iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** V **Month of publication:** May 2021

DOI: https://doi.org/10.22214/ijraset.2021.34741

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue V May 2021- Available at www.ijraset.com

App-Controlled Smart Anti-theft Security System for Studio Type Condominium Units

Alva John T. Lacuesta
MIT – 1, Northern Negros State College of Science and Technology

Abstract: ***Small studio-type condominium units are often the victim of unorganized thefts and burglaries. Even with CCTV cameras and security guards, criminals can still get away with their crime. The installation of a small security system which can detect and record intrusions and alert security can help stop these crimes while they are in progress. The ability to control the system through Internet gives the user different options depending on the nature of the intrusion. The user also has the choice to remotely take a picture to monitor their room, disable the system when they or someone they know is about to enter, or shutdown the system should they wish. Although the apps Pushbullet and MyMQTT, which are used to receive pictures and send commands respectively, are available publicly, the use of API tokens for Pushbullet and username/password authentication for MyMQTT function as a layer of security to anyone who tries to bypass the system.***

I. INTRODUCTION

A. Background

Multi-unit residences are increasingly becoming more common. A census by the Philippine Statistics Authority in 2015 revealed that 11.9 percent of the Philippine populace live in multi-unit residences, the second highest percentage after those living in single houses. The close proximity to urban areas, availability of amenities, and low maintenance cost compared to whole homes make condominiums more attractive to fresh workers entering the workforce than house and lot deals. Unfortunately, there is a common misconception of a false sense of security that burglaries would rarely happen in a condominium building because of the presence of security measures such as access control and even a door man. In actuality, condominium theft remains one of the top 10 modus operandi of common crimes in the Philippines. The thieves look for rooms left unlocked, or simply break in. Once inside, they ransack the unit for money and other valuables. While most high-end condominium units come equipped with advanced security measures such as access control, perimeter security and CCTV, and intruder alarms, these systems are only normally present in high-end luxury condominiums with a price tag to match. Plenty of condominium units which are targeted by the aforementioned fresh workers make do with scarce CCTV coverage and security guards only at the entrance to the building. Once a thief manages to enter a room and help themselves to whatever is inside, there is very little preventing them from just walking out of the building, particularly since security guards tend to be more watchful of people entering than those leaving.

B. Statement of the Problem

1) What app-controlled anti-theft smart security is applicable for small condominium units?
2) What will be the design of an effective security system that is accessible, has visual aid, and controllable via internet?
3) What is the response rate and reliability of the system when it comes to motion detection and commands?
4) What is the runtime of the security system in which it can effectively function?

C. Conceptual Framework

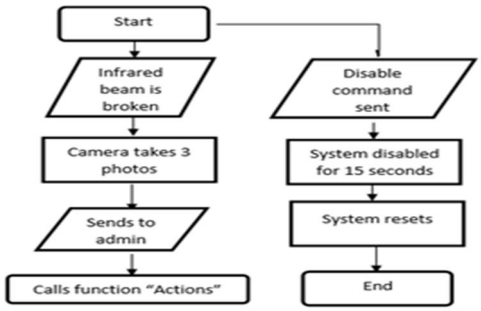


Fig. 1 A flow chart showing the process flow of the smart security system. This shows the step by step functions that occur in the system

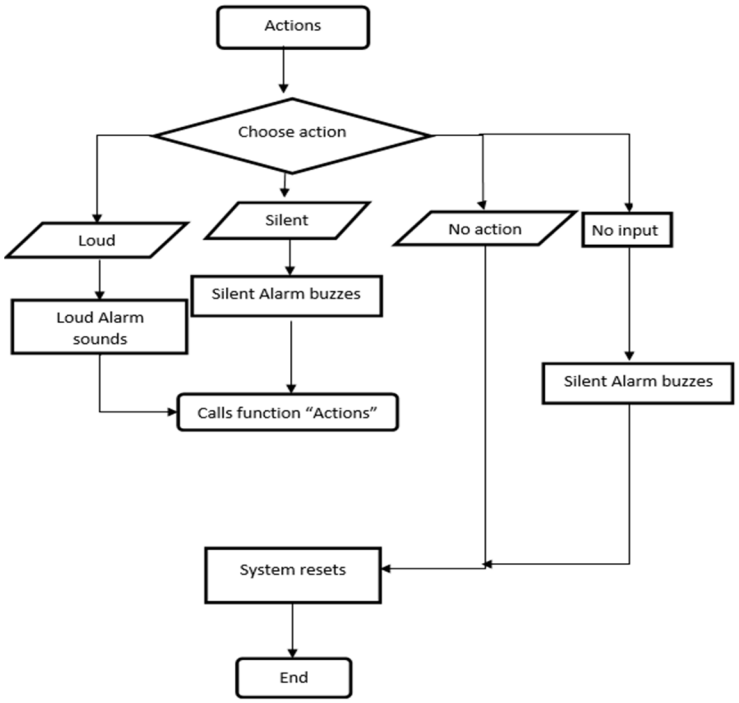


Fig. 2 The flow chart of the function "Actions". This flow chart occurs within the application and shows the output of the choices.

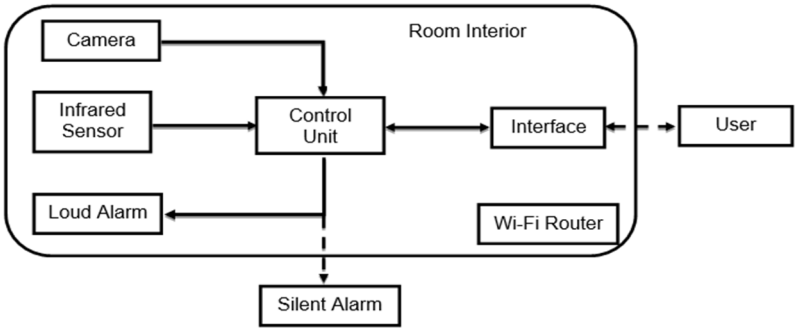


Fig. 3 Block diagram of the whole system. This diagram shows how the devices are interconnected in the system.

