(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :18/10/2021

(21) Application No.202141047283 A
(43) Publication Date : 29/10/2021

(54) Title of the invention : Anti-Theft system based on the Internet of Things (IoT) to monitor unusual movements.

(51) International classification	:H04N0007180000, G08B0013196000, H04W0004700000, G08B0015000000, G08B0013000000
(86) International Application No Filing Date	:PCT// :01/01/1900
(87) International Publication No	: NA
(61) Patent of Addition to Application Number Filing Date	:NA :NA
(62) Divisional to Application Number Filing Date	:NA :NA

(71)**Name of Applicant :**
1)Arumugam Ranjith
Address of Applicant :32 B Mazhuppan street ---------- ----------
2)Mr. Uttam Basu
3)Mr. Nandkishor Balu Gosavi
4)Dr. Yusuf Perwej
5)Mr. S G Nagaraju Valluri
6)Mr.Y. M. MAHABOOBJOHN
7)Dr. Rachit Garg
8)Mr. Keshav Kaushik
9)Dr.Harmandeep Singh Gill
10)Dr. Arun Kumar Pallathadka
11)Dr. Harikumar Pallathadka
Name of Applicant : NA
Address of Applicant : NA
(72)**Name of Inventor :**
1)Mr. Uttam Basu
Address of Applicant :Senior IoT Engineer, Terra Motors India Pvt Ltd. JIS Institute of Advanced Studies and Research, Kolkata 713146, West Bengal, India. ---------- ----------
2)Mr. Nandkishor Balu Gosavi
Address of Applicant :Assistant Librarian SVKM'S NMIMS University Mumbai (Dhule Campus) 424001,Maharashtra, India ---------- ----------
3)Dr. Yusuf Perwej
Address of Applicant :Associate professor Department: computer science and engineering 226001, U.P, India. ---------- ----------
4)Mr. S G Nagaraju Valluri
Address of Applicant :Asst professor Sreenidhi Institute of Science and technology Hyderabad, 500076, Telangana, India. ---------- ----------
5)Mr.Y. M. MAHABOOBJOHN
Address of Applicant :ASSISTANT PROFESSOR MAHENDRA COLLEGE OF ENGINEERING MINNAMPALLI, SALEM , 636106, TAMILNADU INDIA ---------- ----------
6)Dr. Rachit Garg
Address of Applicant :Deputy Secretary Lovely Professional University 144001, Punjab, India. ---------- ----------
7)Mr. Keshav Kaushik
Address of Applicant :Assistant Professor School of Computer Science College: University of Petroleum and Energy Studies Dehradun, Uttarakhand, 248001, India ---------- ----------
8)Dr.Harmandeep Singh Gill
Address of Applicant :Assistant professor (senior scale) in computer science Guru Arjan Dev khalsa college, Chohla Sahib(Tarn Taran) 143408, Punjab , India. ---------- ----------
9)Dr. Arun Kumar Pallathadka
Address of Applicant :Adjunct Director Center for Polar Studies, Manipur International University, Ghari, Imphal, Imphal West, Manipur, India ,795140. ---------- ----------
10)Dr. Harikumar Pallathadka
Address of Applicant :Director Manipur International University, Ghari, Imphal, Imphal West, Manipur , India ,795140 ---------- ----------

(57) Abstract :
When a homeowner or family member becomes aware of an ongoing theft, the suggested research approach seeks to provide a broadly applicable strategy for notifying them (unauthorized access to their premises). This was achieved by doing a thorough examination of current systems in order to identify research requirements. The previous systems' incapacity to differentiate between human and non-human items, as well as their ability to identify the thief only after the crime had occurred, were discovered to be problems. Wireless sensor networks (WSNs) are collaborating with the IoT and the Cognitive Internet of Thing- CIoT to make clever homes and their applications more widely available (CIoT). Researchers have developed a new smart home anti-theft system that can detect intruders even if their faces are partially or fully obscured by clothing or other materials such as leather, fiber, or plastic, according to the researchers. The suggested technique may identify a nocturnal intruder by using a CCTV. The overall aim of this project was to develop a low-cost, high-performance system that anybody could use to identify and report any kind of theft in real time, no matter how little. According to the creators, it would also provide real-time video data processing for home security systems. The study's findings indicate that the suggested method is feasible. When an intruder's face was partially or fully hidden, or when he was seen in the dark, the system's accuracy rose from 85.13 percent to 97.01 percent, 84.13 percent to 78.19 percent, and 66.51 percent, respectively. The accuracy increased from 85.13 percent to 64.13 percent, 56.70 percent, and 44.01 percent in these circumstances.

