© 2018 IJSRSET | Volume 4 | Issue 9 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology

An Analytics Enabled Wireless Anti-Intruder Monitoring and Alarm System

Victor O. Matthews[1], Etinosa Noma-Osaghae[*2], Uzairue Stanley Idiake[3]
[1, *2, 3]Department of Electrical and Information Engineering, Covenant University, Ota, Ogun State, Nigeria

ABSTRACT

Home intruder detection and alarm system rely on a number of factors to determine if an alarm should be triggered. These factors depend greatly on the type of sensors used and the amount of analytical capability built into the alarm system. Presently, most home intruder detection and alarm systems in the market are highly prone to false alarms because they do not have any analytical capability. In this paper, an analytics enabled wireless anti-intruder monitoring and alarm system that is simple and low in cost is proposed. The proposed alarm system uses still images and the location of sensed motion within the premises of the home to help home owners make informed alarm triggering decisions. The designed security system offers the option of allowing multiple key holders receive security alerts via the cellular network's Short Message Service (SMS). The system also gives the option of sending distress messages to the police or trusted neighbours.

Keywords: Alarm, Anti-Intruder, Motion Sensing, Images, Analytics, Cloud, Server, Application Programme Interface, Security, Home.

I. INTRODUCTION

Home owners all over the world are beginning to take precautionary steps to secure their properties and lives from violent criminals, burglars and intruders. The most common entry points like doors and windows are usually protected with tamper-proof security circuits that break when a forced entry is attempted. Interior spaces containing valuables like art, computers, coin collections, guns and jewelries are usually protected with motion sensors that trigger an alarm when it senses movement within the space. Security systems are usually a combination of several devices that form an electro-mechanical shield around the valuable or property they protect. Most security systems have a control panel that coordinates and receives information from the sensors that are deployed around the home. The control panel receives electrical signals from doors/window sensors, the interior/exterior motion sensors, wired/wireless security cameras and uses the information got to decide if it is necessary to trigger a high-decibel siren or alarm. In some few cases a yard sign or window sticker indicating that a house is covered by a security system can be used to scare off potential intruders.

The security system in homes can be controlled remotely using a mobile device or a remote control called Key Fobs. The control panel arms or disarms the alarm system and is also responsible for alerting home owners, key holders, security companies or the police of an invasion or intrusion. Windows and doors are usually protected using two separate circuits. A part of the circuit is placed on the window and door. The other part of the circuit is placed on the window sill and door frame. The two separate circuits form a

complete circuit when they are joined together by the closing of the window and door. This provides a means of protecting the doors and windows from intruders or burglars. Motion sensors are usually used to protect internal and external spaces within the home using an invisible zone that triggers an alarm whenever it is breached. Security cameras can be used to monitor hard to see places, remote buildings, entry points, children and delivery personnel. The security camera also comes very handy whenever there is no one in the house. But, due to the long hours of recordings made by video surveillance systems, it takes an enormous amount of human effort and time to comprehensively review it. Analytics helps with the finding of incidents within a stretch of video recordings that warrants more scrutiny. Analytics in security systems has the capability to alert security personnel or selected key holder to incidents based on how the incident triggering parameters are set.

The proposed analytics enabled wireless anti-intruder monitoring and alarm system provided a cloud enabled security system that makes use of the human face and the location of sensed motion to form a basic analytic that informs the home owner and designated key holders of an intrusion on their property through an android application that the home owner and key holders can use to trigger the high decibel alarm in the event that a security threat is a real one.

II. LITERATURE REVIEW

Mikro C and an android application were used by [1] to carry out health and weather monitoring in an automated home setting [2]. Authors in [3] used a Zigbee-based wireless sensor network to automate these same home functions and an alarm system [4]. Juan et al [5] made a low power wireless smoke alarm system in home fires. The device discriminates between different types of smoke using a variety of sensors. This makes it very easy to differentiate between a true and false smoke/fire alarm. The system optimized energy consumption using a sleek hardware and software design to give the proposed smoke detector a life span of five years. The device communicates with the control panel via radio waves. [6] stressed the importance of being able to weigh the hazard level of a triggered alarm. This ability was termed "informativeness". The authors suggested several ways to measure the "informativeness" of an alarm to improve alarm response in medical settings [7]. Mohammed et al [8] presented a designed and implemented device-free intruder detection and alarm system named "WiGarde". The authors used a special off-the-shelf Wi-Fi Channel State Information (CSI) to design unique intruder detection and alarm system. The authors claimed that the system was capable of detecting intrusions through windows and doors [9]. The alarm system was implemented using the commercially available IEEE 802.11 wireless protocol. Support Vector Machine (SVM) and a Bad Stream algorithm were used to classify what could be termed as human intrusion. The test of the designed system was tried in a dynamic environment and according to the authors; the system was 94.5% accurate. The authors also claimed that the novel intrusion system was better than all already existing channel state information based intruder alarm systems.