D. Scope and Limitations

The system contains only one infrared sensor and one camera, because it is meant to be used for a small area, preferably a small condominium unit. Most multi-unit residential buildings are also high-rise buildings, with the living units placed 2 or more floors above ground level. As such, the researcher assumes that an entrance through the windows will be impractical for intruders, and that they can only enter through the front door. Another limitation of the system is the reliance on an Internet connection to communicate with the user. If it is unavailable to the system or the user, the system will be unable to send notifications or receive commands. Due to the prevalent use of mobile data in smart phones, as well as the reliability and stability of Wi-Fi connections, an assumption is made that cases where there is no Internet connection will be few and far between, and therefore not covered by the system. The system does not contain any components designed to contain any intruder in the room. The system operates under the assumption that at least one security guard or equivalent building security personnel is present at their post at all times. The system itself contains no restraining ability, and a timely response from the appropriate authorities will be key to catching intruders.

Finally, the system is meant to be a portable, easily installed security system. As such, it does not have an auxiliary power supply, as that will add to the total weight of the system. High rise residencies tend to be located in well-urbanized cities; as such, the researcher made the assumption that the building is connected to a stable power grid, or has its own auxiliary power supply such as a generator.

E. Review of Related Literature

In the patent of Ronald E. Pyle (1984) entitled "Home Security System", the main concept is about notification and intrusion or disturbance detection. In the case of an intrusion or disturbance, the monitoring unit will receive electronically transmitted signal and automatically activates the alarm or will be transmitted a coded radio frequency in which the monitoring unit can manually activate the alarm. This system can be used for more than one or multiple entrances for security monitoring efficiency. This is relevant to the study as it is similar to what the researcher is studying, which is the usage of sensors and the possible automatic or manual activation of alarm through the monitoring device.

In the patent of Milton O. Smith (1992) entitled "Infrared Alarm System", A battery-powered infrared sensor security system capable of operating on a single set of batteries for a minimum of one year. The system is connected to a telephone line and employs a bidirectional dual-tone multiple frequency (DTMF) tone generator/receiver to allow communication to and from a remote location. The system status may be checked from the remote location and certain system parameters may be varied from the remote location. The system uses a Fresnel lens arrangement and a pair of infrared sensors to provide a substantially uniform field of coverage of 180°. The system also uses real time digital analysis of the output signals from the infrared sensors. The digital analysis uses time sequence analysis of the output signals, performs variance measurements between the current measurement of the infrared sensor signals and the stored time sequence, coherence measurements between the two sensors, and can compare measured amplitude spectra to predefined signature spectra entered by the user.

In the patent of Makoto Kodaira entitled "Infrared intrusion alarm system capable of preventing false signals" it focuses on an alarm device responsive to entering or trespassing comprising:

1) A sensor circuit, including an infrared ray sensor, producing an output having positive and negative peaks based on outputs of said sensor being produced when a target to be sensed passes within the region of vision monitored by said sensor,

2) A level detecting circuit comprising a first detector producing an output when the positive peak of the output fed from said sensor circuit exceeds a predetermined level, and a second detector producing an output when the negative peak of the output fed from said sensor circuit exceeds a predetermined level,

3) A timer circuit comprising a first timer producing an output which continues for a predetermined time interval or above from a time at which the output of said first detector is produced, and a second timer producing an output which continues for a predetermined time or above from a time at which the output of said second detector is produced,

4) An AND circuit comprising a first circuit producing an output when there exists an output of said first timer and the output of said second detector at the same time, and a second circuit producing an output when there exists an output of the said second timer and the output of said first detector at the same time, and

5) An output circuit responsive to the output of said AND circuit to produce an alarm signal.

In a patent by Lin Kao entitled" Infrared Intrusion Alarm System" An improved dual-sensor infrared intrusion alarm system includes a motion discriminator that renders the system responsive to only radiation-emanating objects that are moving through the system's scope of surveillance. A positive or negative sensor signal is developed depending on the relative amounts of radiation impinging on the sensors. A switching amplifier selectively discharges one of two capacitors depending on the polarity of the sensor signal. The voltages across the capacitors are coupled to the inputs of a voltage comparator and the capacitor recharge time constants are selected so that an alarm is indicated only when the length of the time interval between the occurrence of a sensor signal of a given polarity and the subsequent occurrence of a sensor signal of the opposite polarity is within prescribed limits, for example, two seconds.

In a patent by Arnold St. J. Lee entitled "Home Medical Surveillance System" it explains that many subscriber patients are served by this system. In each patient's home is an apparatus that includes special furniture on which the patient lies and sits, and embedded in which are devices that automatically sense multiple parameters related to the patient's health. The patient cooperates only passively. The parameters are so chosen--and are sufficiently numerous and accurate--as to provide in the aggregate a comprehensive profile of the patient's general state of health. The apparatus also generates electronic health-parameter signals related to the sensed parameters, and it transmits these signals from the patient's home to a central surveillance and control office. Equipment there receives the signals, displays corresponding indicia of the parameters, and transmits control signals back to the patient's apparatus. Two-way voice communication between the patient and a highly trained observer at the central office supplements the electronic measurements. The observer conducts routine diagnostic sessions except when an emergency is noted from these sessions or from a patient-initiated communication. The observer determines whether a nonroutine therapeutic response is required, and if so, facilitates such a response. Selection among emergency cases follows a highly refined emergency-priority hierarchy.

In a patent by Carl Snyder entitled "Door Alarm and Method of Use" The present invention relates generally to a personal door alarm and more specifically to a battery powered door alarm that can be easily transported from location to location, can be installed on most door knob assemblies and is simple to deploy. The personal door alarm provides protection for valuable property and to the occupants of the habitation.

In the study of Yanbo Zhao and Zhaohui Ye (2008) titled "A Low-Cost GSM/GPRS Based Wireless Home Security System", they developed a design which uses GSM/GPRS based wireless home security system. The designed they implemented has low cost and power consumption and uses three wireless security sensors which are door security, infrared security and fire alarm nodes. This is relevant to the study because almost all or majority of the people as of today uses wireless devices such as mobile phones and such and through such devices the researcher can monitor our homes more efficiently.

