A FRAMEWORK FOR PHYSICAL HOME SECURITY USING MOBILE INTRUSION DETECTION SYSTEM

By

SHEFIU OLUSEGUN GANIYU *

ABIDEEN ISMAIL **

JOSEPH A. OJENIYI ***

TOHEEB ADEDIRAN ****

* Lecturer, Department of Information and Media Technology, Federal University of Technology Minna, Nigeria.
** Research Scholar, Department of Telecommunication Engineering, Federal University of Technology Minna, Nigeria.
*** Lecturer, Department of Cyber Security Science, Federal University of Technology Minna, Nigeria.
**** PG Scholar, Department of Cyber Security Science, Federal University of Technology Minna, Nigeria.

Date Received: 11/01/2019 Date Revised: 18/02/2019 Date Accepted: 04/03/2019

ABSTRACT

Physical Intrusion Detection Systems (PIDS) are deployed as complementary security measures to ensure safety of home and other edifices from burglars. Several systems have been proposed for physical intrusion using single or multiple detection sensors, surveillance cameras amongst others. Often, some systems send messages containing text, image, or video of suspected intruders to responders via wireless communication networks. However, the systems were custom-built from assemblage of disparate hardware components, which increased the cost of implementation and required some levels of expertise to setup. Also, research efforts to curtail false intrusion alerts from the PIDS have not been sufficiently addressed. Thus, this paper presents a framework for Mobile-based Physical Intrusion Detection System (M-PIDS) that turns smart mobile devices to PIDS for home or personal usage. Subsequently, the framework was conceptually and empirically validated for physical home security. In reality, the proposed M-PIDS could save cost, reduce false intrusion alert rate, and minimize setup effort, while increasing physical security for smart city dwellers.

Keywords: Intrusion Detection System, Physical Intrusion, Smart Home Security, Physical Security, Mobile Intrusion Detection.

INTRODUCTION

Generally, security means being safe from harm in digital and physical environments. As such, it has become something of interest not only to private and public organizations, but individuals as well. Thus, lots of security solutions, including software, hardware, and human security guards are deployed by those concerned to protect valuable assets from targeted and unintentional impairments. These efforts are responsible for the emergence of more enterprises and cottage industries that offer security products and services for domestic and industrial protections.

Physical security is an integral component of security policy, design, and implementation. It ensures protection of hardware, software, network infrastructures, data, and people from physical threats like burglary, vandalism, natural disaster, and terrorism (Harris, 2013; Rouse, 2016). Particularly, this component of security must be implanted to prevent invaders from having physical access to objects of value (Hutter, 2016). Thus, security devices like Closed-Circuit Television (CCTV), Burglar Alarm, Smoke Detector, Bodyguards, Gas Detector, Bulletproof Gadgets (door, window and vehicle) are installed by citizens to complement those provided by governments. Hence, an efficient physical security system for home usage should be layered on four factors consisting of environmental design, access control (mechanical and electronic), intrusion detection, and video monitoring (Oludele, Ayodele, Oladele, & Olurotimi, 2009).

In physical security, intrusion occurs when attackers used series of active and associated events to gain unlawful access into secured perimeter by breaking through doors or windows, tailgating and drudging access control devices. Really, the first line of defence against these attacks includes Physical Intrusion Detection Systems (PIDS), mantraps, alarm system, CCTV, guards, and motion detector (Hutter, 2016). While some of these countermeasures are conspicuously displayed to dissuade adversaries, others are hidden to covertly gather evidences about criminals in the act. In the latter case, crime data like time, location, tools, and specific features of attackers (e.g. voice, photograph, and fingerprint) are essential for forensic investigation.

Presently, smartphones have advanced beyond the conventional voice call and Short Message Service (SMS) facilities to include other utile hardware, namely - camera, memory, sensors, and wireless network modules. For example, sensors like accelerometer, gyroscope, digital compass, ambient light sensor, and proximity sensor are often used by device manufacturers and mobile application developers to create services that enhance users' experience. Similarly, the wireless network operators that provide connections for these portable devices have continued to mature in provision of data services to match user's connection requirements for active participations in Internet of Things (IoT). Thus, researchers are leveraging on the improvements recorded by smart devices and wireless networks to enhance PIDS (Choudhury, Choudhury, Pramanik, Arif, & Mehedi, 2015).