A Multi-agent System (MAS) that can be merged with information got from wireless sensor networks and social behaviour to create a better living environment for the elderly was proposed by [10]. The authors collected data for a day and made several preliminary tests to ascertain the effectiveness of the system [11]. A sensor web node was implemented using Raspberry PI in [12]. The web node was developed from scratch to be flexible, durable and inexpensive. The developed system could collect data from various monitoring devices with customizable precision [13]. In [14] the Raspberry PI module was used to design a system that sends photos and videos of a detected intruder to a cloud network. The Raspberry PI gets this information from the motion sensor and surveillance

camera. It used a low power chip and could store photos and videos in the memory of the chip whenever the Raspberry PI cannot connect to the internet. It resends the stored photos and videos when the internet connection is restored) [15]. A cloud based and android supported scalable home automation system was proposed by [16]. Multiple users were given the privilege of controlling their appliances via a web-based outlet. Extensive research on the viability and scalability of the model was carried out. The outcome was presented as a commercial way of controlling household devices remotely [17].

III. METHODS AND MATERIAL

The hardware devices used to set up the hardware architecture are as under listed:

- The mobile device – Tablet, Phone or Laptop
- Motion sensors
- Internet protocol (IP) Cameras
- High decibel siren or alarm
- Adruino microcontroller – Control Panel
- GSM module – For SMS

These IP cameras and motion sensors were placed in the following location:

Table 1: Motion Sensor and Camera Locations

DEVICE	LOCATION
IP Camera	a. Front porch b. Backyard c. Right exterior side d. Left exterior side
Motion Sensor	a. Living room b. Kitchen c. Garage d. Dining Room e. Bedroom 1 f. Bedroom 2 g. Bedroom 3 h. Store

The software architecture of the designed system was enabled by the under listed:

- SMS cloud server
- Mobile application programme interface – with image processing and location determining ability.
- Database

The overall system architecture is shown in Figure 1.

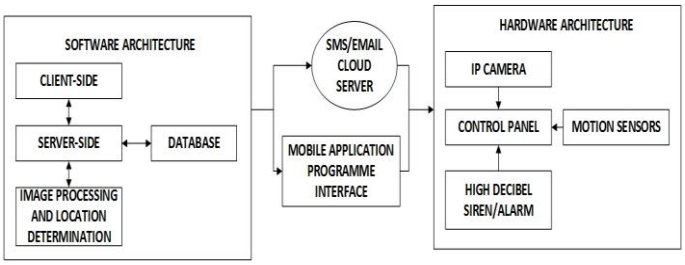

Figure 1 : Overall System Architecture

The model of the proposed anti-intruder monitoring and alarm system is a cloud-based model that makes remote access possible from any internet enabled mobile device. The view of the system's model is shown in Figure 2.

The system's analytics algorithm was implemented using the mobile application programme interface. Still images taken with the installed IP camera and the location of the motion sensor triggered were used as inputs to the algorithm that implemented the analytics. The control panel sends an SMS alert to authorized persons whenever the motion sensor senses motion or when the IP camera picks up the image of any potential intruder. The message includes a link to the customized application in the user's mobile device which when launched, immediately runs through the following steps shown by the analytics algorithm to aid home owners with alarm triggering decisions.