In the study of Rajeev Piyare (2013) entitled "Internet of Things: Ubiquitous Home Control and Monitoring System using Android Based Smart Phone", the main concept is the use of a micro-web server and the usage of wireless controlling devices which uses android based Smart phone app. The system which was implemented in this study has low cost and flexible home control and monitoring system. It does not require a dedicated server PC and offers monitor and control over home environment due to devices such as light switches and temperature sensor which was integrated in the system. This is relevant to current study as our research is based on the "Internet of Things" category and mainly the researcher will use app-based security system with the use of a common open-source platform such as Arduino.

In the study of Andy Stanford and Hong Linh Truong entitled "MQTT For Sensor Networks Protocol Specification", the purpose of this document is to specify MQTT-SN, a pub/sub protocol for wireless sensor networks. MQTT-SN can be considered as a version of MQTT which is adapted to the peculiarities of a wireless communication environment. Wireless radio links have in general a higher failure rates than wired ones due to their susceptibility to fading and interference disturbances. They have also a lower transmission rate. For example, WSNs based on the IEEE 802.15.4 standard provide a maximum bandwidth of 250 Kbit/s in the 2.4 GHz band. Moreover, to be resistant against transmission errors, their packets have a very short length. In the case of IEEE 802.15.4, the packet length at the physical layer is limited to 128 bytes. Half of these 128 bytes could be taken away by the overhead information required by supporting functions such as MAC layer, networking, security, etc.

In the study conducted by John S. Usher entitled "How to Determine System Reliability", there is a wide variety of issues that should be addressed when talking about material handling system reliability. Some of the most important are:

a) To define "failure." This is the key issue, and for many systems, it is also very difficult. Consider a light bulb; we know when it fails, and we could even (fairly easily) measure the time to failure. But what about a complex material handling system. When is it "failed?" For example, consider a 5-vehicle AGVS; if a single vehicle fails, is the system failed? Or a 5-ailse AS/RS; if one crane goes down, is the system even affected? Probably not, if the repair takes only 16 minutes, but what if the repair takes 16 weeks? Generally, for complex systems, failures should be stated in terms of specific component failures or be related to system performance. For example, if a vehicle fails to operate, that's a system failure. Or if throughput drops below 200 packages per hour (for any reason), that's a failure. The point is, both customer and supplier must agree on the definition of "failure."

b) Customers should demand that the supplier generate accurate predictions about the likelihood of system failure, the effect of those failures, and the time (and cost) to repair those failures. These can be done in a number of ways: reliability, availability and maintainability are commonly used concepts. However, what generally happens is the customer says "I want 99 percent availability," and the supplier says "Yeah, we can do that," but neither party ever really analyses it. The supplier simply use intuition, experience, etc., and hopes the system is designed well enough to meet the goal. Most of the time the supplier is right, but occasionally he is not. That's when the system does not live up to expectations and there is trouble. There is a variety of techniques that can be used for correcting this problem and getting everything on the table in plain sight, including: block diagrams, fault trees, FMEAs, computer simulation, etc.

c) Both customer and supplier should utilize experienced reliability engineers to define goals for reliability and availability, test programs, etc. Many companies get themselves into trouble because they assume that their design engineers can do the reliability work. Unfortunately, most design engineers have never studied reliability theory or probabilistic modelling (most of that is taught in industrial engineering programs). As a result, many contracts I have reviewed are seriously flawed when they are analysed carefully, for a number of reasons: incorrect terminology, non-standard methodologies, incorrect calculations, etc. This is disturbing to me because there is a wide array of well-known reliability standards and textbooks that could help the situation.

In an article entitled "How to Measure Systems Performance Reliability", System performance can have a direct business impact. According to the article even the most advanced system is going to fail. It may not fail for a very long time, or it might fail every so often, but be easily fixed. The worst scenario is a system that fails consistently, takes a long time to fix issues, or both. We want a reliable system, just as drivers want reliable vehicles. As IT professionals, our customers and decision makers will want us to be able to measure reliability.

We definitely will hear when the system is down, but anecdotes are not data. Instead, we can measure reliability as a combination of two important measurements: Mean Time Between Failures (MTBF) and Mean Time to Repair (MTTR).

Mean Time Between Failures (MTBF) is the measurement of time between system breakdowns, but it only includes the time the system is working (and not being worked on). A system that had been running strong for a year may suddenly have two down times in a one-month period; this will drag down MTBF. It should also warrant discussion on what updates/patches may have been missed during those long stretches of uptime.

Mean Time to Repair (MTTR) is the number you use to measure the average time it takes to fix a system. The following chart shows sample data on a given system and the mean time for repairs.

Scheduled maintenance is not included in these numbers: If you have told users that the system will be down from 3AM to 4AM on the last Tuesday of every month, we cannot count these hours against reliability. However, if the system fails at 5AM and takes three more hours to repair, this time is definitely counted against MTTR.

In a study by Raeyoung Jang, Sung-Jae Jung, and Wooyoung Soh titled "Design and Implementation of Data-Report Service for IoT Data Analysis", they attempt to design and implement an online data system for IoT applications. Their proposed system, the Data Report Service System (DRSS) is constructed by having a server store data from sensors using HTTP Requests. This system is meant to be installed on the devices, which means that some kind of memory is required. Notable is the ability to send notifications to smartphones, accomplished by using the free app Pushbullet.

In a study by Alexander Maier, Andrew Sharp, and Yuriy Vagapov titled "Comparative Analysis and Practical Implementation of the ESP32 Microcontroller Module for the Internet of Things", they do a comprehensive analysis on the ESP32 microchip and its various capabilities. Noting the built-in ADC in the chip, they manage to use it to construct a wireless oscilloscope, highlighting the versatility of the chip.

In a study by Lee Han Keat and Chuah Chai Wen titled "Smart Indoor Home Surveillance Monitoring System Using Raspberry Pi", they developed a Raspberry Pi-based system that takes and sends pictures and video when motion is detected. Their system only sends information and uses email and SMS; however, it provides a useful ground point for our study. It is also able to store the images and videos it sends in the Raspberry Pi's SD card.