Security of smart home is an important requirement for smart city security (Hui, Sherratt, & Sánchez, 2017; Sharma & Thanaya, 2016; Smart Home - A fundamental constituent of a Smart City, 2017) and the increasing numbers of home burglars necessitated a system that can alert home owners (Sharma & Thanaya, 2016; Nwalozie, Aniedu, Nwokoye, & Abazuonu, 2015), as well as gather digital evidence to prosecute offenders. However, home security is often feebly handled in the realm of security (Hutter, 2016). This in turn, could have negative impact on the benefits envisaged from smart city due to intrusion. Meanwhile, existing studies focused on assemblage of sensors, GSM module, and microcontrollers to build custom devices for PIDS, which require additional cost and some levels of expertise to setup. Hitherto, Section 2 of this paper showed that PIDS that employs integrated set of features in mobile smartphones for intrusion detections is yet to be researched. Again, the section revealed that more research efforts are needed on how to distinguish human intruders from other animate beings, so as to reduce the number of false alarms (Suresh, Bhavya, Sakshi, Varun, & Debarshi, 2016).

Therefore, the aim of this paper is to develop a framework that utilizes the features of smartphone for user-friendly and low-cost physical intrusion detection, while reducing false alarms arising from non-human beings. To achieve this, the proposed framework utilizes in-built sensors and auxiliary components of smartphones or personal computer for intrusion detection. Also, it classifies the image captured from camera or motion detector as either human or non-human. In addition, it sends information about trespass to registered stakeholders for prompt response to intrusion alert.

1. Related Literature

Chen and Wang (2006) developed alarm system for smart home using ZigBee technology. The system could detect occurrences like water flooding, smoke, gas leak, intrusion through windows, doors, etc., and sends alert signal when the need arises. Also, Assaf et al. (2012); Bangali and Shaligram (2013) separately designed systems with different architectures that could detect home security occurrences that are similar to Chen and Wang (2006). While Assaf et al. (2012) implemented their system with Field Programmable Gate Array (FPGA) and user interacts with the solution through web-based interface and alert is received by the user via email, Bangali and Shaligram (2013) utilized GSM model to send email and SMS to user. In their study, Sharma, Mohammed, Kalita, and Kalita (2014) paid more attention to communication existing between intrusion detection system and user by developing an Android application that repeatedly inform user about possible intrusion through mobile interface.

Furthermore, Govinda, Prasad, and Susheel (2014) proposed and implemented intrusion detection system for intelligent home using laser ray as light dependent resistor. The system is capable of sending SMS using GSM module when laser sensor detects intruder. As well, Parab, Joglekar, and Parab (2015) developed low-cost home security system using Global System for Mobile Communication (GSM), magnetic sensor nodes (for intrusion through door), and microcontroller. The system sends SMS to registered mobile number whenever intrusion occurs. Again, Zhao and Ye (2008) built similar security system with GSM and General Packet Radio Service (GPRS) wireless networks, magnetic sensor nodes (for intrusion through door), and infrared security node (to detect human body). The system was able to send both voice and picture to mobile device of the home owner. Using similar intrusion detection mechanism but different sets of hardware (Eseosa & Promise, 2014; Huang, Xiao, Meng, & Xiong, 2010; Kumar et al., 2015) exchanges text message between home security system and owner using GSM and Wireless Sensor Network (WSN). In the case of Eseosa and Promise, (2014); Kumar, et al., (2015) detectors for gas, smoke, temperature, proximity (PIR) and light dependent resistors were utilized to detect unusual occurrences at home. Also, Farid, Rehan, Faizan, and Qadri (2010) demonstrated the possibility to remotely control home security systems using Public Switched Telephone Network (PSTN). Instead of using PIR, Cortez et al., (2016) used ultrasonic sensor to detect home intruder and sends SMS to home owner.