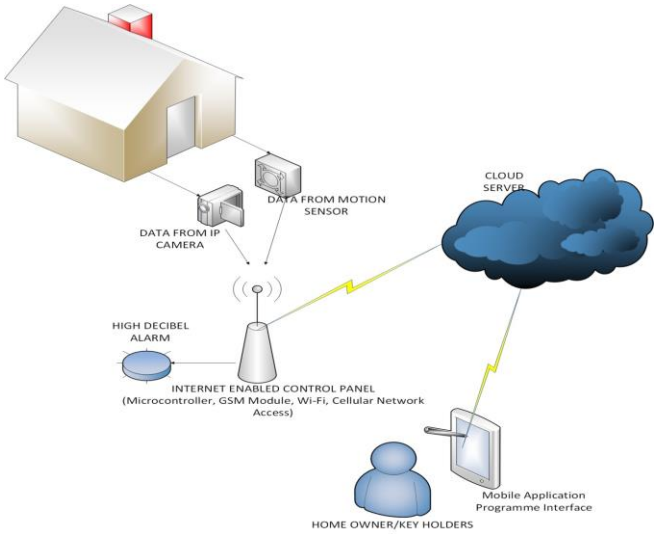

Figure 2 : The Proposed Analytics Enabled Anti-intruder System's Model

A. The Analytics Algorithm:

Step 1: SMS alert arrives
Step 2: Initialize analytics
Step 3: If "sensed-motion" location and human face/body image is present
Go to Step 7
Else
Go to Step 4
Step 4: If only "sensed-motion" location is present
Go to Step 5
Else
Go to Step 6
Step 5: If more than one "sensed-motion" locations are present
Go to Step 7
Else
Go to Step 6
Step 6: If only human face/body image is present
Go to Step 7
Else
Go to Step 2

The flow chart for the entire analytics based anti-intruder alarm system is shown in Figure 3. The designed alarm system enables home owners to send distress SMS messages to anyone. The system can also automatically send distress SMS to phone numbers stored on its database.

IV. RESULTS AND DISCUSSION

During the initial tests of the system a list of potential triggers for the IP camera and the motion sensors were discovered. These triggers are shown in Table 2. All possible triggers caused both the motion sensor and the IP camera to respond and send an SMS alert. This discovery made the need for some form of analytics important. The frequency of false alarms with and without analytics was determined and the result is shown in Table 3.

Table 2: Potential Motion Sensor and Camera Triggers

Potential Trigger	Motion Sensor	IP Camera
Dog	Triggered	Triggered
Bird	Triggered	Triggered
Chicken	Triggered	Triggered
Goat	Triggered	Triggered
Man	Triggered	Triggered
Object	Triggered	Triggered

Table 3: Frequency of False Alarms with and without Analytics

	False Alarms without Analytics	False Alarms with Analytics
Day 1	3	0
Day 2	4	0
Day 3	2	1
Day 4	5	0
Day 5	7	0

The designed system was tested over a period of five days to ascertain how frequently false alarms are made without any analytic feature and with analytics. False alarms were very incessant and common without the analytics feature in the security system. False alarms were almost non-existent when the analytics feature was used with the security system. From Figure 4, the highest frequency of false alarm was recorded when

the security system was used without the analytics feature on Day 5. The only false alarm recorded when the security system was used with the analytics feature occurred on Day 3. This was due to error in human judgment.

A. Software Deployment

For the deployment of the security system's mobile application, the frontend was built using Ionic's build command typed into the command prompt (CMD) application. The command generates an executable android application file (APK) which was then installed onto an android device.

The backend of the mobile application was deployed as an API on Heroku (a cloud platform as a service (PaaS) for hosting applications in various languages).

Git (a distributed version control system (VCS)) was used to enable the management of different builds of the application and accurately track changes