In a study by Mirjana Maksimović, Vladimir Vujović, Nikola Davidović, Vladimir Milošević, and Branko Perišić titled "Raspberry Pi as Internet of Things Hardware: Performances and Constraints", they compared the capabilities and limitations of the Raspberry Pi computer as an addition to an IoT system, compared to other existing devices such as the Arduino boards, the Udoo, and such. They found that the Raspberry Pi boasted moderate computing power, peripheral support, and versatility for a low cost, and that it "brings the advantages of a PC to the domain of sensor network."

In an article made by Sudhir Chitnis, Neha Deshpande and Arvind Shaligram entitled "An Investigative Study for Smart Home Security: Issues, Challenges and Countermeasures", home security should be a top concern for everyone who owns or rents a home. Moreover, safe and secure residential space is the necessity of every individual as most of the family members are working. The home is left unattended for most of the day-time and home invasion crimes are at its peak as constantly monitoring of the home is difficult. Another reason for the need of home safety is specifically when the elderly person is alone or the kids are with baby-sitter and servant. Home security system i.e. HomeOS is thus applicable and desirable for resident's safety and convenience. This will be achieved by turning your home into a smart home by intelligent remote monitoring. Smart home comes into picture for the purpose of controlling and monitoring the home. It will give you peace of mind, as you can have a close watch and stay connected anytime, anywhere. But, is common man really concerned about home security? An investigative study was done by conducting a survey to get the inputs from different people from diverse backgrounds. The main motivation behind this survey was to make people aware of advanced HomeOS and analyze their need for security. This paper also studied the necessity of HomeOS investigative study in current situation where the home burglaries are rising at an exponential rate. In order to arrive at findings and conclusions, data were analyzed. The graphical method was employed to identify the relative significance of home security. From this analysis, we can infer that the cases of having kids and aged person at home or location of home contribute significantly to the need of advanced home security system. At the end, the proposed system model with its flow and the challenges faced while implementing home security systems are also discussed.

In a study by Hongyue Luo entitled “Intelligent Home Security System”, the present invention relates an intelligent home security system and method for protecting homes. It does this by detecting an approach, intelligently making decision for active responses, alarming and contacting the respective person or organization through communication link. With the associated hardware by applying psychological knowledge and human intelligence, the intelligent home security system and method can significantly reduce the possibility of an intruder breaking-in or even prevent a breaking-in from happening by real-life simulating, reactive real-life simulating, active and intelligent responding; help to identify and track intruders by taking photos at the suitable time, which offers valuable information for crime investigation and eventually reduces the crime rate, in addition to the conventional intruder detection, alarming and reporting to a security monitoring center or the respective person.

In a study made by Touradj Ebrahimi and Frederic Dufaux entitled “Smart Video Surveillance System Ensuring Privacy” This invention describes a video surveillance system which is composed of three key components 1—smart camera(s), 2—server(s), 3—client(s), connected through IP-networks in wired or wireless configurations. The system has been designed so as to protect the privacy of people and goods under surveillance. Smart cameras are based on JPEG 2000 compression where an analysis module allows for efficient use of security tools for the purpose of scrambling, and event detection. The analysis is also used in order to provide a better quality in regions of the interest in the scene. Compressed video streams leaving the camera(s) are scrambled and signed for the purpose of privacy and data integrity verification using JPSEC compliant methods. The same bit stream is also protected based on JPWL compliant methods for robustness to transmission errors. The operations of the smart camera are optimized in order to provide the best compromise in terms of perceived visual quality of the decoded video, versus the amount of power consumption. The smart camera(s) can be wireless in both power and communication connections. The server(s) receive(s), store(s), manage(s) and dispatch(es) the video sequences on wired and wireless channels to a variety of clients and users with different device capabilities, channel characteristics and preferences. Use of seamless scalable coding of video sequences prevents any need for transcoding operations at any point in the system.

In a study conducted by Rudolf C. King which is titled “Door and Home Security System and Method” the present invention relates to a door security system and method. More particularly, the present invention provides a door security system and method increasing the home security for elder people without limiting the privacy of or convenience for residents. The method comprises detecting closing of a door; keeping a first locking mechanism of said door in an open position for a first predetermined period of time after said closing; after said predetermined period of time, changing said first locking mechanism into a locked position. The re-entry time frame permits a user to re-enter without a key, immediately after realizing they forgot it. The invention further provides a home security method comprising recognizing a motion of a person on a door of a house through a camera provided in or near the door; producing streaming footage through a video camera; sending the produced streaming footage to a central processing server hidden inside the house; processing the streaming footage for face recognition purpose and checking against several databases in order to assess, if the person on the outside is either a person positively marked by the homeowner, such as friend and family, or negatively marked; and storing all data on the server. The home security method finds a compromise between the security of the residents while maintaining the privacy using a step-up-evaluation process of potential incidents.

In an article published by an editor which is titled “What Is an Acceptable Life Cycle for A Physical Security or Video System?” and “Are You Seeing A Trend Toward Systems Being Replaced More or Less Often?” he explains that most end users would say that a "good" system should last a certain amount of time. Each system or device has a generally established and expected life span, and anything that falls short of its life expectancy is generally deemed as "poor quality." He even tried to conduct an interview with some of his panellist to get their insights on trends they have observed in the frequency of system replacements as well as what variables impact the life cycle of physical security systems. One panellist named Brenda Koesterman said that “Security is no longer a hardware game; in fact, it is the software and IT technology that is taking huge leaps forward.” She also stated that “As an industry, we really need to be looking to IT to utilize best practices in technology lifecycle”. Another panellist named John Davies stated that “We haven’t seen any overall evidence of customers renewing their security more frequently than the normal five to seven years period. He also stated that “in this instance, the heightened interest might result in increased demand for system replacements, or at least refurbishment, so operators can avail themselves of the latest technology.” Overall, the editor tries to explain that security systems are a significant investment and states that “The start of a new life cycle isn't always simply the point at which the entire system is renewed.