Also, Toochi and Ibe (2014) advanced an intrusion detection system using combination of infrared device, PIC 168F77A Microcontroller, and webcam connected to laptop, which takes snapshots of intruder. Though, the system could alert user of intrusion via SMS using GSM module, it cannot send snapshots to online storage location. In related studies, but using different microcontrollers, Nwalozie et al. (2015); Joseph, Nwankwo, Eniola and Eneh, (2015); Potnis, Chimnani, Chawla, and Hatekar (2015); Rajani and Kadari (2017) developed home intrusion detection systems which used pyroelectric (passive) infrared (PIR) sensor to detect human body, microcontroller to control activities between the sensor and GSM to send SMS or calls home owner when it detects burglar. Nevertheless, Potnis et al. (2015) used infrared sensor, the researchers used relay to switch on the camera that snaps picture of burglar when an SMS is received from home owner by the system.

Additionally, Suresh et al. (2016) developed security system for home monitoring with PIR and other sensors to detect changes in temperature and humidity, the authors used Arduino as microcontroller. Likewise, the system developed by Sunehra and Bano (2014) which was aided by internet-enabled webcam could send alert to GSM and upload video to cloud storage once unauthorized access is detected by PIR and IR sensors that were controlled by ARM7 microcontroller. Using combination of Arduino and surveillance camera, Sharma and Thanaya (2016); Zeki, Elnour, Ibrahim, Haruna, and Abdulkareem (2013) developed neighbourhood watch security systems (NWSS) which stores trespasser's images in offline and online modes. The system developed by Zeki, Elnour, Ibrahim, Haruna, and Abdulkareem (2013) used PIR and it could communicate intrusion to people on web platform and Android device. However, Sharma and Thanaya (2016) utilized ultrasonic for (motion detection) amongst other sensors, but GSM and IoT were employed for offline and online communication, respectively.

Moreover, transmitting and storing images and videos of intruders via wireless or wired connections in real-time to monitoring centres were notable contributions of Zhai, and Cheng (2011). Likewise, the authors utilized several sensors together with PXA270 Xscale and single chip as core hardware. Also, Rakesh, Sreesh, and George (2012) developed real-time surveillance system to detect interloper with the aid of PIR, webcam, and ZigBee protocol. The system sends video to remote location using File Transfer Protocol (FTP) and SMS to registered number from a computer system designed with Beagle-Board Single Board Computer.

Besides, Kodali, Jain, Bose, and Boppana (2016) approached smart wireless home security from IoT standpoint. The prototype system developed by the authors was used to manage and control domestic security and electrical appliances from the Internet using TI-CC3200 Launchpad board, which has embedded microcontroller and Wireless Fidelity (Wi-Fi) capability. Thus, home owner can use any internet enabled phone to interact and receive message from the system using other internet access points apart from GSM module. Nevertheless, the system did not have provision to capture trespasser's picture.

A common trend among the reviewed literatures revealed that most of the home intrusion detection systems used GSM module, motion detector (infrared or magnetic contacts), microprocessors, and sensors for motion, voice, humidity, temperatures, etc. As such, the intrusion detection systems were packaged as separate hardware devices, often requiring configuration or display of status information through Liquid Crystal Display (LCD). Correspondingly, varying costs were incurred on their implementations and installations, despite being economical and affordable compared to those manufactured for industrial usage as claimed by previous authors (Parab et al., 2015; Toochi & Ibe, 2014; Rajani & Kadari, 2017). Currently, some smart mobile devices have inbuilt sensors and peripherals that can be tailored toward achieving some functionalities implemented by the existing systems. Thus, a study that explores the features of smart mobile devices for home intrusion detection could be worthwhile.

2. Proposed Framework

This section presents high-level overview and detailed view of the proposed framework. The former presents brief discussion of the four units in the framework and the latter provides detailed explanation of each unit. Henceforth, this framework would be referred to as Mobile Physical Intrusion Detection System (M-PIDS). The framework offers user many choices over the kind of wireless network, the type, and cost of mobile device to use for intrusion detection. Thus, its implementation could be considered affordable and economical as the cost of external sensors, LCD, and Web camera are eliminated.

2.1 High-level Overview of the Framework

The high-level overview of M-PIDS as shown in Figure 1 consists of four units. Among these units are; smart mobile devices, networks, and responders, which are referred to as core units, whereas personal computer is regarded as optional unit. This framework is designed to employ inbuilt sensors and camera on smart mobile device to monitor intruders and alert home owners or other responders through wireless connections. Also, M-PIDS could classify suspected intruding objects as either human being or inanimate using some existing algorithms. In spite of computing limitation of some mobile devices, implementation and execution of the classification algorithm can be optionally transferred to other personal computers with better processing facilities and subsequent result will be returned to the mobile device.

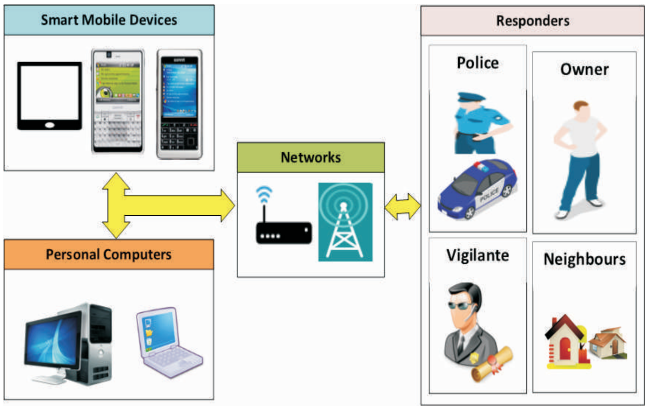

Figure 1. High-level Overview of M-PIDS

2.2 The Detailed M-PIDS Framework

This section further illustrates the proposed framework with exhaustive diagram as shown in Figure 2, as well as, comprehensive descriptions of the four units as presented in following subsections. Furthermore, the framework was validated with the four factors of physical home intrusion detection reported by Oludele et al. (2009).

2.2.1 Smart Mobile Device Unit

The mobile device unit comprises of wide range of smart devices with some built-in sensors and camera. It has the ability to send or receive messages in form of SMS, Multimedia Messaging Service (MMS) or video files through wireless network unit. Generally, some sensors are meant to acquire information about environmental factors like temperature, humidity, light, etc. Also, most smart devices have cameras which could snap

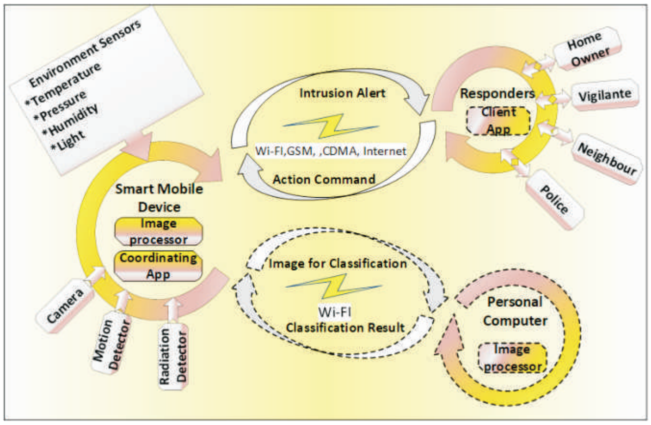

Figure 2. Detailed M-PIDS

photographs and record videos. In addition, the devices are sensitive to motion and some could even detect certain radiations with or without external peripherals. Though, the sensors and cameras could vary in terms of sensitivity based on device manufacturers, but one advantage is that they all came bundled with mobile device. Therefore, they could be channelled toward intrusion detection amongst other purposes from security and system development point of views.

Again, the unit establishes wireless network connections with responders. Unlike previous researches, there is no need to construct separate hardware module (GSM, CDMA) for network connectivity in M-PIDS. That is, the unit communicates intrusion information to responders by encapsulating them in message medium like SMS, MMS, or client app (M-PIDS-Client) on responder mobile device. Similarly, action commands which inform the unit about responder's next line of action are encapsulated and delivered to the unit via same messaging media.

Another feature of this unit is the increasing computing capabilities of emerging mobile devices which enable them to run fairly complex searching, sorting, or encryption algorithms. Hence, this unit runs the coordinating mobile application (app), which serves as control centre for all activities relating to M-PIDS in the mobile phone, as well as, managing communication between the unit and other units. In addition, the unit hosts image processing algorithm that classifies snapshot of intruding objects as either human or non-human without referring such decision to responders. Otherwise, when optionally configured, the unit sends image file or video to Personal Computer (PC) unit for image classification and receives result from the PC unit using onboard Wi-Fi module. For any other reasons, when classification of image snapshot cannot be digitally performed, then the raw image file will be sent to responders. The essence of image processor is to minimize the number of false alerts due to non-human intruders from being sent to responders, which invariably reduces the cost of sending such disturbing alerts.

2.2.2 Network Unit

The network unit connects other units both locally and remotely through wireless connection channels like GSM, Code Division Multiple Access (CDMA), Wi-Fi, and internet. Thus, the unit provides the communication links between smart mobile device and responders units, as well as between the mobile device and personal computer units.

2.2.3 Responder Unit

Responder unit includes the owner of M-PIDS, security agents, vigilantes, and neighbours who are registered to act on alert messages emanating from smart mobile device unit. Accordingly, each responder is expected to have a device that can receive SMS, MMS, or image file from mobile device unit and ability to send action command to mobile device unit. Optionally, client mobile app (M-PIDS-Client) could be installed on responder's device to enable communication with mobile device unit to further reduce the cost of SMS or MMS. Recipients of intrusion alert would be enrolled in smart mobile device unit by the home owner, and this can be done even from remote location. All the responders can take same or differentiated actions upon receipt of intrusion alert by physically visiting the intruded home or sending command to smart mobile device unit or follow established security countermeasures or crime reporting routines.

2.2.4 Personal Computer Unit

This unit, which is represented with dashed line in Figure 2, is optional. Again, depending on the computing capacity of smart mobile device, resource intensive tasks that are beyond the processing power of smart mobile unit can be deployed to laptops and desktop computers as auxiliary processing devices. One of such tasks is image processing. In this case, smart mobile unit sends raw images/snapshots to personal computer unit for classification as either human or non-human. Subsequently, the result of the classification is returned to smart mobile unit for subsequent decision making.

2.3 Framework Validation

This study employed conceptual and experimental validations to ascertain the completeness of the framework and to test the performance of its prototype implementation, respectively. Indeed, conceptual validation was used by Liu, Yu, Zhang, and Nie (2011) as worthwhile approach to validate conceptual model. In reality, the approach is to ensure that a model reasonably meets its envisioned uses. Thus, it suffices to mention that M-PIDS as proposed in this paper has addressed the requirement of physical intrusion detection system for home use as outlined by Oludele et al. (2009). That is, the components available in M-PIDS could be aligned to meet or serve the four factors earmarked by Oludele et al. (2009) as shown in Table 1.

In order to carry out empirical validation on the proposed framework, its prototype was developed. The prototype comprised the implementations of the four units in the framework. The mobile and PC units were implemented on Android and Windows platforms, respectively. Figure 3 shows the captured image by mobile device unit which was received for processing by PC unit.

Factor Required by Oludele et al. (2009)	Corresponding M-PIDS Component
Environmental factors	Temperature, pressure, humidity, light sensors, radiation detectors
Physical access control (mechanical and electronic)	Motion detector, coordinating and client apps
Intrusion detection	Image processor, coordinating and client apps
Video monitoring	Camera

Table 1. Conceptual Validation

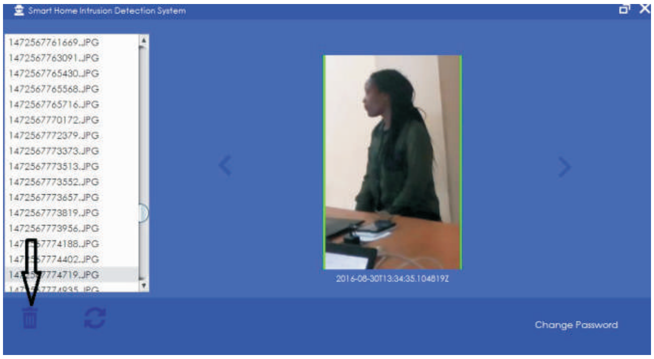

Figure 3. Image for Processing by PC Unit

The experimental validation was conducted to test operational accuracy of the M-PIDS. Specifically, the testing was carried out with a total of 37 trials using animate objects. The implemented setup was placed in front of a closed door and intrusion detection process is triggered when the door is open and objects enters through the door. The essence of the experimental validation is to test how the prototype could accurately classify an intruding object as either human being or not. Thus, they measured the accuracy of the prototype using true positive or correct detection rate ($R_{correct}$) and false positive or false alarm rate (R_{false}) as expressed in equations (1) and (2) (Wei, 2007).