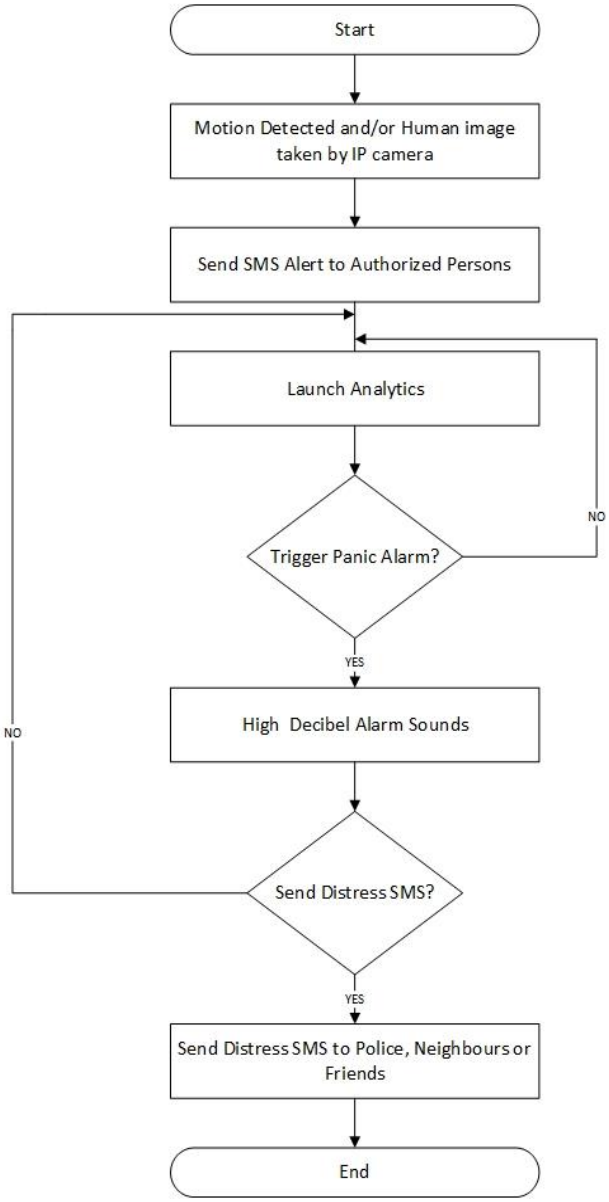

Figure 3 : Flowchart of Implemented Analytics Based Anti-Intruder Monitoring and Alarm System.

Throughout the project. Git is operated either via a command line interface (Git Bash) or a desktop application (Git for Desktop).

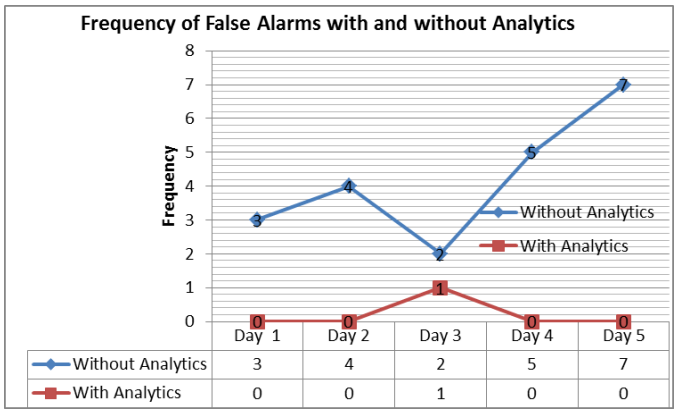

Figure 4 : Frequency of False Alarms with and without Analytics

B. The Application Programme Interface Test

The application programming interface (API) within the security system's mobile application as well as third-party endpoints were tested to ensure they provided the correct response and in the correct format. The API testing was done using Postman – software for API development, testing and debugging. This test was carried out using the following format:

- Endpoint – a Uniform Resource Identifier (URI) which serves as a means of gaining access to a specific service in the API.
- Method – either one of GET or POST depending on the nature of the service being accessed.
- URI Parameters and/or Body parameters – these are variables required by the API in order to process the requested service.
- Response – this is the result given by the API in response to the requested service and parameters combination. The result can yield a 'success' or 'failure'.

All Objects created and received are in the JavaScript Object Notation (JSON) format. The tested services are described by Table 4 and Figure 5:

Table 4: Format of the Create User Service

	Format
Endpoint	/create
Method	POST
URI Parameters	None
Body Parameters	firstName, lastName, mobile, role, profileImage, password.
Response	Status ("success" or "failure")

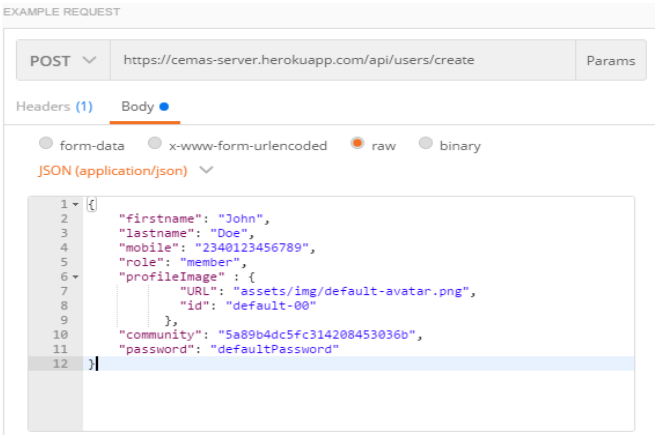

Figure 5: A test request sent for Create User Service

V. CONCLUSION

An analytics enabled wireless anti-intruder monitoring and alarm system was designed. The system used a mobile application to assist home owners in making informed alarm triggering decisions using an embedded analytics feature. The system uses a combination of still images and "sensed-motion" location to alert owners to an invasion or intrusion on their properties. The home owner has the option of triggering the high decibel alarm via the panic button on the mobile application program interface. The control panel of the designed system and the mobile device has connections to a cloud service and can communicate with each other remotely. It was discovered that deploying a simple analytics algorithm in the designed system made the probability of a false alarm almost non-existent. This is a huge

improvement on current residential alarm systems that are very prone to false alarms.