End users want to make the most of the initial investments they have made, so they make purchases to upgrade their existing system to use the latest technologies and/or to allow for greater integration. Often, one security system will see various changes to its different components, but rarely a complete system overhaul”.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue V May 2021- Available at www.ijraset.com

II. MATERIALS AND METHODS

A. System Design

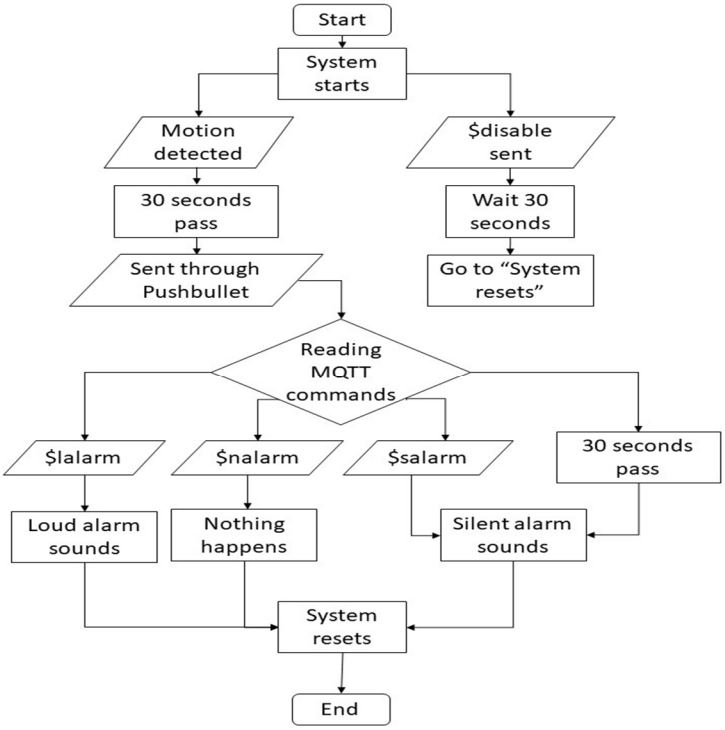


Fig. 4 The figure shows how the system works when powered on. It also shows the choices of the user and their respective output.

B. Description of Product/Prototype

In terms of runtime, since the system is supposed to be a small security system, it should be able to run for at least 80 hours per week. This equates to more than 11 hours daily, which should be enough to cover work shifts or classes. During this time, all system devices should be running correctly. In terms of response rate, the system is expected to have a correct response rate of no less than 95%. It should be able to recognize proper commands, and provide the correct response. For example, the "$snap" command should take exactly one picture and send it to the device, while the "$lalarm" and "$salarm" command should sound both the loud alarm and silent alarm, respectively.

C. Quality Testing/ Performance Evaluation

1) *Uptime Testing:* To test the robustness of the system, the trial will involve keeping the device on for at least 12 hours straight. Every hour, the researcher will monitor the status of the device, noting whether the device is still functioning as intended, as well as whether the device is still operating at an acceptable temperature. For the motion sensor and camera, this means that they should be able to do their intended functions; to sense motion and take pictures respectively. For the loud and silent alarms, this means that they should still be connected to the Wi-Fi network and able to receive commands through MQTT.
2) *Response Rate:* Loud/Silent alarm response rate will be tested. These alarms receive commands using MQTT. To check whether they are receiving commands properly, the researcher will perform a trial. First send a command to turn on the loud alarm. Second, send a command to turn on the silent alarm. Then, send an unrecognized command to the server. Lastly, record the responses. If the command to turn on the loud alarm ($lalarm) is sent, the loud alarm should sound. If the command to turn on the silent alarm ($salarm) is sent, the silent alarm should then sound. If the command is an improper command, there will be no effect, and the system will default. Response rate will be the percentage of successful trials over total trials. This test will be performed 50 times daily for 12 days, for a total sample size of 600 trials. This test will be used to determine the reliability of the silent alarm to fulfill its function of alerting security personnel.

III.RESULTS AND DISCUSSION

A. Response Rate Tests

TABLE 1.1
Response Rate for Commands – Morning

Trial Number	$lalarm	$salarm	$none	$snap	$disable
1	1.47	1.14	0.99	2.44	1.19
2	0.81	0.80	0.86	2.02	1.15
3	1.32	0.77	0.88	1.87	0.99
4	1.15	0.93	1.20	1.69	1.28
5	1.88	1.32	1.30	1.97	1.26
6	0.70	1.45	1.21	2.35	1.31
7	1.30	1.14	1.17	3.47	1.85
8	1.37	1.24	1.26	3.15	1.20
9	1.51	0.98	0.79	2.97	1.26
10	1.11	0.85	0.83	2.55	1.32
Average	1.262	1.062	1.049	2.448	1.281

TABLE 1.2
Response Rate for Commands – Afternoon

Trial Number	$lalarm	$salarm	$none	$snap	$disable
1	2.29	1.18	1.30	3.01	0.97
2	1.56	1.13	1.55	2.44	1.12
3	1.44	0.88	1.98	2.78	1.28
4	2.10	0.97	2.56	1.99	1.36
5	1.95	0.75	2.22	2.44	1.87
6	1.77	0.60	1.87	2.14	2.03
7	1.58	1.12	1.36	2.36	1.79
8	1.66	1.33	0.89	2.88	1.73
9	1.41	1.25	0.99	3.03	1.38
10	1.33	1.91	1.10	2.85	0.91
Average	1.709	1.112	1.582	2.592	1.444

TABLE 1.3
Response Rate for Commands – Evening

Trial Number	$lalarm	$salarm	$none	$snap	$disable
1	0.89	0.66	0.70	3.45	1.25
2	1.23	1.23	0.88	2.14	0.66
3	5.44	0.90	1.23	1.95	2.20
4	3.45	0.87	1.14	4.01	1.88
5	0.97	1.61	1.56	7.46	2.43
6	3.14	0.94	0.91	5.33	2.78
7	2.37	0.68	2.47	3.20	0.87
8	1.77	1.99	2.81	1.77	0.99
9	4.26	1.34	1.82	2.16	1.14
10	2.48	0.78	1.84	2.32	0.85
Average	2.60	1.10	1.536	3.379	1.505