$$R_{correct} = \frac{\text{number of true positive detections}}{\text{total number of detections}} \text{ x } \frac{100}{1} \quad (1)$$

$$R_{false} = \frac{\text{number of false positive detections}}{\text{total number of detections}} \text{ x } \frac{100}{1} \quad (2)$$

Table 2 shows result of the evaluation with the smartphone fixed at varied distances of 4 and 8 meters away from targeted objects. Though the distances were arbitrarily chosen, other environmental factors like lightning and temperature were unaltered throughout the validation exercise. The result revealed that the best correction rate of 75.67% was obtained when the objects were 4 meters away, while the worst false detection rate was 37.83%. Furthermore, the result showed that correct detection rate decreases as the distance between mobile device unit and object of interest increases. This decrease in accuracy could be partly attributed to quality of the image produced by the mobile device camera (8 Megapixel) and other environmental factors listed in

Distance (m)	No. of True Positive	No. of False Positive	$R_{correct}$ (%)	R_{false}(%)
4	28	9	75.67	24.32
8	23	14	62.16	37.83

Table 2. Experimental Validation

Table 1. For all the trials, SMS were promptly delivered to mobile device of responders, to report perceived intrusion cases via GSM network.

Conclusion and Future Works

Protecting tangible assets within a confinement from intruders is one of the functions of physical security, which also concerns everybody. Thus, physical intrusion detection systems that employ tools and techniques are being deployed to detect or dissuade intrusion within given perimeter. Very likely, using mobile device for intrusion detection presents some advantages over static intrusion detection mechanism in terms of implementation cost, mobility, and simplicity of operations. Similarly, image captured using camera on smart mobile devices and some environmental sensors utilized by M-PIDS could aid identification and detection of intruders, respectively. As well, responders to intrusion incidents could leverage on other features of smart mobile devices like wireless network modules, location and time information to communicate, and track intruders amongst others. Above all, the outcome of the validation conducted on the proposed M-PIDS framework and its prototype revealed that the envisaged benefits of smart city, which is branch of IoT could be realized with appropriate deployment of personal and mobile intrusion devices.

In future, the authors plan to extend the prototype developed in this paper with more functionalities to handle more environmental factors relating to real intrusion scenarios. Also, the evaluation will be expanded to include statistical analysis of images captured under differing environmental conditions. Similarly, the effect of the coordinating app and image processor on normal functioning and resources utilization of host devices will be verified.

References

[1]. **Assaf, M. H., Mootoo, R., Das, S. R., Petriu, E. M., Groza, V., & Biswas, S. (2012, May).** Sensor based home automation and security system. In *2012 IEEE International Instrumentation and Measurement Technology Conference Proceedings* (pp. 722-727). IEEE.

[2]. **Bangali, J., & Shaligram, A. (2013).** Design and implementation of security systems for smart home based on GSM technology. *International Journal of Smart Home*, 7(6), 201-208.

[3]. **Chen, D., & Wang, M. (2006, November).** A home security ZigBee network for remote monitoring application. In *Inst. Eng. Technol. Int. Conf. Wireless Mobile Multimedia Netw.* (pp. 1-4). doi: 10.1049/cp:20061246

[4]. **Choudhury, B., Choudhury, T. S., Pramanik, A., Arif, W., & Mehedi, J. (2015, March).** Design and implementation of an SMS based home security system. In *2015 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT)* (pp. 1-7). IEEE.

[5]. **Cortez, C. D., Santos, J. L., Alberto, K. M., Kua, P. O., Muncada, R. C., and Pontiveros, K. R. (2016).** Development of Multi-Home Alarm System Based on GSM Technology, *International Journal of Electronics and Electrical Engineering*, 4(4), pp. 365-369.