No. of Pages : 12 No. of Claims : 6

Anti-Theft system based on the Internet of Things (IoT) to monitor unusual movements.

Abstract:

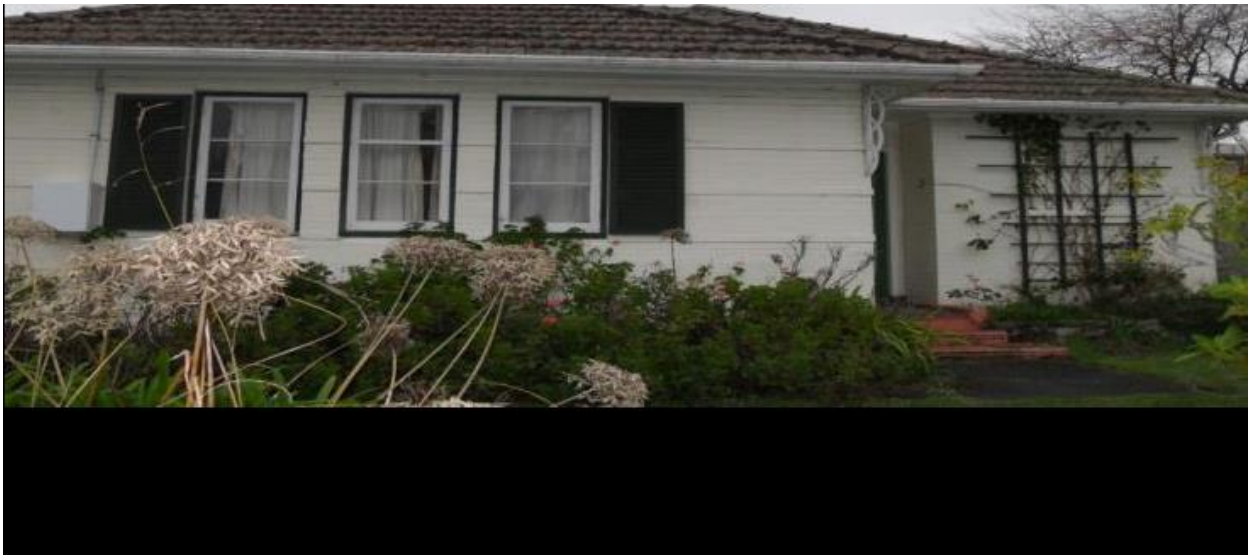
When a homeowner or family member becomes aware of an ongoing theft, the suggested research approach seeks to provide a broadly applicable strategy for notifying them (unauthorized access to their premises). This was achieved by doing a thorough examination of current systems in order to identify research requirements. The previous systems' incapacity to differentiate between human and non-human items, as well as their ability to identify the thief only after the crime had occurred, were discovered to be problems. Wireless sensor networks (WSNs) are collaborating with the IoT and the Cognitive Internet of Thing- CIoT to make clever homes and their applications more widely available (CIoT). Researchers have developed a new smart home anti-theft system that can detect intruders even if their faces are partially or fully obscured by clothing or other materials such as leather, fiber, or plastic, according to the researchers. The suggested technique may identify a nocturnal intruder by using a CCTV. The overall aim of this project was to develop a low-cost, high-performance system that anybody could use to identify and report any kind of theft in real time, no matter how little. According to the creators, it would also provide real-time video data processing for home security systems. The study's findings indicate that the suggested method is feasible. When an intruder's face was partially or fully hidden, or when he was seen in the dark, the system's accuracy rose from 85.13 percent to 97.01 percent, 84.13 percent to 78.19 percent, and 66.51 percent, respectively. The accuracy increased from 85.13 percent to 64.13 percent, 56.70 percent, and 44.01 percent in these circumstances.

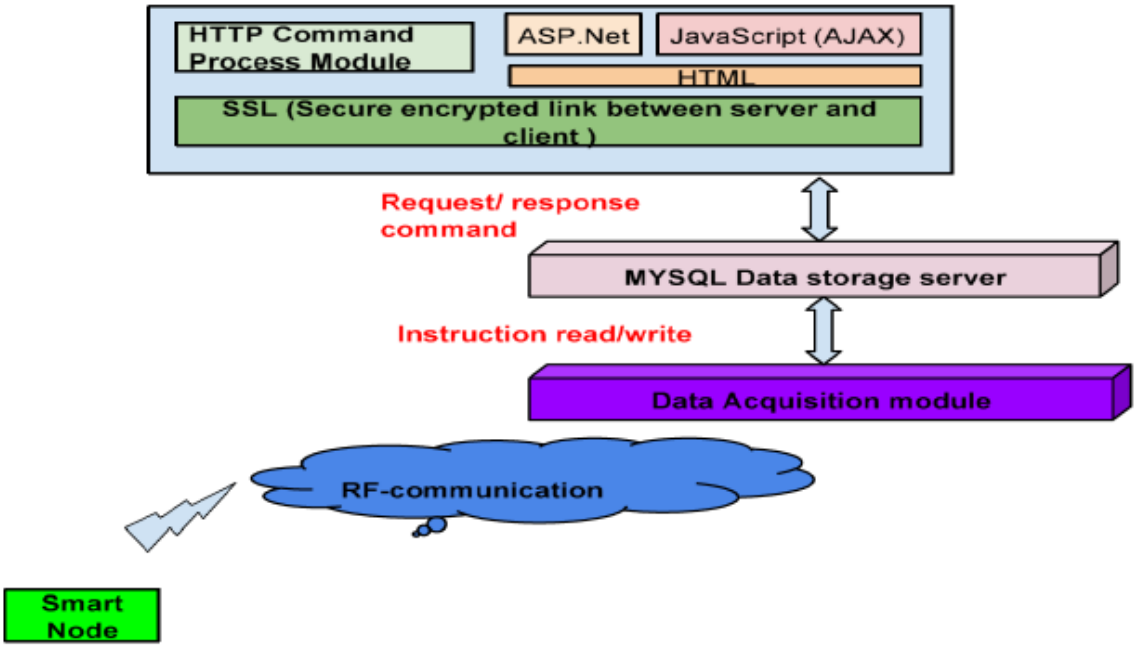
Descriptions:

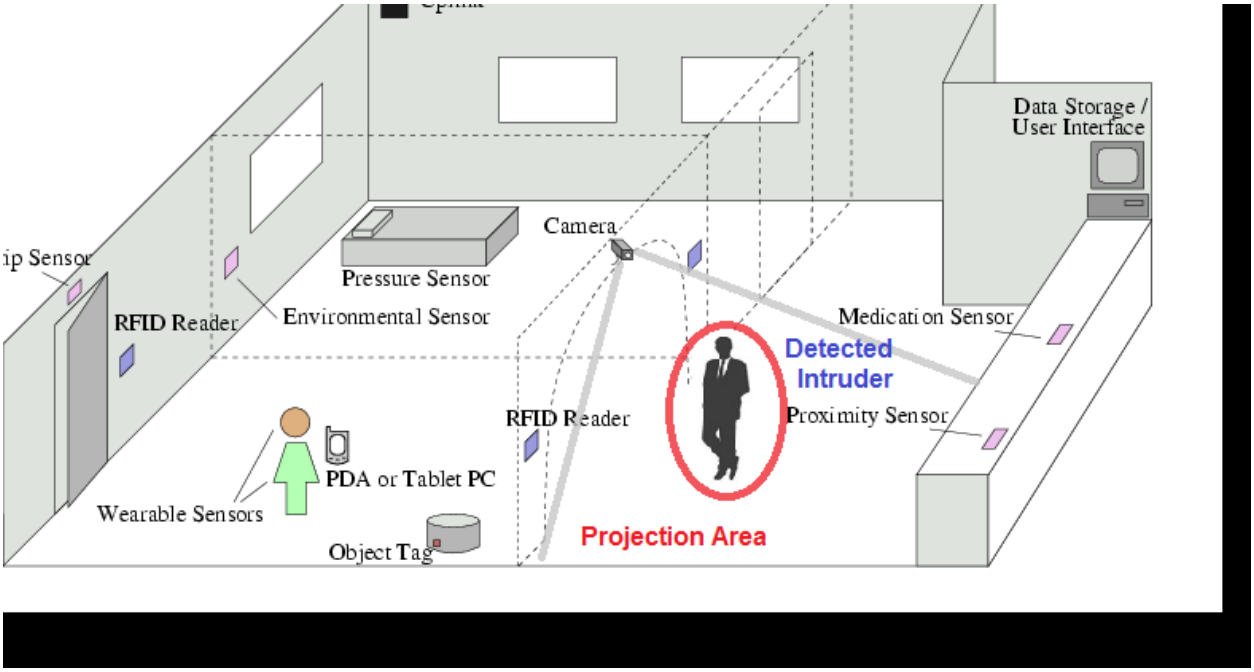
The use of technology to improve the overall comfort of contemporary houses is a well-established field of study and research, and the smart home is no exception. Since the Internet has become an important element of wide communication in contemporary life, the Internet of Things (IoT) has enabled houses to evolve from basic structures to interactive settings. The Internet of Things is being used in many areas of human life at an exponential pace, including environmental monitoring, home management, and cloud storage of data produced by devices in the home. A smart house is made up of many components, technologies, and devices that produce valuable data that can be used to anticipate actions both inside and outside the home. Keeping oneself and one's surroundings safe and secure are top concerns in today's society. As a consequence of terrorist-related robberies and thefts, there is an urgent need for effective video surveillance systems as well as on-site alerts to property owners and other family members of ongoing crimes. There are now closed-circuit TV cameras and digital video on the market that can capture trespassers' illegal actions but cannot differentiate between human and non-human objects. Systems from the past can't recognize faces when they're partly or completely obscured, so they can't give a real-time theft warning to the home's owner. It's also tough for older systems to identify an intruder in the dark when they're using CCTV cameras that don't have night vision. To utilize such a system, someone must be at home or a member of the family must be accessible at all times, which is almost impossible to accomplish manually [3–5]. When a potential theft is discovered, it is time-consuming to look through all of the recorded video footage one by one. There's a possibility the storage server has a large amount of private video from family members that can't be utilized to track

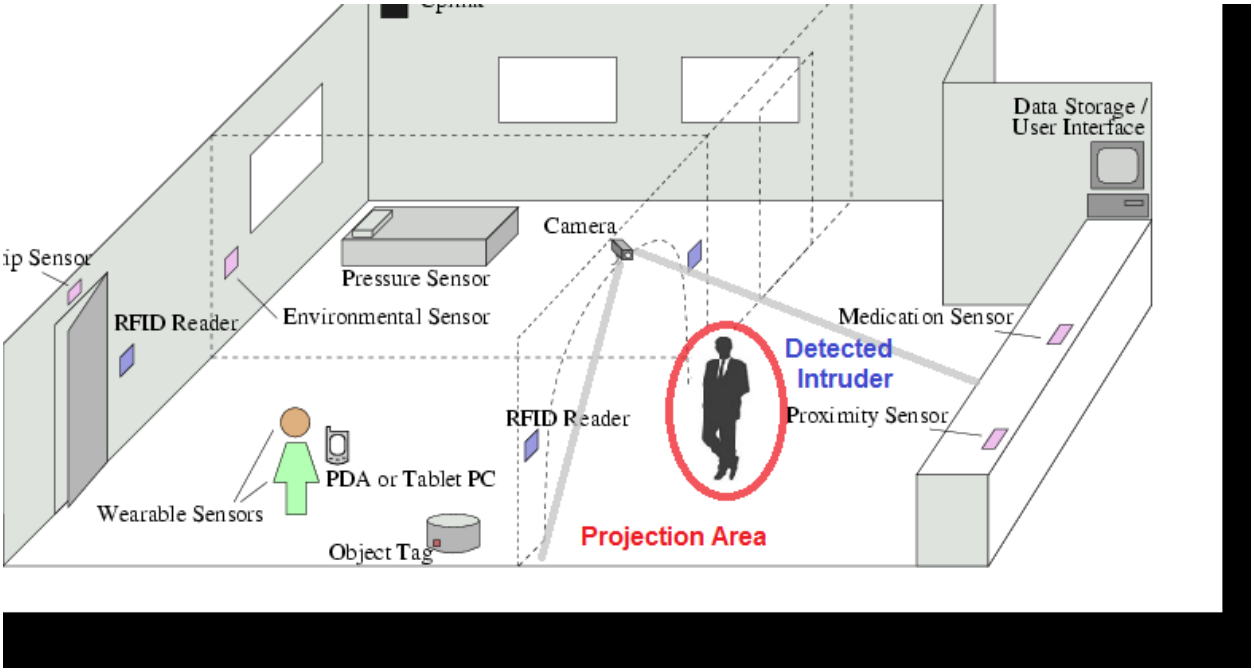
down trespassers. The suggested method may be used to give near-real-time feedback in a smart home monitoring system based on the Internet of Things. Figures 1 and 2 depict schematics for a smart house outfitted with sensors, cameras, and specialized hardware for detecting and assessing illegal entry. Through a hardware interface that comprises an intelligent sensor node linked to a central sensor node, data is identified and transmitted to a storage server for storage. Among the functions contained in the software modules are data logging, data retrieval, and data storage. To identify and report on unsupervised human behavior, the program employs massive data processing methods that are as near to real time as feasible. The presentation that follows provides an overview of the project. The first part discusses legacy systems, possible problems, and the social effect they have. Section 2 discusses the importance of the study as well as the reasons for its implementation. This section also discusses the system's intelligent characteristics, such as its ability to identify veiled faces using graphical and statistical techniques. Section 3 goes on to describe the system's architecture and experimental setup. A description of how to recognize veiled faces and detect an intruder in complete darkness is also given. Section 4 is divided into three sections, each with three elements: a graphical analysis and statistical findings. The methods are presented in three parts in Section 4. The findings of the research are presented in detail in the last section (Section 5). The figure below depicts an overview of the sensor devices. Monitoring and managing a smart home occurs on two levels: hardware and code. The sensor configurations are built into the machine's structure. An impact sensor has been added to the BSS. A remote BSS gathers data about people in various physiological states. Physiological monitoring sensors may be installed in smart house residents' dwellings without interfering with their regular activities.

DRAWINGS:




HTTP Command Process Module
ASP.Net
JavaScript (AJAX)
HTML
SSL (Secure encrypted link between server and client)
Request/ response command
MYSQL Data storage server
Instruction read/write
Data Acquisition module
RF-communication
Smart Node


Data Storage /
User Interface
Camera
ip Sensor
Pressure Sensor
RFID Reader
Environmental Sensor
Medication Sensor
Detected
Intruder
RFID Reader
Proximity Sensor
PDA or Tablet PC
Wearable Sensors
Object Tag
Projection Area


Data Storage /
User Interface
Camera
ip Sensor
Pressure Sensor
RFID Reader
Environmental Sensor
Medication Sensor
Detected
Intruder
RFID Reader
Proximity Sensor
PDA or Tablet PC
Wearable Sensors
Object Tag
Projection Area

CLAIMS

1. Anti-Theft system based on the Internet of Things (IoT) to monitor unusual movements consist of wireless sensor, camera, DVR, RFID, eye and face detection, display module etc.,

2. Anti-Theft system based on the Internet of Things (IoT) to monitor unusual movements of claim 1, wherein said this study proposes a novel way to keep smart homes safe from burglary by sending out automatic notifications whenever an intruder is detected.

3. Anti-Theft system based on the Internet of Things (IoT) to monitor unusual movements of claim 1, wherein said new wireless sensing technology has been developed as a result of the study to monitor and identify a human intruder while also sending an instantaneous notice of the incursion to deter theft.

4. Anti-Theft system based on the Internet of Things (IoT) to monitor unusual movements of claim 1, wherein said that the technology can detect human intruders and avoid false alerts.

5. Anti-Theft system based on the Internet of Things (IoT) to monitor unusual movements of claim 1, wherein said that the performance metrics for intruder detection are recorded for four situations.

6. Anti-Theft system based on the Internet of Things (IoT) to monitor unusual movements of claim 1, wherein stated that as more goods link the online and physical worlds, new security and privacy research problems have emerged.