TABLE 2.1
Response Rate for Sending Images – Morning

Trial Number	On trigger			On Snap
	1st	2nd	3rd	
1	7.81	15.44	22.5	14.32
2	9.2	18.9	21.7	12.28
3	8.89	16.37	26.41	16.44
4	10.4	18.52	28.32	13.81
5	11.37	19.76	30.23	14.65
6	12.15	18.02	22.56	17.82
7	11.27	21.13	28.74	13.83
8	9.17	19.44	25.33	15.78
9	9.86	17.53	26.53	12.06
10	10.14	21.88	29.87	13.13
Average	10.026	18.699	26.219	14.412

TABLE 2.2
Response Rate for Sending Images – Afternoon

Trial Number	On trigger			On Snap
	1st	2nd	3rd	
1	19.47	25.63	32.47	14.55
2	17.55	22.78	29.4	11.4
3	19.33	26.22	30.18	11.57
4	21.42	28.44	33.68	17.25
5	16.3	21.69	25.36	18.24
6	16.45	21.44	28.9	12.98
7	15.52	19.67	24.88	13.24
8	18.4	24.18	29.51	11.1
9	12.06	18.61	25.45	16.35
10	13.11	27.78	29.64	14.71
Average	16.961	23.644	28.947	14.139

TABLE 2.3
Response Rate for Sending Images – Evening

Trial Number	On trigger			On Snap
	1st	2nd	3rd	
1	19.47	25.63	32.47	14.55
2	17.55	22.78	29.4	11.4
3	19.33	26.22	30.18	11.57
4	21.42	28.44	33.68	17.25
5	16.3	21.69	25.36	18.24
6	16.45	21.44	28.9	12.98
7	15.52	19.67	24.88	13.24
8	18.4	24.18	29.51	11.1
9	12.06	18.61	25.45	16.35
10	13.11	27.78	29.64	14.71
Average	16.961	23.644	28.947	14.139

TABLE 3
Response Rate for Sending Images – Dual Devices

Trial Number	Using Mobile Data	Using Home Wi-Fi
1	10.47	11.35
2	12.51	14.76
3	11.16	12.04
4	9.83	10.41
5	10.66	13.14
6	12.24	13.9
7	10.87	14.49
8	9.5	12.86
9	10.32	12.45
10	12.59	13.96
Average	11.015	12.936

The results of the tests indicate that while sending commands can be done very quickly, sending images from the system to the user is quite slow. The commands sent through MQTT are simple text, which require much less bandwith than the JPEG images sent through Pushbullet. The time it takes to send a picture in the morning is significantly less (approximately five seconds less for the first and second pictures, two to three seconds less for the third) compared to the time it takes in the afternoon and evening, which can be attributed to the speed and quality of the connection degrading in those times. Still, since the 30 second countdown to send an option starts after the third image is sent, the user has enough time to view a picture of the intruder and determine a course of action before the silent alarm is triggered by default.

TABLE 4.1
Silent Alarm Uptime Tests

14-Jan		16-Jan		17-Jan		18-Jan		20-Jan	
Time	Response	Time	Response	Time	Response	Time	Response	Time	Response
5:29	□	12:02	□	9:21	□	9:44	□	14:26	□
6:28	□	13:02	□	10:21	□	10:44	□	15:26	□
7:28	□	14:02	□	11:21	□	11:44	□	16:26	□
8:28	□	15:02	□	12:21	□	12:44	□	17:26	□
9:28	□	16:02	□	13:21	□	13:44	□	18:26	□
10:28	□	17:02	□	14:22	□	14:44	□	19:26	□
11:28	□	18:02	□	15:22	□	15:44	□	20:26	□
12:28	□	19:02	□	16:21	□	16:44	□	21:26	□
13:28	□	20:02	□	17:21	□	17:44	□	22:26	□
14:28	□	21:02	□	18:21	□	18:44	□	23:26	□
15:28	□	22:02	□	19:21	□	19:44	□	0:26	□
16:28	□	23:02	□	20:21	□	20:44	□	1:26	□
System Uptime	100%	System Uptime	100%	System Uptime	100%	System Uptime	100%	System Uptime	100%
Response Rate	100%	Response Rate	100%	Response Rate	100%	Response Rate	100%	Response Rate	100%

TABLE 4.2
Silent Alarm Uptime Tests – Continued

14-Jan		16-Jan		17-Jan		18-Jan		20-Jan	
Time	Response	Time	Response	Time	Response	Time	Response	Time	Response
5:29	□	12:02	□	9:21	□	9:44	□	14:26	□
6:28	□	13:02	□	10:21	□	10:44	□	15:26	□
7:28	□	14:02	□	11:21	□	11:44	□	16:26	□
8:28	□	15:02	□	12:21	□	12:44	□	17:26	□
9:28	□	16:02	□	13:21	□	13:44	□	18:26	□
10:28	□	17:02	□	14:22	□	14:44	□	19:26	□
11:28	□	18:02	□	15:22	□	15:44	□	20:26	□
12:28	□	19:02	□	16:21	□	16:44	□	21:26	□
13:28	□	20:02	□	17:21	□	17:44	□	22:26	□
14:28	□	21:02	□	18:21	□	18:44	□	23:26	□
15:28	□	22:02	□	19:21	□	19:44	□	0:26	□
16:28	□	23:02	□	20:21	□	20:44	□	1:26	□
System Uptime	100%	System Uptime	100%	System Uptime	100%	System Uptime	100%	System Uptime	100%
Response Rate	100%	Response Rate	100%	Response Rate	100%	Response Rate	100%	Response Rate	100%

What the researcher needs in this testing is for it to run in an operational state for several days without any issues. The researcher was able to determine that the ESP32 is capable of functioning as a silent alarm for 12 hours straight at a time. There were no complications in the device, save for occasionally getting hotter than usual during testing. However, this did not impede its ability to function properly, nor did it have any noticeable effect in performance.