[6]. **Eseosa, O., & Promise, E. (2014).** GSM based intelligent home security system for intrusion detection. *International Journal of Engineering and Technology*, 4(10), 595-605.

[7]. **Farid, F., Rehan, M., Faizan, F., & Qadri, M. T. (2010, June).** Home automation and security system via PSTN. In *2010 2nd International Conference on Education Technology and Computer* (Vol. 1, pp. V1-52). IEEE.

[8]. **Govinda, K., Prasad, S. K. and Susheel, S. R. (2014).** Intrusion detection system for smart home using laser rays. *International Journal for Scientific Research & Development,* 2(3), 176-178.

[9]. **Harris, S. (2013).** *Physical and Environmental Security: CISSP Exam Guide,* 6th Ed. USA: McGraw-Hill.

[10]. **Huang, H., Xiao, S., Meng, X., & Xiong, Y. (2010, April).** A remote home security system based on wireless sensor network and GSM technology. In *2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing* (Vol. 1, pp. 535-538). IEEE.

[11]. **Hui, T. K., Sherratt, R. S., & Sánchez, D. D. (2017).** Major requirements for building smart homes in smart cities based on Internet of Things technologies. *Future Generation Computer Systems*, 76, 358-369.

[12]. **Hutter, D. (2016).** Physical Security and Why It Is Important. SANS Institute Information Security Reading Room, 1-31.

[13]. **Joseph, G. M., Nwankwo, E. L., Eniola, O. M., and Eneh, C. D. (2015).** Design of a Real-Time Microcontroller Based Gsm-Embedded Intrusion Security System, *International Journal of Scientific & Engineering Research*, 6(12), 232-241.

[14]. **Kodali, R. K., Jain, V., Bose, S., & Boppana, L. (2016, April).** IoT based smart security and home automation system. In *2016 International Conference on Computing, Communication and Automation (ICCCA)* (pp. 1286-1289). IEEE.

[15]. **Kumar, M. S., Mounika, M., Pavani, L. R., Ranadeep, E., Siddhartha, B., & Subramanyam, K. B. V. S. R. (2015).** GSM based Industrial Security System. *International Journal of Current Engineering and Scientific Research*, 2(5), 33-38.

[16]. **Liu, J., Yu, Y., Zhang, L., & Nie, C. (2011).** An overview of conceptual model for simulation and its validation. *Procedia Engineering*,24,152-158. https://doi.org/ 10.1016/j.proeng.2011.11.2618.

[17]. **Nwalozie, G. C., Aniedu, A. N., Nwokoye, C. S., & Abazuonu, I. E. (2015).** Enhancing home security using SMS-based Intruder Detection System. *International Journal of Computer Science and Mobile Computing*, 4, 1177-1184.

[18]. **Oludele, A., Ayodele, O., Oladele, O., & Olurotimi, S. (2009).** Design of an automated intrusion detection system incorporating an alarm. *Journal on Computing*. 1(1), 149-157.

[19]. **Parab, A. S., Joglekar, A., & Parab, A. S. (2015).** Implementation of home security system using GSM module and microcontroller. In *International Journal of Computer Science and Information Technologies,* 6(3), 2950-2953.

[20]. **Potnis, M., Chimnani, A., Chawla, V., Hatekar, A. (2015).** Home security system using GSM modem, *Int. J. Eng. Res. Appl*., 5(4), 143-147.

[21]. **Rajani, U. S., & Kadari, A. A. (2017).** GSM based Home Security System using PIR sensor. *Int. Journal of Engineering Research and Applications*, 8(2), 87-89.

[22]. **Rakesh, V. S., Sreesh, P. R., & George, S. N. (2012, December).** An improved real-time surveillance system for home security system using Beagle Board SBC, ZigBee and FTP webserver. In *2012 Annual IEEE India Conference (INDICON)* (pp. 1240-1244). IEEE.

[23]. **Rouse, M. (2016).** *Physical Security.* Retrieved from https://searchsecurity.techtarget.com/definition/physical-security

[24]. **Sharma, R. K., Mohammad, A., Kalita, H., & Kalita, D. (2014, February).** Android interface based GSM home security system. In *2014 International Conference on Issues And Challenges In Intelligent Computing Techniques (ICICT)* (pp. 196-201). IEEE.

