminology & Public Policy, 18(1), 135-159.