IV. CONCLUSIONS AND RECOMMENDATIONS

The researcher concludes that the design of an effective security system that is accessible, has visual aid, and controllable via internet is the researcher's design. It is easily accessible because it can be used by any smartphone with an Internet connection and proper authentication. It can send the user picture messages and notifications through Pushbullet. It is controllable by the Internet since the app used to control it can connect to and communicate through the Internet.

Since the system contains only one infrared sensor and one camera, it is only meant to be used for a small area, preferably a small condominium unit. It is easy to install and only requires low power consumption. It only requires a stable Wi-Fi connection so the device can respond accurately.

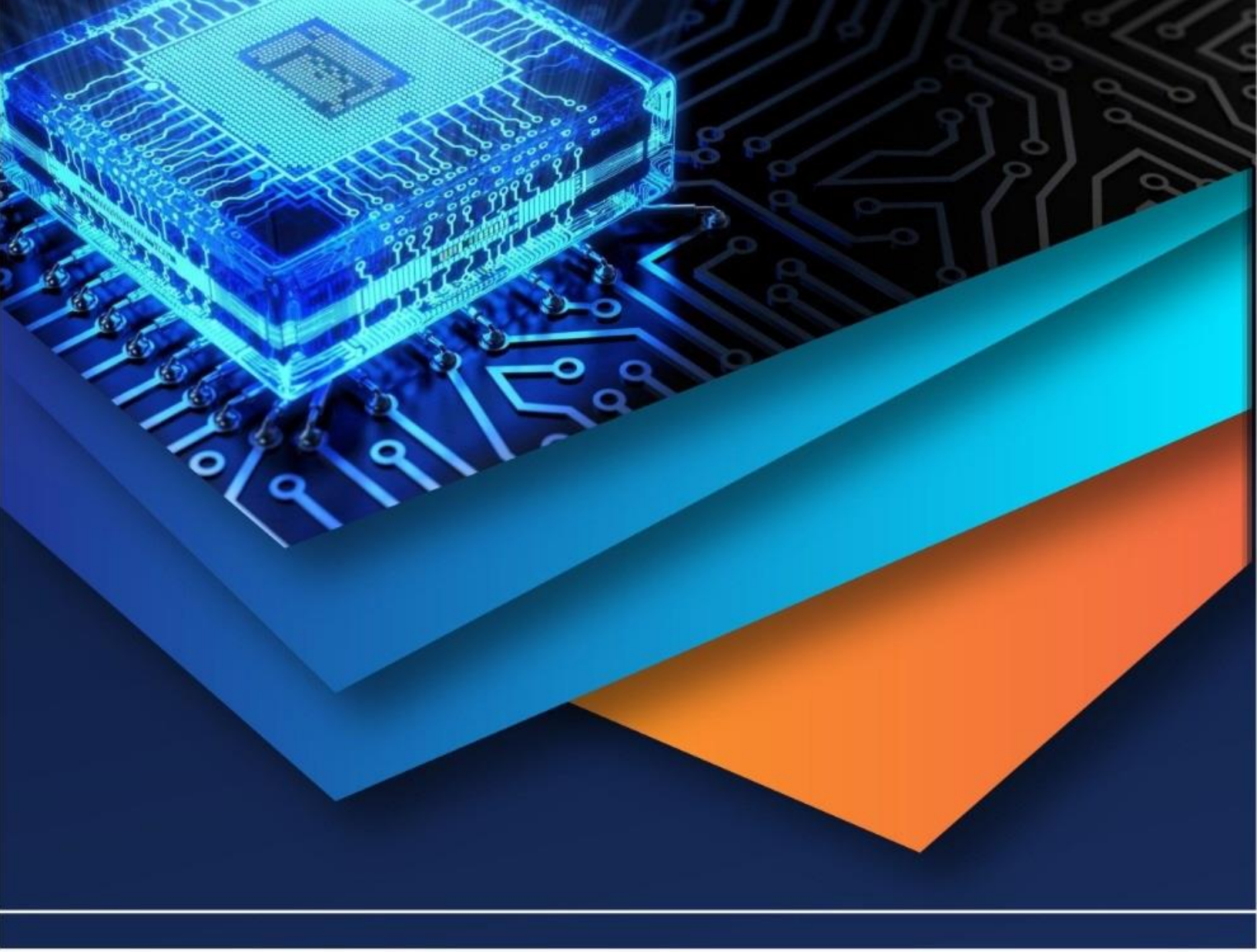
Most condo units don't have proper security system which makes our device applicable and effective. The app-controlled security system should effectively cover the time and run correctly for at least 12 hours straight, which should usually be enough to cover the time when the user is away from home. The response rate of our system is 100 percent working correctly to our commands. Overall, our device is able to meet our expectations regarding our motion sensing and commands.

At the time this study was conducted the devices used were low quality devices. For better security the researcher suggests using devices with better security against cyber-attacks. For better clarity of images, better cameras can also be installed. The same goes with the alarms. The louder the loud alarm the better. If the condo unit to be installed has more entrances, extra sensors will be needed on each entrance.

REFERENCES

[1] Bersales, L. (2015). Census of Population|Philippine Statistics Authority. Retrieved from https://psa.gov.ph/statistics/census/2015-census-of-population
[2] Camera definition and meaning|Collins English Dictionary. Retrieved from https://www.collinsdictionary.com/dictionary/english/camera
[3] Chitnis, S. & Deshpande, N. & Shaligram, A. An Investigative Study for Smart Home Security: Issues, Challenges and Countermeasures. Retrieved from https://file.scirp.org/pdf/WSN_2016042516164326.pdf?fbclid=IwAR1zDIdy5Ty4B7RluX1oIjpmUJbaWUgWUc85Qrxiwkl8b7hwZo-jbAr_ILY
[4] condominium| Definition of security in English by Oxford Dictionaries. Retrieved from https://en.oxforddictionaries.com/definition/condominium