[25]. **Sharma, N., and Thanaya, I. (2016).** Multilayered Home security system with backup capability. *Advances in Computer Science and Information Technology*, 3(5), 413-416.

[26]. **Smart Home - A fundamental constituent of a Smart City.(2017).** *Smart City Press.* Retrieved from http://www.smartcity.press/smart-home-a-fundamental-constituent-of-smart-city/ [Accessed: 11-Feb-2018].

[27]. **Sunehra, D., & Bano, A. (2014, December).** An intelligent surveillance with cloud storage for home security. In *2014 Annual IEEE India Conference (INDICON)* (pp. 1-6). IEEE.

[28]. **Suresh, S., Bhavya, J., Sakshi, S., Varun, K., & Debarshi, G. (2016, November).** Home monitoring and security system. In *2016 International Conference on ICT in Business Industry & Government (ICTBIG)* (pp. 1-5). IEEE.

[29]. **Toochi, E., & Ibe, O. G. (2014).** A microcontroller based Intrusion Detection System. *International Journal of Engineering Research and Applications*, 4(11), 69-79.

[30]. **Wei, L. (2007).** Evaluation of Intrusion Detection Systems. University of Auckland.

[31]. **Zeki, A. M., Elnour, E. E., Ibrahim, A. A., Haruna, C., & Abdulkareem, S. (2013, November).** Automatic interactive security monitoring system. In *2013 International Conference on Research and Innovation in Information Systems (ICRIIS)* (pp. 215-220). IEEE.

[32]. **Zhai, Y., & Cheng, X. (2011, August).** Design of smart home remote monitoring system based on embedded system. In *2011 IEEE 2nd International Conference on Computing, Control and Industrial Engineering* (Vol. 2, pp. 41-44). IEEE.

[33]. **Zhao, Y., & Ye, Z. (2008).** A low cost GSM/GPRS based wireless home security system. *IEEE Transactions on Consumer Electronics*, 54(2), 567-572.

ABOUT THE AUTHORS

Dr. Shefiu Olusegun Ganiyu is a Lecturer in the Department of Information and Media Technology at Federal University of Technology Minna, Nigeria. He holds a PhD in Computer Science in risk-aware access control for pervasive environments. Similarly, he has obtained Bachelor degree in Mathematics/Computer Science and Master Degree in Information Science from Federal University Minna and University of Ibadan, respectively. Prior to joining academic environment, he acquired valuable work experience as programmer/information system developer. His research interests include Information Technology Risk Management, Risk-Adaptive Access Control, Pervasive Computing including Bring Your Own Device (BYOD) and Physical Security. Also, he participates in projects involving information systems security and development.

Abideen Ismail is currently working towards his PhD in Telecommunication Engineering from Federal University of Technology FUT Minna. He had Degrees in Electronics Engineering from University of Maiduguri Unimaid and Computer engineering from Ladoke Akintola University of Technology LAUTECH. His current area of interest is in Detecting Covert Members from Criminal Networks. He is a staff of Unimaid.

Dr. Joseph A. Ojeniyi is a Lecturer in the Department of Cyber Security Science at School of Information and Communication Technology, Federal University of Technology (FUT) Minna, Nigeria. He received his PhD in Cyber Security Science from the same University, M.Sc. in Computer Science from University of Ibadan, Nigeria and a B.Tech. in Mathematics/Computer Science from FUTMinna, Nigeria. He has been appointed as a reviewer to several indexed Journals. He currently serves as the chairman of Conference Organizing Committee of the faculty, 'ICTA 2018' and the assistant coordinator of cyber security science postgraduate programmes. His area of interest includes Cyber Security, Digital Forensics, Deep Learning, Artificial Intelligence in Information Assurance/Security, and Cyber Physical Systems.

Toheeb Adediran holds a Bachelor Degree in Information and Media Technology from Federal University of Technology, Minna. Also, he is a Certified Ethical Hacker and currently a prospective Master Degree student in Cyber Security Science. His research Interest is in Information System Security.