**PROJECT PROPOSAL TOPIC**:

DEVELOPMENT OF SMART INTRUTION DETECTION AND ALARM SYSTEM TO CURB THEFT VANDALIZATION OF TELECOMMUNICATIONS INFRASTRUCTURE

**PRESENTED BY**

JOSHUA OLAMILEKAN OLANIYAN

19/67EC/00871

KWARA STATE UNIVERSITY

ENGINEERING AND TECHNOLOGY FACULTY

THE DEPARTMENT OF ELETRICAL AND COMPUTER ENGINEERING

**SUPERVISED BY:**

DR. MUSA ABDULWAHEED

**ABSRACT**

Network interruption is one of the major problems of telecommunication companies due to the fact that there are high activities of vandalization on the onsite telecommunication infrastructure. The effect of this act vandalization affect the quality of services rendered from poor data management and internet connectivity, short message services (SMS) been undelivered or aborted, drop calls and failed calls countless times and much other effect. Development and implementation of this system would help reduce, curb and control the kind of people that enter onsite where the telecommunication infrastructures are kept by creating a motion detector and alarm system that can also send signals to the nearest telecommunication station for quick response.

**INTRODUCTION**

A security system monitors a building or other protected area for intrusion trespassing or unauthorized entry into building or other protected areas preventing danger or vandalization of both life and properties. Since the development of modern technology, business and industries, several forms of protection system have been extensively used in protection of life and vandalization or damage of property.

In recent years, the significance and demand of security system have been clearly increasing as well, especially in urban settlement having to protect telecommunication infrastructure is essential since most of the infrastructure are based in environment where fewer human activities are carried out. Studies also have shown that intrusion related crimes happen less in places that have at least a security system installed.

Intrusion detector system and monitoring were previously impossible to compete without human intervention. However, to deal with this problem given how technology is developing, sensor-based intrusion detection system is functionable with minimal human involvement to safe guard properties and life whether authorized personnel are on site or not. This sensor-based intrusion would help protect telecommunication infrastructure and with the inclusion of alarm and SMS signal it is easier to alert neighboring law enforcement agencies and receive help withing short period of time. This intrusion detection system would reduce theft vandalization in telecommunication infrastructure by scaring away potential treat away. This system is a developed with a low-cost equipment but still achieves it aim of protecting telecommunication infrastructure like telecommunication mast and control stations.

**PROBLEM STATEMENT**

The issue of theft vandalization on telecommunication infrastructure tends to affect quality of service rendered thereby restricting the flow of information at times when necessary and can also lead to loss of data, money and affect the income flow of those that make living from telecommunication industries. The sensor-based intrusion detection system would provide solid protection and awareness by sending alarm and SMS when it senses any form of malicious activities or movement around telecommunication infrastructure.

**AIM & OBJECTIVE**

* Aim of the Project

This project aims to develop a security system for telecommunication infrastructure against theft vandalization using sensor-based intrusion detection system.

* Objective of the Project
* To develop a sensor-based intrusion detection system
* To send signal of suspected movement around telecommunication infrastructure like the telecommunication mast, control station.

**PURPOSE & RELEVANCE OF PROJECT**

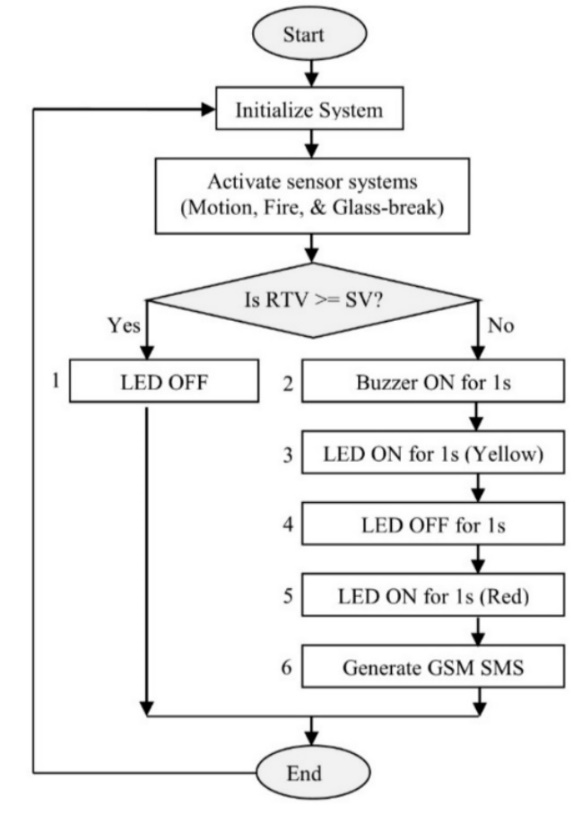
The purpose of the study is to help develop a security system that would protect telecommunication infrastructure from theft vandalization. This study shows how sensor-based intrusion system would help protect this infrastructure and help telecommunication bodies curb expenses. This project also tends to answer the question of how it improves quality of service rendered by different telecommunication organization. This is a form of protection against theft vandalization on telecommunication infrastructure majorly telecommunication mast, control station.

**LITERATURE REVIEW**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| S/N | Authors | Focus | Methodology Used | Strength Of Idea | Weakness of Idea |
| 1 | Saikumar Iyer  (2020) | IoT based Intruder Detection System Using GSM | Mobile network (GSM) serves as the system's interface for communication between the user and the hardware module. The ATMEGA8A-PU serves as the system's brain in our setup. It is an 8-bit AVR RISC-based Microcontroller with good performance and low power. Only registered numbers can receive the SMS alert of intrusion when this is used with an application, which can be switched on and off once the essential registration is completed. | It can be controlled an app which disable the alarm when there is a false alert as well as an option to put the device in the power down mode. | It is unpredictable and hacks can render the system ineffective. |
| 2 | Philokypros P. Ioulianou (2018) | A Signature-based Intrusion Detection System for the Internet of Things | The seven-layer model from Cisco is the most in-depth of the various proposed IoT reference models, and it was chosen for this work. This work displays the CISCO model's layers; however, we are mostly interested in Levels 1-3. Physical devices that communicate or receive created or filtered data are Level 1 smart devices. The connectivity between the devices, whether it be inside the same network or across separate networks, is referred to as Level 2. IoT devices should be able to send data reliably on current networks. Data transformation and analysis are on level 3 | This IDS module is connected via wired communication channels in order to avoid jamming or other types of wireless attacks. | This system is prone to attack at the physical level |
| 3. | Khirod Chandra et U.C (2017) | IoT Based Intrusion Detection System Using PIR Sensor | The suggested system comprises of an alert generation system that, when an intrusion is discovered by SMS, is utilized to alert the resident of the home or business. In this study, a public server by ThingSpeak is employed for monitoring and recording intrusion. Then a CCTV surveillance system is installed to keep an eye on the region. | It is easy to detect false alarm and high monitoring from remote area is effective. |  |
| 4. | Geethanjali T M, Raushani Kumari (2018) | Security System using Arduino | When it comes to how the system functions, electricity is its only source of power. The ultrasonic sensor emits ultrasonic waves when it is in operation. When an intrusion occurs, it bounces the ultrasonic signal back to the echo pin to determine how far away the invader is from the sensor. The LED lights begin to blink, and the sensor begins to make noise when it finds an object. | It enables real-time awareness and alerts from your home, and combating many of the vulnerabilities you will find on other types of system | The signal produced by the sensor can be jammed and can take the sensors anywhere from a few minutes to three hours to reestablish communication with the object |
| 5. | Shoewu, O.O., Ayangbekun Oluwafemi J., Johnson Emmanuel O (2020) | Design and Construction of Micro-Controller Based Intrusion Detector | Using an assembly language programming compiler that has been used at the micro integrated development environment, a microcontroller is purchased and programmed with the fundamental codes to do the desired operation (MIDE). Also, using a universal programmer and other circuitry, this compiler translates assembly language codes into machine or HEX codes that are then prepared to be burned into the microcontroller's ROM and other circuitry that is tested for ratings verification and defective parts identification. The circuit diagram was created with tested circuits from standardized sources and common electronic components. | it is reliable and can be monitored | This system cannot work without electricity |
| 6. | Imran Chowdhury, Taslim Ahmed (2021) | Design and Prototyping of Sensor-based Anti-Theft Security System using Microcontroller | The Atmega8 microcontroller is used in this project and is connected to a temperature sensor, an LDR motion sensor, a precision temperature sensing IC with an output voltage linearly proportional to temperature, and a glass sensor. The buzzer, led bulb, and SMS module are then connected to the microcontroller as output devices. | Without electricity this system is backed by a sun tracking solar system | This cannot work during the night time. |
| 7. | Rao Kamran Javed (2022) | A Novel Approach Using Deep Learning for Network Based Intrusion Detection System | The intrusion detection system based on deep neural networks is represented by our proposed model. The shallow machine learning based models and the signature-based intrusion detection systems were commonly replaced by DNN based IDS because they provide more accurate results than the prior ones. The first dataset has four different assault types, while the second dataset has nine different attack types. Since there are some missing values in the datasets. In our approach, rows with missing values are removed from the dataset in the first scenario, and text data is transformed into numerical values in the second scenario. |  | With the use of dataset leakage of data can incur an attack |
| 8. | Markus Ring (2019) | A Survey of Network-based Intrusion Detection Data Sets | Depending on the format, either flow-based or packet-based network traffic is collected. Mirroring ports on network devices is typically how network activity is captured at the packet level. All payload data is included in packet-based data. Flow-based data are more aggregated and typically just include network connection metadata. |  | With the use of dataset leakage of data can incur an attack |
| 9. | Olutosin Taiwo (2021) | Enhanced Intelligent Smart Home Control and Security System Based on Deep Learning Model | An intelligent smart home automation system with a variety of features and a multipurpose smart home automation system are designed and developed in this project. It is suggested that a CNN deep learning model be used to improve our system's ability to detect unusual invader movement. | Human interference is highly minimal |  |
| 10. | Dhanke Jyoti Atul (2021) | A machine learning based IoT for providing an intrusion detection system for security | This model is built on the IoT-based CBS system for efficient machine learning techniques in communication. Here, many machine techniques are assessed using various performance rating criteria in order to provide an efficient machine learning technique. |  |  |
| 11. | Zipporah Tarus (2017) | PIR Sensor-based Security System | The goal of development is to provide a cheap security system for domestic use. Little PIR (Pyroelectric Infrared) sensors built around a microprocessor are used by the system. The microcontroller detects infrared emissions from a human body to determine human motion. The central controller and the equipment required for home security and monitoring are connected by cables in the home security system. | It is cost effective both o build and install | Can detect a body farer than 10meters |
| 12. | Arya Singh S (2016) | Design and Simulation of Elephant Intrusion Detection System | To detect elephants, the device primarily uses microphones and IR LEDs. A microphone that is placed 50 meters from the housing colony is the focus of the first level of detection. It records audio, sends it through an FM transmitter, and then uses MATLAB to analyze the received signal. With this first-level sensor system, we may thus detect an elephant's incursion up to 50 meters away from a human settlement. | It gives signals quicker from a far range. |  |
| 13. | Prerna Bhatnagar (2019) | Smart Security and Intrusion Prevention System | The Smart Security and Intrusion Prevention system has a rather straightforward overall structure. It is made up of an Arduino board as the primary microcontroller, a PIR sensor for heat signature detection, and an IR sensor for motion detection. The Arduino board, which is connected to a power source and a computer, has the sensors attached to it. Also, a buzzer that is attached to the board and activates when there is an intrusion | The system has a friendly user interface and employs some methods to reduce power consumption |  |
| 14. | Difan Zhang, Wei Yu, Rommie Hardy (2011) | A Distributed Network-Sensor Based Intrusion Detection Framework in Enterprise Networks | It examines incoming and outgoing traffic as well as other questionable host behavior and malicious activity detection. the effective identification, analysis, and aggregation of suspicious traffic and system records using a deep packet inspection (DPI) technique. Attack alarms will be sent to the network administrator if compromised hosts are found, who may then take additional action to recover the compromised hosts and address the system vulnerability. | It can prevent the same kind of attack to happen again. |  |
| 15. | Imran, Faisal Jamil, Dohyeun Kim (2021) | An Ensemble of Prediction and Learning Mechanism for Improving Accuracy of Anomaly Detection in Network Intrusion Environments | The ensemble of learning and prediction models serves as the foundation for the intrusion detection system. Training comes first, followed by deployment in an environment where intrusion detection is used. the initial stage of the ensemble intrusion detection model's methodology, which is based on extensive datasets. Using feature engineering methods, two extensive benchmark datasets are created to evaluate the effectiveness of the suggested ensemble model. |  | Large data set required |
| 16. | Akeem T. Otapo (2019) | OFFICE- AUTOMATED INTRUSION DETECTION SYSTEM (O-AIDS) | Construction, simulation, and modeling are involved in this. The Office Automated Intrusion Detection System (O-AIDS) was built with the help of the Arduino Mega and Arduino Uno microcontrollers, a passive infrared sensor, an alarm buzzer, a keypad module, a liquid crystal display (LCD), a camera module, a push button, a resistor, a toggle switch, a jumper wire, a light-emitting diode (LED), an IP camera relay module, a GSM Following construction, Proteus Simulator was used to simulate the system. | It has a provision for expansion in a large space | It does not support weather climate therefore can’t be used outdoor |
| 17. | Zhi Sun, Pu Wang (2010) | Border Sense: Border patrol through advanced wireless sensor networks | The foundation of current WSNs for border patrol is a flat, uniform architecture where each sensor has the same physical capabilities and can only interface with. Such a framework causes a number of border patrol issues, including limited coverage and a high false alert rate, which necessitate additional human intervention. As an alternative, we take into account a hierarchical WSN architecture with diverse sensor nodes. Three different types of sensors are used in three separate stages of the hierarchy in this system. | Limited coverage | It needs more human intervention than necessary |
| 18. | Abhishek S. Parab, Amol Joglekar (2015) | Implementation of Home Security System using GSM module and Microcontroller | This system is built on an 8051 microcontroller, which runs code for a certain activity. The GSM modem will take the necessary measures, i.e., notify the owner of an intruder or a hazard to the home. This gadget must be mounted on the door; when an intruder opens the door, the magnet inside it disengages from the relay, causing the LED to glow red, signaling the GSM modem to take the necessary action. | The GSM technology gives a good response after received a message of particular action from microcontroller |  |
| 19. | Amit Kumar (2017) | Border Security System using Arduino & Ultrasonic Sensors | The system is built in such a way that it requires the least amount of human assistance and constant monitoring of the area it is used to secure. The system's eyes that detect the intruder are the ultrasonic sensors. The RADAR, buzzer, and signaling LEDs are then activated via sensors. These outputs' actuations are based on several sensor systems. For greater system precision, rotational sensors activate the RADAR while stationary sensors activate the buzzer and Lights. Servomotors are used to program the rotatory sensors to rotate back and forth between a variety of angles. | Can detect from a large range of distance. | It is cannot filter false alarm |
| 20. | Mohamad Huzaimy Jusoh (2015) | Wi-Fi and GSM Based Motion Sensor for Home Security System Application | The transmitting and receiving components of the system are divided into two segments. The microcontroller is connected to the motion sensor, camera, RF transmitter, SD card, solar panel, and batteries for the transmitting portion. The sensor and microcontroller exchange data through an RF link made up of a transmitter and a receiver. The system's receiving portion is made up of an RF receiver, an alarm, and a GSM module. | Transmitting and receiving over a remote area. |  |

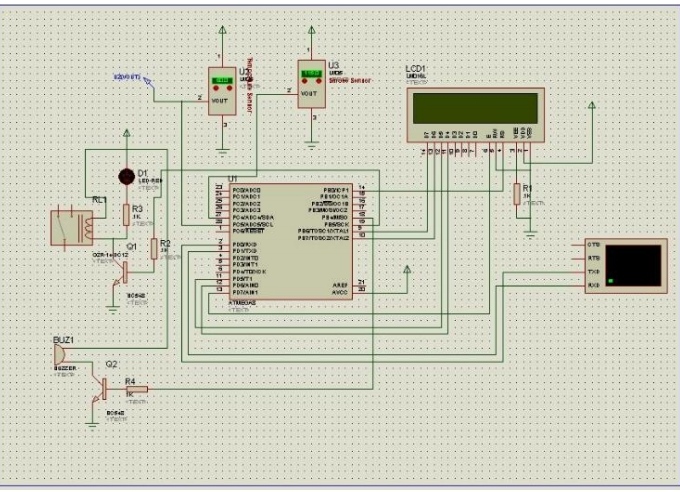
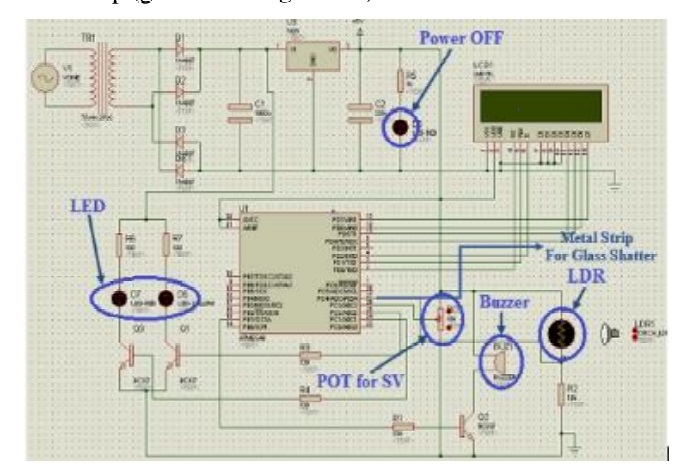
**METHODOLOGY**

The method adopted in this design of a sensor base intrusion system mainly involves the brain using a microcontroller (Atmega8), two sensors; a motion sensor (PIR), fire and temperature sensor connected as an input to the microcontroller, while for the output signals when intrusion is being detected we have three outputs; a LED, buzzer, SMS module to produce alert. Other peripherals component needed are resistors, capacitors, integrated circuit, transistors, diodes, power source. This design is presented with two circuit; one for motion sensing and another for fire/temperature detection. Below the step-by-step representation and it aim to monitor and project the outcome of this system.

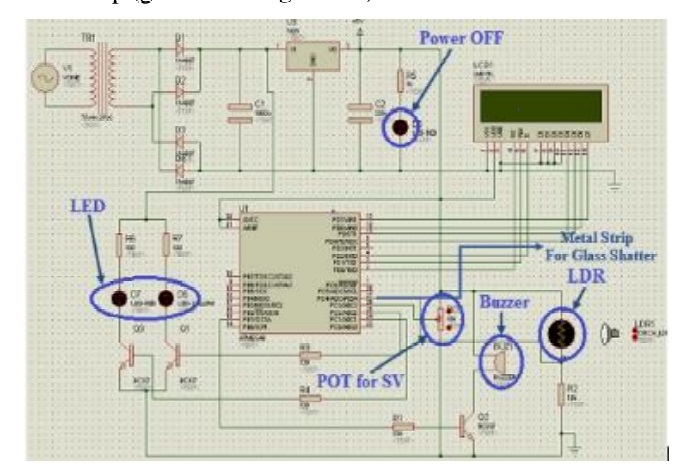
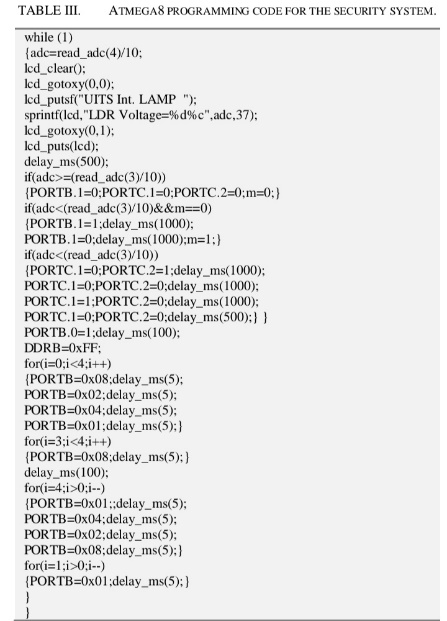
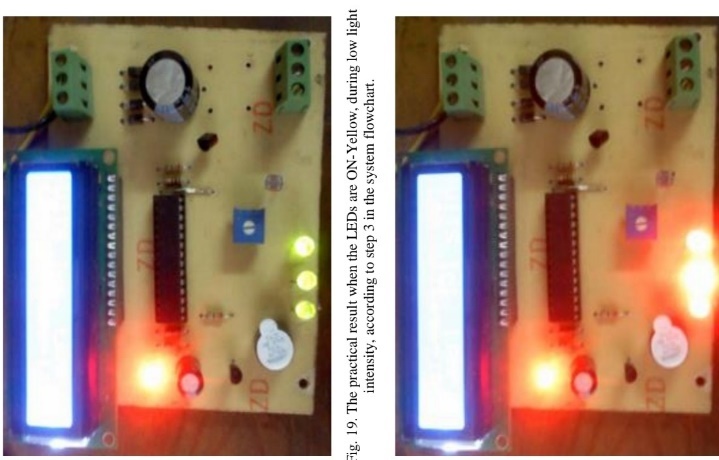


**PROOF OF CONCEPT**

The proof of concept for this sensor-based intrusion detection system was implemented and tested on proteus 7.7 and presented in the figures below



**TANGABLE RESULT**



**PROTOTYPE**

**GANTT CHART**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Tasks | 27th Jan | 5th Feb | 27th Feb | March | Feb. 2024 | Feb. 2024 | March.  2024 |
| Project topic research |  |  |  |  |  |  |  |
| Project topic approval |  |  |  |  |  |  |  |
| Submission of project proposal |  |  |  |  |  |  |  |
| Presentation of project proposal |  |  |  |  |  |  |  |
| Report  Writing |  |  |  |  |  |  |  |
| Submission of report |  |  |  |  |  |  |  |
| Presentation of report |  |  |  |  |  |  |  |

**COST ANALYSIS**

BILL OF ENGINEERING MEASUREMENT AND EVALUATION (BEME)

|  |  |  |
| --- | --- | --- |
| S/N | DESCRIPION OF ITEMS | PRICE (#) |
| 1. | Microprocessor | 5,000 |
| 2. | PIR sensor | 3,000 |
| 3. | SMS module | 6,000 |
| 4. | Buzzer | 2,000 |
| 5. | Intergrated circuit |  |
| 6. | Code for the microprocessor | 50,000 |
| 7. | Relay | 6,000 |
| 8 | Temperature sensor |  |
| 9 | Miscellaneous | 20,000 |
|  | TOTAL |  |

**REFERENCES**

1. SaikumarIyer, P ranjalGaonkar, ShwetaW adekar, N ayanKohmaria and P rashantU padhyay *“IoT based Intruder Detection System Using GSM*” 2021 K J Somaiya Institute of Engineering and Information Technology Mumbai, India.
2. Philokypros P. Ioulianou, Vassilios G. Vassilakis, Ioannis D. Moscholios and Michael D. Logothetis “*A Signature-based Intrusion Detection System for the Internet of Things”* July 2018 White Rose Research Online URL <https://eprints.whiterose.ac.uk/133312/>
3. Khirod Chandra Sahoo and Umesh Chandra Pati *“IoT Based Intrusion Detection System Using PIR Sensor”* 2017 IEEE International Conference on Recent Trends in Electronics Information Communication Technology, May 19-20, 2017, India.
4. Geethanjali T M, RaushaniKumari, Srividya M and Shreeraksha M *“Security System using Arduino”* 2018 International Journal of Computer Trends and Technology (IJCTT) – Volume 60 Issue 2 - June 2018 <https://www.researchgate.net/publication/327935942>
5. Shoewu, O.O., AyangbekunOluwafemi J. and Johnson Emmanuel O *“Design and Construction of Micro-Controller Based Intrusion Detector”* 2020 International Journal of Innovative Research in Electronics and Communications (IJIREC) Volume 7, Issue 3, 2020, PP 1-6 ISSN 2349-4050 (Online) DOI: <http://doi.org/10.20431/2349-4050.0703005>
6. Imran Chowdhury and Taslim Ahmed “*Design and Prototyping of Sensor-based Anti-Theft Security System using Microcontroller”* 2021 International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 IJERTV10IS030019 Vol. 10 Issue 03, March-2021
7. Rao Kamran Javed *“A Novel Approach Using Deep Learning for Network Based Intrusion Detection System”* 2022 Department of Computer Science Federal Urdu University of Arts, Science and Technology Islamabad <https://www.researchgate.net/publication/363639283>
8. Markus Ring, Sarah Wunderlich, Deniz Scheuring, Dieter Landes and Andreas Hotho *“A Survey of Network-based Intrusion Detection Data Sets”*2019 arXiv:1903.02460v2 [cs.CR] 6 Jul 2019
9. Olutosin Taiwo, Absalom E. Ezugwu, Olaide N. Oyelade and Mubarak S. Almutairi *“Enhanced Intelligent Smart Home Control and Security System Based on Deep Learning Model”* 2022 Hindawi Wireless Communications and Mobile Computing Volume 2022, Article ID 9307961, <https://doi.org/10.1155/2022/9307961>
10. Dhanke Jyoti Atul, R. Kamalraj, G. Ramesh, K. Sakthidasan Sankaran, Sudhir Sharma and Syed Khasim *“A machine learning based IoT for providing an intrusion detection system for security”* 2021 Microprocessors and Microsystems 82 (2021) 103741 [www.elsevier.com/locate/micpro](http://www.elsevier.com/locate/micpro)
11. Zipporah Tarus “PIR Sensor-based Security System” 2017 Helsinki Metropolia University of Applied Sciences Bachelor of Engineering Degree in Electronics Thesis.
12. Arya Singh S., Maneesha V. Ramesh and Divya P. “*Design and Simulation of Elephant Intrusion Detection System”* 2016 6th International Workshop on Computer Science and Engineering (WCSE 2016) ISBN 978-981-11-0008-6 Tokyo, Japan, 17-19 June, 2016, pp. 749-753.
13. Prerna Bhatnagar, Vasu Gupta, Sumit Chauhan and Mr. Sandeep Sharma “*Smart Security and Intrusion Prevention System”* 2019 International Journal for Research in Applied Science & Engineering Technology (IJRASET) ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177 Volume 7 Issue XI, Nov 2019
14. Difan Zhang, Wei Yu, and Rommie Hardy *“A Distributed Network-Sensor Based Intrusion Detection Framework in Enterprise Networks”* 2011 Conference Paper · November 2011 DOI: 10.1109/MILCOM.2011.6127462 <https://www.researchgate.net/publication/261091400>
15. Imran, Faisal Jamil and Dohyeun Kim *“An Ensemble of Prediction and Learning Mechanism for Improving Accuracy of Anomaly Detection in Network Intrusion Environments”* Sustainability 2021, 13, 10057. <https://doi.org/10.3390/su131810057>
16. Akeem T. Otapo, Lateef A Saliu, Kazeem A. Sodiq, Mary O. Tokunbo-Cole, Favour U. Okia *“Office- Automated Intrusion Detection System (O-Aids)”* 2019Department of Computer Engineering, Yaba College of Technology, Lagos State, Nigeria
17. Zhi Sun, Pu Wang, Mehmet C. Vuran, Mznah A. Al-Rodhaan, Abdullah M. Al-Dhelaan and Ian F. Akyildiz *“BorderSense: Border patrol through advanced wireless sensor networks”* 2010 Ad Hoc Networks 9 (2011) 468–477 www.elsevier.com/locate/adhoc
18. Abhishek S. Parab and Amol Joglekar *“Implementation of Home Security System using GSM module and Microcontroller”* 2015 (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (3), 2015, 2950-2953
19. Amit Kumar, Anchal Baranwal, Arun Kumar, Brijesh Kumar Kushwaha, Dhanajay Mishra, Deepu Kumar and Varun Singhal *“Border Security System using Arduino & Ultrasonic Sensors”* 2017 International Journal of Scientific Engineering and Technology Research (IJSETR) ISSN 2319-8885 Vol.06, Issue.13 April-2017, Pages:2489-2492
20. Mohamad Huzaimy Jusoh, Muhammad Firdaus Bin Jamali, Ahmad Faizal bin Zainal Abidin, Ahmad Asari Sulaiman and Mohamad Fahmi Hussin *“Wi-Fi and GSM Based Motion Sensor for Home Security System Apllication”* 2015 4th International Conference on Electronic Devices, Systems and Applications 2015 (ICEDSA) IOP Publishing IOP Conf. Series: Materials Science and Engineering 012010 doi:10.1088/1757-899X/99/1/012010