VI. REFERENCES

[1] M. A. E.-L. Mowad, A. Fathy, and A. Hafez, "Smart home automated control system using android application and microcontroller," *International Journal of Scientific & Engineering Research,* vol. 5, pp. 935-939, 2014.

[2] K. Okokpujie, E. Noma-Osaghae, S. John, and P. C. Jumbo, "Automatic home appliance switching using speech recognition software and embedded system," in *Computing Networking and Informatics (ICCNI), 2017 International Conference on*, 2017, pp. 1-4.

[3] J. A. Luis, J. A. G. Galán, and J. A. Espigado, "Low power wireless smoke alarm system in home fires," *Sensors,* vol. 15, pp. 20717-20729, 2015.

[4] K. O. Okokpujie, A. Orimogunje, E. Noma-Osaghae, and O. Alashiri, "An Intelligent Online Diagnostic System With Epidemic Alert," *An Intelligent Online Diagnostic System With Epidemic Alert,* vol. 2, 2017.

[5] M. F. Rayo and S. D. Moffatt-Bruce, "Alarm system management: evidence-based guidance encouraging direct measurement of informativeness to improve alarm response," *BMJ Qual Saf,* pp. bmjqs-2014-003373, 2015.

[6] M. A. A. Al-qaness, F. Li, X. Ma, and G. Liu, "Device-Free Home Intruder Detection and Alarm System Using Wi-Fi Channel State Information," *International Journal of Future Computer and Communication,* vol. 5, p. 180, 2016.

[7] K. O. Okokpujie, E. Noma-Osaghae, G. Kalu-Anyah, and I. P. Okokpujie, "A Face Recognition Attendance System with GSM Notification," 2017.

[8] S. Rodríguez, J. F. De Paz, G. Villarrubia, C. Zato, J. Bajo, and J. M. Corchado, "Multi-agent information fusion system to manage data from a WSN in a residential home," *Information Fusion,* vol. 23, pp. 43-57, 2015.

[9] N.-O. Etinosa, C. Okereke, O. Robert, O. J. Okesola, and K. O. Okokpujie, "Design and Implementation of an Iris Biometric Door Access Control System," in *Computational Science and Computational Intelligence (CSCI), 2017*, Las Vegas, USA, 2017.

[10] V. Vujović and M. Maksimović, "Raspberry Pi as a Sensor Web node for home automation," *Computers & Electrical Engineering,* vol. 44, pp. 153-171, 2015.

[11] C. Atuegwu, S. Daramola, K. O. Okokpujie, and E. Noma-Osaghae, "Development of an Improved Fingerprint Feature Extraction Algorithm for Personal Verification," *International Journal of Applied Engineering Research,* vol. 13, pp. 6608-6612, 2018.

[12] A. N. Ansari, M. Sedky, N. Sharma, and A. Tyagi, "An Internet of things approach for motion detection using Raspberry Pi," in *Intelligent Computing and Internet of Things (ICIT), 2014 International Conference on*, 2015, pp. 131-134.

[13] C. Atuegwu, K. O. Okokpujie, and E. Noma-Osaghae, "A Bimodal Biometric Student Attendance System," 2017.

[14] Z.-y. Liu, "Hardware design of smart home system based on ZigBee wireless sensor network," *Aasri Procedia,* vol. 8, pp. 75-81, 2014.

[15] K. Okokpujie, E. Noma-Osaghae, S. John, and R. Oputa, "Development of a facial recognition system with email identification message relay mechanism," in *Computing Networking and Informatics (ICCNI), 2017 International Conference on*, 2017, pp. 1-6.

[16] I. Korkmaz, S. K. Metin, A. Gurek, C. Gur, C. Gurakin, and M. Akdeniz, "A cloud based and Android supported scalable home automation system," *Computers & Electrical Engineering,* vol. 43, pp. 112-128, 2015.

[17] K. Okokpujie, E. Noma-Osaghae, S. John, and A. Ajulibe, "An Improved Iris Segmentation Technique Using Circular Hough Transform," in *International Conference on Information Theoretic Security*, 2017, pp. 203-211.