[5] Ebrahimi, T. & Dufaux, F. Smart Video Surveillance System Ensuring Privacy. Retrieved from https://patents.google.com/patent/US20070296817A1/en
[6] How to Measure Systems Performance Reliability. Retrieved from https://study.com/academy/lesson/how-to-measure-systems-performance-reliability.html?fbclid=IwAR0pYayEZB6Fj2qFbn924GgFAxcwOlEvZAMqYiHOmNnfK7JhPBoYaOVB_4I
[7] Jang, R. & Jung, S. & Soh, W. Design and Implementation of Data-Report Service for IoT Data Analysis. Retrieved from https://www.atlantis-press.com/php/download_paper.php?id=25836357
[8] Kao, L. Infrared Intrusion Alarm System. Retrieved from https://patents.google.com/patent/US4377808A/en
[9] Keat L. & Wen, C. Smart Indoor Home Surveillance Monitoring System Using Raspberry Pi. Retrieved from http://joiv.org/index.php/joiv/article/viewFile/172/161
[10] King, R.C. Door and Home Security System and Method. Retrieved from https://patents.google.com/patent/EP3189502A1/en
[11] Kodaira, M. Infrared intrusion alarm system capable of preventing false signals. Retrieved from https://patents.google.com/patent/US4570157A/en
[12] Lee A. St. J. Home Medical Surveillance System. Retrieved from https://patents.google.com/patent/US4838275A/en
[13] Luo, H. Intelligent Home Security System. Retrieved from https://patents.google.com/patent/US20070182543
[14] Macsimovic, M. & Vujovic, V. & Davidovic, N. & Milosevic, V. & Perisic, Branko. Raspberry Pi as Internet of Things Hardware: Performances and Constraints Retrieved from https://www.researchgate.net/profile/Vladimir_Vujovic/publication/280344140_ELI16_Maksimovic_Vujovic_Davidovic_Milosevic_Perisic/links/55b3368608ae9289a08594aa.pdf
[15] Maier, A. & Sharp, A. & Vagapov, Y. Comparative Analysis and Practical Implementation of the ESP32 Microcontroller Module for the Internet of Things. Retrieved from https://www.researchgate.net/publication/320273388_Comparative_Analysis_and_Practical_Implementation_of_the_ESP32_Microcontroller_Module_for_the_Internet_of_Things
[16] MQTT. Retrieved from https://en.wikipedia.org/wiki/MQTT
[17] National Capital Region Police Office. (2018). Top 10 Modus Operandi of the most common Crimes in Manila and other areas in the Philippines. Retrieved from https://www.ncrpo.pnp.gov.ph/index.php/crime-prevention-tips/30-top-10-modus-operandi-of-the-most-common-crimes-in-manila-and-other-areas-in-the-philippines
[18] Piyare, R. (2013). Internet of Things: Ubiquitous Home Control and Monitoring System using Android Based Smart Phone. Retrieved from http://article.sapub.org/10.5923.j.ijit.20130201.02.html
[19] Pyle, R. E. (1984). Home Security System. Retrieved from http://patents.com/us-4446454.html
[20] Rouse, M. (2011). What is app?. Retrieved from https://searchmobilecomputing.techtarget.com/definition/app
[21] Rouse, M. (2012). What is sensor?. Retrieved from https://whatis.techtarget.com/definition/sensor
[22] Rouse, M. (2018). What is IOT devices? (internet of things devices?). Retrieved from https://internetofthingsagenda.techtarget.com/definition/IoT-device
[23] security|Definition of security in English by Oxford Dictionaries. Retrieved from https://en.oxforddictionaries.com/definition/security
[24] Smart Device. Retrieved from https://en.wikipedia.org/wiki/Smart_device
[25] Smith, M. O. (1992). Infrared Alarm System. Retrieved from https://patents.google.com/patent/US5317620A/en
[26] Snyder, C. Door Alarm and Method of Use. Retrieved from https://patents.google.com/patent/US20110254689A1/en
[27] Stanford, A. & Linh, H. MQTT For Sensor Networks Protocol Specification. Retrieved from http://mqtt.org/new/wp-content/uploads/2009/06/MQTT-SN_spec_v1.2.pdf?fbclid=IwAR18DvVUjvvJtHkPjbYCTJVb9gh-i_Qi4olnkI5lJ1g_pPqgGH3WQAPx9JQ
[28] subject|Definition of subject in English by Oxford Dictionaries. Retrieved from https://en.oxforddictionaries.com/definition/subject
[29] Uptime. Retrieved from https://en.wikipedia.org/wiki/Uptime
[30] Usher, J. S. How to Determine System Reliability. Retrieved from https://www.mhlnews.com/archive/how-determine-system-reliability?fbclid=IwAR3OX29Loyj_BzSAStNt9TjAnTArXG8ql2PK---q_wiNJJ1r_CXFTxK9Ijg
[31] Villena, D. (2016). Internet of Things (IoT) is the network of physical objects.
[32] Retrieved from https://medium.com/@darotvillena/the-internet-of-things-iot-is-the-network-of-physical-objects-devices-vehicles-buildings-and-63b621d47aa
[33] (2014). Wifi Definition. Retrieved from https://techterms.com/definition/wi-fi
[34] VinTech Systems. (2012). Condo Tenants Can Be Just As Vulnerable to Burglaries as Home Owners. Retrieved from https://vintechnology.com/2012/02/09/condo-tenants-can-be-just-as-vulnerable-to-burglaries-as-home-owners/
[35] What Is An Acceptable Life Cycle For A Physical Security Or Video System?" and "Are You Seeing A Trend Toward Systems Being Replaced More Or Less Often?. Retrieved from https://www.securityinformed.com/insights/what-is-an-acceptable-life-cycle-for-a-physical-security-or-video-system-are-you-seeing-a-trend-toward-systems-being-replaced-more-or-less-often-and-what-variables-impact-the-life-cycle-of-physi.html?fbclid=IwAR0ggqzzNsl1sWMoh9It4NN3rXHbTvjFQ9tosip1l1XZTkxi0i-42D_8Ci4
[36] Zhao, Y. & Ye, Z. (2008). A Low Cost GSM/GPRS Based Wireless Home Security System. Retrieved from https://ieeexplore.ieee.org/document/4560131/



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY